Acalvio ShadowPlex for Early Threat Detection

Detect threats early in attack lifecycle to prevent attack propagation

Modern adversaries are gaining in speed

Today's cyber adversaries employ increasingly sophisticated techniques and automated tools, dramatically speeding up their operations within targeted networks. These attackers quickly escalate their activities, moving from initial access at an endpoint to gaining situational awareness, securing credentials, and pivoting towards critical systems. This acceleration in hostile activities has led to a significant reduction in "adversary breakout time" — the period from initial compromise to substantial lateral movement within the network — which has decreased from 98 minutes in 2022 to just 62 minutes in 2024.

Threat vectors targeting financial services

2024 demonstrated a significant increase in the efficiency and speed of modern adversaries. This reduction is driven primarily by two key factors:

- Sophisticated Automation: Adversaries are increasingly employing advanced automation techniques, which streamline their attack processes and reduce the time required to achieve their objectives.
- Utilization of Built-in OS Tools: By leveraging built-in operating system tools and utilities for offensive actions, adversaries eliminate the need to introduce external malware into the environment. This approach not only speeds up their operations but also reduces their digital footprint and the likelihood of detection.

These factors collectively contribute to the swift pace at which adversaries can move within compromised networks, significantly shortening the window for defensive response.

Typical Attack Sequence of APT groups

1. **Situational Awareness:** Perform endpoint reconnaissance to understand the environment.
2. **Defense Evasion:** Disable security measures and clear logs to avoid detection.
3. **Privilege Escalation:** Gain higher-level permissions to access sensitive system areas and functions.
4. **Credential Access:** Extract valuable credentials from system caches.
5. **Establish Persistence:** Secure a foothold for ongoing access.
6. **Lateral Movement:** Move across the network to reach high-value targets.

Adversarial actions performed on the endpoint

Adversaries begin their infiltration by gaining initial access to an endpoint. Their first objective is to establish situational awareness, followed by obtaining credentials to facilitate lateral movement within the network.

Living Off the Land (LotL) Exploits:
Modern adversaries often utilize "living off the land" (LotL) techniques, exploiting built-in operating system tools and utilities for their malicious objectives. This approach allows them to blend in with normal system activity, making detection more challenging.

Implications for cyber defense

The significant decrease in adversary breakout time necessitates a swift response from cyber defense teams. To counter these rapid threats, the focus must be on reducing the Mean Time to Detect (MTTD)—the period from an adversary's initial access to their detection.

Traditional security solutions are unable to keep pace

Traditional security solutions are primarily designed to observe actions and apply rules and analytics to identify malicious activity based on those observations.

However, as adversaries use built-in tools and utilities along with valid credentials to carry out lateral movement, traditional security solutions struggle to differentiate between malicious activity from legitimate system administration actions.

Consider an attack sequence that performs reconnaissance to gain situational awareness:

The event logs and network traffic from the attacker's actions *appear identical to the activity from the legitimate system administrator actions.* This makes detection challenging, with traditional security solutions requiring additional observations to classify activity as malicious.

Cyber deception: An effective strategy for accelerated detection

Cyber deception serves as a potent method for enhancing detection by setting strategic traps for attackers. These traps are placed in locations likely to be encountered by an adversary, and any interaction with these traps is a clear indicator of malicious activity, as they are not utilized in normal operations.

Early threat detection using deception technology

Defense teams aiming to detect threats early and reduce the Mean Time to Detect (MTTD) can effectively utilize deception technology. By deploying deceptions broadly—across endpoints, identity stores, and networks—teams can create targeted traps for attackers. Should an attacker gain initial access to an endpoint and start executing offensive steps, they are likely to encounter one or more of these strategically placed traps. Interaction with these traps provides immediate detection, giving the defense team an early warning and enabling quick response actions to isolate the threat and prevent further adversary movement.

By incorporating deception into their defensive strategy, security teams can detect stealth actions more quickly and effectively than traditional methods allow.

Considerations for an effective deception strategy for early threat detection

1. **Comprehensive Deployment Across the Organization:** To maximize the effectiveness of deception technology, it's critical to deploy deceptions pervasively throughout the organization. This ensures that whether an adversary gains initial access through compromised insiders or other methods, they encounter deceptions at every potential point of entry.
2. **Strategic Placement of Deceptions:** By strategically placing deceptions in areas where attackers are most likely to search for sensitive information, such as credential caches on endpoints, security teams increase the chances of early detection during the preliminary phases of an attack.
3. **Diverse Types of Deceptions to Cover Attacker Actions:** Attackers can perform reconnaissance on the endpoint, in enterprise catalogs (such as Active Directory and Domain Name Server), or the network. Through a strategic combination of decoys in the network and honeytokens in identity stores and on endpoints, the deceptions can be surfaced during the reconnaissance phase itself, providing an early warning of adversary actions.
4. **Attractiveness and Authenticity of Deceptions:** Making the deceptions attractive and plausible is another key aspect. Adversaries find an attractive set of deceptive targets and attempt to exploit these, resulting in immediate detection.

Implementing these detailed strategic considerations significantly elevates the organization's defensive capabilities by facilitating early detection of threats.

Acalvio ShadowPlex: Advanced deception technology for early threat detection

ShadowPlex provides advanced deception technology, deployable at scale across organizations, to facilitate the early detection of cyber threats. This comprehensive approach ensures broad coverage and swift detection capabilities.

Comprehensive Palette of Deceptions: ShadowPlex provides a rich set of deceptions, including decoys positioned within the network and honeytokens placed within identity stores and on endpoints. These decoys simulate real network assets, while honeytokens mimic user and service account credentials stored across various caches such as operating system and application caches.

AI for Automated Recommendations: Utilizing advanced AI algorithms, ShadowPlex automates the deployment of realistic and attractive deceptions. This automation simplifies the administration process, reducing the complexity associated with manual configuration.

Broad Detection Capabilities Covering a Wide-variety of Attack Tactics: ShadowPlex is adept at identifying a wide range of attacker tactics, providing defense teams with the crucial ability to detect attacks early in their lifecycle. This capability spans various attack stages, including reconnaissance, credential access, defense evasion, privilege escalation, and persistence, ensuring detection prior to adversary propagation.

Actionable, High-fidelity Alerts: Equipped with a sophisticated threat analytics engine, ShadowPlex efficiently processes interactions with deceptions to generate high-fidelity alerts. These alerts are designed to be actionable, allowing Security Operations Center (SOC) teams to quickly respond without the need for extensive manual investigation or deduplication of alerts.

ShadowPlex early threat detection in IT environments

ShadowPlex Detection Strategy: ShadowPlex deploys honeytokens in credential caches on endpoints, in identity stores, and decoys in the network. These are designed to detect attacks early in the attack lifecycle.

Example attack scenario in an IT environment

Adversaries have multiple points of entry to an IT environment, ranging from phishing to internet facing exploits. Consider a scenario where an adversary gains access to an endpoint via a phishing exploit. The attacker then attempts to move laterally within the network. A common method involves the use of built-in tools to extract credentials from the caches on the endpoint.

The adversary successfully obtains credentials but unknowingly accesses a set of deceptive credentials (honeytokens) introduced by the ShadowPlex deception technology. These honeytokens are strategically placed in credential caches.

Immediate Detection and Response: The use of these deceptive credentials triggers an immediate alert within the security operations center. This rapid detection allows for swift containment and mitigation actions to isolate the attack and prevent further adversary movement.

ShadowPlex early threat detection in OT environments

ShadowPlex Detection Strategy: ShadowPlex excels in detecting early threats within OT environments by deploying decoys and honeytokens across both IT and OT assets. This strategy enhances the defense team's ability to identify threats specifically targeting operational technologies.

Example attack scenario in an OT environment

Adversaries transition from IT networks to OT environments by exploiting shared infrastructure vulnerabilities, such as those found in jump servers. Their goal is typically to access critical assets within the OT landscape, such as Programmable Logic Controllers (PLCs) and Controllers.

ShadowPlex's Strategic Deployment: To counteract these threats, ShadowPlex decoys are strategically positioned across the OT environment, encompassing both networks with IT and OT equipment. Additionally, ShadowPlex honeytokens are embedded within endpoints and identity stores throughout the OT network. These decoys are designed to mimic legacy assets that have known vulnerabilities and support critical OT protocols like Modbus, making them highly appealing to attackers.

Decoy Interaction and Immediate Alerts: When an adversary engages with these decoys, believing them to be vulnerable legacy systems, it triggers an immediate alert within the security operations center. This quick detection allows for swift response actions, enabling teams to isolate the attack and prevent further adversarial movement.

ShadowPlex early threat detection in cloud environments

Deception deployment in cloud workloads: ShadowPlex enhances security in cloud environments by embedding deceptions, including honeytokens, within Cloud IAM stores and credential repositories. This strategic deployment allows for the detection of threats at the earliest stages of their lifecycle.

Example attack scenario in a cloud environment

- **Adversarial Entry and Tactics:** Adversaries exploit public-facing cloud properties or pivot from IT environments to compromise cloud workloads. Their objectives often include accessing critical cloud resources like databases or storage buckets. During their infiltration, adversaries engage in reconnaissance to identify and exploit cloud identities for lateral movement.
- **Strategic Deployment of Honeytokens:** ShadowPlex positions honeytokens that appear legitimate and attractive to adversaries in key cloud locations, such as Cloud IAM stores. These honeytokens are designed to be particularly enticing, mimicking the access patterns and privileges of genuine IAM users and machine identities.
- **Immediate Detection and Alerting:** When an adversary attempts to utilize these honeytoken accounts, it triggers an alert to the security operations center. This quick identification of unauthorized access attempts allows security teams to act swiftly, isolating the threat and preventing further exploitation.

Automated Response Actions with ShadowPlex: ShadowPlex provides advanced capabilities to automatically execute response actions through integrations with existing security and network management platforms to isolate threats and prevent further adversarial actions. This proactive response is critical in mitigating risks swiftly and effectively. Security operations teams can configure automated response policies tailored to their specific security needs. Combined with the high-fidelity alerts generated by ShadowPlex, these automated policies ensure that threats are not only quickly detected but also immediately contained, reducing the potential for damage and disruption.

Summary: ShadowPlex enables defense teams to gain early detection of threats across IT, OT, and Cloud

As modern adversaries rapidly evolve, gaining speed and stealth—reducing adversary breakout time from **84 minutes in 2023 to just 62 minutes in 2024**—the need for innovative defense strategies becomes more critical than ever. Traditional security solutions often struggle to swiftly differentiate between legitimate and malicious activities. ShadowPlex rises to this challenge by implementing cyber deception, a pivotal strategy that positions targeted traps outside of standard enterprise workflows. Any interaction with these traps provides and early warning system that signals malicious intent, enabling immediate detection. This comprehensive approach spans IT, OT, and cloud environments, and prevents adversary breakout while allowing defense teams to swiftly detect, isolate, and respond to threats, thereby protecting critical assets and sensitive data from compromise.

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**

Crop Marks
(use these when making a Printer PDF)