INDUSTRIAL CONTROL SYSTEMS
Community of Interest

What to log and monitor in an ICS/OT Environment - Consequence-driven engineered approach – Meet Admin Corp.

Introduction

This article supplements the guidance "What to log and monitor in an ICS/OT Environment" and provides a worked example of the Consequence-driven engineered logging and monitoring (CEMoL) approach to logging and monitoring. A second example will explain the approach based on the Simplified Collection Management Framework.

For this example, we will re-use fictional case study "Admin Corp" previously used by the NCSC to explore the application of the Secure Design Principles.

Admin Corp runs a plant that produces Adminox, a highly volatile, refined form of administrative paperwork that is essential to every organisation in the country. It is created from volatile raw products using a continuous chemical process.

Admin Crop have followed various NCSC principle-based guidance elements, including:

- secure design principles,
- the security architecture includes Logging Made Easy (LME) in the business environment,
- a single, multi-factor authenticated VPN gateway providing access to the ICS/OT environment,
- a Privileged Access Workstation (PAW) combined with a Virtual Desktop Infrastructure (VDI) solution, using a separate Privileged Access Management (PAM) System for the ICS/OT Environment, is used to constrain user activity to agreed policies, with network (using a network intrusion detection solution) and host (using a host based intrusion detection solution) detection rules applied across the network of ICS/OT assets.

A jump server is used to constrain user activity to agreed policies, and provide an opportunity for logging and monitoring, although Admin Corp recognise that it does not necessarily improve the security posture of remote access. In addition, network and host detection rules are applied across the network of ICS/OT assets.

CEMoL Step 1: Consequence Identification

A previous Tabletop Exercise (TTX) undertaken by the Admin Corp ICS/OT Security team, had identified potential unacceptable consequences resulting from a compromise of the Safety Systems within the Admin Corp environment. This could require that monitoring be undertaken to reduce the impact to the local environment due to an unsafe release of Adminox.

This had resulted in new controls being implemented to improve the control of the transfer of data via removable media onto the engineering laptops. Whilst the chosen controls had the capability to be integrated into a monitoring and logging solution, it was not implemented in the first phase.

CEMoL Step 2: Attack Trees

In order to identify the monitoring and logging requirements associated with the new controls, a high-level attack tree was developed, which highlighted the potential paths, associated with the use of Identifying removeable media, through which a system could be compromised, and an unacceptable consequence realised.

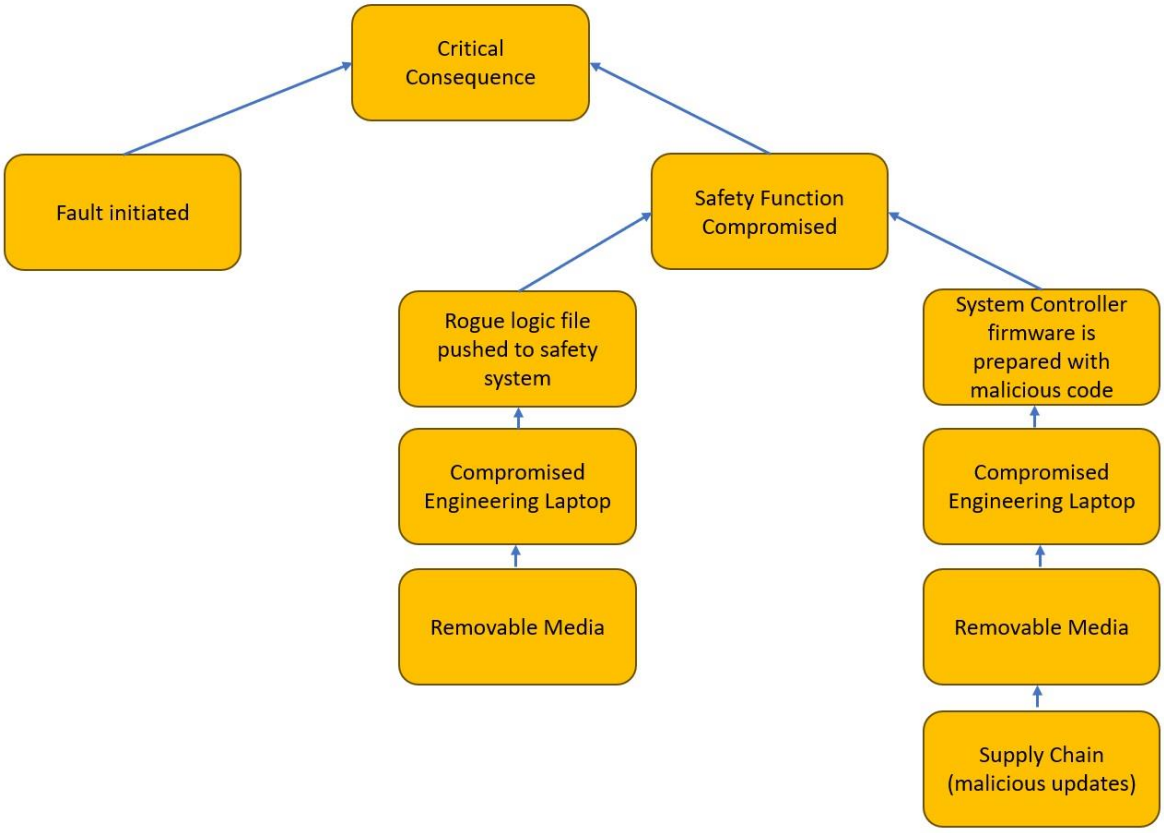

Figure 1: Basic high level Attack Tree example

CEMoL Step 3: ATT&CK Matrix

Given the ICS/OT environment used within Admin Corp, it was decided to use the standard MITRE ATT&CK for Industrial Control Systems framework. (MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations).

CEMoL Step 4: Kill Chain Analysis

The previously generated Attack trees were then used, in conjunction with the ATT&CK Matrix, to highlight potential methods by which malicious activity associated with the use of removeable media could be identified, and suitable actions undertaken within the timeframe required to prevent realisation of the identified consequences.

Assets associated with the specific kill chain steps, including the new controls, were included on the kill chain.

CEMoL Step 5: Tactics, Techniques and Procedures Identification

The kill chain analysis was updated, using the Tactics, Techniques, and Procedures (TTPs) from the MITRE ATT&CK Matrix, to identify the relevant TTPs associated with the steps in the kill chain.

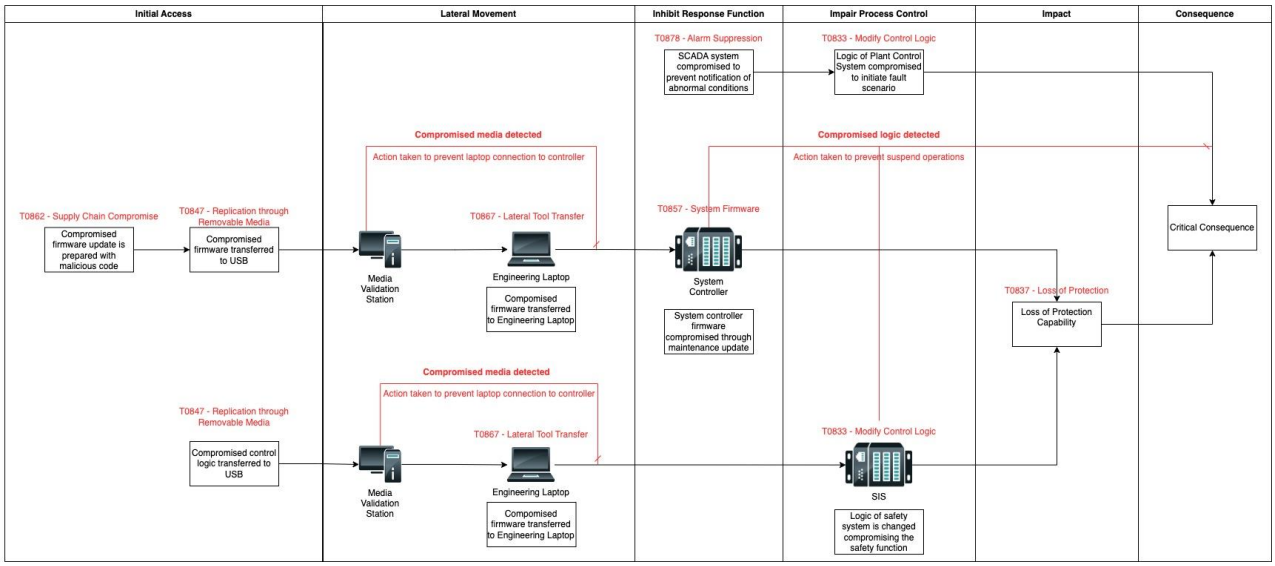

Figure 2 - Kill Chain steps with respective identified TTPs

CEMoL Step 6: Identification of Indicators

The information from the Kill Chain was summarised in table 3 below as a start of development of a data collection schedule. This focused initially on the information/logging needed to undertake threat detection, tied to the specific phases of the ICS Kill Chain and specific Mitre Att&CK Matrix TTPs.

Table 3: Kill Chain Summarisation example (With TTPs)

Asset ID	Information	Data Source	ICS Kill Chain Phase(s)	Mitre TTP	Action Enabled
MVS_01	Malware Detected	Application Logs	Lateral Movement	TA0109	Prevent connection of laptop to controller
Laptop_01	Compromised code detected	Application Logs	Lateral Movement	TA0109	Prevent connection of laptop to controller
Laptop_01	Compromised firmware detected	Application Logs	Lateral Movement	TA0109	Prevent connection of laptop to controller
SIS_01	Compromised code detected		Impair Process Control	T0833	Suspend Operations
SIS_01	Compromised firmware detected		Impair Process Control	T0857	Suspend Operations

CEMoL Step 7: Develop Data Collection Schedule

From the initial collections schedule, additional capabilities were added to address other requirements associated with Incident Response, Control Validation, and Compliance to the NIS CAF. Supplementary information identifying aspects such as data retention requirements, alert priority, were also added to give a comprehensive data collection schedule, as shown in Table 4.

Table 4: CEMoL data collection schedule example

Asset ID	Information	Data Source	Data Storage Location	Data Retention Period	ICS Kill chain Phase(s)	Mitre TTP	Alert Priority	Alert Presented At	Action Enabled
MVS_01	Malware Detected	Application Logs	SIEM	6 Months	Lateral Movement	TA0109	High	CSOC	Prevent connection of laptop to controller
MVS_01	Files written to media (with media ID)	Device Logs	SIEM	6 Months	N/A				Incident Response
MVS_01	User Authenticated	Authentication Logs	SIEM	6 Months	N/A				Incident Response
Laptop_01	Compromised code detected	Application Logs	Local	6 Months	Lateral Movement	TA0109	High	Local	Prevent connection of laptop to controller
Laptop_01	Compromised firmware detected	Application Logs	Local	6 Months	Lateral Movement	TA0109	High	Local	Prevent connection of laptop to controller
Laptop_01	Malware Detected	Application Logs	Local	6 Months	N/A				Incident Response
Laptop_01	Connection made to PLC	Application Logs	Local	6 Months	N/A				Incident Response
Laptop_01	User Authenticated	Authentication Logs	Local	6 Months	N/A				Incident Response
SIS_01	Compromised code detected	Periodic validation of SIS code	Local	6 Months	Impair Process Control	T0833	High	Local	Suspend Operations

SIS_01	Compromised firmware detected	Periodic validation of SIS firmware	Local	6 Months	Impair Process Control	T0857	High	Local	Suspend Operations

Next Steps

Having analysed the threat, identified the TTPs related, and the logging and monitoring required to understand if the threat was present in their ICS/OT environment, the Admin Corp ICS/OT Security team then start a piece of work to understand "how" to undertake logging and monitoring of their ICS/OT environment to be able to implement what is required to help monitor against the specific threats they worked through the process.

Statement of support

This guidance has been produced with support from members of the Industrial Control System Community of Interest (ICS-COI) for publication via the Research Institute for Trustworthy Inter-connected Cyber-Physical Systems (RITICS), with support from the National Cyber Security Centre (NCSC). This guidance is not intended to replace formal NCSC guidance where already available, and care has been taken to reference such existing guidance where applicable.