Threat Hunting and False Negatives

Author: Jeffrey Legg, Jeffrey.legg@sans.student.edu
Advisor: *Lenny Zeltser*

Accepted: *23 January 2024*

Abstract

The more complete telemetry captured inside a network, the more chance analysts have of understanding if an attack took place. Although modern endpoint detection and response tools have alert logs and additional full capture logs for additional cost, what level of value does each bring an organization? Because each environment is unique, organizations should attempt to find a baseline that their logging provides. This research examines the differences between the default alert telemetry and full telemetry available for additional cost. This research will determine how many more indicators of compromise should be captured and how close to 100% does it get us.

1. An Introduction to Indicators of Compromise

Indicators of compromise (IOC) represent a piece of forensic evidence that could represent malicious activity (CrowdStrike, 2023). Vendors and private and government organizations distribute IOCs from attacks, which allows others to search their network for similar artifacts that could represent an attack. Although IOCs are reactive in nature, they enable organizations to identify attacks that have gone undetected by their security controls.

The cybersecurity vendor CrowdStrike defines threat hunting as "the practice of proactively searching for cyber threats" (CrowdStrike, 2023). It can be difficult for an organization to know if an IOC has taken place. The crux of the problem is that the correctness of the answer depends upon the information being available. A vendor tool such as Microsoft Defender might not provide all the necessary information to answer that question. Other industry recommendations suffer the same flaw, such as implementing native tools like Sysmon (Aldauiji et al., 2022) and collecting all artifacts and native events. Does the information available allow us to answer the question correctly, or will it give us a false negative?

Compounding this issue is that modern attacks utilize widely used processes and can easily bypass our security controls. An executable like psexec is a possible sign of malicious activity or a legitimate business process. As detection tools have improved, the malicious actors have realized that it is better to escalate and move laterally throughout a network with compromised credentials and known executables rather than place their tools on the system (Lemos, 2018).

1.1 The Problem

1.1.1. Telemetry size and type

The ability to ingest Windows event logs in large enterprise networks becomes challenging because of the cost and scale of data required. Even though, in practice, they are the gold standard and provide forensic-level evidence of what happened in the system (Lemos, 2018). The telemetry provided standard by modern endpoint detection and response (EDR) tools for ingestion into an SIEM shrinks this by providing data based on

alerts only, leaving the full capture behind. This full capture is available at additional licensing and storage costs. Which set of telemetry gives enough information to hunt for an indicator of compromise effectively?

1.1.2. More investment does not guarantee reduced risk

Due to the interconnected networks and relationships organizations have with partners, vendors, and external services, these relationships create a form of systematic risk, which may not be affected by the amount of investment in security (Dambra et al., 2023). Threat hunting reduces this risk by answering questions about whether an event occurred. Answering these questions is not tied to the amount of information available to search, but access to the correct information. It is not possible to answer the question at times, and the ability to recognize that will reduce the risk of a false negative answer.

Research dating back to 2018 noted that 52% of 461 members of a cybersecurity group listed improving the speed and accuracy of threat response as the highest concern (Lemos, 2018). The research and analysis proposed in this document focus on the accuracy of threat hunting. To be accurate, the question should be asked according to the correct set of information.

1.1.3. Thesis

An analysis of the number of indicators of compromise available between the default alert telemetry provided standard versus the full telemetry capture of an EDR product at an additional cost. Is the alert telemetry a viable information set to discover indicators or is the full telemetry capture by the EDR required.

1.1.4. Objectives

- Simulate 10 different attack sceneries against three victim systems utilizing the AttackIQ breach and attack simulation software.
- Compare the ability to find the simulated attacks indicators of compromise inside the standard alert telemetry versus the full telemetry.
- Compare the difference in available indicators of compromise when a system has both CrowdStrike Falcon and Microsoft Defender installed versus only one.

2. Research Method

In section 2 and further in Appendix A and B, the configurations of the breach and attack simulation tool will be outlined, including selected tests, and victim hosts. Future research and peer reviews can use this information to replicate the environment and tests.

2.1. Tool Telemetry vs Ingested Alerts

Tool telemetry will be defined as logs retained inside the EDR tool and not sent to the SIEM as a part of the standard configuration and licensing agreements. To ingest this set of telemetry, an organization would have to agree to additional costs from the vendor and provide extra storage capability to retain the logs. Ingested alerts will be defined as logs provided for ingestion into an SIEM standard and requiring no additional licensing. Microsoft Defender for Endpoints P2 and CrowdStrike Falcon will be used as our EDR tooling. Appendix A includes specific configurations such as version numbers.

Three hosts will be utilized in the testing with three different EDR tool configurations to test all available tool deployment possibilities.

- System 85 is configured with Windows Defender for Endpoint P2.
- System 86 is configured with CrowdStrike Falcon.
- System 87 is configured with both Windows Defender for Endpoint P2 and CrowdStrike Falcon.

To collect the alert logs from the systems and help with searching Splunk Enterprise Security will be utilized. The use of a security information and event management (SIEM) tool is recommended when attempting to correlate separate log sources together.

The presence of an indicator of compromise does not confirm malicious activity since it could be a false positive. EDR alert telemetry captures both legitimate and potentially malicious activity and presents areas of concern for possible investigation. Past research has utilized these logs to show how often malware is found in environments in statements such as “Using malware encounters logs we identify where, how many

times, and which signatures were triggered for each malware encounter" (Dambra et al., 2023). This can be flawed because not all alerts are malicious, and many are legitimate activity and not caused by an encounter with malware.

2.2. Breach and Attack Simulation

Gartner defines breach and attack simulation (BAS) as a tool that "enables organizations to gain a deeper understanding of security posture vulnerabilities by automating testing of threat vectors such as external and insider, lateral movement, and data exfiltration" (Gartner, 2024). To ensure proper execution of the attacks, a BAS tool was selected to simulate the attacks because it allows analysts to replicate the research in different situations and allows for peer review of the research. The enterprise version of AttackIQ was used as a representative tool that allowed analysts to simulate attacks that generate alerts or other activities.

All selected attacks utilized standard AttackIQ configurations with no customization. The attacks are listed in detail per host in Appendix B. The combination of both Appendices will allow for future research and peer review.

2.3. Attack Selection

Attacks available for simulation are nearly endless in today's modern breach and attack simulation tools. Ten attacks were selected to representing a wide array of basic attacks, including initial access, lateral movement, privilege escalation, and reconnaissance. The goal is to produce a wide selection of artifacts that will be represented as indicators of compromise from the selected attack and create telemetry from real-world situations.

Future research should consider using multiple attacks and multiple breach and attack simulation vendors. The use of manual attacks could generate a different data set entirely and remove possible false positives from BAS tools. These tools depend upon launching their attacks through Python scripts that can sometimes generate separate alerts if not configured properly.

3. Findings and Discussion

Section 3.2 Summary of Findings lists all indicators of compromises and their prevalence. Sections 3.1.1. through 3.1.10, provide details and discussion on each test. Appendix A is a roll-up of technical data for each system utilized as the attack victim and its applicable software and configurations. Appendix B is a roll-up of all attacks from AttackIQ against the victim systems in Appendix A.

3.1. Test Discussions

The following sections give a short description, discussion, and statistical representation of findings for each of the ten tests. Simulated attack execution happens through Python scripts from the BAS tool AttackIQ. When reviewing the individual telemetry, readers will see a Python file execution before each attack that triggers the simulated commands. Additional commands are executed after each simulation to clean up generated files and return the system to its prior state. These commands can cause the generation of false positive alerts inside the EDR tools.

3.1.1. Test One – Shadow Copy and Mimikatz.exe

Test 1 executed by AttackIQ tests a form a privilege escalation which consists of dumping SAM hashes with Mimikatz using a volume shadow copy. The test utilized PowerShell commands to create a volume shadow copy export in JSON format and then utilized Get-WMIObject Win32_ShadowCopy to create the file in the global root of the device. After successfully creating the shadow copy, Mimikatz was downloaded to extract the password hashes.

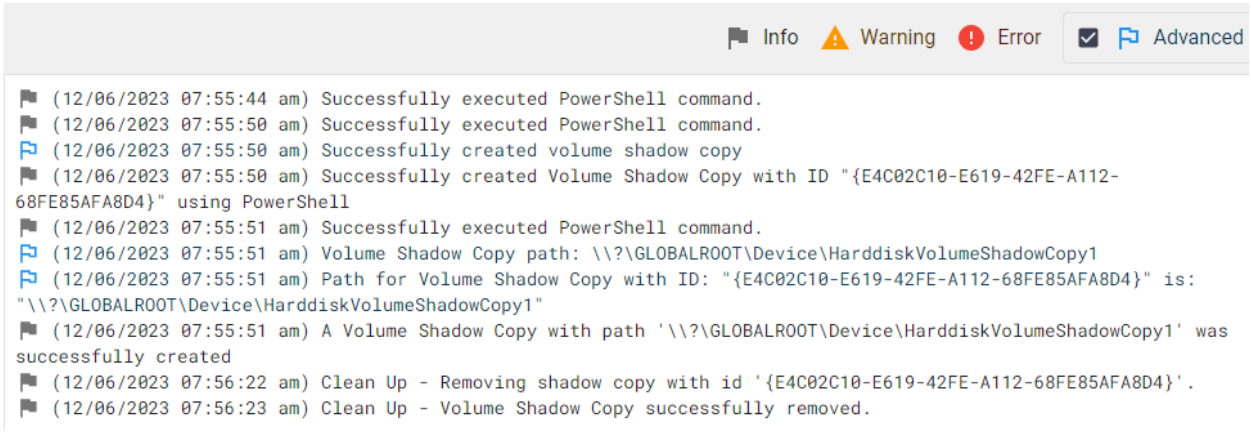

Figure 1. AttackIQ activity details for Test 1 Step 1 against system 87 (AttackIQ, 2023)

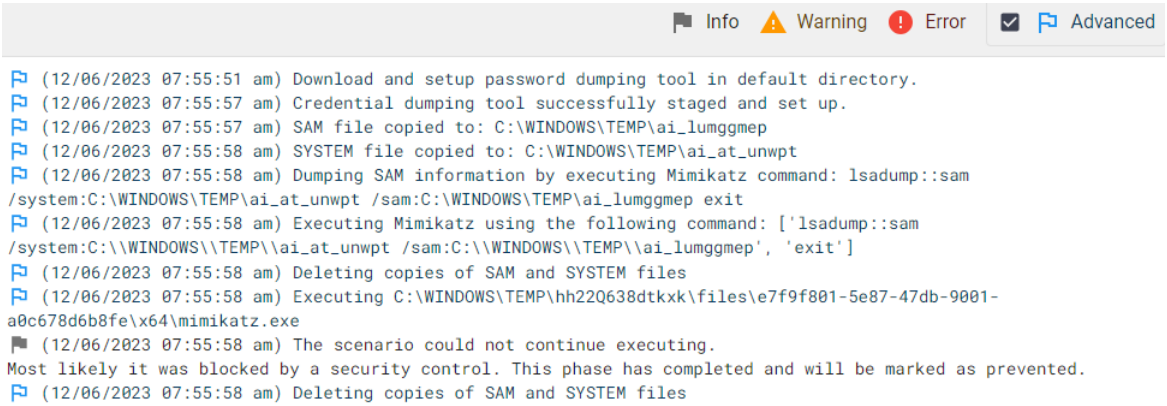

Figure 2. AttackIQ activity details for Test 1 Step 2 against system 87 (AttackIQ, 2023)

Step 1, shown in Figure 1, did not generate any true positive alerts in the three configurations. However, a high percentage of the indicators of compromise were found in the full telemetry of the EDR tool available at an additional cost from the vendors which is included as an export in Appendix C. The full telemetry across all three configurations showed the IOCs. CrowdStrike Falcon created one false positive alert, which was detected when the BAS tool attempted to clean up the attack by deleting the generated files shown in Figure 3 below. Full telemetry is required to find indicators in Step 1; the alert telemetry was insufficient.

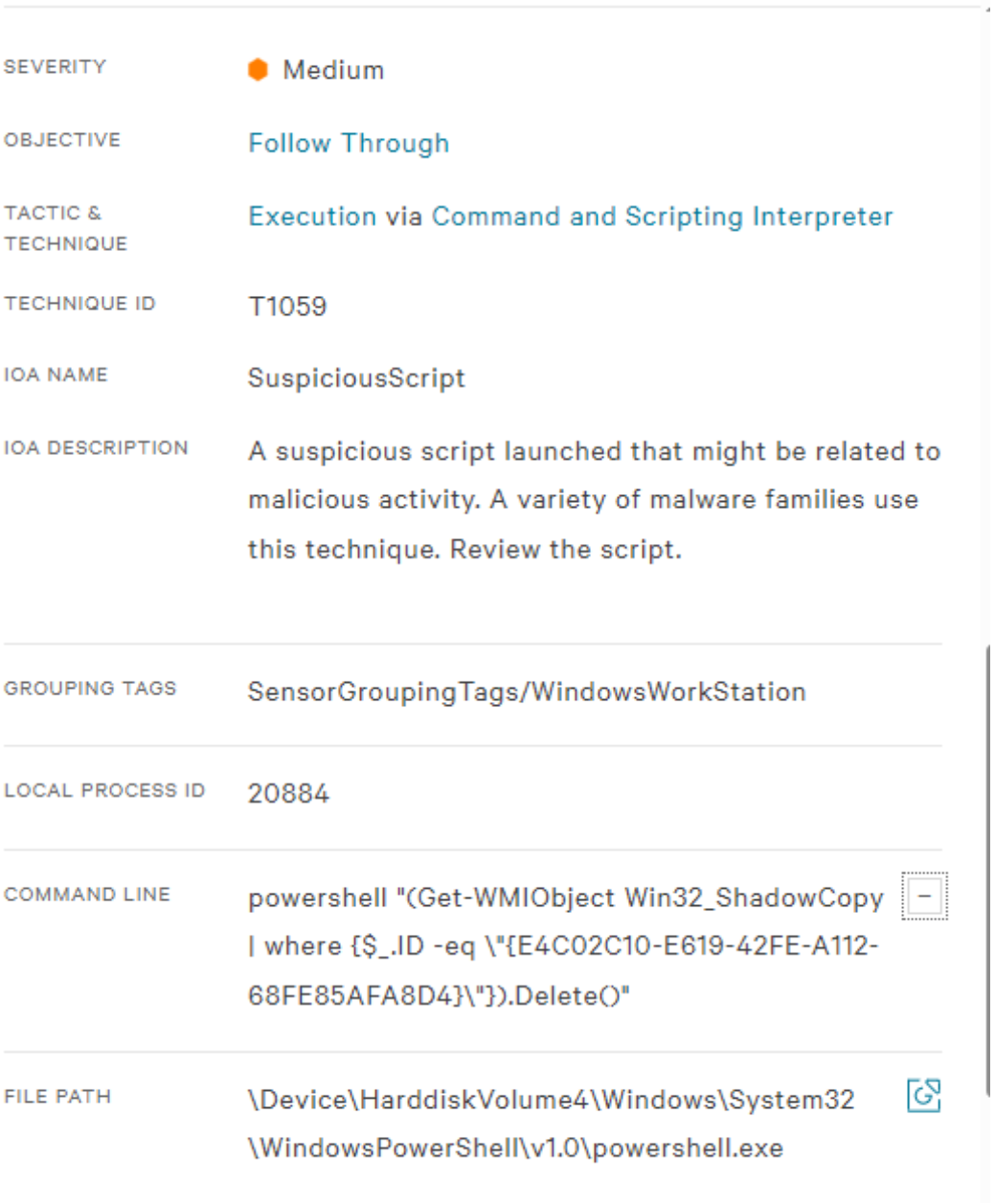

Figure 3. CrowdStrike Falcon alert for deleting shadow copy on system 86.

Step 2 and the use of Mimikatz generated alert telemetry inside the EDR tools for file write, not execution as seen in Figure 4 below. In the system that had both Defender and Falcon, we find only alert telemetry with Defender because it has precedence to do the detection and remediation first. Only alert telemetry is required to find indicators in Step 2, the full telemetry would not be required.

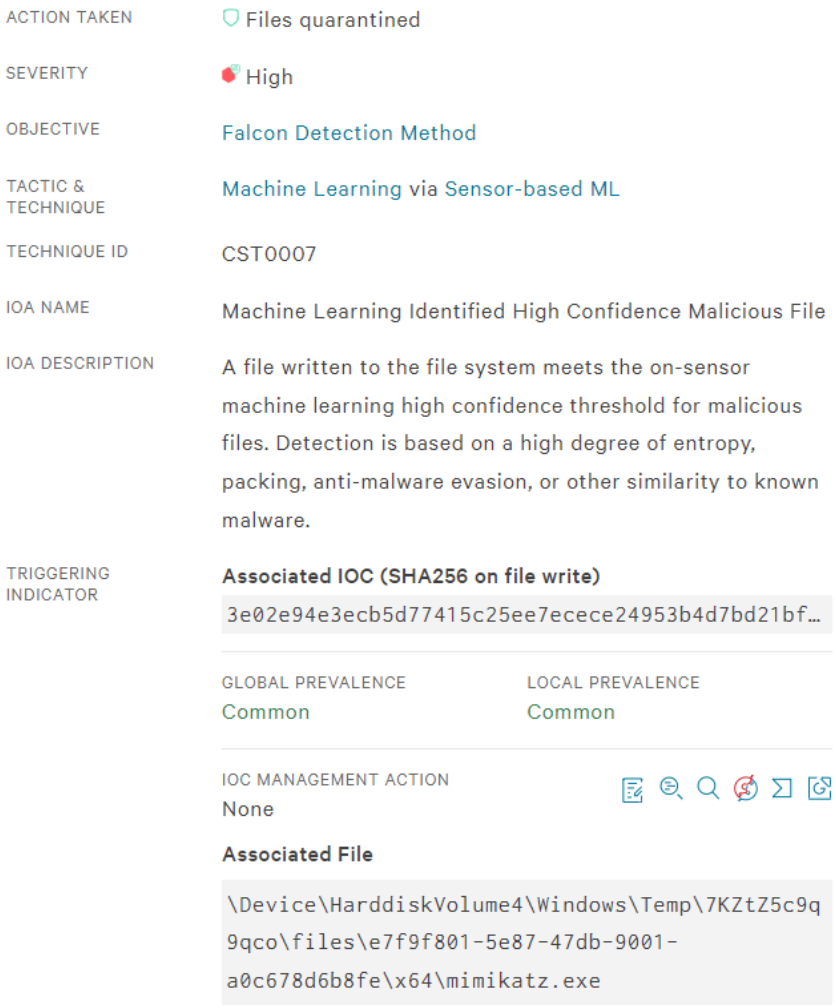

Figure 4. CrowdStrike Falcon alert for writing Mimikatz.exe to system 85

This AttackIQ scenario could have generated a maximum of eight indicators of compromise artifacts. Presence of IOCs included in full telemetry for Test 1 had a rate of visibility of 87.5% for Defender (7 of 8), 100% for Falcon (7 of 7), and 87.5% for the configuration of Defender as primary and Falcon as secondary (7 of 8). Alert telemetry had a rate of visibility of 37.5% for Defender (3 of 8), 28.57% for Falcon (2 of 7), and 26.67% (4 of 15) for the configuration of Defender as primary and Falcon as secondary (Defender, Falcon, Splunk Log Telemetry, 2023).

3.1.2. Test 2 – Malware Download

The second test executed by AttackIQ consists of attempting to download a malware sample from APT35 to memory with the name user.exe. The simulated attack would then attempt to save the file to disk.

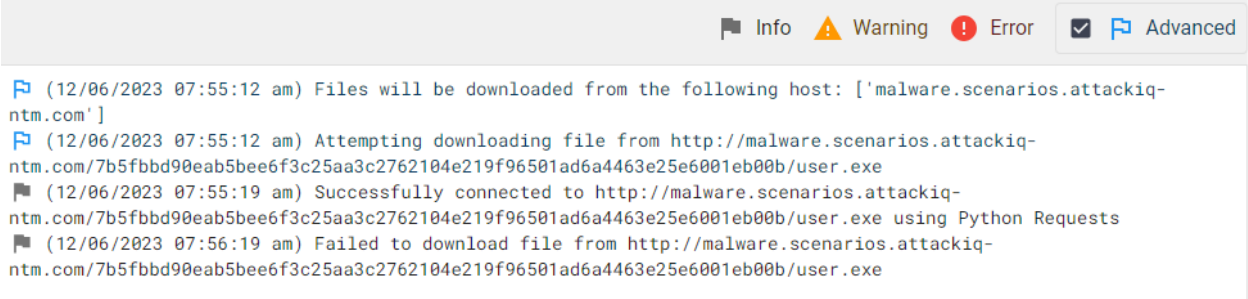

Figure 5. AttackIQ activity details for Test 2 against system 85 (AttackIQ, 2023)

Test 2 completely bypassed the EDR tools, and the IOCs do not exist in the full or alert telemetry. The attack simulation tool AttackIQ shows an established connection and failed download. No telemetry exists to allow us to discover the indicators of the attack. Missing indicators include an HTTP connection, domain name, and file name. The full telemetry showed other HTTP connections but did not include these. Further research would need to be conducted to understand why. It is unknown why this connection is unavailable when other HTTP connections are. Both full telemetry and alert are inadequate to discover the IOCs.

AttackIQ scenario two generated four indicators of compromise artifacts. Presence of IOCs included in full telemetry for Test 2 had a rate of visibility of 0% for Defender, 0% for Falcon, and 0% for the configuration of Defender as primary and Falcon as secondary. Alert telemetry had a rate of visibility of 0% for Defender, 0% for Falcon, and 0% for the configuration of Defender as primary and Falcon as secondary (Defender, Falcon, Splunk Log Telemetry, 2023).

3.1.3. Test 3 - Save and Copy Beep Malware Sample

The third test executed by AttackIQ consists of saving a file to the filesystem and pausing for three seconds before making a copy of that file in another location. The

sample file is from the beep malware family (Lakshmanan, 2023), and the included file is a DDL injector.

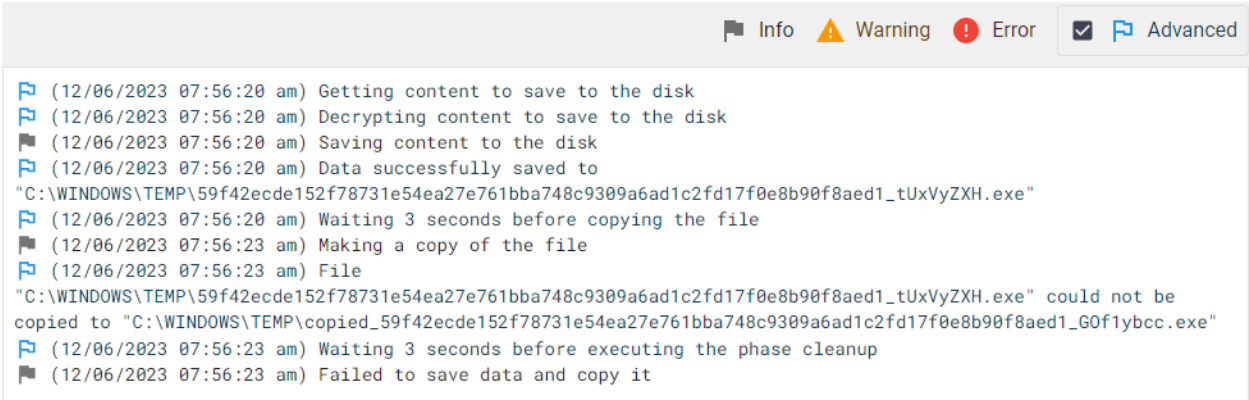

Figure 6. AttackIQ activity details for Test 3 against system 86 (AttackIQ, 2023)

Test 3 is the first of multiple tests that save, delay for three seconds, and copy malicious files. The main difference between Defender and Falcon is telemetry on the original saved file. It is unavailable inside the Falcon-only telemetry but appears in Defender and dual configuration system—another example of inconsistencies in what the endpoint detection tools capture. Both full telemetry and alert are inadequate to discover the IOCs.

An anomaly found during the test is that when the simulation executes against the system with only Falcon installed, it captures two of four possible artifacts. When configured with Defender as the primary, it captures all four alerts. It requires further research to understand but the hypothesis is that Falcon is triggering to capture the additional two based on a Microsoft alert.

AttackIQ scenario three generated four indicators of compromise artifacts. Presence of IOCs included in full telemetry for Test 3 had a rate of visibility of 100% for Defender, 50% for Falcon, and 100% for the configuration of Defender as primary and Falcon as secondary. Alert telemetry had a rate of visibility of 100% for Defender, 25% for Falcon, and 100% for the configuration of Defender as primary and Falcon as secondary (Defender, Falcon, Splunk Log Telemetry, 2023).

3.1.4. Test 4 - Save and Copy Turla Malware Sample

The fourth test executed by AttackIQ consists of saving a file to the filesystem and pausing for three seconds before making a copy of that file in another location. The sample file is from the Turla malware family, and the included file is a PNG Dropper.

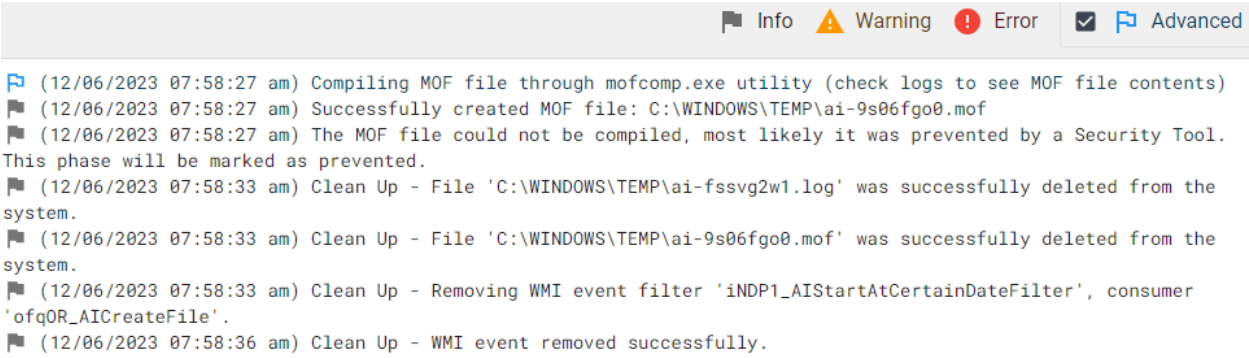

Figure 7. AttackIQ activity details for Test 4 against system 87 (AttackIQ, 2023)

Microsoft Defender and CrowdStrike Falcon blocked the copy action and provided alert telemetry. Neither EDR tool was able to capture the new file name as a part of its telemetry. Further research is needed to fully understand why CrowdStrike Falcon does not generate an alert when both tools are stacked. The hypothesis is Microsoft Defender prevents the command, so it is not seen by the secondary EDR. Full telemetry is required to find indicators; the alert telemetry was insufficient.

AttackIQ scenario four generated four indicators of compromise artifacts. Presence of IOCs included in full telemetry for Test 4 had a rate of visibility of 50% for Defender, 50% for Falcon, and 50% for the configuration of Defender as primary and Falcon as secondary. Alert telemetry had a rate of visibility of 50% for Defender, 50% for Falcon, and 25% for the configuration of Defender as primary and Falcon as secondary (Defender, Falcon, Splunk Log Telemetry, 2023).

3.1.5. Test 5 – WMI Persistence

The fifth test executed by AttackIQ consists of gaining persistence through a WMI event consumer and filter. The test compiles the .mof file using the mofcomp.exe utility and gains persistence through the MOF file compilation. The simulated attack also creates and writes files to disk, including a .mof and .log files.

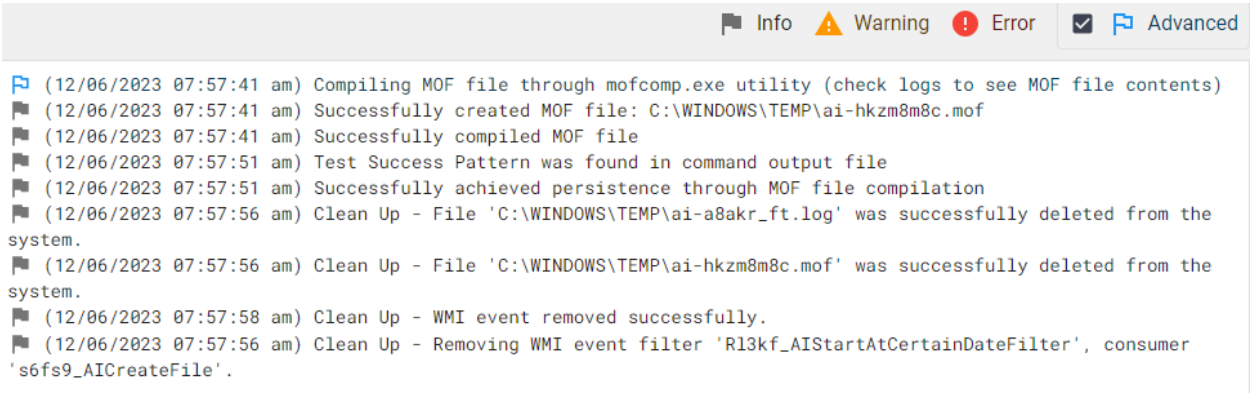

Figure 8. AttackIQ activity details for Test 5 against system 85 (AttackIQ, 2023)

The system configured with only Microsoft Defender captured all four artifacts in the full telemetry but did not generate any alerts. The CrowdStrike Falcon configuration captured two artifacts in its full telemetry and generated alerts for both. Test 5 is the first test where Microsoft Defender telemetry changed between an individual and dual configuration system. Further research is required to understand why this took place. Full telemetry is required to find indicators; the alert telemetry was insufficient.

AttackIQ scenario five generated four indicators of compromise artifacts. Presence of IOCs included in full telemetry for Test 5 had a rate of visibility of 100% for Defender, 100% for Falcon, and 50% for the configuration of Defender as primary and Falcon as secondary. Alert telemetry had a rate of visibility of 0% for Defender, 50% for Falcon, and 25% for the configuration of Defender as primary and Falcon as secondary (Defender, Falcon, Splunk Log Telemetry, 2023).

3.1.6. Test 6 – Process Hollowing

The sixth test executed by AttackIQ simulates process hollowing against svchost.exe as a host file. The attack replaces a portion of svchost.exe's code with that of SleepingBinary5sec.exe.

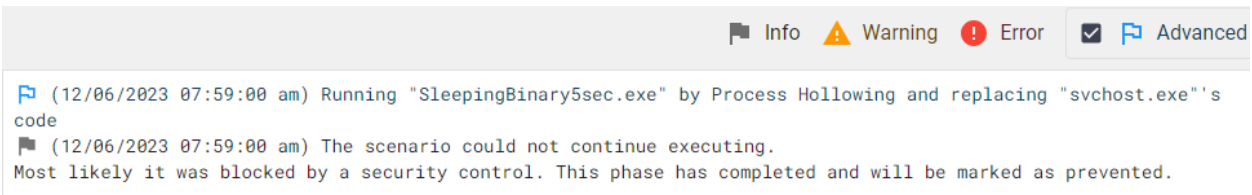

Figure 9. AttackIQ activity details for Test 6 against system 87 (AttackIQ, 2023)

Microsoft Defender captured three indicators of compromise and produced alerts for all three, and CrowdStrike Falcon captured one and provided an alert. Anomalies were present inside the configuration with both Defender and Falcon. Microsoft Defender captured one less indicator of compromise and generated no alerts when in a stacked configuration. CrowdStrike Falcon did the opposite in a stacked configuration and found more, from one to two of the three indicators possible, and generated two alerts. Inconsistencies in capture logic continue to appear when the tools are configured together, and further research is required to understand if they are consistent or random issues. Full telemetry is required to find indicators; the alert telemetry was insufficient.

AttackIQ scenario six generated four indicators of compromise artifacts. Presence of IOCs included in full telemetry for Test 6 had a rate of visibility of 100% for Defender, 100% for Falcon, and 100% for the configuration of Defender as primary and Falcon as secondary. Alert telemetry had a rate of visibility of 100% for Defender, 100% for Falcon, and 50% for the configuration of Defender as primary and Falcon as secondary (Defender, Falcon, Splunk Log Telemetry, 2023).

3.1.7. Test 7 – Kerberoasting

The seventh test executed by AttackIQ consists of a kerberoasting (CrowdStrike, 2023) attack utilizing the Rubeus tool. The attack simulates the kerberoasting attack with the following parameters: [kerberoast /format:hashcat /outfile:C:\WINDOWS\TEMP\momyxj33.hashcat]

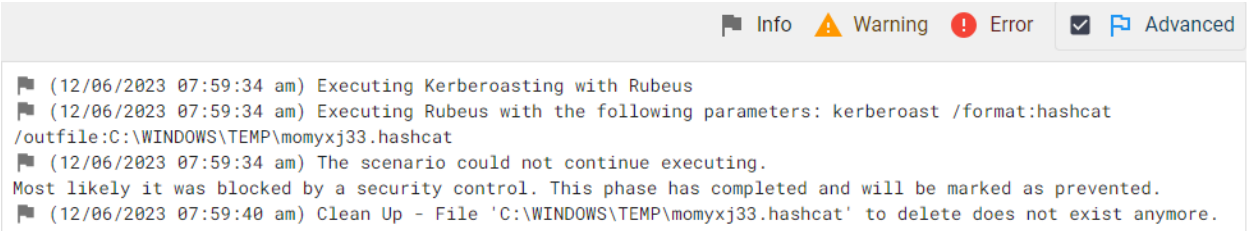

Figure 10. AttackIQ activity details for Test 7 against system 87 (AttackIQ, 2023)

All three configurations captured all artifacts in both the full and alert telemetry. AttackIQ reported that it errored in execution on system 85, but upon inspection of the

telemetry, all indicators of compromise were present with alerts. Test 7 aligns with Test 3, where CrowdStrike Falcon generated alerts in a stacked configuration even though Defender had already prevented the attack. This is in contrast to Test 4 where no alerts were captured by CrowdStrike Falcon in a stacked configuration. Both full telemetry and alert is inadequate to discover the IOCs.

AttackIQ scenario seven generated two indicators of compromise artifacts. Presence of IOCs included in full telemetry for Test 7 had a rate of visibility of 100% for Defender, 100% for Falcon, and 100% for the configuration of Defender as primary and Falcon as secondary. Alert telemetry had a rate of visibility of 100% for Defender, 100% for Falcon, and 100% for the configuration of Defender as primary and Falcon as secondary (Defender, Falcon, Splunk Log Telemetry, 2023).

3.1.8. Test 8 – Egress Port Checker

The eighth test executed by AttackIQ consists of an egress port checker that executes nmap to see if ports 1-1000 are open on the system. The simulated recon attack executes nmap with the following parameters: [-oX –vvv –stats-every 1s –host-timeout 20m -sS -n -Pn -p1-65535]

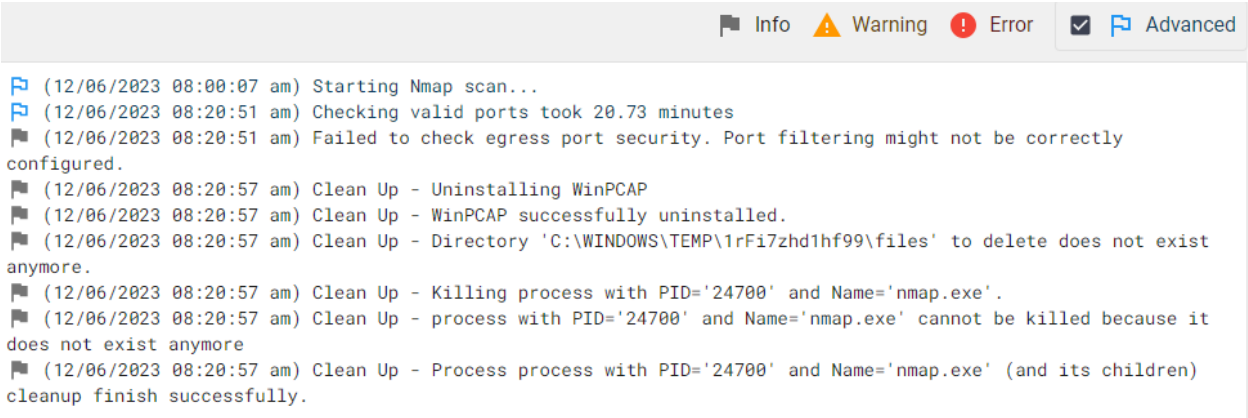

Figure 11. AttackIQ activity details for Test 8 against system 86 (AttackIQ, 2023)

All configurations captured an artifact of the original Nmap execution with parameters but not the individual port connections created during the scan. Both tools are inconsistent as they display other connections at the IP and port levels. NMAP command

was not seen as malicious by either tool, resulting in no alerts. Full telemetry is required to find indicators; the alert telemetry was insufficient.

AttackIQ scenario eight generated one indicator of compromise artifacts. Presence of IOCs included in full telemetry for Test 8 had a rate of visibility of 100% for Defender, 100% for Falcon, and 100% for the configuration of Defender as primary and Falcon as secondary. Alert telemetry had a rate of visibility of 0% for Defender, 0% for Falcon, and 0% for the configuration of Defender as primary and Falcon as secondary (Defender, Falcon, Splunk Log Telemetry, 2023).

3.1.9. Test 9 – XSL Script through WML

The ninth test executed by AttackIQ simulates an attack by processing an XSL script through WMI. The attack simulation executes a WMI command utilizing wmic.exe, which executes a VBScript embedded in the local XSL file that writes a text file to disk to prove execution.

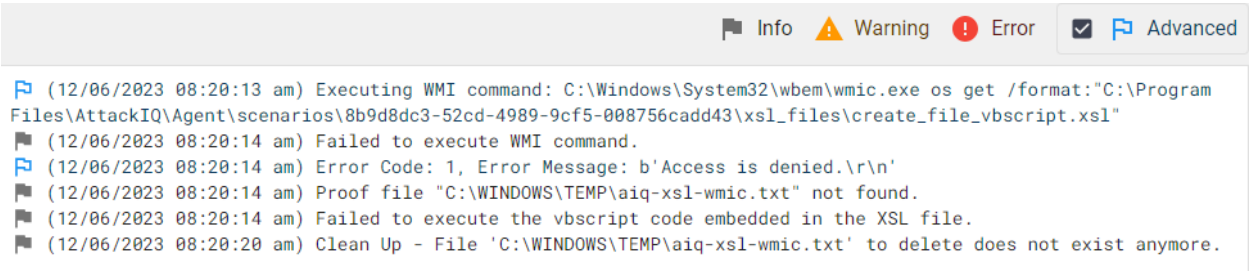

Figure 12. AttackIQ activity details for Test 9 against system 86 (AttackIQ, 2023)

Test 9 aligns with Test 7 and 3, where the telemetry does not change in solo and stacked configurations. Microsoft Defender captured the indicators of compromise in the full telemetry but generated no alerts, and CrowdStrike Falcon captured the telemetry and generated alerts. Full telemetry is required to find indicators with Microsoft Defender; the alert telemetry was capable in a stacked configuration or just CrowdStrike Falcon.

AttackIQ scenario nine generated two indicators of compromise artifacts. Presence of IOCs included in full telemetry for Test 9 had a rate of visibility of 100% for Defender, 100% for Falcon, and 100% for the configuration of Defender as primary and Falcon as secondary. Alert telemetry had a rate of visibility of 0% for Defender, 100%

for Falcon, and 50% for the configuration of Defender as primary and Falcon as secondary (Defender, Falcon, Splunk Log Telemetry, 2023).

3.1.10. Test 10 – Registry Update for Remote Assistance

The tenth test executed by AttackIQ consists of enabling remote assistance capabilities on the system through registry edits. The simulated attack creates and modifies a registry key through the reg add command with the value "AllowToGetHelp" and a data field 1.

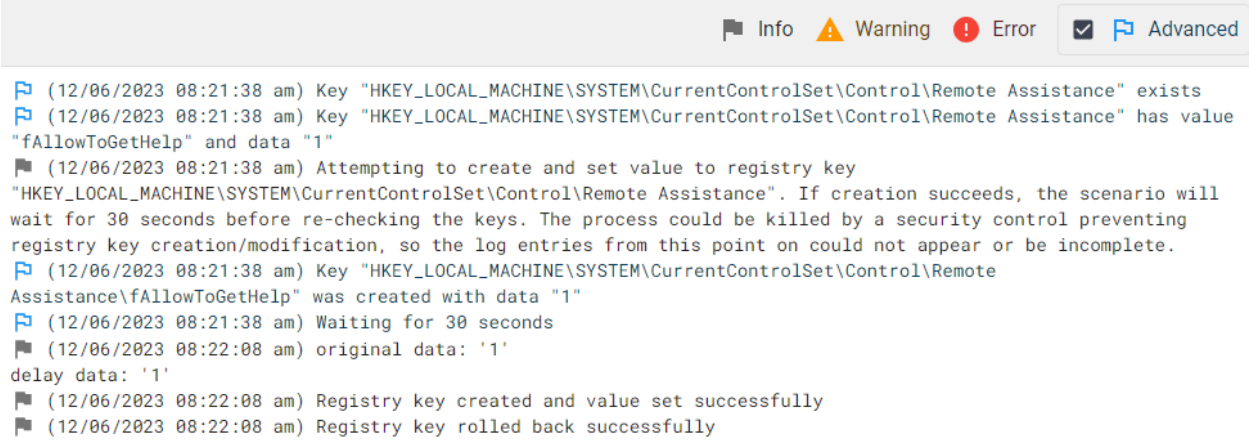

Figure 13. AttackIQ activity details for Test 10 against System 85 (AttackIQ, 2023)

CrowdStrike Falcon and Microsoft Defender capture the indicators of compromise but fail to generate alerts in both a solo and dual/stacked configuration. Full telemetry is required to find indicators; the alert telemetry was insufficient.

AttackIQ scenario ten generated two indicators of compromise artifacts. The presence of IOCs included in full telemetry for Test 10 had a rate of visibility of 100% for Defender, 100% for Falcon, and 100% for the configuration of Defender as primary and Falcon as secondary. Alert telemetry had a rate of visibility of 0% for Defender, 0% for Falcon, and 0% for the configuration of Defender as primary and Falcon as secondary (Defender, Falcon, Splunk Log Telemetry, 2023).

3.2. False Positives

When utilizing BAS tools to conduct automated attack testing, the telemetry and alerts must be analyzed for instances where the setup and cleanup activities generated telemetry and alerts. These actions are taken before and after each simulated attack to ensure the system is returned to its original state. These artifacts could be assumed to be detections of the simulated attack and skew the analysis of available artifacts. AttackIQ utilizes a standard setup name and provides full logging capability that makes finding these stray objects easy. There were multiple instances where the BAS Python script file used to initiate the attack was detected or cleanup activities to return the system to its previous state. A specific example is shown below from Test 1 where cleanup activities removed the created shadow copy file. Although a good detection, this is not a part of the attack and was not counted during the analysis.

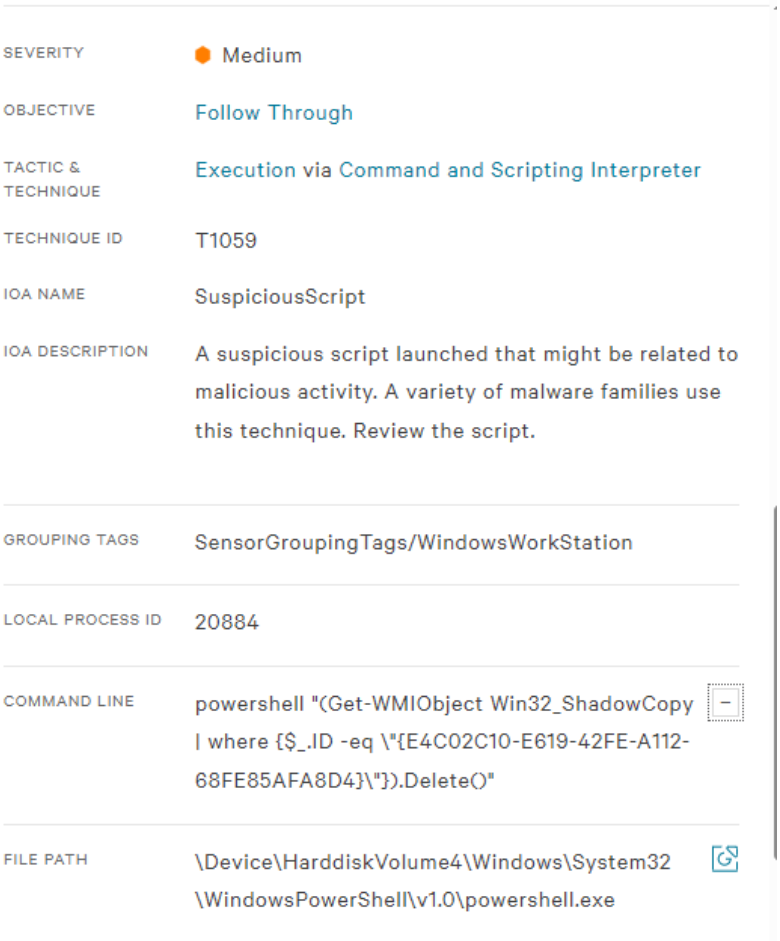

Figure 14. CrowdStrike Falcon alert for delete of shadow copy

3.3. Statistical Significance

The prevalence of indicators of compromise available inside the tool telemetry versus alerts is drastically higher. Each of the three configurations full telemetry outperformed the alert telemetry and demonstrated a statistical significance with a p-value of .001. This value was calculated utilizing a T test inside Excel. An array average value for the full telemetry successes, an array of the average value for the alert telemetry successes, two tails, and type one was utilized. Full telemetry included the indicator of compromise at an average rate of 75%, where alerts telemetry was at 39%. Full EDR configurations ranged from 72.41% to 79.41%. The same configurations for alerts ranged from 37.7% to 41.18%. The full telemetry captured by EDR is preferred if both sets of logs are available.

Figure 15 shows the prevalence of indicators of compromise between alert ingestion and tool telemetry for configuring Defender and CrowdStrike on one system.

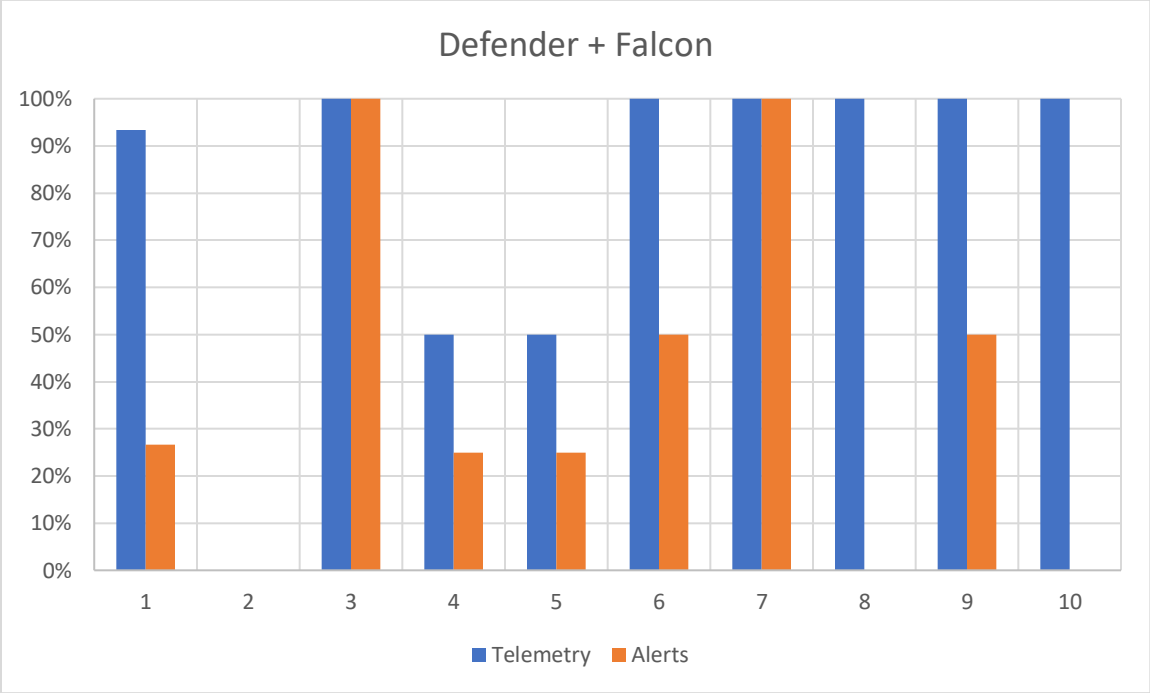

Figure 15. Total indicators of compromise present in data sets.

3.4. Summary of Findings

Neither the alert nor full telemetry captured all available IOCs during the simulated attacks. Although the full telemetry is better as should be expected, each allowed for a threat hunt to provide a false negative where an attack took place, but threat hunting would not find an artifact from it based on these sources alone. The tables below show the complete findings for all three systems and their security control telemetry and alerts generated and ingested into an SIEM. Extraction of AttackIQ indicators of compromise came from log files from all three systems and ingested log alerts from CrowdStrike Falcon and Microsoft Defender for Endpoint.

Indicator of Compromise - System 85 (Part 1)	Defender	
	Telemetry	Alert
powershell "$PSVersionTable.PSVersion | Select -ExpandProperty Major"	Yes	No
powershell "(Get-WMIObject Win32_ShadowCopy -List).Create(\"C:\\\\\", \"ClientAccessible\") | Select-Object ReturnValue,ShadowID | ConvertTo-Json"	Yes	No
powershell "(Get-WMIObject Win32_ShadowCopy | where {$_.ID -eq \"{4FC2E7E7-98BB-48AE-8982-9705BEA6033D}\"}).DeviceObject"	Yes	No
mimilib.dll	Yes	Yes
mimidrv.sys	Yes	Yes
C:\WINDOWS\TEMP\3xnnjbaivud8f\files\e7f9f801-5e87-47db-9001-a0c678d6b8fe\mimikatz-x64.zip	Yes	No
C:\WINDOWS\TEMP\3xnnjbaivud8f\files\e7f9f801-5e87-47db-9001-a0c678d6b8fe\x64\mimikatz.exe	Yes	Yes
C:\WINDOWS\TEMP\3xnnjbaivud8f\files\e7f9f801-5e87-47db-9001-a0c678d6b8fe\x64\mimikatz.exe "lsadump::sam /system:C:\WINDOWS\TEMP\ai_v14qnxbb /sam:C:\WINDOWS\TEMP\ai_xw8kh4h6" exit	No	No
/7b5fbbd90eab5bee6f3c25aa3c2762104e219f96501ad6a4463e25e6001eb00b/user.exe	No	No
malware.scenarios.attackiq-ntm.com	No	No
GET	No	No
user.exe	No	No
C:\WINDOWS\TEMP\59f42ecde152f78731e54ea27e761bba748c9309a6ad1c2fd17f0e8b90f8aed1_Fi90SOTO.exe	Yes	Yes
C:\WINDOWS\TEMP\copied_59f42ecde152f78731e54ea27e761bba748c9309a6ad1c2fd17f0e8b90f8aed1_FEvOhl14.exe	Yes	Yes
C:\WINDOWS\TEMP\59f42ecde152f78731e54ea27e761bba748c9309a6ad1c2fd17f0e8b90f8aed1_Fi90SOTO.exe	Yes	Yes
C:\WINDOWS\TEMP\copied_59f42ecde152f78731e54ea27e761bba748c9309a6ad1c2fd17f0e8b90f8aed1_FEvOhl14.exe	Yes	Yes
C:\WINDOWS\TEMP\JPEGView_Ehfioevh.exe	Yes	Yes
C:\WINDOWS\TEMP\copied_JPEGView_v0rG31Zx.exe	No	No
C:\WINDOWS\TEMP\JPEGView_Ehfioevh.exe	Yes	Yes
C:\WINDOWS\TEMP\copied_JPEGView_v0rG31Zx.exe	No	No
C:\WINDOWS\TEMP\ai-hkzm8m8c.mof	Yes	No
C:\WINDOWS\TEMP\ai-a8akr_ft.log	Yes	No
C:\WINDOWS\System32\Wbem\mofcomp.exe C:\WINDOWS\TEMP\ai-hkzm8m8c.mof	Yes	No
C:\WINDOWS\system32\cmd.exe /c echo AttackIQ WMI Persistence	Yes	No
'ProcessHollowing_x64.exe' 'C:\WINDOWS\system32\svchost.exe' 'C:\WINDOWS\TEMP\aiqy98s5qgvpayload\SleepingBinary5sec.exe'	Yes	Yes
C:\WINDOWS\TEMP\ProcessHollowing_x64.exe	Yes	Yes
C:\WINDOWS\system32\svchost.exe	Yes	Yes
Rubeus.exe	Yes	Yes
C:\WINDOWS\TEMP\yPz8S0l8bu8s9\files\a55b7b33-24de-4222-8e2c-b560cc9e5e52\Rubeus.exe kerberoast /format:hashcat /outfile:C:\WINDOWS\TEMP\q0ugvf_n.hashcat	Yes	Yes
nmap.exe -oX - -vvv --stats-every 1s --host-timeout 20m -sS -n -Pn -p1-65535 open-ports.scenarios.attackiq-ntm.com	Yes	No
C:\Program Files\AttackIQ\Agent\scenarios\8b9d8dc3-52cd-4989-9cf5-008756cadd43\xsl_files\create_file_vbscript.xsl	Yes	No
C:\Windows\System32\wbem\wmic.exe os get /format:"C:\Program Files\AttackIQ\Agent\scenarios\8b9d8dc3-52cd-4989-9cf5-008756cadd43\xsl_files\create_file_vbscript.xsl"	Yes	No
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Remote Assistance	Yes	No
reg add HKLM\SYSTEM\CurrentControlSet\Control\Remote Assistance /v fAllowToGetHelp /d 1 /f /t REG_DWORD	Yes	No

Figure 16. System 85 Indicators of Compromise Summary

Indicator of Compromise - System 86	Falcon	
	Telemetry	Alert
powershell "$PSVersionTable.PSVersion | Select -ExpandProperty Major"	Yes	No
powershell "(Get-WMIObject Win32_ShadowCopy -List).Create(\"C:\\\\\", \"ClientAccessible\") | Select-Object ReturnValue,ShadowID | ConvertTo-Json"	Yes	No
powershell "(Get-WMIObject Win32_ShadowCopy | where {$_.ID -eq \"{00AF3380-3720-43C9-B45E-A688D4EB84D4}\"}).DeviceObject"	Yes	No
mimilib.dll	Yes	Yes
mimidrv.sys	Yes	No
mimikatz-x64.zip	Yes	No
mimikatz.exe	Yes	Yes
/7b5fbbd90eab5bee6f3c25aa3c2762104e219f96501ad6a4463e25e6001eb00b/user.exe	No	No
malware.scenarios.attackiq-ntm.com	No	No
GET	No	No
user.exe	No	No
C:\WINDOWS\TEMP\59f42ecde152f78731e54ea27e761bba748c9309a6ad1c2fd17f0e8b90f8aed1_tUxVyZXH.exe	Yes	Yes
C:\WINDOWS\TEMP\copied_59f42ecde152f78731e54ea27e761bba748c9309a6ad1c2fd17f0e8b90f8aed1_GOf1ybcc.exe	No	No
C:\WINDOWS\TEMP\59f42ecde152f78731e54ea27e761bba748c9309a6ad1c2fd17f0e8b90f8aed1_tUxVyZXH.exe	Yes	No
C:\WINDOWS\TEMP\copied_59f42ecde152f78731e54ea27e761bba748c9309a6ad1c2fd17f0e8b90f8aed1_GOf1ybcc.exe	No	No
C:\WINDOWS\TEMP\JPEGView_JoRzU67C.exe	Yes	Yes
C:\WINDOWS\TEMP\copied_JPEGView_REZX5pN1.exe	No	No
C:\WINDOWS\TEMP\JPEGView_JoRzU67C.exe	Yes	Yes
C:\WINDOWS\TEMP\copied_JPEGView_REZX5pN1.exe	No	No
C:\WINDOWS\TEMP\ai-qjw7ls5b.mof	Yes	Yes
C:\WINDOWS\TEMP\ai-ep5yqawl.log	Yes	No
C:\WINDOWS\TEMP\ProcessHollowing_x64.exe	Yes	Yes
Rubeus.exe	Yes	Yes
C:\WINDOWS\TEMP\Ov1Iffdo47x0o\files\a55b7b33-24de-4222-8e2c-b560cc9e5e52\Rubeus.exe kerberoast /format:hashcat /outfile:C:\WINDOWS\TEMP\ndqmc_yz.hashcat	Yes	Yes
nmap.exe -oX - -vvv --stats-every 1s --host-timeout 20m -sS -n -Pn -p1-65535 open-ports.scenarios.attackiq-ntm.com	Yes	No
C:\Program Files\AttackIQ\Agent\scenarios\8b9d8dc3-52cd-4989-9cf5-008756cadd43\xsl_files\create_file_vbscript.xsl	Yes	Yes
C:\Windows\System32\wbem\wmic.exe os get /format:"C:\Program Files\AttackIQ\Agent\scenarios\8b9d8dc3-52cd-4989-9cf5-008756cadd43\xsl_files\create_file_vbscript.xsl"	Yes	Yes
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Remote Assistance	Yes	No
reg add HKLM\SYSTEM\CurrentControlSet\Control\Remote Assistance /v fAllowToGetHelp /d 1 /f /t REG_DWORD	Yes	No

Figure 17. System 86 Indicators of Compromise Summary

Indicator of Compromise	Defender		Falcon	
	Telemetry	Alert	Telemetry	Alert
powershell "$PSVersionTable.PSVersion | Select -ExpandProperty Major"	Yes	No	Yes	No
powershell "(Get-WMIObject Win32_ShadowCopy -List).Create(\"C:\\\\\", \"ClientAccessible\") | Select-Object ReturnValue,ShadowID | ConvertTo-Json"	Yes	No	Yes	No
powershell "(Get-WMIObject Win32_ShadowCopy | where {$_.ID -eq \"{E4C02C10-E619-42FE-A112-68FE85AFA8D4}\"}).DeviceObject"	Yes	No	Yes	No
mimilib.dll	Yes	Yes	Yes	Yes
mimidrv.sys	Yes	Yes	Yes	No
C:\WINDOWS\TEMP\hh22Q638dtkxk\files\e7f9f801-5e87-47db-9001-a0c678d6b8fe\mimikatz-x64.zip	Yes	No	Yes	No
C:\WINDOWS\TEMP\hh22Q638dtkxk\files\e7f9f801-5e87-47db-9001-a0c678d6b8fe\x64\mimikatz.exe	Yes	Yes	Yes	No
C:\WINDOWS\TEMP\hh22Q638dtkxk\files\e7f9f801-5e87-47db-9001-a0c678d6b8fe\x64\mimikatz.exe "lsadump::sam /system:C:\WINDOWS\TEMP\ai_at_unwpt /sam:C:\WINDOWS\TEMP\ai_lumggmep" exit	No	No	N/A	N/A
/7b5fbbd90eab5bee6f3c25aa3c2762104e219f96501ad6a4463e25e6001eb00b/user.exe	No	No	No	No
malware.scenarios.attackiq-ntm.com	No	No	No	No
GET	No	No	No	No
user.exe	No	No	No	No
C:\WINDOWS\TEMP\59f42ecde152f78731e54ea27e761bba748c9309a6ad1c2fd17f0e8b90f8aed1_hatrgSid.exe	Yes	Yes	Yes	Yes
C:\WINDOWS\TEMP\copied_59f42ecde152f78731e54ea27e761bba748c9309a6ad1c2fd17f0e8b90f8aed1_f3C4HwPA.exe	Yes	Yes	Yes	Yes
C:\WINDOWS\TEMP\59f42ecde152f78731e54ea27e761bba748c9309a6ad1c2fd17f0e8b90f8aed1_hatrgSid.exe	Yes	Yes	Yes	Yes
C:\WINDOWS\TEMP\copied_59f42ecde152f78731e54ea27e761bba748c9309a6ad1c2fd17f0e8b90f8aed1_f3C4HwPA.exe	Yes	Yes	Yes	Yes
C:\WINDOWS\TEMP\JPEGView_QDuWEF2Q.exe	Yes	Yes	Yes	No
C:\WINDOWS\TEMP\copied_JPEGView_URryYk2l.exe	No	No	No	No
C:\WINDOWS\TEMP\JPEGView_QDuWEF2Q.exe	Yes	Yes	Yes	No
C:\WINDOWS\TEMP\copied_JPEGView_URryYk2l.exe	No	No	No	No
C:\WINDOWS\TEMP\ai-9s06fgo0.mof	No	No	Yes	Yes
C:\WINDOWS\TEMP\ai-fssvg2w1.log	No	No	Yes	No
ProcessHollowing_x64.exe' 'C:\WINDOWS\system32\svchost.exe' 'C:\WINDOWS\TEMP\aiqx78l159kpayload\SleepingBinary5sec.exe'	Yes	No	Yes	Yes
C:\WINDOWS\TEMP\ProcessHollowing_x64.exe	Yes	No	Yes	Yes
Rubeus.exe	Yes	Yes	Yes	Yes
C:\WINDOWS\TEMP\WCXWIere9unn3\files\a55b7b33-24de-4222-8e2c-b560cc9e5e52\Rubeus.exe kerberoast /format:hashcat /outfile:C:\WINDOWS\TEMP\momyxj33.hashcat	Yes	Yes	Yes	Yes
nmap.exe -oX - -vvv --stats-every 1s --host-timeout 20m -sS -n -Pn -p1-65535 open-ports.scenarios.attackiq-ntm.com	Yes	No	Yes	No
C:\Program Files\AttackIQ\Agent\scenarios\8b9d8dc3-52cd-4989-9cf5-008756cadd43\xsl_files\create_file_vbscript.xsl	Yes	No	Yes	Yes
C:\Windows\System32\wbem\wmic.exe os get /format:"C:\Program Files\AttackIQ\Agent\scenarios\8b9d8dc3-52cd-4989-9cf5-008756cadd43\xsl_files\create_file_vbscript.xsl"	Yes	No	Yes	Yes
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Remote Assistance	Yes	No	Yes	No
reg add HKLM\SYSTEM\CurrentControlSet\Control\Remote Assistance /v fAllowToGetHelp /d 1 /f /t REG_DWORD	Yes	No	Yes	No

Figure 18. System 87 Indicators of Compromise Summary

4. Recommendations and Implications

4.1. Recommendations for Threat Hunting

This research has shown that the alert telemetry from EDR tools contains roughly 40% of the available indicators. While better, full telemetry still misses one in four indicators at 75% of available indicators. Although full telemetry produces a great chance of finding indicators, each still comes with the same limitation that it is likely to miss artifacts. Organizations should always opt for more telemetry when financially feasible, but the additional telemetry will not ensure a gap does not exist.

Although valuable, threat hunting should be viewed in context that certain actions could have taken place and were not captured in telemetry. The research findings of the ten tests continue to show that when an indicator of compromise is not present, this does not guarantee the attack did not take place.

4.2. Implications for Future Research

The recommendations and research provided focused on the differences in available indicators of compromise between full EDR logging available at additional cost and alert logging provided by default. In the process of that research, more topics and inconsistencies require further research.

4.2.1. Dual Endpoint Detection and Response Tool Configurations

Multiple tests demonstrated inconsistencies in the telemetry and alerting logic of both Microsoft Defender for Endpoint P2 and CrowdStrike Falcon when running on the same system. Further testing may show the telemetry to be inconsistent over multiple executions.

The research demonstrated that when one tool partially blocks a process or file, it is unknown to the secondary tool. An analyst could misclassify the incident, requiring further research to understand the implications.

4.2.2. The missing 20%

Although the research clearly showed that one data set is more suited for threat hunting. Further research and analysis into the missing 20% of indicators of compromise. Comparison with Windows event logs and system monitoring would shed light on what was available to the EDR tools.

5. Conclusion

The amount of telemetry collected by organizations is a complex decision based on multiple variables. The research has shown that utilizing modern EDR tools such as Windows Defender and CrowdStrike Falcon will not capture 100% of artifacts. Having this context about its completeness will allow cybersecurity professionals to understand the differences each environment presents and challenge them to test their own environment to establish a baseline. Understanding the chance an artifact happened and is not present gives context to threat-hunting results.

Did this command take place? Has this process run inside our environment? Does this file exist on our systems? With the proper context and answers to these questions, threat hunting can correctly influence a sound decision-making process and reduce risk for the organization. The challenge of our original question still stands: have they asked the question to the correct data set or introduced a false negative into the decision-making process?

This research and analysis have shown that the full capture telemetry inside the EDR tool is superior to the alert logs but does not capture 100% of the artifacts from an attack. This lack of completeness allows for the possibility that an attack could have taken place even if the telemetry does not show any IOCs from it.

References

Aldauiji, F., Batarfi, O., & Bayousef, M. (2022). *Utilizing cyber threat hunting techniques to find ransomware attacks: A survey of the state of the art.* IEEE Access, 10, 61695–61706. https://doi.org/10.1109/access.2022.3181278

AttackIQ [Computer Software]. (2023). Retrieved from https://www.attackiq.com

CrowdStrike. (2023, August 11). *What are indicators of compromise? IOC explained - crowdstrike*. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/

CrowdStrike. (2023, April 17). *Threat Hunting.* crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/threat-hunting/

CrowdStrike. (2023, March 1). *Kerberoasting Attacks.* crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/kerberoasting/

DAMBRA, S., BILGE, L., & BALZAROTTI, D. (2023). A Comparison of Systemic and Systematic Risks of Malware Encounters in Consumer and Enterprise Environments. ACM Transactions on Privacy & Security, 26(2), 1–30. https://doi.org/10.1145/3565362

Gartner, Inc. (n.d.). *Best breach and attack simulation (BAS) tools reviews 2024: Gartner Peer insights*. https://www.gartner.com/reviews/market/breach-and-attack-simulation-bas-tools

Lakshmanan, R. (2023, February 15). *Experts warn of "beep" - A new evasive malware that can fly under the Radar*. The Hacker News. https://thehackernews.com/2023/02/experts-warn-of-beep-new-evasive.html

LEMOS, R. (2018). On the Hunt for Security: Tired of waiting for signs of an attack, companies large and small add threat hunting capabilities to their playbooks. Information Security, 20(6), 4–9.

Perumal, P. S. (2022, June 12). *Triaging Windows Event Logs for Ransomware Investigations. SANS Institute*. https://www.sans.org/white-papers/triaging-windows-event-logs-for-ransomware-investigations/

85_Defender_Splunk.csv. (2023, December 17).

85_Defender_Telemetry_6Dec.csv (2023, December 17).

Jeffrey Legg, jeffrey.legg@student.sans.edu

86_Defender_Splunk.csv. (2023, December 17).

86_Defender_Telemetry_6Dec.csv (2023, December 17).

86_Falcon_Splunk.csv. (2023, December 17).

86_Falcon_Telemetry_6Dec.csv (2023, December 17).

87_Defender_Splunk.csv. (2023, December 17).

87_Defender_Telemetry_6Dec.csv (2023, December 17).

87_Falcon_Splunk.csv. (2023, December 17).

Appendix A
System Configurations

Victim System 1 (85):

Windows 10 64-bit

(Release 21H2 Build 19044.3693)

1.1.16400.2 – Defender Version

None – CrowdStrike Falcon

Victim System 2 (86):

Windows 10 64-bit

(Release 21H2 Build 19044.3693)

1.1.16400.2 – Defender Version

Defender Antivirus Mode – Passive

7.01.17312.0 – CrowdStrike Falcon Version

Victim System 3 (87):

Windows 10 64-bit

(Release 21H2 Build 19044.3693)

1.1.16400.2 – Defender Version

7.01.17312.0 – CrowdStrike Falcon Version

Appendix B
AttackIQ Test Scenarios

Date	Assessment	MITRE tactics	Test	Scenario	User Privileges	Asset
12/06/2023 **07:54 am**	Threat Detection and Response Test	Credential Access	Test 1	Dump SAM hashes with Mimikatz using a Volume Shadow Copy	SYSTEM	[redacted]085
12/06/2023 **07:56 am**	Threat Detection and Response Test	Command And Control	Test 1	Download 2021-11 APT35's user.exe Sample to Memory	SYSTEM	[redacted]085
12/06/2023 **07:56 am**	Threat Detection and Response Test	Command And Control	Test 1	Save 2023-02 Beep DLL Injector to File System	SYSTEM	[redacted]085
12/06/2023 **07:57 am**	Threat Detection and Response Test	Command And Control	Test 1	Save 2018-09 Turla PNG Dropper to File System	SYSTEM	[redacted]085
12/06/2023 **07:58 am**	Threat Detection and Response Test	Persistence	Test 1	Persistence Through WMI	SYSTEM	[redacted]085
12/06/2023 **07:58 am**	Threat Detection and Response Test	Defense Evasion	Test 1	Process Hollowing	SYSTEM	[redacted]085
12/06/2023 **07:59 am**	Threat Detection and Response Test		Test 1	Attack with Rubeus	SYSTEM	[redacted]085
12/06/2023 **08:20 am**	Threat Detection and Response Test		Test 1	Egress Open Ports Checker	SYSTEM	[redacted]085
12/06/2023 **08:21 am**	Threat Detection and Response Test	Defense Evasion	Test 1	XSL Script Processing Through WMI	SYSTEM	[redacted]085
12/06/2023 **08:22 am**	Threat Detection and Response Test	Defense Evasion	Test 1	Use Registry to Disable Security Features: Enable Remote Assistance Capabilities	SYSTEM	[redacted]085

Figure 19. AttackIQ attack simulations against host 85 (AttackIQ, 2023)

Date	Assessment	MITRE tactics	Test	Scenario	User Privileges	Asset
12/06/2023 **07:55 am**	Threat Detection and Response Test	Credential Access	Test 1	Dump SAM hashes with Mimikatz using a Volume Shadow Copy	SYSTEM	86
12/06/2023 **07:56 am**	Threat Detection and Response Test	Command And Control	Test 1	Download 2021-11 APT35's user.exe Sample to Memory	SYSTEM	86
12/06/2023 **07:56 am**	Threat Detection and Response Test	Command And Control	Test 1	Save 2023-02 Beep DLL Injector to File System	SYSTEM	86
12/06/2023 **07:57 am**	Threat Detection and Response Test	Command And Control	Test 1	Save 2018-09 Turla PNG Dropper to File System	SYSTEM	86
12/06/2023 **07:57 am**	Threat Detection and Response Test	Persistence	Test 1	Persistence Through WMI	SYSTEM	86
12/06/2023 **07:58 am**	Threat Detection and Response Test	Defense Evasion	Test 1	Process Hollowing	SYSTEM	86
12/06/2023 **07:58 am**	Threat Detection and Response Test		Test 1	Attack with Rubeus	SYSTEM	86
12/06/2023 **08:19 am**	Threat Detection and Response Test		Test 1	Egress Open Ports Checker	SYSTEM	86
12/06/2023 **08:20 am**	Threat Detection and Response Test	Defense Evasion	Test 1	XSL Script Processing Through WMI	SYSTEM	86
12/06/2023 **08:21 am**	Threat Detection and Response Test	Defense Evasion	Test 1	Use Registry to Disable Security Features: Enable Remote Assistance Capabilities	SYSTEM	86

Figure 20. AttackIQ attack simulations against host 86 (AttackIQ, 2023)

Date	Assessment	MITRE tactics	Test	Scenario	User Privileges	Asset
12/06/2023 **07:56 am**	Threat Detection and Response Test	Credential Access	Test 1	Dump SAM hashes with Mimikatz using a Volume Shadow Copy	SYSTEM	87
12/06/2023 **07:56 am**	Threat Detection and Response Test	Command And Control	Test 1	Download 2021-11 APT35's user.exe Sample to Memory	SYSTEM	87
12/06/2023 **07:57 am**	Threat Detection and Response Test	Command And Control	Test 1	Save 2023-02 Beep DLL Injector to File System	SYSTEM	87
12/06/2023 **07:58 am**	Threat Detection and Response Test	Command And Control	Test 1	Save 2018-09 Turla PNG Dropper to File System	SYSTEM	87
12/06/2023 **07:58 am**	Threat Detection and Response Test	Persistence	Test 1	Persistence Through WMI	SYSTEM	87
12/06/2023 **07:59 am**	Threat Detection and Response Test	Defense Evasion	Test 1	Process Hollowing	SYSTEM	87
12/06/2023 **07:59 am**	Threat Detection and Response Test		Test 1	Attack with Rubeus	SYSTEM	87
12/06/2023 **08:21 am**	Threat Detection and Response Test		Test 1	Egress Open Ports Checker	SYSTEM	87
12/06/2023 **08:21 am**	Threat Detection and Response Test	Defense Evasion	Test 1	XSL Script Processing Through WMI	SYSTEM	87
12/06/2023 **08:22 am**	Threat Detection and Response Test	Defense Evasion	Test 1	Use Registry to Disable Security Features: Enable Remote Assistance Capabilities	SYSTEM	87

Figure 21. AttackIQ attack simulations against host 87 (AttackIQ, 2023)