INDUSTRIAL CONTROL SYSTEMS
Community of Interest

GUIDANCE: WHY YOU NEED TO UNDERTAKE CYBER SECURITY LOGGING AND MONITORING IN AN INDUSTRIAL CONTROL SYSTEM / OPERATIONAL TECHNOLOGY ENVIRONMENT.

Why use logging and monitoring in ICS/OT?

Understanding why it's important to use logging and monitoring in Industrial Control Systems (ICS)/ Operational Technology (OT) systems helps organisations define objectives and success criteria when putting in place new solutions, or when improving existing ones. This is particularly important for ICS/OT systems, which historically haven't been designed or required to support security logging and monitoring.

Logging and monitoring capabilities in ICS/OT environments have improved significantly in recent years, and there are now many products specifically designed for ICS/OT assets and networks. Setting clear objectives about what you want to achieve helps your organisation choose, configure and put in place the right logging and monitoring solutions.

Organisations should apply the principles described in this section when setting logging and monitoring objectives.

Principles

An outcome-based approach

The NCSC's principle-based IT logging and monitoring guidance states that organisations should 'understand objectives for logging and monitoring'. It's now widely recognised in IT security that monitoring is essential for defence in depth, and recent work in the regulatory environment indicates this is also true for ICS/OT security. Your objectives should clearly explain *why* logging and monitoring is necessary.

In an ICS/OT environment, the ICS/OT automation and safety systems will almost certainly be delivering or facilitating the core functions of the business, such as production, operation or

transport. Effective logging and monitoring therefore allows ICS/OT owners and operators to better protect their core business functions and understand when security that they rely upon is not functioning as expected. Logging and monitoring requirements should therefore be in line with your organisation's overall desired business outcomes.

If the ICS/OT environment is in a regulated sector, and the ICS/OT owner or operator is subject to NIS Regulations 2018, having effective logging and monitoring meets the CAF IGPs under C1. Security Monitoring Principle and is considered a valid outcome.

Other typical outcomes of logging and monitoring include:

- allowing **response initiation** in sufficient time to prevent any unacceptable consequences
- providing **timely identification** of an attack and allowing onward reporting
- **protection capabilities** to confirm they are performing as required
- to **identify that an attack** has taken place and assist in the response
- to facilitate a **baseline understanding** of 'normal' behaviour which can also support business, process and functional improvements

Priority and importance

For an outcome-based approach, it's important to have a clear understanding of the asset base, the relative importance of the different assets and how they support the overall business objectives. Assets with the most impact on the key business functions can be considered the 'crown jewels' in a system. Further detail to understand what the term asset refers to in the ICS/OT context can be found in this ICS/OT Asset Management guidance article.

Developing a clear understanding how these assets map to key unacceptable consequences (including providing an essential service) allows organisations to prioritise security controls for the most important system elements.

Organisations also have finite resources. Setting clear objectives at the start allows logging and monitoring to align to the resources available in your organisation, from design all the way through to operation.

You can prioritise resource requirements and tailor them to the risk appetite in your organisation.

Defence in depth

Linking back to NCSC's 'what is OT malware?', the compromise of ICS/OT systems ('cyber-physical' attacks) can result in unacceptable consequences, ranging from minor business disruption or environmental impact to physical destruction, loss of vital societal functions or industrial espionage. As outlined in many security frameworks and standards, a defence-in-depth approach which includes detection, response and recovery, as well as protection, provides the most effective way of mitigating unacceptable consequences.

The use of monitoring and logging is essential to overall defence in depth because for each security control an organisation uses to mitigate a particular risk, it should be assumed that a threat actor can circumvent this control or some other failure can happen. To provide defence in depth, a logging and monitoring system must detect any control failures as early as possible, so an organisation can take appropriate action. If logging and monitoring isn't in place, threat actors

could breach an organisation's network and achieve their objectives, before your organisation is aware of it. Or worse, your organisation may never know.

For example, logging and monitoring firewall logs, even from a well-configured, stateful firewall, may not be enough to detect and respond to a malicious actor that has gained access by compromising VPN credentials. In this scenario, another layer of defence could therefore be required for greater protection. This might be an intrusion detection system (IDS) which identifies anomalous traffic patterns, or monitoring user activity against accepted 'normal' behaviours to identify anomalous activity resulting from the presence of a threat actor. Security Operation Centre's (either run by the operator or provided by a external service provider) can provide a level of assurance on monitoring what is logged within an ICS/OT environment. NCSC has guidance on what considerations should be taken into account when building or selecting a SOC.

Determine the reasons

A good summary of the benefits of general logging and monitoring for your organisation taken from the NCSC's logging and monitoring guidance for IT are that it offers:

- the ability to understand, trace and react to system and security events
- an insight into systems, and active detection of threats and potential security incidents
- an additional layer of defence to systems
- an opportunity to react to early signs of compromise, meaning organisations can respond effectively

To develop these points further, the four reasons below explain why logging and monitoring should be carried out in ICS/OT environments:

Threat detection

Logging and monitoring is the basis for detecting threats, anomalies or events in any digital environment.

Incident response (IR) investigations

Determining root cause is key for incident responders to determine what has happened and how it occurred. Root cause analysis relies on collection and analysis of forensic artefacts obtained from host and network assets, and the log files they generate. The Dragos year in review for 2020 highlighted that many ICS/OT environments don't carry out centralised and automated logging from hosts and network sources, significantly slowing down the IR process.

Compliance

Obtaining and maintaining compliance with relevant regulation and standards requires ICS/OT owners and operators to perform adequate monitoring and logging, such as compliance with IEC 62443 and NIST CSF. As recognised good practice, along with the NCSC Cyber Assessment Framework (CAF), those standards identify requirements for monitoring OT, and providing forensics to support investigations if an incident occurs.

As recognised good practice, UK regulators expect organisations to apply these standards and therefore put in place an appropriate monitoring and logging capability (such as OG-0086, ONR Security Assessment Principles (SyAPs).

A requirement under NIS legislation is that an operator of essential services (OES) must '*take appropriate and proportionate measures to prevent and minimise the impact of incidents*'. The duty in this legislation to notify if an incident occurs requires an organisation to be able to detect and determine incidents.

But it's worth remembering that being compliant with standards does not necessarily guarantee a system is free of vulnerabilities that could lead to cyber security incidents.

Validating security controls

This means confirming independently that 'protect' measures are delivering their required security function. Although this often happens when red teams are tasked to conduct penetration testing, assurance testing or exercising, logging and monitoring can detect when controls have failed, are incorrectly implemented or when actions previously not thought possible have taken place (such as unexpected traffic flows between ICS/OT devices, despite control measures in place to enforce no connectivity).

It's sometimes difficult to see exactly how a principle should be applied. In the example below, we'll consider the design process for monitoring and logging in an ICS/OT system, guided by the principles described in the **Principles** section.

In this example, we'll use a fictional case study of the organisation 'Admin Corp'.

Applying the above principles to Admin Corp

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

Having followed the NCSC's secure design principles, the security architecture includes logging made easy (LME) in the business environment, and 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 restrict user activity to agreed policies, with network and host detection rules applied across the network of ICS/OT assets.

Admin Corp follows ICS/OT cyber security management principles, and one aspect of this is managing risk to understand the current risk levels in its ICS/OT systems. Following some high-profile cyber incidents (SolarWinds and Colonial pipeline), Admin Corp has conducted a risk assessment to assess its security posture, especially for its detection and response capabilities. It has followed the processes for conducting an ICS/OT cyber security risk assessment as per ISA/IEC 62443-3-2.

This has highlighted several areas of risk where logging and monitoring could potentially provide useful mitigation of these risks.

Admin Corp is therefore looking to apply the principles as described above.

Outcome-based approach

Firstly, for an **outcome-based approach**, Admin Corp establishes a set of outcome-focused objectives to support the safe production of Adminox, putting in place monitoring to:

- allow for **initiation of response effort,** with sufficient time to prevent an unacceptable consequence
- reduce the **impact to the local environment** in the event of an unsafe release of Adminox
- ensure **production and availability** of Adminox is maintained for customers (and therefore reducing impact on profitability for Admin Corp)
- provide **timely indication of an attack** and allow onward reporting (within 72 hours to the competent authority for 'significant' or 'substantial' incidents)

Priority and importance

Secondly, when considering **priority and importance**, Admin Corp understands that it won't be feasible to monitor and log everything in its asset inventory. It is therefore looking to understand the priority and importance of assets in its facility, and use the methodologies below to gain a clear understanding of the assets that could most impact its key business functions. Examples of methodologies that Admin Corp uses for this exercise are:

- Crown jewels analysis (CJA)
- Cyber security performance hazard analysis (PHA).
- Consequence-driven cyber-informed engineering (CCE)
- Existing business impact assessments (BIA)

Defence in depth

Thirdly, for **defence in depth**, Admin Corp understands that threat actors can circumvent deployed security controls, such as the VPN gateway, and so is looking to implement monitoring of these controls to provide an additional layer of security.

Admin Corp has applied the above four outcome-based objectives to its environment.

Threat detection

Admin Corp is aware of historical and recent cyber attacks on ICS/OT networks. It has observed the lessons learned from the Ukrainian Power Grid attack, and is aware of tactics used by adversaries, such as credential theft, VPN access and workstation remote access. It is familiar with the steps in the ICS killchain to detect adversary activity. Admin Corp is also part of the NCSC industry Information Exchange (IE) for its sector, which alerts to sector-specific threats.

Having set a monitoring outcome that allows a response effort in sufficient time to prevent an unacceptable consequence, Admin Corp is now looking to monitor its ICS/OT environment for anomalies and events that might indicate either a malicious actor's presence on the network, or an attempt to gain access to or interfere with its production facility. This threat detection capability complements other sources of event discovery, such as reports of suspicious behaviour by users, notifications of breaches from vendors or commercial and NCSC threat information alerts.

IR investigation

When investigating anomalous activity or after detecting a threat, Admin Corp initiates its pre-prepared cyber incident response process, following an agreed playbook of actions including:

- capturing and analysing data
- containing and mitigating the threat
- remediating and eradicating the threat
- recovering data and systems, if needed
- conducting a post-incident review and report

Admin Corp understands the need for root cause analysis to determine what has happened and how it occurred. As root cause analysis relies on collection and analysis of forensic artefacts obtained from host and network assets and the log files they generate, Admin Corp will need to understand what data sets are available from its assets, and how to obtain them for an IR investigation.

Admin Corp is also aware of recent cyber incidents which required asset owners to carry out retrospective investigation to determine a compromise. For example, in response to the Solarwinds incident, log collection and retention for DNS query and response would quickly determine if an entity has been attacked, and if it has, whether the malicious actor has proceeded to the next stage. Without DNS logs, the response time and effort is substantially greater because analysing multiple host-based artefacts would be required to identify malicious actor activity.

Finally, a cyber insurance policy requires Admin Corp to collect and handle forensic evidence as part of a formal IR process.

Compliance

Admin Corp is an operator of essential services (OES) under the NIS regulations, which requires them to take appropriate and proportionate security measures to manage risks to their network and information systems, and to notify serious incidents to the relevant national authority.

The NCSC's CAF has multiple areas where monitoring and logging are indicators of good practice (IGP) which Admin Corp wishes to put in place. They are:

- B2.c Privileged User Management – close monitoring of the higher privileged accounts in your system
- B4.a Secure by Design – designing systems that allow effective monitoring
- C1.a Monitoring Coverage – providing sufficient monitoring to detect security events
- C1.b Securing Logs – monitoring of access to log data
- C1.c Generating Alerts – ability to use the information from logging and monitoring
- C1.e Monitoring Tools and Skills – having the right expertise and tools in your environment.

Having performed a risk assessment for one of Admin Corp's safety instrumented systems (SIS) and assigned security level 2 (SL2) to the system under consideration (SuC), the IEC 62443 standard provides requirements for Admin Corp to implement, which includes continuous monitoring. This could include via an intrusion detection system (IDS), malicious code protection and network-monitoring mechanisms.

Validating security controls

The final reason Admin Corp is looking to implement logging and monitoring, is to provide a mechanism that validates the effectiveness of its implemented protection measures. These validation mechanisms could include, but should not be limited to:

- using network monitoring to confirm a firewall isn't allowing unexpected traffic
- using logging and monitoring to inform purple team exercises and support penetration testing
- validating integrity changes identified across the network against configuration management databases (CMDB) activity

Next steps

Having carried out these steps, Admin Corp believes it now has appropriate risk mitigations in place to defend against both deliberate acts of cyber intrusion and malware infections that might impact the production process.

The next steps are to ensure there are iterative improvement processes in place to initiate improvements from any events which could impact Admin Corp's availability and safety requirements.

As an operator of critical national infrastructure (CNI), Admin Corp ensures that it continues to manage the Adminox process safely and effectively by joining the NCSC's CISP platform and maintaining a relationship with the NCSC private sector CNI team.

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.