INDUSTRIAL CONTROL SYSTEMS
Community of Interest

GUIDANCE: How to log and monitor in an Industrial Control System / Operational Technology Environment

Introduction

This article provides guidance and considerations for CNI operators when implementing logging and monitoring within their Industrial Control System (ICS)/Operational Technology (OT) environment. It is part of a series of articles to help operators undertake better logging and monitoring within their ICS/OT environments. Each of the categories listed in this article are intended to capture the majority of logging and monitoring sources (note this is not designed to be exhaustive) which are typically available within ICS/OT networks including legacy environments. The categories are structured as:

- Network traffic.
- Devices
    - Host
        - Engineering Workstations
    - Applications
        - SCADA
        - Databases
        - Historian
        - PLC applications
- Security appliances
- Remote Access Solutions
- Other sources
    - Operator & maintenance logs
    - Diagnostics and condition monitoring

Each category is provided with recommended practices, common pitfalls and general tips and guidance for operators and architects to consider once they have established the scope of monitoring using the methodologies provided in the previous section.

This article is intentionally focused on providing the guidance for **how** to monitor and log from ICS/OT assets. For monitoring and logging guidance on assets which do not have any specific ICS/OT requirements, readers are recommended to consider existing guidance available for those IT assets which can be found in ICS/OT environments. For example, proxy servers and domain controllers are not listed here, however are assets that should be monitored using existing guidance such as the following from:

- NCSC - Logging and protective Monitoring
- NIST - Cybersecurity Log Management Planning Guide
- CREST -Cyber Security Monitoring Guide

System-wide considerations

Accurate time stamping of all logging and monitoring sources is required to allow for the correlation of data from multiple devices. It is strongly recommended to ensure that log sources are accurately timestamped. For ICS/OT environments this is particularly important due to the presence of legacy systems many of which do not typically use common Network Time Protocol (NTP) sources and therefore can have significant clock skew from other systems.

For ICS/OT systems it is also important to avoid inadequate separation of the NTP and plant data (i.e., failure to apply the zone/conduit approach from IEC62443), which can present additional attack paths into the plant environment.

Network

Introduction

Passive network monitoring is lower risk than active monitoring because it doesn't require deployment of agents or configuration changes for OT assets, however it may still require configuration changes to network assets. Collecting traffic from mirror or span ports still requires significant consideration, such as the existing capacity of switches, the type of switches in use, and how to route captured traffic to a monitoring solution (further detail on Asset Visibility methods can be found in this ICS COI guidance article).

Tips

- Be aware of the type of network traffic that is required to be monitored, as this will determine where to capture traffic from. For example, monitoring East-West traffic may require collection from different switches, or different span/mirror configurations compared to North-South traffic.
- Check maximum switch traffic capacity prior to selecting SPAN/mirror ports to avoid over burdening the switch or causing dropped packets from the SPAN/mirror ports resulting in the monitoring solution missing key events during times of heavy network load.
- Taps can be retro fitted to legacy environments, though they will require a degree of downtime.
- Be aware that not all legacy switches have SPAN/mirror capabilities and may need replacing or upgrading before monitoring can be performed.
- It is recommended to use a combination of SPAN/mirror Ports.
- Aggregation devices can be used to consolidate the data into a single stream before feeding into the network monitoring solution, either for simplifying the maintenance of the solution, or overcoming limitations of network monitoring solution hardware such as number of input monitoring ports.
- Evaluate network monitoring solutions to ensure that file inspection can be performed using the likes of YARA signatures or alternatives.
- Consider the lists provided in Appendix A – Consolidated List of Indicators for network anomalies and exceptions to monitor for within any selected network monitoring solution.
- Environments with unmanaged switches can prove troublesome to obtain adequate monitoring. In these cases, it can be worthwhile to use configuration suites on engineering workstations to browse the network to generate traffic that enables further asset discovery and help scope additional monitoring locations.
- Some environments can support RSPAN (Remote SPAN) and/or ERSPAN (Encapsulated Remote SPAN) which means multiple switches can be monitored from a single switch e.g., a Core switch. This provides some consolidation and may require fewer monitoring devices but can increase network loading and complexity.

Common pitfalls

- Selection of ICS/OT protocol aware solutions but placement of appliances only monitoring North-South traffic or ICS/OT boundary traffic, and therefore missing the monitoring of East-West traffic which could include configuration of controllers, commands being sent to controllers, interaction with engineering workstations etc.
- Misconfiguration of SPAN/mirror ports can lead to monitoring solutions only "seeing" broadcast traffic, rather than unicast traffic and session monitoring.
- Inadequate segmentation and segregation of the monitoring and plant data (i.e., failure to apply the zone/conduit approach from IEC62443) can present additional attack paths into the plant environment.
- Anomaly detection systems are selected but become a source of false positives due to the extensive tuning required to be effective.
- Anomaly detection systems are relied upon that have an insufficient window of analysis and therefore do not detect abnormalities across relatively static networks, as are commonly found in ICS/OT environments.
- It is common for communications or activities within ICS/OT environments to be scheduled e.g., batch manufacturing, scheduled backups, etc. If monitoring is not being performed at the right place at the right time it can result in missing key activities and connections.
- Many ICS/OT environments are flat networks, either by design or due to legacy reasons. These networks can make monitoring particularly challenging due to the amount of noise created by enterprise assets and connectivity across multiple sites and countries.
- Environments are established with monitoring, but the monitoring is lost when containment/isolation is performed, or the security team's access to the monitoring platform and/or analytics is lost.
- Logging and Monitoring solutions are turned off during maintenance periods which can be the period of most risk of introduction of Malware.
- The need to log/monitor data import/export on removable media.

Reference guidance documents & further reading

- NIST SP 800-82 Rev. 3 Guide to Industrial Control Systems (ICS) Security

Devices

Host

Introduction

ICS/OT environments often utilise numerous devices that host Operating Systems (OS) and Realtime Operating Systems (RTOS). Examples of commonly used devices within the ICS/OT network are Programmable Logic Control's (PLCs), Historian servers, Engineering Workstations, application servers and HMI servers. Such systems often run a version of Microsoft Windows or Linux operating system either directly on the hardware or as a virtualised environment.

Endpoint Detection Response (EDR) solutions are not commonly deployed across entire ICS/OT networks due to their "ability to control devices" inside the ICS/OT network, and EDR management architectures conflicting with segregation/segmentation policies. This takes importance when the management endpoints of such EDR solutions are in lower trust zones in either cloud hosted or outside of the ICS/OT network. in addition, some EDR solutions typically require some connectivity back to cloud services for real-time signature checks as well (this may be acceptable but in a lot of ICS/OT environments at the lower Purdue layers, this is not, due to segregation/segmentation policies).

Where they are found is typically higher up in the levels of the Purdue model. However, logging from ICS/OT endpoints such as workstations, PLCs and controllers using solutions such as log forwarding can provide valuable sources of logging and monitoring. Logs can be forwarded to a SIEM or to a dedicated ICS/OT monitoring solution that has host log ingestion capability.

Tips

Configuration of Windows Event logs (please note this is not deemed an exhaustive list but is intended to provide a starting point with understanding):

- Event logs
    - Windows event logs can provide good coverage to detect potentially malicious activity, however they do require some careful configuration to avoid creation of large amounts of unnecessary logs. Additionally, they are susceptible to anti-forensic techniques and can therefore be deleted by malicious actors. Nevertheless, the following Windows Event Logs should be considered when filtering which logs to collect:
        - Clearing of audit log (Port 1102)
        - Account log on/off and failures (Ports 4624, 4634, 4648, 4634, 4672, 4688)
        - Service installed (Port 4697)
        - Scheduled task changes (Ports 4698 – 470)
    - Further detail on suggested minimum logging configuration is provided in "Appendix A Minimum recommended audit policy" of the "Microsoft guide for using Windows Event Forwarding to help with intrusion detection".
    - Additionally, it is recommended to consider configuration of Event Log to enable Process Creation events via GPO:
        - Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Detailed Tracking >> "Audit Process Creation" with "Success" selected.
    - The default event log file size is 20MB, therefore it is recommended to increase this size to ensure logging coverage is increased depending on your requirements.
- Sysmon
    - Sysmon is a flexible monitor for Windows machines that was developed by the Microsoft acquired team SysInternals. As such, it is a vetted, approved, and signed Windows binary. This is often useful in assessing if the binary can be installed on a Windows workstation or server in an ICS/OT environment.
    - Swift-On-Security has provided a well referenced and respected configuration for Sysmon configuration that is easy to setup and tune.
- PowerShell and scripting monitoring
    - As seen from the 2016 Ukraine attack, adversaries have demonstrated their capability to use relatively simple scripting and PowerShell without being detected in ICS/OT environments.
    - Changes to default Local Device Policy can facilitate for additional logging coverage for scripting and command line usage.
    - Windows 10 does not require any updates to support enhanced PowerShell logging, however for Windows 7, 8.1, Server 2008 and Server 2012 require upgrading PowerShell to 5.0 to enable enhanced logging. (It is important though to realise the risk of running legacy/End of Life software, and efforts should be focused on

updating to the latest version). Various options are available to increase logging coverage including:

- Enabling Module logging
- Enabling PowerShell Script Block Logging

- Windows host log forwarding options for ICS/OT environments are well described in the SANS Whitepaper “*Gaining Endpoint Log Visibility in ICS environments”.* The options for ICS/OT environments usually consist of the following:
    - WMI
        - Legacy Windows systems (pre-Vista and Server 2008) can be configured to use Windows Management Instrumentation (WMI) to pull logs from legacy Windows assets.
    - WEF
        - Windows hosts can be configured with Windows Event Forwarding (WEF) to push logs to a dedicated server operating as a Windows Event Collector (WEC). The configuration on the endpoints can be performed without requiring rebooting, and the event log subscription can be tailored and targeted if bandwidth and resources are limited.
        - Windows Event Collector (WEC) can be used to forward logs from within ICS/OT zones out to dedicated monitoring zones, and multiple WEC servers can be chained together.
- Agent based.
    - NXLog and Elastic Beats are examples of agent-based log collection and forwarding solutions. These clients are available for Windows Hosts and *nix based platforms and are configurable to collect and forward specific logs.
    - Commercial Security information and event management (SIEM) solutions commonly provide SIEM agents to deploy on hosts that forward logs to a SIEM indexer.
- Linux, in this guidance document is regarded as GNU Linux without additional services or patches.
    - Linux includes a large selection of built in tools that enable users and administrators to gain an understanding of all the software layers from machine boot state.
    - Linux System Activity:
        - dmesg command provides a view on messages that Linux/Unix kernel generates from the working of hardware and driver messages.
        - Any changes in the hardware are sent as messages to the kernel ring buffer.
        - The ring buffer messages are logged only following boot and starting of the syslogd or klogd daemons. Therefore, boot time logs can only be seen in dmesg. Note that the ring buffer size needs to be specified to provide adequate insight into the working of the system during boot.
        - As an example, connecting a USB drive (or virtual connections), which aligns to MITRE ATT&CK “initial access” and “collection” tactics, can be seen in the dmesg output.

- ps (and up) commands provide a view on current processes, resource usage, initiating command etc. This level of information is not logged but will provide a snapshot of the current state of the system.
- Although a system user should be familiar enough to identify abnormal processes and activities, auxiliary applications and custom scripts can provide alerts.
- The audit daemon, or auditD, is a Linux kernel feature that logs various actions such as systems calls, file opening, killing a process or creating a new network connection

- Linux Global System Logs:
  - rsyslog service (not part of Linux Core) can be started and configured via systemctl utility to capture and log Global system logs to disk.
  - Linux stores its log files under /var/log. Common log files recommended for review are:
    - /var/log/syslog – Debian-based Linux such as Ubuntu stores its global system activity data in this file.
    - /var/log/messages – Red Hat-based systems such as CentOS stores its global system activity data in this file.
    - /var/log/cron.log - Contains records of the cron jobs that are configured on the system, for user commands and scripts designated to run at specific times.
- Linux Login Activities:
  - Linux stores logs pertaining to log in activities into a number of log files depending on type of events and the Linux type and capabilities. These logs contain system authorisation information, user login attempts, authentication and authorisation data.
    - /var/log/auth.log – Debian-based Linux such as Ubuntu stores its login activity data in this file.
    - /var/log/secure – Red Hat-based systems such as CentOS stores its login activity data in this file.
  - As an example, these logs would contain SSH daemon logs that would aid identification of MITRE ATT&CK “initial access” and “Lateral Movement” tactics in play.
- Commercial or Open-Source applications such as rsyslog, Logstash and greylog can be utilised to aggregate logs across Linux systems and transmit them to a central platform for storage and analysis.

- If log forwarding is not feasible, it is still recommended to detail in a Collection Management Framework document what logs can be obtained from a host manually, to facilitate threat hunting and incident response investigations.

Common pitfalls

- Poor configuration or lack of configuration (i.e., event log filtering) can lead to excessive log creation and forwarding, taking up valuable network bandwidth and storage space.

- Using DCOM as the transfer mechanism for WMI may require large port ranges to be open on firewalls and may also require deployment of firewalls which are capable of understanding the DCE-RPC protocol.

Reference guidance documents & further reading

- Sysmon configuration guide from Swift on Security
- Gaining Endpoint Log Visibility in ICS environment

Applications

In some instances it not possible to integrate logs from typical process control ICS/OT applications (Supervisory Control and Data Acquisition (SCADA) systems, Historians etc.) directly into monitoring solutions. In some instances, it may be possible to forward events (e.g., from a SCADA) via Syslog into another platform, other attributes (e.g., historical process data) are often in a format that isn't compatible with typical monitoring solutions.

This often results in access to the required information only being available by accessing the application itself, as part of the incident response. Dedicated accounts, allowing appropriate access to the data, should be configured within the application to allow this activity, with consideration given to consolidating these events at appropriate locations.

SCADA applications

Introduction

Generation of appropriate logs of events within a SCADA application requires specific configuration within that application. In some cases, this may be through general configuration settings within the application (e.g., recording of user log on/log off), while other aspects (e.g., sequence prompts) will require specific configuration within the application.

Tips

Please note this is not deemed an exhaustive list but is intended to provide a starting point with understanding:

- Many SCADA applications can be configured to drop logs into the host's Application logging, where these logs can be collected and forwarded in a similar/same manner as host logs, as described above.
- The following attributes should be recorded for the activity where possible:
  - User undertaking the activity.
  - Date/time of activity.
  - Activity details
- Typical events that can be recorded through a SCADA application include:
  - User logon (when not through windows authentication)
  - Sequence stop/start, Sequence Step
  - Operator Prompt and associated response
  - Operational mode of devices
  - Internal application diagnostic alerts
  - 'Privileged' user activities (e.g., alarm setting changes, set point changes)
  - Process Alarm State (initiation, acceptance, clearing)
    - There are many alarm management solutions which can be used to consolidate these alarm events into a single solution providing a more useful component to support incident response.
- In some instances, legacy systems may have these attributes configured to be output to a printer. In these instances, consideration should be given to consolidating all such messages via an alarm management solution, some of which have the capability to manage alarms, and other messages, separately.

Common pitfalls

- To allow this information to be used and correlated with information from other sources requires the time to be synchronized across the relevant devices. This can be a challenge in some environments where the time on a SCADA system is changed manually (e.g., GMT – BST change) due to process batch reporting requirements, while other elements of the system may implement such changes automatically.

- Interpretation of the information provided by the SCADA logs requires an understanding of the specific SCADA application and the process being controlled to be able to determine any anomalies and identify any potential consequences resulting from those anomalies.
- Using the SCADA system itself as the only source of monitoring can be troublesome, given that if it is compromised, the value of the monitoring is somewhat negated.

Databases

Introduction

Databases are often used to track product, or other elements, through plant processes. They can be linked with Manufacturing Execution Systems (MES) which in turn set the parameters to be used at relevant stages of the production processes.

Currently, while some File Integrity Monitoring (FIM) solutions can monitor for changes to the structure of a database, the ability to monitor for changes to the integrity of data within the database itself in real time is limited, with additional logging required to allow for reviews of data integrity.

Tips

- Ensure that the database logging options are enabled, and record not just changes to the database structure but changes to data within the database. Where possible the following attributes should be recorded for the change:
    - User undertaking the change.
        - To allow differentiation between sequence generated changes, and manual corrections (e.g., when recovering from a plant fault) ensure that different user roles are configured and used, with privileges (including the areas of the database which can be accessed) restricted to those necessary for specific duties.
    - Date/time of change.
    - Change details.

Common pitfalls

- Interpretation of the information provided by the database logs requires an understanding of the specific database application and also the process being controlled to be able to determine any anomalies and identify any potential consequences resulting from those anomalies.

Historian applications

Introduction

Monitoring of process data and comparing against known good baselines through a plant historian system can assist process engineers in identifying anomalous changes in a process operation. While a historian is typically configured to record process variable data, it is often useful to configure the historian to record additional data attributes including set-points, register/variable values, and event/change of state parameters to allow correlation between process information, and state/mode of operational sequences.

For incident response investigations, the historian data can provide the incident response team with valuable insights into the timeframe of an incident and help to determine if cybersecurity events have resulted in physical process change events.

Tips

- The historian data must be timestamped and synced by the same clock as the other logging services to allow for correct correlation of events. The accuracy, and frequency of process data logging will be dependent on the variability of data and operational requirements. This is determined during plant design.
- Dedicated ICS/OT security monitoring solutions are available which have the capability for Historian software integration that allows for event frames (such as setpoint or alarm limit changes) to be integrated into the solution to provide additional asset discovery, threat detection, and facilitate additional incident response investigations.

Common pitfalls

- Interpretation of the information provided by the historian data requires an understanding of the process being controlled to be able to determine any anomalies and identify any potential consequences resulting from those anomalies.

Engineering Workstations

Introduction

Engineering workstations provide a capability to implement modifications to a control system and can also be used to support fault diagnostics and recovery, and other maintenance activities.

Given that laptops used for engineering/maintenance often aren’t connected to a network (indeed having a permanently connected engineering workstation can be a vulnerability for any system), they often require manual collection of the relevant logs to support incident response investigations.

Tips

As well as recording the typical security events associated with a host device (as described earlier) Engineering Workstations and Maintenance Laptops should also be configured to record activities such as:

- changes to programs
- changes to program states (running, program etc.)
- connection to devices (e.g. PLCs)
- software upload/download from/to a device.

Common pitfalls

- Interpretation of the information provided by the workstation logs requires an understanding of the process being controlled to be able to determine any anomalies and identify any potential consequences resulting from those anomalies.

PLC applications

Introduction

Recording of changes to PLCs provides information that can be used to identify any unauthorised, or anomalous, changes to the PLC code or other potentially unauthorised activities which could result in an unwanted consequence.

Tips

There are a number of secure PLC coding practices identified by the Top 20 Secure PLC Coding Practices Project. Of these practices there are a number which, if implemented in the PLC and associated HMI/Historian solution (as required), can support anomaly detection and subsequent incident investigation including:

- Use cryptographic and / or checksum integrity checks for PLC code.
  - Use cryptographic hashes, or checksums if cryptographic hashes are unavailable, to check PLC code integrity and raise an alarm when they change.
- Track operating modes.
  - Keep the PLC in RUN mode. If PLCs are not in RUN mode, there should be an alarm to the operators.
- Use PLC flags as integrity checks.
  - Put counters on PLC error flags to capture any math problems.
- Summarise PLC cycle times and trend them on the HMI.
  - Summarise PLC cycle time every 2-3 seconds and report to HMI/Historian for visualization on a graph.
- Log PLC uptime and trend it on the HMI.
  - Log PLC uptime to know when it's been restarted. Trend and log uptime on the HMI/Historian for diagnostics.
- Log PLC hard stops and trend them on the HMI.
  - Store PLC hard stop events from faults or shutdowns for retrieval by HMI alarm systems/Historians to consult before PLC restarts. Time sync for more accurate data.
- Monitor PLC memory usage and trend it on the HMI.
  - Measure and provide a baseline for memory usage for every controller deployed in the production environment and trend it on the HMI/Historian.

Common pitfalls

- Interpretation of the information provided by the PLC logs requires an understanding of the process being controlled to be able to determine any anomalies and identify any potential consequences resulting from those anomalies. In many cases, reference to other data sources (e.g., maintenance records) is required to identify such anomalies.

Reference guidance documents & further reading

- Top 20 Secure PLC Coding Practices Project

Security devices and solutions

Introduction

Host and Network Firewalls, Antivirus (AV) solutions, application allow-listing and user access control solutions can all be categorised as security devices and solutions capable of providing valuable logging and monitoring if deployed within an ICS/OT environment.

Tips

- Evaluate application allow-listing solutions on their capability beyond enforcement of executable exclusions lists. Solutions are available that can be configured to also prevent execution of scripts, macros, and memory attacks.
- As a minimum, logging from these systems should include notification of:
    - changes to policies, i.e., updated signatures or changes to application allow-list configurations.
    - blocking of application execution or script
    - detection of malicious or potentially malicious files
- Firewall logging should be configured to capture changes made to firewall ruleset.
- Firewall logging as a minimum should provide notification and logging of firewall policy violation. Therefore, there should always be a deny all policy at the bottom of each firewall policy configuration to ensure any violation is blocked and logged.
- Assuming the capability is present, the firewall's recording of log hit count should be collected to enable checks on overly permissive firewall rules or policies which are not being used and could be removed.
- Logging from firewalls should also include connectivity to the management interface of the firewall appliance or the firewall management solution.
- Logging from user access control should include logging events such as:
    - Logon
    - Logoff
    - session disconnect/reconnect.
    - session timeout
        - This is important for RDP user access as adversaries can hijack RDP sessions which are left idle if the user has not disconnected.

Common pitfalls

- Antivirus solutions need regular updates to be able to alert, quarantine and act on detection of threats based on signatures. Use of AV in ICS/OT environments therefore need careful consideration for obtaining, validating and deployment the latest signatures across the ICS/OT environment.
- It is common for ICS/OT applications on endpoints to require exclusion lists for AV solutions, such that the AV solution is not providing full coverage of file directories and signatures. Care should be taken to assess which endpoints are suitable for AV deployment

in the ICS/OT environment, and which application exclusion lists may be required that would reduce the effectiveness of the solution.

- Remember that Application White Listing (AWL) solutions will not prevent adversary misuse of legitimate applications and actions associated with valid credentials.
- There have been many documented EDR bypass techniques, operators should not solely rely on the protective monitoring of AWL alone.
- Default configuration of user access control solutions may not provide adequate coverage of event logging, for example the ability to log unauthenticated web requests.

Remote Access Solutions

Introduction

Remote access to ICS/OT environments is a common attack vector, as highlighted by the Oldsmar Water Treatment facility incident in 2021. Monitoring ICS/OT networks for remote access usage is important to ensure secure architectures and restrict usage of remote access to only approved solutions to authorised users during authorised times. Monitoring for common remote access solution Domain Name Service (DNS) queries, Transmission Control Protocol (TCP) port numbers and X509 certificates is recommended as part of a regular auditing and threat hunting operation to minimise the risk associated with uncontrolled remote access.

Tips

- If a remote access solution is approved for an environment, ensure that the deployed configuring allows for logging and monitoring from the installed applications and servers.
    - Remote access solutions will record log files to different directories. For example, by default:
        - TeamViewer records logs to:
            - C:\Program Files (x86)\TeamViewer\Connections_incoming.txt
            - C:\Program Files (x86)\TeamViewer\TeamViewer<version>_logfile.log
        - LogMeIn records logs to:
            - C:\ProgramData\LogMeIn\
    - Some remote access solutions default configuration is zero logging verbosity, users must enable logging before usage.
    - Many remote access solutions will use DNS, and therefore logging outbound DNS resolution provides valuable logging.

Common Pitfalls

- Multiple remote access solutions within a single organisation's environment are common, which can make logging and monitoring more challenging.

Reference guidance documents & further reading

- Recommendations following the Oldsmar water treatment facility cyber attack

Other sources of ICS/OT logs

Introduction

Within an ICS/OT environment, there are many other sources of information which can be referenced to support incident response and assist in determining anomalous activities. In some instances, the information may be held in applications residing on the corporate infrastructure (e.g., in a Computerised Maintenance Management System (CMMS)).

Tips

Other sources of data which can provide supporting information during an incident include:

- Records of process data taken during operator rounds.
    - While less easy to integrate into a monitoring solution, the use of hard copy logs taken during plant operations (e.g., operator rounds) can provide a trustworthy source of information, useful in identifying process anomalies.
- Records of maintenance activities
    - These records can be used to correlate events detected through other sources (e.g., detection of a maintenance laptop being connected to a PLC) with authorised activities and, as such, identify any anomalies.
    - While these records could be derived from electronic maintenance management systems (and as such could be integrated with the security monitoring solution), a more trustworthy solution is provided by using the actual hardcopy maintenance records (job cards etc.).
- Records of Engineering activities, e.g., software changes
    - These records can be used to correlate events detected through other sources (e.g., change in integrity of PLC code) with authorised activities and, as such, identify any anomalies.
    - While these records could be derived from electronic systems (and as such could be integrated with the security monitoring solution), a more trustworthy solution is provided by using the actual hardcopy records.
- Physical Process & Sensor Monitoring
    - Technology Solutions are available that monitor the electrical signals direct from either the physical process (i.e., Level 0) or the sensors, analysers, and actuators (Level 1) to detect process anomalies and cyber security threats. Such monitoring solutions are generally connected in parallel to the plant I/O via dedicated electrical isolators and diodes. The process signals are then analysed via Machine Learning algorithms which can detect anomalies to the normal plant operation. Alerts can then be raised directly with the plant operators and/or fed into a SIEM/Security Operations Centre (SOC).
    - The benefits of this Level 0/1 monitoring are that as most devices at these levels lack authentication, there is no protection to unauthorised access to the sensors. Therefore, data can be modified, and any anomalous or malicious control

commands will be accepted. Therefore, for the most critical processes, this method of detecting anomalies within process variables can be an effective way to mitigate the risk of bad sensor data (i.e., Integrity).

Common Pitfalls

- When integrating data from applications residing on the corporate infrastructure (e.g., in a Computerised Maintenance Management System (CMMS)), with a SIEM, careful consideration of the network architecture is required to ensure the required system security is achieved. Providing analysts with a read-only view into these systems may be a more secure alternative than integrating the systems.
- Interpretation of the information provided by these logs requires an understanding of the activity being logged, and the process being controlled to be able to determine any anomalies and identify any potential consequences resulting from those anomalies. In many cases this data is more relevant in supporting the review of other system logs and identifying anomalies.

Appendix A

Consolidated List of Indicators

Network

- Network Intrusion Detection
  - Unexpected Network Connections
  - Unknown Network Protocols
  - Deviation from Baseline Communications
  - Unexpected File Transfers
  - Use of insecure protocols
  - PLC configurations downloads
  - Deviation in clock which should be synced against same reference time.
  - Change to running mode of controllers (e.g. run/programme)
  - Unknown device on the network
  - Unknown IP address on the network
  - Communications traffic (IP, ModbusTCP etc.) outside specification
  - Detection of network scanning / ping requests
  - Detection of port scanning
  - Detection of unexpected ARP Broadcasting

Hosts

- IT like asset types (Servers, Workstations)
  - User Account creation/modification
  - Elevation of User privileges

  - Malware detected.
  - unexpected connection / attempted connection of portable media to device
  - unexpected process started.
  - unexpected service started.
  - High CPU usage

- Network asset types (firewalls, switches, routers, etc.)
  - Firewall rule change.
  - Firewall policy rule violation.
- ICS asset types (PLC, IED, HMI, etc.)
  - PLC Key switch position change
  - Controller uptime

Application

- Databases
  - Deletion / attempted deletion of backups.
- Historians
  - Process data, typically logged by the local historian servers will provide contextual data on the state of plant and operation. The process logging should be used to enhance efficiency and inform decision making during an incident, or post incident evaluation. The historian data must be timestamped and synced by the same clock as the other logging services to allow for correct correlation of events. The accuracy, and frequency of process data logging will be dependent on the variability of data and operational requirements. This is determined during plant design.
- SCADA Applications
  - Attempt to change parameter outside of prescribed bounds.
  - Alarm setting change.
- PLC programming suites

    - Controller program/configuration upload/download

    - Change to program/configuration

ICS operator and maintenance rounds

- Maintenance records, Operator logs and defect notifications
- monitor opening of panel doors
- record permit to work to cross reference with any deviation from the baseline.
- record design changes and re-align detection cases.

Indicators of Compromise

- User Behaviour

    - Logins at unexpected times of the day

    - Multiple failed logins

    - Attempts to access files/folders that are not related to the process.

    - Copying/Modification/Deletion of files

    - Anomalies in Privileged User Account Activity

- Entity Behaviour

    - Unusual Outbound Network Traffic

    - Geographical Irregularities

    - Anomalies in Database Activity

    - HTML traffic anomalies

    - Mismatched Port-Application Traffic

    - Registry/File changes

    - Unusual DNS requests

    - Unexpected Patching

    - Device Profile changes

- Collation of information in unplanned locations
- Unexpected Switch or PLC Firmware change
- Database logs showing irregularities.

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.