INDUSTRIAL CONTROL SYSTEMS
Community of Interest

Admin Corp Example - Where to store logs from Industrial Control Systems / Operational Technology environments.

Introduction

This publication provides guidance and considerations for Critical National Infrastructure (CNI) operators when considering where to store the logs captured within their Industrial Control System (ICS) / Operational Technology (OT) environment. It is the sixth of a series of articles to help operators undertake better logging and monitoring within their ICS/OT environments. It should be read in conjunction with the related guidance article "Where to store logs from Industrial Control Systems/Operational Technology environments". Given this Admin Corp Example also covers the use of Cloud technologies within an ICS/OT environment then the NCSC guidance article "Cloud-hosted supervisory control and data acquisition (SCADA)" is also relevant.

We have already addressed the why you need to monitor, what you need to monitor and how to log and monitor in previous publications. These previous publications also take a deeper look into different approaches such as collection driven and consequence driven approaches.

Important Note: *While the ICS COI is supported by the NCSC, and NCSC staff are involved in a range of its activities, no formal review of this guidance article has been undertaken by the NCSC. The ICS COI and its members strive to produce relevant ICS/OT specific cyber security guidance to supplement principle based cyber security guidance published by NCSC and have taken care to reference this guidance where applicable. This guidance article will be reviewed every 18 months to ensure that it has not been superseded by guidance published by NCSC, relevance and that any references are still accurate. The ICS COI and its activities are purely voluntary, with guidance articles produced that are deemed needed by UK Operators and their supportive industry partners. The fact that this guidance article has been published by the ICS COI has no relevance to the priority and focus of guidance published by NCSC.*

Architecture Overview

Regardless of the type of systems within the ICS/OT environment or the type of logs obtained (network, host, application, and others) from the systems, there is a need to store the logs securely.

This article will focus on the general considerations for a typical ICS/OT environment to guide ICS/OT operators to a position of collating the logs securely. Other guidance articles will address the skills required to perform ICS/OT log analysis and who should perform the analysis. The focus here is on how to architect secure log storage.

What drives the decision?

There is no defined template or operational architecture which outlines where is the best place to store log files: the most important decision is to agree to collect these in the first instance. It may be effective for a small site to collect data locally, equally, it may make more sense to send these direct to cloud for other reasons such as time, efficiency, access in real time, lack of local resources etc.

Another consideration for log storage will be the expected volume of log data, how sensitive the data is, what is the maturity of the site, budget, risk etc. For larger systems or sites, the volume of data collected can scale rapidly, so it is crucial that the advice from the other guidance papers (Why and What to Log) is taken into account to ensure a manageable number of logs are collected and stored.

The key point is that only relevant data is captured depending on the identified risk mitigations, Security Operations Centre (SOC) use cases, Data Forensics etc. that logging/monitoring can be useful for.

Deciding where to store log files is equally as important as what to store, who will have access to them and how long they should be stored for. What may influence the storage location is the requirement on how the data is accessed and what happens to data if the site is placed into island mode. While there are many more factors to consider, these are just a few to note.

Operational Size and Maturity vs Criticality?

Approaches to security and log collection should always be undertaken under the context of the organisations, the associated risks, regulatory requirements and what is appropriate to collect. Operational maturity will often underpin the next logical step in improving overall maturity of an organisation, those which are early on their journey may have easy to apply controls to address which are low hanging fruit that will quickly accelerate their status however, we need to not lose the focus on site criticality and operational safety.

Within this article we will look at a single organisation that has three sites, their business has grown overtime, some through acquisition. To keep things simple, we also assume that the size of the site has a linear maturity level attributed.

What Constitutes Maturity?

NIST Cybersecurity maturity levels describe an organisation's progress in implementing and strengthening its cybersecurity controls. They are typically represented as a series of stages or levels, each indicating a higher degree of sophistication and maturity in managing cybersecurity risks. Below is a brief overview of common cybersecurity maturity levels:

Partial: Cybersecurity risk management is typically performed in an ad hoc/reactive manner. Cybersecurity activities are typically performed with little to no prioritisation relative to the degree of risk that those activities address.

Risk Informed: Risk management practices are typically not established as organisation wide policies. Although risk management practices are not standard, they directly inform the prioritisation of cybersecurity activities alongside organisational risk objectives, the threat environment, and business requirements.

Repeatable: There is a higher level, organisation wide approach to managing cybersecurity risk. The organisation has formally approved risk management practices expressed as policy. Practices are regularly updated based on changes to business requirements and the threat landscape.

Adaptive: The organisation adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive factors. It implements a process of continuous improvement, including incorporating advanced cybersecurity technologies and practices, actively adapting to a changing threat and technology landscape.

Figure 1 - NIST Cybersecurity maturity levels

Operational Size and Maturity

While it is often assumed that size is relatable to maturity, this is not always the case. A large site is likely to have a mixture of technology which may span multiple vendors and have a variety of legacy and modern equipment in play.

It may be far simpler to achieve a high level of maturity for a smaller site, simply owed to the fact of scale. Either way, it is important to understand what the risk to the operation is of doing nothing and applying controls that will make a step change in operational maturity as well as security.

Regardless of size, the approach to log collection should follow simple principles that afford the best coverage, whilst providing access to key data sets that are stored in a location that is accessible for processing. Considerations need to be applied so far as the site has the ability to continue collecting data or processing should there be a disruption to the primary collection service e.g. during an incident. Collected data needs to have sufficient controls to protect against unauthorised viewing, tampering or inadvertent deletion.

Meet Admin Corp

Let's imagine we're following a fictional organisation who are responsible for managing the cyber security of a processing plant associated with CNI. 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.

As an essential service, Admin Corp must comply with the UK NIS Regulations. This means that Admin Corp's assets needed to produce Adminox must be protected from cyber-attack. Furthermore, because Admin Corp are regulated for safety by the UK Health and Safety Executive using OG86, they must take steps to ensure the continued cyber security of the Adminox production process.

While this example is for regulated sector, the purpose and approach can also be used where operations are not covered under these regulations.

Admin Corp has three sites in the UK attributed to a log collection project; these are:

1. **Stones**: Is a small production site recently acquired through acquisition to reduce the need for an international supply chain. This site creates key non-volatile components for other Admin Corp sites; this is not connected to the wider enterprise infrastructure but does have public internet access.

Maturity: Partial

2. **Rocks**: Is a medium sized, legacy operational processing site which creates key components for the main site Boulders, there is a mix of volatile and non-volatile products manufactured, some parts of the process require compliance to OG86. This site, which started off as a disconnected system, now has connections to the enterprise. There is a mixture of old and new technology in place with an established production base with legacy machinery.

Maturity: Risk Informed

3. **Boulders:** Is a large and modern processing plant, this site creates volatile chemicals. This site is connected to the Admin Corp enterprise network. This site is a relatively new build and operates with limited legacy debt, most of the operational system are still fully supported by industry with a few systems that can no longer be patched. The site has been through a number of assessments and is working its way to meeting the requirements of the enhanced CAF.

Maturity: Repeatable

Small Site (Stones) Locally Collection & Cloud Collection

Stones is a production facility which doesn't have connection to a wider enterprise infrastructure, its maturity is 'Partial', therefore there is typically an ad hoc approach to risk management and little prioritisation is given to cyber security.

To collect log data from this site there are two (2) approaches that we will look at: local collection, and data sent direct to cloud.

We will explore both of these scenarios separately.

Local log collection

Use Case: In an ICS/OT environment where uptime and safety are critical, collecting event log data locally rather than sending it to the cloud often makes more sense, especially for organisations with only partial maturity.

Rationale: The 'Stones' site is a small site with limited risk, manufacturing non-volatile components. This site has 'Partial' maturity and therefore is unlikely to have the local skills or infrastructure to support a complex logging approach. In this example it is assumed that to address this challenge, local log collection will be undertaken as there is no requirement to have access to files in real time.

- A small, partially mature site might not have the expertise or resources to design or properly manage a fully connected system.
- When incidents occur, having logs local on the site and immediately accessible enables faster diagnosis and response.
- Site engineers won't have delays accessing the information they need.
- Local collection provides the site more control over how long logs are stored, rotated, or backed up, based on actual operational needs.

When local logging might be a problem:

- If logs are rarely/never reviewed or correlated, the benefit is limited.
- No redundancy if local storage fails, logs could be lost or tampered with.
- Harder to detect long term trends, requires engineering effort to collect and correlate, data is not real time.

Why it matters: Local collection ensures that log data is available immediately, without relying on the complexity of establishing secure internet connectivity. In critical systems, engineers or system administrators may need to respond to situations such as unauthorised access, misconfigurations, or equipment faults in real time. Local collection means your monitoring tools always have access to the data, even during outages. There is a trade-off here, as manual collection takes time and effort to collect and correlate, and data collected is a snapshot in time.

How to Implement:

This approach is the most manually intensive and will often require attending each asset area to collect local logs files.

- First you must ascertain what logs files are of interest and then how best to collect them, this is likely to be on clean and trusted removable media. On some legacy systems, logging will need to be manually enabled to ensure security events of interest are recorded in the log files.
- Establish the frequency that the task will be undertaken and the format the logs will be in, these may need manual intervention to get them into a consistent format.
- Import the data to a log collector and establish the review and search criteria, this may vary depending on the collection format, size and quality of the data.

Advantages:

- **Faster access to data:** If there's a safety event, system failure, or potential cyber threat requiring activation of island mode, engineers need immediate access to logs. Local storage keeps data close to the plant floor, so it's always available. Consider sending critical alarms to the Supervisory Control and Data Acquisition (SCADA) where time critical events need to be visualised.
- **Works in low connectivity environments:** Many ICS/OT environments have limited external capability. Cloud solutions depend on a constant connection, local logging systems continue working even during network outages, ensuring no data is lost.
- **Easier integration with legacy systems:** Many ICS/OT networks use older systems that don't use modern cloud transport protocols or log format.
- **Better control and security:** Cloud systems require strong identity, encryption, and access controls, things that take time and expertise to set up. A partially mature organisation may not be ready to handle cloud security well. Keeping logs local reduces the risk of misconfigured cloud access or data leakage.
- **Supports compliance:** Regulations in CNI often require data to stay on premises or within national borders. Local logging simplifies compliance and helps during audits because the data never leaves your control.

Disadvantages:

- **Limited scalability:** Local storage systems can fill up quickly, especially if logging high volumes of events. You'll need to manage disk space and backup strategies locally.
- **Harder to centralise data across business areas:** If you operate multiple production areas or systems, collecting everything locally means you'll have data silos. It becomes harder to get a single view of your organisation's ICS/OT activity.
- **Manual effort for analysis:** Without cloud tools, local log analysis may be slower or require manual steps. You might need to move files or use offline tools to investigate events, which can delay response times.
- **Less use of advanced analytics:** Cloud platforms often offer Artificial Intelligence (AI) based threat detection or correlation engines that are hard to replicate locally. With local logs, you may miss out on these benefits unless you invest in on premise analytics tools.

How could this be improved:

- There may be opportunities to collect logs not from every device but from central source. An example for a small site like this could be SCADA, Human Machine Interface (HMI) Operating system events, these could be sent to the local engineering workstation, thus removing the need to collect these from every device.
- Extract log files in a common format (where possible) and ingest into a tool which can import open standard or normalise different formats. There are a number of paid, free and open-source solutions that can be used for this purpose.

- Leverage existing passive network scanners (where available) to ingest critical logs. Many Intrusion Detection Systems can recognise, and parse security events sent in a common format. If these exist, they can provide an additional and local data visualisation and analysis overlay.
- Establish what is required from the logs that have been collected, there is no point in collecting data just for the sake of it. Make use of pre-configured dashboard or alerts, once the data is parsed this can quickly identify the data sets you were intending to capture and undertake action upon

For an organisation still building its ICS/OT security maturity, local log collection is often the first step. It provides reliability, visibility, and simplicity, which are important factors in safety critical environments. While it may require more effort to scale or analyse data across sites, it's a solid foundation to build visibility and incident response capabilities before moving to other collection methods such as cloud-based solutions.

Cloud log Storage

Use Case: In an ICS/OT environment where uptime and safety are critical, sending event log data to the cloud often makes more sense, especially where there is a need for real time information to be viewed that is centralised, especially when the efforts to collect logs locally outweigh the risks of cloud storage.

Rationale: The 'Stones' site is a small site with limited risk, manufacturing non-volatile components. This site has 'Partial' maturity therefore is unlikely to have the local skills or infrastructure to support a complex logging approach. In this example it is assumed that to address this challenge, cloud storage will be undertaken as there are benefits to reduce engineering effort for local collection, as well as providing access to data in near real time. Data flows can be sent to the cloud securely through a well-managed firewall.

- Local log storage/capacity planning is reduced.
- Aligns with small sites with limited Information Technology (IT)/OT resources or where collecting local data is not practical or time intensive.
- Cloud log collection platforms often provide prebuilt dashboards, detection rules, and alerting mechanisms.
- Data is correlated and can help with investigations and forensics.

When cloud logging might be a problem:

- Highly regulated environments prohibiting offsite data transfer.
- Poor or unreliable internet connectivity.
- If logs contain sensitive operational data that must stay local or inside of local jurisdiction and meet local governance requirements.
- If the network infrastructure is unreliable to handle logging traffic passed on the network to the edge firewall, especially with verbose legacy systems.

Why it matters: With event data exported to the cloud, engineers, analysts, or external support partners can access the data securely from anywhere, without needing to remote into each plant network. This makes incident management faster and helps when specialist skills aren't available onsite. If configured correctly, there will also be a local copy of critical events if there was an issue with connectivity.

How to Implement:

Sending event data direct to cloud requires a secure method that does not place the plant at risk. Robust firewall rules should be established that only permit approved devices to communicate with approved platforms, this should be implemented with strong authentication, data which is encrypted in transit and strict access control lists, ideally with a northbound only connection to the cloud, utilising functions like Network Address Translation (NAT) on the ICS/OT edge firewall.

- The system pushes logs from ICS/OT systems (e.g. SCADA servers, Programmable Logic Controllers (PLCs), firewalls, switches) in real time or on a regular schedule.
- The logs are stored in the cloud tenancy in a searchable format.
- The solution can later be integrated into wider IT-ICS/OT Security information and event management (SIEM) systems if needed, but that's not a requirement at this stage.

Advantages:

- **Centralised visibility across the site:** If you have more than one process area on the plant, logging data to the cloud helps you collect and view event data from all of them in one place. This gives the OT and security teams a bigger picture view of what's happening across the whole organisation. That's especially useful for spotting trends or detecting coordinated threats.
- **Better storage and retention:** Local systems often have limited disk space, especially legacy ones. Cloud platforms offer scalable storage across multiple regions for resilience; this also allows logs retention for months or years without running out of space or needing to rotate data too aggressively. This supports longer investigations and compliance with regulations that require extended retention. Storage costs here may rapidly increase depending on the size of data sets and retention periods.
- **Use of cloud-based analytics and tools:** Cloud logging platforms often come with built in tools like dashboards, alerts, and even AI driven threat detection. These can help partially mature organisations "level up" their monitoring capabilities without needing to buy and manage expensive on premises software.
- **Reduced local infrastructure burden:** Managing log servers, backup routines, and hardware failures onsite takes time and skills. Cloud collection reduces this burden, log data is sent securely to the cloud, where it's stored and managed. This simplifies operations and lets engineers focus on process and safety. Note depending on operational factors, it may be necessary to backup cloud data locally.

Disadvantages:

- **Requires reliable and secure internet**: Cloud logging depends on a secure and stable internet connectivity. If a site has poor or unreliable access, you may experience delays or data loss during outages unless buffered locally.
- **Security maturity must be improving:** Sending sensitive ICS/OT data to the cloud requires good security practices like, encrypting data in transit, using strong authentication, sensitive data filtering and properly managing access rights. A partially mature organisation may need to strengthen these areas to reduce the risk of data exposure.
- **Potential latency in log review:** If logs are sent to the cloud for storage and analysis, there may be some delay in how fast alerts are generated compared to real time local systems.
- **Data privacy and compliance:** Depending on your sector, there may be rules about where log data can be stored and also what category of data. Some CNI sectors require data to stay in country or locally on site. You'll need to check if the chosen cloud platform complies to local or sector requirements, including security guidance.
- **May place additional burden on the local network:** logging traffic will need to be routed to the edge firewall, and this may add an overhead if the network infrastructure is not robust enough to handle additional traffic volumes.
- **Loss of visibility during incidents or activation of island mode:** logs at are stored in the cloud may not be accessible during outages, either locally or from the cloud provider. This may hamper incident response processes or event discovery.

How could this be improved:

- Routing event data to the cloud assumes there will always be an on connection, if this is not always going to be possible it may have merits to create a small environment where data can be stored locally and processed in the event of the site operating in island mode. While this is moving closer towards a hybrid model (discussed later), this may be a simple approach with the use of 3rd party software.
- Deploying a proxy agent within a Demilitarised Zone (DMZ) which is responsible for routing traffic to the cloud broker creates a protocol break and delivers a more secure architecture than allowing devices to connect to the internet directly.
- The use of unidirectional gateways or data diodes could be utilised to provide further assurance of no back flow of data from publicly connected networks or other assets that may have a wider connection to external networks.
- Utilise network functionality such as VLANs and Quality of Service to reduce potential impact on the network.
- Many logging software system support throttling to reduce the impact of logging on the endpoints and the network infrastructure

For organisations working toward greater ICS/OT security maturity, cloud log collection offers better visibility, scalability and access to advanced analysis tools. While it requires a secure and reliable connection, it is likely to also require some improvements in cloud security practices to

deploy correctly. It can help sites to accelerate detection and response capabilities for sites that can also scale into wider enterprise class solutions.

The use of cloud will require wider supply chain reviews and clear understanding of the terms of use, contract requirements on both parties and also service restrictions and or limitation.

Medium Site (Rocks) Centrally collected

Rocks is a production facility which has connection to a wider enterprise infrastructure and its maturity is 'Risk Informed', therefore risk management practices are typically not established as organisation wide policies. To collect log data from this site, event information is forwarded to a local collector(s) for local processing and visualisation.

Use Case: In an ICS/OT environment, event log data is essential for understanding what's happening on the network, whether it's operator actions, device behaviour, system changes, or potential security events. Manually pulling logs from PLCs, HMIs, or network devices is time consuming and inconsistent. It might work in small environments, but it's unreliable at scale. With automated local collection, logs are gathered centrally from relevant systems using standard protocols, agentless or agent-based collection methods.

Rationale: The 'Rocks' site is a medium sized site with increased risk, manufacturing volatile and non-volatile components. This site has 'Risk Informed' maturity. There is a blend of legacy and modern operations, with a connection to the enterprise. Due to the safety risk for this site, connection to public networks are highly restricted from the ICS/OT environment, compliance to OG86 is also required.

In this example local storage has been deemed the best approach to reduce the risk of the legacy components of the process, with data being collected and stored in the DMZ which is accessible to the enterprise. Strict zones and conduits are in place between the enterprise and operational technology to allow for real time alerts to be sent through to an enterprise SIEM.

- Keeping logs onsite ensures full ownership and control, which supports risk management goals such as data confidentiality, system integrity, and asset classification.
- Risk informed ICS/OT environments typically segment ICS/OT from IT and avoid external dependencies
- Keeps operational responsibility with internal staff or trusted third party with fixed scope and known cost.
- When events occur, logs stored locally under strict access control may have higher evidentiary value, as they were never exposed to external environments.

When central logging might be a problem:

- Local logs stored on a single system (e.g., a historian server or syslog appliance) are at risk of loss due to hardware failure, power outages, ransomware attacks or accidental deletion.

- Limited integration with broader security strategy, insufficient correlation or skilled personnel to undertake analysis.
- Log storage is not sized correctly or doesn't age data out efficiently, logs may be overwritten or rotated too quickly, leading to gaps in visibility.

Why it matters: For an organisation with risk informed maturity, choosing to collect data centrally but locally (on-site), rather than manually from each device or sending it to the cloud, offers a balance of efficiency, control, and security.

How to Implement:

Instead of logging into each system or device to download logs manually, a centralised logging server is deployed on site.

- The system pulls or receives logs from ICS/OT systems (e.g. SCADA servers, PLCs, firewalls, switches) in real time or on a regular schedule.
- The logs are stored locally in a searchable format, and appropriate analysis or alerting can be done using on premise tools.
- The solution can later be integrated into wider enterprise systems if needed.

Advantages:

- **Local control and faster access and response:** By keeping logs locally on site in a centralised location, this avoids the delays and risks of relying on cloud services or remote storage. In the event of a system fault, safety issue, or cyber incident, the ICS/OT team has immediate access to all relevant logs, even if the site is in island mode or restricted for safety reasons. This is especially useful in ICS/OT environments where uptime and availability are critical, and support may not be readily available.
- **Improved detection through correlation:** When log data is collected centrally, this can correlate events across multiple systems, e.g. linking a change on a PLC with operator access on an engineering workstation. This improves the ability to detect threats or abnormal behaviour that wouldn't be obvious when looking at logs from one device at a time.
- **Supports compliance without sending sensitive data off site:** In CNI and other regulated sectors, keeping operational data on site is often a compliance requirement. Centralised local collection helps meet those requirements without the risks associated with transferring sensitive system logs over the internet to a cloud platform.
- **Enables phased maturity:** Organisations with risk informed maturity are aware of their key risks but may not be ready to fully adopt cloud or enterprise wide SIEM systems. Local collection provides a scalable, controlled foundation for building toward more advanced monitoring without jumping ahead of current capabilities.
- **Respects air gapped or isolated network designs:** Many ICS/OT environments intentionally restrict internet access or are air gapped for safety. Cloud based solution can't

always operate in these environments without major changes. Local centralised logging fits into current architecture without breaking isolation, making it safer and easier to adopt.

Disadvantages:

- **Needs initial setup and ongoing maintenance:** There is an initial expenditure of cost, time and effort to correctly deploy and secure operations. Devices must be configured to send logs to the central collector. This can take time but is a one-off task. Deployment will need to be planned to ensure that collections doesn't degrade the existing security boundaries. It may be required to collect data out of band, i.e. on an alternative network to the primary process control network.
- **Limited analytics compared to cloud:** Local tools might not offer AI or threat hunting features. The use of rule-based alerts and dashboards may provide limited value and coverage. There may be extended efforts required to process the data in a way that is conducive to the site's needs.
- **Storage and backups must be managed:** Logs take up space, so storage, security and backup routines need to be in place. While some of these can be automated or handled during regular maintenance, understanding retention periods and securing the data in use and on cold backup storage may be complex.
- **Visibility is site specific**: Each site has its own logs. If corporate teams need cross site views, logs may eventually need to be aggregated centrally or forwarded upstream.

How could this be improved:

- Event data collected may be used to further establish security actions, for example if a device is operating out of normal operations, this data could be fed into a Network Access Control (NAC) and the device quickly isolated from the network. Approached such as this will require robust testing and due consideration given if this was ever to be automated.
- Alerts or events such as changes to device configuration can be automated into change management platforms such as ServiceNow. Being able to correlate identified changes to configuration against approved change management platforms creates better traceability and improves business maturity.
- If you're using local logging, treat it as a system in its own right, include it in disaster recovery plans, apply log integrity and access controls and consider forward critical logs (or summaries) to a secure offsite location for resilience.

For a risk-informed ICS/OT organisation, centrally collecting event logs locally may be the most effective and secure method. It offers:

- Automation and speed over manual collection
- Local security and control over data
- Scalable, real-time insight into system activity

This approach provides a solid foundation for monitoring and incident response, without jumping ahead of other collections methods which may open up wider security concerns, especially if the

data is sensitive or the architecture is consistent with air gapped design. It also allows for expansion opportunities in the future as well as local processing of data with the capability to expand coverage to cloud at a later date.

Large Site (Boulders) – Hybrid Collection

Boulders is large production facility which has a connection to the enterprise infrastructure and public networks. Its maturity is 'Repeatable' therefore there is a higher level, organisation wide approach to managing cybersecurity risk. To collect log data from this site, event information is forwarded to a local site collector(s) for processing and visualisation, a set of this data is also sent to a cloud collector for long term storage, enterprise use or in-depth analysis.

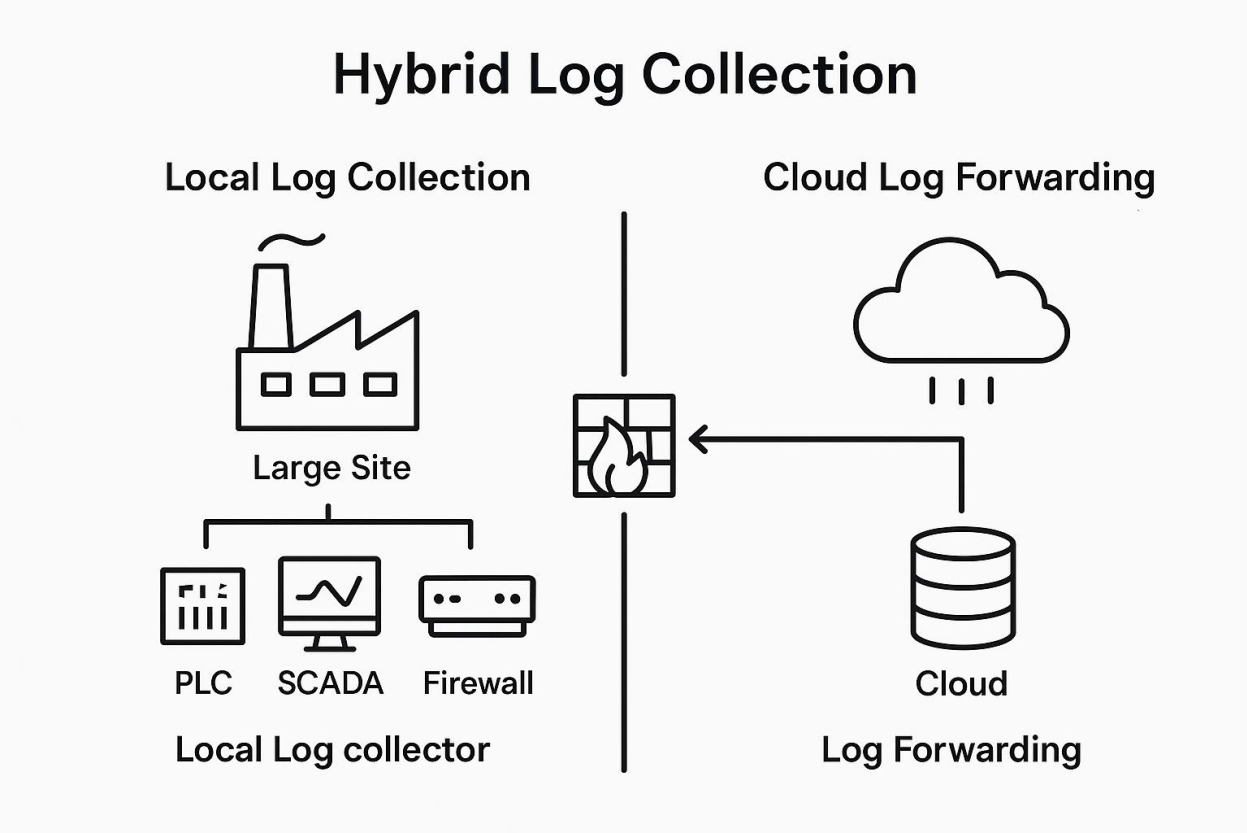

Figure 2 Hybrid Log Collection at the Boulders Site

Use Case ICS/OT Event Login: In an ICS/OT environment, comprehensive event log data is essential for understanding network activity, including operator actions, device behaviour, system changes, and potential security events. Manually extracting logs is time consuming and inconsistent, making it an unreliable approach, especially at scale. Storing logs centrally allows for consolidation and a single view of the truth, when this needs to scale to a larger audience it is often beneficial to expand reporting and storage to cloud which allows stakeholder and security teams to view and analyse data without the need to provide direct access into the ICS/OT environment.

With the elasticity of cloud, it provides a platform that will enable large scale processing of data with the benefits of powerful machine learning to provide outputs that is often difficult with on premise only solutions.

Rationale for Hybrid Logging at Boulders:

Site Profile: The 'Boulders' site is a large site with medium to high risk, manufacturing volatile components. This site has 'Repeatable' maturity. The site is modern plant with limited legacy components. Due to the safety risk for this site, connection to public networks are highly restricted from the ICS/OT environment, compliance to OG86 is required.

Hybrid Strategy: In this example hybrid storage has been deemed the best approach, this is addressed with local collection of data to a central source in the enterprise, the cloud component is utilised to allow for long term storage and wider accessibility of data collected for use internally as well as 3rd parties who help support and protect operations. Strict zones and conduits are in place between the enterprise and operational technology to allow for real time alerts to be sent through to an enterprise SIEM. Sensitive recipe data is stored locally and does not leave the local site.

- Local log collection ensures uninterrupted monitoring and log access, even if internet or cloud connectivity fails.
- Cloud log forwarding allows higher level analysis, long term retention, and external threat detection, supporting a more strategic cybersecurity posture.
- Scalable storage and retention with enhanced resilience and redundancy.
- Supports multi-site visibility and standardisation which allows for a large site that's part of a bigger estate detect cross site threats.

Challenges of Hybrid Logging

When hybrid logging might be a problem namely complexity, data sensitivity and latency and cost:

- Increased complexity without sufficient process discipline, this may increase the attack surface.
- If logs contain sensitive operational data that must stay local or inside of local jurisdiction.
- Latency or reliability, hybrid setups often start small but grow quickly which may lead to additional cloud storage costs.
- Getting inadvertently locked into a single cloud provider.

Why it matters: A hybrid log collection delivers the security and automation of centrally stored data with the added flexibility to use all the functionality and scalability that comes with cloud storages. Logs from ICS/OT systems (PLCs, SCADA, firewalls, sensors, etc.) can be first collected and stored locally, at or near the industrial site. Those logs can then be transferred to the cloud, either in real time or via schedule, depending on connectivity and priority. If the site loses internet access, the system stores logs locally and automatically forward them when the connection returns.

How to Implement: Log files are sent to a local log collector for processing, and a defined set (or subset) is then forwarded to a cloud collector. Data can be accessed locally or from the cloud platform, retention polices may differ according to business needs. In this deployment, considerations need to be given for when a connector may not be present to the cloud and how this data is sent without losing events, e.g. store and forward.

Robust firewall rules should be established that only permit approved devices to communicate with approved platforms, this should be implemented with strong authentication, data which is encryption in transit and strict access control lists, ideally with a northbound only connection to the cloud, utilising functions like NAT on the ICS/OT edge firewall or through the use of unidirectional gateways such as a data diode.

Operational Workflow:

Depending on the use case, it may be beneficial to undertake large data queries on the cloud platform due to the elastic nature of this processing platform.

- The system pulls or receives pushed logs from ICS/OT systems (e.g. SCADA servers, PLCs, firewalls, switches) in real time or on a regular schedule.
- The logs are stored locally in a searchable format, and basic analysis or alerting can be done using on premise tools.
- The solution can then forward into wider IT/OT SIEM or cloud systems either at pre-defined intervals or in real time.

Advantages:

- **Local Speed and access with cloud scalability:**
    - **Locally:** Logs are collected in real time. Engineers on site get immediate access to troubleshoot faults or review changes.
    - **In the Cloud:** Data can be centralised from all production areas, or sites into one platform. This supports organisation wide analytics, compliance reporting, and cybersecurity operations.
- **Store and Forward:** If internet or WAN connectivity drops, local systems keep collecting logs. Once connection resumes, the system forwards missing data to the cloud. This prevents data loss and ensures continuous monitoring, even in remote or isolated locations.
- **Supports Mixed Environments:** Many ICS/OT environments include a mix of vendors, protocols, and legacy equipment. A hybrid model allows for:
    - Local customisation (tailoring how logs are collected per device or vendor)
    - Cloud normalisation and enrichment (tagging, standardising, or correlating data at scale)
- **Reduces Manual Workload:** No need for engineers to manually collect logs from individual systems or upload them to a shared drive. Automation handles the heavy lifting, reducing errors, delays, and missed incidents.

- **Enables Better Security Monitoring:** With all logs flowing to the cloud, central security teams can run threat detection across the organisation, spot patterns across multiple sites. Trigger alerts or investigations even when sites themselves are unaware of issues. Local teams will still have full access to logs and can respond quickly to operational events.
- **Handles Large Data Volumes:** For large organisations, collecting data from thousands of assets can quickly consume local storage. The cloud provides elastic storage, powerful analytics tools without overloading site infrastructure. Cost optimisation, since old or infrequent access logs can be moved to cheaper cloud tiers.

Disadvantages:

- **Very Small, Isolated Sites:** If a site is standalone, has limited staff, or low risk operations, A simple local only setup might be easier to manage.
- **Fully Cloud Ready, Modern ICS/OT Setups:** Some new plants are designed from scratch with strong connectivity, hardened cloud gateways, and no legacy systems. These may benefit from a cloud first or even cloud only logging architecture.
- **Extreme Air Gapped Environments:** If you operate in highly secure, air gapped networks, cloud may be completely off limits. Local only log collection with manual exports or centrally stored and processed may be necessary.
- **No Skilled Staff on Site:** If sites lack the resources or skills to manage local storage, or relying more on cloud centralisation may reduce onsite workload.
- **Too Complex to Operate and Maintain:** Managing both local and cloud log storage means maintaining Local storage infrastructure (servers, databases, backups etc), Cloud integrations (connectivity, data pipelines, cloud log analytics) and synchronisation logic (to ensure no data is lost or duplicated). For ICS/OT teams with limited cybersecurity or IT resources, this can become a burden. Instead of simplifying operations, hybrid logging may create additional failure points, especially across multiple vendor systems or legacy devices. If the organisation's risk processes are "repeatable" but not fully matured, adding this layer of complexity might outpace the team's ability to manage it reliably.
- **Cost Can Spiral:** Hybrid solutions often require investment in edge hardware or collectors, cloud ingestion platforms and network bandwidth, including licensing for both local and cloud systems. At scale, this can be expensive, especially when log volumes are high. Cloud egress and storage costs can add up, and local hardware still needs to be maintained.
- **Connectivity Challenges Undermine Cloud Use:** Hybrid approaches rely on periodic or real time data transfer to the cloud. ICS/OT environments will have a number of challenges such as, unreliable or low bandwidth connections, remote or unmanned sites and network segmentation or air gaps.
- **Skills Gap in ICS/OT:** Managing cloud based log collection typically requires API integration knowledge, Security hardening of cloud interfaces, understanding of IAM (Identity and Access Management) and ongoing monitoring of cloud costs and performance. If the ICS/OT or plant engineering team lacks these skills and relies heavily on local systems, pushing part of the logging workflow into the cloud can increase dependence on corporate IT or third-party vendors, introducing operational friction.

- **Security and Data Sovereignty Risks:** Sending logs to the cloud, even in part may raises concerns:

    - Are we exposing sensitive control system data to the internet?
    - Are we meeting compliance requirements (e.g. NIS, IEC62443)?
    - Who has access to the logs once they're in the cloud?
    - Where does the data reside, are there copies in forbidden jurisdictions?

How could this be improved:

- Event data collected may be used to further establish security actions, for example if a device is operating out of normal operations, this data could be fed into a Network Access Control (NAC) and the device quickly isolated from the network. Approached such as this will require robust testing and due consideration given if this was ever to be automated.
- Alerts or events such as changes to device configuration can be automated into change management platforms such as Service Now. Being able to correlate identified changes to configuration against approved change management platforms creates better traceability and improves business maturity.
- Technologies such as SD-WAN, satellite and 5G may be possible to improve resilience for external connections to public networks, this may be important where there is limited option for fixed line providers in a geographical area. Where public networks are considered, data should be adequately secured using appropriate methods such as TLS and VPN.

For an organisation with repeatable maturity, hybrid logging is a good approach that can deliver on site resilience and fast response, enterprise-wide visibility and security insight with room to grow, without needing to rip and replace legacy infrastructure.

It's not the simplest or cheapest solution; however, it's one of the most balanced, scalable, and risk aware approaches for industrial ICS/OT environments facing growing cybersecurity, compliance, and operational complexity.

Finally, the hybrid model may sound like the best of both worlds, but for some organisations, it can become a compromise that pleases no one. If the added complexity, cost, or risk outweighs the value of centralised analytics, a more focused local or cloud only approach may be simpler, cheaper, and easier to manage, at least until the organisation's maturity level increases.

Pros and Cons of each storage medium

Centrally/Local Collected location

Pros:

- **Enhanced Control:** Organisations maintain direct oversight of data, facilitating tailored security measures.
- **Reduced Latency:** Local data access ensures minimal latency, crucial for real-time ICS/OT operations.
- **Compliance:** Simplifies adherence to regulatory requirements by keeping data within organisational boundaries.

Cons:

- **High Initial Investment:** Significant capital expenditure for infrastructure setup and maintenance.
- **Scalability Challenges:** Expanding storage capacity requires additional hardware, leading to potential delays and increased costs.
- **Resource Intensive:** Necessitates dedicated personnel for system management and security oversight.

Suitability by Maturity Level:

- **Partial:** May lack resources for robust on premises solutions, leading to potential security gaps.

Hybrid location

Pros:

- **Flexibility:** Combines on premises control with cloud scalability, allowing data to reside where it is most appropriate.
- **Cost Optimisation:** Balances capital and operational expenditures by allocating resources based on specific needs.
- **Enhanced Resilience:** Offers robust disaster recovery options by diversifying data storage locations.

Cons:

- **Complex Management:** Requires sophisticated strategies to manage and secure data across multiple environments. May have issues with loss of connectivity?

- **Integration Challenges:** Ensuring seamless interoperability between on premises and cloud systems can be difficult. Security issues?
- **Variable Compliance:** Navigating differing regulatory requirements across storage environments necessitates diligent oversight. Who has access, auditing etc?

Suitability by Maturity Level:

- **Partial:** May find hybrid solutions overly complex without established processes and resources.
- **Risk Informed:** Can adopt hybrid storage by aligning it with their risk management strategies.
- **Repeatable:** Well positioned to implement and manage hybrid solutions effectively due to mature processes and capabilities.

Cloud Location

Pros:

- **Scalability:** Easily adjust storage capacity to meet evolving data needs without significant infrastructure changes.
- **Cost Efficiency:** Reduces upfront capital expenditure by utilizing a pay as you go model.
- **Accessibility:** Enables remote access to data, supporting flexible operations and disaster recovery plans. Could be double edge sword for Island mode.
- **Tamper Protection:** Offsite copies of the data reduce the likelihood that data is manipulated or modified.

Cons:

- **Security Concerns:** Data stored off site may be more susceptible to breaches if not properly secured.
- **Compliance Issues:** Storing data in the cloud can complicate compliance with industry regulations and data sovereignty laws.
- **Dependence on Internet Connectivity:** Accessing data relies on stable internet connections, which may be a vulnerability.
- **Integrity:** Cloud metrics, pressure to ingest data, possible loss if no store and forward, costs etc?

Suitability by Maturity Level:

- **Partial:** May benefit from cloud solutions due to limited resources but must address security and compliance challenges.
- **Risk Informed:** Can leverage cloud benefits while implementing measures to mitigate identified risks.

- **Repeatable:** Capable of integrating cloud storage into a comprehensive security framework with continuous monitoring.

Storage Summary

The use-cases above detail how the different approaches to log collection and storage can be determined based on the operational need and the maturity of the organisation. As a concise summary, the table below shows some advantages and disadvantages of each approach for the security aspects that need to be considered.

Aspect	Hybrid Approach	Local Only	Central Only	Cloud Only
Availability during outages	✅ Yes (local buffer)	✅ Yes	✅ Yes	❌ No (needs internet)
Site level access	✅ Full access	✅ Full access	✅ Full access	❌ Not immediate
Centralised visibility	✅ Yes	❌ No	✅ Yes	✅ Yes
Scalability for large organisations	✅ Strong	❌ Limited	✅ Yes	✅ Strong
Security control	✅ Balance between local and cloud	✅ Strong local control	✅ Strong local control	⚠️ Higher cloud exposure
Automation readiness	✅ Suits repeatable	⚠️ More manual config	✅ Suits repeatable	✅ Cloud automation possible
Cost efficiency	✅ Optimised balance	⚠️ Local storage can be expensive	⚠️ Local storage can be expensive	⚠️ Long term cloud costs can grow
Latency (speed of access)	✅ Local fast, cloud for historical	✅ Always fast locally	✅ Always fast locally	⚠️ Depends on internet
Ongoing maintenance	⚠️ Local updates needed	❌ High effort for local only collection	⚠️ Local updates needed	✅ Minimal once established

Best Practice Approaches for Monitoring and Logging

Best Practices for Security Data and Log Collection in ICS/OT environments:

- **Comprehensive Monitoring:** Implement continuous monitoring to detect anomalies and potential threats promptly.
- **Standardised Logging:** Adopt uniform logging formats to facilitate efficient analysis and correlation of events.
- **Regular Audits:** Conduct periodic reviews of log data to ensure the effectiveness of security measures and compliance with policies.
- **Access Controls:** Restrict access to log data to authorised personnel only, minimising the risk of internal threats.
- **Incident Response Integration:** Ensure that log collection processes are integrated with incident response plans to enable swift action when necessary.
- **Operational Isolation:** Critical log data is available in the event of island mode, either enforced or unplanned.
- **Clear Responsibilities:** while security events are being monitored and analysed by security operations, it is important to ensure that the health of the monitoring systems are also monitored by the teams responsible for its maintenance (e.g., security engineers).

Selecting the appropriate data and log collection strategy requires a nuanced understanding of an organisation's maturity level, resource availability, and specific security requirements. By aligning storage solutions with organisational capabilities and risk profiles, ICS/OT environments can achieve robust security and operational efficiency.

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). 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, and whilst ICS-COI members have exercised reasonable care in compiling the guidance, they provide no warranty as to its accuracy, completeness, or suitability for any particular purpose.

To the fullest extent permitted by law, neither the ICS-COI or its members accept any liability for any loss, damage, cost, or expense arising directly or indirectly from the use of and / or reliance on, this document. Users of this guidance are advised to exercise their own judgement and consider taking independent professional advice.

Any reference to commercial products, services, or entities by name or otherwise, does not constitute or imply endorsement, recommendation or preference by the ICS-COI. The views and opinions expressed in this document shall not be used for advertising or product endorsement purposes.

Document Details

This document is version 1.0 and was published on 17/10/2025. It will be reviewed every 18 months.