SOLUTION BRIEF

Acalvio ShadowPlex for Threat Hunting

How deception technology and analytics enables active threat hunting

What is threat hunting?

Threat hunting is a proactive approach to cybersecurity, involving the identification of potential threats within an environment to mitigate them before they cause harm.

Advanced Persistent Threats (APTs) and modern ransomware are often stealthy, waiting for an opportune moment to launch their offensive. The proactive nature of threat hunting enables defense teams to uncover these latent threats, allowing for timely mitigation actions to protect the enterprise.

Threat hunting is also performed to confirm low-fidelity detections or alerts raised by security tools within the enterprise.

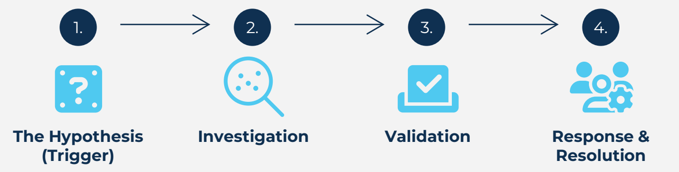
Threat-hunting actions can be iterative, conducted by defenders with expertise in identifying the presence of threats.

Hypothesis testing and confirmation

Threat hunting exercises start with the formation of a hypothesis. This hypothesis can be based on an existing alert, threat intelligence information, or findings from security posture management tools.

The hypothesis guides the threat-hunting investigation, providing direction and objectives. The investigation involves testing the hypothesis through various steps and either confirming or disproving it.

4 STEPS OF **CYBER THREAT HUNTING**



Traditional Techniques for Threat Hunting

Traditional threat-hunting techniques include:

Indicator of Compromise (IoC) Sweeps: IoC sweeps is a popular approach for threat hunting. The security team obtains access to an IoC that is indicative of a malware artifact or a compromised domain/IP address. The IoC data is obtained through threat intelligence sources, from vulnerability feeds, or through data sharing across organizations.

The threat hunting team takes an IoC and performs a sweep in the environment, looking for files, entries in logs that match the IoCs. A matching IoC provides indication of the presence of a threat in the target environment.

Log and event searches

Identifying patterns in logs and events that indicate malicious activity. These searches can be iterative and require domain expertise to uncover patterns indicative of malicious activity. An example would be a search in a Windows event log looking for a specific event ID that is indicative of an offensive activity or the presence of a type of malware.

Limitations of traditional threat hunting techniques

Threat hunting is inherently an iterative process and can be time and resource intensive. Threat hunting actions require skilled defenders that can analyze and interpret the outcome of each iteration as part of the exercise.

The skilled teams formulate an initial hypothesis and initiate the threat hunting action. The threat hunt is initiated, with approaches including IoC sweeps and log/event searches to identify the presence of the threat and confirm the hypothesis. As modern adversaries evolve their offensive techniques and gain sophistication and stealth, traditional approaches to threat hunting have shown limitations. Adversaries are leveraging custom tooling and modified tool variants to evade IoC-based detection. They also use in-memory exploits, living-off-the-land (LotL) techniques, obfuscated scripts to evade detection through log searches. Defense evasion is a popular and effective technique leveraged by adversaries to erase evidence in logs, making log and event-based searches challenging for threat-hunting teams.

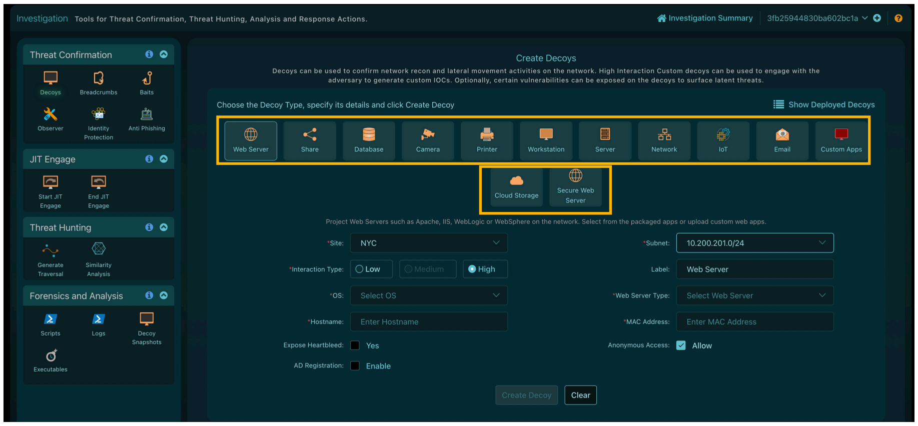
With threat hunting teams requiring skilled domain experts, it is essential to identify tools and platforms that can improve the effectiveness of these actions.

Acalvio ShadowPlex

Acalvio ShadowPlex: Active Threat Hunting

ShadowPlex combines deception with advanced analytics to bring an "active" dimension to threat hunting. This enables threat hunting teams to identify latent threats, accelerate the confirmation of threat hunting hypothesis, and gain visibility into the attacker TTPs.

ShadowPlex provides a comprehensive threat-hunting workbench that combines purpose-built deceptions with precision analytics to bring the active dimension to threat hunting.



Tools for Threat Confirmation, Threat Hunting, Analysis and Response Actions.

Create Decoys

Decoys can be used to confirm network recon and lateral movement activities on the network. High Interaction Custom decoys can be used to engage with the adversary to generate custom IOCs. Optionally, certain vulnerabilities can be exposed on the decoys to surface latent threats.

Choose the Decoy Type, specify its details and click Create Decoy

Project Web Servers such as Apache, IIS, WebLogic or WebSphere on the network. Select from the packaged apps or upload custom web apps.

*Site: NYC

*Interaction Type: ○ Low ○ Medium ● High

*OS: Select OS

*Hostname: Enter Hostname

Expose Heartbleed: □ Yes

AD Registration: □ Enable

*Subnet: 10.200.201.0/24

Label: Web Server

*Web Server Type: Select Web Server

*MAC Address: Enter MAC Address

Anonymous Access: ☑ Allow

Figure 1: Threat hunting workbench to deploy targeted deceptions for hypothesis confirmation

1 **Threat hunting team formulates hypothesis**

2 **Initiates new threat hunting activity**

3 **Deploy decoy from threat hunting workbench**

4 **ShadowPlex detects threat and confirms hypothesis**

Deceptions to Surface Latent Threats and Perform Hypothesis Confirmation

ShadowPlex provides the ability to deploy purpose-built deceptions through the threat hunting workbench. Deceptions can be deployed in the respective part of the environment that is under threat.

By deploying deceptions in the target environment, threat-hunting teams can provoke latent threats into action, enabling the identification and confirmation of these threats.

Modern threats lie dormant, waiting for a suitable opportunity to emerge to perform an exploit. Finding these threats through traditional mechanisms can be challenging, with the dormant threat not resulting in log traces or event generation. Deception provides an effective approach to confirm the presence of such latent threats. Through the introduction of a controlled set of deceptions in the environment, threat hunting teams gain the ability to provide a controlled opportunity to the latent threat. Any attempt by the threat actor to perform an exploit results in an immediate detection and confirmation of the threat hunting hypothesis.

Sample Scenario: Deception-Based Threat Hunting in Action

An adversary gains access to an environment and attempts lateral movement using vulnerability exploits against the legacy SMBv1 protocol. Although SMBv1 is typically disabled for security reasons, the threat remains latent, waiting for a suitable opportunity, such as an unpatched legacy endpoint.

Using the ShadowPlex workbench, a decoy can be deployed that surfaces the legacy SMBv1 protocol. This allows the threat-hunting team to detect the latent threat when it attempts the exploit, leading to immediate detection and confirmation of malicious activity.

Visibility to provide a starting point for threat hunting

The proactive nature of threat hunting introduces a challenge for the defenders. Identifying the starting point or the initial environment that is the origination of a threat hunt can be challenging, especially for a large and complex enterprise environment. Traditional approaches to identity the starting point of a threat hunt have been based on analysis of a low fidelity alert raised by a security control. With the large false positive rates associated with low fidelity alerts, threat hunts can often lead limited benefits when the starting point may not be indicative of a threat.

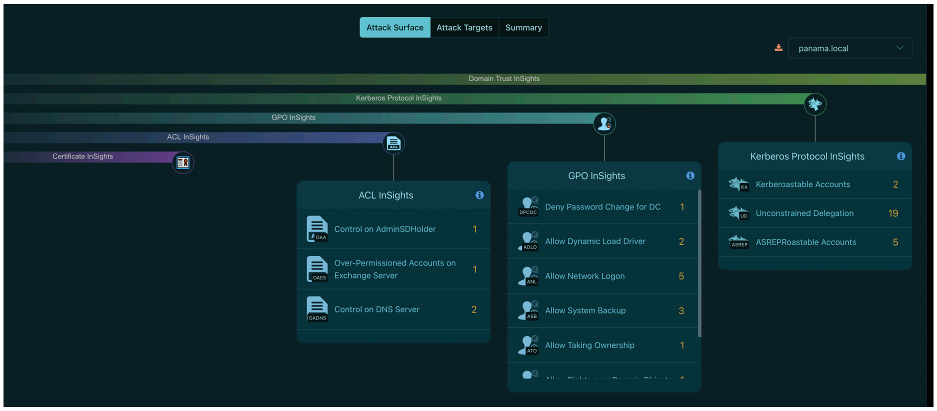
ShadowPlex leverages purpose-built analytics to provide visibility to the defense teams that serves as a reliable starting point for threat hunting actions.

Active Directory (AD) Insights

ShadowPlex AD Insights provides pre-attack stage visibility capabilities to enable defense teams to identify the attack surface that can be exploited by adversaries. This visibility is an “attacker view” of the environment, enabling defenders to gain a unique perspective on the available attack surface for adversaries. The attack surface arises from misconfigurations, lack of sufficient security hygiene, over-permissioning, in addition to the vulnerabilities and unpatched equipment.

ShadowPlex performs a 150+ point analysis of AD and provides visibility to the attack surface that can be exploited by an adversary. The insights include service accounts that are vulnerable to Kerberoasting, shadow admin accounts, computer objects with unconstrained delegation. These are examples of the misconfigured or over-permissioned accounts that provide an exploitable attack surface.

The findings from AD Insights provide a reliable starting point for threat hunting actions. ShadowPlex AD Insights are prioritized based on importance and magnitude of impact. Threat hunting teams gain the benefit of a reliable starting point to initiate a threat hunting and formulate and confirm a hypothesis.



ACL InSights	
Control on AdminSDHolder	1
Over-Permissioned Accounts on Exchange Server	1
Control on DNS Server	2

GPO InSights	
Deny Password Change for DC	1
Allow Dynamic Load Driver	2
Allow Network Logon	5
Allow System Backup	3
Allow Taking Ownership	1

Kerberos Protocol InSights	
Kerberoastable Accounts	2
Unconstrained Delegation	19
ASREPRoastable Accounts	5

Figure 2: Acalvio ShadowPlex AD Insights

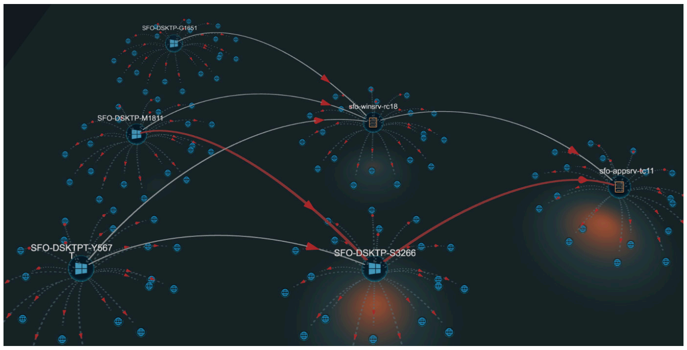


Figure 3: Acalvio ShadowPlex Adversary Traversal Analytics

Adversary Traversal Analytics

ShadowPlex provides adversary traversal analytics, this is purpose-built analytics to find the set of possible pathways that an adversary took as part of the propagation in the environment. Adversary traversal performs a look back analysis, based on a detection event from a third-party alert or a ShadowPlex deception alert. The nodes along the adversary traversal pathways have a high likelihood of being compromised and provide a reliable starting point for threat hunting actions.

The visibility provided by the AD Insights and adversary traversal analytics serves as a reliable indicator of threat hunting.

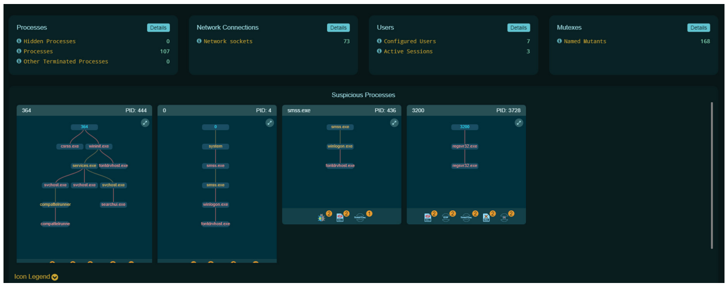
Precision Analytics to Identify Stealthy Threats

Modern threats often employ stealthy techniques, such as in-memory exploits and LotL methods, to evade traditional security measures. These techniques do not leave traces in logs or events, posing challenges for traditional threat hunting.

ShadowPlex offers precision analytics capabilities, including memory forensic analysis and PowerShell script analysis, to detect these stealthy threats. This provides threat-hunting teams with additional visibility into the tactics, techniques, and procedures (TTPs) used by threat actors.

Memory forensic analysis

Modern threats are leveraging in memory exploits (such as *Process Hollowing*) to evade detection approaches that are focused on disk and log-based detection. Gaining visibility to attacker TTPs for memory resident malware is challenging, as it requires deep domain expertise in memory forensics. Performing memory forensics manually is an extremely time consuming and complex task. Threat hunting teams that are looking to gain visibility into attacker TTPs for memory resident threats can benefit from ShadowPlex memory forensic analysis that is a part of the ShadowPlex threat hunting workbench. ShadowPlex memory forensic analysis performs automated analysis of a disk and memory snapshot to identify memory resident threats, including evasive offensive techniques that are challenging to detect.



Processes
Hidden Processes 0
Processes 107
Other Terminated Processes 0

Network Connections
Network sockets 73

Users
Configured Users 7
Active Sessions 3

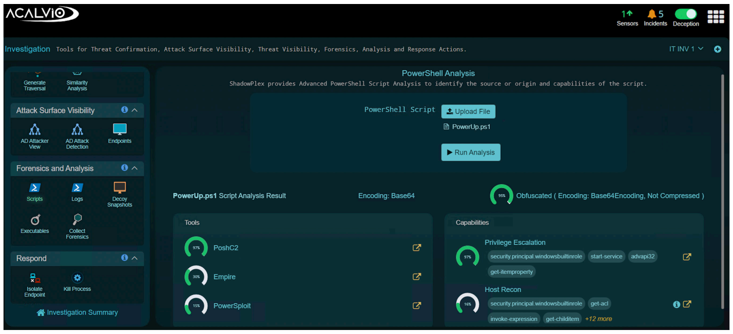
Mutexes
Named Mutants 168

Figure 4: Acalvio ShadowPlex Memory Forensic Analysis

Purpose-built analytics such as memory forensics are an essential element of a strategy for threat hunting. Threat hunting teams can expand their coverage beyond the traditional log and event searches to find latent, memory-resident threats with precision.

PowerShell script and log analysis

Adversaries are leveraging PowerShell for living off the land (LotL) exploits. While organizations use PowerShell for IT automation, threat actors leverage the wide availability of PowerShell to execute custom offensive scripts. Adversaries leverage obfuscated PowerShell scripts that are evasive and challenging to detect. The obfuscated nature of the scripts evades attempts to detect the offensive scripts based on log analytics.



Investigation Tools for Threat Confirmation, Attack Surface Visibility, Threat Visibility, Forensics, Analysis and Response Actions.

PowerShell Analysis
ShadowPlex provides Advanced PowerShell Script Analysis to identify the source or origin and capabilities of the script.

PowerShell Script: PowerUp.ps1

PowerUp.ps1 Script Analysis Result — Encoding: Base64 — 95% Obfuscated (Encoding: Base64Encoding, Not Compressed)

Tools
97% PoshC2
30% Empire
15% PowerSploit

Capabilities
97% Privilege Escalation: security.principal.windowsbuiltinrole, start-service, advapi32, get-itemproperty
16% Host Recon: security.principal.windowsbuiltinrole, get-acl, invoke-expression, get-childitem, +12 more

Figure 5: Acalvio ShadowPlex PowerShell script and log analysis

Threat hunting teams that are looking to gain visibility into the stealthy, PowerShell based attacker actions can leverage the PowerShell script and log analytics capability in the ShadowPlex threat hunting workbench. ShadowPlex PowerShell script analysis uses advanced AI algorithms to identify the attacker TTPs, including for stealthy and obfuscated scripts used by the attacker.

Summary: ShadowPlex brings an active dimension to threat hunting

ShadowPlex threat hunting workbench has a purpose-built combination of deception and precision analytics to bring an active approach to threat hunting. Threat hunting teams can confirm latent threats by placing targeted deceptions and gain visibility into stealthy attacker TTPs. By expanding the set of capabilities for threat hunting teams, organizations gain the ability to proactively defend their environments against advanced threats.

Acalvio, the leader in cyber deception technology, helps enterprises actively defend against advanced security threats. Acalvio Active Defense Platform, built on 25 issued patents in autonomous deception and advanced AI, provides robust solutions for Identity Threat Detection and Response (ITDR), Advanced Threat Detection, OT Security, Zero Trust, Active Directory Protection and Ransomware Protection. The Silicon Valley-based company's solutions serve Fortune 500 enterprises, government agencies and are available to deploy on-premises, in the cloud or via marquee managed service providers. For more information, please visit **www.acalvio.com**