ACALVIO

DECEPTION USE CASES AND KEY CAPABILITIES

An Acalvio Guide

EXECUTIVE SUMMARY

Deception Technology is quickly becoming an important part of cybersecurity strategy for many enterprises. Though Deception solutions for cyber defense have existed for a while, it is only of late that breakthrough inventions in the field are making the adoption go mainstream in the industry.

When the right Deception Solution is chosen, the value that such a platform can bring goes beyond just threat detection and reporting on the network.

In this paper, we take a look at some of the most popular Deception use cases, key capabilities necessary for each one them, and the value that Acalvio's Autonomous Deception Platform brings.

DECEPTION USE CASES AND KEY CAPABILITIES

A well-designed Deception solution can serve as an efficient platform in provisioning a collection of use cases in any Enterprise, spanning network visibility and security training, moving up to asset protection, threat detection, threat hunting, investigation and response, with precision and speed.

Among the many use cases for a Deception platform, the following section focuses on the most prominent aspects, and the key capabilities of each of them.

Rapid and Precise Threat Detection, Investigation and Response

After an initial network compromise, attackers seldom land on the intended part of the network to complete their mission. They need to move laterally outside of the initial beachhead to other systems on the network.

According to CrowdStrike, advanced attackers need less than 2 hours on average to accomplish their mission. The Breakout rule dictates how much time the organization has to detect and eject the intruder. This is the new cyber defender's metric.

Need for Rapid And Precise Threat Detection

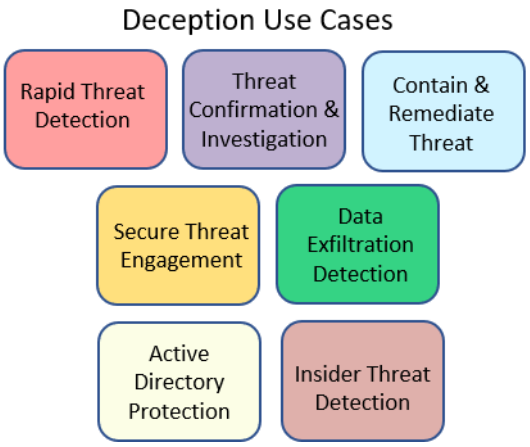
In order to prevent an intrusion from becoming a breach, it is imperative for Organizations to **rapidly and precisely detect a new threat, human or Malware.**

Malware and APTs continue to be the most prevalent cyber threats for organizations, with Malware providing an effective entry point for establishing a foothold to carry out stealthy, sophisticated attacks**.**

CrowdStrike Breakout Rule

Organizations should strive to surpass the **1/10/60 rule**:

1 minute to **Detect** the threat
10 minutes to **Investigate**
60 minutes to **Remediate**



Need for Rapid Threat Confirmation and Investigation

Confirming a threat and finding the intruders in a matter of minutes is critical to understand the threat, for attribution as well as for threat containment and remediation.

Traditional investigation methods depend partly on automated and largely on manual investigation steps. A significant part of the defender's toolkit is log analysis on a SIEM system, such as Splunk. Endpoint scanning, captured file/URL reputation checks using VirusTotal, detonation, and analysis of forensic PE files in a sandbox are some of the other techniques that are used.

Identifying all compromised endpoints involved in an attack is critical**. Qualifying and listing the endpoints to investigate is the very first of many challenges.** Hunting for APTs requires thorough knowledge of the threat landscape and prevalent tactics, appropriate skill and heavy automation.

A considerable manual time is also spent on analyzing other types of forensic evidence such as scripts for capability or attribution. Many modern attacks use **LotL (Living off the Land) techniques**. These attacks leverage **downloadable scripts** such as **PowerShell Scripts** or VBS and dual-use tools already available on the endpoint or local network.

Similarly, many modern threats including Ransomware have become **memory resident threats**. There are very few or no files written to the filesystem and therefore, often bypass Antivirus and EDR defenses. Finding and cleaning such memory-resident malware is challenging and requires the appropriate knowledge, skill, time and speed on part of the Threat Defense teams. The problem only worsens if multiple memory dumps from several endpoints have to be analyzed for malicious memory-resident software. Such a task is nearly impossible to execute manually, let alone in a few minutes.

Need to Contain Threat and Remediate in The Golden Hour

The need to contain and remediate the threat in less than an hour is strenuous to achieve in real-world attacks. This is despite leveraging SOAR products such as Phantom, to rapidly orchestrate the response.

Acalvio ShadowPlex has been designed with the goal of rapid and precise threat detection, rapid and automated investigation and automating the response phase.

By using a combination of Deception and AI-based analysis, Acalvio ShadowPlex detects various tactics and techniques as defined in the MITRE ATT&CK framework. Some of the tactics include Impact, Discovery, Credential Access, Lateral Movement, Privilege Escalation, Defense Evasion, Data Exfiltration, Persistence.

Acalvio ShadowPlex uses a **unique Ransomware kill-chain** to detect known, unknown, and fileless Ransomware with precision and speed. This enables automated response to protect the endpoints, including the senior team and CXO laptops, even when they are not connected to the enterprise network.

Acalvio ShadowPlex uses a unique combination of Deception and AI-based techniques to detect and investigate the growing script-based attacks such as **PowerShell /LotL attacks**.

ShadowPlex brings novel **attack surface reduction techniques** to proactively reduce the attack surface.

Acalvio has strategically partnered with CrowdStrike to create a unique Threat Confirmation, Investigation and Threat Hunting application to help organizations meet and surpass the 1/10/60 breakout rule. This tightly integrated offering includes patented Attacker Traversal Analysis, Link Analysis for situational awareness, automated PowerShell Analysis for evidence forensic scripts and logs. Acalvio ShadowPlex also offers **automated** memory analysis, a **unique and powerful capability designed for the IR and Threat Hunting teams.**

Effective threat hunting should involve dynamically changing the landscape to observe and analyze, as opposed to traditional methods of data collection and analysis.

Acalvio introduces novel **response** options for Threat Defenders. ShadowPlex can be leveraged to **divert** the attacks away from Key Assets such as Splunk web interface and Citrix ADC.

A new powerful approach is to try to **slow-down** or **confuse** the attacker and/or divert the attacker away from the enterprise assets, so that the defense team gains more time to respond to the attack. Using ShadowPlex's rich palette of deceptions, an effective deception placement strategy can be devised to completely divert the attacker away from the assets, and on to the decoys.

Acalvio's patented **Just-in-Time deceptions** are leveraged to slow-down and confuse the attacker when the organization is under attack. ShadowPlex deceptions can be used to slow-down an attack by increasing the deception density on the fly, to surround the assets. Key assets can be surrounded by hundreds of deceptions within minutes to slow-down the attack progression and/or create confusion for the attacker.

Acalvio's pre-built integrations with multiple ecosystem solutions such as SIEM, SOAR, Network Management, Sandbox, EDR, Email Servers speeds up response actions. Acalvio ShadowPlex can also automate the responses by leveraging orchestrator product capabilities, and this includes varied responses such as isolate or quarantine infected hosts, alert notifications, suspend or kill a process, and Malware detonation, among other actions.

Acalvio ShadowPlex offers:

- ✓ Threat Detection using Deceptions & AI
- ✓ Threat Confirmation using Deceptions
- ✓ Hypothesis Testing & Threat Hunting
- ✓ Slow-down, Divert or confuse the attacker

Secure Threat Engagement

The technique of Securely Engaging with an attacker is used when forensic data such as IOCs, PCAP, Memory & Disk Snapshots, SQL Queries, Screenshots, Snort Signals, Process details and other artifacts are to be collected. Given the malicious nature of the attack, robust containment is necessary for the engagement. Secure engagement must prevent blowback into the enterprise network – this means the access policies have to be well-defined and controlled.

Active Directory Protection

Active Directory is undeniably one of the most important assets in an enterprise, given that it is at the heart of most networks and is a repository of rich network data. Tools like ***dsquery***, ***net command***, and the more prevalent ****BloodHound*** are used by the attackers to assess the lay-of-the-land and find the shortest path to the key assets in the enterprise.Bloodhound enumerates the domain trust relationship and extracts user, privileges, group and membership information and reduces the network complexity to create the shortest path to key assets.

Acalvio weaves in blended deceptions into the enterprise Active Directory, covering all entity types and relationships. Using Deceptions combined with AI provides a strong layer of protection in detecting recon, lateral movement, credential access and other malicious activities against the enterprise AD.

Acalvio recommends registering deceptions (such as decoy users, computers, groups and services) in Active Directory. In addition to making the deceptions look authentic, this also enables tools like dsquery and bloodhound to report deceptions along with real assets. Acalvio's AI-based Recommendation Engine automatically recommends the appropriate users, groups and services based on the AD discovery data.

Acalvio has the capability to create a full walled garden comprising subdomain(s), facilities, backup servers, trust relationships and other entities. This can be particularly useful to securely engage with an attacker to generate critical TTPs. Decoys, Fake Users, Groups and Services can be registered in this domain. This approach would be effective in diverting the attacker away from real assets to a network of deceptions.

Acalvio also enables proactive attack surface reduction by auto-discovering saved credentials on endpoints and clearing them. Additionally, powerful cached credentials can be modified to become part of the deception strategy.

*The 2019 CrowdStrike Services Report indicates that leveraging BloodHound to expediate Network Reconnaissance as a recurring theme in their 2019 investigations.

Data Exfiltration Detection

Data Exfiltration attempts from Databases, Network Shares, SharePoint Servers, Mailboxes and Cloud Storages are hard to detect with traditional tools like DLP and UEBA.

Acalvio deception palette offers a rich variety of deceptions such as storage, mailbox, network share and cloud storage bucket decoys, breadcrumbs and baits to detect data exfiltration attempts. This deception-based detection is effective for on-premise repositories, Cloud storage buckets, Cloud services like box.com as well as SaaS services like Office 365.

Acalvio's Deceptions, combined with the power of AI, can detect access, copy, and data operations on any data store. Data exfiltration attempts from traveling employee laptops is also detected, even when the employee is not connected to the enterprise network.

Data exfiltration attempts from Databases, Network Shares, SharePoint Servers, Mailboxes, Cloud Storage Servers and other hosted solutions are hard to detect using traditional tools like DLP and UEBA.

Insider Threat Detection

Insider threat is a security risk that many enterprises face today. These can stem from compromised or negligent users, or malicious users within the organization. Indicators can range from unusual network activities such as authenticated but unauthorized users accessing assets or data, unusual network traffic volumes or activity times, critical data exfiltration, among many others. Traditional tools like SIEMs, UEBA, EDRs and DLP solutions cannot detect these malicious activities.

Acalvio's powerful InSights™ capability can detect these activities and help formulate a deception strategy based on the observed activities. Acalvio's deceptions too can be well-crafted and placed strategically to detect, investigate and respond to insider threats.

2520 Mission College Boulevard, Suite 110
Santa Clara, CA 95054
www.acalvio.com