INDUSTRIAL CONTROL SYSTEMS
Community of Interest

How to log in ICS/OT Environments - Meet Admin Corp

Introduction

In this "Admin Corp" example, we're going to walk through the design process for logging and monitoring in an Industrial Control System (ICS)/Operational Technology (OT) environment, guided all the way through by the principles described in the associated How to log in an ICS/OT environment guidance document**.** In this article we provide two different examples, one based on the **Collection Management Framework (CMF) approach**, and one based on the **Consequence Driven Engineered approach**. The CMF approach covers two further sub-examples, one focused **Security Appliance logging and monitoring**, the other on **network traffic logging and monitoring.**

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.

Identifying HOW to implement the monitoring from a Collection Management Framework Perspective

1st example – Security Appliances

How Admin Corp made use of the "How to log and monitor guidance", using the provided "Tips"

Using recommended practices for perimeter access control to ICS/OT environments, the Admin Corp architecture ensures that users accessing the OT environment are funnelled through a VPN gateway and require separate authentication from a jump-host located in the DMZ.

From the CMF analysis, Admin Corp had identified shortfalls in the logging and monitoring associated with the VPN solution; short retention period of logs and only available locally, as shown in Figure 1.

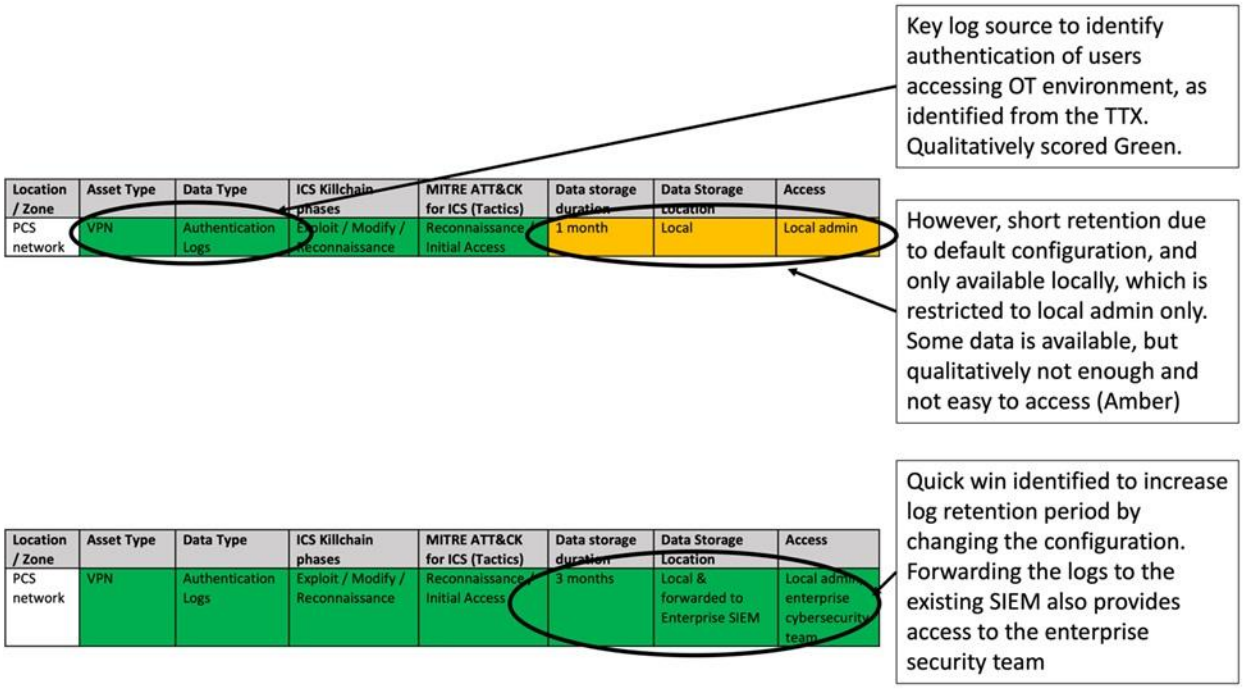

Figure 1: Logging and Monitoring gaps identified in VPN solution

Changing the logging and monitoring configuration on the VPN gateway (number 1 in figure 2 below) provides Admin Corp with a longer event horizon for user access to the ICS/OT environment. Extending the log visibility to the enterprise security team via log forwarding to the enterprise SIEM increases the monitoring coverage. Additional logging is also obtained from the jump server (number 4 in figure 2 below) to provide the cybersecurity team with additional sources of access attempts and authentication logs.

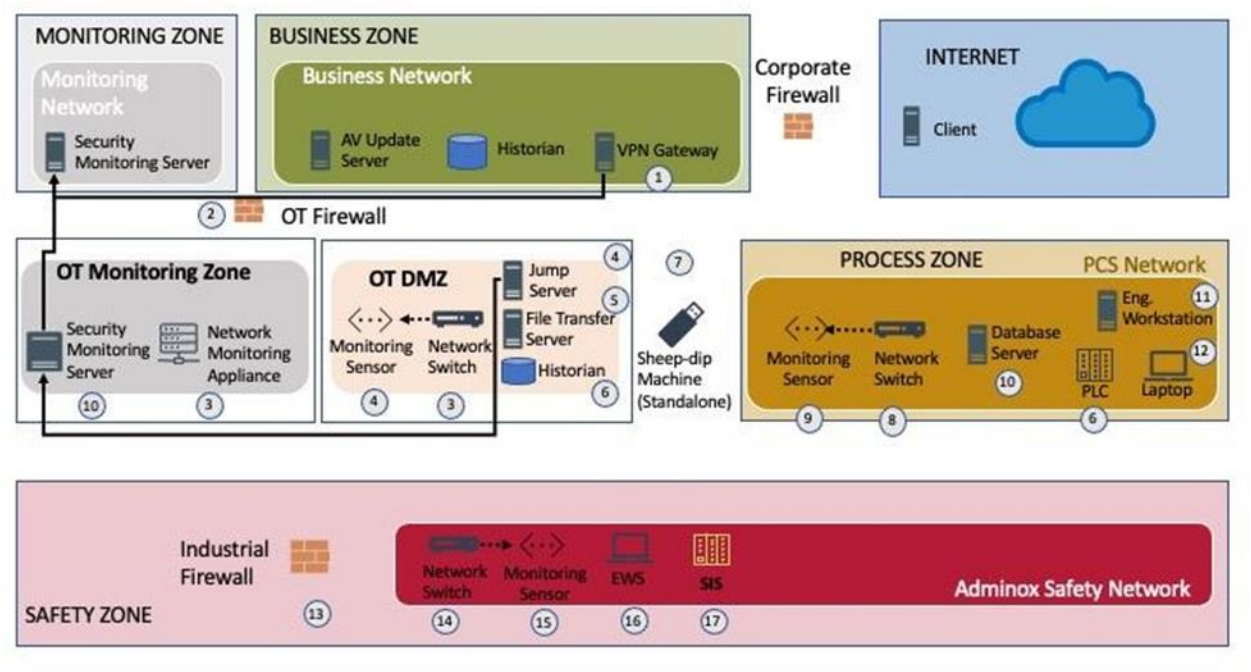

Figure 2: Admin Corp example – user access logging and monitoring

This enhancement to logging, also allows the enterprise security team to run reports on user access to the ICS/OT environment to ensure only authorised users and groups are attempting to access the ICS/OT environment. The improvement also provides the ability of the team to correlate user access to the ICS/OT environment using potentially compromised accounts from IT related compromises. A nice win for IT and ICS/OT team collaboration also.

How Admin Corp made use of the "How to log and monitor guidance", to avoid common pitfalls

The default configuration of the logging and monitoring of VPN sessions provided a short retention period, which didn't provide at least 3 months' worth of user access logs.

How this helps Admin Corp address the 4 key reasons for logging and monitoring

Threat Detection:

Although not directly improving the retention period, forwarding users access attempts and records for the ICS/OT environment to the enterprise SIEM allows for the Admin Corp security team to better detect threats associated with compromised IT credentials being used to attempt to access the ICS/OT environment. (The NCSC recommends using transport encryption where possible. The NCSC has not examined and does not endorse particular protocols, but common choices include Syslog, SNMP traps, and Windows Event Forwarding. When sending logs across trust boundaries, they should be sent across a one-way flow control (e.g. UDP or a unidirectional data diode) to make it harder for an attacker to modify stored logs.)

Incident Response Investigation:

Increasing the log retention period allows for Admin Corp to hunt and investigate with a longer event horizon, to be able to act on reports from known cyberattacks, such as those that began with zero days being used successfully on perimeter devices, or those that utilized credential harvesting campaigns targeting remote users.

Compliance:

Without the ability to monitor medium to long term user access to the environment, Admin Corp will be challenged to meet their requirements under NIS regulations to minimize the impact of an attack, by not being able to identify if known compromised accounts have been used to access the ICS/OT environment. This improvement in both log retention, additional logging and the feed into the Enterprise SIEM, helps Admin Corp achieve more CAF C1. Security monitoring IGPs.

Validation:

Validation of VPN and firewalls operation can now be performed by using the logs from the VPN server to identify if any unauthorized users have accessed the jump-host, or if there has been evidence of brute force attacks used to authenticate.

2nd example – Network (traffic) monitoring

Referring to their updated CMF earlier, the Admin Corp security team identified from the threat modelling exercise that they are lacking the ability to log or monitor from the safety zone. Additionally, they observe that they do not have the capability to detect adversary behaviour targeting the safety system, which is identified as a crown jewel for Admin Corp.

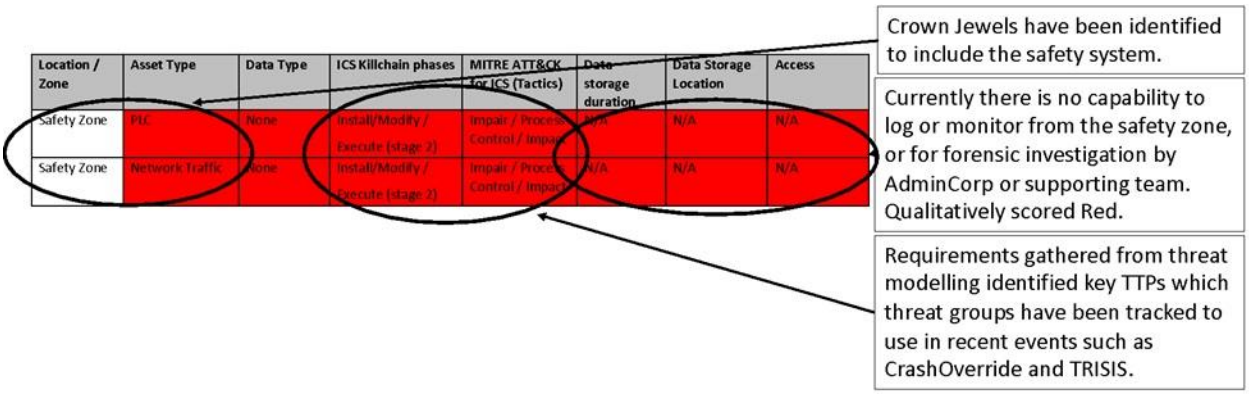

Figure 3: Example of Admin Corp identifying gaps in monitoring of priority systems

Monitoring of the existing safety system is recognized to be difficult due to safety case requirements and maintaining integrity of the systems.

Passive network monitoring in the safety zone provides the visibility to detect commands sent to safety system controllers, status of operation and ability to monitor for, and alert on, any file transfers into the zone or unauthorized user access. Given the logs are being sent across trust boundaries to the SIEM in the monitoring zone, they should be sent across a one-way flow control (e.g. UDP or a unidirectional data diode).

How Admin Corp made use of the "How to log and monitor guidance", using the provided "Tips"

The Admin Corp security team, identify locations from their network that would be suitable for collection of network traffic with minimal or no impact on operations, i.e., they identify switches that have the ability to be configured with span or mirror ports to mirror the traffic from across the switch ports as a preference over network taps.

Admin Corp then check and confirm that existing switches are not close to operating capacity.

Admin Corp then identify other monitoring locations requiring sensors (numbers 13 and 14 in figure 2), and location of monitoring server.

Admin Corp consider available solutions and ensure that the selected solution provides the ability to monitor for behaviour and signature-based threat detection, not just reliance on use of anomaly

detection. Admin Corp then take into consideration how threat intelligence feeds can be integrated into the solution to ensure up-to-date adversary behaviours can be detected, rather than reliance on IOCs alone.

The result is that Admin Corp deploy a sensor (number 15 in figure 2) to monitor traffic within the Safety Zone, by monitoring the traffic from a spare port on the switch (14) that is configured with SPAN / port mirroring. Sensors are also deployed within the DMZ and Process Zone (4, 9), to monitor traffic across the OT/ICS environment to provide visibility of potential malicious behaviour traversing the network and trying to reach the Safety Zone.

The solution is configured to connect to a dedicated monitoring appliance (number 3 in figure 2) located in a monitoring zone, where the metadata from the sensor will be forwarded for logging, analysis, correlation and providing analysts with a user interface to monitor, investigate and configure the threat detection solution. Firewalls, actually unidirectional diodes, are deployed to ensure that the monitoring sensor can forward metadata out of the process and safety zones via specific ports only, and the monitoring sensors utilise network interfaces configured as promiscuous ports such that they can listen to traffic from the network switches but cannot send data to the switch. Attention is also given to any bandwidth limitations that might impact on the ability to forward logs across the trust boundaries, however ideally bandwidth will be adequate or increased to facilitate appropriate logging and monitoring.

How Admin Corp made use of the "How to log and monitor guidance", to avoid common pitfalls

Selection of a monitoring solution to monitor the collected traffic requires Admin Corp to consider the requirements to monitor East-West traffic, not just North-South. Initial consideration was made to monitor the ingress and egress of the ICS/OT network by monitoring traffic across the DMZ (number 4 in figure 4 below).

However, Admin Corp realised that this would not provide the visibility of interaction with assets that can interact with controllers, such as PLCs, or being able to detect changes being made to control and protection equipment via ICS/OT protocols such as stop commands and logic downloads. Therefore, Admin Corp also deployed sensors (numbers 4 and 9 in figure 4 below) to passively monitor from other network switches across the environment (number 3 and 8 in figure 4 below).

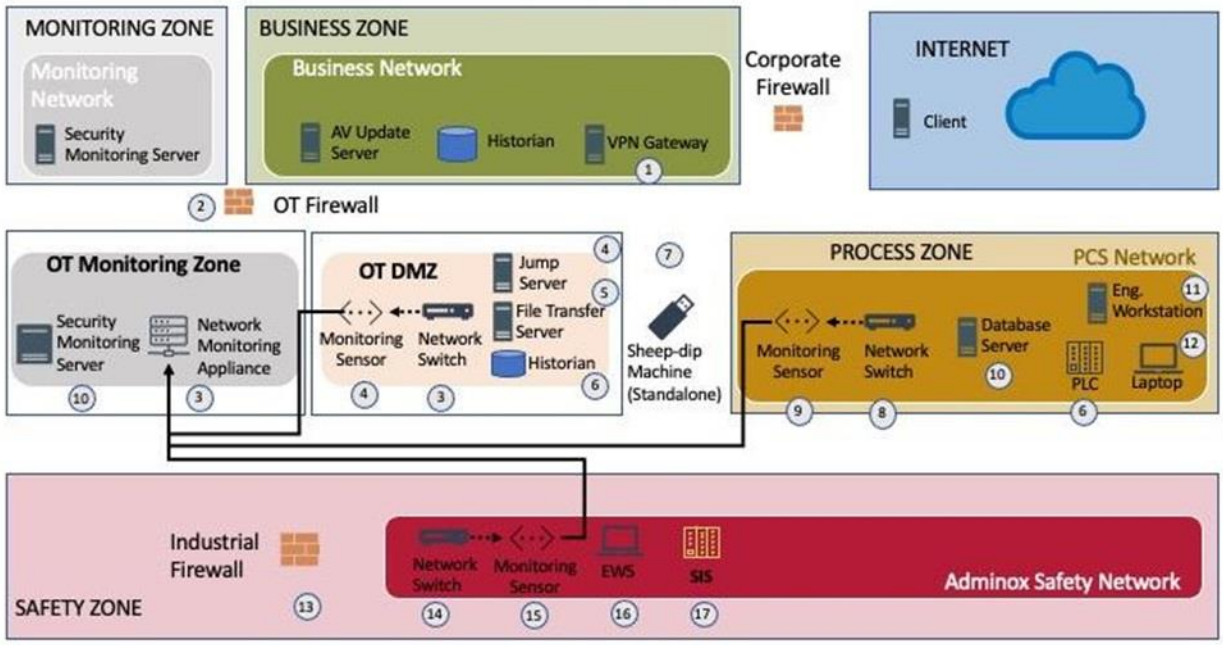

Figure 4: Admin Corp example of deploying passive network monitoring

How this helps Admin Corp address the 4 key reasons for logging and monitoring

Threat Detection:

An ICS/OT protocol aware network monitoring solution selection provides Admin Corp with the ability to detect threats.

Incident Response Investigation:

Visibility provided from network monitoring provides support to any incident response investigation by helping to identify relevant sources of forensic collection, i.e., which hosts are in scope for memory, disk, other artifact collection. Monitoring also provides ability for the Incident Response Team to validate effectiveness of any containment and eradication strategies later in the Incident Response lifecycle.

Compliance

Network monitoring provides Intrusion Detection System capability to the ICS/OT network, in particular the safety zone which has been identified to require compliance against the IEC62443 standard with the zone security level target (SL-T) to be 2.

Additionally, the Admin Corp team can then use the monitoring solution to help identify threats and act to contain them to minimize the impact to operations and the ability for timely reporting of identified incidents.

Validation

The selected network monitoring solution allows for Admin Corp to validate the effectiveness of the security controls in place for the perimeter of the safety network, by providing visibility of network connections, sessions, and file transfers into the safety zone.

Next Steps

Having undertaken this work, the Admin Corp Cyber Security Team are now looking to focus on ensuring they develop good practice to verify and secure the logs created within the ICS/OT monitoring zone, in addition to improvements on how they can be analysed and cross referenced with other source data to improve the end to end understanding of the logs.

Identifying HOW to implement the monitoring from a Consequence Driven Engineered Approach.

Table 1: Consequence drive engineered 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 (Media Validation Station)	Malware Detected	Application Logs	SIEM	6 Months	Lateral Movement		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		High	Local	Prevent connection of laptop to controller
Laptop_01	Compromised firmware detected	Application Logs	Local	6 Months	Lateral Movement		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

Using the data collection schedule in table 1 the requirement to forward selected log information from the Media Validation Station (MVS) (number 7 in figure 5 below) to the Security Monitoring Server (number 18 in figure 5 below) in the ICS/OT Monitoring Zone was identified. Recognising the stand-alone nature of the MVS, the Admin Corp cyber security engineers decided to use UDP based Syslog to forward the logs generated by the station associated with:

- Malware Detected
- Files written to media (with media ID)
- User Authentication details

via a simple unidirectional gateway/diode, to the Security Monitoring Server (number 18 in figure 15 below).

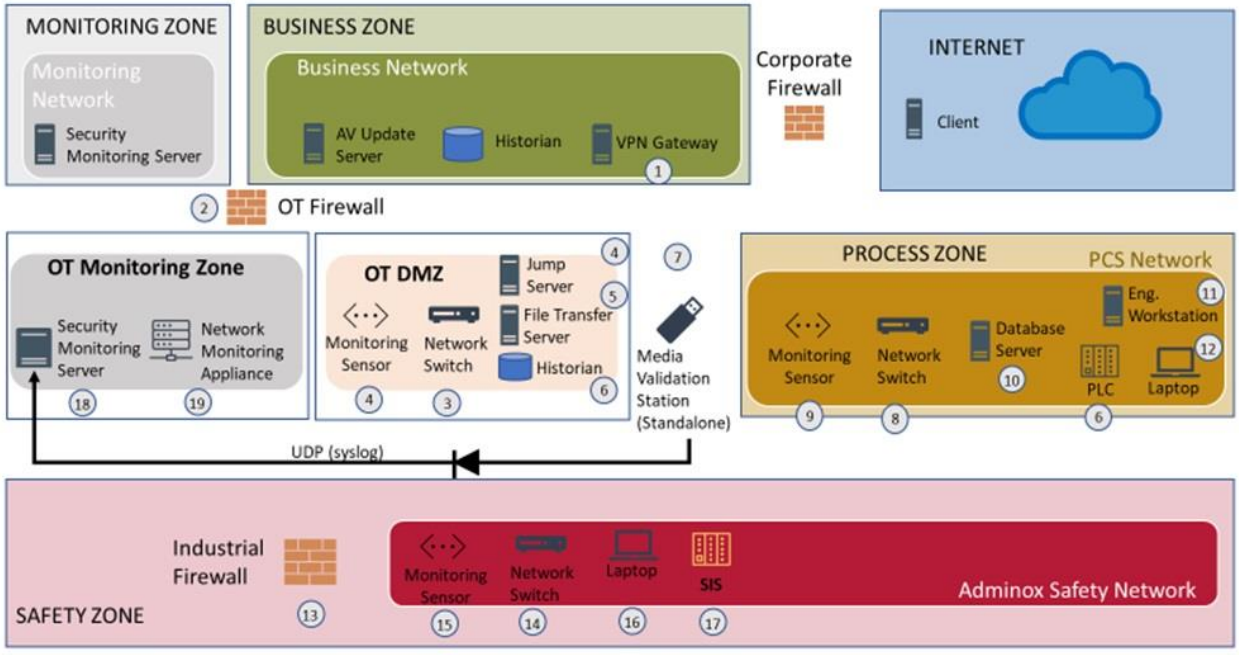

Figure 5: Admin Corp example of deploying logging and monitoring of Media Validation Station

Alert rules were then configured within the Security Monitoring Server to provide an alert in the event of the MVS detecting malware, with the additional information identified in the table below also being stored to support investigations as part of the incident response process.

Table 2: Kill Chain (With TTPs) focused logging and monitoring

Diagram Ref.	Asset ID	Information	Data Source	ICS Killchain Phase(s)	Mitre TTP	Action Enabled
7	MVS_01	Malware Detected	Application Logs	Lateral Movement		Prevent connection of laptop to controller

16	Laptop_01	Compromised code detected	Application Logs	Lateral Movement		Prevent connection of laptop to controller
16	Laptop_01	Compromised firmware detected	Application Logs	Lateral Movement		Prevent connection of laptop to controller
17	SIS_01	Compromised code detected		Impair Process Control	T0833	Suspend Operations
17	SIS_01	Compromised firmware detected		Impair Process Control	T0857	Suspend Operations

Next Steps

Specific response instructions were also prepared to identify the steps to be undertaken in response to the specified alerts to ensure that the desired action (prevent connection of laptop to controller) was able to be undertaken in sufficient time to prevent realisation of any unacceptable consequence.

Tests were also developed to demonstrate the correct operation of the configured alerts and allow ongoing operational assurance, with prompts configured within the Admin Corp Maintenance Management System to ensure the tests were undertaken at an appropriate periodicity.

Given the independent nature of the laptop (number 16 in figure 5 above), it was decided to implement the associated monitoring aspects through routine, periodic reviews of the device logs. Prompts were configured within the Admin Corp Maintenance Management System to drive the implementation of this activity, and allow for the recording of the results. Response instructions were also prepared identifying the steps to be taken should any suspicious activity be detected during these reviews, again preventing the connection of the laptop to the SIS controller.

As no automated method of detecting a compromise of the code, or firmware, within the SIS (number 17 in figure 5 above) it was again decided to implement the required monitoring activities through the periodic review of the SIS code (through comparison with the master copy of the code) and its firmware (using a checksum method). Prompts were configured within the Admin Corp Maintenance Management System to drive the implementation of this activity, and allow for the recording of the results. Response instructions were also prepared identifying the steps to be taken should any suspicious activity be detected during these reviews, potentially suspending process operations.

The Admin Corp Security team also recognise that further effort is required to fine tune the alerting on the logging being provided, with effort to understand any weird alerts, in addition to those suspected as being malicious. They also note that should further changes be made to the ICS/OT process or safety zones, that a baselining and review activity would be needed, to ensure that the decisions and capability deployed for security monitoring currently is still best practice.

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.