Best practices for event logging and threat detection

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

National Cyber Security Centre
a part of GCHQ

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre
PART OF THE GCSB

General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

Table of contents

Executive summary

This publication defines a baseline for event logging best practices to mitigate cyber threats. It was developed by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) in cooperation with the following international partners:

- United States (US) Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA)
- United Kingdom (UK) National Cyber Security Centre (NCSC-UK)
- Canadian Centre for Cyber Security (CCCS)
- New Zealand National Cyber Security Centre (NCSC-NZ) and Computer Emergency Response Team (CERT NZ)
- Japan National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and Computer Emergency Response Team Coordination Center (JPCERT/CC)
- The Republic of Korea National Intelligence Services (NIS) and NIS's National Cyber Security Center (NCSC-Korea)
- Singapore Cyber Security Agency (CSA)
- The Netherlands General Intelligence and Security Service (AIVD) and Military Intelligence and Security Service (MIVD).

Event logging supports the continued delivery of operations and improves the security and resilience of critical systems by enabling network visibility. This guidance makes recommendations that improve an organisation's resilience in the current cyber threat environment, with regard for resourcing constraints. The guidance is of moderate technical complexity and assumes a basic understanding of event logging.

An effective event logging solution aims to:

- send alerts to the network defenders responsible for monitoring when cyber security events such as critical software configuration changes are made or new software solutions are deployed
- identify cyber security events that may indicate a cyber security incident, such as malicious actors employing living off the land (LOTL) techniques or lateral movement post-compromise
- support incident response by revealing the scope and extent of a compromise
- monitor account compliance with organisational policies
- reduce alert noise, saving on costs associated with storage and query time
- enable network defenders to make agile and informed decisions based on prioritisation of alerts and analytics
- ensure logs and the logging platforms are useable and performant for analysts.

There are four key factors to consider when pursuing logging best practices:

1. enterprise-approved event logging policy
2. centralised event log access and correlation
3. secure storage and event log integrity
4. detection strategy for relevant threats.

Introduction

The increased prevalence of malicious actors employing LOTL techniques, such as LOTL binaries (LOLBins) and fileless malware, highlights the importance of implementing and maintaining an effective event logging solution. As demonstrated in the joint-sealed publication Identifying and Mitigating Living Off the Land Techniques, Advanced Persistent Threats (APTs) are employing LOTL techniques to evade detection. The purpose of this publication is to detail best practice guidance for event logging and threat detection for cloud services, enterprise networks, enterprise mobility, and operational technology (OT) networks. The guidance in this publication focuses on general best practices for event logging and threat detection; however, LOTL techniques feature as they provide a great case study due to the high difficulty in detecting them.

Audience

This guidance is technical in nature and is intended for those within medium to large organisations. As such, it is primarily aimed at:

- senior information technology (IT) and OT decision makers
- IT and OT operators
- network administrators
- critical infrastructure providers.

Best practices

Enterprise-approved event logging policy

Developing and implementing an enterprise approved logging policy improves an organisation's chances of detecting malicious behaviour on their systems and enforces a consistent method of logging across an organisation's environments. The logging policy should take into consideration any shared responsibilities between service providers and the organisation. The policy should also include details of the events to be logged, event logging facilities to be used, how event logs will be monitored, event log retention durations, and when to reassess which logs are worthy of collection.

Event log quality

Organisations are encouraged to implement an event logging policy focused on capturing high-quality cyber security events to aid network defenders in correctly identifying cyber security incidents. In the context of cyber security incident response and threat detection, event log quality refers to the types of events collected rather than how well a log is formatted. Log quality can vary between organisations due to differences in network environments, the reason behind the need to log, differences in critical assets and the organisation's risk appetite.

Useful event logs enrich a network defender's ability to assess security events to identify whether they are false positives or true positives. Implementing high-quality logging will aid network defenders in discovering LOTL techniques that are designed to appear benign in nature.

Note: Capturing a large volume of well-formatted logs can be invaluable for incident responders in

forensics analysis scenarios. However, organisations are encouraged to properly organise logged data into 'hot' data storage that is readily available and searchable, or 'cold' data storage that has deprioritised availability and is stored through more economical solutions – an important consideration when evaluating an organisation's log storage capacity.

For more information on how to prioritise collection of high-quality event logs please refer to CISA's Guidance for Implementing M-21-3: Improving the Federal Government's Investigative and Remediation Capabilities[1].

To strengthen detection of malicious actors employing LOTL techniques, some relevant considerations for event logging include:

- On Linux-based systems, logs capturing the use of curl, systemctl, systemd, python and other common LOLBins leveraged by malicious actors.
- On Microsoft Windows-based systems, logs capturing the use of wmic.exe, ntdsutil.exe, Netsh, cmd.exe, PowerShell, mshta.exe, rundll32.exe, resvr32.exe and other common LOLBins leveraged by malicious actors. Ensure that logging captures command execution, script block logging and module logging for PowerShell, and detailed tracking of administrative tasks.
- For cloud environments, logging all control plane operations, including API calls and end user logins. The control plane logs should be configured to capture read and write activities, administrative changes, and authentication events.

Captured event log details

As a part of an organisation's event logging policy, captured event logs should contain sufficient detail to aid network defenders and incident responders. If a logging solution fails to capture data relevant to security, its effectiveness as a cyber security incident detection capability is heavily impacted.

The *US Office of Management and Budget's M-21-31*[2] outlines a good baseline for what an event log should capture, if applicable:

- properly formatted and accurate timestamp (millisecond granularity is ideal)
- event type (status code)
- device identifier (MAC address or other unique identifier)
- session/transaction ID
- autonomous system number
- source and destination IP (includes both IPv4 and IPv6)
- status code
- response time
- additional headers (e.g. HTTP headers)
- the user ID, where appropriate
- the command executed, where appropriate
- a unique event identifier to assist with event correlation, where possible.

Note: Where possible, all data should be formatted as 'key-value-pairs' to allow for easier extraction.

1 While the audience for the cited guidance is U.S. Federal Civilian Executive Branch agencies, it may provide useful guidance to all entities regarding logging best practices.

2 While only binding on US federal information systems, excluding national security systems, this memorandum may provide useful guidance to all entities regarding logging best practices.

Operational Technology considerations

Network administrators and network operators should take into consideration the OT devices within their OT networks. Most OT devices use embedded software that is memory and/or processor constrained. An excessive level of logging could adversely affect the operation of those OT devices. Additionally, such OT devices may not be capable of generating detailed logs, in which case, sensors can be used to supplement logging capabilities. Out-of-band log communications, or generating logs based on error codes and the payloads of existing communications, can account for embedded devices with limited logging capabilities.

Additional resources

The following resources include examples of details to be logged:

- ASD's ACSC Information Security Manual (ISM) provides event log details to record in the Guidelines for System Monitoring.
- CISA's *Guidance for Implementing M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities* details another approach to prioritising log collection and is aimed at US federal civilian executive branch organisations.
- NIST has outlined OT considerations for event logging in their Guide to Operational Technology (OT) Security.
- For examples of detection uses cases, consider visiting the MITRE ATT&CK® list of data sources.

Content and format consistency

When centralising event logs, organisations should consider using a structured log format, such as JSON, where each type of log captures and presents content consistently (that is, consistent schema, format and order). This is particularly important when event logs have been forwarded to a central storage facility as this improves a network defender's ability to search for, filter and correlate event logs. Since logs may vary in structure (or lack thereof), implementing a method of automated log normalisation is recommended. This is an important consideration for logs that can change over time or without notice such as software and Software-as-a-Service (SaaS) logs.

Timestamp consistency

Organisations should consider establishing an accurate and trustworthy time source and use this consistently across all systems to assist network defenders in identifying connections between event logs. This should also include using the same date-time format across all systems. Where possible, organisations should use multiple accurate time sources in case the primary time source becomes degraded or unavailable. Note that, particularly in distributed systems, time zones and distance can influence how timestamps read in relation to each other. Network owners, system owners and cyber security incident responders are encouraged to understand how this could impact their own environments. ASD's ACSC and co-authors urge organisations to consider implementing the recommendations below to help ensure consistent timestamp collection.

- Time servers should be synchronised and validated throughout all environments and set to capture significant events, such as device boots and reboots
- Using Coordinated Universal Time (UTC) has the advantage of no time zones as well as no daylight savings, and is the preferred time standard.
    - Implement ISO 8601 formatting, with the year listed first, followed by the month, day, hour, minutes, seconds, and milliseconds (e.g. 2024-07-25T20:54:59.649Z).
- Timesharing should be unidirectional. The OT environment should sychronise time sync with the IT environment and not the other way around.

- Data historians may be implemented on some operational assets to record and store time-series data of industrial processes running on the computer system. These can provide an additional source of event log data for OT networks.

Additional resources

- ASD's ACSC has released Windows Event Logging and Forwarding guidance that details important event categories and recommendations for configurations, log retention periods and event forwarding.
- For more information about logging, please explore CISA's Logging Made Easy (LME), a no-cost solution providing essential log management for small to medium-sized organisations, on CISA's website or GitHub page.
- The Joint SIGINT Cyber Unit (JSCU) of the AIVD and MIVD has published a repository on GitHub with a Microsoft Windows event logging and collections baseline focused on finding balance between forensic value and optimising retention. You can find this repository on the JSCU's GitHub.

Event log retention

Organisations should ensure they retain logs for long enough to support cyber security incident investigations. Default log retention periods are often insufficient. Log retention periods should be informed by an assessment of the risks to a given system. When assessing the risks to a system, consider that in some cases, it can take up to 18 months to discover a cyber security incident and some malware can dwell on the network from 70 to 200 days before causing overt harm.[3] Log retention periods should also be compliant with any regulatory requirements and cyber security frameworks that may apply in an organisation's jurisdiction. Logs that are crucial in confirming an intrusion and its impact should be prioritised for longer retention.

It is important to review log storage allocations, in parallel with retention periods. Insufficient storage is a common obstacle to log retention. For example, many systems will overwrite old logs when their storage allocation is exhausted. The longer that logs can be kept, the higher the chances are of determining the extent of a cyber security incident, including the potential intrusion vectors that require remediation. For effective security logging practices, organisations should implement data tiering such as hot and cold storage. This ensures that logs can be promptly retrieved to facilitate querying and threat detection.

Centralised log collection and correlation

The following sections detail prioritised lists of log sources for enterprise networks, OT, cloud computing and enterprise mobility using mobile computing devices. The prioritisation takes into consideration the likelihood that the logged asset will be targeted by a malicious actor, as well as the impact if the asset were to be compromised. It also prioritises log sources that can assist in identifying LOTL techniques. Please note that this is not an exhaustive list of log sources and their threats, and their priority may differ between organisations.

Logging priorities for enterprise networks

Enterprise networks face a large variety of cyber threats. These include malware, malicious insiders, and exploitation of unpatched applications and services. In the context of LOTL, enterprise networks provide malicious actors with a wide variety of native tools to exploit.

ASD's ACSC and co-authors recommend that organisations prioritise the following log sources within their enterprise network:

1. critical systems and data holdings likely to be targeted

3 CISA's "First 48": What to Expect When a Cyber Incident Occurs

2. internet-facing services, including remote access, network metadata, and their underlying server operating system
3. identity and domain management servers
4. any other critical servers
5. edge devices, such as boundary routers and firewalls
6. administrative workstations
7. highly privileged systems such as configuration management, performance and availability monitoring (in cases where privileged access is used), Continuous Integration/Continuous Delivery (CI/CD), vulnerability scanning services, secret and privilege management
8. data repositories
9. security-related and critical software
10. user computers
11. user application logs
12. web proxies used by organisational users and service accounts
13. DNS services used by organisational users
14. email servers
15. DHCP servers
16. legacy IT assets (that are not previously captured in critical or internet-facing services)

ASD's ACSC and co-authors recommend organisations monitor lower priority logs as well. These include:

- underlying infrastructure, such as hypervisor hosts
- IT devices, such as printers
- network components such as application gateways.

Logging priorities for operational technology

Historically, IT and OT have operated separately and have provided distinct functions within organisations. Advancements in technology and digital transformation have led to the growing interconnectedness and convergence of these networks. Organisations are integrating IT and OT networks to enable the seamless flow of data between management systems and industrial operations. Their integration has introduced new cyber threats to OT environments. For example, malicious actors can access OT networks through IT networks by exploiting unpatched vulnerabilities, delivering malware, or conducting denial-of-service campaigns to impact critical services.

ASD's ACSC and co-authors recommend that organisations prioritise the following log sources in their OT environment:

1. OT devices critical to safety and service delivery, except for air-gapped systems[4]
2. internet-facing OT devices
3. OT devices accessible via network boundaries.

4 The prioritised list focuses on logs that enable the detection of a malicious actor operating remotely. In this context, collecting logs from an air-gapped system is not a high priority unless malicious insiders are a concern.

Note that in cases where OT devices do not support logging, device logs are not available, or are available in a non-standard format, it is good practice to ensure network traffic and communications to and from the OT devices are logged.

Logging priorities for enterprise mobility using mobile computing devices

Enterprise mobility is an important aspect of an organisation's security posture. Mobile device management (MDM) solutions allow organisations to manage the security of their enterprise mobility, typically including logging functionality. In the context of enterprise mobility, the aim of effective event logging is to detect compromised accounts or devices; for example, due to phishing or interactions with malicious applications and websites.

ASD's ACSC and co-authors recommend organisations prioritise the following log sources in their enterprise mobility solution:

1. web proxies used by organisational users
2. organisation operated DNS services
3. device security posture of organisationally managed devices
4. device behaviour of organisationally managed devices
5. user account behaviour such as sign-ins
6. VPN solutions
7. MDM and Mobile Application Management (MAM) events[5].

Additional monitoring should be implemented in collaboration with the telecommunications network provider. Such monitoring includes:

- signalling exploitation
- binary/invisible SMS
- CLI spoofing
- SIM/eSIM activities such as SIM swapping
- null cipher downgrade
- connection downgrade (false base station)
- network API/query against user
- roaming traffic protection
- roaming steering.

Organisations should obtain legal advice about what can be logged from any personally owned mobile devices that are enrolled in an MDM solution. For example, logging GPS location may be subject to restrictions.

Logging priorities for cloud computing

ASD's ACSC and co-authors recommend organisations adjust event logging practices in accordance with the cloud service that is administered, whether Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), or SaaS are implemented. For example, IaaS would include a significant amount of logging responsibility on the tenant, whereas SaaS would place a significant amount of the logging

5 MDM and MAM events are likely to be server-sent events, but they may also be generated by software deployed to the mobile device.

responsibility on the provider. Therefore, organisations should coordinate closely with their cloud service provider to understand the shared-responsibility model in place, as it will influence their logging priorities. Logging priorities will also be influenced by different cloud computing service models and deployment models (that is, public, private, hybrid, community). Where privacy and data sovereignty laws apply, logging priorities may also be influenced by the location of the cloud service provider's infrastructure. See NSA's Manage Cloud Logs for Effective Threat Hunting guidance for additional information.

Organisations should prioritise the following log sources in their use of cloud computing services:

1. critical systems and data holdings likely to be targeted
2. internet-facing services (including remote access) and, where applicable, their underlying server operating systems
3. use of the tenant's user accounts that access and administer cloud services
4. logs for administrative configuration changes
5. logs for the creation, deletion and modification of all security principals, including setting and changing permissions
6. authentication success and/or failures to third party services (e.g. SAML/OAuth)
7. logs generated by the cloud services, including logs for cloud APIs, all network-related events, compliance events and billing events.

Secure storage and event log integrity

ASD's ACSC and co-authors recommend that organisations implement a centralised event logging facility such as a secured data lake to enable log aggregation and then forward select, processed logs to analytic tools, such as security information and event management (SIEM) solution and extended detection and response (XDR) solutions. Many commercially available network infrastructure devices have limited local storage. Forwarding event logs to a centralised and secure storage capability prevents the loss of logs once the local device's storage is exhausted. [CPG 2.U] This can be further mitigated by ensuring default maximum event log storage sizes are configured appropriately on local devices. In the event of a cyber security incident, an absence of historical event logs will frequently have a negative impact on cyber security incident response activities.

Secure transport and storage of event logs

ASD's ACSC and co-authors recommend that organisations implement secure mechanisms such as Transport Layer Security (TLS) 1.3 and methods of cryptographic verification to ensure the integrity of event logs in-transit and at rest. Organisations should prioritise securing and restricting access to event logs that have a justified requirement to record sensitive data.

Protecting event logs from unauthorised access, modification and deletion

It is important to perform event log aggregation as some malicious actors are known to modify or delete local system event logs to avoid detection and to delay or degrade the efficacy of cyber security incident response. Logs may contain sensitive data that is useful to a malicious actor. As a result, users should only have access to the event logs they need to do their job.

An event logging facility should enable the protection of logs from unauthorised modification and deletion. Ensure that only personnel with a justified requirement have permission to delete or modify event logs and view the audit logs for access to the centralised logging environment. The storage of logs should be in a separate or segmented network with additional security controls to reduce the risk of logs being tampered with in the event of network or system compromise. Events logs should also be

backed up and data redundancy practices should be implemented.

Organisations are encouraged to harden and segment their SIEM solutions from general IT environments. SIEMs are attractive targets for malicious actors because they contain a wealth of information, provide an analysis function, and can be a single point of failure in an organisation's detection capability. Organisations should consider filtering event logs before sending them to a SIEM or XDR to ensure it is receiving the most valuable logs to minimise any additional costs or capacity issues.

Centralised event logging enables threat detection

The aggregation of event logs to a central logging facility that a SIEM can draw from enables the identification of:

- deviations from a baseline
  - A baseline should include installed tools and software, user account behaviour, network traffic, system intercommunications and other items, as applicable. Particular attention should be paid to privileged user accounts and critical assets such as domain controllers.
  - A baseline is derived by performing an analysis of normal behaviour of some user accounts and establishing 'always abnormal' conditions for those same accounts.
- cyber security events
  - For the purpose of this document, a cyber security event is an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.
- cyber security incidents
  - For the purpose of this document, a cyber security incident is an unwanted or unexpected cyber security event, or a series of such events, that either has compromised business operations or has a significant probability of compromising business operations.

Timely ingestion

Timely ingestion of event logs is important in the early detection of a cyber security events and cyber security incidents. If the generation, collection and ingestion of event logs is delayed, the organisation's ability to identify cyber security incidents is also delayed.

Detection strategy for relevant threats

Detecting living off the land techniques

ASD's ACSC and co-authors recommend that organisations consider implementing user and entity behavioural analytics capabilities to enable automated detection of behavioural anomalies on networks, devices, or accounts. SIEMs can detect anomalous activity by comparing event logs to a baseline of business-as-usual traffic and activity. Behavioural analytics plays a key role in detecting malicious actors employing LOTL techniques. Below is a case study that shows how threat actors leveraged LOTL to infiltrate Windows-based systems.

Case study – Volt Typhoon

Since mid-2021, Volt Typhoon has targeted critical infrastructure organisations by relying almost exclusively on LOTL techniques. Their campaign has been enabled by privately-owned SOHO routers, infected with the 'KV Botnet' malware.

Volt Typhoon uses PowerShell, a command and scripting interpreter, to:

- discover remote systems [T1059.001, T1018]
- identify associated user and computer account names using the command `Get-EventLog security -instanceid 4624` [T1033]
- enumerate logs to search for successful logons using *wevtutil.exe* and the command `Get-EventLog Security` [T1654].

Volt Typhoon consistently obtains valid credentials by extracting the Active Directory database file NTDS.dit[6]. To do so, Volt Typhoon has been observed to:

- execute the Windows-native `vsssadmin` command to create a volume shadow copy [T1006]
- use Windows Management Instrumentation Console (WMIC) commands [T1047] to execute *ntdsutil.exe* to copy NTDS.dit and the SYSTEM registry from the volume shadow copy
- move laterally to the Microsoft Active Directory Domain Services (AD DS) domain controller via an interactive RDP session using a compromised user account with domain administrator privileges [T1021.001].

Other LOTL techniques that Volt Typhoon has been observed to use includes:

- accessing hashed credentials from the Local Security Authority SubSystem Service (LSASS) process memory space [T1003.001]
- using *ntdsutil.exe* to create installation media from Microsoft AD DS domain controllers, either remote or locally, which contain username and password hashes [T1003.003]
- using PowerShell, WMIC, and the `ping` command, to facilitate system discovery [T1018]
- using the built-in `netsh portproxy` command to create proxies on compromised systems to facilitate access [T1090].

While Volt Typhoon uses LOTL techniques to make detection more difficult, the behaviours that the malware exhibits would be considered abnormal compared to business-as-usual activity and could be used to create detection use cases.

For more information, consider visiting MITRE ATT&CK®'s Volt Typhoon page and the MITRE ATT&CK framework.

Examples of anomalous behaviour can include:

- a user logging in during unusual hours (e.g. non-working hours, holidays or on leave)
- an account accessing services that it does not usually access; for example, administrator or HR services
- a user logging in using an unusual device

6 NTDS.dit contains usernames, hashed passwords, and group memberships for all domain accounts, allowing for full domain compromise if the hashes can be cracked offline.

- a high volume of access attempts
- instances of impossible travel[7] or concurrent sign-ins from multiple geographic locations
- downloading or exporting a large volume of data[8]
- network logins without defined computer access or physical access log validation
- a single IP address attempting to authenticate as multiple different users
- the creation of user accounts, or disabled accounts being re-enabled, especially accounts with administrative privileges
- netflow data indicating one device talking to other internal devices it normally does not connect to
- unusual script execution, software installation, or use of administrative tools
- unexpected clearing of logs
- an execution of the process from an unusual or suspicious path
- configuration changes to security software, such as Windows Defender, and logging management software.

Note that the above items could be legitimate behaviour and not malicious activity. In these instances, further investigation by a network defender is required to determine if they are, in fact, evidence of a cyber security event.

To detect threats on endpoints such as user devices, organisations should consider implementing an endpoint detection and response solution. These solutions enable an organisation to monitor malicious activity, such as malicious actors disabling security monitoring services, and process creation events with enhanced detail and fidelity.

By following the guidance in this publication to improve the collection and centralisation of event logs, it will improve an organisation's ability to undertake effective threat hunting to proactively investigate LOTL compromises. Organisations should consider conducting threat hunting on their networks as a proactive measure to detect cyber security incidents. This is a particularly effective activity for detecting malicious actors employing LOTL techniques.

Organisations may also consider the following methods to increase the effectiveness of detecting potential LOTL techniques:

- Always enable detailed logging that includes process creation events and command-line auditing. This enhances log visibility and facilitates threat hunting, if needed.
- Establish a baseline for the usage of legitimate binaries within the organisation and flag any anomalous behaviour.
- Create specific SIEM detection rules based on the evolving threat landscape for different operating systems. For example, *powershell.exe, cmd.exe, regedit.exe* for Microsoft Windows, or *curl, systemctl* and *python* for Linux, with encoded commands.

7 Impossible travel occurs when a user logs in from multiple IP addresses that are a significant geographic distance apart (i.e. a person could not realistically travel between the geographic locations of the two IP addresses during the time period between the logins).

8 Large/continuous data exports should be alerted by default.

Cloud considerations

The joint-sealed publication Identifying and Mitigating Living Off the Land Techniques contains detailed detection guidance for cloud environments. One point states that if machine learning-powered detection capabilities are available within cloud provider security services, organisations should consider leveraging these capabilities and provide log data in real time from multiple sources to enhance log analysis. Using machine learning allows for the detection of anomalous behaviours that may indicate malicious activity. These include irregular API call patterns (especially those that involve changes to security groups, configuration of cloud resources or access to sensitive data), unusual cloud storage access and atypical network traffic.

Operational technology considerations

Effective detection in an OT environment typically involves expertise from both IT and OT personnel; thus, an effective network security instrumentation involves collaborative efforts from both parties. This collaborative approach helps ensure that network defenders can quickly investigate relevant issues, and OT experts can raise operational concerns that may be tied to a cyber security incident. Furthermore, network defenders should leverage real-time alerts to determine any abnormal activity on an OT network. These alerts can include safety data, availability data, logins, failed logins[9], configuration changes, and network access and traffic. Organisations may need to consider whether alerts for OT environments should be approached differently. For example, OT devices may be in remote or hard-to-reach locations.

For detecting anomalous behaviour in OT environments, look for:

- unexpected use of engineering and configuration tools
- abnormal use of vendor or third-party accesses, maintenance methods, or remote monitoring
- unauthorised updates or changes to operating systems, software, firmware, configurations, or databases
- unexpected communication between the control system and external network or unusual communication between components that do not usually communicate
- execution of scripts that are not part of regular operations.

Intrusion detection and intrusion prevention systems (IDS/IPS) are often designed with rules based on IT protocols; therefore, they may be more useful in OT operation systems or the OT demilitarised zone (DMZ) than in supervisory and process areas. Note, it is not recommended to deploy an IPS unless it is tailored to the OT environment, or is outside of critical process control. IPS risk interrupting critical OT devices.

9 Note that not all successful authentication events will be benign; e.g. credential theft or malicious insiders.

Additional guidance

For further guidance, consider visiting:

- Joint-sealed Identifying and Mitigating Living Off the Land Techniques
- ASD ACSC's Windows Event Logging and Forwarding
- CISA's Guidance for Implementing M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities
- CISA's SCuBA TRA and eVRF Guidance Documents
- NSA's Cyber Event Forwarding Guidance
- NCSC-UK's What exactly should we be logging?
- NIST's SP 800-92 Rev. 1, Cybersecurity Log Management Planning Guide
- NIST's Guide to Operational Technology (OT) Security
- US White House's M-21-31
- Malcolm | A powerful, easily deployable network traffic analysis tool suite
- MITRE ATT&CK®'s Data Sources

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre