





## **D7.3 Pilot execution report in Tallinn**

Work Package	7
Task	7.2
Authors	A. Roberts, L. Luts, F. Pornet, R. Mancilla, L. Bianconi, L. Tarchi, S. Haddad, A. Giannakoulias, P. Devito, D. David
Dissemination Level	Public
Status	Final
Due Date	15.08.2022 (review) 31.08.2022 (initial)
Document Date	29.08.2022
Version Number	1.0

#### **Quality Control**

Name		Organisation	Date
Editor	L. Luts	TALLINN	15.08.2022
Peer review 1	Konstantinos Maliatsos	UPRC	29.08.2022
Peer review 2	Amedeo D'Arcangelo	KSP	29.08.2022
Authorised by (Technical Coordinator)	Jason Sioutis	ICCS	30.08.2022
Authorised by (Quality Manager)	Vasileios Sourlas	ICCS	30.08.2022
Submitted by (Project Coordinator)	Angelos Amditis	ICCS	31.08.2022

# CitySCAPE



#### Contributors

Name	Organisation	Date
L. Luts	TALLINN	01.08.2022
A. Roberts	TALTECH	15.08.2022
F. Pornet	ACS	15.08.2022
R. Mancilla	ENG	18.08.2022
L. Bianconi	SIGLA	23.08.2022
L. Tarchi	SIGLA	23.08.2022
S. Haddad	OPPIDA	22.08.2022
A. Giannakoulias	ED	22.08.2022
P. Devito	STAM	15.08.2022
D. David	DNSC	23.08.2022

#### **Document Revision History**

Version	Date	Modification	Partner		
0.1	01.08.2022	Creation of ToC	TALLINN		
0.2	17.08.2022	Added contents	TALLINN, TALTECH		
0.3	22.08.2022	Document reviewed for second iteration of contributes	TALLINN, TALTECH, ICCS,		
0.4	25.08.2022	Added contents	TALLINN, TALTECH, STAM, ED, OPPIDA, ENG, DNSC, SIGLA, ACS		
0.5	29.08.2022	Added contents	TALLINN, TALTECH, STAM, ED, OPPIDA, ENG, DNSC, SIGLA, ACS		
0.6	29.08.2022	Final version of the document internally reviewed	TALLINN, TALTECH, ICCS,		
0.7	30.08.2022	Final version of the document ready for final quality control	TALLINN		
0.8	30.08.2022	Quality control	ICCS		
Final version 1.0	31.08.2022	Final version of the document ready for submission	ICCS		

# CitySCAPE

#### Legal Disclaimer

CitySCAPE is an EU project funded by the Horizon 2020 research and innovation programme under grant agreement No. 883321. The information and views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The CitySCAPE Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.







## **Table of Contents**

List of Tables		6
LIST OF FIGUR	ES	6
List of Abbrev	viations and Acronyms	8
Executive Sum	mary	10
1 Introductio	n	11
1.1 Project	Introduction	11
1.2 Deliver	able Purpose	11
2 Methodolo	gy	12
3 Infrastructu	ure deployment	13
3.1 Tallinn	CPAAS infrastructure table	13
3.2 CitySC	APE toolkit	14
4 Cityscape T	allinn pilot	15
4.1 Overvie	9W	15
4.2 Low-Le	evel Deployment Timeline	15
4.3 Cybers	ecurity Test Case Scenarios	17
	t Case 1: Availability of AV Shuttle Network Comr	munication
17		
4.3.1.1	Pilot scenario description	
4.3.1.2	Attack scenarios	
4.3.1.3	Modules behaviour	21
4.3.1.3.1	SIEM	
4.3.1.3.2	IDS/IPS engine	24
4.3.1.3.3	RITA	
4.3.1.3.4	FIMCA	32
4.3.1.3.4.1	Tangible assets	32
4.3.1.3.4.2	Intangible assets	37
4.3.1.3.5	CTIP	43
4.3.1.3.6	CSIRP	44
	st Case 2: Integrity of Multi-Modal Intelligent ure	-
4.3.2.1	Pilot scenario description	44
4.3.2.2	Attack scenarios	47
4.3.2.3	Modules behaviour	48
4.3.2.3.1	SIEM	48

## 

CitySCAPE		1
4.3.2.3.2	IDS/IPS engine	
4.3.2.3.3	RITA	
4.3.2.3.4	XSOAR	53
4.3.2.3.5	CTIP	53
4.3.2.3.6	CSIRP	53
4.3.2.4	Future activities	53
4.3.3 Tes System 53	t Case 3: Fraudulent manipulation of the Payment Val	idation
4.3.3.1	Test-case scope	53
4.3.3.2	Attack scenarios	54
4.3.3.2.1	Outcome of the vulnerable PoC study	55
4.3.3.2.2	Future activities	55
4.3.4 Tes	t Case 4: Integrity of GNSS System	55
4.3.4.1	Test-case scope	55
4.3.4.2	Attack scenarios	57
4.3.4.3	Outcomes	58
4.3.4.4	Future activities	58
	t Case 5: Transport Data Integration with Mobile App /e)	
4.3.5.1	Test-case scope	59
4.3.5.2	Attack scenarios	63
4.3.5.2.1	Scenario A	64
4.3.5.2.2	Scenario B	64
4.3.5.2.3	Scenario C	66
4.3.5.2.4	Scenario D	68
4.3.5.3	Outcomes	68
4.3.5.4	Future activities	68
Conclusions		69
ANNEX I - IDS/I	PS engine user guide	70
ANNEX II - RITA	Test-Case 1 Demo Functionality	79
ANNEX III - RITA	A Test-Case 2 Demo Functionality	
ANNEX IV - CTI	exchange with DNSC	103

.\*\*\*.



## **List of Tables**

Table 1. CitySCAPE toolkit modules used in Tallinn pilot	14
Table 2. Low-Level Deployment Timeline	16
Table 3. Assets involved in the scenario 1	19
Table 4. Additional Technologies used in Tallinn pilot	26
Table 5. Countermeasure's data for "secured" configuration	35
Table 6. Assets involved in the scenario 2	47
Table 7. Assets involved in the scenario 3	54
Table 8. Assets involved in the scenario 4	57
Table 9. Elements of Transport Data Integration with SIGLA App	

## **LIST OF FIGURES**

Figure 1. Tallinn CPaaS infrastructure	13
Figure 2. Tallinn High-Level CPaaS Assets	14
Figure 3. Sub-testcase 1.1 involved element	20
Figure 4. Sub-testcase 1.2 scanning targets	20
Figure 5. Sub-testcase 1.2 DoS target	21
Figure 6. Alerts received to Greylog	
Figure 7. Aggregated alert sent to the XSOAR component	21
Figure 8. Received messages transmitted to XSOAR component	22
Figure 9. XSOAR receives alerts from Graylog	
Figure 10. Alerts displayed in incident dashboard	23
Figure 11. Incident description	
Figure 12. XSOAR provided description of the actions to the handling of	the
incident	
Figure 13. SYN flood attack	
Figure 14. CityScape IDS/IPS engine internal architecture	
Figure 15. IDS/IPS engine log with the alerts generated for test case 1	
Figure 16. IDS/IPS engine alerts viewed through the GUI for Test case 1.1.	
Figure 17. IDS/IPS alerts generated during test case 1.2, no alerts related	d to
FTP protocol	
Figure 18. Overall Risk and Impact	
Figure 19. Taltech TeleOperation Business Service (Basic Information)	
Figure 20. Taltech TeleOperation Business Service (Composite Assets)	
Figure 21. AV TeleOperation Server (AV Control PC OS-Ubuntu Threats o	
Likehoods)	
Figure 22. FIMCA Homepage	
Figure 23. Input data (i)	
Figure 24. Input data (ii)	
Figure 25. Input data (iii)	
Figure 26. Results of FIMCA - tangible assets	
Figure 27. FIMCA Integration Architecture	
Figure 28. FIMCA Security configuration	
Figure 29. FIMCA impact evaluation	
Figure 30. FIMCA list of composite assets	
Figure 31. FIMCA suggestion of the possible impacts	
Figure 32. FIMCA Mont-Carlo simulation results	41





CITYSCALE	* * *
Figure 33. FIMCA calculated statistical values for CBA	41
Figure 34. ROSI formula and its parameters	
Figure 35. Three different values of ROSI (confidentiality, i	ntegrity,
availability)	
Figure 36. CSIRP analyst created	
Figure 37. Sub-test case 2.2 involved elements	48
Figure 38. Graylog receives alerts from the IDS/IPS component	48
Figure 39. IDS/IPS unique alerts generated during sub-testcase 2.1	49
Figure 40. All the IDS/IPS alerts related to PostgreSQL brute force ge	enerated
during the sub-testcase 2.1	49
Figure 41. AV Shuttle Network Communication Overall Risk and Imp	bact50
Figure 42. AV Shuttle Network Communication Business Servic	e (Basic
Information)	51
Figure 43. AV Shuttle Network Communication Business Service (Co	mposite
Assets)	52
Figure 44. Test case 4.2 involved elements	58
Figure 45. Mob-Sec CitySCAPE deployment architecture	63
Figure 46. SiglaMoving App	64
Figure 47. Selected provider	65
Figure 48. Routes and timetables	65
Figure 49. Bus line and stops	
Figure 50. Selected bus lines	67
Figure 51. Bus line information and arrival time	67



## List of Abbreviations and Acronyms

ACS         Airbus Cyber Security           AV         Autonomous Vehicle           AMT         AMT Genova           BiBo         Bounded-input, Bounded-output           CBA         Cost-Benefit Analysis           CERT/CIRT         Computer Emergency Response Team/ Cyber Incident Response Team           CPaaS         Communications Platform as a Service           CSIRP         Collaborative security incident response platform           CTI         computer-telephony integration           CTIP         Collaborative threat investigation platform           DNSC         DNSC Romania           DoA         Description of Action           ED         European Dynamics           ENG         Engineering           FIMCA         Financial impact assessment engine           GDPR         General Data Protection Regulation           GUI         Graphical user interface           HTTP         Hypertext Transfer Protocol           ICCS         Institute of Communication and Computer Systems           IOC         Indicators of Compromise           IPS         Intrusion Prevention Systems           IOC         Indicators of Compromise           IPS         Intrusion Prevention Systems           IOC         In	Abbreviation	Meaning			
AV       Autonomous Vehicle         AMT       AMT Genova         BiBo       Bounded-input, Bounded-output         CBA       Cost-Benefit Analysis         CERT/CIRT       Computer Emergency Response Team/ Cyber Incident Response Team         CPaaS       Communications Platform as a Service         CSIRP       Collaborative security incident response platform         CTI       computer-telephony integration         CTIP       Collaborative threat investigation platform         DNSC       DNSC Romania         DoA       Description of Action         ED       European Dynamics         ENG       Engineering         FIMCA       Financial impact assessment engine         GDPR       General Data Protection Regulation         GUI       Graphical user interface         HTTP       Hypertext Transfer Protocol         ICCS       Institute of Communication and Computer Systems         IOC       Intrusion Detection Systems         IOC       Intrusion Prevention Systems         IOC					
AMT       AMT Genova         BiBo       Bounded-input, Bounded-output         CBA       Cost-Benefit Analysis         CERT/CIRT       Computer Emergency Response Team/ Cyber Incident Response Team         CPaaS       Communications Platform as a Service         CSIRP       Collaborative security incident response platform         CTI       computer-telephony integration         CTIP       Collaborative threat investigation platform         DNSC       DNSC Romania         DoA       Description of Action         ED       European Dynamics         ENG       Engineering         FIMCA       Financial impact assessment engine         GDPR       General Data Protection Regulation         GUI       Graphical user interface         HTTP       Hypertext Transfer Protocol         ICCS       Institute of Communication and Computer Systems         IOC       Institute of Commonise         IPS       Intrusion Prevention Systems         IOC       Institute of Compromise         IPS       Intrusion Prevention Systems         IOC       Institute of Information Sharing Platform         OPP       Oppida         PT       Public Transport         RITA       Risk analysi					
BiBo       Bounded-input, Bounded-output         CBA       Cost-Benefit Analysis         CERT/CIRT       Computer Emergency Response Team/ Cyber Incident Response Team         CPaaS       Communications Platform as a Service         CSIRP       Collaborative security incident response platform         CTI       computer-telephony integration         CTIP       Collaborative threat investigation platform         DNSC       DNSC Romania         DoA       Description of Action         ED       European Dynamics         ENG       Engineering         FIMCA       Financial impact assessment engine         GDPR       General Data Protection Regulation         GNSS       Global Navigation Satellite System         GUI       Graphical user interface         HTTP       Hypertext Transfer Protocol         ICCS       Institute of Communication and Computer Systems         IDS       Intrusion Detection Systems         IOC       Indicators of Compromise         IPS       Intrusion Prevention Systems         IDS       Intrusion Prevention Systems         IOC       Indicators of Compromise         IPS       Intrusion Prevention Systems         IDS       Intrusion Prevention Systems					
CBA       Cost-Benefit Analysis         CERT/CIRT       Computer Emergency Response Team         CPaaS       Communications Platform as a Service         CSIRP       Collaborative security incident response platform         CTI       computer-telephony integration         CTIP       Collaborative threat investigation platform         DNSC       DNSC Romania         DoA       Description of Action         ED       European Dynamics         ENG       Engineering         FIMCA       Financial impact assessment engine         GDPR       General Data Protection Regulation         GNSS       Global Navigation Satellite System         GUI       Graphical user interface         HTTP       Hypertext Transfer Protocol         ICCS       Institute of Communication and Computer Systems         IOC       Indicators of Compromise         IPS       Intrusion Prevention Systems         IOC       Ind					
CERT/CIRT       Computer Emergency Response Team         CPaaS       Communications Platform as a Service         CSIRP       Collaborative security incident response platform         CTI       computer-telephony integration         CTIP       Collaborative threat investigation platform         DNSC       DNSC Romania         DoA       Description of Action         ED       European Dynamics         ENG       Engineering         FIMCA       Financial impact assessment engine         GDPR       General Data Protection Regulation         GNSS       Global Navigation Satellite System         GUI       Graphical user interface         HTTP       Hypertext Transfer Protocol         ICCS       Institute of Communication and Computer Systems         IOC       Indicators of Compromise         IPS       Intrusion Detection Systems         IOC       Indicators of Compromise         IPS       Intrusion Prevention Sharing         PDF       Oppida         PT       Public Transport         RITA       Risk analysis and impact assessment engine         RFILS       Real-time location system         SFTP       Secure file transfer protocol         SIEM       SIEM as		· · · · · ·			
Team/CyberIncidentResponseCPaaSCommunicationsPlatform as a ServiceCSIRPCollaborativesecurityincident response platformCTIcomputer-telephony integrationCTIPCollaborative threatinvestigation platformDNSCDNSC RomaniaDoADescription of ActionEDEuropean DynamicsENGEngineeringFIMCAFinancialimpactassessment engineGDPRGeneral Data Protection Regulation GNSSGUIGraphical user interfaceHTTPHypertext Transfer ProtocolICCSInstitute of Communication and Computer SystemsIDSIntrusion Detection SystemsIDSIntrusion Prevention SystemsIDSIntrusion Prevention SystemsIDSMalwareInformationSharing PlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers		J. J			
ServiceCSIRPCollaborative security incident response platformCTIcomputer-telephony integrationCTIPCollaborative threat investigation platformDNSCDNSC RomaniaDoADescription of ActionEDEuropean DynamicsENGEngineeringFIMCAFinancial impact assessment engineGDPRGeneral Data Protection RegulationGUIGraphical user interfaceHTTPHypertext Transfer ProtocolICCSInstitute of Communication and Computer SystemsIDSIntrusion Detection SystemsIOCIndicators of CompromiseIPSIntrusion Prevention SystemsIDCIndicators of CompromiseIPSKasperskyLANLocal area networkMISPMalware Information Sharing PlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers		Team/ Cyber Incident Response Team			
response platformCTIcomputer-telephony integrationCTIPCollaborative threat investigation platformDNSCDNSC RomaniaDoADescription of ActionEDEuropean DynamicsENGEngineeringFIMCAFinancial impact assessment engineGDPRGeneral Data Protection Regulation GNSSGUIGraphical user interfaceHTTPHypertext Transfer ProtocolICCSInstitute of Communication and Computer SystemsIDSIntrusion Detection SystemsIOCIndicators of CompromiseIPSIntrusion Prevention SystemsIOCIndicators of CompromiseIPSIntrusion Prevention SystemsIOCIndicators of CompromiseIPSRasperskyLANLocal area networkMISPMalware Information Sharing PlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	CPaaS				
CTIPCollaborative threat investigation platformDNSCDNSC RomaniaDoADescription of ActionEDEuropean DynamicsENGEngineeringFIMCAFinancial impact assessment engineGDPRGeneral Data Protection RegulationGNSSGlobal Navigation Satellite SystemGUIGraphical user interfaceHTTPHypertext Transfer ProtocolICCSInstitute of Communication and Computer SystemsIDSIntrusion Detection SystemsIOCIndicators of CompromiseIPSIntrusion Prevention SystemsKSPKasperskyLANLocal area networkMISPMalware Information Sharing PlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers		response platform			
platformDNSCDNSC RomaniaDoADescription of ActionEDEuropean DynamicsENGEngineeringFIMCAFinancial impact assessment engineGDPRGeneral Data Protection RegulationGNSSGlobal Navigation Satellite SystemGUIGraphical user interfaceHTTPHypertext Transfer ProtocolICCSInstitute of Communication and Computer SystemsIDSIntrusion Detection SystemsIOCIndicators of CompromiseIPSIntrusion Prevention SystemsKSPKasperskyLANLocal area networkMISPMalware Information Sharing PlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers					
DoADescription of ActionEDEuropean DynamicsENGEngineeringFIMCAFinancial impact assessment engineGDPRGeneral Data Protection RegulationGNSSGlobal Navigation Satellite SystemGUIGraphical user interfaceHTTPHypertext Transfer ProtocolICCSInstitute of Communication and Computer SystemsIDSIntrusion Detection SystemsIOCIndicators of CompromiseIPSIntrusion Prevention SystemsISPKasperskyLANLocal area networkMISPMalwarePTPublic TransportRITARisk analysis and impact assesment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	CTIP	Ŭ			
EDEuropean DynamicsENGEngineeringFIMCAFinancial impact assessment engineGDPRGeneral Data Protection RegulationGNSSGlobal Navigation Satellite SystemGUIGraphical user interfaceHTTPHypertext Transfer ProtocolICCSInstitute of Communication and Computer SystemsIDSInstitute of Communication and Computer SystemsIOCIndicators of CompromiseIPSIntrusion Detection SystemsKSPKasperskyLANLocal area networkMISPMalware Information Sharing PlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	DNSC	DNSC Romania			
ENGEngineeringFIMCAFinancial impact assessment engineGDPRGeneral Data Protection RegulationGNSSGlobal Navigation Satellite SystemGUIGraphical user interfaceHTTPHypertext Transfer ProtocolICCSInstitute of Communication and Computer SystemsICCSInstitute of Communication and Computer SystemsIDSIntrusion Detection SystemsIOCIndicators of CompromiseIPSIntrusion Prevention SystemsKSPKasperskyLANLocal area networkMISPPlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	DoA	Description of Action			
ENGEngineeringFIMCAFinancial impact assessment engineGDPRGeneral Data Protection RegulationGNSSGlobal Navigation Satellite SystemGUIGraphical user interfaceHTTPHypertext Transfer ProtocolICCSInstitute of Communication and Computer SystemsICCSInstitute of Communication and Computer SystemsIDSIntrusion Detection SystemsIOCIndicators of CompromiseIPSIntrusion Prevention SystemsKSPKasperskyLANLocal area networkMISPPlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	ED	European Dynamics			
engineGDPRGeneral Data Protection RegulationGNSSGlobal Navigation Satellite SystemGUIGraphical user interfaceHTTPHypertext Transfer ProtocolICCSInstitute of Communication and Computer SystemsICCSInstitute of Communication and Computer SystemsIDSIntrusion Detection SystemsIOCIndicators of CompromiseIPSIntrusion Prevention SystemsKSPKasperskyLANLocal area networkMISPMalware Information Sharing PlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	ENG				
GDPRGeneral Data Protection RegulationGNSSGlobal Navigation Satellite SystemGUIGraphical user interfaceHTTPHypertext Transfer ProtocolICCSInstitute of Communication and Computer SystemsICCSInstitute of Communication and Computer SystemsIDSIntrusion Detection SystemsIOCIndicators of CompromiseIPSIntrusion Prevention SystemsKSPKasperskyLANLocal area networkMISPMalware Information Sharing PlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	FIMCA	Financial impact assessment			
GNSSGlobal Navigation Satellite SystemGUIGraphical user interfaceHTTPHypertext Transfer ProtocolICCSInstitute of Communication and Computer SystemsICCSInstitute of Communication and Computer SystemsIDSIntrusion Detection SystemsIOCIndicators of CompromiseIPSIntrusion Prevention SystemsKSPKasperskyLANLocal area networkMISPMalware Information Sharing PlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	GDPR	-			
GUIGraphical user interfaceHTTPHypertext Transfer ProtocolICCSInstitute of Communication and Computer SystemsICCSInstitute of Communication and Computer SystemsIDSIntrusion Detection SystemsIOCIndicators of CompromiseIPSIntrusion Prevention SystemsKSPKasperskyLANLocal area networkMISPMalware Information Sharing PlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers					
HTTPHypertext Transfer ProtocolICCSInstitute of Communication and Computer SystemsICCSInstitute of Communication and Computer SystemsIDSIntrusion Detection SystemsIOCIndicators of CompromiseIPSIntrusion Prevention SystemsKSPKasperskyLANLocal area networkMISPMalware Information Sharing PlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers					
ICCSInstitute of Communication and Computer SystemsICCSInstitute of Communication and Computer SystemsIDSIntrusion Detection SystemsIOCIndicators of CompromiseIPSIntrusion Prevention SystemsKSPKasperskyLANLocal area networkMISPMalware Information Sharing PlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers					
ICCSInstitute of Communication and Computer SystemsIDSIntrusion Detection SystemsIOCIndicators of CompromiseIPSIntrusion Prevention SystemsKSPKasperskyLANLocal area networkMISPMalware Information Sharing PlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	ICCS	Institute of Communication and			
IDSIntrusion Detection SystemsIOCIndicators of CompromiseIPSIntrusion Prevention SystemsKSPKasperskyLANLocal area networkMISPMalware Information Sharing PlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	ICCS	Institute of Communication and			
IPSIntrusion Prevention SystemsKSPKasperskyLANLocal area networkMISPMalware Information Sharing PlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	IDS				
IPSIntrusion Prevention SystemsKSPKasperskyLANLocal area networkMISPMalware Information Sharing PlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	IOC	Indicators of Compromise			
LANLocal area networkMISPMalware Information Sharing PlatformOPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	IPS				
MISPMalware PlatformInformation Sharing PlatformOPPOppidaPTPublic TransportRITARisk assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	KSP	Kaspersky			
OPPOppidaPTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	LAN	Local area network			
PTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	MISP	_ · · · · · · · · · · · · · · · · · · ·			
PTPublic TransportRITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	OPP	Oppida			
RITARisk analysis and impact assessment engineRTLSReal-time location systemSFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	PT				
SFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	RITA	Risk analysis and impact			
SFTPSecure file transfer protocolSIEMSIEM as a Correlation engine with backlog of markers	RTLS	Real-time location system			
SIEM SIEM as a Correlation engine with backlog of markers	SFTP	Secure file transfer protocol			
		SIEM as a Correlation engine with			
	SIGLA				

<u>டி இத்தி</u> CitySCAPE			
SOAR	Security orchestration, automation and response		
XSOAR	Comprehensive security orchestration, automation and response (SOAR) platform		
STAM	StamTech		
Tallinn	City of Tallinn		
TalTech	Tallinn University of Technology		
UPRC	University of Piraeus Research Center		
VPN	Virtual Private Network		
XSOAR	Comprehensive security orchestration, automation and response platform		





## **Executive Summary**

This deliverable presents the results of the work conducted during Task 7.2 entitled "Pilot demonstrator - Tallinn". The main objectives of the task were to demonstrated cybersecurity test cases on the multi-modal transportation business services and assets in the Tallinn transportation ecosystem. Current deliverable specifies the procedures of the conducted Tallinn pilot with a detailed description of the progress.

The first part of the deliverable includes Tallinn CpaaS infrastructure with assets and interactions, to have a better overview of the nature of the testcase. Involvement of the modules from CitySCAPE toolkit are presented in detail.

The second part of the document is dedicated to a comprehensive overview of the conducted pilot with low-level timelines, high-level outcomes and description of the activities performed in preparatory phase from 1<sup>st</sup> of July and during actual testing on 24<sup>th</sup> and 25<sup>th</sup> of August.

The final part of this deliverable breaks down each test-case into details, including scenario description, assets involved, defined attack scenarios and modules used in demonstration.

This document reports the results of demonstrating the benefits and usability of the CitySCAPE toolkit for detecting cyber-attacks and for cyber incident response in the multi-modal transport environment.

## **1 INTRODUCTION**

## **1.1 Project Introduction**

The traditional security controls and security assurance arguments are becoming increasingly inefficient in supporting the emerging needs and applications of the interconnecting transport systems, allowing threats and security incidents to disturb all dimensions of transportation.

CitySCAPE is a project funded by the EU's Horizon 2020 research and innovation program, which consists of 15 partners from 6 European countries united in their vision to cover the cybersecurity needs of the multimodal transportation.

More specifically, the CitySCAPE software toolkit will:

- ✓ Detect suspicious traffic-data values and identify persistent threats
- ✓ Evaluate an attack's impact in both technical and financial terms
- Combine external knowledge and internally-observed activities to enhance the predictability of zero-day attacks
- ✓ Instantiate a networked overlay to circulate informative notifications to CERT/CSIRT authorities and support their interplay

The project duration extends from September 2020 to August 2023.

## **1.2 Deliverable Purpose**

The purpose of this deliverable is to provide a comprehensive progress description of the conduct of the Tallinn pilot. The report will cover the system level evaluation of the pilot that is based on the integrated software system specified and developed in WP5 and WP6.







## 2 METHODOLOGY

The pilot deployment methodology is fully described in D7.1 "Site Surveys & Scenario Planning", it is structured as follows:

**Step 1:** Exercise objectives definition.

**Step 2:** Scenario elaboration (definition of scenario and chronological elements and events).

**Step 3:** Technical definition (definition of components to be used, definition of what will be simulated and what real hardware will be used, definition of technical events and attack paths).

**Step 4:** Technical implementation (clones' creation and deployment, attack scenarios implementation).

**Step 5:** CitySCAPE installation in pilot location, interconnection with cloned CPaaS when relevant, interconnection with remote CitySCAPE services when relevant.

**Step 6:** Platform test and pilot dry run.

**Step 7:** Pilot run phase.

Step 8: Pilot results analysis and feedback.

This document concerns Steps 4-8 where the technical definition of the test was carried out.



## **3 INFRASTRUCTURE DEPLOYMENT**

### **3.1** Tallinn CPAAS infrastructure table

The TALLINN pilot environment consisted of infrastructure depicted in Figure 1.

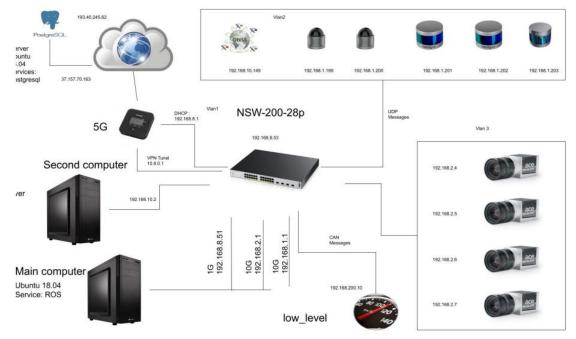


Figure 1. Tallinn CPaaS infrastructure

The "Control Room server" in the Firgure is denoted as the Cloud, which contains multiple important applications and services of the CPaaS and CitySCAPE Toolkit such as Teleoperation, Data Logging, Transportation Ticket Validator Application, IDS/IPS, SIEM, etc.. The AV Shuttle is represented by the network part segmented by the switch (NSW-200-28P), and a set of sensors is depicted (Camera and LiDAR). The control of the AV (where the self-driving modules (algorithms) are contained) is located on the main computer and the secondary computer.

The high-level infrastructure as related to the multi-modal transportation journey is represented in Figure 2.

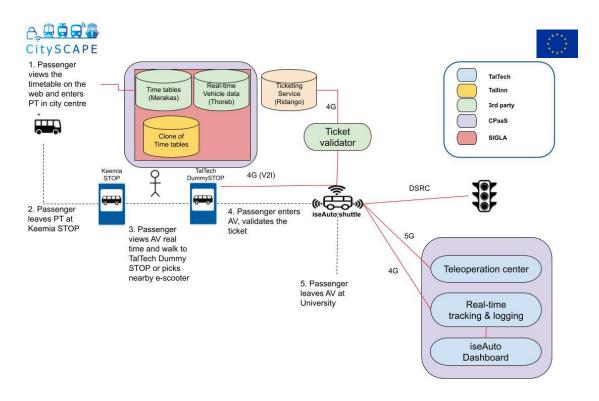


Figure 2. Tallinn High-Level CPaaS Assets

## **3.2** CitySCAPE toolkit

The CitySCAPE toolkit components are involved in the Test Case scenarios as depicted in Table 1.

Test Case	SIEM	IDS	RITA	FIMCA	CTIP	CSIRP
Test Case 1	х	х	х	х	X	х
Test Case 2	X	Х	Х	X	X	X
Test Case 3	×		X	X	X	X
Test Case 4	×		X	X	X	X
Test Case 5	Х		X	X	X	X

Table 1. CitySCAPE toolkit modules used in Tallinn pilot

The X represents the functionality able to be reported in the TALLINN Pilot deployment during the 24<sup>th</sup> to 25<sup>th</sup> of August. The red X represents the functionality which will be demonstrated on the completion of the TALLINN Pilot and will be detailed in the final report in D7.5 "Pilot Evaluation and Knowledge capitalisation". Since the IDS is a network monitoring engine, not all test cases involve its use.

# A CITYSCAPE TALLINN PILOT



#### 4.1 Overview

The TALLINN Pilot started on 1<sup>st</sup> of July, commencing with a 2-week period where the AV shuttle was in operation in the TalTech campus area, collecting data. Based on the collected data, partners started to develop modules and interfaces among CitySCAPE toolkit components in order to perform attacks and develop mechanisms to detect them. After 5 weeks of preparatory works, all relevant partners gathered in Tallinn to perform live demo. On the first day of the demo, technical partners carried out comprehensive training for internal and external experts on the following subjects:

- how to use CitySCAPE tools in real conditions;
- how to operate scenarios in Cyber Range;
- how to exchange CTI using MISP or SFTP (see Annex IV).

In the trainings there were 29 participants from DNSC, ENISA – European Union Agency for Cybersecurity, CERT France and CSIRT Greece and local experts from TalTech and TALLINN.

After the training sessions, technical partners performed and then showcased live demo with 2 pre-defined scenarios in real conditions (Test-Case 1 & Test-Case 2). Intrusion attacks were performed on the live iseAuto systems, and the performance of the CitySCAPE modules was evaluated. When conducting test-case 3 and 4, unexpected issues with the integration of CitySCAPE modules were found. Furthermore, the SIEM required more data ingestion and analysis to adequately create detection rules for testcase 3 and 4 attacks. To ensure the ability to demo the remaining 3 scenarios (Ticketing system, GNSS Spoofing and SiglaMoving transport data) the pilot group identified the scope, and the preparatory works have been successfully completed. However, due to the unexpected problems with integration of the modules during the Tallinn pilot period, it was impossible to finalize all scenarios on time. Within upcoming weeks, project partners will continue working with the remaining three scenarios and results of all scenarios will be reported in the respective deliverable 7.5 "Pilot Evaluation and Knowledge capitalisation".

Week	Activity	Resource Required
July 4 to 8	AV Shuttle Operational – Monday Tuesday Wednesday Thursday	AV Shuttle Engineer. IDS Engineer.
	IDS Monitoring of Data Collection	ACS Engineer.

#### **4.2 Low-Level Deployment Timeline**



	Preparation of Cyber Range Environment	
July 11 to 15	Prepare Training Scenarios	ACS, TalTech, CitySCAPE Tool Owners, DNSC.
	Test/Prepare Cyber Attacks (Test Case DDoS & RSU)	Oppida, TalTech.
	AV Shuttle Operational – Monday Tuesday	AV Shuttle Engineer.
	Wednesday Thursday	IDS Engineer.
	IDS Monitoring of Data Collection	ACS Engineer.
	Preparation of Cyber Range Environment	
July 18 to 5 August	Any remediation of the IDS & SIEM (CitySCAPE Platform)	CitySCAPE Tool Owners
	Any remediation of the iseAuto network and infrastructure	iseAuto team
August 8 to 12	Setup/preparation of the Tallinn Pilot Environment	TalTech, Oppida, CitySCAPE Tool Owners.
August 15 to 18	Setup/preparation of the Tallinn Pilot Environment SIEM & IDS monitoring of data collection	TalTech, Oppida, CitySCAPE Tool Owners. SIEM & IDS engineer.
August 24	Cybersecurity testing in the CyberRange environment and Tallinn Environment	Oppida, TalTech, ACS.
August 24	Tallinn Pilot Demonstration CitySCAPE Training	CitySCAPE Consortium. DNSC, ACS, ED, Tallinn Stakeholders.
August 24 to 25	Tallinn Pilot Demonstration CitySCAPE Training	CitySCAPE Consortium. DNSC, ACS, ED, Tallinn Stakeholders
	Draft Pilot Report	realing

Table 2. Low-Level Deployment Timeline



Tallinn test cases focused on the following cybersecurity aspects:

- 1. Improved confidence of efficient handling of day-one and specific DoS attacks.
- 2. Minimizing security risks introduced by (less security-aware) external service providers.
- 3. Improving the fraud prediction caused by recent EU finTech market opening directives and technological advancements.
- 4. Minimizing the risks to personal privacy related to fraud prevention and new ticketing services like GNSS/ indoor RTLS based BiBo.

These test-cases involve a diverse range of transportation technologies, from AV shuttles to transportation fare card validation and from adaptive traffic management, from vehicle to infrastructure (V2I) communications. The Tallinn pilot described attacks on each of the transportation areas, and deployed attacks on all, except the Test-Case 4 (GNSS) which required further investigation in order to conduct the attack, and Test-Case 3 (Fraud Detection), which required further exploration of the logs by the SIEM operators to construct effective detection rules. Also, Test-Case 5 (Mobile Application) required further log analysis by the SIEM operators to construct detection rules and develop the playbooks for security orchestration.

#### 4.3.1 Test Case 1: Availability of AV Shuttle Network Communication

#### 4.3.1.1 Pilot scenario description

In this scenario, the passenger is able to move seamlessly from the city transportation modes to the last-mile services (AV Shuttle). The passenger interactions to achieve this are listed below:

- 1. Passenger departs from the city-transport mode and reaches the AV Shuttle.
- 2. The AV Shuttle drives the passenger to the end destination.

The desired behaviour of the system is described below:

- 1. The remote operations center of the AV Shuttle monitors the operation of the AV Shuttle.
- 2. The remote operations center monitors the passenger in the AV Shuttle.
- 3. If there are any safety events, the emergency stop can be used to stop the AV Shuttle, or the remote operator can assume control and make driving decisions.

The following table describes the assets involved in the scenario and the scope of each of them.





			Autonomous S	Self-Driving Shuttle	
Vehicle on-board Computer	Hardware	Taltech	Physical computing units, Operating System, APIs, Application Server, Software components, Local data assets (databases), Log files, configuration data	Network interfaces (Ethernet, CAN, Serial) OS (Ubuntu 16.01) Applications (ROS, Autoware.Auto, Skyhook)	The vehicle computer.
Camera Sensors	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP Connected to On-board Unit.	The vehicle on-board cameras.
Camera Data	Data asset	Taltech	Physical Unit, Log files, configuration data	Camera data is stored in the ROSBag logging system.	The video files from on- board camera.
GNSS	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected GNSS sensor using Skyhook GPS application.	The vehicle GNSS system. Used for geo- location/ SLAM.
ΙΜυ	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	CAN bus interface, integrated with GPS	Vehicle IMU for capturing of measurement data of AV (acceleration, orientation, heading).
Ultrasonic Sensors	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected to on-board L2 switch.	Used for short-range object detection.
Lidar	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected to on-board L2 switch.	LiDAR used for 3D point cloud mapping to build dynamic maps for SLAM.
Local Dynamic Map	Data asset	Taltech	configuration data	Application interfaces (APIs, REST, JSON etc.) Web services Database connectors	The vehicle complete database.
Communic ation modem	Hardware, Firmware, Software	Taltech	4G and 5G Router	Network interface (Ethernet, CAN) V2X 4G M2 Nighthawk Router 5G Router	The modem ensuring communication with other vehicles and infrastructure.
Switch	Hardware, Firmware, Software	Taltech	L2 Switch	Ethernet (Cat 6, 5E) L2 (VLAN segmentation)	Switch connects on- board unit, sensors and router. Manages access to the network and segments network in VLANs).
AV Shuttle Operating System	Middlewa re/Firmwa re OS	Taltech	-	OS interfaces (Proprietary port enabled, protected by access and authentication mechanisms)	ROS Melodic, Autoware 1.14
Self- driving applicatio n	Software	Taltech		Application interfaces (APIs, REST, JSON etc.) Messaging protocols Web services Database connectors	Autoware.ai Application framework for self-driving vehicles.

CitySCAPE Teleoperat	Hardware,	Teleoper	Physical or	Network interfaces (Ethernet,	Control PC
ion services	Middlewa re, Software, Data, Redunda ncies	ation services provider	virtual computing units, Operating System, Application Server, Web services, Databases and DBMS, Log files, configuration data	Wi-Fi, 4G, Bluetooth) OS interfaces (SSH, RDP, etc.) Application interfaces (APIs, REST, etc.) Database connectors File Transfer Services (e.g., SFTP)	communicating using the teleoperation software which is a module of the ROS.
Teleoperat ion Module	Software	Taltech	API	OS interfaces (SSH) – Access and Authentication using FIDO 2FA, TLSv1.3 and VPN	Module implemented in the ROS implementation.
Actuators	Hardware, Firmware, Software	Taltech		Network interface (Ethernet, CAN)	Actuators

Table 3. Assets involved in the scenario 1

#### 4.3.1.2 Attack scenarios

The aim of Test Case 1 (Availability of AV Shuttle Network) is to test the ability of the CitySCAPE toolkit to detect cyber-attacks that impact the availability of the AV Shuttle teleoperation network. Without communication of the AV Shuttle to the teleoperation server, the AV cannot be safely monitored and controlled by the teleoperator and thus the last mile extension journey of the passenger is either not possible or unsafe. The aim of this test case was to assess the CitySCAPE toolkit against availability attacks such as DDoS, and this includes techniques within the cyber-attack kill chain, from reconnaissance (scanning and fingerprinting) to exploitation (delivery of DDoS packets).

In order to perform Test Case 1 and try to affect the AV communication availability, OPPIDA has performed the following tests scenario steps:

- Fingerprinting
  - o Try to identify targets and potential vulnerabilities
- DoS Attacks
  - From the internet
  - From inside the vehicle (inside attacker simulation)

To perform these scenarios and after several preliminary test, Oppida has finally used the following tools:

- Nmap
- Metasploit
- Command line
- Exploit scripts available on the internet for specific identified service with potentially known vulnerability

Two different sub scenarios have been played.

The first one (sub-testcase 1.1) consisted of identifying and attack targets from the internet (system elements with public IPs) which is actually equivalent to targeting the control server (see Figure 1) as depicted in Figure 3.

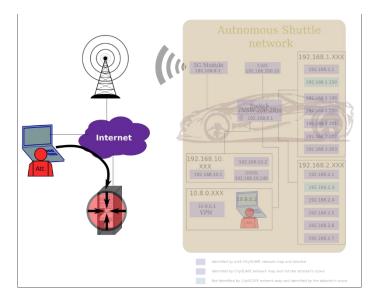


Figure 3. Sub-testcase 1.1 involved element

The second test case (sub-testcase 1.2) simulated inner vehicle attacks. This was performed through a VPN connection to the AV network, provided by a VPN server installed in the vehicle (see Figure 1). Thus, enabling Oppida to lunch sub-testcase 1.2 steps from the AV LAN, allowed to simulate an attacker able to get access to the AV LAN, either physically connected to the vehicle (e.g. a passenger able to find an accessible physical port) or a roadside attacker, able to hack the AV communication device.

From this position we performed in sub-testcase 1.2 a complete scan of the accessible sub-networks and then performed a targeted DoS attack on its most significant equipment - the communication unit (see Figure 1), as depicted in Figure 4 and Figure 5.

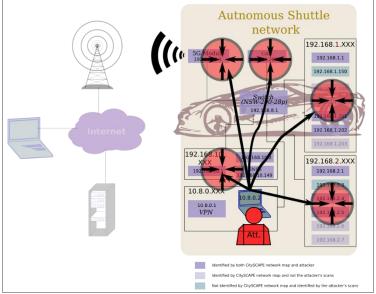
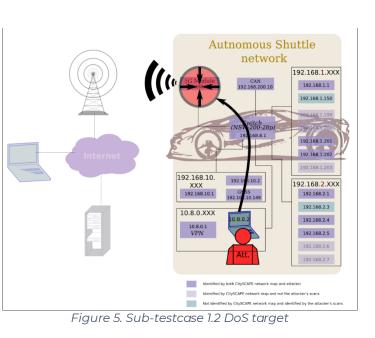


Figure 4. Sub-testcase 1.2 scanning targets



Classic synflood attacks have been performed, running the dedicated Metasploit plugin plus command line hping as well as a scprit dedicated to attack the specific version of the ftp server of the control server.

#### 4.3.1.3 Modules behaviour

#### 4.3.1.3.1 SIEM

**Graylog** - Graylog receives alerts from the IDS/IPS component, as represented in the following picture.

· ⇒ C	0	👌 graylog:	9000/search?q=&r	angetype=al	bsolute&from=	2022-08-251	T06%3A00%3A00.000	Z&to=2022-08-25		
ıraylog	Search Strea	ms Alerts	Dashboards	Enterprise	Wizard 👻	System •	0			2 0
0 -	From: 2022- 08:00:00.00		Until: 2022-08-2 23:30:00.000	5	Select stream	s the search	should include. Search	es in all stre 👻	Not u	updating <del>*</del>
	yoe your search	query here a	nd press enter. E	a.: ("not f	ound' AND http)	OR http://e	ssionse_code:[488 9	☆ Save ⊡ Lo	ad 🔒 Share	0
	age Count								4	×××
8,000		- 1								
6,000 4,000		- In	d -							
2,000										
08:00 Aug 25, 202		:00	12:00	14:00		16:00	18:00	20:00	22:00	
≡ All Me	ssages								12	×××

Figure 6. Alerts received to Greylog

In particular, during the first SYN flood attack, several messages concerning TCP sessions without 3-way handshakes were received and aggregated into an alert sent to the XSOAR component., as detailed in the picture below

⊟ All Messages		3	: ×	ľ v
timestamp 17	source	17		
2022-08-25 11:58:36.000 +02:00	server-d	lesktop		
server-desktop snort[31371]: message repeated 21 times: [ [129:20:1] TCP session without 3-way handshake [Classification c] [Priority: 2] {TCP} 193.40.250.237:504 -> 193.40.245.62:22]	: Potenti	ally B	ad Tra	ff1

Figure 7. Aggregated alert sent to the XSOAR component







The same kind of messages was received, aggregated, and transmitted to the XSOAR component when the second iteration of the SYN flood attack was executed, as shown in the following picture.

O Gray	ylog - Unsaved Search	× +										
← -	→ C	0 🔒 g	raylog:9000/se	earch?q=&r	angetype=ab	solute&fror	n=2022-08-25T	06%3A00%3A00.(	000Z&to=2022-08-25	☆		
gray	ylog Search	Streams	Alerts Da	shboards	Enterprise	Wizard •	System +	0		1 in 1 out	ľ	0
>	≡ Message Count										0 8	B. ~
;	8,000		1 - A									
	6,000											
+	4,000											
Image: Provide the second s	2,000	-										
x,	08:00 Aug 25, 2022	10:00	12	:00	14:00		16:00	18:00	20:00	22:0	00	
~1	≡ All Messages										$\odot \times$	e ~
	timestamp <b>†</b> ₹				*				s	ource 17		
	-desktop snort[3137 1ty: 2] {TCP} 193.4					TCP sessio	n without 3-w	ay handshake [C	lassification: Pote	ntially B	lad Traf	fic]
2022-0	8-25 12:28:17.000 +02	2:00							ser	ver-desktop	2	
	-desktop snort[3137 7:50457 -> 193.40.2		20:1] TCP ses	sion with	out 3-way h	andshake [C	lassification	: Potentially B	ad Traffic] [Priori	ty: 2] {T	CP) 193	.40.
2022-0	8-25 12:28:17.000 +02	2:00		1	5				ser	ver-desktop	þ	
	-desktop snort[3137 7:50457 -> 193.40.2		20:1] TCP ses	sion with	out 3-way h	andshake [C	lassification	: Potentially B	ad Traffic] [Priori	ty: 2] {T	CP) 193	.40.

Figure 8. Received messages transmitted to XSOAR component

**XSOAR** - XSOAR receives alerts from Graylog, maps them to its internal data model, and assigns them to a user. In the picture below, the dashboard of an analyst is detailed.

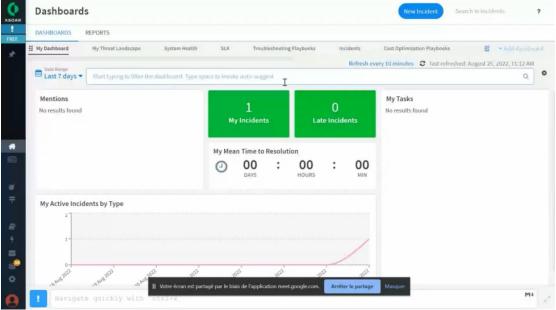


Figure 9. XSOAR receives alerts from Graylog

The alert received following the first SYN flood attack is displayed in the incident dashboard, as detailed in the screenshot below.

In	ncidents					New Incident Search	in Incidents ?
	Frank					Refresh every 5 minutes	
1	Last 7 days -	-category:job and -status:arc	hived and -status:closed an	nd owner:"{me}"		×Q	Add to Saved queries [
	Severity -		Туре 🕶		SLA -	Owner 🕶	
						fabien.pornel	. (11
	Medium 1	0	Deface 1	C			A 44
ø	Hide Chart Pane wing incidents 1 t	0	Deface 1	C			
Sho	> Hide Chart Pane		Deface 1	C	eiete	) -	iew III Summary View
She Ass	Hide Chart Pane nowing incidents 1 t		tun Command Export	C	C		

Figure 10. Alerts displayed in incident dashboard

The description of this incident is available in the following interface.

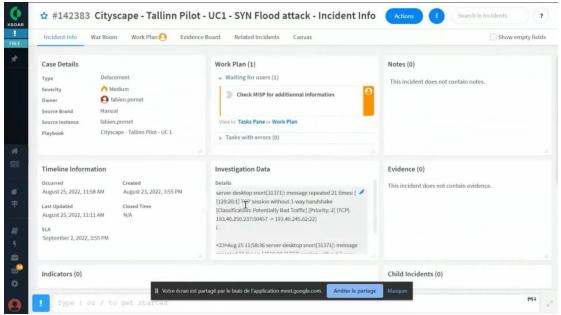


Figure 11. Incident description

XSOAR associated the incident with a playbook, i.e. a description of the actions to be executed automatically or manually by the analyst to accelerate the handling of the incident, as represented below.

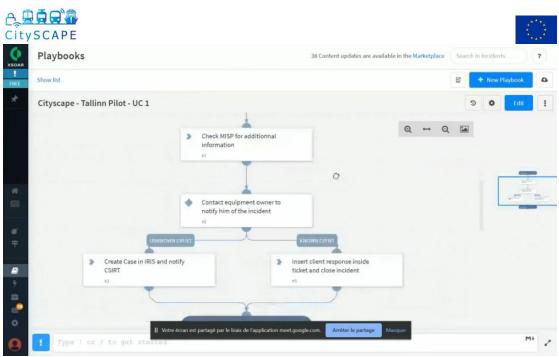


Figure 12. XSOAR provided description of the actions to the handling of the incident

On the second iteration of the SYN flood attack, a new alert was created into XSOAR, while the old one was assigned to a service account in order not to "pollute" the analyst interface with data from the old alert, as showed in the following picture.

E Cre	sated st 7 days 🕶 S	earch in incidents					Refresh eve	Q Add to Sav	ved queries 🛛 🗠
	verity <del>•</del> edium 2		Type ▼ ■ Deface 2		SLA ▼ ■ within 2			Owner ▼ fabien.pornet (1) ■ Ladm	(1)
			Ģ			(	) -		
	de Chart Panel						•	Table View III Co	All and a second second
	ng incidents 1 to 2	out of 2 Mark as Duplicate	Run Command	Export Close	Delete		-	Table View III St	ummary View
Showin	ng incidents 1 to 2		Run Command	Export Close Type	Delete	Status	Owner	Table View III St	
Showin Assign	ng incidents 1 to 2	Mark as Duplicate	Run Command ilot - UC1 - SYN Flood			Status Active	Owner ladm		4

Figure 13. SYN flood attack

#### 4.3.1.3.2 IDS/IPS engine

The solution version used for this demonstration is the alpha version, where the basic integration of the internal module has been developed and an initial version of the Anomaly Detection Procedure is implemented as a separate API.

The internal architecture of the CityScape IDS/IPS engine is depicted in Figure 14, details are available in deliverable D5.4 "IDS/IPS final prototype".

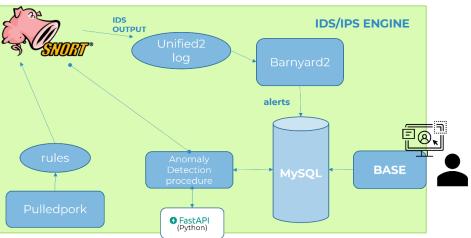


Figure 14. CityScape IDS/IPS engine internal architecture

The deployment has been executed during month M24 by ENG IDS engineers using the bash files provided in the code repository.

As mentioned in D7.1 "Pilot scenarios, validation plan, and Pre-piloting preparation", the IDS/IPS engine is used in the first two test case scenarios (sections **Error! Reference source not found.** and section **Error! Reference source not found.**):

- 1. AV Shuttle Network Communication;
- 2. Integrity of RSU;

In both test cases, the IDS/IPS is used to identify possible threats, in particular in the first test case the IDS/IPS engine should be used in ON-LINE mode while for the latter one the OFF-LINE mode:

- Online: the IDS/IPS engine is running and analysing in real-time the traffic that is passing through a specific interface,
- Off-line: the IDS/IPS engine analyses a pre-recorded traffic dataset pcap file) and identifies potential threats, then the idea is to try to use the ADP-API to test the Anomaly detection Procedure with to pre-recorded dataset, the first one to train the procedure and create the ADP model and the second one to test the model.

For the TALLINN pilot the IDS/IPS engine has been deployed on the TALLINN Control Room Server (See Figure 1 in section 3.1).

The TALLINN Control Room Server is connected to AIRBUS VPN through OpenVPN client to be able to forward the engine alerts to the CityScape SIEM which is, for this pilot, deployed into the AIRBUS servers.

In the following table, additional technologies used for this pilot are listed with a short description.

#	Name	Description	Use in the pilot
0		Open-source HTTP server for modern operating systems	Used to expose the GUI to view alert (BASE)

<sup>&</sup>lt;sup>1</sup> https://httpd.apache.org/



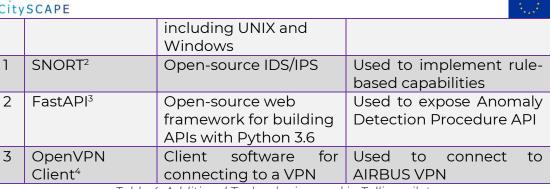


Table 4. Additional Technologies used in Tallinn pilot

During the first day of TALLINN's Pilot live demo, August 24, 2022, the ENG colleagues illustrated a brief guide on the usage of the IDS/IPS engine submodules to the pilot's participants based on the type of users. The presentation used is available in ANNEX I - IDS/IPS engine user guide. Then the IDS/IPS engine has been activated in Online mode the day after,

August 25, 2022, monitoring the enp2n0 interface.

The IDS/IPS engine, as mentioned before, was running in Online mode and the following alerts have been generated (see Figure 15):

- a. TCP session without 3-way handshake [Classification: Potential Bad Traffic] [Priority: 2]
- b. (spp\_ssh) Protocol mismatch [Classification: Detection of nonstandard protocol or event] [Priority: 2]

The first type of alert was generated with a huge number of instances, indicating that the alerts are related to a potential SYN flood attack, while the second type of alert had a limited number of records.

In Figure 16 is depicted the GUI to view the generated alerts.

💣 server@server-desktop: ~		×
Aug 25 12:21:06 server-desktop snort[31371]: [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad Traffic] [ P) 193.40.250.237:50387 -> 193.40.245.62:22	Priority: 2]	{TC ^
-Aug 25 1221106 server-desktop snort[31371]: [128:4:2] (spp ssh) Protocol mismatch [Classification: Detection of a non-standard protoco	l or eventl	[Pri
ority: 2] {TCP} 193.40.250.237:50387 -> 193.40.245.62:22		
Aug 25 12:21:06 server-desktop snort[31371]; [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad Traffic] [ P) 193.40.250.237:50387 -> 193.40.245.62:22		{TC
F) 19.40.2012/16050 - 7 19.40.40162122 Aug 25 12:21:06 server-desktop snort(31371); [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad Traffic] [	Priority: 21	{TC
P} 193.40.250.237:50387 -> 193.40.245.62:22		
Aug 25 12:21:06 server-desktop snort[31371]: [128:4:2] (spp_ssh) Protocol mismatch [Classification: Detection of a non-standard protoco		[Pri
ority: 2] (TCP) 193.40.250.237.50387 -> 193.40.245.62:22		(TC
$R_{12} = 22 + 22 + 100 + 52 + 52 + 50 + 50 + 50 + 51 + 51 + 52 + 52 + 51 + 52 + 52 + 51 + 52 + 52$	FILOTICY. 2]	110
Aug 25 12:21:07 server-desktop snort[31371]: [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad Traffic] [		{TC
P) 193.40.250.237:50387 -> 193.40.245.62:22		1.0.1
Aug 25 12:121:07 server-desktop snort[31371]: [128:44:2] (app_ssh) Protocol mismatch [Classification: Detection of a non-standard protoco lority: 2] (TCP) 193.40.250.237:50387 -> 193.40.245.62:22	I or event]	[PT1
Aug 25 12:21:07 server-desktop snort(31371): [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad Traffic] [	Priority: 2]	{TC
P} 193.40.250.237:50387 -> 193.40.245.62:22		
Aug 25 12:121:07 server-desktop snort[31371]: [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad Traffic] [ [P] 193.40.250.237:5037 -> 193.40.245.62:22	Priority: 2]	{TC
Aug 25 12:21:07 server-desktop snort(31371): [128:4:2] (spp ssh) Protocol mismatch [Classification: Detection of a non-standard protoco	l or event]	[Pri
ority: 2] {TCP} 193.40.250.237:50387 -> 193.40.245.62:22		
Aug 25 12:21:07 server-desktop snort[31371]: [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad Traffic] [		{TC
[P] 193.40.250.237:50387 -> 193.40.245.62:22 Jaug 25 12:107 server-desktop snort[31371]: [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad Traffic] [		(TC
$R_{12}$ (2) (2) (2) (2) (2) (2) (2) (2) (2) (2)		110
Aug 25 12:21:07 server-desktop snort[31371]: message repeated 2 times: [ [129:20:1] TCP session without 3-way handshake [Classification		у Ва
d Traffic] [Priority: 2] {TCP} 193.40.250.237:50457 -> 193.40.245.62:22]		100
Aug 25 12:121:07 server-desktop snort[31371]: [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad Traffic] [ [9] 193.40.250.237:5037 -> 193.40.245.62:122	Priority: 2]	{TC
Aug 25 12:21:07 server-desktop snort[31371]: [128:4:2] (spp ssh) Protocol mismatch [Classification: Detection of a non-standard protoco	l or event]	[Pri
ority: 2] {TCP} 193.40.250.237:50387 -> 193.40.245.62:22		
Aug 25 12:121:07 server-desktop snort[31371]: [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad Traffic] [ [9] 133.40.250.237:50457 -> 133.40.245.62:122	Priority: 2]	{TC
F) 190.40.200.237:50457 -> 193.40.240.02:22 Aug 25 12:21:07 server-desktop snort[31371]: [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad Traffic] [	Priority: 21	{TC
P} 193.40.250.237:50387 -> 193.40.245.62:22		
Aug 25 12:21:07 server-desktop snort[31371]: [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad Traffic] [		{TC
P) 193.40.250.237:50457 -> 193.40.245.62:22	804.1	77% ×

Figure 15. IDS/IPS engine log with the alerts generated for test case 1

<sup>2</sup> https://snort.org

<sup>&</sup>lt;sup>3</sup> https://fastapi.tiangolo.com/

<sup>&</sup>lt;sup>4</sup> https://openvpn.net/vpn-client/





$\leftarrow$	$\rightarrow$ G	Iocalhost/base/base_qry_main.php?se	arch=1&prev_sort_order=time_o	l&action_lst[0]=%23480-(1-	566 <b>90% ☆</b>	$\boxtimes$ $\pm$
IP Crit TCP C	Criteria time = [ Clear	[anong streams, ror session workers		Sensors     Unique Alerts     (classifications)     Unique addresses: Source   De     Unique IP links     Source Port: TCP   UDP     Destination Port: TCP   UDP     Time profile of alerts	estination	
		ſ	Displaying alerts 721-768 of 2513 total			
	ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
	#720-(1-56408)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:36	193.40.250.237:50457	193.40.245.62:22	TCP
	#721-(1-56407)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:36	193.40.250.237:50457	193.40.245.62:22	TCP
	#722-(1-56406)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:36	193.40.250.237:50457	193.40.245.62:22	TCP
	#723-(1-56405)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:36	193.40.250.237:50457	193.40.245.62:22	TCP
	#724-(1-56404)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
	#725-(1-56403)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
	#726-(1-56402)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
	#727-(1-56401)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
	#728-(1-56400)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
	#729-(1-56399)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
	#730-(1-56398)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
	#731-(1-56396)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
	#732-(1-56395)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
	#733-(1-56394)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
Ō	#734-(1-56393)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
0	#735-(1-56392)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
	#736-(1-56391)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
	#737-(1-56390)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
	#738-(1-56389)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
	#739-(1-56388)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
	#740-(1-56387)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
ō	#741-(1-56386)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
	#742-(1-56385)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
	#743-(1-56384)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
	#744-(1-56383)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
0	#745-(1-56382)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
Ó.	#746-(1-56381)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
Õ.	#747-(1-56380)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP
0	#748-(1-56379)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:58:35	193.40.250.237:50457	193.40.245.62:22	TCP

Figure 16. IDS/IPS engine alerts viewed through the GUI for Test case 1.1

For sub-testcase 1.2, alerts related to the attack on the communication unit (previously described) have not been generated; mostly due to the fact that the IDS/IPS engine was deployed on the server machine and was not receiving all the traffic in the subnetwork.

#2-(1-3117)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:02	193.40.250.237:50457	193.40.245.62:22	TCP
#3-(1-3118)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:03	193.40.250.237:50457	193.40.245.62:22	TCP
#4-(1-3119)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:03	44.240.140.78:443	193.40.245.62:51310	TCP
#5-(1-3120)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:03	44.240.140.78:443	193.40.245.62:51310	TCP
#6-(1-3121)	[snort] stream5; TCP session without 3-way handshake	2022-08-25 11:27:04	193.40.250.237:50457	193.40.245.62:22	TCP
#7-(1-3122)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:04	193.40.250.237:50457	193.40.245.62:22	TCP
#8-(1-3123)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:05	193.40.250.237:50457	193.40.245.62:22	TCP
#9-(1-3124)	[snort] stream5; TCP Small Segment Threshold Exceeded	2022-08-25 11:27:06	146.59.87.96:36932	193.40.245.62:22	TCP
#10-(1-3125)	[snort] stream5; TCP session without 3-way handshake	2022-08-25 11:27:06	193.40.250.237:50457	193.40.245.62:22	TCP
#11-(1-3126)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:07	193.40.250.237:50457	193.40.245.62:22	TCP
#12-(1-3127)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:08	193.40.250.237:50457	193.40.245.62:22	TCP
#13-(1-3128)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:09	193.40.250.237:50457	193.40.245.62:22	TCP
#14-(1-3129)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:10	193.40.250.237:50457	193.40.245.62:22	TCP
#15-(1-3130)	[snort] ssh: Protocol mismatch	2022-08-25 11:27:10	193.40.250.237:50457	193.40.245.62:22	TCP
#16-(1-3131)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:10	193.40.250.237:50457	193.40.245.62:22	TCP
#17-(1-3132)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:11	193.40.250.237:50457	193.40.245.62:22	TCP
#18-(1-3133)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:11	193.40.250.237:50457	193.40.245.62:22	TCP
#19-(1-3134)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:12	193.40.250.237:50457	193.40.245.62:22	TCP
#20-(1-3135)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:13	193.40.250.237:50457	193.40.245.62:22	TCP
#21-(1-3136)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:14	193.40.250.237:50457	193.40.245.62:22	TCP
#22-(1-3137)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:15	193.40.250.237:50457	193.40.245.62:22	TCP
#23-(1-3138)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:15	34.120.208.123:443	193.40.245.62:60718	TCP
#24-(1-3139)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:15	34.120.208.123:443	193.40.245.62:60718	TCP
#25-(1-3140)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:16	34.120.208.123:443	193.40.245.62:60718	TCP
#26-(1-3141)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:16	34.120.208.123:443	193.40.245.62:60718	TCP
#27-(1-3142)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:16	34.120.208.123:443	193.40.245.62:60718	TCP
#28-(1-3143)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:16	34.120.208.123:443	193.40.245.62:60718	TCP
#29-(1-3144)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:16	34.120.208.123:443	193.40.245.62:60718	TCP
#30-(1-3145)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:16	34.120.208.123:443	193.40.245.62:60718	TCP
#31-(1-3146)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:16	34.120.208.123:443	193.40.245.62:60718	TCP
#32-(1-3147)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:16	34.120.208.123:443	193.40.245.62:60718	TCP
#33-(1-3148)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:16	34.120.208.123:443	193.40.245.62:60718	TCP
#34-(1-3149)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:16	34.120.208.123:443	193.40.245.62:60718	TCP
#35-(1-3150)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:16	34.120.208.123:443	193.40.245.62:60718	TCP
#36-(1-3151)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:16	34.120.208.123:443	193.40.245.62:60718	TCP
#37-(1-3152)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:16	193.40.250.237:50457	193.40.245.62:22	TCP
#38-(1-3153)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:16	193.40.250.237:50457	193.40.245.62:22	TCP
#39-(1-3154)	[snort] stream5: TCP session without 3-way handshake	2022-08-25 11:27:16	193.40.250.237:50457	193.40.245.62:22	TCP
#40-(1-3155)	fenort1 stream5: TCD session without 3-way handshake	2022-08-25 11:27:16	193.40.250.237:50457	193.40.245.62:22	TCP

Figure 17. IDS/IPS alerts generated during test case 1.2, no alerts related to FTP protocol





Prior to the attack, the RITA operator had already modeled the multimodal transport ecosystem in order to get the business service (namely Taltech-Teleoperation) overall risk and impact, as shown in Figure 18.

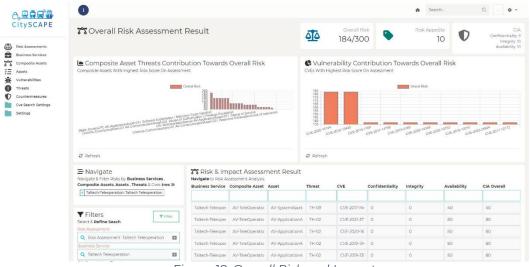


Figure 18. Overall Risk and Impact

For that reason the risk assessor has decomposed the business service to the list of composite assets as shown in Figure 19 and Figure 20.



TYSCAPE		
Ξ		:
-		
Business Service		Save × Delete
Edit Business Service Taltech Teleoperation	n	
Business Service Details 73 Compos	ite Assets & Composite Asset Relationships	
		·
Basic Information		
Set Business Service's Basic Information		
Code		
Taltech-Teleoperation		
Required Field		
Name		
Taltech Teleoperation		
Required Field		
Description		
10 Required Field Field Range [0-300]		
Set Security Objectives	Integrity	Availability
✓ 3 (Low)	v 10 (Extreme)	V 10 (Extreme)
The Unauthorized Disclosure Of Data Or Information Could Be Expected To Have A 1-4 Limited Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 5-6 Serious Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 7-10 Severe Or Catastrophic Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals * Required Field	The Unauthorized Modification Or Destruction Of Data Or information Could Be Expected To Have A 1-4 Limited Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 5-6 Serious Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 7-10 Severe Or Catastrophic Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals * Required Field	The Disruption Of Access To Or Use Of Information Or An Information System Could Be Expected To Have A 1-4 Limited Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 5-6 Serious Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 7-10 Severe Or Catastrophic Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals * Required Field
Accountability	Non Repudiation	Authenticity
Not Being Able To Ensure That The Actions Of An Entity May Be Traced Uniquely To That Entity Could Be Expected To Have A 1-4 Limited Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 5-6 Serious Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals	Not Being Able To Protect Against An Individual Falsely Denying Having Performed A Particular Action Could Be Expected To Have A 1-4 Limited Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 5-6 Serious Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals	Not Being Able To Be Prove That Data Or Information Is Genuine And Can Verified And Trusted Could Be Expected To Have A 1-4 Limited Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 5-6 Serious Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals
7-10 Severe Or Catastrophic Adverse Effect On	7-10 Severe Or Catastrophic Adverse Effect On	7-10 Severe Or Catastrophic Adverse Effect On

Figure 19. Taltech TeleOperation Business Service (Basic Information)

Business Service Details Composite Assets Business Service Composite Assets Select Composite Assets Supporting The Business Service Composite Asset Composite	ess Service ervice Taltech Teleoperation	Composite Asset Relationships
Vehicle-Communications-01 AV communications comp	usite Assets	Composite Asset

Figure 20. Taltech TeleOperation Business Service (Composite Assets)

Following that, the risk assessor decomposed each composite asset to its basic assets, including the identified threats, their likelihood and any applicable counter measures. TalTech AV TeleOperation Server Threats and Countermeasures are shown in Figure 8.

During the Pilot Demo, as soon as the CSIRP operator has finished their incident analysis, the identified threats and vulnerabilities (included in the IRIS incident reports) were sent to RITA. As a result, the risk assessor had to re-evaluate the security posture and impact of the business service by reviewing and updating the threat probabilities and any available countermeasures. This is depicted also in Figure 21.

2		
	tySCAPE	



ITYSCAPE	-				
Ξ					1
	posite Asset Asset <b>av Teleoperatio</b>				Save × Delete
ি Composite A	sset Details 🛛 🖓 🗄 Asse	ts යි Asset Relationsh	ips		
E Assets I Select Basic Ass					
		Asset Selector		Priority In Terms	of Economic Value
× 0		<b>Q</b> AV storage		Medium	×
×		Q AV-ControlPC In	tel	🔽 Medium	×
× 0		Q AV-ControlPC O	S (Ubuntu)	🔽 Medium	×
× 0		Q AV-ROS		🖬 Medium	
×		Q AV-OnBoard-Da	tabase (PostegreSζ	🖬 Medium	
•					
		PC OS (Ubuntu) #			
Navigate To Thr		S (Ubuntu) ?Ξ Asset & 💿 A			6
ď	Code TH-01	Name Malware Injection	Likelihood ✓ 2 - Rare (Happ€	Active	Counter Measures
		Manual Algebrain			Inventory
					( X Continuous Vulnerability Management
					× application
					(+) whitelisting
Ľ	TH-02	Denial of Service	✓ 3 - Periodic (Ha		× Countermeasure
					for DoS of Ubuntu OS
					(+)
Ľ	TH-09	Failure of System	✓ 2 - Rare (Happ∈		(+)
Ľ	TH-11	Software Exploitati	✓ 3 - Periodic (Ha		× Software Exploitation / Malicious Code
					Injection
					× Patching
					× application whitelisting
					(+)
Ľ	TH-14	Device Modificatio	✓ 2 - Rare (Happ∈		× application whitelisting
					+
	TH-21	Resource Exhausti	✓ 3 - Periodic (Ha		× Audit logs +
Ľ					$\bigcirc$
ß	TH-22	Isolation/Virtualiza	✓ 2 - Rare (Happ€		( <del>)</del>
2	TH-22 TH-23	Isolation/Virtualiza Management Inter	<ul> <li>2 - Rare (Happe</li> <li>2 - Rare (Happe</li> </ul>		+
ď					(+) (+)
2	TH-23	Management Inter	✓ 2 - Rare (Happ€		(+) (+) (+)
2 2 2	TH-23 TH-24	Management Inter Unauthorized Acce	<ul> <li>✓ 2 - Rare (Happ∉</li> <li>✓ 2 - Rare (Happ∉</li> </ul>		
2 2 2 2	TH-23 TH-24 TH-25	Management Inter Unauthorized Acce Abuse of Authorise	<ul> <li>2 - Rare (Happe</li> <li>2 - Rare (Happe</li> <li>2 - Rare (Happe</li> </ul>		÷ ÷ ÷

Figure 21. AV TeleOperation Server (AV Control PC OS-Ubuntu Threats and Likehoods)





Additional Figures demonstrating the RITA functionality for the TALLINN Pilot are contained in Annex II.

- For AV TeleOperation Server (AV-TeleOperationServer), this is shown in Annex II *Figure*], Error! Reference source not found.2, Error! Reference source not found.3, Error! Reference source not found.4, and Error! Reference source not found.5, including the assets relationships shown in Error! Reference source not found.6.
- For AV communications (Vehicle-Communications-01), this is shown in Annex II Error! Reference source not found.7, Error! Reference source not found.8, Error! Reference source not found.9 and Error! Reference source not found.10, including the assets relationships shown in Error! Reference source not found.11.
- For Taltech self-driving vehicle control PC (Main-Control-PC), this is shown in Annex II Error! Reference source not found.12, Error! Reference source not found.13, Error! Reference source not found.14, Error! Reference source not found.15, Error! Reference source not found.16, Error! Reference source not found.17 and Error! Reference source not found.18, including the assets relationships shown in Error! Reference source not found.19.

#### 4.3.1.3.4 FIMCA

#### 4.3.1.3.4.1 Tangible assets

During the Tallinn demo, STAM demonstrated a first release of the FIMCA component, related to the assessment of the financial impact on the tangible assets. FIMCA aims to assess the economic losses associated with the risk assessed by RITA, which instead estimates the risk using qualitative scales. The details about the architecture, version, and deployment of the CitySCAPE FIMCA (Intangible Assets) engine for the Tallinn pilot are shown in chapter 4.3.1.3.4.2.

The user accessed the tool from RITA, after having successfully filled the data related to business services, assets, threats and countermeasures and after having performed a risk assessment of the organization (see chapter 4.3.1.3.3).

In FIMCA, the user found in the Homepage two configurations: the "baseline" and the "secured". The first configuration included the data that have been set in RITA, in particular the countermeasures currently applied. The second one included the countermeasures that the user aim to implement in its organization. These two configurations are then compared in the Cost Benefit Analysis to assess the sustainability of the "secured" configuration that has been created.

tySCAP	E					·
				MCA		
imary		Welcome to FIMCA) Here you co	an abbest the financial r	report on your organization's assets and business serv	Ces	
		Most Important Services		Composite assets ordered by risk		
		Autonomous-Driving	CIA 18	Main-Cantrol-PC Carthdentiaity \$ integrity 16	CIA 36 Avoilebility 16	
		ADDI 2		Stribbenberty  integrity 16	CIA 36	
				Confidentiality & Integrity 14	Availability 14	
<b>6</b> 1						
onfigurations Na section you can odd, adit onc	d delete different configurations of your organis	otion. A configuration is it set of countermodures opplied to yo	w organisation. The co	et-benefit analysis will be carried out by comparing two	of the configurations created.	+ Add Configuration
Risk Assessment	Risk Assessment					
(Autonomous Driving) Eoseline configuration	(Autonomous Driving) Secured configuration					

Figure 22. FIMCA Homepage

To perform the CBA, the user inserts additional data on FIMCA regarding to his organization. The data are related to company size, the number of employees and the personnel costs (both internal and external). The remaining information is related to the costs of the Composite Assets (defined in RITA) and the financial weight of the investigated service on the company turnover.

dit Configuration his page requests additional inf efore saving the configuration, lanage" menu.			ion for the c	issets, services an	d safeguards i		🍫 Manage 👻
Name							
Risk Assessment (Taltech S	martCity Traffic Communicatio	n)					
Company size	Number of employees	Company annual I	revenue	Employee avar	age cost	Technician ava	irage cost
Medium company 👻	100	5000000	€	40	€	50	€
Description							
Baseline configuration							4
Save and Exit							
	F	- igure 23. Inp	ut dat	a (i)			

<u>டி</u> Cityscape				4
	Id, edit and delete different configurations of your organisa be carried out by comparing two of the configurations crea e: 5000000 €		termeasures applied to yo	ur organisation. The
	Name	Economic weight on revenue in %	Economic Value	
	Taltech-SmartCity-Traffic-Communication	25 %	1250000€	
	Save			



Service	N	ame Economic	Value
Taltech-SmartCity-Traffic-Con	nmunication Vehicle-Com	munications-01 10000	€
Taltech-SmartCity-Traffic-Con	nmunication AV-RSUCo	mmunication 10000	€

Figure 25. Input data (iii)

Once the required data is inserted, the user selects the countermeasures he aims to apply to the organization. For demonstration reasons, the initial set of countermeasures present in the "baseline" configuration was empty (no countermeasure applied). The "secured" configuration is populated with new cyber-security solutions (provided by the CIS Controls). FIMCA allows the possibility to apply the measures globally (for the whole organization) or for each single asset. During the demo, they have been globally applied to the whole organization. In addition, FIMCA allows the user to modify the costs and mitigation factors of the countermeasures to have more accurate results in the financial impact estimation. However, during the test, information on these costs and these mitigation factors were not modified by the user because he did not have the means and knowledge to do it. The table below shows the information related to the countermeasures selected for the "secured" configuration.



#### Table 5. Countermeasure's data for "secured" configuration

source_id	confidentiality	integrity	availability	CAPEX	OPEX
1,2	40	60	50		500
1,3	30	30	20	100	
2,3	30	30	15	300	100
2,6	20	25	20		600
2,7	25	0	0	830	
3,1	40	40	15		200
3,4	20	25	20		200
3,6	40	35	30	50	108
3,9	30	25	20		100
4,4	30	25	15	2150	300
4,5	45	40	20	2150	300
4,6	40	35	20	100	150
4,9	45	40	30		100
5,4	30	25	30	800	
6,2	40	40	30		250
6,3	60	60	40		385
6,7	25	25	15		460
7,2	20	25	15		600
7,3	25	20	25		600
7,5	25	0	0	200	3500
7,6	30	0	0	200	3500
7,7	50	0	0		1000
8,1	35	25	20		200
8,5	50	50	50	200	
8,8	25	40	50		600
9,1	25	20	20	100	
9,2	40	45	30	100	215
9,3	45	40	35		200
9,4	40	45	40		100
9,5	40	40	40	100	100
9,6	30	35	20		100
9,7	30	35	25		260
10,1	45	45	45	100	45
10,2	40	40	40	50	
10,3	45	45	45		50
10,4	35	35	35	100	
10,5	50	45	40	50	
10,6	40	40	40		50
10,7	30	30	30	200	120
11,2	0	40	30	50	
12,3	50	30	30	5000	200
12,5	60	35	30	1300	100
12,7	60	40	30	4400	
13,1	70	40	35	2400	
13,1	0	30	25		600
13,11	60	55	55	2700	500
15,5	10	10	10		100
15,6	10	10	10		200
15,7	40	30	30		200
16,1	60	55	55		100
16,3	40	40	40		100
,-					

#### Applied Y

•
Y
Y
Y
Y
Y
Y
Y
Y Y
Y Y Y Y
Y
Y
Y
Y Y Y Y Y Y Y Y
Y
Y
Y
Y
Y
Y
Y
Y
Y Y
Y
Y
Y
Y
Y
Y Y
Y
Y
Y
Y
Y
Y
Y
Y
Y
Y
Y
Y
Y
Y Y Y Y Y Y Y Y
Y
Y
Y
Y
Y
Y
Y
Y





source_id	confidentiality	integrity	availability	CAPEX	OPEX	Applied
16,5	30	30	30		200	Y
16,12	75	60	60		600	Y
16,13	50	50	50		1200	Y
16,14	50	50	50		1200	Y
17,1	0	30	30		200	Y
17,2	0	30	30		100	Y
18,2	60	60	60		200	Y
18,3	80	80	80		100	Y
18,4	85	80	80		200	Y
18,5	65	60	60		400	Y

#### Applied

Υ	
Υ	
Υ	
Υ	
Y	
Y	
Y	
Y	





Through the ROSI index, the results of the cost-benefit analysis show the quality of the changes made to the set of countermeasures. The ROSI takes into account the financial impact of the original configuration (the "baseline"), the "secured" one and the cost of the solutions adopted (the countermeasures implemented in the "secured" one). If the ROSI is negative, then the solutions are ineffective, because the balance is negative. On the other hand, if the ROSI is positive, it means that the new configuration is effective and has an overall reduction in the organisation's costs. The FIMCA results also show an overview of the applied countermeasures, indicating the number of controls of the different CIS control groups applied to the different configurations.



Figure 26. Results of FIMCA - tangible assets

## 4.3.1.3.4.2 Intangible assets

The details about the architecture, version and deployment of the CitySCAPE FIMCA (Intangible Assets) engine for the Tallinn pilot are provided in this section.

**Infrastructure** - The architecture of the FIMCA engine is based on an Angular user interface, consuming the REST API endpoints of a Spring-Boot service.

The exposed API are well documented using the OpenAPI standard and secured via the shared authentication, thatauthentication, which is the Single Sign-On, thanks to the OpenID Connect and OAuth 2.0 protocols.

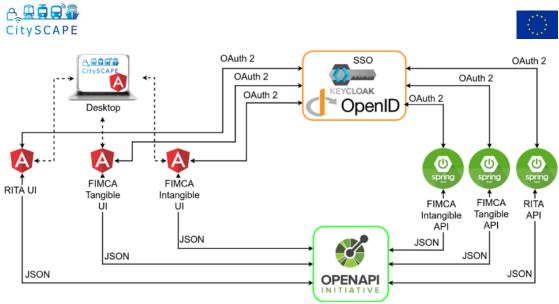


Figure 27. FIMCA Integration Architecture

The authentication mechanism is therefore possible thanks to the adoption of a mature and reliable Identity and Access Management (IAM) system such as Keycloak. However, it can be easily replaced by any other IAM supporting the OpenID Connect standard.

**Version** - The version of the engine used for this demonstration is tagged as 1.0.0 and includes all the main features, as well as the required scripts to Dockerize and deploy the tool on any system supporting the Docker engine.

**Deployment** - Thanks to the Docker images available for both the Angular app and the Spring-Boot service, deploying the FIMCA engine for Intangible Assets is just a matter of configuring a few environment variables and running two docker-compose commands.

The deployment has been executed on an ENG server by using the provided Docker-Compose file and instructions. As a result, the bare minimum to run the FIMCA engine is to have a machine with Docker and Docker-Compose installed.

**Demonstration** - At the Tallinn demonstration, ENG provided a detailed overview of the FIMCA engine for intangible assets. Starting from the security configurations, coming from the RITA and FIMCA for tangible assets engines, and listed in the following picture, the goal is to evaluate the economic impact in case of an intangible asset being compromised.



CISO TalTech 🙎

**Risk Management** 

Name	Created	Revenue	Actions	
Risk Assessment (Taltech SmartCity Traffic Communication)	Aug 24, 2022, 3:19:04 PM	€5 M	=,	
Risk Assessment (Taltech SmartCity Traffic Communication) (secured)	Aug 24, 2022, 3:19:05 PM	€5 M	=,	
	ltems per pag	e: <b>5 🔻</b> 1	- 2 of 2	> >

Figure 28. FIMCA Security configuration

The user can therefore select one of the risk-assessment configurations from the list and proceed with the impact evaluation step of a business service.

≡			CISO TalTe	ch 😫
isk Assessmen secured)	t (Taltech Sma	rtCity Traffic Co	ommunication)	
Risk Management Se Gelect a Risk Service from				~
Name	Minimum Impact	Mode Impact	Maximum Impact	
Taltech-SmartCity- Traffic-Communication	€1.52 M	€1.62 M	€1.64 M	
	Items per	page: 5 💌 1 - 1	of 1 🛛 🕹 🕹 🕹	>

Figure 29. FIMCA impact evaluation

Each business-service can contain different composite assets and each one can be analysed on its own for the impact evaluation.





#### Impact Evaluation

Assessing the cost of intangible assets related to the composite assets (CA) of the **Taltech-SmartCity-Traffic-Communication** service

Expand All	Collapse All

CA: Vehicle- Communications-01	Intangible Asset list	⊙	~
CA: AV- RSUCommunication	Intangible Asset list	lacksquare	~

Figure 30. FIMCA list of composite assets

Once selected a composite asset, the engine lists all the connected intangible assets that could be indirectly compromised. For each intangible asset, the engine provides a suggestion of the possible impacts (minimum, mode, maximum) in case of attack, based on the revenue of the organization. The user can then customize the initial values as desired if he has deeper knowledge about them. When the user has completed the definition of the different impact values, at first, he can proceed to the definition of the resulting PERT distribution and then he can execute the Monte-Carlo simulation for the possible impacts.

npact Evaluation	e assets related to the composite	e assets (CA) of the <b>Taltech-Smart(</b>	City-Traffic-Communication service	۵	
pand All Collapse All				C	
A: Vehicle-Communica	ations-01 Intangible Ass	et list		⊘	`
A: AV-RSUCommunica	ation Intangible Ass	et list		⊘	,
Intangible Asset	Minimum Impact Value	Mode Impact Value	Maximum Impact Value		
Data	€ 432400	€ 460000	Maximum Impact value * € 466900		_
Reputation	Minimum Impact value * € 235000	€ 250000	Maximum Impact value * € 253750		
Brand	€ 70500	€ 75000	Maximum Impact value * € 76125		
Organizational Capital	Minimum Impact value * € 117500	Mode Impact value * € 125000	Maximum Impact value * € 126875		

Figure 31. FIMCA suggestion of the possible impacts





The results of the Monte-Carlo simulation are displayed both in tabular and chart format.

≡	CISO TalTech 🔮	
Composite Asset	AV-RSUCommunication	
Monte Carlo simulations	Minimum Impact: €855.4 K   Mode Impact: €910 K   Maximum Impact: €923.65 K   Alpha: 4.2   Beta: 1.8	

It is wrong to consider the historical cost of the asset because it does not allow the variation in value over the years to be assessed and therefore corresponds to the actual value of the valued object. There is always variability due to uncertainty and risk that generates more or less marked deviations from what was planned. Monte Carlo simulation helps in the construction of this variability.

	No.	1	2	3	4	5	6	7		
	Value	917200.23	902090.99	917843.44	904278.72	912893.58	909331.89	908662.15		
-										

Figure 32. FIMCA Mont-Carlo simulation results

Taking into account all the generated values for the possible impacts, the engine calculates some representative statistics, useful for the next step of the cost-benefit analysis, that are visible after clicking on the ROSI button positioned on the top-right corner of the page.

#### Descriptive statistic

To analyze the data coming from the Monte Carlo Simulation we will use the Descriptive statistics, starting with the collection of data from a representative sample, derives from these a whole range of information on the central tendency and variability of the data.

Minimum	Mean	Maximum
€862,573.97	€903,213.99	€923,050.71

Figure 33. FIMCA calculated statistical values for CBA

At the beginning of the ROSI Analysis page, a brief description of the ROSI formula and its parameters can be found, before moving to the actual results.



~

#### How to calculate ROSI

ROSI, or Return on Security Investment, is a modified Return on Investment (ROI) calculation, where the net benefit is the annual cost of security breaches avoided as compared to the prevention cost incurred. The calculation of ROSI is based on three variables: Annualized Loss Expectancy (ALE), Estimated Risk Mitigation and Cost of the Solution. If the cost of the solution is easier to predict, provided all indirect costs are considered, the two other variables are estimations that make ROSI more approximate. Here is how to calculate your return on security investments.

	ROSI (%)	ALE * Mitigation Ratio – Cost of Solution
	Quantitative Risk Assessment Formula	Cost of Solution
-		y loss per year expected to result from a specific exposure factor if the ate ALE, we multiply the Single Loss Expectancy (SLE) by the Annualized
		e of risks that the security investment would address.
The Cost	of the solution is the total co	st of all selected countermeasures.

Figure 34. ROSI formula and its parameters

The ROSI analysis considers a single composite asset at each time and all its interconnected intangible assets.

The cost of the countermeasures and their individual values of mitigation ratios for confidentiality, integrity, availability are used to calculate the total cost, the total mitigation ratios, as well as an average overall mitigation ratio. These values are then used to calculate the three different values (confidentiality, integrity, availability) of ROSI and an average ROSI that considers all of them. CISO TalTech 😫

## Composite Asset: AV-RSUCommunication

Linked Intangible As	sets						
Data Reputation Bra	and	Organ	izational (	Capital			
w are the ROSI by Confidentiali	ity, Integ	rity and	Availabili	ty (CIA). The Ov	erall is the	e average of	the previous one
confidentiality		grity		Availa		<u>ה</u> ר	Overall
		<u>,</u>					
353%	33	5%		29	7%		325%
	_						
RSU-HW-01	RSU-AP	1-01		OBU-HW-01		OBU-API-	01
Countermeasure	Capex	Opex	Cost of the Solution	Confidentiality	Integrity	Availability	Implementation Groups
		€71	€71	40%	60%	50%	IG1
Address Unauthorized Assets	€0	6/1					
	€0 €14	€0	€3.5	30%	30%	20%	IG1 IG2
Assets Utilize an Active Discovery			€3.5 €85	30%	30% 25%	20% 20%	lG1 lG2
Assets Utilize an Active Discovery Tool Address Unauthorized	€14	€0 €85					

Figure 35. Three different values of ROSI (confidentiality, integrity, availability)

The evaluation of the FIMCA results found issues with its integration with RITA and with the ingestion of intangible assets. The shortcomings have been identified and will be remediated in September and October, to allow the demos to be conducted again.

#### 4.3.1.3.5 CTIP

CTIP was not active in this test-case. In the background, Graylog periodically launches requests to the CTIP to gather relevant IOCs. Since the attacker in the test-case I was a new unknown actor, no data was available to enrich the alert generated.





#### 4.3.1.3.6 CSIRP

CSIRP was displayed as a stand-alone application in this test-case, where an analyst created a case to continue investigations.

Graylog	g-Sign in × 3 Rils-Manage Cases (CSI) × +				a 😣
$\leftarrow \   \rightarrow$	C O A https://192.168.0.11:4433/manage/casestcid=1	☆		6	9 =
÷	Current case : #1-Initial Demo	¢	Ø		888
1	Cases management				
6) 	Now Update View				
x Q	General info				
B	Cityscape •				
0	Case name Gityscape - Tallinn Pilot - UC1 - SYN Pilod attack				
	Short description SYN flood attack in progress against AV shuttle control center				
î¢î	SOC ticket # #142384				
0					
IRIS v1.4.5			Create		



# 4.3.2 Test Case 2: Integrity of Multi-Modal Intelligent Road Sign Infrastructure

#### 4.3.2.1 Pilot scenario description

The defined scenario for the Tallinn Adaptive Traffic Control test-case is as follows:

- 1. A city bus/trolley and the autonomous vehicle shuttle travel through the smart campus roadway of the TalTech Mektory.
- 2. The Autonomous vehicle shuttle reaches an intersection.
- 3. The Autonomous vehicle shuttle communicates with the smart city traffic management road sign unit.
- 4. The traffic management node then receives communication from the RSU and a traffic control decision is made. This is communicated back to the RSU and then from the RSU to the AV Shuttle.
- 5. The TalTech Smart Campus Traffic Management monitors the traffic environment, and the teleoperation operator monitors the safety of passengers on the AV shuttle.

Name	Туре	Manage d by / Owned by	Basic Asset breakdown	Interfaces	Role
Mobile Network (4G/5G/)	Network	TalTech	4G and 5G Router	Via network (DSRC, UDP, TLS1.3) to anyone having a valid subscription to the network (Access via 2F Authentication using FIDO tokens and VPN).	Communication between Remote Operations Center and AV Shuttle.

The assets involved in this scenario are listed below:

<u>~ @ ā @`@</u>				_	
CitySCAPE					
Adhoc vehicular network	Network	Taltech	-	Via ITS messages to anyone part of the ITS-V2X network OBU (CohDA Mk5) RSU (CohDA MKX) CAMS Messages (CohDA proprietary protocol (MAP, SPAT, etc.), ITS-G5 Application Compliant).	Direct adhoc communication between vehicles and roadside units.
Vehicle on-	Hardware	Taltech	Physical	Self-Driving Shuttle Network interfaces (Ethernet, CAN,	The vehicle computer.
board Computer	Haluwale	Taitech	computing units, Operating System, APIs, Application Server, Software components, Local data assets (databases), Log files, configuration data	Serial) OS (Ubuntu 16.01) Applications (ROS, Autoware.Auto, Skyhook)	me venicle computer.
Camera Sensors	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP Connected to On-board Unit.	The vehicle on-board cameras.
Camera Data	Data asset	Taltech	Physical Unit, Log files, configuration data	Camera data is part of ROSbag logging system.	The video files from on-board camera.
GNSS	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected GNSS sensor using Skyhook GPS application.	The vehicle GNSS system. Used for geo- location/ SLAM.
IMU	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	CAN bus interface, integrated with GPS.	Vehicle IMU for capturing of measurement data of AV (acceleration, orientation, heading).
Ultrasonic Sensors	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected to on-board L2 switch.	Used for short-range object detection.
Lidar	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected to on-board L2 switch.	LiDAR used for 3D point cloud mapping to build dynamic maps for SLAM.
Local Dynamic Map	Data asset	Taltech	configuration data	Application interfaces (APIs, REST, JSON etc.) Web services Database connectors	The vehicle complete database.
Communic ation modem	Hardware, Firmware, Software	Taltech	4G and 5G Router	Network interface (Ethernet, CAN) V2X 4G M2 Nighthawk Router 5G Router	The modem ensuring communication with other vehicles and infrastructure.
Switch	Hardware, Firmware, Software	Taltech	L2 Switch	Ethernet (Cat 6, 5E) L2 (VLAN segmentation)	Switch connects on- board unit and sensors and router. Manages access to the network and segments network in VLANs).
AV Shuttle Operating System	Middlewa re/Firmwa re OS	Taltech	-	OS interfaces (Proprietary port enabled, protected by access and authentication mechanisms)	ROS Melodic, Autoware 1.14
Self- driving applicatio n	Software	Taltech		Application interfaces (APIs, REST, JSON etc.) Messaging protocols Web services	Autoware.ai Application framework for self- driving vehicles.



				Database connectors	
Teleoperat ion services	Hardware, Middlewa re, Software, Data, Redundan cies	Teleoper ation Services Provider	Physical or virtual computing units, Operating System, Application Server, Web services, Databases and DBMS, Log files, configuration data	Network interfaces (Ethernet, Wi-Fi, 4G, Bluetooth) OS interfaces (SSH, RDP, etc.) Application interfaces (APIs, REST, etc.) Database connectors File Transfer Services (e.g., SFTP)	Control PC communicating using the teleoperation software which is a module of the ROS.
Teleoperat ion Module	Software	Taltech	ΑΡΙ	OS interfaces (SSH) – Access and Authentication using FIDO 2FA, TLSv1.3 and VPN	Module implemented in the ROS implementation.
AV OBU	Hardware, Firmware, Software	TalTech	Hardware – Network ports, Firmware/Route r OS, web application	CAMS (SPAT, MAP) CohDA proprietary protocol (ITS-G5)	On-board unit for communication with CohDA MKx smart RSU.
AV Shuttle Journey Planning Web Interface	Applicatio n, Log files, configurat ion data, Keys	Applicati on interface s – APIs to Web services GUI Integrati ons with sensor/te lematics data	Application, Log files, configuration data, Keys	Application interfaces – APIs to Web services GUI	Uses the GNSS location data to present a web interface to track the AV shuttle .
HSM	Hardware, Firmware, Software	Taltech		Network interface (Ethernet) Physical access (USB, Serial) HSM interfaces (STM32)	Hardware security module for the certificates of the V2X/ITS PKI. HSMs are contained in the embedded STM controllers in the Autonomous Vehicle and embedded IoT devices such as OBU, RSU.
Actuators	Hardware, Firmware, Software	Taltech		Network interface (Ethernet, CAN)	Actuators
				npus Infrastructure	
Smart RSU	Hardware Firmware, Software	TalTech	Hardware – Network ports, Firmware/Route r OS, web application	CohDA proprietary protocol (ITS-G5)	Illuminated road side unit which contains the CohDA OBU.
Smart RSU Relay	Hardware	TalTech	Network- Arduino	CohDA proprietary protocol (ITS-G5)	Arduino relay device for traffic light.
Traffic Managem ent Server	Hardware, Software	TalTech	Hardware – Network Ports, Physical Disk etc. Software – Application, OS, firmware	Intelligent Traffic Management Software.	Traffic management node for communication with RSUs.

Database connectors





## 4.3.2.2 Attack scenarios

The aim of Test-Case 2 (Adaptive Traffic Management) is to test the CitySCAPE toolkit's ability to detect cyber-attacks that target the integrity of the data and systems of the adaptive traffic management (V2X, OBU) process. The integrity of the adaptive traffic management data and systems is of utmost importance for ensuring safe navigation of multi-modal transportation components and users that use the traffic system. In this scenario, network traffic for V2X and AV OBU communication is enabled and the systems such as the AV OBU and V2X OBU are operational.

As in the previous test case, in order to perform test case 2 and try to attempt to affect the integrity of the roadside infrastructure, the following attack scenario steps were implemented:

- 1. **Fingerprinting** Trying to identify targets and potential vulnerabilities;
- 2. Getting in Trying to exploit vulnerabilities to break in;
- 3. **Modification of data** sent by the vehicle to the control server.

To perform this scenario and after several preliminary tests, Oppida has finally used the following tools in order to implement the attacks:

- Nmap,
- Wfuzz,
- Web browser,
- Postgres command lines,
- Hydra / crunch,
- Existing exploits scripts.

Due to the demonstrator configuration, it has not been possible to directly attack the roadside equipment. Attacks towards the ITS communication have been performed through the elements accessible by the central server and the vehicle network.

As in test case 1, this test case has also been divided into the same 2 sub test cases. The first case (sub-testcase 2.1) consisted in identifying and attacking targets from the internet (system elements with public IPs), which also targeted the control server (see Figure 1). In fact, this server hosts the postgresql database containing all the driving information sent by the vehicle to the server.

The second sub-testcase (sub-testcase 2.2) focused on identifying and targeting vulnerable vehicle sensors to modify their configuration or the data they transmit to the control server. This scenario focused on targeting the lidar administration web interface, as depicted in *Figure 37*.

More specifically for sub-testcase 2.1 a dedicated password list has been generated to brute force (with hydra) the PostgreSQL interface accessible from the internet to gain access to this data and then modifying it, while for the sub-testcase 2.2, the web administration interface has been used via web to modify the sensor configuration.



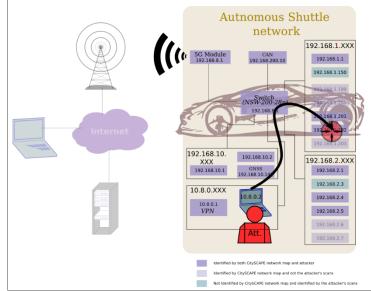


Figure 37. Sub-test case 2.2 involved elements

## 4.3.2.3 Modules behaviour

#### 4.3.2.3.1 SIEM

**Graylog** - Graylog receives alerts from the IDS/IPS component. In particular, during the scanning activity, several messages concerning the 'reset outside window ' were received.

	⇒ C	0 🔒 gr	<b>aylog</b> :9000	/search?q=rese	t&ranget	ype=absolute&fro	m=2022-08-2	25T06%3A00	%3A00.000Z&tc	=2022	ି <b>ଯ</b>	${igsidential}$
gray	log Search	Streams	Alerts	Dashboards	Enterpris	e Wizard +	System 👻	0			0 in 0 out	0
•	timestamp †₹										source 17	
-	2022-08-25 12:52:24	4.000 +02:00									server-desktop	
	server-desktop sn > 193.40.245.62:5		[129:15:2	] Reset outsid	e window	[Classification:	Potentially	Bad Traffic	[Priority: 2]	(TCP)	193.40.250.239:44	1452 -
	2022-08-25 12:51:39	.000 +02:00									server-desktop	
	server-desktop sn > 193.40.245.62:5		[129:15:2	] Reset outsid	e window	[Classification:	Potentially	Bad Traffic	[Priority: 2]	{TCP}	193.40.250.239:44	436 -
	2022-08-25 12:51:39	0.000 +02:00									server-desktop	
	server-desktop sn > 193.40.245.62:5		[129:15:2	] Reset outsid	e window	[Classification:	Potentially	Bad Traffic	[Priority: 2]	{TCP}	193.40.250.239:44	436 -
	2022-08-25 12:51:19	.000 +02:00									server-desktop	
	server-desktop sn > 193.40.245.62:5		[129:15:2	] Reset outsid	e window	[Classification:	Potentially	Bad Traffic	[Priority: 2]	{TCP}	193.40.250.239:53	8990 -
	2022-08-25 12:51:19	9.000 +02:00									server-desktop	
	server-desktop sn > 193.40.245.62:5				ais de l'anni	ication meet.google.co			[Destority: 2]	{TCP}	193.40.250.239:54	4022 -

Figure 38. Graylog receives alerts from the IDS/IPS component

This alert was not enough to conclude that an attack was in progress.

#### 4.3.2.3.2 IDS/IPS engine

In this test case, the IDS/IPS engine was still running in online mode. The new alerts identified during this attack were the following:

- Snort Alert [1:2010939:3] ET SCAN Suspicious inbound to PostgreSQL port 5432 [Classification: Potentially Bad Traffic] [Priority: 2]
- Stream5: Reset outside window [Classification: Potentially Bad Traffic] [Priority: 2]





In Figure 40, the summary of alerts generated during a specific time frame is depicted (12:59 CEET): the last one summarizes the alerts related to the PostgreSQL brute force.

In Figure 39, all the alerts have been generated during the whole sub-testcase 2.1.

		Di	splaying alerts	1-5 of 5 total				
	< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
	[snort] stream5: Reset outside window	bad-unknown	6610(7%)	1	2	2	2022-08-25 12:50:23	2022-08-25 12:50:59
	[snort] stream5: TCP Small Segment Threshold Exceeded	bad-unknown	3577(4%)	1	1	1	2022-08-25 12:50:23	2022-08-25 12:50:59
	[snort] ssh: Protocol mismatch	non-standard-protocol	80(0%)	1	1	1	2022-08-25 12:50:13	2022-08-25 12:50:59
	[snort] stream5: TCP session without 3-way handshake	bad-unknown	1825(2%)	1	4	2	2022-08-25 12:50:00	2022-08-25 12:50:59
Ō	[snort] Snort Alert [1:2010939:3]	bad-unknown	5(0%)	1	1	1	2022-08-25 12:50:23	2022-08-25 12:50:23
	ACTION							

Figure 39. IDS/IPS unique alerts generated during sub-testcase 2.1

			Displaying alerts 1-27 of	27 total		Displaying alerts 1-27 of 27 total									
	ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >									
	#0-(1-88843)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:59:10	118.193.31.186:46200	193.40.245.62:5432	TCP									
	#1-(1-88839)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:59:09	118.193.31.186:46162	193.40.245.62:5432	TCP									
	#2-(1-88838)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:59:08	118.193.31.186:46130	193.40.245.62:5432	TCP									
	#3-(1-88832)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:59:04	118.193.31.186:45950	193.40.245.62:5432	TCP									
	#4-(1-88806)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:58:42	118.193.31.186:54350	193.40.245.62:5432	TCP									
	#5-(1-77712)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:51:46	193.40.250.239:44452	193.40.245.62:5432	TCP									
	#6-(1-77369)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:51:39	193.40.250.239:44436	193.40.245.62:5432	TCP									
	#7-(1-62180)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:50:23	193.40.250.239:54330	193.40.245.62:5432	TCP									
	#8-(1-62179)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:50:23	193.40.250.239:54246	193.40.245.62:5432	TCP									
	#9-(1-62178)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:50:23	193.40.250.239:54250	193.40.245.62:5432	TCP									
	#10-(1-62177)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:50:23	193.40.250.239:54326	193.40.245.62:5432	TCP									
	#11-(1-62176)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:50:23	193.40.250.239:54252	193.40.245.62:5432	TCP									
	#12-(1-61430)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:45:12	162.142.125.160:5189	193.40.245.62:5432	TCP									
	#13-(1-61429)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:45:11	162.142.125.8:43102	193.40.245.62:5432	TCP									
	#14-(1-61428)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:45:11	162.142.125.8:35286	193.40.245.62:5432	TCP									
	#15-(1-61423)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:45:11	162.142.125.8:42748	193.40.245.62:5432	TCP									
	#16-(1-61422)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:45:10	162.142.125.136:24619	193.40.245.62:5432	TCP									
	#17-(1-60762)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:38:27	193.40.250.239:58232	193.40.245.62:5432	TCP									
	#18-(1-60749)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:38:18	193.40.250.239:28285	193.40.245.62:5432	TCP									
	#19-(1-60343)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:35:28	193.40.250.239:45492	193.40.245.62:5432	TCP									
	#20-(1-60342)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:35:28	193.40.250.239:45490	193.40.245.62:5432	TCP									
5	#21-(1-60341)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:35:28	193.40.250.239:45542	193.40.245.62:5432	TCP									
	#22-(1-60340)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:35:28	193.40.250.239:45496	193.40.245.62:5432	TCP									
	#23-(1-60339)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:35:28	193.40.250.239:45494	193.40.245.62:5432	TCP									
-	#24-(1-58055)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:10:30	212.70.149.10:58026	193.40.245.62:5432	TCP									
5	#25-(1-5395)	[snort] Snort Alert [1:2010939:3]	2022-08-25 11:41:05	36.139.53.192:54051	193.40.245.62:5432	TCP									
1	#26-(1-5365)	[snort] Snort Alert [1:2010939:3]	2022-08-25 11:40:42	37.157.70.163:38404	193.40.245.62:5432	TCP									

ACTION
[{ action } v] Selected ALL on Screen Entire Query]

Figure 40. All the IDS/IPS alerts related to PostgreSQL brute force generated during the subtestcase 2.1

Like sub-testcase 1.2, in sub-testcase 2.2 alerts related to the attack on the sensors in the vehicle (previously described) have not been generated, mostly the reason was that the IDS/IPS engine is deployed on the server machine and was not receiving all the traffic in the subnetwork.

#### 4.3.2.3.3 RITA

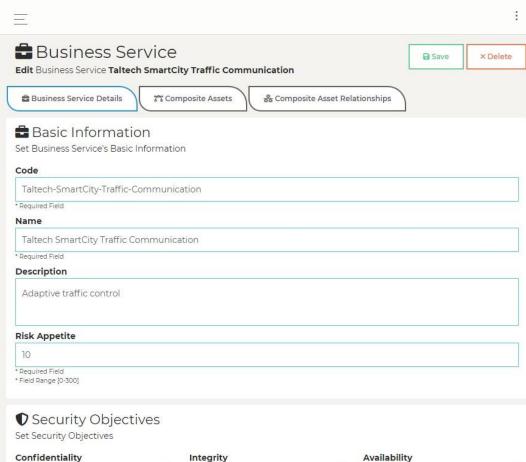
Prior to the attack, the RITA operator had already modeled the multimodal transport ecosystem in order to get the business service (namely Taltech-SmartCity-Traffic-Communication) overall risk and impact, as shown in Figure 41.

<u>A.B</u>	0								A Sea	nch	Q - Ø
CITYSCAPE	😚 Overall Risk Asse	essment	Result			00	Overall Ris 84/300		Risk Appe	tite	( Confidentiali
Risk Assessments Business Services						_	04,500				Integrity: 9 Availabi
Composite Assets Co	Composite Asset Thre		© Vulnerability Contribution Towards Overall Risk CVEs With Highest Risk Score On Assessment								
Vulnerabilities Threats	Overal Risk						Overal Risk				
Countermeasures			1973			90 80 70 60					
Cve Search Settings						50			_		
Settings		son seltatore Exp	Ichalion / Malicious Code Inte www.hasee.02) unauthorized	Access to Premises (Access to Premises uncationAcset-03) Denial	al Service	30 20 10					
	Netroincations-01 N/-Communications	Assitions-01 AV-Commune Ostorns-01 AV-Commune (Vehicle-0	Durating series of the series			0 CVE-2020-3404 CV	6-2020-3393 CVE-2018-100	10 CVE-2020-3503 CVE-2016-1	OVE-2020-3393 CVE-2020-3393	020-3408 CVE-2020-3407	2020-3407 CVE-2019-14626
0	Vehiclesconn					Care Ca	Const	Cre. Crew	Can- Can-	Core - Core	CALA
	(Weeks Communications of Ref Communications (1) Shares Explanations (2) Provide Communications (2) Pro										
						Ø Refresh					
e	C Refresh		Total & Inc	anact Assass	oent Decult	Ø Refresh					
e = Ne	♂ Refresh ■ Navigate lavigate & Filter Risks by <b>Business Se</b>	ervices,	75 Risk & Im Navigate to Risk A	pact Assessr	nent Result	Ø Refresh					
e = Ne	3 Refresh ■ Navigate avigate & Filter Risks by Business Se omposite Assets , Assets , Threats &	ervices, S Cvos tree 🚍	Navigate to Risk A			Ø Refresh	CVE	Confidentiality	Integrity	Availability	CIA Overall
e = Ne	♂ Refresh ■ Navigate lavigate & Filter Risks by <b>Business Se</b>	ervices, S Cvos tree 🚍	Navigate to Risk A	ssessment Analysis.			CVE	Confidentiality	Integrity	Availability	CIA Overall
e = Ne	3 Refresh Navigate lavigate & Filter Ricks by <b>Business Se</b> omposite <b>Assets</b> , <b>Assets</b> , <b>Threats</b> &	ervices, S Cvos tree 🚍	Navigate to Risk A	ssessment Analysis. Composite Asset		Threat	CVE CVE-2020-34		Integrity 0	Availability 36	CIA Overall 36
2 = Ni [	Refresh     Navigate     Navigate Stier Risks by Business Se     monoite Assets Assets - Threats 5     Interhommerication     Interhommerication     Filters	ervices, S Cvos tree 🚍	Navigate to Rick A Business Service Taltech-SmartCr	ssessment Analysis. Composite Asset	Asset AV-Communicat	Threat TH-09		0			
2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Befresh     Novigate     Novigate     Novigate Fiter Risk by Business Se     monoite Assets. Assets. Threats S     monoite Assets Assets.     Tratels-SmartChynaffe Communication     Fitters     elect & Befree Seach	ervices , a Cives tree = ation: Taltech	Navigate to Risk A Business Service Taltech-SmartCi Taltech-SmartCi	Composite Asset	Asset AV-Communicat	Threat TH-09 TH-11	CVE-2020-34	0	0	36	36
	Befrein     Novigate     N	ervices , 5 Cives tree = ation: Taitech	Navigate to Risk A Business Service Taitech-SmartCi Taitech-SmartCi Taitech-SmartCi	Steps and the set of t	Asset AV-Communicat AV-Communicat AV-Communicat	THreat TH-09 TH-11 TH-11	CVE-2020-34 CVE-2020-33 CVE-2020-34	0 12 0	0 36 0	36 36 36 36	36 84 36
	Befresh     Novigate     Novigate     Novigate Fiter Risk by Business Se     monoite Assets. Assets. Threats S     monoite Assets Assets.     Tratels-SamarConfunctionenum     Filters     elect & Befree Seach	ervices , 5 Cives tree = ation: Taitech	Navigate to Risk A Business Service Taitech-SmartQi Taitech-SmartQi Taitech-SmartQi Taitech-SmartQi	Vehicle-Commu Vehicle-Commu Vehicle-Commu	Asset AV-Communicat AV-Communicat AV-Communicat	Тнгеат Тн-09 Тн-11 Тн-11 Тн-21	CVE-2020-34 CVE-2020-34 CVE-2020-34 CVE-2020-34 CVE-2020-33	0 12 0 0	0 36 0 0	36 36 36 36 36	36 84 36 36 36
	Befresh     Navigate     N	ervices ; 8 Cives tree and attor: Taitsch Tritter tCity Traff)	Navigate to Risk A Business Service Taitech-SmartQi Taitech-SmartQi Taitech-SmartQi Taitech-SmartQi	Steps and the set of t	Asset AV-Communicat AV-Communicat AV-Communicat	Тнгеат Тн-09 Тн-11 Тн-11 Тн-21	CVE-2020-34 CVE-2020-33 CVE-2020-34	0 12 0 0	0 36 0	36 36 36 36	36 84 36
	Refresh     Navigate     Navigate     Navigate     Navigate     Navigate     Navigate     Singet     Sing	ervices ; 8 Cives tree and attor: Taitsch Tritter tCity Traff)	Navigate to Risk A Business Service Taitech-SmartO Taitech-SmartCi Taitech-SmartCi Taitech-SmartCi Taitech-SmartCi	Vehicle-Commu Vehicle-Commu Vehicle-Commu	Asset AV-Communicat AV-Communicat AV-Communicat AV-Communicat	TH-09 TH-11 TH-11 TH-21 TH-21	CVE-2020-34 CVE-2020-34 CVE-2020-34 CVE-2020-34 CVE-2020-33	0 12 0 0 0	0 36 0 0	36 36 36 36 36	36 84 36 36 36
	Befreish     Navigate	ervices ; 8 Cives tree and attor: Taitsch Tritter tCity Traff)	Navigate to Risk A Business Service Taitech-SmartCi Taitech-SmartCi Taitech-SmartCi Taitech-SmartCi Taitech-SmartCi Taitech-SmartCi	Sessment Analysis. Composite Asset Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu	Asset AV-Communicat AV-Communicat AV-Communicat AV-Communicat AV-Communicat	TH-09 TH-11 TH-21 TH-21	CVE-2020-34 CVE-2020-34 CVE-2020-34 CVE-2020-34 CVE-2020-34	0 12 0 0 0 0 12	0 36 0 0 0	36 36 36 36 36 36 36	36 84 36 36 36 35
	Befreish     Navigate	ervices ; 8 Cives tree and attor: Taitsch Tritter tCity Traff)	Navigate to Risk A Business Service Taitech-SmartCi Taitech-SmartCi Taitech-SmartCi Taitech-SmartCi Taitech-SmartCi Taitech-SmartCi Taitech-SmartCi	Sessment Analysis. Composite Asset Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu	Asset AV-Communicat AV-Communicat AV-Communicat AV-Communicat AV-Communicat AV-Communicat	TH-09 TH-11 TH-11 TH-21 TH-21 TH-24 TH-25	CVE-2020-34 CVE-2020-34 CVE-2020-34 CVE-2020-34 CVE-2020-34 CVE-2020-34 CVE-2020-34	0 12 0 0 0 12 12 12	0 36 0 0 0 36	36 36 36 36 36 36 0	36 84 36 36 36 36 36 36 48
	Befreish     Navigate	ervices ; 8 Cives tree and attor: Taitsch Tritter tCity Traff)	Navigate to Risk A Business Service Taitech-SmartCi Taitech-SmartCi Taitech-SmartCi Taitech-SmartCi Taitech-SmartCi Taitech-SmartCi Taitech-SmartCi Taitech-SmartCi	Composite Asset Composite Asset Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu	Asset AV-Communicat AV-Communicat AV-Communicat AV-Communicat AV-Communicat AV-Communicat AV-Communicat	TH-09 TH-11 TH-11 TH-21 TH-21 TH-24 TH-25 TH-25	CVE-2020-34 CVE-2020-34 CVE-2020-33 CVE-2020-33 CVE-2020-34 CVE-2020-34 CVE-2020-35 CVE-2020-34	0 12 0 0 0 12 12 12 12	0 36 0 0 0 36 36 36	36 36 36 36 36 36 0 0 0 36	36           84           36           36           36           36           48           48           48           48
	Befreish     Navigate	ervices ; 8 Cives tree and attor: Taitsch Tritter tCity Traff)	Navigate to Bisk A Business Service Taltech-SmartCi Taltech-SmartCi Taltech-SmartCi Taltech-SmartCi Taltech-SmartCi Taltech-SmartCi Taltech-SmartCi	Composite Asset Composite Asset Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu	Asset AV-Communicat AV-Communicat AV-Communicat AV-Communicat AV-Communicat AV-Communicat AV-Communicat AV-Communicat	TH-09 TH-09 TH-11 TH-21 TH-21 TH-22 TH-25 TH-25 TH-25 TH-02	CVE-2020-34 CVE-2020-32 CVE-2020-32 CVE-2020-33 CVE-2020-34 CVE-2020-34 CVE-2020-34 CVE-2020-34 CVE-2020-34 CVE-2020-34	0 12 0 0 0 12 12 12 12 12 0	0 36 0 0 0 36 36 36 36 36 0	36 36 36 36 36 36 0 0 0 36 36 36 36	36           84           35           36           36           48           48           84           35           36           36           36           36           36           36           36           36           36           36           36           36           36           36           36           36           37           38           39           36
	Befreish     Navigate	ervices ; 8 Cives tree and attor: Taitsch Tritter tCity Traff)	Navigate to Bisk A Business Service Taltech-SmartCi Taltech-SmartCi Taltech-SmartCi Taltech-SmartCi Taltech-SmartCi Taltech-SmartCi Taltech-SmartCi	Composite Asset Composite Asset Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu Vehicle-Commu	Asset AV-Communicat AV-Communicat AV-Communicat AV-Communicat AV-Communicat AV-Communicat AV-Communicat AV-Communicat	TH-09 TH-09 TH-11 TH-21 TH-21 TH-22 TH-25 TH-25 TH-25 TH-02	CVE-2020-34 CVE-2020-34 CVE-2020-33 CVE-2020-33 CVE-2020-34 CVE-2020-34 CVE-2020-35 CVE-2020-34	0 12 0 0 0 12 12 12 12 12 0	0 36 0 0 0 36 36 36	36 36 36 36 36 36 0 0 0 36	36           84           36           36           36           36           48           48           48           48

Figure 41. AV Shuttle Network Communication Overall Risk and Impact

For that reason, the risk assessor has decomposed the business service to the list of composite assets, as shown in Figure 42 and Figure 43.





#### 3 (Low)

The Unauthorized Disclosure Of Data O Information Could Be Expected To Have A 1-4 Limited Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 5-6 Serious Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 7-10 Severe Or Catastrophic Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals \* Required Field

#### Accountability

Not Being Able To Ensure That The Actions Of An Entity May Be Traced Uniquely To That Entity Could Be Expected To Have A 1-4 Limited Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 5-6 Serious Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 7-10 Severe Or Catastrophic Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals \* Required Field

#### Integrity

#### ✓ 9 (Very High)

The Unauthorized Modification Or Destruction Of Data Or Information Could Be Expected To Have A 1-4 Limited Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 5-6 Serious Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 7-10 Severe Or Catastrophic Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals \* Required Field

#### Non Repudiation

Not Being Able To Protect Against An Individual Falsely Denying Having Performed A Particular Action Could Be Expected To Have A 1-4 Limited Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 5-6 Serious Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 7-10 Severe Or Catastrophic Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals \* Required Field

#### Availability

9 (Very High)

The Disruption Of Access To Or Use Of Information Or An Information System Could Be Expected To Have A

1-4 Limited Adverse Effect On Organ Operations, Organizational Assets, Or Individuals 5-6 Serious Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 7-10 Severe Or Catastrophic Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals \* Required Field

#### Authenticity

Not Being Able To Be Prove That Data Or Information Is Genuine And Can Verified And Trusted Could Be Expected To Have A 1-4 Limited Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 5-6 Serious Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals 7-10 Severe Or Catastrophic Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals \* Required Field

Figure 42. AV Shuttle Network Communication Business Service (Basic Information)



Business Service	affic Communication
Business Service Details	te Assets 🔓 Composite Asset Relationships
Composite Assets	
ect Composite Assets Supporting The Bi	composite Asset
	Q Vehicle-Communications-01 AV communication
]	Q AV-RSUCommunication AV RSU and OBU Com

Figure 43. AV Shuttle Network Communication Business Service (Composite Assets)

Following that, the risk assessor decomposed each composite asset to its basic assets, extracting the identified threats, their likelihood and any applicable counter-measures.

During the Pilot Demonstration, as soon as the CSIRP operator finished their incident analysis, the identified threats and vulnerabilities (included in the IRIS incident reports) were sent to RITA. As a result, the risk assessor had to re-evaluate the security posture and impact of the business service by reviewing and updating the threat probabilities and any available countermeasure.

Additional figures depicting the RITA functionality during the Pilot Demonstration can be found in Annex III.

- For AV communications (Vehicle-Communications-01) this is shown in Annex II Figure 7, Figure 8, Figure 9 and Figure 10, including the assets relationships shown in Figure 11.
- For AV RSU and OBU Communications, this is shown in Annex III Error! Reference source not found., Error! Reference source not found., Error! Reference source not found., Error! Reference source not found. and Error! Reference source not found., including the assets relationships shown in Error! Reference source not found.

### 



XSOAR was not active in this test-case.

#### 4.3.2.3.5 CTIP

CTIP was not active in this test-case. In the background, Graylog periodically launches requests to the CTIP to gather relevant IOCs. Since the attacker in the use-case 1 was a new, unknown actor, no data was available to enrich the alert generated.

#### 4.3.2.3.6CSIRP

CSIRP was not active in this test-case.

#### 4.3.2.4 Future activities

Tallinn Pilot permitted identifying that more data was needed inside the SIEM to perform effective detection.

In the following month, log collection from shuttle internal server into Graylog will be implemented, and specific parsers and detection rules will be added to ensure those logs will be correctly exploited. A playbook to handle this incident will also be implemented into the SOAR.

# 4.3.3 Test Case 3: Fraudulent manipulation of the Payment Validation System

#### 4.3.3.1 Test-case scope

In this scenario, a passenger wants to validate her ticket/card for the transportation journey. The passenger will be on-board the means of transportation. The passenger has multiple methods for ticket validation for her user journey:

• The passenger taps their Tallinn Transport smart card on the Validator.

The desired behaviour of the system is as below:

 The payment validator service/app checks the passenger data against a database. If the smart card, ticket, or credit card are fraudulent/expired/not valid, the validation will be rejected. If the validation is genuine, then a sound from the validator will acknowledge the successful validation.

The following table describes the assets involved in the scenario and the scope of each of them:

Name	Туре	Manage d by / Owned by	Basic Asset breakdown	Interfaces	Role
Payment service system	Hardware , Middlewa re, Software, Data, Redunda ncies	TalTech	Physical or virtual computing units, Operating System, Application Server, Web services,	Network interfaces (Ethernet, Wifi, 4G, Bluetooth) OS interfaces (SSH, Telnet, RDP, etc.) Docker Flask Web Server Application interfaces (APIs, REST, etc.)	System that manages ticketing service, holds the information on the active subscriptions, allows new registrations and manages payments.

CitySCAPE					
			Databases and DBMS, Log files, configuration data	Database connectors File Transfer Services (e.g., SFTP) NFC interface/RFID interface	
			Payment Va	alidation System	
HMI Machine Validator	Hardware , Middlewa re, Software	TalTech	Hardware (network interfaces, sensors, credit card, micro- computer, touch display), Firmware, OS, Log and configuration files	Network interfaces - RFID, Ethernet, NFC, QR Code, Credit Card, User Interface	Selling/Ticket Validator.
Gateway	Hardware , Middlewa re, Software	TalTech	Physical computing units, Operating System, APIs, Application Server, Software components, Local data assets (databases), Log files, configuration data	Standard computer hw interfaces Network interfaces (Ethernet) OS interfaces (SSH, Telnet, RDP, etc.) Application interfaces (APIs, REST, JSON etc.) Web services Database connectors Interfaces for ISO8583 (financial transactions)	Gateway between ticketing system and the acquiring bank.
Communi cation Module	Hardware , Middlewa re	TalTech	Modem, Firmware, Log and configuration files	CAN bus, 3G/4G	Used for communication of the Payment service with internal network and external network.

Table 7. Assets involved in the scenario 3

# 4.3.3.2 Attack scenarios

The aim of this Test-Case is to test the ability of the CitySCAPE toolkit to detect fraud attacks on the ticket validation system. The integrity of the ticket validation system is of paramount importance for enabling authentication of users and tickets on public transport journeys. This Test-Case focuses on a cyber-attack which consists of a fraudulent user, who has cloned a transportation card to obtain free transport journeys.

The attack was carried out as follows:

1. Ticket validator has a hidden configuration window for connections it makes, that can be found by clicking on the screen. Validator is also not locked in kiosk mode.

2. Knowing IP scan website through the dirb scanner, as follows. dirb <u>http://193.40.245.62/validator</u>

---- Scanning URL: <u>http://193.40.245.62/validator/</u> ----+ <u>http://193.40.245.62/validator/add</u> (CODE:405|SIZE:178)





- + <u>http://193.40.245.62/validator/logs</u> (CODE:401|SIZE:19)
- + <u>http://193.40.245.62/validator/manage</u> (CODE:401|SIZE:19)
- + <u>http://193.40.245.62/validator/sync</u> (CODE:200|SIZE:63)

3. Finding validator/sync/ endpoint, which would provide to the attacker valid UID-s.

4. Cloning the card with the UID found in the database, example: DEADBEEF, using mifare card tool on android and magic mifare 1k card.

5. Getting successful validation on the bus using the cloned card.

Other possible attacks include brute force incremental and random sampling.

#### 4.3.3.2.1 Outcome of the vulnerable PoC study

The attack shown during the Pilot could have been detected at the following stages:

- When the attacker scan the server for accessible folders using dirbuster;
- When the attacker accesses the confidential endpoint /sync containing the cards' UIDs.

Those two detections possibilities can only be carried on if the access logs generated by the apache server are sent to Graylog SIEM for analysis, which was not available in the time required for analysis and customisation. The fraudulent manipulation of the payment validation system cannot be detected, since the fraudulent card generated is a perfect clone of the original one; thus, to the system, it appears legitimate. The detection solution presented above can only detect the fact that the information necessary to fraud has been stolen, but not that it has been exploited.

#### 4.3.3.2.2 Future activities

Tallinn Pilot permitted to identify that more data was needed inside the SIEM to perform effective detection. In the following month, log collection from the apache server into Graylog will be implemented, and specific parsers and detection rules will be added to ensure those logs will be correctly exploited. A playbook to handle this incident will also be implemented into the SOAR. Nonetheless, as stated previously, the solution will detect that information necessary to fraud has been stolen, but not that it has been exploited.

# 4.3.4 Test Case 4: Integrity of GNSS System

#### 4.3.4.1 Test-case scope

This Test-Case has a similar scope with Test-Case 1, i.e. the AV Shuttle provides last-mile transportation for Tallinn Passengers. The difference is in the target system, which, for this Test-Case, focuses on the Global Positioning System (GPS) which localises the transportation mode.







In this scenario, the passenger is able to move from the city transportation mode to the last-mile services (AV Shuttle) seamlessly. The passenger interactions to achieve this are presented below.

- 1. Passenger departs from the city-transport mode and reaches the AV Shuttle.
- 2. The AV Shuttle carries the passenger to the end destination.

The following table describes the assets involved in the scenario and the scope of each of them.

Name	Туре	Manage d by / Owned by	Basic A breakdown	Asset	Interfaces	Role
Mobile Network (4G/5G/)	Network	TalTech	4G and Router	5G	Via network (DSRC, UDP, TLS1.3) to anyone having a valid subscription to the network (Access via 2F Authentication using FIDO tokens and VPN)	Communication between Remote Operations Center and AV Shuttle.
Adhoc vehicular network	Network	Taltech	-		Via ITS messages to anyone part of the ITS-V2X network OBU (CohDA Mk5) RSU (CohDA MKx) CAMS Messages (CohDA proprietary protocol (MAP, SPAT etc.), ITS-G5 Application Compliant)	Direct adhoc communication between vehicles and roadside units.
			Autonor	nous S	Self-Driving Shuttle	
Vehicle on- board Computer	Hardware	Taltech	Physical computing units, Opera System, Application Server, Soft component Local assets (databases), files, configuratic data	APIs, ware s, data , Log	Network interfaces (Ethernet, CAN, Serial) OS (Ubuntu 16.01) Middleware (ROS Kinetic Kame) Applications (Autoware.Auto, Skyhook)	The vehicle computer.
Camera Sensors	Hardware, Firmware	Taltech	Physical Log configuratic data	Unit, files, on	IP Connected to On-board Unit.	The vehicle on-board cameras.
Camera Data	Data asset	Taltech	Physical Log configuratic data	Unit, files, on	Camera data is stored in the ROSBag logging system.	The video files from on- board camera.
GNSS	Hardware, Firmware	Taltech	Physical Log configuratic data	Unit, files, on	IP connected GNSS sensor using Skyhook GPS application.	The vehicle GNSS system. Used for geo- location/ SLAM.
IMU	Hardware, Firmware	Taltech	5		CAN bus interface, integrated with GPS	Vehicle IMU for capturing of measurement data of AV (acceleration, orientation, heading).
Ultrasonic Sensors	Hardware, Firmware	Taltech	Physical Log configuratic data	Unit, files, on	IP connected to on-board L2 switch.	Used for short-range object detection.
Lidar	Hardware, Firmware	Taltech	Physical Log	Unit, files,	IP connected to on-board L2 switch.	LiDAR used for 3D point cloud mapping to build dynamic maps for SLAM.

# CitySCAPE



CITYDEAL					* 4 *
			configuration data		
Local Dynamic Map	Data asset	Taltech	configuration data	Application interfaces (APIs, REST, JSON etc.) Web services Database connectors	The vehicle complete database.
Communic ation modem	Hardware, Firmware, Software	Taltech	4G and 5G Router	Network interface (Ethernet, CAN) V2X 4G M2 Nighthawk Router 5G Router	The modem ensuring communication with other vehicles and infrastructure.
Switch	Hardware, Firmware, Software	Taltech	L2 Switch	Ethernet (Cat 6, 5E) L2 (VLAN segmentation)	Switch connects on- board unit and sensors and router. Manages access to the network and segments network in VLANs).
AV Shuttle Operating System	Middlewa re/Firmwa re OS	Taltech	-	OS interfaces (Proprietary port enabled, protected by access and authentication mechanisms)	ROS Melodic, Autoware 1.14
Self- driving applicatio n	Software	Taltech		Application interfaces (APIs, REST, JSON etc.) Messaging protocols Web services Database connectors	Autoware.ai Application framework for self-driving vehicles.
Teleoperat ion services	Hardware, Middlewa re, Software, Data, Redundan cies	Teleoper ation Services Provider	Physical or virtual computing units, Operating System, Application Server, Web services, Databases and DBMS, Log files, configuration data	Network interfaces (Ethernet, Wi-Fi, 4G, Bluetooth) OS interfaces (SSH, RDP, etc.) Application interfaces (APIs, REST, etc.) Database connectors File Transfer Services (e.g., SFTP)	Control PC communicating using the teleoperation software which is a module of the ROS.
Teleoperat ion Module	Software	Taltech	API	OS interfaces (SSH) – Access and Authentication using FIDO 2FA, TLSv1.3 and VPN	Module implemented in the ROS implementation.
Actuators	Hardware, Firmware,	Taltech		Network interface (Ethernet, CAN)	Actuators

Table 8. Assets involved in the scenario 4

## 4.3.4.2 Attack scenarios

Software

The aim of this Test-Case is to test the ability of the CitySCAPE toolkit to detect cyber-attacks, which impact the integrity of the GNSS used in the transportation system. Integrity of GNSS is crucial for accurate positioning. The scope of the attack is limited to the GNSS telemetry data received by the AV Shuttle system.

Following the same process as for Test Cases 1 and 2. The attacker performs the following steps:

- Fingerprinting Trying to identify targets and potential vulnerabilities
- Getting in Trying to exploit vulnerabilities to break in;
- Modification of data provided by GNSS.



The same tools as for test case 2 were used:



- Nmap
   N/ab brauraar
- Web browser
- Postgres command lines,
- Hydra / crunch

Here again, the implied elements were the control server (see Figure 1) as depicted in Figure 44 for test case 4.1 and the GNSS unit located in the vehicle, as depicted in Figure 44. In the first case, the final target was to modify the server PostgreSQL to change the stored GNSS data and in the second case to modify the GNSS service configuration itself to affect the GNSS behaviour.

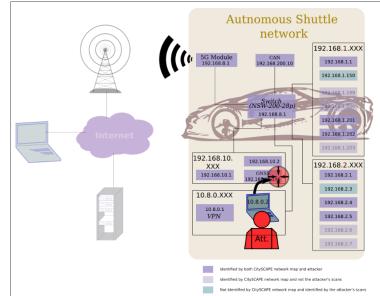


Figure 44. Test case 4.2 involved elements

#### 4.3.4.3 Outcomes

Since this attack involves more complex interactions inside the vehicle data ecosystem than others (the attack was a manipulation of data and did not involve malicious network packet injection or other visible markers), additional time was required to understand which CitySCAPE tools could detect the attack, how and when in the attack kill chain. The attack was workshopped at the TALLINN Pilot and it was conclusion is that the SIEM platform offered the most appropriate tool to detect this attack. The attack couldn't be conducted during the 24th and 25th as additional time is needed to tune and train the SIEM for this attack.

## 4.3.4.4 Future activities

During the operational data collection (beginning of July) it was found that the shuttle server log generation was not compatible with Graylog log collection interface. Therefore, the data analysis by the SIEM operators could not be conducted in time for the TALLINN Pilot on the 24th and 25th of August. Further developments are needed to create a compatible interface and ensure data necessary for detection is available to the SIEM. This is being progressed in September.

# CitySCAPE



# 4.3.5 Test Case 5: Transport Data Integration with Mobile Application (SIGLA Move)

#### 4.3.5.1 Test-case scope

As described in the work proposed initially within the DoA, the project would also consider cyber-security aspects related to mobile technology-based services for passengers using multimodal transportations systems.

In particular, the project wants to address matters of relevance related to the management of the citizens' access to a broad set of city-level multimodal transport organizations services. On one side, the secure access management for citizens to all types of vehicles (thanks to mobile based services) is considered, as well as the assurance and protection of citizens and services against specific cyber-attacks in the multimodal transport domain, addressing interconnected threats and propagated vulnerabilities. The project planned to consider smartphones as the nowadays prominent way to access the multiple means (and the services to use them). As described in deliverable D3.3, the solution implemented integrates in a brand-new development (CitySCAPE Mobile Security Toolkit – also referred as "Mob-Sec"), a commercial product (Kaspersky KMS) to safeguard the passenger's access and data to multimodal transport services.

This Mob-Sec has been integrated into SIGLAMoving, a mobile based solution for the provision of Infomobility services related to multimodal transport systems, that the colleagues from SIGLA designed and developed for CitySCAPE.

This let the consortium to enrich the Tallinn pilot activities (and the project) with activities related to mobile security investigations and experimentation.

Having as objective to validate Mob-Sec - through SIGLAMoving - the efficiency in detecting vulnerabilities and attacks against mobile-based technological solutions and services, four attack scenarios (described within the next section) has been designed, implemented and executed during the Tallinn pilot activities.

As described in CitySCAPE deliverables (e.g., D7.1 "Pilot scenarios, validation plan, and Pre-piloting preparation"), a number of elements are necessary to be available to perform the piloting activities. It needs to consider that the pilot activity - focusing on SIGLAMoving and, consequently, on CitySCAPE Mob-Sec - adopts Kaspersky Mobile Security SDK by KSP on mobile application and integrates with SIEM by ACS and RITA by ED and UPRC.

Name	Туре		Basic Asset Breakdown	Interfaces	Role
Mobile device	Hardwa re	Tallinn	A mobile device where SIGLAMoving (and	-	Hosting installation of mobile apps

The elements are reported in the following table.

CitySCAPE	

CitySCAPE					· · · · · · · · · · · · · · · · · · ·
			consequently the CitySCAPE Mobile Security Toolkit) can be installed		
Mobile Network (4G/5G)	Networ k	Tallinn	The Mobile device should have access / is endowed of a mobile network access	Via SIM card and WiFi	Supporting communicat ion features
SIGLAMovi ng Mobile App	Softwar e	SIGLA	The mobile app delivering both info- mobility services and CitySCAPE Mobile Security Toolkit cyber- security features	Via dedicated registration to "beta tester" channel on PlayStore	Detecting threat and vulnerabilitie s on mobile services (as infomobility ones)
SIGLAMovi ng back- end API	Softwar e	SIGLA	The back-end API of SIGLAMoving solution	Via HTTP Restful based API and json	Provides services on infomobility to access local transports
CitySCAPE Mobile Security Toolkit API	Softwar e	SIGLA & KSP	The back-end API element of the CitySCAPE Mobile Security Toolkit	Via HTTP Restful based API and json	Collects cyber- security information from mobile and forwards them to SIEM and RITA
SIEM	Softwar e	ACS	The SIEM of the CitySCAPE toolkit (see D3.3)	<ul> <li>Via HTTP Restful</li> <li>based API</li> <li>and json</li> <li>User</li> <li>Interface</li> <li>dedicated</li> <li>dashboard</li> <li>s</li> </ul>	Supports analysis and monitoring activities of LTP cyber- security managemen t team

<u>A</u> ₽₽₽₽₽ CitySCAPE					an a
RITA	Softwar e	ED	Element of CitySCAPE toolkit called RITA (see D3.3)	Restful based API and json - User Interface dedicated	activities of LTP cyber- security managemen
				dashboard s	t team

Table 9. Elements of Transport Data Integration with SIGLA App

Besides these elements, Android mobile phone accounts are also needed to be registered for installation of SIGLAMoving solution from the Android PlayStore "alpha channel".

They were communicated via email to SIGLA contact persons to be enrolled into the "alpha channel" programme.

The piloting activity lasted for 5 days, repeating the same tests for two people each day.

The attack scenarios were designed considering the guideline of test cases stories described in deliverable D3.3 "CitySCAPE architecture: modules and interfaces" for the Mob-Sec validation execution, whose relationship with the technical test procedures have been already described in WP7 pilot's documentation (D7.1).

	User Story
User story A	Anna [U]] a citizen of a European city (e.g., Genova or Tallinn), needs to go visit Elena, a friend of hers, staying in the surroundings of the city she lives in. In line with her will to embrace a sustainable lifestyle, Anna wants to use the services provided by the Public Transport System to reach Elena. This implies using a set of multimodal transport services, namely: a bus, a metro, another bus and an urban (small) train. She has already done this trip numerous times and since she already knows what lines and transport services to use, she starts planning her travel. For this reason, she collects information via the transport company's mobile application. The application is linked with the Mob-Sec features. Hence, when she opens the transport company's mobile application, a full antivirus check is performed, and a couple of threats are identified and registered locally in the form of logs transparently to Anna's usage of the mobile application. Those collected data are sent to the Mob-Sec back-end, SIEM and RITA in near real time.
User story B	Anna [U1] a citizen of a European city (e.g., Genova or Tallinn), needs to go visit Elena, a friend of her, staying in the surroundings of the city she lives in. In line with her will to embrace a sustainable lifestyle, Anna wants to use the services provided by the Public Transport System to reach Elena. However, Anna lives close to 2 bus stops, both at walking distance: one closer, one further. Consequently, she needs to check where the closest bus stop is and when the first bus arrives. For this reason, she checks for



	relevant information via the transport company's mobile application. The application is linked with the Mob-Sec features. Hence, when she accesses the transport company's mobile application to query for bus stops and arrival times, Mob-Sec verifies whether the API URLs used by the transport company mobile application are safe. Any identified security issues, such as threats and vulnerabilities, are registered locally and sent to the Mob-Sec backend, SIEM and RITA in near real time. The transport company mobile application indicates to Anna that bus line 3 is coming in 12 minutes, so she walks to the further bus stop to do a bit of exercise.
User story C	Anna [U1] a citizen of a European city (e.g., Genova or Tallinn), needs to go visit Elena, a friend of her, staying in the surroundings of the city she lives in. In line with her will to embrace a sustainable lifestyle, Anna wants to use the services provided by the Public Transport System to reach Elena. After checking for the closest bus stop and arrival times, via the transport company mobile application, she selects the bus stop of preference. When she arrives at the bus stop, she checks on the transport company mobile application that the bus is arriving in 1 minute. She makes use of the transport company mobile application to buy her a ticket. Since the application is linked with the Mob-Sec features, Mob-Sec verifies whether the API URLs used for the payment service are secure. Any identified security issues, such as threats and vulnerabilities are registered locally and sent to the Mob-Sec back-end, SIEM and RITA in near real time.
User story D	Anna [U1] a citizen of a European city (e.g., Genova or Tallinn), needs to go visit Elena, a friend of her, staying in the surroundings of the city she lives in. In line with her will to embrace sustainable lifestyle, Anna uses the services provided by the Public Transport System to reach Elena. Using the transport company mobile application, she selects bus line 3 towards the metro station 'A'. While sat on the bus, she uses her mobile phone and from time to time she checks line 3 stops to understand exactly where to disempark. When she reaches the Metro 'A' station bus stop, she checks on the transport company mobile application the arrival time of the next metro: it arrives in 5 minutes. Since the application is linked with the Mob-Sec features, Mob-Sec verifies that the API URLs used for accessing the arrival times are safe. However, to obtain arrival time information the mobile phone connects to a local Wi-Fi. Since the application is linked with the Mob-Sec registers locally all identified security issues, such as threats and vulnerabilities and sends them to the Mob-Sec back-end, SIEM and RITA in near real time. Later, Anna reaches the train station after having travelled a few minutes on metro and then on bus 22. Her phone connects to a local Wi-Fi, provided by a bar where she sat to have a coffee while waiting for her train. Mob-Sec verifies whether the connection is secure and unfortunately it is not. Mob-Sec registers locally all identified security issues, such as threats and vulnerabilities and sends them to the Mob-Sec back-end, SIEM and RITA in near real time. Later, Anna reaches the train station after having travelled a few minutes on metro and then on bus 22. Her phone connects to a local Wi-Fi, provided by a bar where she sat to have a coffee while waiting for her train. Mob-Sec verifies whether the connection is secure and unfortunately it is not. Mob-Sec registers locally all identified security issues, such as threats

# CitySCAPE

CILYSCF					
	and vulnerabilities and sends them to the Mob-Sec backend, SIEM				
	and RITA in near real time				
User	Fabio [U2] a registered CitySCAPE security officer (SOC) working at				
story	the Local Transport Company, is using the CitySCAPE toolkit to				
E	receive and manage all information produced by Mob-Sec and the				
	rest of CitySCAPE components. Any identified security issues,				
	including threats and vulnerabilities that are sent to the Mob-Sec				
	backend is visualised through the SIEM user interface, allowing				
	Fabio to implement policies to face those vulnerabilities identified				
	Furthermore, once per day the Mob-Sec backend sends the				
	identified security issues to RITA, allowing Fabio to calculate what				
	is the risk and impact to the transport services as a result of the				
	identified security issues, allowing him to plan and implement				
	appropriate countermeasures				

The execution of scenarios was performed with two different smartphones, one per person: one rooted and one not. This is not compulsory, but it was necessary to test "root detection" security feature.

Data produced by Mobile Security Toolkit through SIGLA Moving are regularly sent to SIEM and RITA. In case, connection issue happens between

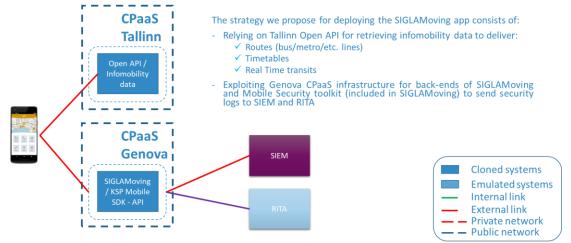


Figure 45. Mob-Sec CitySCAPE deployment architecture

Mobile Security Toolkit and SIEM/RITA, the server elements of Mobile Security Toolkit logs locally the sent data (to avoid permanent data loss).

As described in the previous figure, the deployment of Mob-Sec solution and its integration into Tallin CPaaS involved a mobile application (i.e., SIGLAMoving integrating KMS and Mob-Sec front-end modules), server-side API elements - hosted on Amazon AWS for both pilot sites by AMT and managed by SIGLA (i.e., the Mob-Sec backend), SIEM and RITA.

Within this infrastructure, the vulnerabilities and attacks detected by KSP KMS are logged by Mob-Sec front-end module. This latter sends them (tagged meaningfully according to the detected attack category) to Mob-Sec back-end module that forwards them to SIEM and RITA.

## 4.3.5.2 Attack scenarios

This section describes the attack scenarios referring to the 4 user stories associated to Mob-Sec validation (see previous chapter user stories).





The considered individual attacks and vulnerabilities and the association to each of these four scenarios are described in detail within deliverable D7.1 "Pilot scenarios, validation plan, and Pre-piloting preparation" at section 3.4.6 Test procedures, 3.4.7 Test Cases description and 3.4.8 CitySCAPE User stories.

To support the performance of attack tests and validation, a test configuration manual dedicated to pilot partners was prepared by SIGLA. This action was meant to describe in detail how to produce each attack and vulnerability conditions independently.

### 4.3.5.2.1 Scenario A

[A]: The first scenery is very easy to be replicated. In fact, Anna has to open the SiglaMoving App, the backend will work in background, and will detect smartphone's vulnerabilities. At the end of the detection process, the main page of the app will display (see Figure 46).

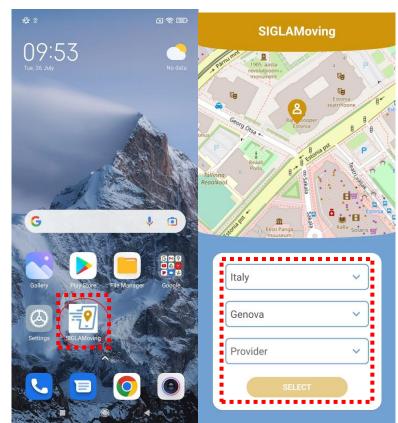


Figure 46. SiglaMoving App

#### 4.3.5.2.2 Scenario B

[B]: To replicate this scenario, first we have to select a provider in the SiglaMoving main page, in that way we unlock the "Select" button. Once we are inside the App, we can click on the routes section.







Figure 47. Selected provider

On the page that will be loaded, all the data on the available routes of the public transport provider (in that case we use the route 3 for example) can be found, then we need to move from the timetable to the maps tab.

< Routes		<		21		
Search here	٩	time startin	table ng point i jaam 6	Stops		maps
7 SELI - SÕJAMÄE	~	to Lan	di			
8 VIRU KESKUS - ÄIGRUMÄE	~	10:21	11:01	11:23	12:03	12:23
9 KADAKA - PRIISLE	~	13:03 15:23	13:23 16:04	14:03 16:24	14:23 17:06	15:03 17:26
10 VÄIKE-ÕISMÄE - VANA-PÄÄSKÜLA	~	18:08 20:55	18:30 21:17	19:25 21:38	20:10 22:01	20:33 22:23
10 (28-31.08) VÄIKE-ÕISMÄE - LAANIKU	~	22:45	23:08	23:30		
11 KADAKA - KIVISILLA	~					
12 VÄIKE-ÕISMÄE - PRIISLE	~					
13 VÄIKE-ÕISMÄE - SELI	~					
14 VIRU KESKUS - VANA-PÄÄSKÜLA Figure 48. Re	<b>~</b>	and tim		08/2022		







From here we can see all the bus stops along the 3 bus route. By enlarging the section of the map, we can see more specifically which bus stop is closer or farther away and decide accordingly which one to reach.



Figure 49. Bus line and stops

#### 4.3.5.2.3 Scenario C

[C] : For this scenario we need, to open SiglaMoving app, and this time, in the main page, we have first to check the arrivals time of the bus, in the "Transits" section .





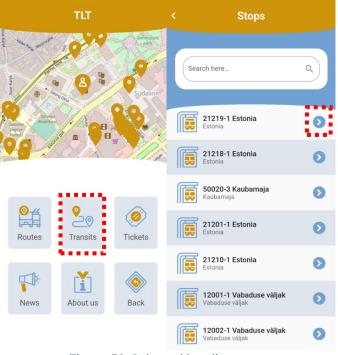
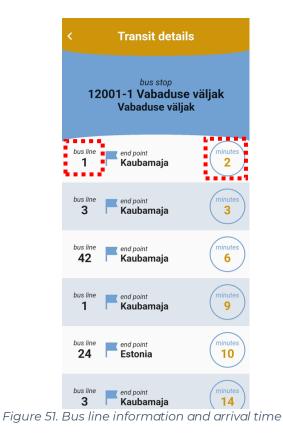


Figure 50. Selected bus lines

Clicking on transits, the bus stops information will display, and opening one of this, we are able to see the Bus Line number, and the time we must wait.







### 4.3.5.2.4 Scenario D

[D]: Anna, in this scenario, could easily check the arrivals time of the bus, with the procedure that we have described in the scenario [C]

#### 4.3.5.3 Outcomes

The results of the pilot campaigns confirmed the correct identification of vulnerabilities by Mob-Sec and the completed integration with SIEM and RITA.

The execution of the pilot testing actions, even though successful under the functional point of view, was of crucial importance in producing reflections on how to configure the second pilot activity related to Mob-Sec and that will be executed during the Genova pilot campaign.

In particular, it underlined the necessity of producing attack conditions to fully test Mob-Sec capabilities given the fact that in a short time frame (e.g., 5 days of piloting) and minimal users sample (e.g., 2 users per day) not all the features may be tested under normal conditions.

Moreover, it stressed the necessity of furtherly tuning the execution of some detection procedures, making coherent waiting time for application's users in order to avoid eventual reduction of usability (due to excessive loading times).

For the Tallinn pilot, every test has been performed successfully as expected, thanks to the limited number of users involved and due to the fact that all the attacks were performed manually.

The integration among all the CitySCAPE elements worked as expected.

#### 4.3.5.4 Future activities

Log collection from Sigla Server to Graylog has already been validated with dummy alerts. To be able to implement a realistic detection scenario, further development is needed to integrate detection rules inside the Graylog SIEM and playbooks inside XSOAR using scenarios that remain to be defined.





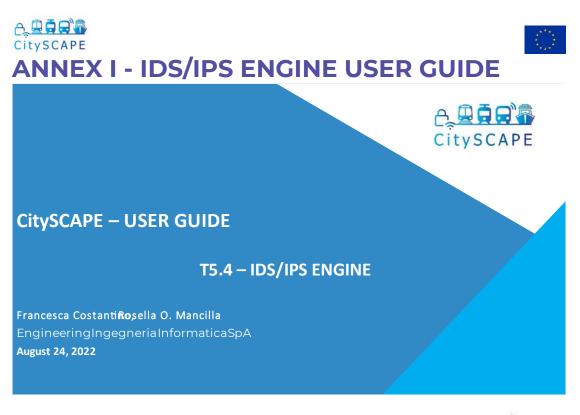
# CONCLUSIONS

This document has detailed the results of the CitySCAPE TALLINN Pilot that was conducted throughout the months of July and August (Piloting August 24th and 25th). The Pilot conducted a number of cyber test cases. For Test Cases 1, 2 and 3, the cyber-attacks were conducted on the Tallinn Pilot infrastructure and utilised the CPaaS data environment. Test-Case 1 demonstrated that the CitySCAPE toolkit could detect a DDoS attack on the AV Shuttle network and initiate a cyber incident response workflow. Test-Case 2 exhibited that the cyber-attack can be partially detected, and a cyber incident workflow can be initiated. Some information necessary for detection was not collected yet; the SIEM package required more log source to detect effectively attack and not just artefacts of it, as well the integration between the RITA and FIMCA, and the RITA and FIMCA calculation of risk and impacts. These issues and the remaining test cases were workshopped during the Pilot and a plan to remediate the issues and conduct the remaining test cases have been identified and actions to achieve completion of the Tallinn pilot activities will be enacted in September and October.

The pilot successfully demonstrated the Availability of AV Shuttle network test case and partially implemented the test-case on Adaptive Traffic Management. In these demonstrated test case the CitySCAPE toolkit functioned to enable effective detection of the cyber-attack and cyber incident response involving collaboration with the CERT partner (DNSC). For the remaining test cases issues were identified with the integration of CitySCAPE modules, specifically the integration within the SIEM tools (SIEM-CTIP) on the security orchestration and the RITA-FIMCA integration. Furthermore, it was identified that the SIEM needed customisation to the TALLINN pilot environment for creation of detection rules and playbooks for orchestration. During the Pilot, these gaps were identified and there is a plan for remediation and completion of the remaining in September and October.

In conclusion, the demo test cases conducted during the Tallinn Pilot showed that the CitySCAPE toolkit can produce the expected results for detection of cyber-attacks and enhanced incident response in the multimodal transportation environment. Whilst the Tallinn Pilot was unable to complete all the test cases on the 24th and the 25th of August, many valuable lessons were learnt for the coming Genoa Pilot. These included that the cybersecurity attack test cases need to contain granularity of detail which enable the SIEM operator to customise it to the pilot environment. Furthermore, the integration of the CitySCAPE toolkit needs to be fully validated before piloting, this includes, specifically, the integration between IDS and SIEM, SIEM toolkit and the RITA and FIMCA.

The completed pilot evaluation for Tallinn and Genoa will be contained in D7.5 "Pilot Evaluation and Knowledge capitalisation".



# INDEX



- Task Objectives Contributors
- State of the art
- Our approach
- USER GUIDE for Cyber-security services operatoror CitySCAPE admin (5')
   Anomaly Detection Procedure (ADP) API user guide (5')
- USER GUIDE for Cyber-security services operator or CitySCAPE admin and CPaaS admin (3')

26/8/2022

# WP5-Task 5.4-IDS/IPS ENGINE



 $\circ$  Objective:

- $\checkmark$  This task focuses on the development of the IDS/IPS engine .
- $\times$  The IDS/IPS module is able to monitor constantly the IT and OT infrastructure and the information gathered will be sent to the higher-level components.
- $\times$  This module is be based on an existing tool (e.g. SNORT) but it is customized according to the needs of the project.
- $\circ$  Leadership: ENG leads; contributors: ED, UPRC, ACS, STAM
- o Deliverable: D5.4 IDS/IPS final prototype [ENG, Other, M30]

# WP5-Task 5.4-IDS/IPS ENGINE



 $\circ$  Objective:

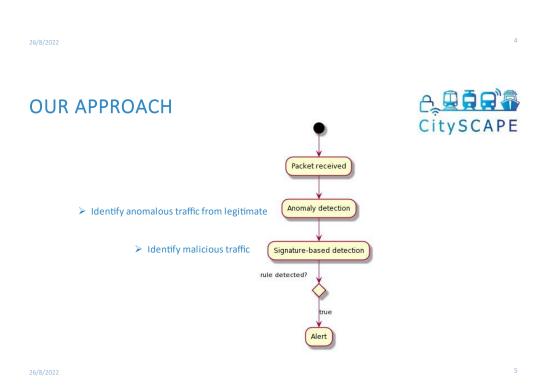
- $\checkmark$  This task focuses on the development of the IDS/IPS engine .
- $\checkmark$  The IDS/IPS module is able to monitor constantly the IT and OT infrastructure and the information gathered will be sent to the higher-level components.
- This module is be based on an existing tool (e.g. SNORT) but it is customized according to the needs of the project.
- $\circ$  Leadership: ENG leads; contributors: ED, UPRC, ACS, STAM
- o Deliverable: D5.4 IDS/IPS final prototype [ENG, Other, M30]





# State of the art IDS/IPS

- IDS/IPS: software and/or hardware devices that detect intrusions into a system or a network.
  - IDS (Intrusion Detection System) is a passive protection system.
  - IPS (Intrusion Prevention System) is an active protection system.
- The IDSs/IPSs are installed in critical points of the network (e.g. next to router, gateway, server web ..)
- Type of detection techniques in real time are:
  - Anomaly based IDS/IPS
  - Signature based IDS/IPS







# USER GUIDE foCyber-security services operator or CitySCAPEdmin



#### $\circ~$ Run the IDS/IPS engine to TEST the configuration:

- sudo snort -T -i <interface name> -c /etc/snort/snort.conf
   Where:
- -T flag indicates to run a test for the SNORT configuration
- -c flag indicates which file to use
- -i flag specifies the name of the network interface.



26/8/2022

# USER GUIDE focyber-security services operator ocitySCAPEadmin



#### **o Run the IDS/IPS offline, with PCAP file :**

o sudo snort -c/etc/snort/snort.conf -l/var/log/snort -r <path pcap file> -u snort - g snort

#### • Run the IDS/IPS online:

o sudo snort -c/etc/snort/snort.conf -l/var/log/snort -u snort -g snort -i <interface>

✓ Where:

- -c flag indicates which configfile to use
- I flag indicates log directory
- -r flag indicates the pcap to be analysed and processed
- -u flag specifiesto run as a specific user
- -g flag specifies to run as a specific group

#### ○ View IDS/IPS logs files:

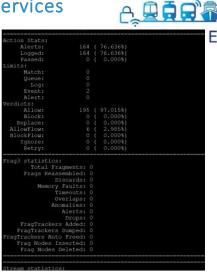
o sudo snort -c/etc/snort/snort.conf -r/var/log/snort/snort.log.1659706028





## USER GUIDE foCyber-security services operator or CitySCAPEadmin

	PS output
Prepro	coessor Object: SF DNS Version 1.1 <build 4=""> t processing (pid-3985)</build>
Snort processed :	ket processing was 1.213 seconds 201 packets. days 0 hours 0 minutes 1 seconds 201
Bytes in mapped Total allocated Total free space	ped bytes (arena): 1033269248 d regions (hblkhd): 24555520 d space (uordblks): 549637344
Packet I/O Total: Received: Analyzed: Dropped: Filtered: Outstanding: Injected:	s: 201 201 (100.000\$) 0 { 0.000\$) 0 { 0.000\$} 0 { 0.000\$} 0 { 0.000\$}
Breakdown by prot Eth: VLAN: IP4: Frag: ICMP: UDP: UDP:	0 ( 0.000%)



26/8/2022

## USER GUIDE focyber-security services operator or CitySCAPadmin



**Barnyard2** is the submodule that stores and processes the SNORT binary output into a MySQL database.

• Continuous processing mode - real-time events' storing (online)

 sudo barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.u2 -w /var/log/snort/barnyard2.waldo -g snort -u snort

#### Where:

- -c flag specifies the config file
- -d flag is the snort output directory
- -f flag specifies the file to look for
- -w flag specifies the bookmark file
- u flag tells Barnyard to run as a specific user
- -g flag tells Barnyardto run as a specific group







#### • File processing mode: processing a single log file (offline).

o sudo barnyard2 -c /etc/snort/barnyard2.conf -o /var/log/snort/snort.u2.1653376944

✓ Where:

- c flag specifies the configuration file
- -o flag enables the file processing mode
  The file snort.u2.\*\*\*\*\* is the specific file that you want process.

snort.log.1652344315	snort.u2.1652085271	snort.u2.1652358307
snort.log.1652344609	snort.u2.1652085294	snort.u2.1652358435
snort.log.1652358307	snort.u2.1652091045	snort.u2.1652957259
snort.log.1652358435	snort.u2.1652164843	snort.u2.1653301703
snort.log.1652957259	snort.u2.1652343423	snort.u2.1653376944
snort.log.1653301703	snort.u2.1652343610	
snort.log.1653304192	snort.u2.1652344315	
snort.log.1653376944	snort.u2.1652344609	
	<pre>snort.log.1652344609 snort.log.1652358307 snort.log.1652358435 snort.log.1652957259 snort.log.1653301703 snort.log.1653304192</pre>	snort.log.1652344609 snort.u2.1652085294 snort.log.1652358307 snort.u2.1652091045 snort.log.1652358435 snort.u2.1652164843 snort.log.1653304139 snort.u2.165243423 snort.log.1653304132 snort.u2.1652344315

## USER GUIDE focyber-security services operator or CitySCAPadmin



To check if new events are stored in the MySQL database launch the following command:

• mysql -u snort -p snort -e "select count(\*) from event"

#### ✓ Where:

- -u flag specifies the MySQL user
- -p flag specifies that a password is required
- -e flag indicate what to show.

Enter password: count(\*) 2730





# CitySCAPEAnomalyDetectionProcedure API

CitySCAPE\_AD API @ @

The API include the APD and several endpoints to test the procedure.

To start the API, lauch:

#### python –m uvicorn main:app --reload

An interactive documentation, is also available at:

http://IP\_ADDRESS8000/docs

ChildChPE Aconsty Descour. KN is able to	
Control answer     Authoritan and suthersforms a user	
<ul> <li>Cruste a trained machine learning thatel</li> <li>Rices have well your model is performing thatels to evaluation metrics</li> </ul>	
Earner: Dig/SU/12 API developer	
	Automa a
	Anter a
Authentication users Gwyting abscrowing surveitation and surveitation user	A.
Post / Prests ser Combar	
POE /REAR Logo Par Assess Taine	~
Anomaly detection model Several southe update and storag of the aronaly device powers	^
Apternarow2yeed: useninar	~ #
Evaluation model Services descendent for anomaly sender provider	^
Josef Formatio Produce Made	~ #
Perform algorithms. Service about evaluation of the anomaly detector procedure among different algorithms	^
/ongaralgettin Security	~
Labelling dataset Sevice state to international states	^
Advillingetavet and	

26/8/2022

## CitySCAPEADP API -authentication



#### AUTHENTICATION:

This service is about creating, authentication and authorization users.

Here we can find two endpoints

✓ Create user: it is possible to create a user
 ✓ Token: after login, you will be obtained a token for authentication .

Authentication users Everything about creating, authentication and authorization users	^
POST /create user Create User	~
POST /token Login For Access Token	~

26/8/2022

13





## CitySCAPEADP API –update model

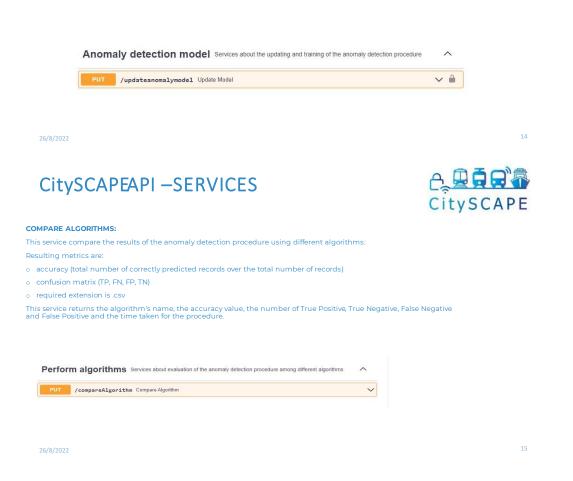


#### UPDATE MODEL:

The ADP model can be updated by importing a new training dataset (.csv). Also, the following metrics are returned

- o accuracy (total number of correctly predicted records over the total number of records)
- confusion matrix (TP, FN, FP, TN)

It returns accuracy value and the number of True Positive, True Negative, False Negative and False Positive



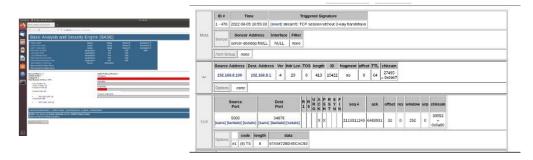




## USER GUIDE for Cyberecurity services operator or CitySCAPEadmin and PaaSadmin CitySCAPE

#### The GUI to view alerts stored in the database is also available to CPaaS admin. Following the link <u>http://IP/base/index.php</u>

The authentication page appears. After authentication you can access the main page.







#### o Test-Case 1 Asset Cost Evaluation

$\equiv$	:
Composite Asset Edit Composite Asset AV TeleOperation Server	Save × Delete
To Composite Asset Details 🛛 🚝 Assets 🖓 Asset Relationships	
<b>75</b> Basic Information Fill Composite Asset's Basic Information	
Code	
AV-TeleOperationServer	
* Required Field	
Name	
AV TeleOperation Server	
* Required Field	
Description	
Linked Intangible Assets Select Intangible Assets From The List By Clicking Select Button. X Data X Brand X Reputation X Organizational Capital +	
€ Economic Values	
Pessimistic Economic Value	
800000 Expressed in EUP	
Expressed in EUR Common Economic Value	
1000000	
Expressed in EUR	
Optimistic Economic Value	
1500000	
Expressed in EUR	

Figure 1. AV TeleOperation Server (Basic Information)



ď

TH-24



#### o RITA Threat Mapping Test-Case 1

	A IIIIeat Me	ipping rest-ca	561		:	
	Sosite Asse Asset <b>AV TeleOperati</b> set Details	on Server	ips		Save × Delete	
Select Basic Asse						
		Asset Selector		1	Of Economic Value	
×		Q AV storage		Medium	×	
×	× 0		tel	Medium	8	
× 0	× 0		S (Ubuntu)	🔽 Medium 🔳		
× 0	× 0			🖬 Medium 🛛		
× 0		Q AV-OnBoard-Da	Q AV-OnBoard-Database (PostegreSC		Medium	
0						
	of AV storage	r ¥Ξ Asset Asset & <b>© Activate/Deactiv</b>	-to Thursda			
Navigate to thre	Code	Name	Likelihood	Active	Counter Measures	
ď	TH-08	Failures of Devices	✓ 2 - Rare (Happ∈		(+)	
Ľ	TH-12	Natural Disaster	✓ 2 - Rare (Happ∈		+	
Ľ	TH-13	Environmental Dis	✓ 2 - Rare (Happ∉		(+)	
Ľ	TH-14	Device Modificatio	🗸 2 - Rare (Happe	1	× backup +	
C C	TH-14 TH-15	Device Modificatio	<ul> <li>2 - Rare (Happe</li> <li>2 - Rare (Happe</li> </ul>		× backup (+)	

Figure 2. AV TeleOperation Server (AV Storage Threats and Likehoods)

✓ 2 - Rare (Happ∉

Unauthorized Acce

(+)

CitySCAPE	

itySCAPE						
Ξ					:	
	posite Asse Asset <b>av Teleoperati</b>				Save × Delete	
🎢 Composite A	Asset Details 🛛 😤 As	sets & Asset Relationsh	ips			
Select Basic Ass						
		Asset Selector		Priority In Term	s Of Economic Value	
× 0		Q AV storage		Medium	×	
× O		Q AV-ControlPC In	tel	S Medium	×	
×		Q AV-ControlPC O	S (Ubuntu)	Medium 🛛		
× 0		O AV-DOS	Q AV-ROS		🖬 Medium 🔳	
× 0		Q AV-OnBoard-Da	tabase (PostegreSC	Medium		
× • • • • •	reats Of AV-ControlPC	Q AV-OnBoard-Da	Deactivate Threats.			
Threats     Navigate To Thr	reats Of AV-ControlPC Code	Q AV-OnBoard-Da	Deactivate Threats. Likelihood	Active	Counter Measures	
Threats Navigate To Thr	reats Of AV-ControlPC Code TH-08	Q AV-OnBoard-Da	Deactivate Threats. Likelihood 2 - Rare (Happe		Counter Measures	
Threats Navigate To Thr	reats Of AV-ControlPC Code TH-08 TH-12	Q       AV-OnBoard-Da         PC Intel ﷺ Asset       Intel ﷺ Asset         Intel ﷺ Asset & ● Activate/         Name         Failures of Devices         Natural Disaster	Deactivate Threats. Likelihood 2 - Rare (Happe 2 - Rare (Happe	Active	Counter Measures + +	
Threats Navigate To Thr	reats Of AV-ControlPC Code TH-08	Q AV-OnBoard-Da	Deactivate Threats. Likelihood 2 - Rare (Happe	Active	Counter Measures	
Threats Navigate To Thr	TH-08         TH-12           TH-13         TH-13	AV-OnBoard-Da      AV-OnBoard-Da      Asset & Asset      Name      Failures of Devices      Natural Disaster      Environmental Dis	Deactivate Threats. Likelihood 2 - Rare (Happe 2 - Rare (Happe 2 - Rare (Happe	Active	Counter Measures (+) (+) (+) (+) (+)	
Threats Navigate To Thr	TH-08           TH-12           TH-13           TH-14	Q       AV-OnBoard-Da         IPC Intel # Asset       Asset         Intel # Asset & Activate/       Asset         Name       Failures of Devices         Natural Disaster       Environmental Dis         Device Modificatio       Device Modificatio	Deactivate Threats. Likelihood 2 - Rare (Happe 2 - Rare (Happe 2 - Rare (Happe 2 - Rare (Happe	Active	Counter Measures (+) (+) (+) (+) (+) (+)	
Threats Navigate To Thr	Freedoc of AV-ControlPC           code           TH-08           TH-12           TH-13           TH-14           TH-15	Q AV-OnBoard-Da         IPC Intel ﷺ Asset         Intel ﷺ Asset & ● Activate/         Name         Failures of Devices         Natural Disaster         Environmental Dis         Device Modificatio         Device Destructior	Deactivate Threats. Likelihood 2 - Rare (Happe 2 - Rare (Happe 2 - Rare (Happe 2 - Rare (Happe 2 - Rare (Happe	Active	Counter Measures + + + + + + + + + + +	

Figure 3. AV TeleOperation Server (AV Control PC Intel Threats and Likehoods)

2	
	tySCAPE

lit Composite Asset AV T	e Asset	🖬 Sav	/e × Delete
S Composite Asset Details	f = Assets 8 Asset Relationships		
Assets List			
IECL BASIC ASSELS	Asset Selector	Priority In Terms Of Econ	omic Value
• •	Q AV storage	Medium	×
0	Q AV-ControlPC Intel	Medium	×
0	Q AV-ControlPC OS (Ubuntu)	Medium	×
	Q AV-ROS	Medium	×
9		Medium	×
< 0	🔍 AV-OnBoard-Database (PostegreSÇ		

	Code	Name	Likelihood	Active	Counter Measures
മ്	TH-01	Malware Injection	🗸 2 - Rare (Happe		+
C,	TH-02	Denial of Service	🗸 4 - Reqular (Tal		(+)
C.	TH-11	Software Exploitati	🗸 2 - Rare (Happe		(+)
Z	TH-14	Device Modificatio	🖌 4 - Reqular (Tal		(+)
2	TH-21	Resource Exhausti	🗸 2 - Rare (Happe		(+)
2	TH-22	Isolation/Virtualiza	🗸 2 - Rare (Happe		(+)
2	TH-23	Management Inter	✓ 2 - Rare (Happ€		+
2	TH-24	Unauthorized Acce	🗸 4 - Reqular (Tal		(+)
2	TH-25	Abuse of Authorisa	🗸 4 - Reqular (Tal		+
3	TH-27	Abuse of Authentic	🗸 4 - Regular (Tal		$(\pm)$

Figure 4. AV TeleOperation Server (AV ROS Threats and Likehoods)

CitySCAPE	

-					
	nposite Asse ite Asset <b>av Teleoperati</b>				Save × Delet
ኛ Composite	e Asset Details 🛛 😤 Ass	sets 윦 Asset Relationshi	ps		
Assets	slist				
lect Basic A					
		Asset Selector		Priority In Ter	ms Of Economic Value
• •		Q AV storage		🖬 Medium	
• •		Q AV-ControlPC In	tel	🗖 Medium	B
•		Q AV-ControlPC O	S (Ubuntu)	🔽 Medium	E
0		Q AV-ROS		🔽 Medium	E
× 0		🔍 AV-OnBoard-Database (PostegreSÇ		🔽 Medium	8
•					
-) Threat		rd-Database (Post Database (PostegreSQL) 汪 /	and the second		ts.
-) Threat		Database (PostegreSQL) ﷺ	and the second		ts. Counter Measures
Threat	Threats Of <b>AV-OnBoard-E</b>	Database (PostegreSQL) ﷺ	Asset & C Activate/De	eactivate Threa	
Threat	Threats Of AV-OnBoard-E	Database (PostegreSQL) źΞ / Name	Asset & O Activate/De	Active	Counter Measures
Threat vigate To T	Threats Of AV-OnBoard-E Code TH-01	Database (PostegreSQL) ﷺ / Name Malware Injection	Asset &  Asset &  Asset A  Ass	Active	Counter Measures
Threat vigate To T	Threats Of AV-OnBoard-I	Name       Malware Injection       Denial of Service	Asset & Activate/De Likelihood 3 - Periodic (Ha 3 - Periodic (Ha	Active	Counter Measures + + +
Threat	Threats Of AV-OnBoard-I Code TH-01 TH-02 TH-11	Name       Malware Injection       Denial of Service       Software Exploitati	Asset & O Activate/Do Likelihood	Active	Counter Measures
Threat Vigate To T	Threats Of AV-OnBoard-I           Code           TH-01           TH-02           TH-11           TH-14	Name       Malware Injection       Denial of Service       Software Exploitati       Device Modificatio	Asset & O Activate/De Likelihood 3 - Periodic (Ha 3 - Periodic (Ha 3 - Periodic (Ha 2 - Rare (Happe	Active	Counter Measures + + + + + + +
Threating Threa	Threats Of AV-OnBoard-I           Code           TH-01           TH-02           TH-11           TH-14           TH-21	Name       Malware Injection       Denial of Service       Software Exploitati       Device Modificatio       Resource Exhausti	Asset & O Activate/De Likelihood 3 - Periodic (He 3 - Periodic (He 3 - Periodic (He 2 - Rare (Happe 3 - Periodic (He	Active	Counter Measures
Threat vigate To T	TH-01           TH-02           TH-11           TH-14           TH-21           TH-22	Database (PostegreSQL) ## /       Name       Malware Injection       Denial of Service       Software Exploitati       Device Modificatio       Resource Exhausti       Isolation/Virtualiza	Asset & O Activate/De Likelihood 3 - Periodic (Ha 3 - Periodic (Ha 2 - Rare (Happe 2 - Rare (Happe	Active	Counter Measures
	Threats Of AV-OnBoard-I           Th-O1           Th-O2           Th-O2           Th-11           Th-12           Th-21           Th-22           Th-23	Name       Malware Injection       Denial of Service       Software Exploitati       Device Modificatio       Resource Exhausti       Isolation/Virtualiza       Management Inter	Asset & O Activate/Do Likelihood 3 - Periodic (Ha 3 - Periodic (Ha 2 - Rare (Happe 2 - Rare (Happe 2 - Rare (Happe 2 - Rare (Happe	Active	Counter Measures

Figure 5. AV TeleOperation Server (AV On Board PostgreSQL Database Threats and Likehoods)

AR	ă 🛱 🖥
	SCAPE

.*	**.
	**

<b>s</b> Asset Links	List		
	Asset A	Asset B	Туре
s -	Q AV-ControIPC OS (Ubunt	Q AV-ROS	Hosts
( )	Q AV-ROS	Q AV-OnBoard-Database (I	Stores
¢ .	Q AV-OnBoard-Database (I	Q AV storage	🖸 Uses 🖪
)			

Figure 6. AV TeleOperation Server (Asset Relationships)

CitySCAPE	

2 Composit	o Accot		 1	
<b>73</b> Composit		•	B Save	× Delete
Edit Composite Asset AV	communications comp	osite asset		
የና Composite Asset Detail	₹≣ Assets	Asset Relationships		
💦 Basic Inform	ation			
Fill Composite Asset's Ba	ic Information			
Code				
Vehicle-Communicatio	ns-01			
* Required Field				
Name				
AV communications co	mposite asset			
* Required Field				
Description				
Elect Intangible Assets From The	ist By Clicking • Select Button.			
Elect Intangible Assets From The	ist By Clicking • Select Button.			
Select Intangible Assets From The  Data Reputation  Economic Valu  Pessimistic Economic V  40000  Expressed In EUR	ist By Clicking Select Button.			
Select Intangible Assets From The  Data  Reputation  Economic Value  A0000  Expressed In EUR  Common Economic Value	ist By Clicking Select Button.			
Every select intangible Assets From The	ist By Clicking Select Button.			
Select Intangible Assets From The Data Reputation     Commic Value     Economic Value     A0000 Expressed In EUR     Common Economic Value     G0000 Expressed In EUR	ist By Clicking © Select Button.			
€ Economic Val Pessimistic Economic V 40000 Expressed In EUR Common Economic Val	ist By Clicking © Select Button.			

Figure 7. AV communications (Basic Information)

CitySCAPE

	<b>YSCAPE</b>	=					
dit Composite Asset AV communications composite asset  Tr Composite Asset Details  TE Asset Selector  Asset Selector  Priority In Terms Of Economic Value  Asset Selector  Asset Selector  Priority In Terms Of Economic Value  Asset Selector  Asset Selector  Priority In Terms Of Economic Value  Asset Selector  Asset Selector  Priority In Terms Of Economic Value  Asset Selector  Asset Selector  Priority In Terms Of Economic Value  Asset Selector  Asset Selector  Asset Selector  Priority In Terms Of Economic Value  Asset Selector  Asset Asset Relationships  Asset Selector  Asset Asset Relationships  Asset Selector  Asset Relationships  Asset Selector  Asset Selector  Asset Selector  Asset Selector  Asset Relationships  Asset Selector  Asset Sele	Ξ						
Asset Selector       Priority In Terms of Economic Value         X       Q       Netgear MR1100 Mobile Router       Medium       R         X       Q       Cisco 4331 Integrated Services Rout       Medium       R         X       Q       Cisco 4331 Integrated Services Rout       Medium       R         X       Q       Cisco 4331 Integrated Services Rout       Medium       R         X       Q       Mikrofic CSS       Q       Medium       R         X       Q       Cisco 4331 Integrated Services Rout       Medium       R         X       Q       Mikrofic CSS       Q       Medium       R         X       Q       Denial of Service       X       A - Regular (Ta       X       Counter Measures         X       TH-02       Denial of Service       X       A - Regular (Ta       X       Counter Measures         X       TH-02       Denial of Service       X       A - Regular (Ta       X       Counter Measures         X       TH-02       Denial of Service       X       A - Regular (Ta       X       Counter Measures         X       TH-03       Interception of Int       X       3 - Periodic (Ht       Imaget and the service       Image						Save × Delete	
Asset Selector Priority In Terms Of Economic Value   X Q Netgear MR1100 Mobile Router Medium Q   X Q Cisco 4331 Integrated Services Roul Medium Q   X Q MikroTic CSS Q Medium Q   Q MikroTic CSS Q Medium Q   O Threats of Netgear MR1100 Mobile Router # EAsset Medium Q   O Name Likelihood Active Counter Measures   Code Name Likelihood Active Counter Measures   V TH-02 Denial of Service 4 - Regular (Ta) * Countermeasure for Das of Uburtu os set   V TH-02 Denial of Service 4 - Regular (Ta) * Network Outage   V TH-03 Interception of Inft 3 - Periodic (Hi Image: Control   Q TH-05 Interception of Inft 3 - Periodic (Hi Image: Control   Q TH-03 Interception of Inft 3 - Periodic (Hi Image: Control   Q TH-03 Pailure of System 2 - Rare (Happ Image: Control   Q TH-03 Failure of System 2 - Rare (Happ Image: Control   Q TH-10 Loss of Support Se 3 - Periodic (Hi Image: Control   Q TH-03 Failure of System 2 - Rare (Happ Image: Control   Q TH-03 Failure of System 3 - Periodic (Hi Image: Control   Q TH-10 Loss of Support Se 3 - Periodic (Hi <td>rፕ Composite</td> <td>Asset Details 😤 Asse</td> <td>ets 🔗 Asset Relations</td> <td>nips</td> <td></td> <td></td>	rፕ Composite	Asset Details 😤 Asse	ets 🔗 Asset Relations	nips			
Asset Selector       Priorig In Terms Of Economic Value         ×       ○       Netgear MR1100 Mobile Router       ○ Medium       ○         ×       ○       Cisco 4331 Integrated Services Rout       ○ Medium       ○         ×       ○       ○       Medium       ○       ○         ×       ○       ○       MikroTic CSS       ○       Medium       ○         O       MikroTic CSS       ○       Medium       ○       ○         O       MikroTic CSS       ○       Medium       ○         O       MikroTic CSS       ○       Medium       ○         O       MikroTic CSS       ○       Medium       ○         O       Medigear MR100 Mobile Router #E Asset       O Active       Counter Measures         Code       Name       Likelihood       Active       Counter Measures         *       ·       ·       ·       ·       ·       ·       ·         ItH-02       Denial of Service       ·       ·       ·       ·       ·       ·       ·         @       TH-04       Man in the Middle       ·       ·       ·       ·       ·       ·       ·       ·         <							
Image: control of decision of decis			Asset Selector		Priority In Term	s Of Economic Value	
Image: Control of the second of the secon	× 0		Q Netgear MR1100	Mobile Router	🖬 Medium	8	
Image: Section of the section of th	×		Q Cisco 4331 Integ	rated Services Rout	🖬 Medium	8	
Threats of Netgear MR1100 Mobile Router # Asset & Activate/Deactivate Threats.         Code       Name       Likelihood       Active       Counter Measures         Code       Name       Likelihood       Active       Counter Measures         Code       Name       Likelihood       Active       Counter Measures         Code       TH-02       Denial of Service       4 - Requiar (Ta       Counter Measure         ITH-02       Denial of Service       4 - Requiar (Ta       Counter Measure         ITH-02       Denial of Service       4 - Requiar (Ta       Counter Measure         ITH-04       Man in the Middle       3 - Periodic (Ht       Ithetwork Coulage         ITH-04       Man in the Middle       3 - Periodic (Ht       Ithetwork Coulage         ITH-05       Interception of Inf       3 - Periodic (Ht       Ithetwork Coulage         ITH-05       Interception of Message       2 - Rare (Happ       Ithetwork <th colspan<="" td=""><td>×</td><td></td><td>Q MikroTic CSS</td><td></td><td>🖬 Medium</td><td>8</td></th>	<td>×</td> <td></td> <td>Q MikroTic CSS</td> <td></td> <td>🖬 Medium</td> <td>8</td>	×		Q MikroTic CSS		🖬 Medium	8
Code       Name       Likelihood       Active       Counter Measures         I       TH-02       Denial of Service       ✓ 4 - Regular (Ta       ✓       ✓         I       TH-02       Denial of Service       ✓ 4 - Regular (Ta       ✓       ✓         I       TH-02       Denial of Service       ✓ 4 - Regular (Ta       ✓       ✓         I       TH-02       Man in the Middle       ✓ 3 - Periodic (Ha       ✓          I       TH-05       Interception of Inft       ✓ 3 - Periodic (Ha       ✓       (+)         I       TH-05       Interception of Inft       ✓ 3 - Periodic (Ha       ✓       (+)         I       TH-06       Replay of Message       ✓ 2 - Rare (Happ)       ✓       (+)         I       TH-07       Network Outage       ✓ 2 - Rare (Happ)       (+)       (+)         I       TH-07       Network Outage       ✓ 2 - Rare (Happ)       (+)       (+)         I       TH-07       Network Outage       ✓ 2 - Rare (Happ)       (+)       (+)         I       TH-09       Failure of System       ✓ 2 - Rare (Happ)       (+)       (+)         I       TH-10       Loss of Support Se       ✓ 3 - Periodic (Ha       (+)       (+)					-		
Image: Section of Sectin of Sectin of Section of Section of Section of Section	avigate To Tł					Counter Measures	
os         ** Network Outage Control         **	2	TH-02	Denial of Service	🗸 4 - Reqular (Ta			
Image: Constraint of the state of the s						× Network Outage Control	
Image: State of the state	ď	TH-04	Man in the Middle	💙 3 - Periodic (Ηε		+	
Image: State of the state	Ľ	TH-05	Interception of Info	✓ 3 - Periodic (Hε	<ul> <li>Image: A start of the start of</li></ul>	+	
Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system         Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system         Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system         Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system         Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system         Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system         Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system         Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system       Image: Constraint of the system         Image: Constraint of the system       Image: Consthe system       Image: Constraint of the system	Ľ	TH-06	Replay of Message	🗸 2 - Rare (Happ		(+)	
Image: Strain	Ľ	TH-07	Network Outage	🗸 2 - Rare (Happ		+	
Image: Sector of the sector	Ľ						
Image: Constraint of the second se	ď	TH-09	Failure of System	🗸 2 - Rare (Happ	$\checkmark$	(+)	
Image: Constraint of the second consecond consecond constraint of the second constraint of	Ľ.					-	
Ľ     TH-21     Resource Exhausti     3 - Periodic (Hi     +       Ľ     TH-23     Management Intel     3 - Periodic (Hi     +		TH-10	Loss of Support Se	V 3 - Periodic (Ha		+	
L'     TH-23     Management Intel     3 - Periodic (Ht     (Ht)	C.	тн-10 тн-11	Loss of Support Se Software Exploitat	<ul> <li>✓ 3 - Periodic (Hε</li> <li>✓ 3 - Periodic (Hε</li> </ul>		(+) (x Patching)(+)	
		TH-10 TH-11 TH-19	Loss of Support Se Software Exploitat Phishing Attacks	<ul> <li>3 - Periodic (Hailet and the second constrained in the second constrained con</li></ul>		+ × Patching + +	
ප් TH-24 Unauthorized Acce 🗸 3 - Periodic (Ht 🖌 🔶	ഗ്	TH-10 TH-11 TH-19 TH-20	Loss of Support Se Software Exploitat Phishing Attacks Network Spoofing	<ul> <li>3 - Periodic (Hage)</li> <li>3 - Periodic (Hage)</li> <li>2 - Rare (Happ)</li> <li>3 - Periodic (Hage)</li> </ul>		(+) (* Patching)(+) (+) (+)	
	Ľ	TH-10 TH-11 TH-19 TH-20 TH-21	Loss of Support Se Software Exploitat Phishing Attacks Network Spoofing Resource Exhausti	<ul> <li>3 - Periodic (Hateleft)</li> <li>3 - Periodic (Hateleft)</li> <li>2 - Rare (Happ)</li> <li>3 - Periodic (Hateleft)</li> <li>3 - Periodic (Hateleft)</li> </ul>		(+) (* Patching) (+) (+) (+) (+) (+)	

Figure 8. AV communications (Netgear MR1100 Mobile Router Threats and Likelihoods)

Abuse of Authorisa

Abuse of Authenti

Social Engineering

Identity Theft

🗸 2 - Rare (Happ

✓ 2 - Rare (Happ)

✓ 2 - Rare (Happ)

🗸 2 - Rare (Happ

TH-25

TH-27

TH-28

TH-29

Ľ

ď

Ľ

Ľ

(+)

(+)

(+)

(+)

CitySCAPE

Ľ

Ľ

Ľ

Ľ

Ľ

Ľ

Ľ

Ľ

SCAPE					
1					
		ations composite asset	hips		Save × Delete
Assets L ect Basic Asse					
		Asset Selector		Priority In Terms	Of Economic Value
0		Q Netgear MR1100	Mobile Router	🔽 Medium	×
0		Q Cisco 4331 Integ	rated Services Rout	🖸 Medium	×
0		Q MikroTic CSS		🔽 Medium	8
_ Threats		Integrated Servic tegrated Services Router ﷺ Name			
	eats Of Cisco 4331 Int	tegrated Services Router ⅔	Asset & 💿 Activate/I	Deactivate Threats	Counter Measures
Threats vigate To Thre	Code TH-02	tegrated Services Router #=	Asset & C Activate/I Likelihood	Active	Counter Measures × Countermeasure for DoS of Ubuntu OS × Network Outage Control +
Threats vigate To Three	Code TH-02 TH-04	tegrated Services Router #= Name Denial of Service Man in the Middle	Asset & Activate/I Likelihood	Active	Counter Measures
Threats vigate To Three	Code           TH-02           TH-04           TH-05	tegrated Services Router ####################################	Asset & Activate/I Likelihood 4 - Requiar (Ta 2 - Rare (Happ) 2 - Rare (Happ)	Active	Counter Measures
Threats vigate To Thre	Code TH-02 TH-04	tegrated Services Router #= Name Denial of Service Man in the Middle	Asset & Activate/I Likelihood	Active	Counter Measures
Threats vigate To Thre	Code           TH-02           TH-04           TH-05	tegrated Services Router ####################################	Asset & Activate/I Likelihood 4 - Requiar (Ta 2 - Rare (Happ) 2 - Rare (Happ)	Active	Counter Measures
Threats vigate To Three	Code TH-02 TH-04 TH-05 TH-06	tegrated Services Router ####################################	Asset & Activate/I Likelihood 4 - Requiar (Ta 2 - Rare (Happ) 2 - Rare (Happ) 2 - Rare (Happ)	Active	Counter Measures
Threats vigate To Three	Code           TH-02           TH-04           TH-05           TH-06           TH-07	Itegrated Services Router #       Name       Denial of Service       Man in the Middle       Interception of Infr       Replay of Message       Network Outage	Asset & Activate/I Likelihood 4 - Requiar (Ta 2 - Rare (Happ) 2 - Rare (Happ) 2 - Rare (Happ) 2 - Rare (Happ)	Active	Counter Measures
Threats	TH-02           TH-02           TH-03           TH-04           TH-05           TH-06           TH-07           TH-09	Name       Image: Denial of Service       Image: Denial of Service	Asset & Activate/I Likelihood 2 - Rare (Happ) 2 - Rare (Happ)	Active	Counter Measures

Figure 9. AV communications (Cisco 4331 Integrated Services Router Threats and Likelihoods)

Network Spoofing

Resource Exhausti

Management Inte

Unauthorized Acce

Abuse of Authorisa

Abuse of Authenti

Social Engineering

Identity Theft

TH-20

TH-21

TH-23

TH-24

TH-25

TH-27

TH-28

TH-29

(+)

(+)

(+)

(+)

(+)

(+)

(+)

(+)

~

~

~

~

~

~

~

1

✓ 2 - Rare (Happ)

✓ 2 - Rare (Happ

2 - Rare (Happ)

🗸 2 - Rare (Happ

🗸 2 - Rare (Happ

✓ 2 - Rare (Happ)

✓ 2 - Rare (Happ)

2 - Rare (Happ)

CitySCAPE	

Composite Asse Assets Lis elect Basic Asset	st	sets 😽 Asset Relationsh	lips		
lect Basic Asset					
	S				
× 0		Asset Selector		Priority In Term	s Of Economic Value
		Q Netgear MR1100	Mobile Router	🗖 Medium	×
< 0		Q Cisco 4331 Integr	rated Services Rout	🖸 Medium	×
× 0		Q MikroTic CSS		D Medium	×
0				Л	
	of MikroTic CS	SS ⅔ Asset ≅ Asset & © Activate/Deact	tivate Threats		
	Code		Likelihood	Active	Counter Measures
5	TH-02	Denial of Service	🗸 2 - Rare (Happ		(+)
5	TH-04	Man in the Middle	✓ 2 - Rare (Happ		+
3	TH-05	Interception of Infe	✓ 2 - Rare (Happ		+
5	TH-06	Replay of Message	✓ 2 - Rare (Happ		+
3	TH-07	Network Outage	✓ 2 - Rare (Happ	2	+
5	TH-09	Failure of System	✓ 2 - Rare (Happ		$(\pm)$
3	TH-10	Loss of Support Se	✓ 2 - Rare (Happ		$(\pm)$
5	TH-11	Software Exploitat	✓ 2 - Rare (Happ		(+)
3	TH-19	Phishing Attacks	✓ 2 - Rare (Happ		$(\pm)$
5	TH-20	Network Spoofing	🗸 2 - Rare (Happ		(+)
5	TH-21	Resource Exhausti	✓ 4 - Requiar (Ta)		$(\pm)$
5	TH-23	Management Inte	🗸 4 - Reqular (Ta		+
6	TH-24	Unauthorized Acce	🗸 4 - Reqular (Ta		+
			Desider (T	1	0
2	TH-25	Abuse of Authorise	💙 4 - Reqular (Ta	$\checkmark$	(+)

Figure 10. AV communications (MikroTic CSS Threats and Likelihoods)

🗸 2 - Rare (Happ

Social Engineering

TH-29

Ľ

(+)

Composite Asset A	te Asset v communications composite ass	et	Save × Delete
mposite Asset Deta	ils (≝ Assets & Asset Re	lationships	
sset Links I	_ist		
	Asset A	Asset B	Туре
	Q MikroTic CSS	Q Netgear MR1100 Mobile	🔽 Connects To 🛛 💌
	Q MikroTic CSS	Q Cisco 4331 Integrated Se	Connects To

Figure 11. AV communications (Asset Relationships)

La caracteria de la car	
Composite Asset Edit Composite Asset Taltech self driving vehicle control PC	Save × Delete
<b>7%</b> Basic Information Fill Composite Asset's Basic Information	
Code	
Main-Control-PC	
* Required Field Name	
Taltech self driving vehicle control PC	
* Required Field Description	
Linked Intangible Assets Select Intangible Assets From The List By Clicking Select Button. Intellectual Property X Data Reputation +	
€ Economic Values	
80000	
Expressed In EUR	
Common Economic Value	
100000	
100000 Expressed In EUR	
Expressed In EUR	

Figure 12. Main-Control-PC (Basic Information)

CitySCAPE	

it Composite Asset Taltech s	elf driving vehicle control PC	
Assets List lect Basic Assets		
	Asset Selector	Priority In Terms Of Economic Value
• 0	Q AV-ControlPC OS (Ubuntu)	🔽 Medium 🛛
	Q AV-ControlPC Intel	🖬 Medium 🛛
•	Q AV-ControlPC-Storage	🖬 Medium 🛛
0	Q AV-Self Driving OS	🔽 Medium 💌
0	Q AV-OnBoard-Database (PostegreSC	🔽 Medium 🛛
0	Q AV-ROS	🔽 Medium 🛛
		- 15

	Code	Name	Likelihood	Active	Counter Measures
Ľ	TH-01	Malware Injection	🗸 🗸 - Periodic (Ha		+
Ľ*	TH-02	Denial of Service	🗸 4 - Reqular (Tal		× Countermeasure for DoS of Ubuntu
					(+) os
Ľ	TH-09	Failure of System	✓ 3 - Periodic (Ha	<ul> <li>Image: A start of the start of</li></ul>	+
Ľ	TH-11	Software Exploitati	✓ 2 - Rare (Happ€		$(\pm)$
Ľ	TH-14	Device Modificatio	✓ 2 - Rare (Happ∉		+
L×	TH-21	Resource Exhausti	🗸 4 - Reqular (Tal		× Audit logs +
Ľ	TH-22	Isolation/Virtualiza	✓ 2 - Rare (Happ€		+
C.	TH-23	Management Inter	🗸 4 - Reqular (Tal		(+)
ď	TH-24	Unauthorized Acce	✓ 2 - Rare (Happ∈		+
്	TH-25	Abuse of Authorisa	🗸 2 - Rare (Happe		+
e"	TH-27	Abuse of Authentic	✓ 2 - Rare (Happ€		+
ď	TH-28	Identity Theft	🗸 2 - Rare (Happe		+
Ľ	TH-29	Social Engineering	✓ 2 - Rare (Happ∉		+

Figure 13. Main-Control-PC (AV Control PC OS Ubuntu Threats and Likehoods)

CitySCAPE

Composite Asset Taltect	ASSET	🖬 Sat	ve × Delete
Composite Asset Details	# Assets Asset Relationships		
Assets List			
ect Basic Assets			
	Asset Selector	Priority In Terms Of Econ	omic Value
0	Asset Selector	Priority In Terms Of Econ Medium	omic Value
0		1	
•	Q AV-ControlPC OS (Ubuntu)	Medium	×
	AV-ControlPC OS (Ubuntu)     AV-ControlPC Intel	Medium Medium	2
	AV-ControlPC OS (Ubuntu)     AV-ControlPC Intel     AV-ControlPC-Storage	Medium     Medium     Medium     Medium	8

### ● Threats of AV-ControlPC Intel = Asset

Navigate To Threats Of AV-ControlPC Intel # Asset & C Activate/Deactivate Threats.

	Code	Name	Likelihood	Active	Counter Measures
Ľ	TH-08	Failures of Devices	🗸 2 - Rare (Happe		$(\pm)$
C.	TH-12	Natural Disaster	🗸 2 - Rare (Happe		(+)
Ľ"	TH-13	Environmental Dis	🗸 2 - Rare (Happe		+
2	TH-14	Device Modificatio	🗸 2 - Rare (Happe		$(\pm)$
Ľ	TH-15	Device Destructior	🗸 2 - Rare (Happe		(+)
C.	TH-16	Device Loss or The	🗸 2 - Rare (Happe		(+)
c"	TH-18	Attacks on Decom	🗸 2 - Rare (Happe		(+)
c"	TH-24	Unauthorized Acce	✓ 2 - Rare (Happ∉		+

Figure 14. Main-Control-PC (AV Control PC Intel Threats and Likehoods)

CitySCAPE	

Composite Asset Talt	e ASSet ech self driving vehicle control PC	C Save	× Delete
75 Composite Asset Details	Z Assets		
EAssets List			
	Asset Selector	Priority In Terms Of Economic	Value
			-
< 0	Q AV-ControIPC OS (Ubuntu)	Medium	×
	AV-ControlPC Intel	Medium     Medium	×
	Q AV-ControlPC Intel	Medium	×
< 0	AV-ControlPC Intel     AV-ControlPC-Storage	Medium     Medium	2

#### ● Threats of AV-ControlPC-Storage ﷺ Asset Navigate To Threats Of AV-ControlPC-Storage ﷺ Asset & ● Activate/Deactivate Threats.

	Code	Name	Likelihood	Active	Counter Measures
Ľ	TH-08	Failures of Devices	🗸 2 - Rare (Happ	e 🖌	$(\pm)$
Ľ"	TH-12	Natural Disaster	✓ 2 - Rare (Happ	e	(+)
ď	TH-13	Environmental Dis	🗸 2 - Rare (Happ	e	+
2	TH-14	Device Modificatio	🗸 2 - Rare (Happ	e 🖌	(+)
Ľ*	TH-15	Device Destruction	✓ 2 - Rare (Happ	e 🗌	+
Ľ*	TH-16	Device Loss or The	🗸 2 - Rare (Happ	e 🗌	+
2	TH-18	Attacks on Decom	🗸 2 - Rare (Happ	ie 🗌	+
ഭ്	TH-24	Unauthorized Acce	🗸 2 - Rare (Happ	ie C	$(\pm)$

Figure 15. Main-Control-PC (AV Control PC Storage Threats and Likehoods)

A	
CitySCA	

0

itySCAPE			
Ξ			:
Composite Asset Talted To Composite Asset Details Composite Asset Details Composite Assets List Select Basic Assets	Asset n self driving vehicle control PC	Save × Delete	
	Asset Selector	Priority In Terms Of Economic Value	
× 0	Q AV-ControlPC OS (Ubuntu)	🔽 Medium 🛛	
×	Q AV-ControlPC Intel	🖬 Medium 🛛	
× O	Q AV-ControlPC-Storage	🖬 Medium 🛛	
× O	Q AV-Self Driving OS	🖬 Medium 🛛	
× 0	Q AV-OnBoard-Database (PostegreSC	🖬 Medium 🛛	1
× 0	Q AV-ROS	🔽 Medium 🛛	

#### I Threats of AV-Self Driving OS ∷ Asset Navigate To Threats Of AV-Self Driving OS 🔁 Asset & O Activate/Deactivate Threats.

	Code	Name	Likelihood	Active	Counter Measures
Ľ	TH-01	Malware Injection	🗸 3 - Periodic (Ha		(+)
2	TH-02	Denial of Service	✓ 2 - Rare (Happ€		(+)
Ľ*	TH-09	Failure of System	💙 2 - Rare (Happe		+
Ľ*	TH-11	Software Exploitati	🗸 3 - Periodic (Ha		+
C,	TH-14	Device Modificatio	🗸 2 - Rare (Happe		(+)
2	TH-21	Resource Exhausti	✓ 3 - Periodic (Ha		+
۲.	TH-22	Isolation/Virtualiza	✓ 2 - Rare (Happ€		(+)
C*	TH-23	Management Inter	✓ 2 - Rare (Happ∈		+
C.	TH-24	Unauthorized Acce	🗸 2 - Rare (Happe		+
Ľ*	TH-25	Abuse of Authorisa	🗸 2 - Rare (Happe		+
C.	TH-27	Abuse of Authentic	🗸 2 - Rare (Happe		+
2	TH-28	Identity Theft	🗸 2 - Rare (Happe		+
C.	TH-29	Social Engineering	✓ 2 - Rare (Happ€		+

Figure 16. Main-Control-PC (AV Self-Driving OS Threats and Likehoods)

CitySCAPE	



Edit Composite Asset Taltech self dri Composite Asset Details ## Asset Select Basic Assets Select Basic Assets	ving vehicle control PC	E Save × Delete
	Asset Selector	Priority In Terms Of Economic Value
× 0	Q AV-ControlPC OS (Ubuntu)	🔽 Medium 🛛
×	Q AV-ControlPC Intel	🔽 Medium
× 0	Q AV-ControlPC-Storage	🔽 Medium 🛛
× 0	Q AV-Self Driving OS	🔽 Medium 🛛
× O	Q AV-OnBoard-Database (PostegreSC	🔽 Medium 🛛
× 0	Q AV-ROS	🔽 Medium 🛛
0		

Navigate To Threats Of AV-OnBoard-Database (PostegreSQL) 🚝 Asset & 💿 Activate/Deactivate Threats.

	Code	Name	Likelihood	Active	Counter Measures
Ľ	TH-01	Malware Injection	✓ 3 - Periodic (Ha		(+)
Ľ*	TH-02	Denial of Service	🗸 3 - Periodic (Ha		(+)
Ľ	TH-11	Software Exploitati	🗸 3 - Periodic (Ha		+
Ľ	TH-14	Device Modificatio	🗸 2 - Rare (Happe		+
C.	TH-21	Resource Exhausti	🗸 🗸 - Periodic (Ha		+
C.	TH-22	Isolation/Virtualiza	🗸 4 - Reqular (Tal		(+)
Ľ*	TH-23	Management Inter	🗸 2 - Rare (Happe		+
Ľ	TH-24	Unauthorized Acce	🗸 🗸 - Periodic (Ha		+
Ľ	TH-25	Abuse of Authorisa	🗸 2 - Rare (Happe		(+)
2	TH-27	Abuse of Authentic	🗸 2 - Rare (Happe		+

Figure 17. Main-Control-PC (AV On-board PostgreSQL Database Threats and Likelihoods)

25	Q	
City	SC	APE

	Asset ch self driving vehicle control PC	B Save	× Delete
Composite Asset Details			
Accentalist			
Assets List ect Basic Assets			
	Asset Selector	Priority In Terms Of Economic	Value
0	Asset Selector	Priority In Terms Of Economic  Medium	Value
0		1	
	Q AV-ControlPC OS (Ubuntu)	Medium	×
	AV-ControlPC OS (Ubuntu)     AV-ControlPC Intel	Medium     Medium	*
•	AV-ControlPC OS (Ubuntu)     AV-ControlPC Intel     AV-ControlPC-Storage	Medium     Medium     Medium     Medium	× ×

#### I Threats of AV-ROS ⅔ Asset

Navigate To Threats Of AV-ROS # Asset & O Activate/Deactivate Threats.

	Code	Name	Likelihood	Active	Counter Measures
Ľ	TH-01	Malware Injection	✓ 3 - Periodic (Ha		(+)
C.	TH-02	Denial of Service	✓ 4 - Requiar (Tal		+
ď	TH-11	Software Exploitati	🗸 4 - Reqular (Tal		+
Ľ	TH-14	Device Modificatio	✓ 2 - Rare (Happe)		+
2*	TH-21	Resource Exhausti	🗸 4 - Reqular (Tal		(+)
Ľ	TH-22	Isolation/Virtualiza	✓ 2 - Rare (Happe)		(+)
Ľ	TH-23	Management Inter	🗸 4 - Reqular (Tal		+
C.	TH-24	Unauthorized Acce	✓ 4 - Reqular (Tal	Ī 🖌	+
Ľ	TH-25	Abuse of Authorisa	🗸 4 - Reqular (Tal		(+)
2	TH-27	Abuse of Authentic	🗸 4 - Reqular (Tal		+

Figure 18. Main-Control-PC (AV-ROS Threats and Likelihoods)



Composite Asset Details	I f = Assets ♣ Asset Relationsh	ips	
Asset Links Lis	Asset A	Asset B	Туре
]	Q AV-ControIPC OS (Ubunt	🔍 AV-OnBoard-Database (I	Stores 5
]	Q AV-ControIPC OS (Ubunt	Q AV-Self Driving OS	Hosts
]	Q AV-ControIPC OS (Ubunt	Q AV-ROS	🖸 Hosts 🚦
	Q AV-ROS	🔍 AV-OnBoard-Database (I	Stores E

Figure 19. Main-Control-PC (Asset Relationships)



#### o Test-Case 2 Asset Cost Evaluation

Composite Asset AV RSU and OBU Communications	Save × Delete
<b>7%</b> Basic Information Fill Composite Asset's Basic Information <b>Code</b>	
AV-RSUCommunication	
AV-RSUCOMMUNICATION *Required Field	
Name	
AV RSU and OBU Communications	
* Required Field	
Description	
Linked Intangible Assets Select Intangible Assets From The List By Clicking O Select Button. X Data X Reputation X Brand X Organizational Capital +	
Select Intangible Assets From The List By Clicking O Select Button.	
Select Intangible Assets From The List By Clicking ● Select Button: × Data × Reputation × Brand × Organizational Capital + € Economic Values	
Select Intangible Assets From The Uit By Clicking ● Select Button:	
Select Intangible Assets From The List By Clicking ● Select Button.	
Select Intangible Assets From The Uit By Clicking ● Select Button:	
Select Intangible Assets From The List By Clicking I Select Button.	
Select Intangible Assets From The List By Clicking I Select Button.	
Select Intangible Assets From The List By Clicking I Select Button.	

Figure 20. AV RSU and OBU Communications (Basic Information)





#### o RITA Threat Mapping Test-Case 2

dit Composite Asset Av	RSU and OBU Communications	B Save	× Delete
∃Assets List elect Basic Assets	Asset Selector	Priority In Terms Of Econom	nic Value
		10	
× 0	Q RSU hardware	🔽 Medium	×
× 0	RSU hardware     RSU application	Medium     Medium	
× 0			×
× 0	RSU application	Medium	× ×

	Code	Name	Likelihood	Active	Counter Measures
്	TH-08	Failures of Devices	✓ 2 - Rare (Happ		+
2°	TH-12	Natural Disaster	🗸 2 - Rare (Happ		$(\pm)$
Ľ	TH-13	Environmental Dis	✓ 2 - Rare (Happ		$(\pm)$
Ľ	TH-14	Device Modificatic	✓ 3 - Periodic (Ha		( <del>+</del> )
ď	TH-15	Device Destruction	✓ 2 - Rare (Happ		$(\pm)$
Ľ	TH-16	Device Loss or The	✓ 2 - Rare (Happ		+
ď	TH-18	Attacks on Decom	✓ 2 - Rare (Happ		(+)
ď	TH-24	Unauthorized Acce	✓ 2 - Rare (Happ		$(\pm)$

Figure 21. AV RSU and OBU Communications (RSU hardware and Likehoods)

CitySCAPE

SCAPE						
Ξ						
		DBU Communications ussets 웂 Asset Relations	ships		Save × Delet	
Assets lect Basic As		Asset Selector		Priority In Term	s Of Economic Value	
• 0		Q RSU hardware		Medium		
< 0		Q RSU application	n	🔽 Medium		
0		Q OBU hardware		Medium		
< 0		Q OBU applicatio	n.	Medium		
		cation ;= Asset tion ;= Asset & • Activate/E Name	Deactivate Threats. Likelihood	Active	Counter Measures	
5	TH-01	Malware Injection	✓ 3 - Periodic (H	έ 🖌	+	
л ,	TH-02	Denial of Service	✓ 4 - Requiar (Ta	•	× Countermeasure for DoS of Ubuntu	
					(+) os	
5	TH-09	Failure of System	🗸 2 - Rare (Happ	9 🖌	+	

C.	TH-09	Failure of System	✓ 2 - Rare (Happ)		(+)
Ľ	TH-11	Software Exploitat	✓ 4 - Reqular (Ta		+
Ľ	TH-14	Device Modificatic	✓ 4 - Reqular (Ta		$(\pm)$
Ľ"	TH-21	Resource Exhausti	🗸 4 - Reqular (Ta		$(\pm)$
Ľ*	TH-22	Isolation/Virtualiza	✓ 2 - Rare (Happ		+
Ľ.	TH-23	Management Inte	✓ 3 - Periodic (Ha		$(\pm)$
Ľ	TH-24	Unauthorized Acce	✓ 3 - Periodic (Ha	<ul> <li>Image: A start of the start of</li></ul>	+
Ľ	TH-25	Abuse of Authorisa	✓ 3 - Periodic (H≀		× Countermeasure for DoS of Ubuntu
					(+) os
ď	TH-27	Abuse of Authenti	✓ 4 - Reqular (Ta	<ul> <li>Image: A start of the start of</li></ul>	÷
്	TH-28	Identity Theft	✓ 2 - Rare (Happ)		(+)
ď	TH-29	Social Engineering	✓ 2 - Rare (Happ)		+

Figure 22. AV RSU and OBU Communications (RSU application Threats and Likehoods)

CitySCAPE

Composite Asset AV RSU				Save × Delete
🕆 Composite Asset Details	출 Assets 응 Asset Re	elationships		
Assets List				
	Asset Selecto	r	Priority In Term	of Economic Value
× 0	Q RSU hard	lware	🖬 Medium	
× 0	🔍 RSU app	lication	Medium	×
× 0	Q OBU har	dware	Medium	×
× 0	Q OBU app	lication	🔄 Medium	
- 1	<b>N</b>			
0				

	Code	Name	Likelihood	Active	Counter Measures
C.	TH-08	Failures of Devices	🗸 2 - Rare (Happ		$(\pm)$
Ľ	TH-12	Natural Disaster	🗸 🗸 - Rare (Happ		(+)
Ľ	TH-13	Environmental Dis	🗸 2 - Rare (Happ		(+)
Ľ	TH-14	Device Modificatic	🗸 3 - Periodic (Ha		+
ď	TH-15	Device Destruction	✓ 3 - Periodic (Ha		(+)
Ľ	TH-16	Device Loss or The	🗸 2 - Rare (Happ		$(\pm)$
Ľ	TH-18	Attacks on Decom	🗸 2 - Rare (Happ		$(\pm)$
C.	TH-24	Unauthorized Acce	🗸 2 - Rare (Happ		$(\pm)$

Figure 23. AV RSU and OBU Communications (OBU hardware Threats and Likehoods)

CitySCAPE

Composite Asset AV RSU and			D Sa	ave × Delete
😚 Composite Asset Details	E Assets 욺 Asset Relation:	ships		
E Assets List elect Basic Assets	Asset Selector		Priority In Terms Of Eco	nomic Value
× 0	Q RSU hardware		Medium	
× 0	Q RSU applicatio	n	Medium	×
× 0	Q OBU hardware		Medium	×
× 0	Q OBU applicatio	วท	Medium	×
•	<u>.</u>		N	
	blication ∷= Asset			

Ľ	TH-01	Malware Injection	✓ 3 - Periodic (Ha)		<b>(+)</b>
Ľ	TH-02	Denial of Service	🗸 4 - Reqular (Ta		× Countermeasure for DoS of Ubuntu
					e os
Ľ	TH-09	Failure of System	🗸 2 - Rare (Happ		$(\pm)$
്	TH-11	Software Exploitat	🗸 4 - Reqular (Ta		+
Ľ	TH-14	Device Modificatic	🗸 4 - Reqular (Ta		$(\pm)$
Ľ	TH-21	Resource Exhausti	🗸 4 - Reqular (Ta		+
Ľ	TH-22	Isolation/Virtualiza	🗸 2 - Rare (Happ		+
Ľ*	TH-23	Management Inte	🗸 3 - Periodic (Ha		+
Ľ	TH-24	Unauthorized Acce	✓ 3 - Periodic (Ha	<ul> <li>Image: A start of the start of</li></ul>	(+)
Ľ	TH-25	Abuse of Authorise	✓ 3 - Periodic (Ha		× Countermeasure for DoS of Ubuntu
					(+) os
Ľ	TH-27	Abuse of Authenti	🗸 4 - Reqular (Ta		+
Ľ	TH-28	Identity Theft	🗸 2 - Rare (Happ		+
Ľ	TH-29	Social Engineering	✓ 2 - Rare (Happ)		+
			N		

Figure 24. AV RSU and OBU Communications (OBU application Threats and Likehoods)

## 



It is essential that the cybersecurity tests do not impact operational systems of Tallinn University of Technology. The cybersecurity tests need to be performed on a network which is isolated from the university and will not have the potentiality to have cascading impacts on real-world/live services. The weeks of August 8<sup>th</sup> to 18<sup>th</sup> will be used to prepare the Tallinn Pilot Demonstration.

Any cybersecurity solution needs to be updated based on changes in the cyber threat landscape, which is where shared CTI enters the picture. Threat sharing platforms such as MISP ensure that new threats can be identified more quickly such that response can be adequately coordinated.

DNSC, the Romanian CERT that is a partner in the CitySCAPE project, uses MISP for the collection of cybersecurity alerts from different stakeholders. The platform is used for the collection, processing, and dissemination of data related to cybersecurity incidents, vulnerabilities, threats, events, and artefacts, including incident notifications received by DNSC. Information such as malicious URLs, IPs, and file signatures are usually distributed through this module.

During pilot execution in Tallinn DNSC presented how it exchanges IOCs with other entities. DNSC's MISP data tagged with 'TLP:WHITE' can be made available to CitySCAPE in a feed that can be imported in the CitySCAPE platform. TLP stands for Traffic Light Protocol; a protocol created to promote the sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four main tags to indicate expected sharing boundaries to be applied by the recipient(s). The four tags are red (named recipients only), amber (limited distribution), green (community-wide distribution), and clear/white (unlimited distribution). CitySCAPE will receive only TLP:CLEAR/TLP:WHITE data for now. DNSC usually shares IOCs from last 7 days. To facilitate sharing, DNSC IOCs are also available via SFTP. The print-screens below show examples of TLP:WHITE type events that can be exported from the DNSC MISP, examples of attributes (IOCs) attached to an event and also examples of IOCs exported to the SFTP server.





Citys	DCAPE									* * *	
D Published	Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr. #Sightings #Prop #Posts	Creator user	Date	Last modified at †	Info
	CERT-Bayern	CERT-RO	₩ 3736		Ip:white	7	3	tehnic@cert.ro	2022-08-10	2022-08-10 04:04:48	Daily Incremental ThreatFox Import - 2022-08-10
- 🗸	Excellium-Services	CERT-RO	<b>¥</b> 3740		CERT-XLM:fraud="phishing" O tlp:white	1		tehnic@cert.ro	2022-08-09	2022-08-09 19:08:13	Phishing page
	Excellium-Services	CERT-RO	<b>¥</b> 3738		CERT-XLM.fraud="phishing" tlp:white	1		tehnio@cert.ro	2022-08-09	2022-08-09 19:02:30	Phishing page
□ ✓	CERT.SI - SLOVENIA NATIONAL CERT	CERT-RO	₿ 3735		Serve Source Server Ser	105	11	tehnic@cert.ro	2022-08-09	2022-08-09 17:47:31	FormBook downloader - dock template relationship
	Excellum-Services	CERT-RO	¥ 3739		CERT-XLM:fraud="phishing" O Up.white	1		tehnic@cert.ro	2022-08-09	2022-08-09 18:01:51	[CSSF] Warning concerning fraudulent activities by persons misusing the name of the European Investment Bank (EIB)
	Excellium-Services	CERT-RO	₿ 3737		CERT-XLM fraud="phishing" tlp:white	1		tehnic@cert.ro	2022-08-09	2022-08-09 12:24:33	Phishing page
	CERT-Bayern	CERT-RO	₿ 3734		Itp:white         Itp:white         Itp:white         Itp:white         Itp://white.org         I	3	1	tehnic@cert.ro	2022-08-09	2022-08-09 02:13:33	Daily Incremental ThreatFox Import - 2022-08-09
	CERT PKO BP	CERT-RO	₿ 3732	Target Information Q	MalSpam 😨 tlp:white 🔇 AgentTesla	18	219	tehnic@cert.ro	2022-08-08	2022-08-08 10:14:14	"Subject: Fwd: Fwd: Zapłata -

0.						From: krkos@meosekfuszert.hu" Campaign
□ ✓	xameco.net	CERT-RO ¥3733	tp:white O Downloader     circl:incident-classification="malware"	72 4	tehnio@oert.ro 2022-08-08 2022-08-08 08:43:45	Downloaders Grabbed From Honeypot Logs (Week 32/2022)
- ~	CERT-Bayern	CERT-RO ¥ 3731	tip white Source:threatfox.abuse.ch     osint source-type="block-or-filter-list"	10 2	tehnic@pert.ro 2022-08-08 2022-08-08 05:11:26	Daily Incremental ThreatFox Import - 2022-08-08
□ ✓	CERT-Bayem	CERT-RO ¥ 3730	tip:white Source:threatfox.abuse.ch     osint_source-type="block-or-filter-list"	44 2	tehnic@cert.ro 2022-08-07 2022-08-07 05:13:50	Daily Incremental ThreatFox Import - 2022-08-07
- ~	CERT-Bayern	CERT-RO \$ 3729	tip:white source:threatfox.abuse.ch     osint:source-type="block-or-filter-list"	11 2	tehnic@cert.ro 2022-08-06 2022-08-06 04:51:13	Daily Incremental ThreatFox Import - 2022-08-08
□ ✓	Hessen3C	CERT-RO - 3728	C tip:white	13	tehnio@oert.ro 2022-08-04 2022-08-05 10:45:12	LazarusGroup IOCs, Week 31
- ~	CERT-Bayem	CERT-RO ¥ 3724	tip white source threatfox abuse ch     osint source type="block or filter-list"	7 3	tehnio@cert.ro 2022-08-05 2022-08-05 05:10:16	Daily Incremental ThreatFox Import - 2022-08-05
□ ✓	Aaron Kaplan	O LSASS Memory - 1		46 1	tehnic@cert.ro 2022-08-04 2022-08-04 23:42:38	Untangling KNOTWEED: European private-sector offensive actor using 0-day evolutio

Has Memory - THUSUN 4: Here Template Macros - 11132/01 9:≣ Figure 26. TLP: WHITE MISP events

+ = =	X Scope toggle -	Deleted 🗠	Decay score 🛱 Sighting DB 🚯 Context 🏷 Related Tags 🍸 Filte	ring tool		
Date *	Org Category	Туре	Value	Tags	Galaxies	Comment
2022-08-09	Network activity	domain	www.mariafonsecafreitas.com Q	(⊗+) 🚨+	⊗+ ≛+	
2022-08-09	Network activity	url	http://www.mariafonsecafreitas.com/mt88/ <b>Q</b>	⊗+ ≥+	(⊗+) ≛+	C2 URL
2022-08-09	Network activity	url	http://webz.cc/oNkgc Q	⊗+] ≛+	⊗+ ≛+	Template URL
2022-08-09	Network activity	url	http://aws3.link/TWkXiI <b>Q</b>	(2)+ (2)+	(⊗+) ≛+	Template URL
2022-08-09	Network activity	url	https://webz.co/oNkgc Q	⊗+] ≛+	⊗+ ≛+	
2022-08-09	Network activity	url	https://aws3.link/IVVxXiI <b>Q</b>	⊗+ ≜+	⊗+ ≛+	
2022-08-09	Network activity	url	$\label{eq:http://jmcglone.com@www.https://www.myftp.biz/https/www_u/www.doc \end{tabular}$	⊗+ ≛+	⊗+ ≛+	RTF download URL
2022-08-09	Network activity	domain ip	www.httpswww.httpwww.myftp.biz 192.210.149.222 <b>Q</b>	⊗+ ≗+	⊗+ ≛+	
2022-08-09	Network activity	url	http://103.149.12.218/winssh/vbc.exe @	⊗+ ≗+	⊗+ ≛+	.NET injector download URL
2022-08-09	Network activity	domain	www.selectendeavor.com Q	⊗+ ≥+	⊗+ ≛+	Decoy C2
2022-08-09	Network activity	domain	www.wwwfreemovies2021.com Q	⊗+ ≗+	⊗+ ≛+	Decoy C2
2022-08-09	Network activity	domain	www.constructiongst.com	⊗+ ≜+	⊗+ ≛+	Decoy C2
2022-08-09	Network activity	domain	www.yanpoake.com Q	⊗+] ≛+	⊗+ ≛+	Decoy C2
2022-08-09	Network activity	domain	www.qxu0l1pgl0jm1.xyz <b>Q</b>	<b>⊗</b> + <b>≜</b> +	⊗+ ≛+	Decoy C2
2022-08-09	Network activity	domain	www.Sid9piB944ktb.xyz	(2)+ (2)+	(⊗+) ≛+	Decoy C2

Figure 27. MISP event attributes





Fig 28. IOCs from SFTP files exported from MISP

Considering that the exchange of IOCs is bidirectional, it was also discussed how DNSC can receive CTI from CitySCAPE (either through the MISP platform installed in CitySCAPE, or through the SFTP server installed at DNSC level).