Acalvio ShadowPlex for Insider Threats

How security teams gain visibility to stealthy insider threats, from compromised users to malicious insiders

What are insider threats

Insider threats represent risks from persons with authorized access to an organization's resources.

These threats can manifest in various forms:

Compromised users: Individuals whose credentials have been stolen or impersonated by external attackers.

Negligent or careless: Those who inadvertently click on phishing links or accidentally leak sensitive company information.

Malicious insiders: Disgruntled employees, rogue administrators, or contractors who intentionally seek to harm the organization.

Why are insider threats rising

The increased use of cloud services, SaaS applications, and remote work has significantly expanded access to sensitive corporate data. This increased accessibility makes traditional segmentation and prevention-based controls less effective in mitigating insider threats. Moreover, threat groups, such as Initial Access Brokers (IABs), actively solicit insiders to gain unauthorized access, further heightening the risk.

Targets of Insider Threats

Insiders typically target sensitive data and intellectual property, including design specifications, source code, and financial statements. Their goal is often to cause harm to the organization by leaking this critical information.

How are insider and external threats different?

Although both insider and external threats may utilize similar attack techniques, insider threats are distinct in several ways:

- Insiders have direct access to organizational resources, eliminating the need for extensive reconnaissance.
- They often do not require malware or Command and Control (C&C) infrastructure, commonly used by external attackers.
- Insider threats seldom rely on vulnerability exploits, leveraging existing access instead.
- Traditional threat intelligence is less effective against insiders, as it focuses primarily on external actors.
- Response actions for insiders differ significantly, with endpoint isolation being less effective.

The MITRE insider threat framework

MITRE has dedicated research to insider threats and provides a comprehensive framework to categorize and classify these threats based on tactics, techniques, and procedures (TTPs). This framework includes a heatmap that highlights the most frequently used TTPs by insiders, making it a valuable tool for developing an effective cyber defense strategy.

What is cyber deception?

Cyber deception involves predicting the goals of an insider, setting traps, and monitoring for interactions with these deceptive elements. Since deception is not used in regular IT or business workflows, any interaction with deceptive elements is a clear indicator of malicious intent.

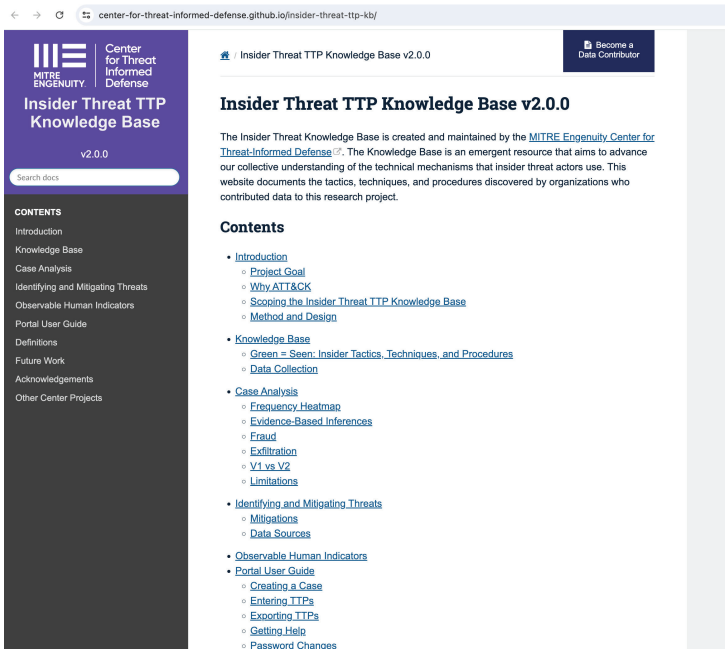
Acalvio ShadowPlex

Challenges with detecting insider threats

Traditional detection methods, such as Data Loss Prevention (DLP) and User Entity Behavior Analytics (UEBA), have limitations:

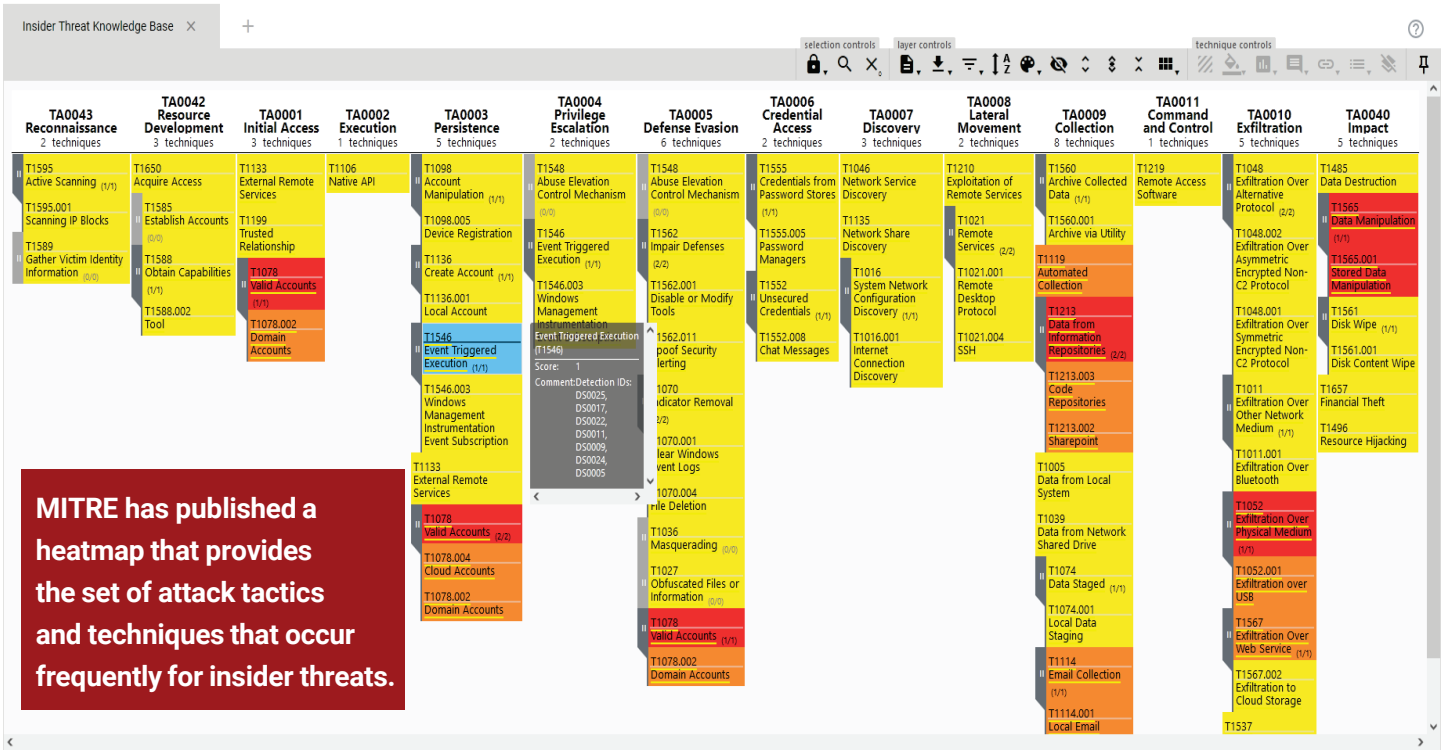
- **DLP Solutions:** Primarily serve as a compliance tool, flagging policy violations when sensitive data is transferred outside the organization. However, they offer limited visibility into pre-egress activities.
- **UEBA Solutions:** Often generate false positives, particularly in environments with remote work and dynamic data access patterns.

Insiders can exploit their trusted status to remain undetected, performing slow, calculated actions that evade traditional anomaly detection systems. Additionally, the use of encrypted communication further complicates detection.



MITRE heatmap for insider threats

Insider threats are characterized by the advanced MITRE tactics, such as Collection, Exfiltration, and Impact. Data exfiltration is one of the primary objectives of insider threats.



The Effectiveness of Cyber Deception in Detecting Insider Threats

Comprehensive Array of Deceptions

Acalvio ShadowPlex employs a wide range of deceptions, including decoys, baits, and honeytokens, to create a realistic environment that lures insider threats. These deceptive elements are strategically placed within identity stores and data repositories, making any interaction with them a clear indicator of malicious activity.

Tailored Deception Strategies

ShadowPlex offers tailored deception strategies to detect compromised, negligent, and malicious insiders. Leveraging AI, the platform automates the creation and deployment of these deceptions across the enterprise, significantly reducing the time and effort required from security administrators.

High-Fidelity Alerts

The platform generates high-fidelity alerts that enable security teams to take precise and swift response actions, such as blocking user accounts, ensuring minimal false positives, and effective threat mitigation.

Defending Against Insider Threats with ShadowPlex

ShadowPlex delivers a customized set of deceptions—such as decoys, baits, and honeytokens—specifically designed to detect insider threats with precision. This includes the detection of compromised insiders, negligent users, and malicious insiders. These deceptions are strategically embedded within identity stores and data repositories, allowing defense teams to identify insiders attempting to exfiltrate sensitive data or escalate privileges.

By meticulously placing these deceptions in critical areas, defense teams can quickly detect and respond to insider threats. ShadowPlex's AI algorithms streamline both the creation and placement of these deceptions, saving considerable time and effort for administrators. The high-fidelity alerts generated by ShadowPlex facilitate immediate response actions, such as blocking user accounts, and ensuring that threats are neutralized before they can cause significant harm.

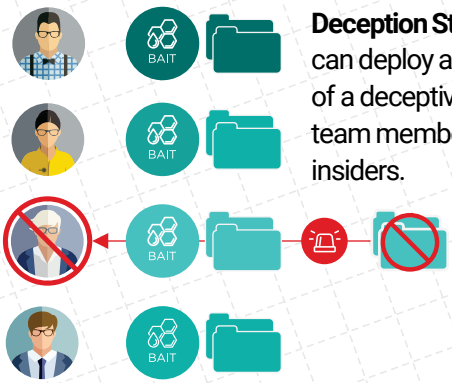
Scenario: Detecting Compromised Insiders

Compromised insiders are external attackers who have obtained insider credentials. ShadowPlex can detect attempts to elevate privileges by deploying honeytokens within identity stores and endpoints, offering precise detection.

Deception Strategy: Defense teams can deploy identity honeytokens in identity stores and on endpoints.

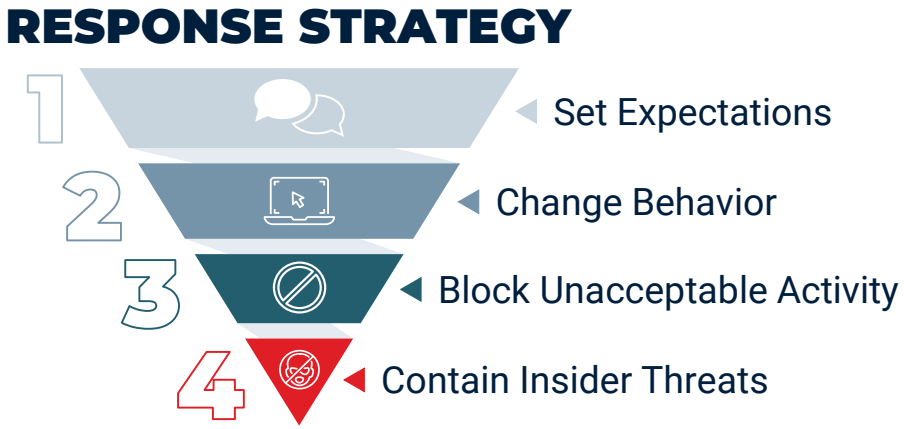
Scenario: Detecting Malicious Insiders

Malicious insiders attempt to exfiltrate data stealthily. ShadowPlex deploys advanced baits and honeytokens in identity stores and in data repositories, making it difficult for insiders to carry out exfiltration without triggering an alert.



Deception Strategy: Defense teams can deploy almost identical copies of a deceptive document to all the team members to detect malicious insiders.

Detection fidelity is critical to enable, block or contain response actions



Tailored Response Actions for Insider Threats

Responding to insider threats requires a different approach than handling external threats. Traditional response actions, such as isolating compromised endpoints or blocking an IP address at the firewall, are often ineffective against insiders. Instead, insider threats demand customized response actions, including blocking the user account of the employee or contractor involved, or adding the user to a watch list. However, blocking a user has direct and potentially significant consequences for the organization, including legal ramifications.

Given the direct impact of these actions, the fidelity of detection is crucial. Inaccurate detection can lead to prolonged investigations, during which insiders may continue their malicious activities unchecked. This risk is particularly high if the insider is a departing employee, as the organization may lose the opportunity to mitigate the threat or recover lost data.

High-fidelity detections are vital for accelerating threat investigations and providing actionable intelligence. This ensures that appropriate response actions, such as blocking the user account, can be taken promptly. Deception technology plays a critical role here, as it is capable of generating high-fidelity alerts that are essential for the accurate detection of insider threats.

Summary: ShadowPlex – An Essential Solution for Defending Against Insider Threats

Insider threats are notoriously difficult to detect, as insiders exploit their trusted access to exfiltrate sensitive data while evading traditional security measures. An effective defense requires a layered approach that combines prevention with advanced detection strategies. ShadowPlex, with its sophisticated and comprehensive palette of deceptions, excels in detecting insider threats across the spectrum—whether they are compromised, negligent, or malicious insiders. By providing early and accurate detection, ShadowPlex enhances visibility for defense teams and significantly strengthens an organization's cybersecurity posture.

ACALVIO

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**

© 2024 Acalvio Technologies, Inc. All rights reserved.