Security Operation Centre Use Cases Developments for Operational Technology

Cyber security threat landscape is a growing source of concern to industrial control systems (ICS). Therefore, improving Operational Technology (OT) infrastructure resiliency and protection against cyber-attacks serves the ultimate objective of minimising production downtime. In order to achieve this, organisations should consider functional and innovative security monitoring strategies as well as use of a Security Operation Centre (SOC). Figure-1 below shows the high-level design stages of SOC for OT: it starts with developing the SOC use cases (UCs), as they are considered the basis for the other stages. Data onboarding is the next stage comprising designing the security logs collection mechanisms, which are required to monitor the defined UCs. Third stage is design of detection rules, investigation and response playbooks and runbooks for each UC. Final stage is implementation, commissioning and moving into production.

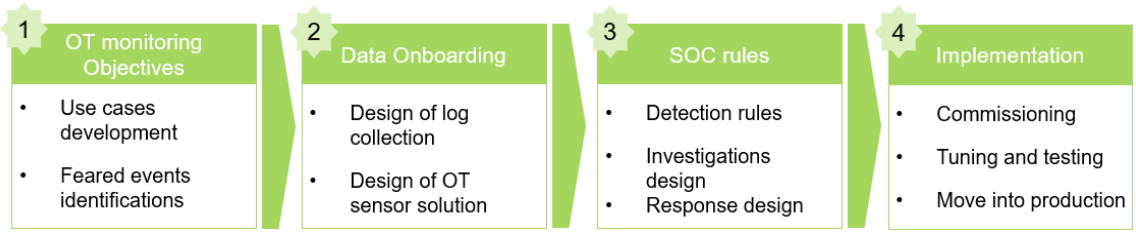

Figure 1 - SOC High-Level Design Stages

Airbus CyberSecurity has developed SOC UCs for OT in several Critical National Infrastructure (CNI) sectors - this report is focused on SOC UCs defined for the water sector. The report will demonstrate Airbus methodology for defining SOC UCs for OT, then illustrates a sample of the SOC UCs that have been developed during the project execution.

Airbus methodology to develop a SOC UC starts by identifying the assets and systems, which are required to be monitored within the SOC. Once this is completed, SOC UCs design can be conducted - in this step, each of the identified assets/systems will be analysed in order to understand their threats profile, the log types that need to be pulled, and the data sources required to pull (or push) these logs. The next step will implement these defined UCs in the SIEM (Security Information and Event Management) by coding the detection rules, investigation & response runbooks and playbooks. Testing step will examine these coded rules and ensure that all defined scenarios for the UC can be detected. Then the final stage is that the UC will be deployed into the production environment. Note – an important aspect of this methodology is to implement version control and change management procedures for the defined UCs across the whole lifecycle.

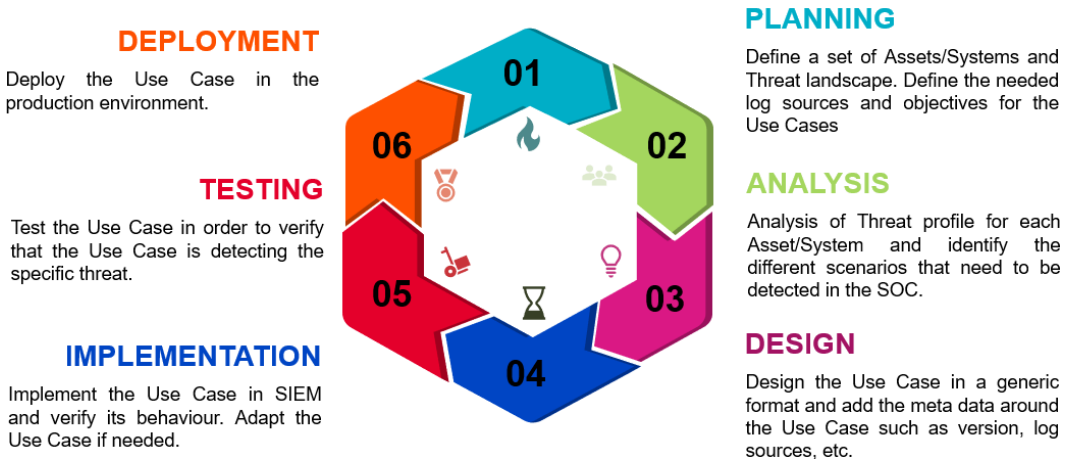

Figure 2 - Airbus Methodology in Developing SOC Use Cases for OT

Each of the UCs, during development, is mapped with the MITRE ATT&CK® models (link): these models are Enterprise ATT&CK; ICS ATT&CK; and Pre-ATT&CK. ATT&CK models assist in mapping the tactics and techniques that can be used by an adversary to attack the system. This exercise also gives the directions to identify the required detection techniques or tools to detect an adversary in the different stages of the attack lifecycle.

Example Use Cases:

This section illustrates a sample of SOC UCs that cover all zones of an OT environment. By referring to the Purdue Model[1], an OT infrastructure comprises 3 main zones: Cell/Area Zone, which contains the embedded controllers and supervisory control hosts; Manufacturing Zone, which contains the manufacturing operations; and the Enterprise Zone, which contains business planning and logistics. The attacker could initiate a cyber-attack from higher zones and go down to OT specific assets or can initiate it directly from the Cell/Area zone. Therefore, UC-1 and UC-2 are focused on the Enterprise and Manufacturing zones. UC-3 is targeting the Manufacturing zone. UC-4, UC-5, and UC-6 are focused on Cell/Area zone.

UC-1: Multiple failed login followed by successful login

An attacker could manage to guess or brute force credentials for servers or network devices at production level, such as engineering station, SCADA server, industrial firewall, or Ethernet switch. With this access, the attacker could elevate the privileges and misuse every accessible function or create further harmful actions.

T1110 Brute Force, T1003 Credential Dumping, and T1078 Valid Accounts are the possible ATT&CK techniques that an adversary could use to perform brute-force attacks. Windows event logs, active directory database logs, and syslogs can be collected to monitor and detect login failures. To mitigate this, account lockout policies after a certain number of failed login attempts need to be defined to prevent passwords from being guessed and applying multi-factor authentication mechanisms.

UC-2: Excessive denied on the network devices

An excessive denied inbound connections on the network devices such as firewalls, Ethernet switches or data diodes could be conducted by an adversary. This indicates adversaries' access to the resource inside these devices in order to initiate a Denial of Service (DoS) attack.

T1205 Port Knocking, T1046 Network Service Scanning, T1110 Brute force, and T1026 Multiband communications are the possible ATT&CK techniques used by the attacker. To detect this type of attacks, syslogs and events from the network devices need to be monitored to check if network service scanning is legitimate, analysis of network data for uncommon data flows, and analysis of packet contents to detect communications that do not follow the expected protocol behaviour for the port that is being used. To mitigate this, network intrusion detection and prevention systems can be employed.

UC-3: SQL injection attacks on the Historian server

An adversary could gain an unauthorised access and execute SQL malicious statements on a compromised Historian server. This includes modify or delete (data tampering) of the records in the database or conducting replay attacks.

T1055 Process injection, T1210 Exploitation of Remote Services, T1043 Commonly Used Port, and T803 Block Command Message are the possible ATT&CK techniques used by the attacker. Detection can be done by monitoring SQL database logs for abnormal behaviour that may indicate attempted or successful exploitation and by using deep packet inspection to look for artifacts of common exploit traffic, such as SQL injection. Mitigations can be done by employing Application Firewalls and applying Application Isolation and least privilege. In addition, blocking potential malicious software that may contain process injection functionality by using whitelisting tools.

[1] Purdue Model is a reference architecture for OT infrastructures. For more information, refer to section 2.1 of this reference (link)

UC-4: USB insertion or addition

An attacker could execute a malicious code by using an infected removable media, this can be delivered physically by inserting a USB removable media on the target host, Human Machine Interface (HMI) or Embedded Controller.

T1091 Replication Through Removable Media, T1055 Process Injection, T1025 Data from Removable Media, and T1092 Communication Through Removable Media are the possible ATT&CK techniques used by the attacker. Detection by monitoring file access on removable media and collecting the windows logs that indicate processes execution from removable media after it is mounted or when initiated by a user. Mitigation can be done by disabling Autorun feature if it is unnecessary and restricting removable media on the endpoints.

UC-5: Modification on the SCADA application software

An attacker could manage to gain unauthorised access to the SCADA server and perform a data tampering attack on the application software, such as modify/delete/replace the project folder, changing the local SCADA values, or perform exfiltration of process information. With this access, the attacker could elevate the privileges and misuse every accessible function or create further harmful actions.

T1078 Valid Accounts, T1044 File System Permission Weakness, T1107 File Deletion, T1222 File Permissions Modification are the possible ATT&CK techniques that an adversary could use to perform these attacks. Detection can be done by monitoring the suspicious account behaviour on the SCADA application that share accounts, either user, admin, or service accounts, this can be done by monitoring the Windows logs. Also, detection by monitoring the file hashes of the SCADA folder and using tools to detect file or folder changes. To mitigate this, follow the best practices for account policy and limit privileges (least privilege) for the SCADA users. Apply whitelisting to prevent execution of any malicious script that modifies SCADA files.

UC-6: Programmable Logic Controller (PLC) code or settings changes

An adversary with unauthorised access to PLC, could perform code change, such as changing a setpoint value, process value or tuning parameters, which could create a physical damage to the environment or shutdown the production system.

T1210 Exploitation of Remote Services, T1046 Network Service Scanning, T830 Man in the Middle, T833 Modify Control Logic, and T803 Block Command Message are the possible ATT&CK techniques used by the attacker. Detection can be done by monitoring the checksum of the online code for the target PLC – if the checksum value changes, this could indicate PLC code changes. Moreover, there are COTS tools which are OT oriented and can detect PLC code changes - these tools generate syslogs that can be monitored to detect PLC code changes. Mitigations can be achieved by hardening the PLC and network devices based on vendor guidelines, applying change management policy for PLC code changes, and employing OT sensor solutions.

In conclusion, the above use cases are all real-world examples developed for a large UK CNI water company to protect their OT assets. Due to the nature of many OT systems, these UCs can be reused across different industries, but the key point is understanding the OT infrastructure’s threat landscape, existing employed security measures and security risks are important to decide if the use case needs to be monitored at SOC level. Then defining the SOC UC needs to go through a well-defined framework in order to capture all possible scenarios that would allow a cyber-attack or create a cyber risk to the target OT environment.