Priority logs for SIEM ingestion: practitioner guidance

Australian Government

Australian Signals Directorate

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

NISC

内閣サイバーセキュリティセンター

National center of Incident readiness and Strategy for Cybersecurity

JPCERT CC®

National Cyber and Information Security Agency

NÚKIB

The authors would like to acknowledge the industry partners that contributed to this publication.

Table of contents

Introduction

In this publication, the authoring agencies provide cyber security practitioners with detailed recommendations on the logs that should be prioritised for ingestion by a Security Information and Event Management (SIEM) platform. The recommendations in this publication should be treated as generic advice; each organisation should tailor the collection, centralisation, and analysis of logs to its specific environment and risk profile. Practitioners should also adopt an approach of gradually building up the number and types of data sources ingested by the SIEM, rather than adding them all at once. The authoring agencies recommend referring to vendor specific guidance where available for information tailored to each operating system.

This publication is therefore generally intended for the team/s responsible for establishing and maintaining their organisation's SIEM. However, a hunt or blue team can also use its guidance on priority event IDs as a starting point to search for adversary activity or build a baseline of business-as-usual activity on the organisation's network.

Note on terminology: All SIEM platforms have a log ingestion function. Some Security Orchestration, Automation, and Response (SOAR) platforms also perform this function, or have an in-built SIEM. If your organisation uses a SOAR platform with an in-built SIEM, the following recommendations will be relevant to its ingestion of logs.

This series of documents

This publication is one of three in a suite of guidance on SIEM/SOAR platforms:

Implementing SIEM and SOAR platforms: Executive guidance

This document is primarily intented for executives. It defines SIEM/SOAR platforms, outlines their benefits and challenges, and provides broad recommendations for implementation that are relevant to executives.

Implementing SIEM and SOAR platforms: Practitioner guidance

This document is intended for cyber security practitioners. In greater technical details, it defines SIEM/SOAR platforms, outlines the benefits and challenges, and provides best practice principles for implementation.

Priority logs for SIEM ingestion: Practitioner guidance

This document is intended for cyber security practitioners and provides detailed, technical guidance on the logs that should be prioritised for SIEM ingestion. It covers log sources including Endpoint Detection and Response tools, Windows/Linux operating systems, and Cloud and Network Devices.

This guidance should be read alongside Best Practices for Event Logging and Threat Detection, which provides high-level recommendations on developing a logging strategy.

Risk considerations

As above, logging decisions should be based on the organisation's specific environment and risk profile. While the below recommendations provide a starting point, it is critical that organisations model their threats and risks and select data sources most relevant to their risk profile. For each data source, your organisation should assess:

- its purpose or use case – the authoring agencies discourage logging for the sake of logging
- its prioritisation– higher priority data sources should be ingested into new SIEM deployments first and their health should be regularly checked. This document provides a suggested order of prioritisation by broad category of data source
- the volume of logs it may generate. For example, the volume of firewall or Domain Name System (DNS) logs may overshadow the importance of the information received
- its analytical value. For example, high volume data sources may be queried for anomalies in timing. They may also be queried for correlations against other data sources (for instance, analysing high volume firewall logs against threat intelligence-identified malicious IP addresses).

Architectural considerations

A key premise of this publication is that the architecture of logging involves a two-stage process:

1. log creation, collection, and transfer to a centralisation point
2. ingestion of those logs by the SIEM, either directly from the source or from the centralisation point.

Organisations are likely to have legal or regulatory reasons for logging a variety of sources and sending these logs to a centralised location. However, the authoring agencies strongly discourage using a SIEM as the central repository for all logs. A SIEM should only be used for centralisation of specific security logs according to the organisation's risk profile.

Prioritised logging list

This document presents tables of logging events in a loose prioritisation by category of data source. The logging tables are not intended to be complete, nor is the order applicable to every organisation. The authoring agencies recommend that organisations treat the following prioritisation as a starting point for a typical enterprise network environment. Organisations may need to account for log reliability, the visibility each log or log type provides, the potential performance impacts of ingest, and the organisational cost of maintaining, as well as analysing this data, them. Organisations may also need to adjust the prioritisation based on their unique threats, capabilities, and needs.

For Active Directory (AD) event IDs, group policy changes have been included as an additional reference at the end of this document.

Priority logs for SIEM ingestion footnote legend

The following authoring agency documents are referenced within this document and presented as footnotes throughout the document:

CCST – Cloud Computing Security for Tenants | Cyber.gov.au
https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/cloud-security-guidance/cloud-computing-security-tenants

CCSCSP – Cloud Computing Security for Cloud Service Providers | Cyber.gov.au
https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/cloud-security-guidance/cloud-computing-security-cloud-service-providers

DMADC – Detecting and mitigating Active Directory compromises | Cyber.gov.au
https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/detecting-and-mitigating-active-directory-compromises

WELF – Windows Event Logging and Forwarding | Cyber.gov.au
https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-monitoring/windows-event-logging-and-forwarding

HMWW – Hardening Microsoft Windows 10 and Windows 11 Workstations | Cyber.gov.au
https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/hardening-microsoft-windows-10-and-windows-11-workstations

Detailed logging guidance

The following categories of data source are loosely in order of prioritisation.

1. Endpoint detection and response (EDR) logs

Endpoint Detection and Response (EDR) Logs		
Category	**Subcategory**	**Event**
AmCache	Registry file used during process creation	All
Antivirus	Signature detection	All
	Reputational alert	All
	Other detections	All
Network Connections & Ports	Ports (recent or active)	All
	Protocols (recent or active)	All
	IPs (recent or active)	All
Dynamic-Link Libraries	Wrong path DLLs	All
Scheduled Tasks	Existing	Modification
	Creation	All
File Events	Unsuccessful unauthorised file access attempts	All
	Execution	All
	Downloads	All
File system changes	User profile creation	All
	User profile registry keys	Modification
	User profile files	Modification
System Information	System name	All
	Hostname	All
	Timestamp	All
	Timezone	All
	OS info	All
	Processor	All
DNS Cache	Domain name resolution	All
	Network connections.	All
Windows Registry	Last modified time	All
	Modifications	All
	Hive location	All

Endpoint Detection and Response (EDR) Logs		
Category	**Subcategory**	**Event**
Windows Services	Service name	All
	Description name	All
	Service description	All
	PID	All
	Path	All
	Arguments	All
	Service status	All
	Service type	All
	ServiceDLL	All
	Registry key last modified timestamp	All
Command History	Recently run commands	All
Prefetch	System boot	All
	Applications launched	All
Alternate Data Streams	Any	All
Browser History	Typed URL cache	All
ShimCache	PE file metadata	Modification
Shellbags	GUI preferences	All
Registry	Registry Modification	All
LNK Files	Shortcut Execution	Creation/Modification
Background Activity Moderator (BAM)	Process activity	Modification
Jump Lists	Execution	Creation/Modification

2. Network device logs

Network Device Logs		
Function	**Subcategory**	**Event**
Firewall	Ingress data flows	Denied
	Egress	Denied
	Egress	Allowed
	Ingress (Optional)	Allowed
	Running-state	Modification
	Configuration	Modification
	Configuration read/dump	All
	Authentication and authorisation	All
	System change events	All
Core Routers/Switches	Ingress	NetFlow
	Authentication and authorisation	All
	Egress	NetFlow
	Running-state	Modification
	System change events	All
	Configuration read/dump	All
	Configuration	Modification
Routers/Switches	Routing Table	Modification
	Authentication and authorisation	All
	Critical servers/services (subnets - VLANs)	NetFlow
	Admin/IT security (subnets – VLANs)	NetFlow
	Development subnets and VLANs	NetFlow
	Running-state	Modification
	System change events	All
	Configuration read/dump	All
	Configuration	Modification
Intrusion Detection/Prevention Systems	Security alerts	Notification
	Authentication and authorisation	All
	Running-state	Modification
	Authentication and authorisation	All
	System change events	All
	Configuration read/dump	All
	Configuration	Modification

Network Device Logs		
Function	**Subcategory**	**Event**
Application Layer Gateways	Content inspection logs	All
	Authentication and authorisation	All
	Running-state	Modification
	System change events	All
	Configuration read/dump	All
	Configuration	Modification
Network Access Controls (NAC)	NAC authentication events	All
Border Firewall	Ingress data flows	Denied
	Authentication and authorisation	All
	Egress	Allowed
	Ingress (Optional)	Allowed
	Running-state	Modification
	Configuration	Modification
	Configuration read/dump	All
	System change events	All
Border Routers / Load Balancers	Ingress	NetFlow
	Authentication and authorisation	All
	Egress	NetFlow
	Running-state	Modification
	System change events	All
	Service/process Restart	All
	Service/process Reload	All
	Configuration read/dump	All
	Configuration	Modification
Web Proxies	Web query logs	All
	Authentication and authorisation	All
	SSL/TLS inspection	All
	Running-state	Modification
	Service/process Restart	All
	Service/process Reload	All
	System change events	All
	Configuration read/dump	All
	Configuration	Modification

Network Device Logs		
Function	**Subcategory**	**Event**
Virtual Private Network (VPN)	Allowed connections	All
	Denied connections	All
	Authentication and authorisation	All
	Configuration read/dump	All
	Running-state	Modification
	System change events	All
	Configuration	Modification
	Configuration read/dump	All
	Timestamp	All
	Event type [CONNECTED, DISCONNECTED, FAILED, or UNKNOWN]	All
	Origin ids	All
	Origin type	All
	User id	All
	Organisation id	All
	Session id	All
	Session type	All
	VPN profile	All
	Public IP	All
	Assigned IP	All
	Connected at	All
	Disconnection reason	All
	Hostname	All
	OS version	All
	VPN version	All
	User agent	All
Mail Appliance	IP and Domain Reputation	All
	Sender	All
	Recipients	All
	Subject Name	All
	Attachment Names	All

3. Microsoft Domain Controller

Please see additional references at the end of this document for the group policy changes relevant to the following event IDs.

Microsoft Domain Controller Log Types		
Category	**Subcategory**	**Event ID**
Account Logon	Audit Credential Validation	4776(S, F)
	Audit Kerberos Authentication Service	**4768**[1](S, F)
	Audit Kerberos Service Ticket Operations	**4769**[2](S, F)
Account Management	**Audit Computer Account Management**[3]	**4741**[4], 4742, 4743
	Audit Other Account Management Events[5]	4739
	Audit Security Group Management[6]	4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4754, 4755, 4756, 4757, 4758, 4764
	DCSync	4928, 4929
	Audit User Account Management[7]	**4675**[8], 4720, 4722, 4723, **4724**[9], 4725, 4726, **4738**[10], **4740**[11], 4767, 4780, 4781, 4794, 5376, 5377

1 For more, see DMADC Table 2, Table 6, Table 10, Table 14.
2 For more, see DMADC Table 1, Table 10.
3 For more, see WELF.
4 For more, see DMADC, Table 4.
5 For more, see WELF.
6 For more, see WELF.
7 For more, see WELF.
8 For more, see DMADC Table 15.
9 For more, see DMADC Table 4.
10 For more, see DMADC Table 2, Table 15.
11 For more, see DMADC Table 3.

Certificate Services	Service failure	**39**[12]
	Service did not start	**40**[13]
	Incompatible SID	**41**[14]
	Certificate export	**70**[15]
	CA Database backup	**4876**[16]
	Certificate Request	**4886**[17]
	Certificate Issued	**4887**[18]
	Template update	**4899** [19]
	Template security updated	**4900**[20]
Detailed Tracking	Audit DPAPI Activity	4695
	Audit Process Creation[21]	**4688**[22], 4696
	Audit Process Termination[23]	4689
	Include command line in process creation events[24]	4688
DS Access	Audit Directory Service Access	4661, **4662**[25]
	Audit Directory Service Changes	**5136**[26] , 5137, 5138, 5139, 5141
Dumping	Shadow copy	**8222**[27]
Federation Services[28]	Configuration change	**307**[29]
	Additional info to support Event ID 307	**510**[30]
	Signing certificate export	**1007**[31]
	Audit log cleared	**1102**[32]
	Token issued	**1200**[33]
	New credential validation	**1202**[34]

12 For more, see DMADC Table 6.
13 For more, see DMADC Table 6, Table 18.
14 For more, see DMADC Table 6, Table 18.
15 For more, see DMADC Table 7.
16 For more, see DMADC Table 7.
17 For more, see DMADC Table 6.
18 For more, see DMADC Table 6.
19 For more, see DMADC Table 6, Table 19.
20 For more, see DMADC Table 6, Table 19.
21 For more, see HMWW.
22 For more, see DMADC Table 5, Table 8.
23 For more, see HMWW.
24 For more, see HMWW.
25 For more, see DMADC Table 8, Table12. See also Detecting using Canaries.
26 For more, see DMADC Table 1, Table 2.
27 For more, see DMADC Table 9.
28 For more, see DMADC Table 12
29 For more, see DMADC Table 12, Table 20.
30 For more, see DMADC Table 12, Table 20.
31 For more, see DMADC Table 12, Table 20.
32 For more, see DMADC
33 For more, see DMADC Table 12, Table 20.
34 For more, see DMADC Table 12, Table 20.

Kerberos	Logon Ticket	4678
	Service Ticket	4679
	Renewed Ticket	**4770**[35]
LDAP	Bind	**2889**[36]
Logon and Logoff	**Audit Account Lockout** [37]	**4625**[38](F)
	Audit Logoff [39]	4634(S), 4647(S)
	Audit Logon [40]	**4624**[41], **4625**[42], **4627**[43], 4634, 4647, **4648**[44], 4779
	Audit Special Logon [45]	4964(S), 4672(S)
Object Access	Audit Kernel Object	**4663**[46](S)
	Audit Other Object Access Events[47]	4671(-), 4691(S), 5148(F), 5149(F), 4698(S), 4699(S), 4700(S), 4701(S), 4702(S), 5888(S), 5889(S), 5890(S)
Privilege Use	Audit Sensitive Privilege Use	**4673**[48](S, F), **4674**[49](S, F), 4985(S, F)
Policy Change	Audit Authentication Policy Change	4670(S), 4706(S), 4707(S), 4716(S), 4713(S), 4717(S), 4718(S), 4739(S), 4864(S), 4865(S), 4866(S), 4867(S)
	Audit Authorisation Policy Change	**4703**[50](S, F)
	Audit Policy Change[51]	4719(S, F)
	Audit Other Policy Change[52]	4719(S, F)

35 For more, see DMADC Table 5.
36 For more, see DMADC Table 3.
37 For more, see HMWW.
38 For more, see DMADC Table 2, Table 3.
39 For more, see WELF.
40 For more, see WELF.
41 For more, see DMADC Table 3, Table 4, Table 5, Table 11.
42 For more, see DMADC.
43 For more, see DMADC Table 11.
44 For more, see DMADC Table 3.
45 For more, see HMWW.
46 For more, see DMADC Table 8, Table 16.
47 For more, see DMADC Table 8, Table 16.
48 For more, see DMADC Table 16.
49 For more, see DMADC Table 6.
50 For more, see DMADC Table 16.
51 For more, see WELF.
52 For more, see WELF.

System	Audit IPsec Driver	4960(S), 4961(S), 4962(S), 4963(S), 4965(S), 5478(S), 5479(S), 5480(F), 5483(F), 5484(F), 5485(F)
	Audit Security State Change	4608(S), 4616(S), 4621(S)
	Audit Security System Extension	4610, 4611, 4614, 4622, **4697**[53]
	Audit System Integrity[54]	4612, 4615, 4618, 5038, 5056, 5061, 5890, 6281, 6410
	Local Security Authority Subsystem Service	**3033**[55], **3063**[56]

4. Active Directory (AD) and Domain Service Security Logs

Please see additional references at the end of this document for the group policy changes relevant to the following event IDs.

Active Directory (AD) and Domain Service Security Logs		
Category	**Subcategory**	**Event ID**
System Integrity	Security event pattern occurred	4618
Logon/Logoff	Replay attack - detected	4649
	Special groups assigned new logon	4964
Directory Service Access	An operation was performed on an object	**4662**[57]
Object Access	Permissions - changed	4670
	Role separation enabled	4897
Privileged Use	Privileged service - called	**4673**[58]
Process Tracking	Protection of auditable protected data was attempted	4694
User Rights[59]	User right - adjusted	**4703**[60]
	User right - assigned	4704
	User right - removed	4705
Domain	New trust created	4706
	Trust removed	4707

53 For more, see DMADC Table 16.
54 For more, see WELF.
55 For more, see DMADC Table 16, Table 18.
56 For more, see DMADC Table 16.
57 For more, see DMADC Table 8, Table 12. See also Detecting using Canaries.
58 For more, see DMADC Table 16.
59 For more, see HMWW.
60 For more, see DMADC Table 16.

Active Directory (AD) and Domain Service Security Logs		
Category	**Subcategory**	**Event ID**
Account Management	Reset of account password	4724
	Domain Policy - changed[61]	4739
Security-enabled Global Group	Member - added	4728
	Member - removed	4729
	Group - change	4737
Security-enabled Local Group	Member - added	4732
	Member - removed	4733
	Group - change	4735
Security-enabled Universal Group	Group - change	4755
	Member - added	4756
	Member - removed	4757
SID History	Account add - success	4765
	Account add - fail	4766
Kerberos	Kerberos policy changed	4713
	TGT authentication ticket requested	**4768**[62]
	Service ticket requested	**4769**[63]
	Pre-authentication failure	**4771**[64]
	Service ticket denied	4821
	Pre-authentication failed using DES or RC4	4824
User Account Management	ACL set - administrators group(s)	4780
	Directory Services Restore Mode - administrator password	4794
NTLM authentication[65]	Failed	4822
OCSP Responder service	Security settings updated	5124
Directory Replication Agent (DRA)	Intersite replication	1102
Directory service object	Directory service object - modified	**5136**[66]
	Directory service object - created	5137
	Directory service object - deleted	5141

61 For more, see WELF.
62 For more, see DMADC Table 6, Table 10, Table 14.
63 For more, see DMADC Table 1, Table 10.
64 For more, see DMADC Table 3.
65 For more, see WELF.
66 For more, see DMADC Table 1, Table 15.

Active Directory (AD) and Domain Service Security Logs		
Category	**Subcategory**	**Event ID**
User Account[67]	User account - disabled	4725
	User account - deleted	4726
	User account - changed[68]	**4738**[69]
	Attempted validation of credentials	4776
Certificate Services	Service failure	**39**[70]
	Service did not start	**40**[71]
	Incompatible SID	**41**[72]
	Certificate export	**70**[73]
	CA Database backup	**4876**[74]
	Certificate Request	**4886**[75]
	Certificate Issued	**4887**[76]
Certificates	Template update	**4899**[77]
	Template security updated	**4900**[78]

5. Microsoft Windows endpoint logs

Please see additional references at the end of this document for the group policy changes relevant to the following event IDs.

Microsoft Windows Endpoint Logs		
Category	**Subcategory**	**Event ID**
Windows Application Event Logs	Process Creation	1 (**Sysmon**[79])
	Crashes (including error messaging)	1001
Windows Task Scheduler Event Logs[80]	Task triggered by computer start-up	118
	Task triggered on logon	119
	Created Task Process	129
	Action started	200

67 For more, see WELF.
68 For more, see HMWW.
69 For more, see DMADC Table 1, Table 15.
70 For more, see DMADC Table 6. For more, see DMADC Table 6
71 For more, see DMADC Table 6
72 For more, see DMADC Table 6
73 For more, see DMADC Table 7.
74 For more, see DMADC Table 7.
75 For more, see DMADC Table 6.
76 For more, see DMADC Table 6.
77 For more, see DMADC Table 6.
78 For more, see DMADC Table 6.
79 For more, see WELF.
80 For more, see WELF.

Microsoft Windows Endpoint Logs		
Category	**Subcategory**	**Event ID**
Windows PowerShell Event Logs[81]	Module Event	**4103**[82]
	Script Block Event	**4104**[83]
	Engine Lifecycle	400
Windows WMI Activity/ Operational Event Logs[84]	ESS Started	5859
	Temporary ESS Started	5860
	ESS To Consumer Binding	5861
	Operation Started	5857
	Client Failure	5858
Windows Security Event Logs	Audit Log Cleared	**1102**[85] [86]
	Local Security Authority (LSA) - authentication package loaded	4610
	LSA - trusted logon process registered	4611
	Security Account Manager - notification package loaded	4614
	LSA - security package loaded	4622
	Account Logon[87] **- Success**	**4624**[88]
	Account Logon[89] **- Failure**	**4625**[90]
	Account Logon - explicit credentials	4648
	Object handle - request	**4656**[91]
	Object access - Failure	**4663**[92]
	Special privileges -new logon	**4672**[93]
	New process - created	4688
	Service - installed	**4697**[94], 7045
	Scheduled task - created[95]	4698
	Scheduled task - updated[96]	4702

81 For more, see WELF.
82 For more, see DMADC Table 5, Table 7, Table 8, Table 13, Table 14, Table 15, Table 16.
83 For more, see DMADC Table 5, Table 7, Table 8, Table 13, Table 14, Table 15, Table 16.
84 For more, see WELF.
85 For more, see DMADC Table 6, Table 7, Table 8, Table 12, Table 13, Table 14, Table 15, Table 16.
86 PRC state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure | Cyber.gov.au
87 For more, see WELF.
88 For more, see DMADC Table 3, Table 4, Table 5, Table 11.
89 For more, see WELF.
90 For more, see DMADC Table 3, Table 4, Table 5, Table 11.
91 For more, see DMADC Table 8.
92 For more, see DMADC Table 8, Table 16.
93 For more, see DMADC Table 8, Table 16
94 For more, see DMADC Table 16.
95 For more, see WELF.
96 For more, see WELF.

Microsoft Windows Endpoint Logs		
Category	**Subcategory**	**Event ID**
	System security access - granted	4717
	System security access -removed	4718
	System audit policy - changed	4719
	User account - created	**4720**[97]
	User account - enabled	**4722**[98]
	Change to account password (Failure)	4723
	Member - added (Security-enabled Local Group)	4732
	Kerberos Ticket-granting-ticket (TGT) denied	4820
	Special groups assigned new logon	4964
	Object handle closed	4658
	Process exited	4689
	Scheduled task - deleted[99]	4699
	Scheduled task - disabled[100]	4701
AppLocker	Policy incorrectly applied	8000
	Disabled	8008
	Policy changed/applied	8001
	Change of mode (enforcement to audit)	
	EXE or DLL blocked	8004
	Script or Microsoft Software Installer (MSI) blocked	8007
	File was prevented from running	8022, 8025
	Packaged app failure due to lack of Packaged app rules	8027
	Config CI policy prevented file or package from running	8029, 8036, 8040
	ManagedInstaller Script check SUCCEEDED/ FAILED	8032, 8035
Windows Systems Log	Handle scavenged	1017

97 For more, see DMADC Table 8, Table 16
98 For more, see DMADC Table 8, Table 16
99 For more, see WELF.
100 For more, see WELF.

Microsoft Windows Endpoint Logs		
Category	**Subcategory**	**Event ID**
Windows Extensible Storage Engine Technology (ESENT) Application	Database location change	**216**[101]
	New database	325
	Mounting of an NTDS.dit file	326
	Database detachment	327
	New flush map file	**637**[102]
Windows Terminal Services Local Session Manager	New local session	21
	Shell start notification received	22
	Successful session logoff	23
	Session disconnect	24
	Session reconnect	25
Windows Defender Application Control	File was blocked	3077
	Signature	3089

6. Virtualisation system logs

Virtualisation System Logs		
Category	**Subcategory**	**Event**
User Authentication	Logon (Success and Failure)	All
	Privileged Access (Success and Failure)	All
User and Administrator/Root Access and Actions	File and Object Access	All
	Audit Log Access (Success and Failure)	All
	System Access (Failure)	All
System Performance and Operational Characteristics	Resource Utilization	All
	Process Status	
	System Events	All
	Service Status Changes	All
System Configuration	Changes to Security Configuration (Success/ Failure)	All
	Changes to Hypervisor	All
	Changes to VMS	All
	Changes Made within VMS	All
	Audit Log Cleared	All

101 For more, see PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

102 For more, see Joint Guidance: Identifying and Mitigating Living Off the Land Techniques

Virtualisation System Logs		
Category	**Subcategory**	**Event**
Creation of VMS	Source	All
	Target Systems	All
	Time	All
	Authorization	All
Deployment of VMS	Source	All
	Target Systems	All
	Time	All
	Authorization	All
Migration of VMS	Source	All
	Target Systems	All
	Time	All
	Authorization	All
System-Level Objects	Creation and Deletion	All

7. Operational technology logging

Operational Technology (OT) logging integration into a SIEM can be challenging due to the specialised nature of OT systems, which are often vendor-specific and segmented from the environments where the SIEM is typically located. The authoring agencies also note that OT devices often come with limited logging. Where possible, it is recommended that OT devices enable logging and then send and store logs in a centralised location. While implementing a dedicated SIEM specific to the OT environment may be feasible, it would also require staff to develop familiarity with the two systems and event types.

Industrial Control System (ICS) monitoring offers a solution that can safely ingest, interpret, and enrich OT data before either forwarding it to a SIEM or storing it in a central repository. Additionally, these products can monitor OT networks and assets, parse the OT-native protocols, and generate additional logs with necessary details and contextual metadata for events that are going to the SIEM.

In cases where security supersedes other requirements, organisations may implement unidirectional gateways or data diodes to securely transmit log data from the OT environment to the IT SIEM without exposing the OT network to external threats.

Due to the safety-critical risks, high speed and deterministic communications of the messaging, organisations should take a conservative approach to logging directly from OT assets and test any logging solution thoroughly before deployment in order to avoid impacting operations.

8. Cloud platform logging[103, 104]

Cloud services may not be enabled by default. Every application may have its own logging format or no logging at all. The recommendations below are only a sample of what may be logged; organisations should seek out advice from their cloud service provider and cloud application provider for security logging that meets the organisation's security requirements and risk profile.

See Best practices for event logging and threat detection for more on this.

Logging priorities for cloud computing

The authoring agencies 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 software-as-a-service (SaaS) are implemented. For example, IaaS includes a significant amount of logging responsibility on the tenant, whereas SaaS places a significant amount of the logging responsibility on the provider. Therefore, organisations should coordinate closely with their cloud service provider to understand the shared-responsibility model that is in place, as it will likely influence their logging priorities. Logging priorities may also be influenced by different cloud computing service models and deployment models (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 the National Security Agency's Manage Cloud Logs for Effective Threat Hunting[105] guidance for additional information.

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

- critical systems and data holdings likely to be targeted
- internet-facing services (including remote access) and, where applicable, their underlying server operating systems
- use of the tenant's user accounts that access and administer cloud services
- logs for administrative configuration changes
- logs for the creation, deletion and modification of all security principals, including setting and changing permissions
- authentication success and/or failures to third party services (for example Security Assertion Markup Language (SAML)/ Open Authorization (OAuth))
- logs generated by the cloud services, including logs for cloud Application Programming Interface (API/s), all network-related events, compliance events and billing events.

103 For more, see CCSCSP.
104 For more, see CCST.
105 https://media.defense.gov/2024/Mar/07/2003407864/-1/-1/0/CSI_CloudTop10-Logs-for-Effective-Threat-Hunting.PDF

Amazon Web Services logs

Amazon Web Services Logs		
Category	**Subcategory**	**Event**
Amazon Web Services	CloudTrail Logs	All
	Server Access Logs	All
	Web Access to S3 Buckets	All
	Load Balancer Logs	All
	Proxied Web Requests	All
	Breakglass account use	All
	VPC Network Flow Logs	All
Secrets Manager	ListSecrets	All
	GetSecretValue	All
S3	ListBuckets	Errors Only
	ListObjects	Errors Only
	GetObject	Errors Only
	CopyObject	Errors Only
	GetObjectAcl	All
	HeadBucket	All
	HeadObject	All
	PutPublicAccessBlock	All
EC2	CreateKeyPair	All
	ImportKeyPair	All
	CreateSnapshots	All
	RunInstances	All
	DescribeSecurityGroups	All
	ModifySecurityGroupRules	All
	GetPasswordData	All
	GetConsoleScreenshot	All
	DescribeInstanceData	Where Attribute='userdata'
VPC	CreateNatGateway	All
	AttachInternetGateway	All
	CreateInternetGateway	All
	CreateEgressOnlyInternetGateway	All
	CreateVpcPeeringConnection	All
	AcceptVpcPeeringConnection	All

Amazon Web Services Logs		
Category	**Subcategory**	**Event**
EBS direct APIs	GetSnaphotBlock	All
IAM	GetAccountAuthorizationDetails	All
	ListUsers	All
	CreateUser	All
	CreateOpenIDConnectProvider	All
STS	GetCallerIdentity	All
SSM	DescribeParameters	Errors
	GetParameter	Errors
RDS	DescribeDBInstances	All
	DescribeDBClusters	All
DynamoDB	Query	Errors
	Scan	Errors
	ListTables	All
	DescribeTable	Errors
Lambda	GetFunction	All

Critical Azure service and app logs

Critical Azure Service and App Logs		
Category	**Subcategory**	**Event**
*Entra & **Entra Connect Servers***[106]	Unified Audit Log	All
	PHS Failure	**611**[107]
	AD password synchronisation - start	**650**[108]
	AD password synchronisation - finish	**651**[109]
	Password synchronisation	**656**[110]
	Password change request	**657**[111]
	Audit log cleared	**1102**[112]
	PowerShell – Pipeline execution and logs	**4103**[113]
	PowerShell – Scripts & Commands	**4104**[114]

106 For more, see DMADC Table 13.
107 For more, see DMADC Table 13.
108 For more, see DMADC Table 13.
109 For more, see DMADC Table 13.
110 For more, see DMADC Table 13.
111 For more, see DMADC Table 13.
112 For more, see DMADC Table 13.
113 For more, see DMADC Table 13.
114 For more, see DMADC Table 13.

Critical Azure Service and App Logs		
Category	**Subcategory**	**Event**
	Signin Log	All
	Managed Identity Signin Log	All
	Non Interactive User Signin Log	All
	Service Principal Signin Log	All
	ADFS Signin Log	All
Azure Audit Log	Read and Write	All
Azure Storage Container Log	Read and Write	All
Breakglass account use	Any	All
Microsoft Office 365	Unified Audit Log	All
Virtual Machine	Linux Operating System Log (Configured on VM OS)	All
	Windows Operating System Log (Configured on VM OS)	All

Google Cloud Platform (GCP) logs

Google Cloud Platform (GCP) Logs		
Category	**Subcategory**	**Event**
Google Cloud Platform	Access Transparency Logs	All
	Admin Activity Logs	All
	Enterprise Group Audit Logs	All
	Login Audit Logs	All
	System Event Logs	All
	Policy Denied Audit Logs	All
	Storage Bucket Logs	All
	Host VM Logs	All
	Platform Audit Logs	All
	Breakglass account use	All
	VPC Firewall Logs	All
	VPC Network Flow Logs	All

Google Workspace (GWS) logs

Google Workspace (GWS) Logging		
Category	**Subcategory**	**Event**
Google Workspace	Access Transparency Logs	All
	Admin Activity Logs	All
	Context Aware Access	All
	Device events	All
	Directory Sync events	All
	OAuth events	All
	Password Vaulted Apps events	All
	Rules events	All
	SAML events	All
	Secure LDAP events	All
	User Audit events	All
	Chrome events	All
	Drive events	All
	Gmail events	All
	Graduation events	All
	Takeout events	All

9. Container logs

Container Logs		
Category	**Subcategory**	**Event**
Container User Logs	Logon (Success and Failure)	All
	Privileged Access (Success and Failure)	All
Container Service Logs	Audit Log Changes	All
	Audit Log Cleared	All
Container and Application API Audit Logs	File and Object Access	All
	Audit Log Access (Success and Failure)	All
	System Access (Failure)	All
Container Management Access Logs	Logon (Success and Failure)	All
	Changes to Container RBAC	All
	Service Status Changes	All

Container Logs		
Category	**Subcategory**	**Event**
Container Resources	Security Configuration Changes	All
	Changes to Container	All
	Audit Log Changes	All
	Audit Log Cleared	All
Container Management Environment	Logon (Success and Failure)	All
	Privileged Access (Success and Failure)	All

10. Database Logs

Database Logs		
Category	**Subcategory**	**Event**
User Authentication	Logon (Success and Failure)	All
	Privileged Access (Success and Failure)	All
	User Roles (Changes)	All
User and Administrator Access and Actions	Table and Object Access	All
	New Users / Privileged Users	All
	Privilege Elevation (Success and Failure)	All
	Audit Log Access (Success and Failure)	All
	Executable Commands	All
	Passwords	All
	Database Permissions	All
	CLI Commands	All
Query, Response, and Traceback Characteristics	Query Execution	All
	Method	All
	Comments or Variables	All
	Multiple Embedded Queries	All
	Alerts or Failures	All
	Time to Execute Query	All
System Configuration	Database Structure Changes	All
	Version updates/roll backs	All
	Keys (including access)	All
	User Roles or Database Permissions changes	All

11. Mobile device management

Mobile Device Management		
Category	**Subcategory**	**Event**
Device Data	Device Name Change	All
	Phone Number Change	All
	OS Version Change	All
	Firmware Version Change	All
	Developer Mode Enabled	All
	Device Synched with Enterprise	All
Application Data	Application installation	All
	Application updates	All
	Uninstalled applications	All
	Data storage location	All
	Application permission changes	All
Device Policy Settings	Enrolment Policy (changes)	All
	Applied policies (success/fail)	All
	Authentication Policies changes	All
Device Configuration	Certificate changes	All
	Device encryption configuration changes	All
	Android Enterprise settings changes	All
	System Integrity Status (Failure)	All
Network Configuration	Networks (Allowed/Disallowed)	All
	Proxy/Tunnel	All
	Per-App VPN details	All
	Connected Network	All
	Captive Portal connections	All
	Network MAC Address	All
	Bluetooth connections	All
	Wi-Fi SSID connections	All
Event / Audit / Crash Logs	Event Timestamp	All
	Event Type	All
	User Authentication (Success/Failure)	All
	Various Services (Success/Failure)	All
	Event Actor	All
	Event ID	All
	Event Change Type (CRUD)	All

Mobile Device Management		
Category	**Subcategory**	**Event**
MTD Agent Info	Agent Status	All
	Agent Configuration changes	All
	Threat Detection	All
	MITM Activities	All
	Remediation Actions	All
	Privilege Escalation	All
	Phishing Protection Status	All
	Last Time Device Synched with Enterprise	All

12. Windows DNS server analytic event logs

Windows DNS Server Analytic Event Logs		
Category	**Subcategory**	**Event ID**
DNS Server Analytic	Response success	257
	Response failure	258
	Ignored query	259
	Query out	260
	Response in	261
	Recursive query timeout	262
	Update in	263
	Update response	264
	Update forward	277
	Update response in	278
DNS Server Zone Transfer	DNS Server Zone Transfer successfully completed	6001

13. Linux endpoint auditing logs

Linux Endpoint Auditing Logs		
Category	**Subcategory**	**Event**
Audit	Configuration	Modification
	Log Files	Modification

Linux Endpoint Auditing Logs		
Category	**Subcategory**	**Event**
Audit Tools	Configuration	Modification
	Reading	Access
	Monitoring	Access
User Access	Sensitive directories and binaries (e.g., /sbin)	All
	Authentication mechanisms (e.g., SSH).	Modification
	Authentication/Authorisation configuration change	All
	Login and logout events (/var/log/wtmp).	All
	Session recording	Modification
	Users (+associations), groups (+associations), and passwords	Modification
	SSH Session initiation	All
Privileged Events	Privileged system calls	All
	Sudoers/root privileges	Modification
	Login information	Modification
	Sensitive access control levels (e.g., chmod >= 500).	Modification
	Public/private keys locations (.ssh directory)	All
	Shell History	Modification
	/etc/passwd using auditctl	All
	Auditing of all privileged functions	All
System Events	Trusted databases (e.g., /etc/passwd).	Modification
	Process ID	Modification
	System file deletion	All
	Drive and file mount operations	All
	Start-up scripts and changes	Modification
	Search paths	Modification
	Special files (e.g., attached block devices)	All
	Mount operations	All
	Swap operations	All
	Standard kernel parameters	All
	Loading and unloading of modules	All
	Package (including sources) • Installation • Removal • Reconfiguration	All

Linux Endpoint Auditing Logs		
Category	**Subcategory**	**Event**
	Modification of boot parameters	All
	Modification of mount options	All
	SSSD log files	All
	kexec usage	All
	Cron configurations and logs (/etc/cron and /var/log/cron).	Modification
	Service and system configurations	Modification
File Events	Unsuccessful unauthorised file access attempts	All
Security Events	Common reconnaissance tools e.g. Netcat	All
	Suspicious binaries e.g. code/data/process injections	All
Network Events	Such as hostname changes and connections	All

14. Apple MacOS endpoint logs

Apple MacOS Endpoint Logs		
Category	**Subcategory**	**Event**
Content Caching	com.apple.AssetCache (subsystem)	All/Default
Gatekeeper	Syspolicyd (policy)	All/Default
	com.apple.syspolicy.exec (subsystem)	All/Default
macOS Installer and Software Update	Softwareupdated (policy)	All/Default
	com.apple.mac.install (subsystem)	All/Default
	com.apple.SoftwareUpdate (subsystem)	All/Default
	com.apple.SoftwareUpdateMacController (subsystem)	All/Default
	com.apple.mobileassetd (subsystem)	All/Default
Mobile Device Management (MDM)	Mdmclient (policy)or	All
	com.apple.ManagedClient (subsystem)	All
Networking	com.apple.network (subsystem)	All
	connection (category)	All
	boringssl (category)	All
OCSP (Certificate Validity)	com.apple.securityd (subsystem)	All
	ocsp (category)	All

Apple MacOS Endpoint Logs		
Category	**Subcategory**	**Event**
User and Administrator Access to OS Components and Applications	File and Object Access	All
	Audit Log Access	Success/Failure
	System Access and Log Off	Success/Failure
	Privilege Access and Log Off	Success/Failure
	Sensitive Privilege Use (sudo)	Success/Failure
	Remote Terminal or Equivalent Access and Log Off	Success/Failure
	Samba/NFS/(S)FTP or Equivalent Access	All
	Mac OS X utmpx / wmtp	All
	Audit Daemon	All
	Permissions/Access Violations	All
	Terminal Commands Sessions	All
	SSH Session initiation	All
	Open Directory	
	Terminal Commands History	All
	Installation or Removal of Applications	All
	Installation or Removal of Storage Volumes or Removable Media	All
System Performance and Operational Characteristics	Resource Utilization, Process Status	All
	System Events	All
	Service Status Changes	Start, Stop, Fail, Restart, etc.
	Service Failures and Restarts	All
	Launch Services Daemon	All
	Jamf	All
	Process Creation and Termination	All
System Configuration	Changes to Security Configuration	Success/Failure
	Audit Log Cleared	All
	Changes to Accounts	All
	User or Group Management Changes	All
	Apple Push Notification Service (APNs)	All
	Snapshots DB	Success/Failure
	Syslog format files	All
	Scheduled Task Changes	All

Apple MacOS Endpoint Logs		
Category	**Subcategory**	**Event**
File Access	Transfer to external Media	All
	Transfer to remote Hosts	All
File Sharing	All	All
Host Network Communications	Port	All
	IP address	All
	Active network comms	All
Command-Line Interface (CLI)	System Log Folder: /Var/Log/*	All
	System Log: /Var/Log/System.Log	All
	Mac Analytics Data: /Var/Log/ Diagnosticmessages/*	All
	Wi-Fi Log: /Var/Log/Wifi.Log	All
	System Application Logs: /Library/Logs/* and / Private/Var/Log/*	All
	System Reports: /Library/Logs/ Diagnosticreports/ *	All
	User Application Logs: /Users/Name/Library/ Logs/*	All
	User Reports: /Users/Name/Library/Logs/Diag nosticreports/*	All
	Audit Log: /Var/Audit/*	All
Basic Input Output System (BIOS), Unified Extensible Firmware Interface (UEFI), and Other Firmware	Version	All
	Created date	All
	Installed date	All
	Manufacturer	All
Keychain Events	Public/private keys locations (.ssh directory)	All
XProtect	Detection events and alerts	All
Misc. Logs	As required or determined through risk assessment	All

Reference and resource annex

Active directory group policy changes

The following table lists the Group Policy changes required to generate the specific event IDs within log sources.

Event ID	Group Policy Object
4618	Audit System Integrity
4649	Audit Other Logon/Logoff Events
4964	Audit Special Logon
4662	Audit Directory Service Access
4670	Audit Other Policy Change Events
4897	Audit Certification Services
4673	Audit Sensitive Privilege Use
4694	Audit DPAPI Activity
4703, 4704, 4705, 4706, 4707	Audit Authorization Policy Change
4724, 4739	Audit Account Management
4728, 4729, 4732, 4733, 4735, 4737, 4755, 4756, 4757	Audit Security Group Management
4765 4766	Audit User Account Management
4713	Audit Authentication Policy Change
4768	Audit Kerberos Authentication Service
4769	Audit Kerberos Service Ticket Operations
4771	Kerberos pre-authentication failed
4821	Audit Kerberos Service Ticket Operations
4780, 4794, 4725, 4726, 4738	Audit User Account Management
5141	Audit Directory Service Changes
5124	Protected Users
5136	OCSP Responder Service
70	Not directly related to a Group Policy setting
4876, 4886, 4887	Audit Certification Services
39, 40, 41, 4776, 4824, 4899 4900, 5137	Windows Default

Windows Endpoint Group Policy Changes

The following table lists the Group Policy changes required to generate the specific event IDs within log sources.

Event ID	Group Policy Object
4103	Turn on Module Logging
4104	Turn on PowerShell Script Block Logging
4610, 4611, 4614, 4622	Audit Security System Extension
4624, 4625, 4648	Audit Logon Events
4656, 4663	Audit Object Access
4688	Audit Process Creation
4697	Audit Security System Extension
4698, 4699, 4701, 4702	Audit Other Object Access Events
4717, 4718, 4719	Audit Authentication Policy Change
4720, 4722, 4723	Audit User Account Management Group Policy
4732	Audit Security Group Management
4820	Device-based access control policies
4964	Audit Special Logon
4658	Audit Handle Manipulation
4689	Audit Process Termination
8000, 8004	NTLM auditing settings
8007, 8022, 8025, 8027, 8029, 8032, 8036, 8040, 8035	AppLocker Policies
3077, 3089	Windows Defender Application Control
1, 118, 119, 129, 200, 1001, 1102, 5857, 5858, 5859, 5860, 5861, 7045	Windows Default

Domain Controller Group Policy Changes

The following table lists the Group Policy changes required to generate the specific event IDs within log sources.

Event ID	Group Policy Object
4768, 4769	Audit Kerberos Authentication Service
4741, 4742, 4743	Audit Computer Account Management
4739	Any Security Settings\Account Policies GPO
4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4754, 4755, 4756, 4757, 4758, 4764, 4928, 4929	Audit Detailed Directory Service Replication
4675, 4720, 4722	Audit Logon
4723, 4724, 4725, 4726, 4738, 4767, 4780, 4781, 4794, 5376, 5377	Audit User Account Management
4876, 4886, 4887	Audit Certification Services
4688, 4696	Audit Process Creation
4689	Audit Process Termination
4661, 4662	Audit Directory Service Access
5136, 5137, 5138, 5139, 5141	Audit Directory Service Changes
8222	Security
307	Administrative Templates\Printers
4679	Audit Policy
4770	Audit Kerberos Service Ticket Operations
2889	Network security: LDAP client signing requirements
4634	Audit logoff
4625, 4647	Audit logon events
4624, 4634, 4648	Advanced Audit Policy Configuration
4627	Audit Group Membership
4779	Audit Other Logon/Logoff Events
4964	Audit Special Logon
4672	Special privileges assigned to new logon
4663	Audit object access
4671, 4691, 4698, 4699, 4700, 4701, 4702, 5148, 5149, 5888, 5889, 5890	Audit Other Object Access Events
4673, 4674	Audit Sensitive Privilege Use
4985	Audit File System

Event ID	Group Policy Object
4670, 4707, 4739, 4864	Audit Object Access
4706, 4707, 4713, 4717, 4718, 4865, 4866, 4867	Audit Authentication Policy Change
4703	Audit Authorization Policy Change
4719	Audit Policy Change
4960, 4961, 4962, 4963, 4965, 5478, 5479, 5480, 5483, 5484, 5485	Audit IPsec Driver
4608, 4616, 4621	Audit Security State Change
4610, 4611, 4614, 4622, 4697	Audit Security System Extension
4612, 4615, 4618, 5038, 5056, 5061, 6281, 6410	Audit System Integrity
5890	Audit Other Object Access Events
6410	Code Integrity
3033, 3063	Code Integrity Policies
39, 40, 41, 70, 510, 1007, 1102, 1200, 1202, 4678, 4695, 4740, 4776, 4899, 4900	Windows Default

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre