"Wise Wednesday – Defensive Security Deep Dives"

course deserves a full-stack tool journey from beginner to expert.

Topic : Windows Event Viewer

Table of Contents

Top 50 important Windows Event IDs

Organized by category, with Event ID, Description, and purpose – ideal for monitoring, alerting, and incident analysis.

Who can attend this?

1. Network Administrators
2. System Administrators
3. Security Analysts (SOC Level 1 & 2)
4. Incident Responders
5. Cybersecurity Engineers
6. IT Support Technicians
7. Infrastructure Engineers
8. Helpdesk Analysts
9. Ethical Hackers (for Blue Team understanding)
10. Threat Intelligence Analysts
11. Digital Forensics Investigators
12. Malware Analysts
13. Security Operations Center (SOC) Managers
14. IT Auditors
15. Compliance Officers (IT Security domain)

16. Cloud Security Engineers
17. Endpoint Security Specialists
18. Penetration Testers (Defensive crossover)
19. DevSecOps Engineers
20. Security Consultants
21. Risk Management Professionals
22. IT Trainers / Security Educators
23. Technical Project Managers (Cyber/IT domain)
24. Blue Team Enthusiasts / Career Switchers
25. **College Students** pursuing Computer Science, IT, or Cybersecurity

Security Log – Account Logon & Logon Events

Event ID	Description	Purpose / Detection Use
4624	Successful logon	Track valid logins (interactive, remote, network).
4625	Failed logon	Detect brute-force or password spray attacks.
4634	Logoff event	Monitor user session termination.
4647	User initiated logoff	Detect manual logoff actions.
4648	Logon with explicit credentials	Track credential use (RunAs, service logins).
4672	Special privileges assigned	Detect admin privilege assignments.
4776	NTLM authentication attempted	Monitor legacy authentication use.
4768	Kerberos TGT requested	Baseline normal Kerberos authentication.
4769	Kerberos service ticket requested	Monitor service access patterns.
4771	Kerberos pre-auth failed	Identify wrong passwords / brute-force on domain accounts.
4627	Group membership info	Capture user group memberships on logon.

System & Policy Changes

Event ID	Description	Purpose / Detection Use
4719	System audit policy changed	Detect changes in security auditing.
4739	Domain policy changed	Detect modification of domain-level security policies.
4902	Per-user audit policy set	Track fine-grained auditing changes.
1102	Audit log cleared	High-severity — potential anti-forensics activity.

Account Management Events

Event ID	Description	Purpose / Detection Use
4720	User account created	Detect unauthorized account creation.
4722	User account enabled	Track re-enabled dormant accounts.
4723	Password change attempt	Monitor self-password changes.
4724	Password reset attempt	Detect admin password resets.
4725	User account disabled	Track account disablement (investigate anomalies).
4726	User account deleted	Detect removal of users.
4732	User added to a security group	Monitor privilege escalation via group changes.
4733	User removed from security group	Detect privilege reduction or cleanup.
4740	Account locked out	Identify brute-force or failed attempts.
4767	Account unlocked	Track recovery from lockouts.

Object Access & Process Tracking

Event ID	Description	Purpose / Detection Use
4656	Handle to object requested	File access attempt (when auditing enabled).
4660	Object deleted	File or registry deletion tracking.
4663	Object access attempt	Detect file access (critical file protection).
4688	New process created	Core event for process execution monitoring.
4689	Process terminated	Detect process lifecycle completion.
4697	Service installed	Detect new or suspicious service creation.
7045	New service installed (System Log)	Detect persistence via services.
4698	Scheduled task created	Detect task-based persistence.
4699	Scheduled task deleted	Detect cleanup of malicious tasks.
4702	Scheduled task updated	Monitor modifications to existing tasks.

Network & Logon Sources

Event ID	Description	Purpose / Detection Use
5156	Windows Filtering Platform allowed connection	Track outbound/inbound connections.
5158	Binding to local port	Detect processes opening network ports.
4649	Replay attack detected	Identify Kerberos replay or session reuse.
4673	Sensitive privilege use	Track usage of special admin privileges.
4674	Operation on protected object	Monitor privileged actions.

System / Kernel / Boot Events

Event ID	Description	Purpose / Detection Use
41	Kernel-Power failure	Detect sudden power loss or forced reboot.
6005	Event log service started	System startup indicator.
6006	Event log service stopped	System shutdown indicator.
6008	Unexpected shutdown	Identify abnormal reboots.
1001	BugCheck (BSOD)	Track system crashes.

Additional Critical Events

Event ID	Description	Purpose / Detection Use
4778	Session reconnected to RDP	Detect remote desktop reconnects.
4779	Session disconnected from RDP	Track RDP session activity.
4622	Security package loaded	Identify changes in authentication providers.
4713	Kerberos policy changed	Detect security hardening or tampering.

Follow us on:

YouTube: https://www.youtube.com/@kanippori

Instagram: https://www.instagram.com/kanippori

Facebook: https://www.facebook.com/kanippori

LinkedIn: https://www.linkedin.com/company/kanippori

Website: www.kanippori.in

5 Star Google Reviews for our Courses: