SCENARIOS TEMPLATE
ONLY FOR YOUR REFERENCE - DONT COMPLETE

CiRCAT
Cybersecurity Infrastructure Resilience, Collaboration and Advanced Training

Submission deadline: July 9, 2026, at 15:00 (Brussels time)

Apply at:https://opportunities.getonepass.eu/open-opportunities/circat-opencalls/opencall1

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however, those of the authors only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them. This project is supported by the European Cybersecurity Competence Centre.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Disclaimer

This document has been produced in the context of the CIRCAT Project. The CIRCAT project is funded by the European Union under Grant Agreement 101249750. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project is supported by the European Cybersecurity Competence Center (ECCC) and its members.

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
V0.1	5/3/2026	Initial version	K3Y

Table of Contents

List of Tables

1 Pilot X - Identification of System Assets

Please provide the system assets of this use case.

Table 1: List of system assets

ID	Asset Name	Asset Type	Description	Owner	Location	Data Processed by the Asset	Criticality	Access Level - Can be adjusted by CIRCAT
A unique identifier for the system asset	*The exact name of the system asset*	*Hardware or Software etc*	*A brief explanation of what the system asset is and its relevance to the use case.*	*The partner responsible for managing the system asset*	*Where the asset is physically or virtually stored/located.*	*What kind of data is used by this asset*	*H (High)/M (Medium)/L (Low)*	*No/Automatic/Manual*

2 Pilot X – Identification of Data Assets

Please enumerate the data assets of this use case.

Table 2: List of data assets

ID	Data Name	Data Format	Description	Data Source	Owner	Storage Location
A unique identifier for the data asset	*The exact name of the data asset*	*The format in which the data is stored (e.g., CSV, JSON, XML, SQL).*	*A brief explanation of what the data asset is and its relevance to the use case.*	*The origin of the data*	*The partner responsible for managing the data asset*	*Where the data is stored.*

3 Pilot X – Identification of Security Mechanisms

Please enumerate the security mechanisms in this pilot.

Table 3: List of security mechanisms in Pilot X

ID	Name (Exact Hardware or Software)	Description	Owner	Location	Access Level #1 – Can be installed in the testbed	Access Level #2 – Can be adjusted by CIRCAT
A unique identifier for the security mechanism	The exact name of the security mechanism.	A brief explanation of what the security mechanism does.	The partner responsible for managing the security mechanism	Where the security mechanism is deployed and used.	Can be installed in the CIRCAT testbed?	Can be adjusted by the CIRCAT mechanisms

4 Pilot X – Topology Diagram

Based on the above information please provide a topology diagram of the system and data assets, including also the available security mechanisms.

5 Threat Prioritisation

Please fill in the table below, by characterising each technique of MITRE ATT&CK as High (H), Medium (M) or Low (L). For more information about each technique, please check MITRE ATT&CK Enterprise: https://attack.mitre.org/matrices/enterprise/

Table 4: Pilot X - Threat Prioritisation

Tactic	Technique ID	Technique Name	System Assets	Data Assets	Criticality (L/M/H)	Justification
Reconnaissance (ID: TA0043)	T1595	Active Scanning				
	T1592	Gather Victim Host Information				
	T1589	Gather Victim Identity Information				
	T1590	Gather Victim Network Information				
	T1591	Gather Victim Org Information				
	T1598	Phishing for Information				
	T1597	Search Closed Sources				
	T1596	Search Open Technical Databases				
	T1593	Search Open Websites/Domains				
	T1681	Search Threat Vendor Data				
	T1594	Search Victim-Owned Websites				

Resource Development (ID: TA0042)	T1650	Acquire Access				
	T1583	Acquire Infrastructure				
	T1586	Compromise Accounts				
	T1584	Compromise Infrastructure				
	T1587	Develop Capabilities				
	T1585	Establish Accounts				
	T1588	Obtain Capabilities				
	T1608	Stage Capabilities				
Initial Access (ID: TA0001)	T1659	Content Injection				
	T1189	Drive-by Compromise				
	T1190	Exploit Public-Facing Application				
	T1133	External Remote Services				
	T1200	Hardware Additions				
	T1566	Phishing				
	T1091	Replication Through Removable Media				
	T1195	Supply Chain Compromise				
	T1199	Trusted Relationship				
	T1078	Valid Accounts				
	T1669	Wi-Fi Networks				
Execution	T1651	Cloud Administration Command				

(ID: TA0002)	T1059	Command and Scripting Interpreter				
	T1609	Container Administration Command				
	T1610	Deploy Container				
	T1675	ESXi Administration Command				
	T1203	Exploitation for Client Execution				
	T1674	Input Injection				
	T1559	Inter-Process Communication				
	T1106	Native API				
	T1677	Poisoned Pipeline Execution				
	T1053	Scheduled Task/Job				
	T1648	Serverless Execution				
	T1129	Shared Modules				
	T1072	Software Deployment Tools				
	T1569	System Services				
	T1204	User Execution				
	T1047	Windows Management Instrumentation				
Persistence	T1098	Account Manipulation				

(ID: TA0003)	T1197	BITS Jobs				
	T1547	Boot or Logon Autostart Execution				
	T1037	Boot or Logon Initialization Scripts				
	T1671	Cloud Application Integration				
	T1554	Compromise Host Software Binary				
	T1136	Create Account				
	T1543	Create or Modify System Process				
	T1546	Event Triggered Execution				
	T1668	Exclusive Control				
	T1133	External Remote Services				
	T1574	Hijack Execution Flow				
	T1525	Implant Internal Image				
	T1556	Modify Authentication Process				
	T1112	Modify Registry				
	T1137	Office Application Startup				
	T1653	Power Settings				
	T1542	Pre-OS Boot				
	T1053	Scheduled Task/Job				

	T1505	Server Software Component				
	T1176	Software Extensions				
	T1205	Traffic Signaling				
	T1078	Valid Accounts				
Privilege Escalation (ID: TA0004)	T1548	Abuse Elevation Control Mechanism				
	T1134	Access Token Manipulation				
	T1098	Account Manipulation				
	T1547	Boot or Logon Autostart Execution				
	T1037	Boot or Logon Initialization Scripts				
	T1543	Create or Modify System Process				
	T1484	Domain or Tenant Policy Modification				
	T1611	Escape to Host				
	T1546	Event Triggered Execution				
	T1068	Exploitation for Privilege Escalation				
	T1574	Hijack Execution Flow				
	T1055	Process Injection				
	T1053	Scheduled Task/Job				
	T1078	Valid Accounts				

Defense Evasion (ID: TA0005)	T1548	Abuse Elevation Control Mechanism				
	T1134	Access Token Manipulation				
	T1197	BITS Jobs				
	T1612	Build Image on Host				
	T1622	Debugger Evasion				
	T1678	Delay Execution				
	T1140	Deobfuscate/Decode Files or Information				
	T1610	Deploy Container				
	T1006	Direct Volume Access				
	T1484	Domain or Tenant Policy Modification				
	T1672	Email Spoofing				
	T1480	Execution Guardrails				
	T1211	Exploitation for Defense Evasion				
	T1222	File and Directory Permissions Modification				
	T1564	Hide Artifacts				
	T1574	Hijack Execution Flow				
	T1562	Impair Defenses				
	T1656	Impersonation				
	T1070	Indicator Removal				

	T1202	Indirect Command Execution				
	T1036	Masquerading				
	T1556	Modify Authentication Process				
	T1578	Modify Cloud Compute Infrastructure				
	T1666	Modify Cloud Resource Hierarchy				
	T1112	Modify Registry				
	T1601	Modify System Image				
	T1599	Network Boundary Bridging				
	T1027	Obfuscated Files or Information				
	T1647	Plist File Modification				
	T1542	Pre-OS Boot				
	T1055	Process Injection				
	T1620	Reflective Code Loading				
	T1207	Rogue Domain Controller				
	T1014	Rootkit				
	T1679	Selective Exclusion				
	T1553	Subvert Trust Controls				

	T1218	System Binary Proxy Execution				
	T1216	System Script Proxy Execution				
	T1221	Template Injection				
	T1205	Traffic Signaling				
	T1127	Trusted Developer Utilities Proxy Execution				
	T1535	Unused/Unsupported Cloud Regions				
	T1550	Use Alternate Authentication Material				
	T1078	Valid Accounts				
	T1497	Virtualization/Sandbox Evasion				
	T1600	Weaken Encryption				
	T1220	XSL Script Processing				
Credential Access (ID: TA0006)	T1557	Adversary-in-the-Middle				
	T1110	Brute Force				
	T1555	Credentials from Password Stores				
	T1212	Exploitation for Credential Access				
	T1187	Forced Authentication				

	T1606	Forge Web Credentials				
	T1056	Input Capture				
	T1556	Modify Authentication Process				
	T1111	Multi-Factor Authentication Interception				
	T1621	Multi-Factor Authentication Request Generation				
	T1040	Network Sniffing				
	T1003	OS Credential Dumping				
	T1528	Steal Application Access Token				
	T1539	Steal Web Session Cookie				
	T1649	Steal or Forge Authentication Certificates				
	T1558	Steal or Forge Kerberos Tickets				
	T1552	Unsecured Credentials				
Discovery (ID: TA0007)	T1087	Account Discovery				
	T1010	Application Window Discovery				
	T1217	Browser Information Discovery				

	T1580	Cloud Infrastructure Discovery				
	T1538	Cloud Service Dashboard				
	T1526	Cloud Service Discovery				
	T1619	Cloud Storage Object Discovery				
	T1613	Container and Resource Discovery				
	T1622	Debugger Evasion				
	T1652	Device Driver Discovery				
	T1482	Domain Trust Discovery				
	T1083	File and Directory Discovery				
	T1615	Group Policy Discovery				
	T1680	Local Storage Discovery				
	T1654	Log Enumeration				
	T1046	Network Service Discovery				
	T1135	Network Share Discovery				
	T1040	Network Sniffing				

	T1201	Password Policy Discovery				
	T1120	Peripheral Device Discovery				
	T1069	Permission Groups Discovery				
	T1057	Process Discovery				
	T1012	Query Registry				
	T1018	Remote System Discovery				
	T1518	Software Discovery				
	T1082	System Information Discovery				
	T1614	System Location Discovery				
	T1016	System Network Configuration Discovery				
	T1049	System Network Connections Discovery				
	T1033	System Owner/User Discovery				
	T1007	System Service Discovery				
	T1124	System Time Discovery				
	T1673	Virtual Machine Discovery				

	T1497	Virtualization/Sandbox Evasion				
Lateral Movement (ID: TA0008)	T1210	Exploitation of Remote Services				
	T1534	Internal Spearphishing				
	T1570	Lateral Tool Transfer				
	T1563	Remote Service Session Hijacking				
	T1021	Remote Services				
	T1091	Replication Through Removable Media				
	T1072	Software Deployment Tools				
	T1080	Taint Shared Content				
	T1550	Use Alternate Authentication Material				
Collection (ID: TA0009)	T1557	Adversary-in-the-Middle				
	T1560	Archive Collected Data				
	T1123	Audio Capture				
	T1119	Automated Collection				
	T1185	Browser Session Hijacking				
	T1115	Clipboard Data				
	T1074	Data Staged				

	T1530	Data from Cloud Storage				
	T1602	Data from Configuration Repository				
	T1213	Data from Information Repositories				
	T1005	Data from Local System				
	T1039	Data from Network Shared Drive				
	T1025	Data from Removable Media				
	T1114	Email Collection				
	T1056	Input Capture				
	T1113	Screen Capture				
	T1125	Video Capture				
Command and Control (ID: TA0011)	T1071	Application Layer Protocol				
	T1092	Communication Through Removable Media				
	T1659	Content Injection				
	T1132	Data Encoding				
	T1001	Data Obfuscation				
	T1568	Dynamic Resolution				
	T1573	Encrypted Channel				

	T1008	Fallback Channels				
	T1665	Hide Infrastructure				
	T1105	Ingress Tool Transfer				
	T1104	Multi-Stage Channels				
	T1095	Non-Application Layer Protocol				
	T1571	Non-Standard Port				
	T1572	Protocol Tunneling				
	T1090	Proxy				
	T1219	Remote Access Tools				
	T1205	Traffic Signaling				
	T1102	Web Service				
Exfiltration (ID: TA0010)	T1020	Automated Exfiltration				
	T1030	Data Transfer Size Limits				
	T1048	Exfiltration Over Alternative Protocol				
	T1041	Exfiltration Over C2 Channel				
	T1011	Exfiltration Over Other Network Medium				
	T1052	Exfiltration Over Physical Medium				
	T1567	Exfiltration Over Web Service				
	T1029	Scheduled Transfer				

	T1537	Transfer Data to Cloud Account				
Impact (ID: TA0040)	T1531	Account Access Removal				
	T1485	Data Destruction				
	T1486	Data Encrypted for Impact				
	T1565	Data Manipulation				
	T1491	Defacement				
	T1561	Disk Wipe				
	T1667	Email Bombing				
	T1499	Endpoint Denial of Service				
	T1657	Financial Theft				
	T1495	Firmware Corruption				
	T1490	Inhibit System Recovery				
	T1498	Network Denial of Service				
	T1496	Resource Hijacking				
	T1489	Service Stop				
	T1529	System Shutdown/Reboot				

6 Pilot X – Penetration Testing Scenarios Definition

6.1 Penetration Testing Scenario X.Y – Name

Please fill in the following table with the description of the scenario.

Table 5: Penetration Testing Scenario X.Y – Name

Penetration Testing Scenario X.Y	<Please provide the name of the scenario
Description	<Please provide a brief description of the scenario>
Type	[Whitebox] [Blackbox] [Greybox] [Agentic]
Involved Testers	<Please list the involved actors and specify their role>
System Assets	<Please list the system assets relevant to this scenario>
Data Assets	<Please list the data assets relevant to this scenario>
Information Gathering	<Please list the information gathering techniques relevant to this scenario. Moreover for each technique indicate also the tools that will be used for this purpose. For instance: T1592 - Nmap>
Vulnerability Assessment	<Please list the vulnerability assessment techniques relevant to this scenario. Moreover for each technique indicate also the tools that will be used for this purpose. For instance: T1592 - Nmap>
Exploitation	<Please list the exploitation techniques relevant to this scenario. Moreover for each technique indicate also the tools that will be used for this purpose. For instance: T1592 - Nmap>
Security Mechanisms	<Please list the security mechanisms that can be utilised in this scenario>
Assumptions	<Please enumerate any assumptions regarding the scenario>

6.2 Penetration Testing Scenario X.Y – Name

Please fill in the following table with the description of the scenario.

Table 6: Penetration Testing Scenario X.Y – Name

Penetration Testing Scenario X.Y	<Please provide the name of the scenario
Description	<Please provide a brief description of the scenario>
Type	[Whitebox] [Blackbox] [Greybox] [Agentic]
Involved Testers	<Please list the involved actors and specify their role>
System Assets	<Please list the system assets relevant to this scenario>
Data Assets	<Please list the data assets relevant to this scenario>
Information Gathering	<Please list the information gathering techniques relevant to this scenario. Moreover for each technique indicate also the tools that will be used for this purpose. For instance: T1592 - Nmap>
Vulnerability Assessment	<Please list the vulnerability assessment techniques relevant to this scenario. Moreover for each technique

Penetration Testing Scenario X.Y	<Please provide the name of the scenario
	indicate also the tools that will be used for this purpose. For instance: T1592 - Nmap>
Exploitation	<Please list the exploitation techniques relevant to this scenario. Moreover for each technique indicate also the tools that will be used for this purpose. For instance: T1592 - Nmap>
Security Mechanisms	<Please list the security mechanisms that can be utilised in this scenario>
Assumptions	<Please enumerate any assumptions regarding the scenario>

6.3 Penetration Testing Scenario X.Y – Name

Please fill in the following table with the description of the scenario.

Table 7: Penetration Testing Scenario X.Y – Name

Penetration Testing Scenario X.Y	<Please provide the name of the scenario
Description	<Please provide a brief description of the scenario>
Type	[Whitebox] [Blackbox] [Greybox] [Agentic]
Involved Testers	<Please list the involved actors and specify their role>
System Assets	<Please list the system assets relevant to this scenario>
Data Assets	<Please list the data assets relevant to this scenario>
Information Gathering	<Please list the information gathering techniques relevant to this scenario. Moreover for each technique indicate also the tools that will be used for this purpose. For instance: T1592 - Nmap>
Vulnerability Assessment	<Please list the vulnerability assessment techniques relevant to this scenario. Moreover for each technique indicate also the tools that will be used for this purpose. For instance: T1592 - Nmap>
Exploitation	<Please list the exploitation techniques relevant to this scenario. Moreover for each technique indicate also the tools that will be used for this purpose. For instance: T1592 - Nmap>
Security Mechanisms	<Please list the security mechanisms that can be utilised in this scenario>
Assumptions	<Please enumerate any assumptions regarding the scenario>

6.4 Penetration Testing Scenario X.Y – Name

Please fill in the following table with the description of the scenario.

Table 8: Penetration Testing Scenario X.Y – Name

Penetration Testing Scenario X.Y	<Please provide the name of the scenario
Description	<Please provide a brief description of the scenario>
Type	[Whitebox] [Blackbox] [Greybox] [Agentic]
Involved Testers	<Please list the involved actors and specify their role>
System Assets	<Please list the system assets relevant to this scenario>
Data Assets	<Please list the data assets relevant to this scenario>

Penetration Testing Scenario X.Y	<Please provide the name of the scenario
Information Gathering	<Please list the information gathering techniques relevant to this scenario. Moreover for each technique indicate also the tools that will be used for this purpose. For instance: T1592 - Nmap>
Vulnerability Assessment	<Please list the vulnerability assessment techniques relevant to this scenario. Moreover for each technique indicate also the tools that will be used for this purpose. For instance: T1592 - Nmap>
Exploitation	<Please list the exploitation techniques relevant to this scenario. Moreover for each technique indicate also the tools that will be used for this purpose. For instance: T1592 - Nmap>
Security Mechanisms	<Please list the security mechanisms that can be utilised in this scenario>
Assumptions	<Please enumerate any assumptions regarding the scenario>

7 Pilot X – User Requirements

Based on the analysis of the previous scenarios, please fill in the following table with the user requirements.

Table 9:List of user requirements

ID	Description	Type	Priority
<A unique identifier>	*<A brief description about the requirement>*	*<Functional or Non-Functional>*	*<Low, Medium, High>*
MSPL Representation: Please provide the MSPL representation based on the following example.			
Example			
UR_UCX_01	The system should be able to allow access only to users with a high trust level.	Functional	High
MSPL Representation: **<mspl>** **<!-- Rule 1: Allow Access Only to High-Trust Users -->** **<rule>** **<name>AllowTrustedUsersOnly</name>** **<action type="allow"/>** **<condition>** **<trust-level>HIGH</trust-level>** **<authentication>MultiFactor</authentication>** **<role>Employee</role>** **<source>TrustedDevices</source>** **<destination>SecureNetwork</destination>** **</condition>** **</rule>** **</mspl>**			

8 Pilot X – Security Requirements

Based on the analysis of the previous scenarios, please fill in the following table with the security requirements.

Table 10: List of security requirements

ID	Description	Type	Priority
<A unique identifier>	*<A brief description about the requirement>*	*<Functional or Non-Functional>*	*<Low, Medium, High>*
MSPL Representation: Please provide the MSPL representation based on the following example.			
Example			
SR_UC4_01	The system should be able to monitor and log all administrative actions.	Functional	High
MSPL Representation: **<mspl>** **<!-- Rule 1: Allow Access Only to High-Trust Users -->** **<rule>** **<name>AllowTrustedUsersOnly</name>** **<action type="allow"/>** **<condition>** **<trust-level>HIGH</trust-level>** **<authentication>MultiFactor</authentication>** **<role>Employee</role>** **<source>TrustedDevices</source>** **<destination>SecureNetwork</destination>** **</condition>** **</rule>** **</mspl>**			

9 Pilot X – Privacy Requirements

Based on the analysis of the previous scenarios, please fill in the following table with the privacy requirements.

Table 11: List of privacy requirements

ID	Description	Type	Priority
<A unique identifier>	*<A brief description about the requirement>*	*<Functional or Non-Functional>*	*<Low, Medium, High>*
MSPL Representation: Please provide the MSPL representation based on the following template.			
Example			
PR_UC4_01	The system should be able to allow users to request data deletion.	Functional	High
MSPL Representation: **<mspl>** **<rule>** **<name>LogAdminActions</name>** **<action type="log"/>** **<condition>** **<user-role>Admin</user-role>** **<log-destination>SecurityLogs</log-destination>** **<log-level>Critical</log-level>** **</condition>** **</rule>** **</mspl>**			