ManageEngine
ADAudit Plus

5 COMMON CYBER THREATS

and the corresponding event IDs to track

www.adauditplus.com

Table of **contents**

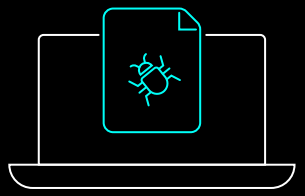
Introduction

The Windows event log is a comprehensive list of system, security, and application notifications maintained by the Windows operating system and utilized by admins to diagnose and anticipate potential security threats such as malware, spyware, insider attacks, brute-force attacks, and privilege escalations.

Admins can detect the above threats using the Administrative tool and Event Viewer to examine the Windows security event logs. However, gathering all the logs and analyzing them can be a tedious and time-consuming process.

In this guide, we are going to look at a few cyberthreats that can be detected by monitoring certain event IDs. Also, apart from detection, we are going to look at how we can expedite and automate the whole process of threat hunting.

Detecting **malware threats**



Viruses, trojans, and other malicious applications used by threat actors to corrupt IT systems or gain access to confidential data are considered malware. One method that threat actors use to evade detection is to use a password-protected malicious document for which the password is in the body of the email.

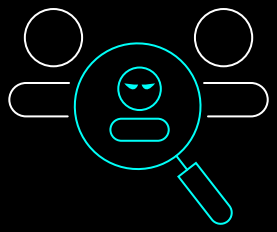
Scenario:

A banking employee receives an email that appears to be from her manager with a catchy subject like Invoice or Payment verification. The email contains a password and an attachment that is zipped and password-protected by a threat actor. The password creates the illusion that the attachment must contain confidential financial information. She enters the password and involuntarily opens a malicious file. The malware starts to create scheduled tasks and processes and installs multiple backdoors. Through the backdoors, the threat actor immediately gains access to multiple files and starts corrupting them.

Monitor the following Windows Security Log Event ID to detect malware threats:

Event ID	Category	Type	Description
4698	Other object access events	Success	This event occurs when a new scheduled task is created and it is logged on domain controllers, member servers, and workstations.
4728	Process creating	Success	This event occurs when a new process is created. This event ID logs information such as who ran the process and what program ran the process.

Detecting **insider threats**



A common type of insider threat is malicious insiders. Malicious insiders are threat actors who intentionally abuse user credentials to steal data for personal or financial gain. They have an edge over external attackers as they are familiar with the enterprise network, its security protocols, and processes, and they may possess the privileged credentials needed to carry out the attack.

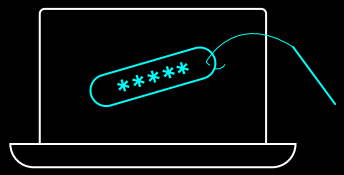
Scenario:

By using his access privileges, a malicious insider gains access to a folder containing $3 million worth of intellectual property (IP). He inserts his personal flash drive and copies all the data. To ensure that his activity is not tracked by admins, he clears the log history and shuts down the system. He later sells the IP on the dark web for over $3 million without the knowledge of his organization.

Monitor the following Windows Security Log Event IDs to detect insider threats:

Event ID	Category	Type	Description
6416	Plug and play	Success	This event occurs when a new external device is recognized by the system.
1102	Log clear	Success	This event occurs when the audit log is cleared. The account name and domain name fields identify the user who cleared the log. Malicious insiders often clear audit logs to cover their tracks. You'll want to know what user cleared the log, as this will be an indicator of account takeover.

Detecting **Kerberoasting attacks**



Using the Kerberos protocol, Kerberoasting is a hacking technique used by threat actors to harvest service account credential hashes from Active Directory (AD). These hashes can be decoded by using password cracking tools such as hashcat. This attack can be used to easily breach user accounts that are secured by weak passwords.

Scenario:

A 48-year old software developer who just got into crypto trading inadvertently visits a bogus crypto website and sees a banner entitled, "Double your money in seven days with this market tracking tool." He clicks on the banner and downloads the tool. Little did he know that the tool was Impacket (Impacket is a hacking tool used by threat actors to execute Kerberoast attacks). Impacket requests multiple Kerberos service tickets and returns ticket hashes to a threat actor. The threat actor then uses tools like hashcat and John the Ripper to extract plaintext credentials from vulnerable hashes and uses these credentials to gain access to sensitive information.

Track the following Windows Security Log Event IDs to detect spyware threats:

Event ID	Category	Type	Description
4769	Kerberos service ticket operations	Success and failure	This event occurs whenever a user requests access to a network resource, which results in the Key Distribution Center getting a Kerberos Ticket Granting Service (TGS) ticket request for authentication.
4771	Kerberos authentication service	Failure	This event occurs whenever a request for a Ticket Granting Ticket fails. It is logged on domain controllers and only for failure events.

Detecting **brute-force attacks**

During a brute-force attack, a threat actor tries out various credentials (i.e., usernames and passwords) until they find a correct combination that can be used to log in to one or more accounts.

Scenario:

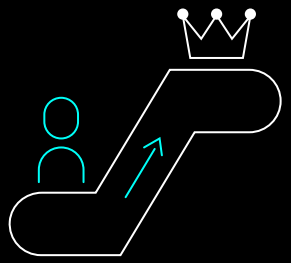
A senior accounting employee's computer is secured with the following credentials:
Username: Lucky John
Password: newpassword123

Ah, a weak password. Now, I don't think we need an entire scenario to explain how a threat actor successfully compromises Lucky John's account by executing a brute-force attack.

Track the following Windows Security Log Event IDs to detect brute-force attacks:

Event ID	Category	Type	Description
4625	Logon/logoff	Failure	This event documents every failed attempt to log on to the local computer regardless of logon type, location of the user, or type of account.
4740	Account management	Success	This event occurs whenever an indicated user account is locked out after repeated logon failures due to incorrect passwords. This event helps in detecting possible brute-force, dictionary, and other passwords guess attacks, which are characterized by a sudden spike in failed logons.

Detecting **privilege escalations**



Privilege escalation occurs when a threat actor gains unauthorized access to enhanced rights or privileges, such as executing operations as a sysadmin. Threat actors acquire access to privileged credentials and exploit them to gain administrative rights by moving laterally.

Scenario:

A malicious actor obtains access to an admin's user account after successfully stealing their password by shoulder surfing (using direct observation techniques like looking over someone's shoulder to gather information). That password grants him access to a blueprint of a soon-to-be-launched product, and he doesn't stop there; he's hungry for more. He looks for additional sensitive information to sell on the dark web.

Since the compromised admin account doesn't have access to certain systems with confidential data, he adds the admin account to different security-enabled groups and then gains access to business-critical systems, installs ransomware, threatens the organization, and demands money.

Track the following Windows Security Log Event IDs to detect privilege escalations:

Event ID	Category	Type	Description
4728	Security group management	Success	This event occurs whenever a member is added to a security-enabled global group.
4732	Security group management	Success	This event occurs whenever a member is added to a security-enabled local group. It helps in detecting privilege abuse by users who are responsible for unauthorized additions.
4756	Security group management	Success	This event occurs whenever a member is added to a security-enabled universal group. It helps in detecting accidental additions.

How does **ADAudit Plus help?**

Admins use administrative tools and the Windows Event Viewer to examine Windows security event logs. This process can be time-consuming and inefficient since admins need to collect all the logs, scrutinize them one by one, and then translate their conclusions into actionable steps, like setting up alerts for specific event IDs. Traditionally these tasks are done by using native tools and running PowerShell commands, which requires a lot of coding skills and patience.

ADAudit Plus is a UBA-driven solution that automates and expedites the process of threat hunting. It helps you to keep AD, Azure AD, file servers (Windows, NetApp, EMC, Synology, and Hitachi), Windows servers, and workstations secure and compliant by providing full visibility into all activities.

To make things easier and more efficient, ADAudit Plus provides in-depth reports, real-time alerts, and graphical displays. It simplifies the continuous monitoring of logons and logoffs, group membership changes, event log clearance, account lockouts, file servers, and much more across your AD, member servers, and workstations.

ManageEngine
ADAudit Plus

ADAudit Plus' real-time alerting console instantly notifies admins of every critical event; alerts are sent straight to admins' inboxes or phones. With ADAudit Plus, admins can keep a close watch on domain users' behavior, and detect compromised credentials, lateral movement, and other malicious behavior on the spot.

$ Get Quote

Download