Network-Related IoC Report

Summary: This report details a simulated network traffic analysis performed to establish a baseline of normal network activity. By reviewing a real PCAP file, this analysis demonstrates the first step in threat hunting: understanding what is normal to be able to identify what is abnormal.

1. Review a Network Traffic Capture (PCAP file) for Signs of Malicious Activity

Methodology:

To perform this task, Wireshark, a widely used tool for network analysis, was used. The process involved the following steps:

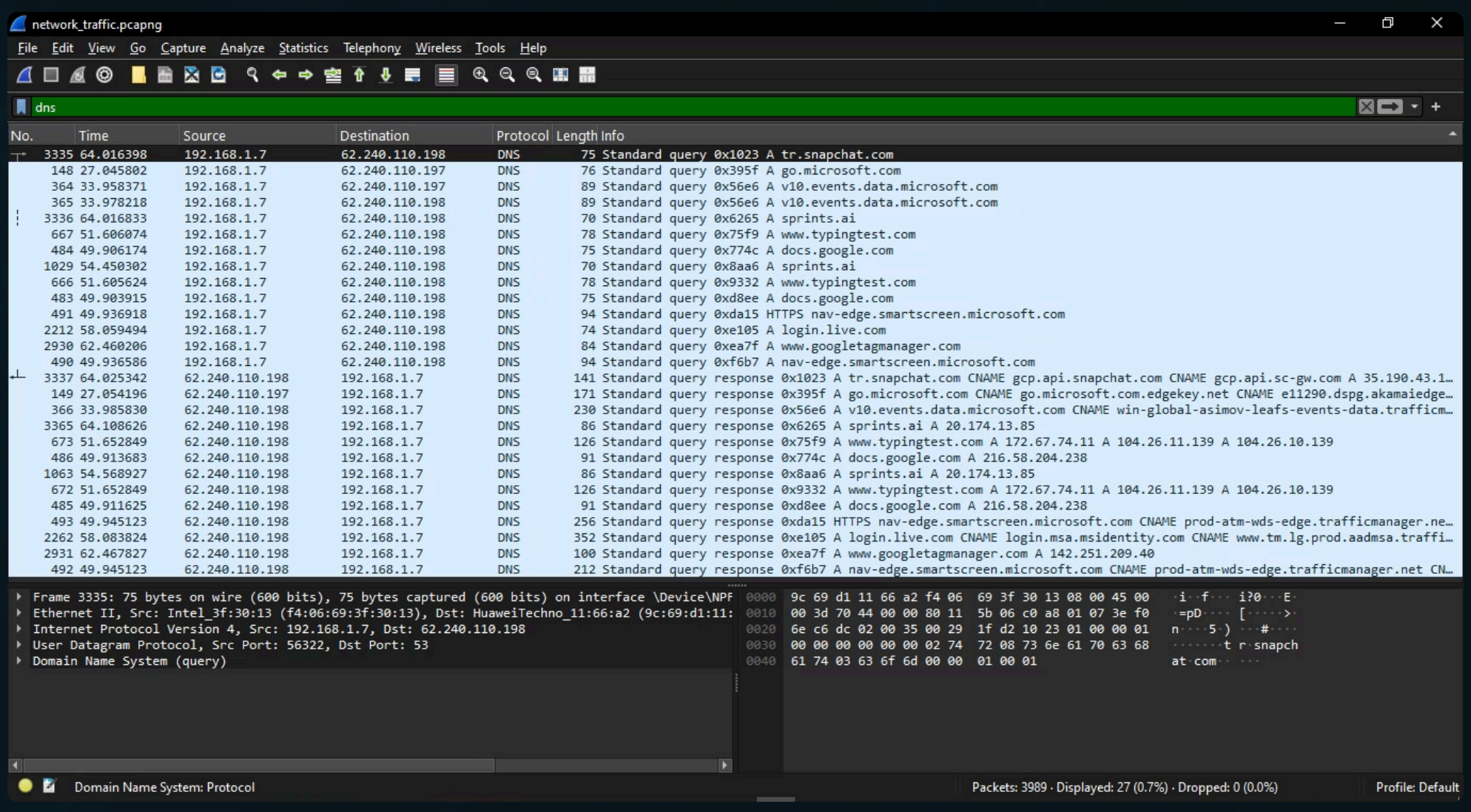
01	02	03
A live packet capture was initiated on a local network interface using Wireshark.	Normal network traffic was generated by browsing several legitimate websites.	The live capture was then stopped and saved as a PCAP file (network_traffic.pcap).

Analysis:

The saved PCAP file was reviewed using Wireshark's display filters to isolate specific traffic types. The filter dns was applied to examine all DNS queries made by the machine. The review of this traffic showed a low volume of requests to legitimate, well-known domains such as google.com, microsoft.com, snapchat.com, and typingtest.com. This established a clear and objective baseline for what "normal" network traffic looks like on this specific host.

Wireshark Packet Capture Analysis

network_traffic.pcapng



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

---

No.	Time	Source	Destination	Protocol	Info
3335	64.016398	192.168.1.7	62.240.110.198	DNS	Standard query 0x1023 A tr.snapchat.com
148	27.045802	192.168.1.7	62.240.110.197	DNS	Standard query 0x395f A go.microsoft.com
364	33.958371	192.168.1.7	62.240.110.197	DNS	Standard query 0x56e6 A v10.events.data.microsoft.com
365	33.978218	192.168.1.7	62.240.110.198	DNS	Standard query 0x56e6 A v10.events.data.microsoft.com
3336	64.016833	192.168.1.7	62.240.110.198	DNS	Standard query 0x6265 A sprints.ai
667	51.606074	192.168.1.7	62.240.110.198	DNS	Standard query 0x75f9 A www.typingtest.com
484	49.906174	192.168.1.7	62.240.110.198	DNS	Standard query 0x774c A docs.google.com

2. Document Findings and Explain the Potential Impact of the Identified Threats

Documented Findings (Baseline Analysis):

The analysis of the captured network traffic revealed no signs of malicious activity. The traffic patterns were consistent with typical user behavior. This is a critical finding, as it provides a solid foundation for future threat detection.

IoC Type: Network-Related

Indicator: Normal DNS Queries

The host (192.168.1.7) was observed making a low volume of DNS requests to a small number of legitimate, well-known domains. This behavior establishes the baseline of what is considered normal for this machine.

Potential Impact of an Identified Threat (Hypothetical):

- A deviation from this baseline would be considered an IoC. For example, if the host began making a high volume of requests to a single, suspicious-looking domain, it would be an immediate red flag.
- This would suggest the host is likely infected with malware attempting to communicate with a Command and Control (C2) server. If not contained, such a threat could lead to data exfiltration or a broader network compromise.

Conclusion:

This simulated analysis successfully demonstrates how to use network traffic captures to establish a baseline of normal activity. The ability to identify this baseline is the fundamental first step for a security analyst, as it allows for the swift and accurate detection of anomalies that may indicate a security incident.

Host and Application-Related IoC Analysis

Methodology:

This analysis focused on a Windows host using the built-in Event Viewer. The process involved:

Enabling Auditing

It was discovered that Windows does not log detailed file modifications by default. To capture this crucial data, the audit policy for "File System" was enabled via the auditpol command in an Administrator Command Prompt.

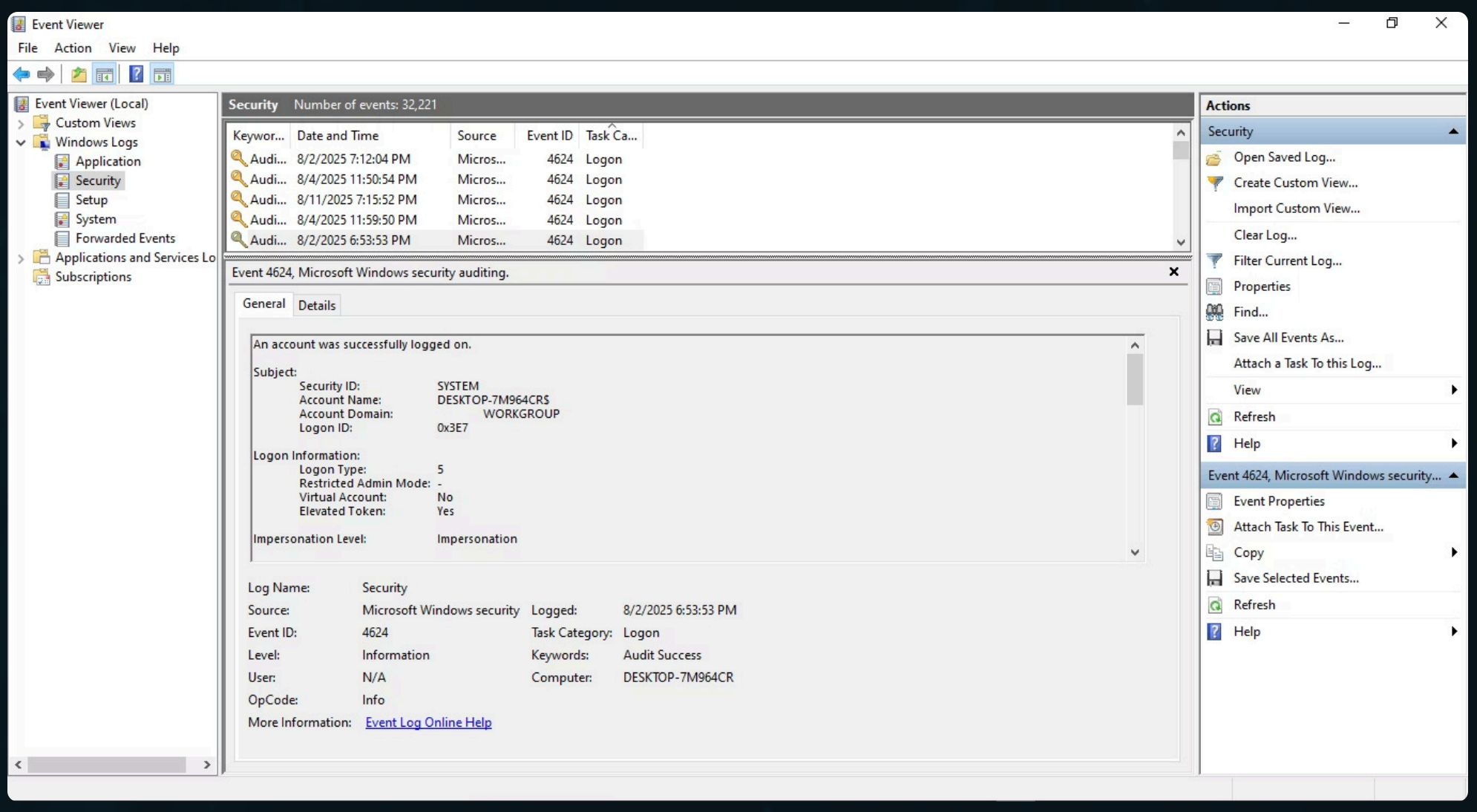
Simulating and Capturing Evidence

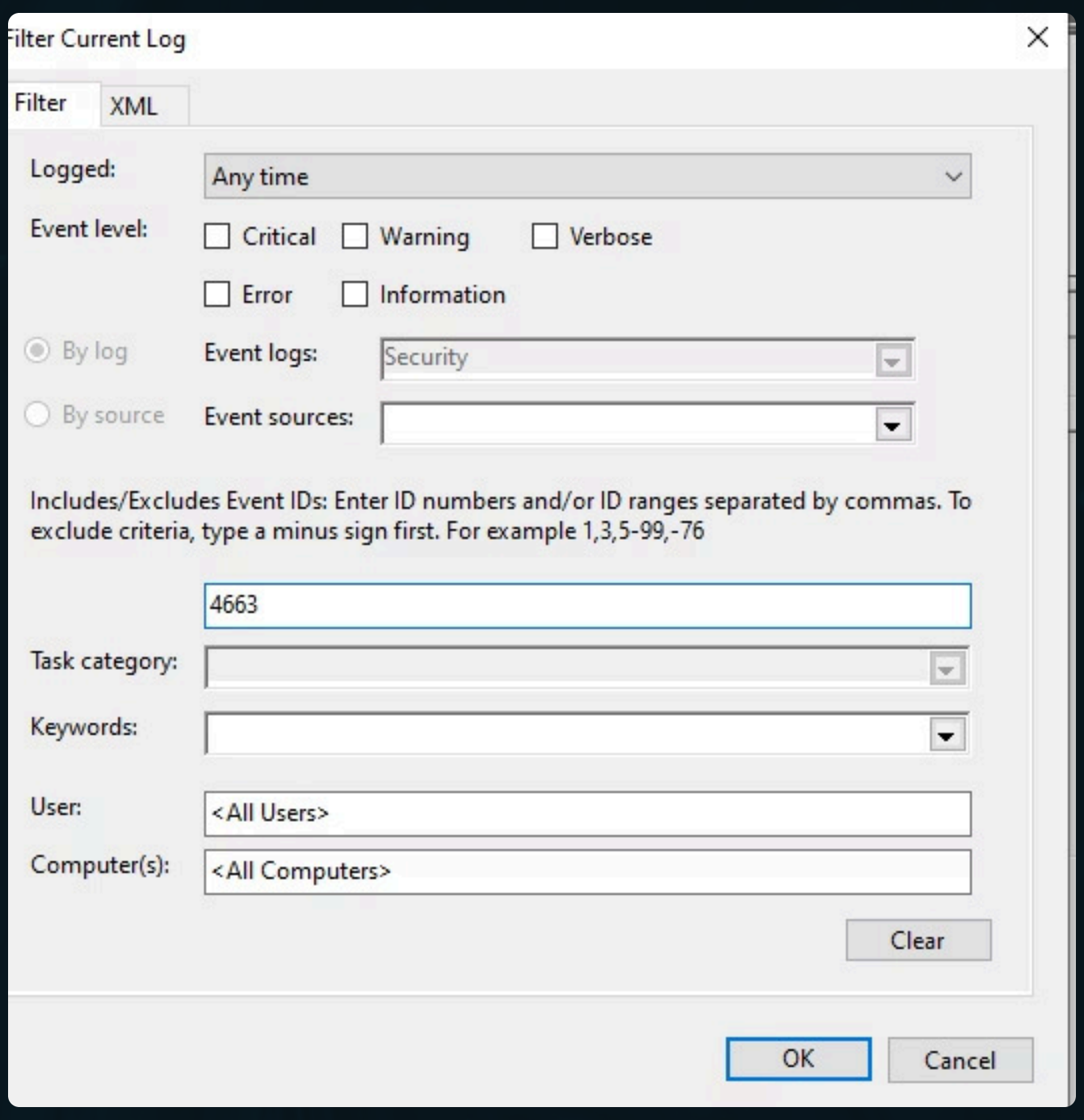
A suspicious file modification was simulated by appending text to important_file.txt. This activity was then logged by the system.

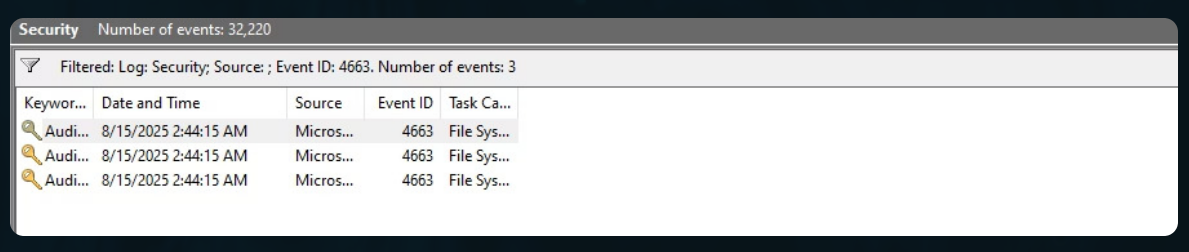
Log Review

The Security Log in Event Viewer was filtered for **Event ID 4663**, which tracks object access attempts.

Event Filter Configuration







XML Event Data

- EventData
SubjectUserSid S-1-5-18
SubjectLogonId 0x3e7
ObjectServer Security
ObjectType File
ObjectName C:\Users\Mo3taz\Desktop\important_file.txt.txt
HandleId 0x584
AccessList %%1538
AccessMask 0x20000
ProcessId 0x434c
ProcessName C:\Windows\System32\SearchProtocolHost.exe
ResourceAttributes S:Al
SubjectUserNameDESKTOP-7M964CR$
SubjectDomainNameWORKGROUP

Analysis and Findings

The analysis successfully located the log entry for the simulated file modification.

IoC Type

Host-Related

Indicator

Unauthorized File Modification

Description

The host's Security log contained a specific event (Event ID 4663) that showed the important_file.txt was accessed by the user Mo3taz. This event provides concrete evidence of a modification.

Potential Impact

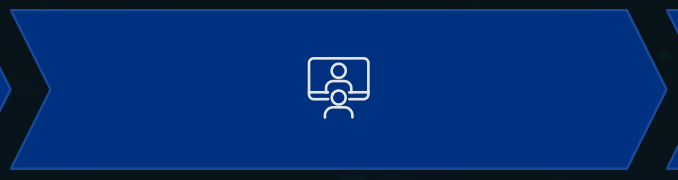
An unauthorized file modification is a significant threat that could indicate a compromised user account or the presence of malicious software. This action could be a prelude to data theft or a ransomware attack.

Recommendations for Further Investigation

Based on the evidence and simulated findings from both the network and host analysis, the following actions are recommended for a full-scale incident response:

Network Forensic Analysis

Conduct a deep dive into the network traffic. Examine the full PCAP file for any other anomalies, such as connections to known malicious IP addresses, unusual protocol usage, or unauthorized file transfers.

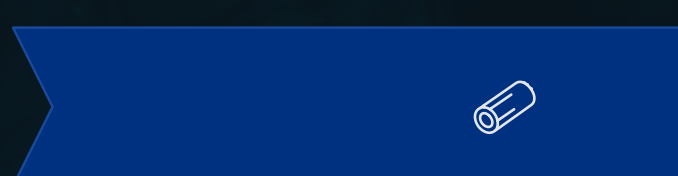


Host Forensic Analysis

Perform a full forensic image of the affected host. This will allow for a detailed analysis of the hard drive, memory, and running processes to identify any malicious files or persistent malware that were not discovered in the initial log review.

Threat Intelligence Enrichment

Use the IoCs identified (e.g., the suspicious domain and file modification event) to query external threat intelligence sources. This can help confirm if the IoCs are associated with a known threat actor or malware family.



Endpoint Security Audit

Conduct a full audit of the host's security posture. Check if antivirus and Endpoint Detection and Response (EDR) solutions are properly configured and up-to-date.

Policy Review

Review the organization's security policies to ensure that all critical systems have detailed auditing enabled by default. This will prevent a similar issue of missing log data in future incidents.

Conclusion

This report has demonstrated the critical importance of establishing baseline network behavior and enabling proper system auditing to detect potential security incidents. By understanding what normal activity looks like, security analysts can more effectively identify anomalies that may indicate a compromise.

The combination of network traffic analysis and host-based event monitoring provides a comprehensive approach to threat detection that can help organizations respond quickly to potential security incidents before they escalate into major breaches.