INDUSTRIAL CONTROL SYSTEMS
Community of Interest

GUIDANCE - What to log and monitor in an ICS/OT Environment - Collection Management Framework 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 Simplified Collection Management Framework approach to logging and monitoring. A second example will explain the approach based on the Consequence-driven engineered logging and monitoring (CEMoL) approach.

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.

Simplified Collection Management Framework for ICS/OT example

Using the Collection Management Framework (CMF) guidance, the Admin Corp ICS/OT cyber security team follow the steps described in the simplified CMF approach flow diagram to identify what to monitor in their ICS/OT environment, aided by a high-level network diagram as shown in Figure 1.

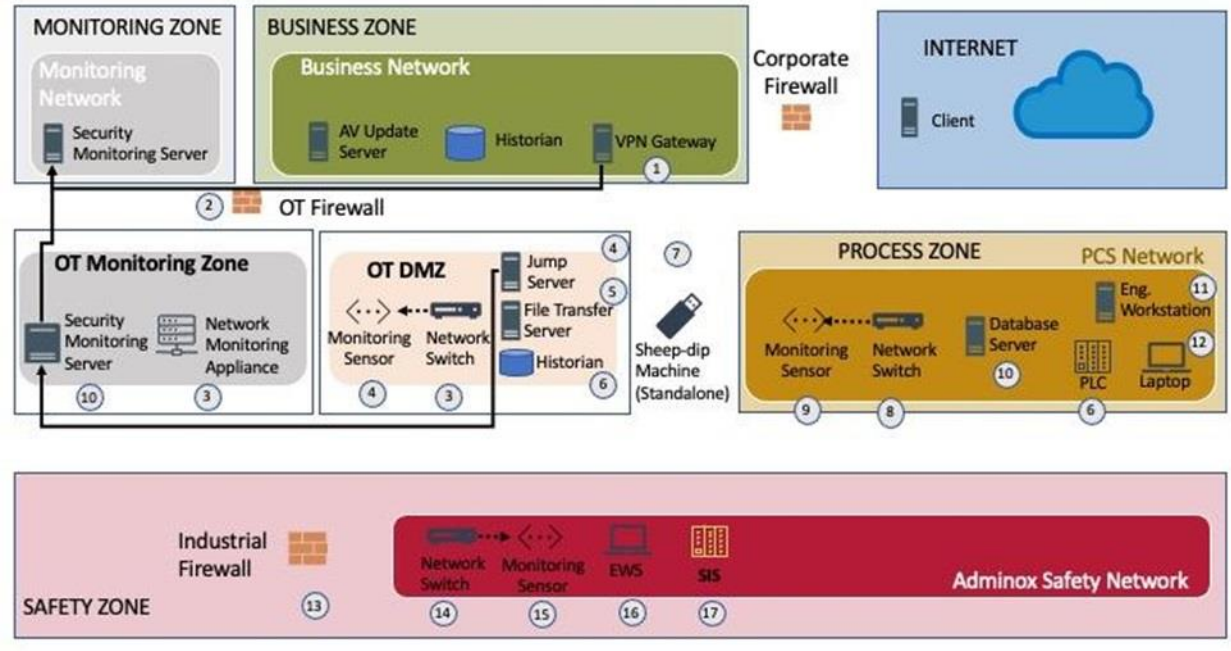

Figure 1: Admin Corp High-Level ICS/OT diagram

CMF Step 1: Identify sources of logging and monitoring requirements

Following the approach, the first step performed by Admin Corp is to identify all requirements. In this case, the Admin Corp executive team require that the ICS/OT cyber security team provide a response to their exposure to ransomware and have therefore organised a Tabletop Exercise (TTX) using a ransomware scenario (for this example, we're only covering the Ransomware threat, other threats were also covered but they're not in the guidance for the sake of brevity).

Additionally, the ICS/OT cyber security team are using information obtained from their own research of ICS/OT threats and are applying threat intelligence information that is deemed relevant and important to Admin Corp and the sector and region in which they operate (i.e. threat modelling).

Identifying requirements (TTX)

A ransomware TTX scenario is used during a tabletop exercise of the Admin Corp's central Adminox facility. Admin Corp use resources available from CISA and NCSC Exercise in a box to create the scenario and run through the exercise.

As the combined teams play through the scenario, which includes the adversary compromising the credentials of both IT and ICS/OT engineering accounts in the Business Network, the team are prompted to confirm if the compromised credentials have been used to access resources in the Process Control System (PCS) Network over the last 3 months.

The ICS/OT cyber security team are aware of the VPN solution and the authentication logs that are present on the system. The team identify that the log retention policy is 1 month, and that the logs must be collected manually, and are not forwarded to a Security information and event management (SIEM) solution or monitored either by themselves or by a third party.

Identifying requirements (threat modelling)

The Admin Corp ICS/OT security team use information obtained from advisories and ICS/OT threat intelligence providers on the Techniques, Tactics and Procedures (TTPs) used by adversaries in the cyber-attacks in Ukraine of 2015 and 2016, and the petrochemical facility in Saudi Arabia of 2017, i.e., Crash Override, Trisis, and 2023 Chemical Security Summit - Cyber Threats Facing the Chemical Sector (cisa.gov).

Admin Corp didn't use all the information verbatim about these incidents, but they did use advisories and TTPs, and interpreted them for their situation and environment.

The Admin Corp ICS/OT security team use the information to map out the adversaries known TTPs using the ICS Kill Chain and use this information to set requirements on how the Admin Corp facilities would detect and investigate the identified TTPs.

CMF Step 2: Document existing log collection arrangements

The Admin Corp ICS/OT cyber security team select their central Adminox facility, and start to document their log collection arrangements through various methods, such as workshops, plant walkdowns, engineer and operator interviews, documentation reviews etc.

The team capture the information in a spreadsheet, shown in Table 1.

Table 1: CMF documenting existing Admin Corp log collection arrangements.

Location / Zone	Asset Type	Data Type	ICS Kill chain phases	MITRE ATT&CK for ICS (Tactics)	Data storage duration	Data Storage Location	Access
PCS network	Historian	Windows Event Logs	Exploit / Install / Modify	Execution / Collection / Inhibit Response Function	7 days	Local	System engineer, local admin
	VPN	Authentication Logs	Exploit / Modify / Reconnaissance	Reconnaissance / Initial Access /	1 month	Local	Local admin
	Jump Server	Authentication Logs	Exploit / Modify / Reconnaissance	Reconnaissance / Initial Access /	1 month	Local	Local admin
	Firewall	Alerts	Delivery / C2	Initial Access / Collection/ C2	3 months	Enterprise SIEM	Enterprise cybersecurity team
	Network traffic	None	Delivery / C2 / Execute	Initial Access / Lateral Movement / Impact	None	None	N/A
	File server	Windows Event Logs	Delivery	Lateral Movement / Collection / Evasion	1 week	PCS security server	local admin

	Antivirus	Alerts	Delivery	Execution / Persistence / Lateral Movement	1 month	Local (Operator Control Room)	local admin
Control Room	Operator workstation	Windows Event Logs	Exploit / Install / Modify	Execution / Persistence / Lateral Movement / Collection	1 month	Local	System engineer, local admin
	Control network	None	N/A	Execution / Persistence / Lateral Movement / Collection / Impact	N/A	N/A	N/A
	SCADA server	Application Logs	Actions on Objectives	Execution / Persistence / Lateral Movement / Collection / Impact	2 months	Local	System engineer, local admin
Safety Zone	PLC	None	Install/Modify / Execute (stage 2)	Impair / Process Control / Impact	N/A	N/A	N/A
	Network Traffic	None	Install/Modify / Execute (stage 2)	Impair / Process Control / Impact	N/A	N/A	N/A

CMF Step 3: Identify quick wins.

As soon as the process is started, the team quickly identify quick wins that can immediately improve their security posture, which will help them achieve the two of the outcomes identified in the why they need to monitor guidance; **timely identification** and **initiation** of response effort to an attack.

Additionally, this process helps the team address the 4 identified reasons for performing logging and monitoring as described in the main guidance document:

Reason 1 – Threat Detection.

The majority of log sources require local collection for analysis. The team can work on improving this situation by exploring log forwarding solutions, SIEM integration, dedicated ICS/OT network monitoring solutions, etc.

Reason 2 – Incident Response Investigation:

The team can work to increase the awareness of which operators have the authority to collect logs manually, and the procedures for doing so. The team can then progress the development of forensic collection procedures and tools, training first responders on how to collect data, and testing collection processes. This will not increase their ability to detect an attack, however it will significantly increase the team's incident response capability.

Reason 3 – Compliance

From the Admin Corp ICS/OT cyber security team's earlier work in identifying requirements for the safety zone (IEC 62443 SL 2), it is clear that monitoring such as an Intrusion Detection System (IDS), malicious code protection, and network monitoring mechanisms is not currently available for the safety zone.

Additionally, as Admin Corp are an Operator of Essential Services (OES) under the NIS regulations, it is clear that the current architecture is insufficient in terms of logging and monitoring sources to meet the Cyber Assessment Framework (CAF) profile required by them currently by their regulator . The Admin Corp ICS/OT security team are not currently well positioned to minimise the impact of an attack, nor are they well positioned for the timely identification and reporting of an incident. The first few steps of the simplified CMF approach, which can be performed relatively quickly and without introducing risk into the ICS/OT environment, have provided the Admin Corp ICS/OT cyber security team with this perspective.

Reason 4 – Validation of Security Controls

The logs available from the VPN server could be used to validate the effectiveness of the authentication security control deployed at the perimeter of the environment. For example, the VPN logs could be reviewed to determine if there have been excessive numbers of failed login attempts, logins from unexpected source destinations, or activity residing in unauthenticated requests logs. Follow-on collection of Windows Event logs from jump-hosts or other assets in the DMZ could be an additional source of logs to validate that authentication security control. Centralised logging in SIEM of both sources is a clear improvement that is easily identified from this step. Another example for validation of security controls in this case could be making use of the logs from the Anti-virus solution to validate that new signatures are being successfully deployed to the AV server.

CMF Step 4: Overlay requirements to the CMF.

Taking the TTX requirements, the Admin Corp ICS/OT cyber security team map them on to the CMF, and using a quick qualitative scoring process, they can clearly see where improvements are required to detect and respond to the ransomware scenario used earlier, as shown in Table 2 and Table 3.

Please note that the colours of the cells in the tables note how the approach has improved the logging and monitoring capability in RAG method, with white showing no change.

Table 2: Admin Corp CMF updated with requirements for data storage/location/who has access overlayed with qualitative scoring applied.

Location / Zone	Asset Type	Data Type	ICS Kill chain phases	MITRE ATT&CK for ICS (Tactics)	Data storage duration	Data Storage Location	Access
PCS network	Historian	Windows Event Logs	Exploit / Install / Modify	Execution / Collection / Inhibit Response Function	7 days	Local	System engineer, local admin
	VPN	Authentication Logs	Exploit / Modify / Reconnaissance	Reconnaissance / Initial Access /	1 month	Local	Local admin
	Jump Server	Authentication Logs	Exploit / Modify / Reconnaissance	Reconnaissance / Initial Access /	1 month	Local	Local admin
	Firewall	Alerts	Delivery / C2	Initial Access / Collection/ C2	3 months	Enterprise SIEM	Enterprise cybersecurity team
	Network traffic	None	Delivery / C2 / Execute	Initial Access / Lateral Movement / Impact	None	None	N/A
	File server	Windows Event Logs	Delivery	Lateral Movement / Collection / Evasion	1 week	PCS security server	local admin

	Antivirus	Alerts	Delivery	Execution/ Persistence / Lateral Movement	1 month	Local (Operator Control Room)	local admin
Control Room	Operator workstation	Windows Event Logs	Exploit / Install / Modify	Execution / Persistence / Lateral Movement / Collection	1 month	Local	System engineer, local admin
	Control network	None	N/A	Execution / Persistence / Lateral Movement / Collection / Impact	N/A	N/A	N/A
	SCADA server	Application Logs	Actions on Objectives	Execution / Persistence / Lateral Movement / Collection / Impact	2 months	Local	System engineer, local admin
Safety Zone	PLC	None	Install/Modify / Execute (stage 2)	Impair / Process Control / Impact	N/A	N/A	N/A
	Network Traffic	None	Install/Modify / Execute (stage 2)	Impair / Process Control / Impact	N/A	N/A	N/A

Table 3: Admin Corp updated CMF with additional quick wins applied, overlayed with qualitative scoring.

Location / Zone	Asset Type	Data Type	ICS Kill chain phases	MITRE ATT&CK for ICS (Tactics)	Data storage duration	Data Storage Location	Access
PCS network	Historian	Windows Event Logs	Exploit / Install / Modify	Execution / Collection / Inhibit Response Function	30 days	Local & forwarded to dedicated ICS monitoring solution (once deployed)	System engineer, local admin, ICS/OT cyber security team
	VPN	Authentication Logs	Exploit / Modify / Reconnaissance	Reconnaissance / Initial Access /	3 months	Local & forwarded to Enterprise SIEM	Local admin, enterprise cyber security team
	Jump Server	Authentication Logs	Exploit / Modify / Reconnaissance	Reconnaissance / Initial Access /	1 month	Local & forwarded to Enterprise SIEM	Local admin, enterprise cyber security team
	Firewall	Alerts	Delivery / C2	Initial Access / Collection/ C2	6 months	Enterprise SIEM	Enterprise cyber security team
	PCS network with dedicated ICS passive network monitoring solution	Notifications	Delivery / C2 / Execute	Initial Access / Lateral Movement / Impact	12 months	(pending) Deployment of dedicated ICS passive security monitoring solution	ICS/OT cyber security team

	File server	Windows Event Logs	Delivery	Lateral Movement / Collection / Evasion	3 months	PCS security server & forwarded to dedicated ICS monitoring solution (once deployed)	local admin, ICS/OT cyber security team
	Antivirus	Alerts	Delivery	Execution / Persistence / Lateral Movement	3 months	Operator Control Room and Enterprise SIEM or 3rd party SOC services	local admin, Enterprise Cyber security team
Control Room	Operator workstation	Windows Event Logs	Exploit / Install / Modify	Execution / Persistence / Lateral Movement / Collection	3 months	PCS security server & forwarded to dedicated ICS monitoring solution (once deployed)	System engineer, local admin
	Control network with Dedicated ICS passive network monitoring solution	None	N/A	Execution / Persistence / Lateral Movement / Collection / Impact	12 months	(pending) Deployment of dedicated ICS passive security monitoring solution	N/A

	SCADA server	Application Logs	Actions on Objectives	Execution / Persistence / Lateral Movement / Collection / Impact	3 months	Operator Control Room and Enterprise SIEM	System engineer, local admin
Safety Zone	PLC	None	Install/Modify / Execute (stage 2)	Impair / Process Control / Impact	N/A	N/A	N/A
	Network Traffic with Dedicated ICS passive network monitoring solution	None	Install/Modify / Execute (stage 2)	Impair / Process Control / Impact	12 months	(pending) Deployment of dedicated ICS passive security monitoring solution	ICS/OT cyber security team

Figure 2 below provides an example of how the simplified CMF approach has quickly improved the security posture of Admin Corp. The examples show how the approach has led to increased capability to initiate response effort and the timely identification of an attack. In this example of preventing ransomware (the identified requirement from the TTX performed in step 1), the increased monitoring of initial access provides the Admin Corp ICS/OT cyber security team with a better ability to investigate user access to the ICS/OT environment.

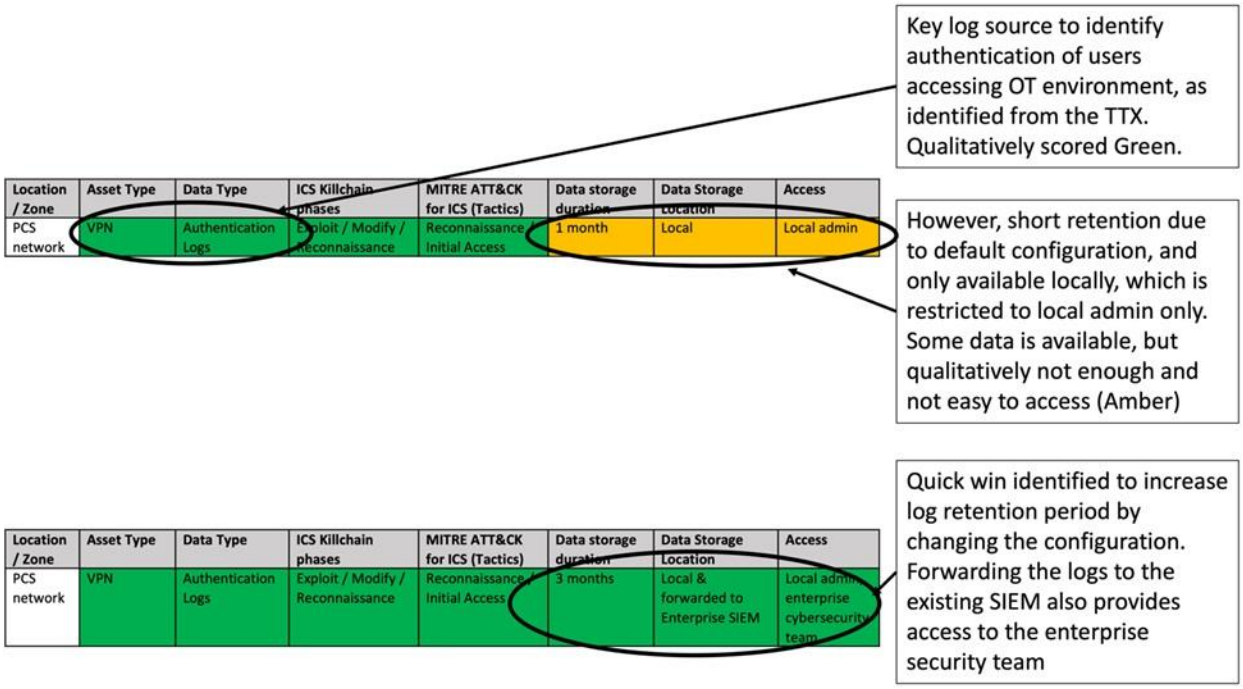

Figure 2: Identified requirements from the TTX performed included the ability to monitor and investigate user access to the OT environment.

Figure 3 below shows how the other requirements from threat modelling (also identified in step 1), have been used to identify required improvements to logging and monitoring to better position Admin Corp to detect and respond to the type of threats that are relevant to them and their identified crown jewel assets. This links back to the principle of logging and monitoring for priority and importance; prioritising what threats are most important for Admin Corp to defend against and what assets need to be prioritised for monitoring and logging.

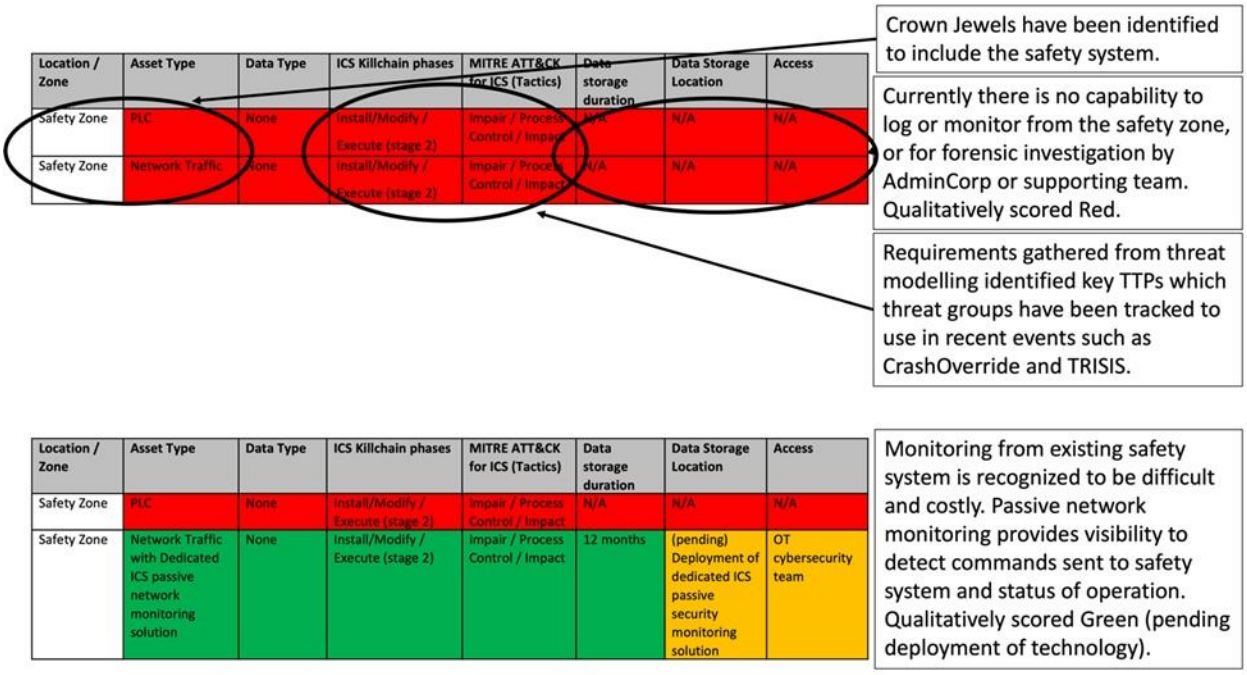

Figure 3: Identified requirements from Threat Modelling included the ability to detect threats based on relevant scenarios to Admin Corp.

Next Steps

By understanding what logging can be implemented easily, the Admin Corp ICS/OT cyber security team implement these measures quickly, and then commission a project to address the other requirements identified during the activity, specifically deployment of dedicated ICS/OT deep packet inspection passive monitoring solution, noting that this will require additional work to ensure it has the best visibility of the ICS/OT network. The team also then start a piece of work to understand "how" to undertake logging and monitoring of their ICS/OT environment.

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.

This document is provided on an information basis only, ICS-COI members and NCSC have used all reasonable care in verifying the guidance contained within using the data sources available to it, they provide no warranty as to its accuracy or completeness. To the fullest extent permitted by law, the NCSC and the ICS-COI accept no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the report or arising from any person acting, refraining from acting, relying upon or otherwise using this document. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances.

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer or otherwise, does not constitute or imply its endorsement, recommendation or favour by the ICS-COI or NCSC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.