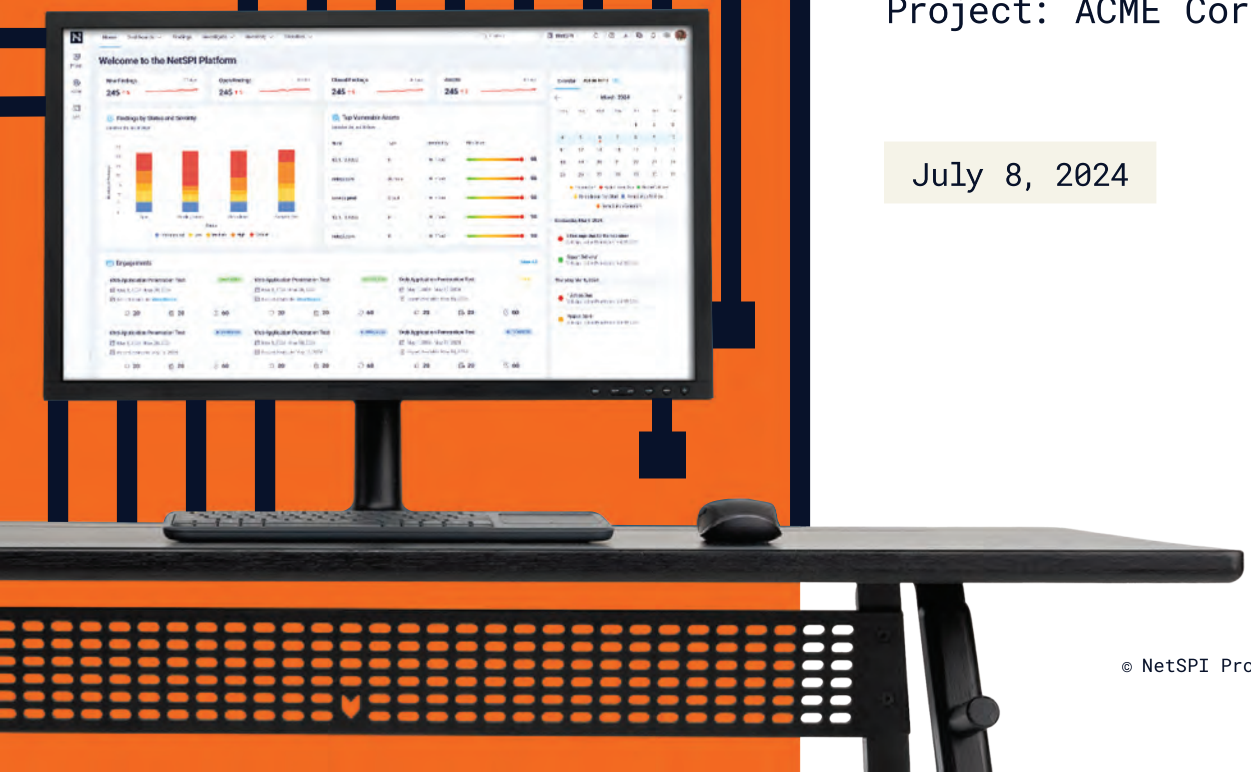
NetSPI™

Sample Security Audit Report

Breach and Attack Simulation

Project: ACME Corporation

July 8, 2024



Contents

Chapter 1 | Executive Summary ---- **4**
1.1 Project Objectives *4*
1.2 Engagement Summary *4*
1.3 Summary of Strengths *4*
1.4 Detection Overview *5*
1.4.1 Peer Comparison ---- 5
1.4.2 Data Source Coverage ---- 5
1.4.3 Detection and Alert Coverage ---- 7
1.4.4 Prevention Coverage ---- 8
1.4.5 YoY Summary ---- 9
1.4.6 Overall Visibility Summary ---- 13
1.4.7 Security Controls Summary ---- 14
1.5 Summary of Recommendations *15*
1.5.1 Short-term Recommendations ---- 15
1.5.2 Long-term Recommendations ---- 15
Chapter 2 | Project Overview ---- **16**
2.1 Scope *16*
2.2 Constraints *16*
2.3 Approach *16*
Chapter 3 | Technical Summary ---- **17**
3.1 Unit Test Summary *18*
Chapter 4 | Penetration Test Attack Narrative ---- **21**
4.1 Attack Narrative Summary *21*
4.2 Attack Narrative Details *21*
4.2.1 Initial Access: Hardware Additions - T1200 ---- 21
4.2.2 Persistence: Valid Accounts – Domain Accounts - T1078.002 ---- 21
4.2.3 Discovery: Network Service Discovery - T1046 ---- 22
4.2.4 Credential Access: Steal or Forge Authentication Certificates T1649 ---- 23
4.2.5 Privilege Escalation: Valid Accounts: Domain Accounts T1078.002 ---- 23
4.2.6 Credential Access: OS Credential Dumping - DCSync - T1003.006 ---- 23
Chapter 5 | Breach and Attack Evasion Summary ---- **25**
5.1 Control Evasion Summary *25*
5.2 Control Evasion Details *25*
5.2.1 Defense Evasion - PowerShell - Bypass AMSI (T1562.001) ---- 25
5.2.2 Defense Evasion – Security Software – Policy Exceptions (T1562.001) ---- 25
5.2.3 Defense Evasion - Process Manipulation - Process Hollowing (T1093) ---- 25
Chapter 6 | Unit Test Details ---- **26**

6.1 Overview.. 26
6.2 High UIP Techniques 26
6.2.1 Control Channel – Reverse Shell – TCP (T1095)---------------------- 26
6.2.2 Control Channel – Tunneling – ICMP Shell (T1572)------------------- 34
6.2.3 Data Exfiltration – BITS – Bitsadmin (T1048.003)------------------ 39
6.2.4 Data Exfiltration - Rclone (1048)---------------------------------- 42
6.2.5 Data Exfiltration – Tor (T1048.003) ------------------------------- 45
6.2.6 Inhibit System Recovery – Custom File Encryption (T1486) ---------- 47
6.2.7 Inhibit System Recovery – Delete Volume ShadowCopy (T1490)--------- 49
6.3 Medium UIP Techniques.. 55
6.3.1 Credential Access – Brute Force – Active Directory Attacks (T1110.003)------------ 55
6.3.2 Credential Access – Cached Domain Credentials Access (T1110.005) -------------- 58
6.3.3 Credential Access – SAM Access (T1003.005) ------------------------ 60
6.3.4 Credential Access – Wdigest Access (T1003.001)-------------------- 68
6.3.5 Lateral Movement – Authenticated Scanning – SMB (T1021.002) ------- 73
6.4 Low UIP Techniques 76
6.4.1 Discovery – Reconnaissance – DNS (T1018) -------------------------- 76
6.4.2 Discovery – Reconnaissance – Port Scan – TCP (T1046)-------------- 80
6.4.3 Discovery – Reconnaissance – SMB – Domain Trusts ------------------ 83
Appendix A | NetSPI Contact Information------------------------------------ 87
Revision History 88

Chapter 1 | Executive Summary

Between June 3, 2024, and June 17, 2024, NetSPI, performed a Breach and Attack Simulation against Acme Corp's (Acme's) IT infrastructure.

The purpose of this engagement was to validate existing detective controls and to help Acme improve their ability to identify and respond to common tactics, techniques, and procedures used by real-world cyber threats. During testing, NetSPI worked directly with the security operations team to perform attacks against the environment to generate security events and determine what level of visibility Acme has for each one.

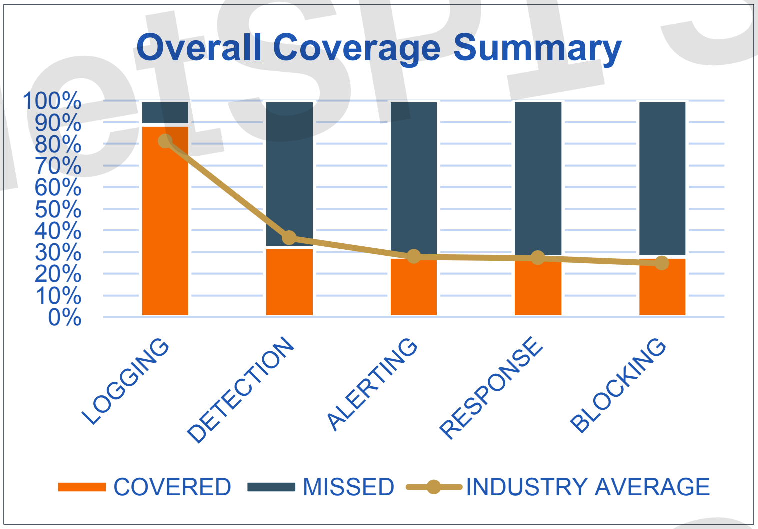
1.1 Project Objectives

The primary objectives during this project were to:

- Work with the Acme team to execute common tactics, techniques, and procedures that will generate security events that can be used to test detective controls.
- Identify detective control gaps that exist in multiple layers of Acme's environment.
- Provide Acme with an understanding of each of the identified weaknesses, overall detection trends, and prioritized remediation approach to address the identified issues.

1.2 Engagement Summary

Below is a summary of the detection coverage the security controls provided for the unit tests that were executed during the project. It should be noted that some coverage could not be implemented due to environmental noise created by normal business operations. More details can be found in Chapter 4:



COVERAGE SUMMARY DATA		
VISIBILITY	COVERED	MISSED
LOGGING	89%	11%
DETECTION	32%	68%
BLOCKING	28%	72%
ALERTING	28%	72%
RESPONSE	28%	72%

1.3 Summary of Strengths

Below is a summary of the detective controls' strengths observed during the project:

- 100% of the actionable alerts triggered a response from the security operations team.
- The controls can support custom detection, forensic investigations, and threat hunting.
- The team has the technology and tool understanding required to mature the existing detective control capabilities.
- The current controls provide good coverage for commodity malware.

1.4 Detection Overview

One of the biggest challenges facing security tooling vendors today is ensuring that their products do not generate too many false positives or environmental “white noise” after being deployed. To avoid those issues, most vendors only enable high-fidelity detections by default. Based on NetSPI’s experience, by default, most Endpoint Detection and Response (EDR) software only detects around 25% of the most common MITRE ATT&CK TTPs.

As a result of those vendor choices, Security Operations Center (SOC) teams must spend a lot of time developing custom detections that are not provided or enabled by default by the EDR vendor. The greatest challenge for many SOC teams is developing custom detections that provide a volume of alerts that can be sufficiently managed by their security analysts and managed service providers.

1.4.1 Peer Comparison

Compared to peers of a similar size and maturity level, Acme’s detective control capabilities have been ranked as **average**.

This was due to a few factors including:

- Excellent response rate from MSSP partner.
- Lack of custom detections built into detection pipeline.
- Low fidelity detections that have not been tuned correctly.
- Reliance on default settings in the environment.
- Low internal NetFlow visibility.

1.4.2 Data Source Coverage

Data sources are network, application, database, and endpoint events that create telemetry used to identify potentially malicious behavior in an environment. Without proper data sources, detections and alerts used by response teams cannot be created. Generically, data sources may also be referred to as logs.

Data Source Coverage Summary

Overall, Acme had data source coverage that could potentially be leveraged during investigations and to build new detections on 89% of all unit tests conducted. This is **above average**, as the average coverage is around 81%. The chart below shows 11% of the unit tests were missing data sources.

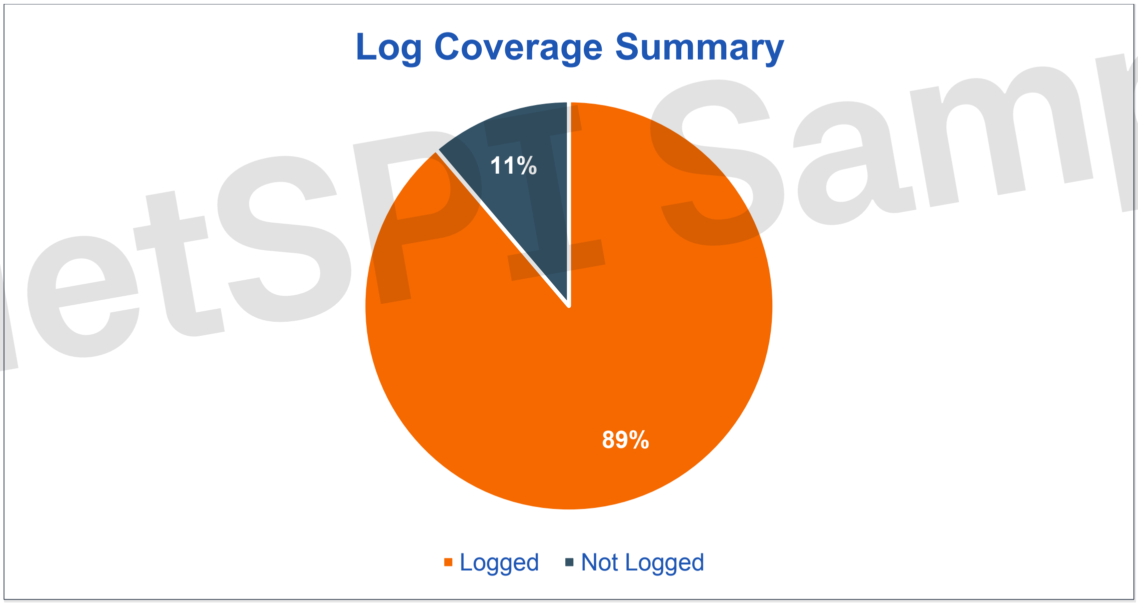


FIGURE 1: LOG COVERAGE SUMMARY

The chart below shows a breakdown of that coverage by tactic to help highlight gap categories. Data source gaps were related to a lack of internal network traffic data, and dns logs. The gaps resulted in limited visibly for a subset of the Discovery and Lateral Movement phases of the cyber kill chain.

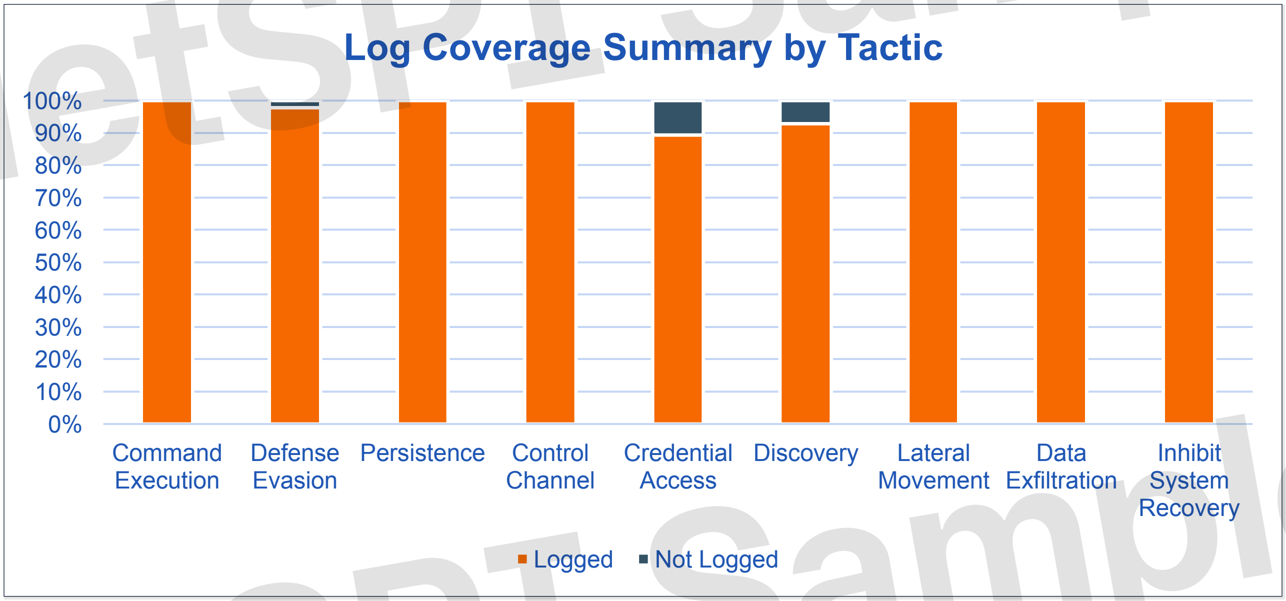


FIGURE 2: LOG COVERAGE SUMMARY BY TACTIC

Major Data Source Gaps
Below is summary of the specific data sources that are missing, disabled, not sent to the SIEM, or had broken data ingestion.

CATEGORY	AFFECTED COMPONENTS
Missing	• DNS Logs • Internal NetFlow • PowerShell Script Block Logging
Disabled	• None
Not Forwarded to SIEM	• None
Failed Importing into SIEM	• None

TABLE 1: MAJOR DATA SOURCE GAPS

1.4.3 Detection and Alert Coverage

Below is a summary of the detection and actionable alert coverage.

Detection Coverage
27% of all unit tests were detected at some level. This is **below average**, as the long-term goal should be to achieve between 60%-80% coverage. The intent should be to have enough cyber kill chain coverage to detect, block, and respond to a threat before they have a chance to accomplish their objectives. Due to the noise generated by normal business operations it's unlikely that it will be possible to hit 100% detection coverage.

Actionable Alert Coverage
An actionable alert is any event, detection, or correlation that warrants response based on criteria defined by the security operations team or managed security services provider.

The percentage of unit tests that generated actionable alerts was 28%. This is **average**, which is around 28%.

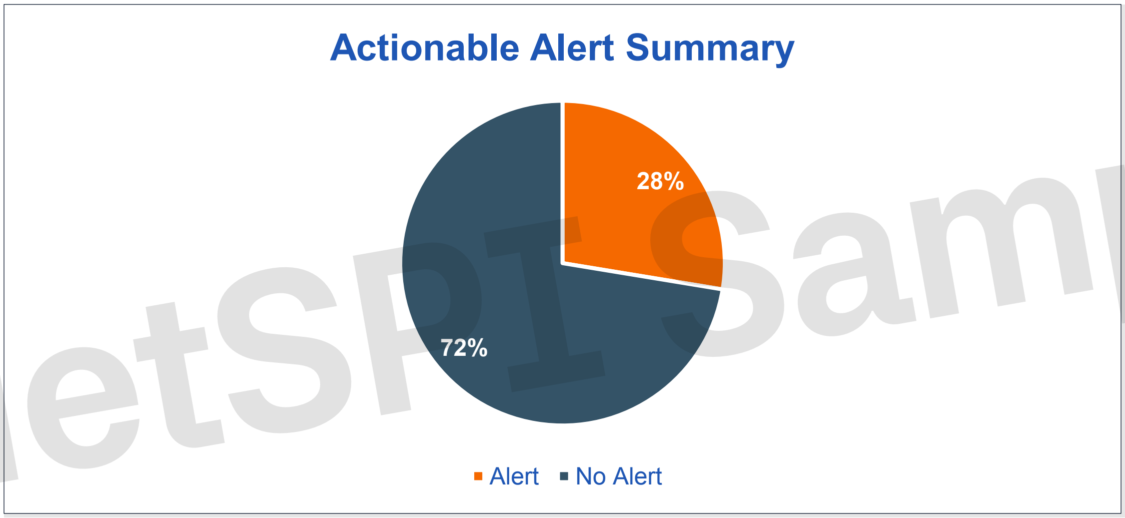


FIGURE 3: ACTIONABLE ALERT SUMMARY

Actionable Alert Coverage Breakdown
To provide additional context, the illustration below summarizes the visibility that Acme has into common techniques used within each phase of the MITRE ATT&CK post-exploitation process. The chart below shows that visibility into common Credential Access and Command Execution techniques represents some areas of strength.

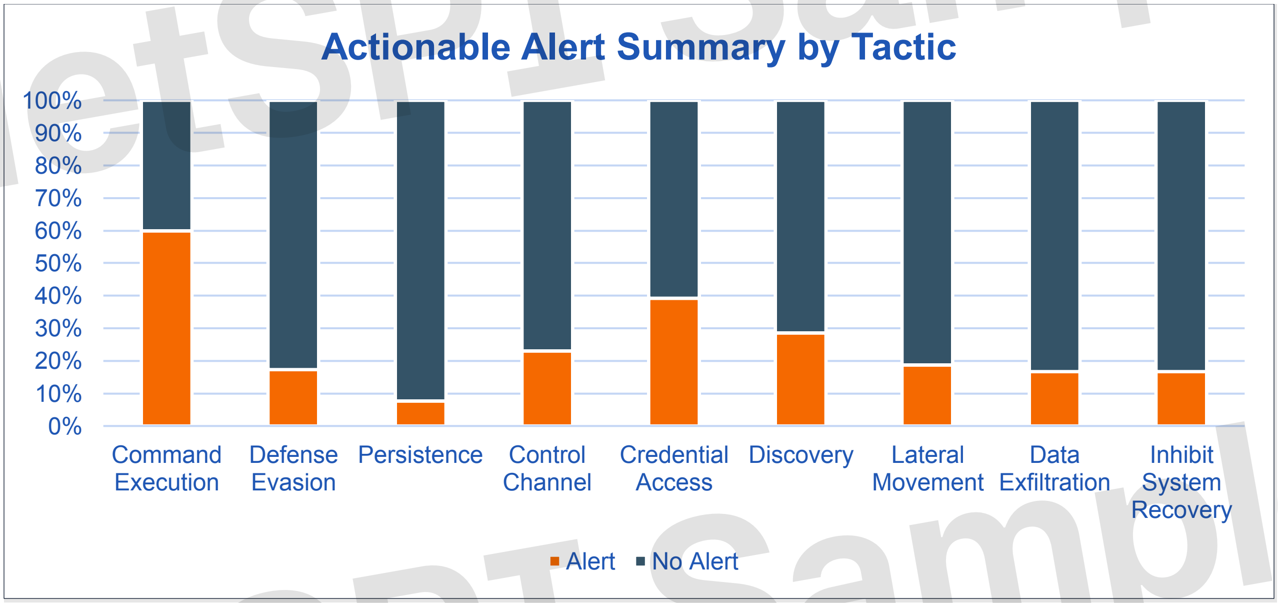


FIGURE 4: ACTIONABLE ALERT SUMMARY BY TACTIC

1.4.4 Prevention Coverage

Below is a summary of the prevention coverage.

Prevention Coverage
34% of all unit tests were prevented at some level. This is **above average**, as the average prevention coverage is around 22%. Prevention is an important step but also needs to be joined to alerting so that adversaries can be expelled from the environment before they are able to complete their objectives.

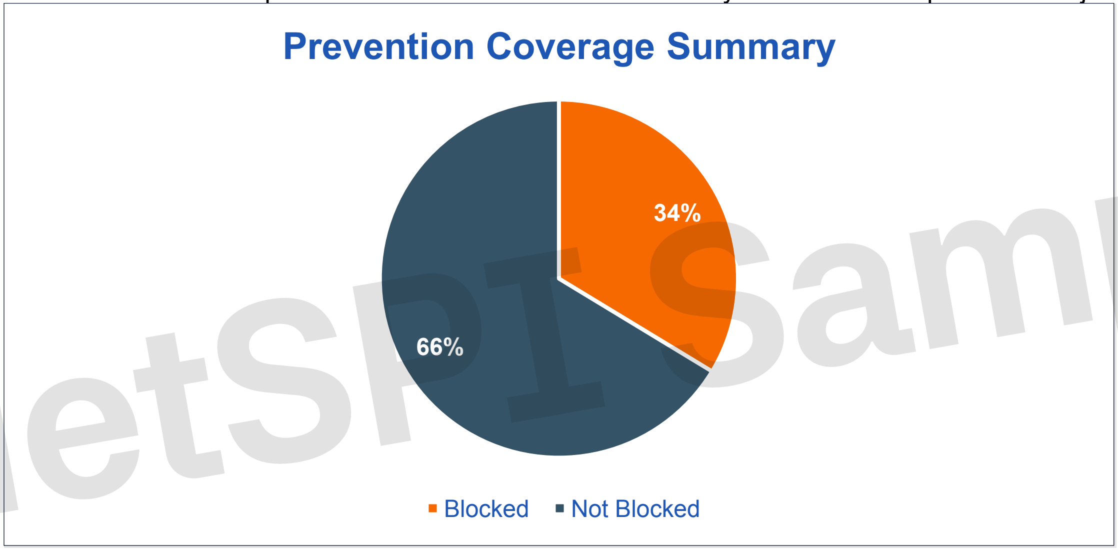


FIGURE 3: PREVENTION COVERAGE SUMMARY

Prevention Breakdown
To provide additional context, the illustration below summarizes Acme's ability to prevent common techniques used within each phase of the MITRE ATT&CK post-exploitation process. The chart below shows that prevention of Defense Evasion and Inhibit System Recovery techniques represents areas of strength relative to other areas.

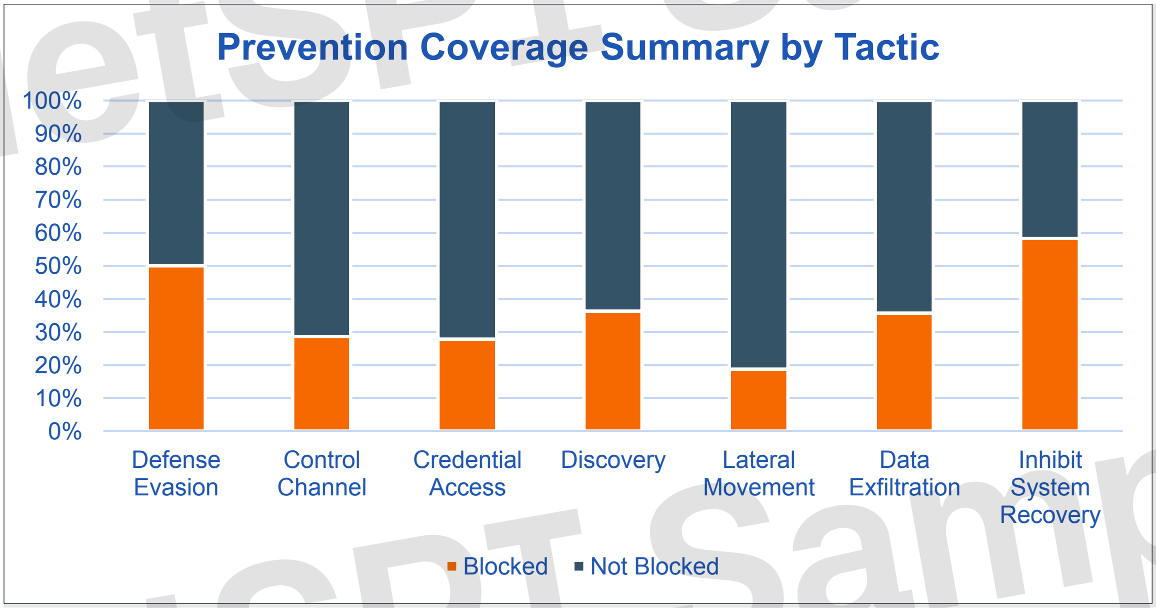
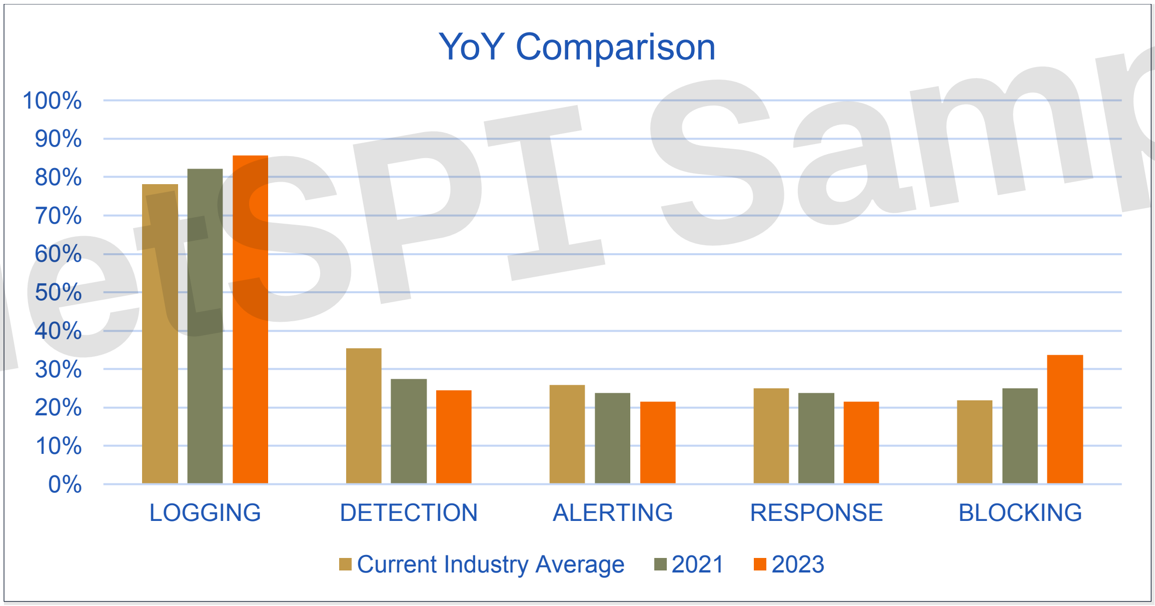


FIGURE 4: PREVENTION SUMMARY BY TACTIC

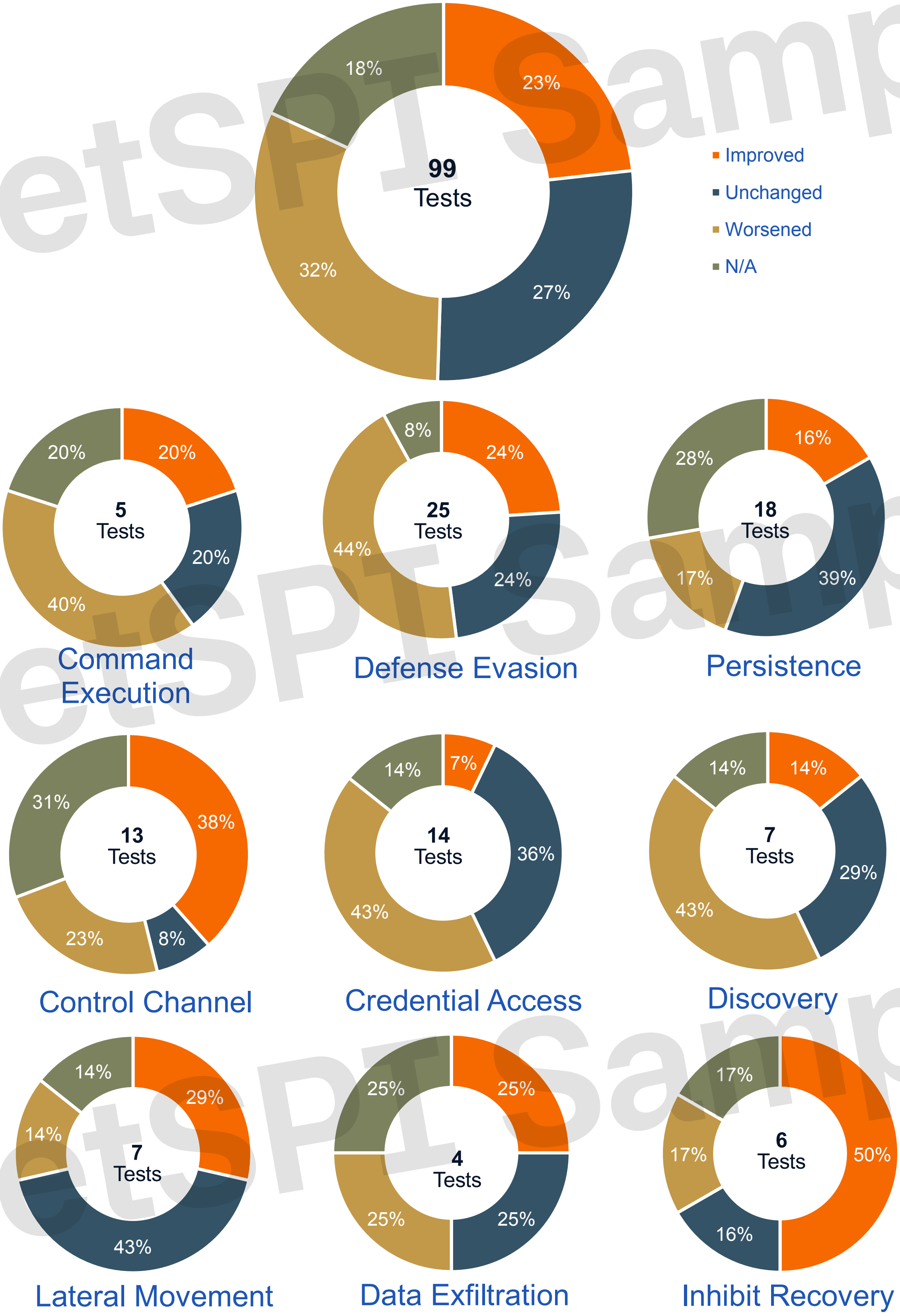
Comparison to the previous section also shows that when testing occurred, actionable alerts had not been developed for several of the detective control tests that were either fully or partially blocked.

1.4.5 YoY Summary

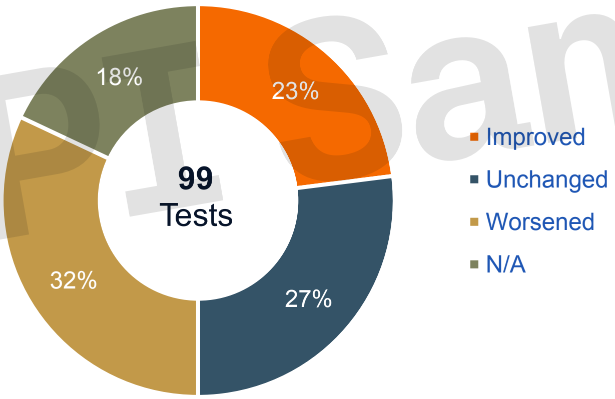
Overall compared to last year, NetSPI ran five new tests that do not have a correlation. Of the 44 tests re-run, 30% had a better outcome, 52% performed consistent with last year's performance, and 18% seemed to have degraded. This could be due to a couple of factors other than the degradation of detective or alerting capabilities. The number of procedures within tested techniques has changed to align with MITRE ATT&CK and as new techniques are seen in the wild. Below is a chart breaking out year-over-year (YoY) performance by tactic.

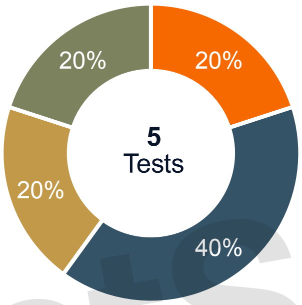

YoY Comparison
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
LOGGING
DETECTION
ALERTING
RESPONSE
BLOCKING
Current Industry Average
2021
2023

YoY Alerting

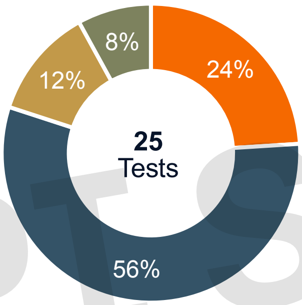


YoY Prevention

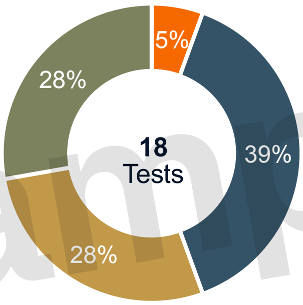




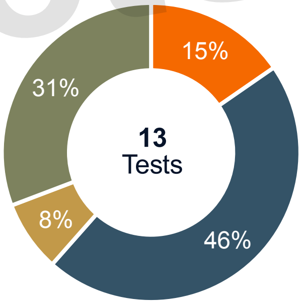
Command Execution



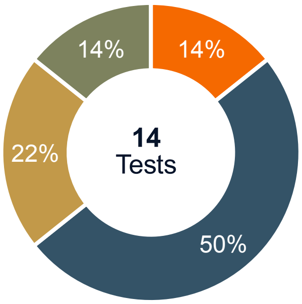
Defense Evasion



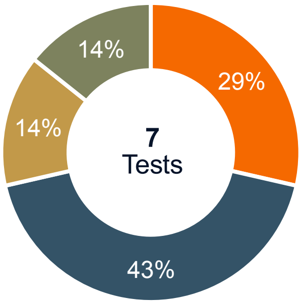
Persistence



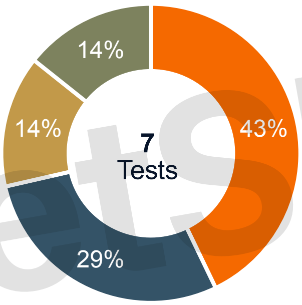
Control Channel



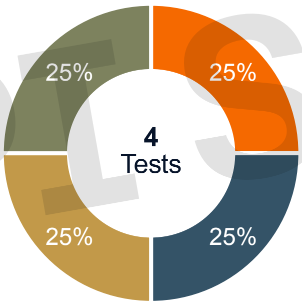
Credential Access



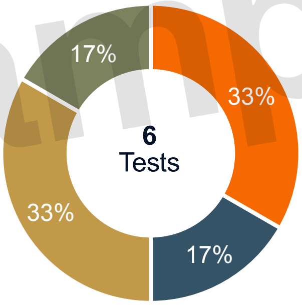
Discovery



Lateral Movement



Data Exfiltration



Inhibit Recovery

1.4.6 Overall Visibility Summary

The chart below provides a summary for overall visibility throughout the cyber kill chain.

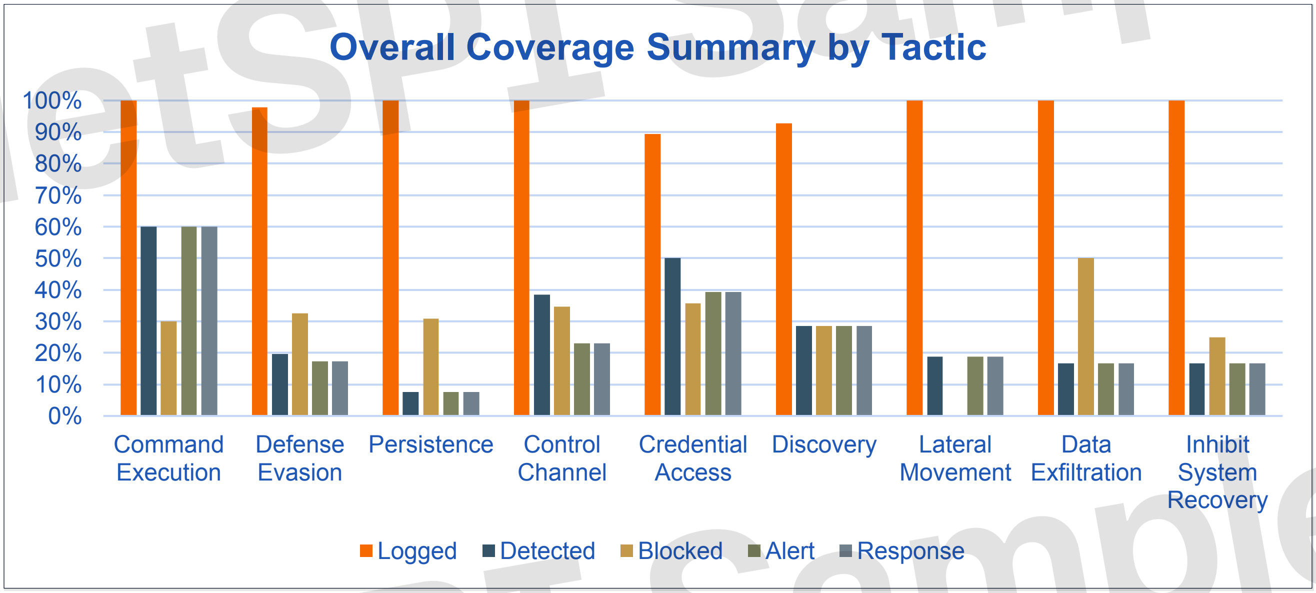


FIGURE 5: OVERALL COVERAGE SUMMARY BY TACTIC

1.4.7 Security Controls Summary

During this engagement multiple interviews were conducted with internal teams to inventory the technical detective controls being used. Below is a summary of that information broken out by detective control category.

#	CONTROL	SUMMARY
1	Asset and Vulnerability Management	Microsoft System Center Configuration Manager (SCCM) is the primary asset management database. SCCM is used to deploy standard images for VDIs, Workstations, and Servers.
2	Log Consolidation and SIEM Configuration	Logs are consolidated and sent to Splunk. Logs are retained for one year in Splunk.
3	Backup and Recovery Capabilities	Employee files are stored in personal folders on a network share. Veritas NetBackup is used to backup network shares, applications, databases, domain controllers, and virtual infrastructure. Hot Sites are in place to support failover if needed. Veritas NetBackup stores data in Hot Sites, but the sites may be domain joined. The Veritas NetBackup local credentials and service accounts are stored in LastPass. Overall, the backups are not hosted in an isolated network or Active Directory domain. However, there are some Domain Controller backups that are isolated from the default Active Directory Domain. Backups are available for 60 days.
4	Active Directory, Application, and Database Controls	LDAP queries from the client are not being logged. Some logs are present on the domain controller, but they may not provide full visibility. High profile groups are being monitored for changes, but robust auditing of high-risk Active Directory configurations and events could not be tested due to lack of Domain Admin privileges during the engagement.
5	Threat Intelligence, Threat Hunting, and Adversary Simulation	Splunk serves as the primary threat intelligence feed. However, there are also additional commercial threat feeds used that support the team. That information informs different processes including daily threat hunting activities. Internal adversary simulation activities are conducted during detection development, Additionally, a BAS tool is being deployed into the environment. Finally, quarterly penetration testing is conducted, and red/purple teaming is conduct biannually.
6	Cloud Environment Controls	Both Azure and AWS cloud environments are being used by Acme Corp and the associated logs are being sent to Splunk.
7	Email Controls	Symantec Messaging Gateway (SMG) and Exchange native controls are currently being used to identify email-based threats, logging them, and blocking them. Additionally, Sophos is running on the Exchange Server. Malicious attachments do not generate alerts, but if something does get delivered with a detection an alert will be generated. Every DLP alert is reviewed by a third party, and the privacy team gets the alerts. Many of the SMG settings appear to be default, and Acme Corp may want to consider a review. It is unclear how they operate in the web and mobile version. Only digitally signed macros are allowed to execute, and process parent relationships are monitored.
8	External Network Controls	Cisco Firepower, F5, and Palo Alto are all used as part of the perimeter control stack. Akamai offers DDOS protection capabilities for the primary site only. NetFlow data is ingested into Splunk.
9	Internal Network Controls	Carbon Black, Palo Alto, and Splunk are all used as part of the internal network technology stack. NetFlow data is available within Splunk. No network layer DLP was in place at the time of testing. A known blind

#	CONTROL	SUMMARY
		spot includes, when an attacker originates from the internet and attacks a web server exposed in the DMZ, the internet IP is not recorded, only the DMZ IP.
10	Windows Endpoint Controls	Configurations are managed and monitored using Sysmon, Nessus, Group Policy, SCCM, and AirWatch. SCCM is used for both OS and patch management. Nessus is used for vulnerability scanning. Tickets for non-compliance configurations and missing patches are fed into ServiceNow to track remediation efforts. McAfee is used as the DLP solution. Endpoint security software responsibility for logging, detecting, blocking, and generating alerts for threats include Carbon Black, Sysmon, Windows Defender, and Windows Event Logs. Workstations and Server's forward local logs to Splunk via the Splunk universal forwarder.

TABLE 2: SECURITY CONTROLS SUMMARY

1.5 Summary of Recommendations

NetSPI recommends improving and maturing your security program using the prioritized approach below.

1.5.1 Short-term Recommendations

- Plan and begin to execute detection strategy overhaul for lateral movement and discovery tactics. Primarily these data sources rely on windows event logging and internal net flow data. Lateral Movement is a phase that is ubiquitous across ransomware infections.
- Examine Unit Test results to identify and fill low level of effort (LOE) gaps exposed through testing. Specifically Low LOE gaps can be identified by examining where a test is identified but not carried forward in the detection pipeline. Logged -> Detected -> Alerted -> Responded, e.g. detected but not alerted or responded.
- Examine Palo Alto logs and alerts for missed hunting and detection opportunities related to the unit tests executed during this project. Ensure significant events are forwarded to the SIEM.
- Begin concerted effort for creation of anomalous behavior-based detections.
- Consider blocking ICMP at perimeter.

1.5.2 Long-term Recommendations

Below is a list of longer-term initiatives for consideration.

- Formalize Detection Engineering process and begin to regularly work on custom detections to cover procedure level gaps.
- Continue to further invest in improving your capability to perform custom detection engineering.
- Begin regular effort to create anomalous behavior-based detections targeted at lateral movement, internal reconnaissance, command and control and data exfiltration techniques.
- Investigate options to start collecting and leveraging internal netflow data to support detection for scanning and lateral movement.
- Considering enhancing DNS logging and alerting capabilities.

NetSPI™

Want to see the full
Sample security audit report?

Every engagement with NetSPI will provide you with a PDF report of findings, as well as access to The NetSPI Platform, delivering streamlined vulnerability management, team communication, and real-time updates. In this sample report, gain insights into vulnerabilities and misconfigurations that we might find during a NetSPI Breach and Attack Simulation engagement and see how our team can help you secure your environment.

- Project overview: objectives, scope & timeframe, and findings summary
- Technical detail: critical, high, medium, and low severity findings
- Testing methodology
- Risk management approach

Show Me The Sample Security Audit Report!