

SOC Analyst Quick Reference

A practical blue-team quick reference for alert triage, host investigation, Windows/Linux commands, event IDs, and enrichment fields.

DOCUMENT CENTER

Compiled September 2026

Use collection and containment commands only within your authorized environment and according to incident-response procedures. Preserve evidence and document changes when an investigation may become a formal incident.

Use this guide as a practical reference. Verify commands, targets, permissions, paths, versions, and organizational policy before making changes. Examples with placeholders must be adapted to the environment.

Contents

#	Section	Entries
1	Alert triage - first 10 questions	10
2	Windows investigation commands	20
3	Linux investigation commands	20
4	High-value Windows event IDs	19
5	Common enrichment fields	7

Total reference entries: 76

1. Alert triage - first 10 questions

#	Question	Why it matters
1	What exactly fired and what detection logic produced the alert?	Clarifies data source, rule intent, and expected false positives.
2	Which user, host, IP, application, or cloud resource is involved?	Defines principal entities for scope.
3	When did it begin and is it still active?	Sets timeline and urgency.
4	What is normal for this user/host/service?	Separates anomalous from expected activity.
5	What evidence independently corroborates the alert?	Avoids relying on one telemetry source.
6	Was the action successful or blocked?	Determines impact and next steps.
7	What happened immediately before and after?	Builds behavioral context.
8	Are there related alerts, indicators, accounts, or hosts?	Expands or constrains scope.
9	Could this be administrative, automated, or business-approved activity?	Identifies legitimate explanations.
10	What is the safest next action: observe, enrich, contain, or escalate?	Keeps response proportional and evidence-driven.

2. Windows investigation commands

Command	Purpose / Notes
whoami /all	Capture identity, groups, privileges, and token context.
hostname	Identify host name.
systeminfo	Capture OS, boot, hotfix, and general inventory.
ipconfig /all	Capture network configuration.
netstat -ano	Review connections/listeners and PIDs.
tasklist /svc	Map processes to hosted services.
sc queryex type= service state= all	Review services and PIDs.
schtasks /query /fo LIST /v	Review scheduled tasks.
wevtutil el	List event logs.
Get-WinEvent -LogName Security -MaxEvents 100	Review recent Security events.
Get-WinEvent -FilterHashtable @{LogName="Security";Id=4624,4625,4688}	Review logon and process events.
Get-MpComputerStatus	Check Defender health.
Get-MpThreatDetection	Review Defender detection details.
Get-FileHash <file> -Algorithm SHA256	Hash a suspicious file.
Get-AuthenticodeSignature <file>	Inspect Authenticode signature status.
Get-NetTCPConnection	Review TCP connections.
Get-DnsClientCache	Review current DNS cache where supported.
Get-SmbSession	Review SMB server sessions.
Get-SmbOpenFile	Review files opened through SMB server.
qwinsta	Review interactive/RDP sessions.

3. Linux investigation commands

Command	Purpose / Notes
<code>id && whoami</code>	Capture identity context.
<code>hostnamectl</code>	Capture host/OS identity.
<code>uptime</code>	Show uptime/load.
<code>who && w</code>	Review current sessions.
<code>last -n 30</code>	Review recent login history.
<code>lastb -n 30</code>	Review failed login history where available.
<code>ps aux --sort=-%cpu head</code>	Review high CPU processes.
<code>ss -tulpen</code>	Review listening sockets.
<code>ss -tan state established</code>	Review established TCP sessions.
<code>ip -br addr && ip route</code>	Capture interfaces and routes.
<code>systemctl --failed</code>	Review failed services.
<code>journalctl -p warning..alert --since today</code>	Review warning/error journal entries.
<code>journalctl -u ssh --since today</code>	Review SSH service logs.
<code>find /tmp /var/tmp -type f -mtime -1 -ls</code>	Review recently modified temporary files; scope carefully.
<code>sha256sum <file></code>	Hash a file.
<code>stat <file></code>	Review file metadata.
<code>getfacl <file></code>	Review ACLs.
<code>crontab -l</code>	Review current user scheduled cron entries.
<code>sudo crontab -l</code>	Review root crontab where authorized.
<code>systemctl list-timers --all</code>	Review systemd timers.

4. High-value Windows event IDs

ID	Use
1102	Security audit log cleared.
4624	Successful logon.
4625	Failed logon.
4648	Explicit credentials used.
4672	Special privileges assigned.
4688	Process created.
4697	Service installed.
4698	Scheduled task created.
4720	User created.
4724	Password reset attempted.
4728	Member added to global security group.
4732	Member added to local security group.
4740	Account locked out.
4768	Kerberos TGT requested.
4769	Kerberos service ticket requested.
4771	Kerberos pre-authentication failed.
5136	Directory object modified.
5145	Detailed network share access.
7045	Service installed - System log.

5. Common enrichment fields

Entity	Collect / Compare
User	UPN/SAM name, SID, groups, MFA state, sign-in history, password/reset events, usual devices/locations.
Host	Hostname, IP/MAC, OS, owner, EDR state, uptime, criticality, recent logons, processes, network connections.
IP	Internal/external, ASN/provider, geolocation as weak context, prior sightings, reputation, reverse DNS, VPN/proxy/NAT context.
Domain	Registrar/age, DNS records, hosting, certificate/SNI, prior sightings, categorization; avoid treating age/reputation alone as proof.
File	SHA-256, path, signer, compile/metadata context, prevalence, creation/modification times, parent process.
Process	Image path, command line, parent/child chain, user, integrity, network activity, signer, hash.
Alert	Rule logic, data source, suppression, threshold, first/last seen, related alerts, known false-positive conditions.

Authoritative references

Use vendor and standards documentation for exact syntax, current behavior, version-specific details, licensing, and policy requirements.

NIST SP 800-61 Rev. 3

<https://csrc.nist.gov/pubs/sp/800/61/r3/final>

Microsoft Windows Security Event ID Reference

<https://learn.microsoft.com/azure/sentinel/windows-security-event-id-reference>