sweet.

A Starter's Kit:
How to Leverage Identity Insights to Stop Cloud Attacks

www.sweet.security

A Starter's Kit: How to Leverage Identity Insights to Stop Cloud Attacks

Human and non-human identities (NHI) have become increasingly vulnerable to exploitation. According to Verizon's Data Breach Indication Report, stolen credentials played a role in 31% of all breaches over the past decade, and last year alone, they were involved in 38% of breaches.

With the right identity, threat actors can access critical assets or even shut down cloud systems for ransom. Their tactics often involve blending in with normal behavior through stolen but valid credentials, making it difficult to detect their presence until it's too late.

At the end of the day, the crux of the issue lies in detecting these abnormal yet seemingly legitimate activities by human or non-human identities within the cloud. Yet their obscurity from traditional cloud security tools complicates efforts to monitor and respond to these types of attacks.

In this guide, we aim to address these challenges by exploring how to bridge the gap between identity and cloud security through Identity Threat Detection and Response (ITDR), ensuring a holistic defense against evolving identity-related threats.

This includes:

1. Visibility into secrets and identities across the infrastructure and containers
2. Identifying and mitigating risks related to secrets and identities
3. Establishing a behavioral baseline of the environment and the identities inside
4. Cross correlating the metrics from the identity to the activity happening in the environment
5. Detecting identity-related attacks occurring in real time

1 Visibility: Uncovering the Pandora's Box of Secrets and Identities

Secrets and identities are often hidden away, much like a Pandora's box. Without a clear view of what's inside, you could be unknowingly exposing your environment to significant risks. That's why having an inventory of all your identities is the very first step for effective detection and response against identity-based attacks, such as account takeovers, secret hunting, credential theft, and more.

How to Achieve it:

Comprehensive Secrets Inventory

Secrets are prime targets for attackers, and their exposure can lead to devastating breaches. Security teams need a solution that can ensure all secrets, including those hidden in configuration files, exposed in environment variables, or stored in plaintext, are accounted for and monitored:

- **Secrets Discovery and Usage:** Identify every secret across the your cloud environment, track how it's used at runtime, and highlight whether they're securely managed or at risk of exposure.
- **Managed vs. Unmanaged Secrets:** Integrate with popular secret management systems to identify unmanaged secrets and onboard them into secure management, reducing the risks associated with exposed or mishandled credentials.

Detailed Inventory of Human and Non-Human Identities

Managing who or what accesses your resources is just as important as securing the secrets themselves. That's why you need a detailed inventory of both human and non-human identities:

- **Human Identities:** Integrates with identity providers for visibility into human identity usage. This includes tracking login times, locations, devices, and behaviors, enabling quick detection of unusual or unauthorized access attempts.
- **Non-Human Identities:** From service accounts to API keys, this tracks the usage of non-human identities, providing insights into their interactions with cloud resources and highlighting any anomalies that could signal a security threat.

2 Reducing Exposure and Mitigating Threats

Secrets and identities are critical to cloud security, and mismanagement can lead to severe breaches. Proactively identifying and mitigating identity risks is essential to maintaining a secure cloud environment.

How to Achieve It:

- **Detecting Insecure Credential Storage:** Identify secrets stored in plaintext or exposed through environment variables and alert your team to take action, preventing unauthorized access.
- **Dormant and Over-Privileged Identities:** Highlight unused or dormant identities, particularly those with high privileges, which can be exploited by attackers.
- **Enforcing Secure Management Practices:** Flag unmanaged secrets and facilitate their onboarding into secure management, ensuring that sensitive information is always protected.
- **Over-Privileged Identities Monitoring:** Identify non-human identities, like service accounts or API keys, with excessive permissions, minimizing the risk of these identities being used maliciously.
- **Admin Account Usage Review:** Monitor admin account usage and flag any accounts being overused or accessed in unusual patterns, potentially indicating compromised credentials or insider threats.
- **Static Secrets Rotation:** Identify long-standing static secrets that haven't been updated, prompting regular rotation to reduce the risk of using stale or compromised credentials.

3 Establishing a Baseline

Understanding the normal behavior and access patterns within your cloud environment is key to detecting anomalies. Without a baseline, distinguishing between legitimate and malicious activities becomes impossible.

How to Achieve It:

- **Baseline Monitoring:** Implement monitoring tools that capture and analyze baseline behavior for both users and applications. These tools should track access patterns, resource usage, and interaction with data.

- **Regular Audits:** Conduct regular audits of your cloud environment and identity permissions. Ensure that roles and permissions align with the principle of least privilege.
- **Behavioral Analysis:** Use behavioral analytics to understand typical access patterns and interactions. This helps in setting a clear baseline for normal activity.

4 Cross-Correlating Identity Usage with Application Activity

Threat actors often leverage valid credentials to conduct malicious activities, blending in with legitimate operations. Correlating identity metrics with activity helps in identifying discrepancies that may indicate a compromise.

How to Achieve It:

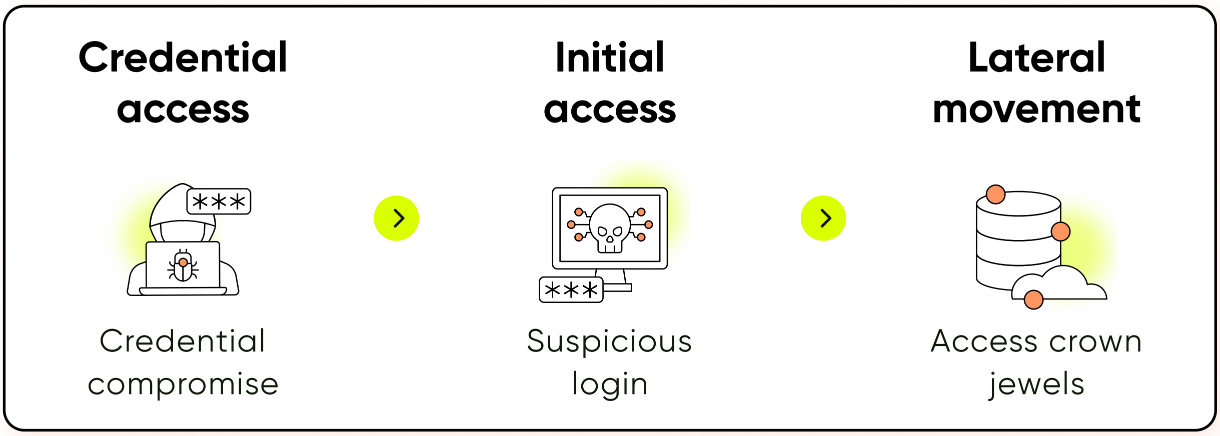
- **Unified Logging:** Ensure that all activities related to identity and access are logged.
- **Correlation Rules:** Set up correlation rules that match user activity patterns against known indicators of compromise (IoCs). For example, detect unusual access to sensitive data by high-privilege accounts.
- **Incident Response Integration:** Integrate identity and access metrics with your incident response workflows to quickly address anomalies.

5 Detecting & Responding to Identity Threats (ITDR) in Real-Time

Despite the increasing prevalence of identity-based attacks, the lack of synergy between identity and security detection tools limits the ability to effectively detect and respond to threats. It's imperative to leverage advanced monitoring and anomaly detection to identify suspicious activities involving secrets and identities. Here are some attack examples that can only be detected when identity and threat detection are merged together.

Attack 1: Account Takeover

Overview: An attacker steals a legitimate user's credentials and attempts to blend in with normal activities. You need to be able to detect deviations from the user's general behavior —such as logging in at strange hours, from unusual locations, or accessing resources outside their typical role.



Credential access — Credential compromise

Initial access — Suspicious login

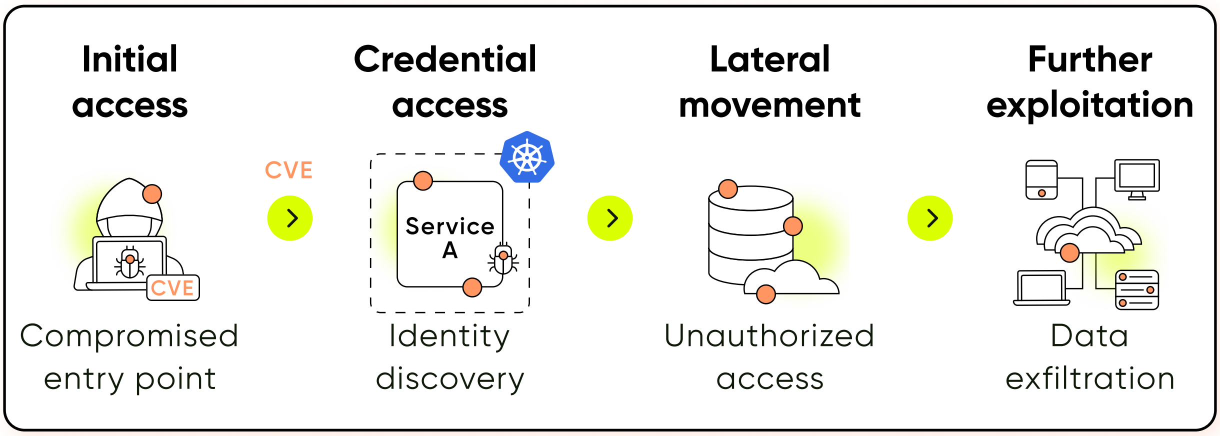
Lateral movement — Access crown jewels

Attacker's Steps:

1. **Credential Compromise:** The attacker acquires credentials through phishing or a data breach.
2. **Suspicious Login:** They attempt to log in from an unfamiliar IP address or at a time that deviates from the user's usual pattern.
3. **Uncharacteristic Actions:** The attacker accesses sensitive resources or performs actions outside the scope of the stolen identity's usual behavior.
4. **Anomaly Detection:** They mimic normal user activities to avoid detection, but the deviations from baseline behaviors trigger alerts.

Attack 2: Compromised Non-Human Identity

Overview: An attacker gains access to a machine and discovers non-human identities, such as a service account with broad access. They use this compromised identity to perform unauthorized actions, like accessing a database or reading sensitive data from a storage bucket, deviating from its normal usage patterns.



Initial access — Compromised entry point

Credential access — Identity discovery

Lateral movement — Unauthorized access

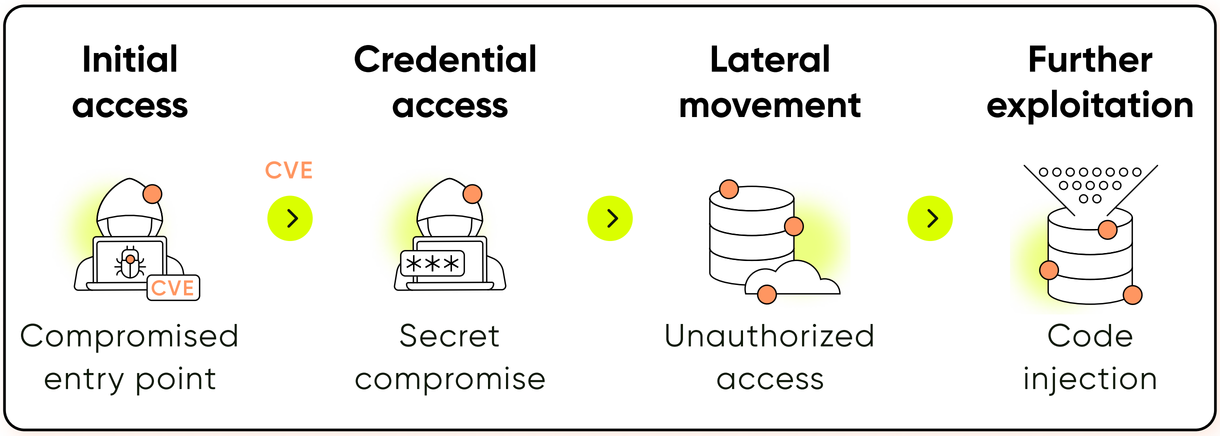
Further exploitation — Data exfiltration

Attacker's Steps:

1. **Compromised Entry Point:** The attacker gains access to a machine, perhaps through a vulnerability exploit.
2. **Identity Discovery:** They locate a service account or API key with significant access rights.
3. **Unauthorized Access:** The attacker uses this identity to access sensitive data in databases or storage buckets that the identity typically does not interact with.
4. **Data Exfiltration:** They leverage the access to escalate privileges or extract sensitive information, setting the stage for further attacks.

Attack 3: Secret Hunting and Exploitation

Overview: An attacker gains access to a compromised machine and starts searching for secrets—plain text credentials, tokens, or API keys—to facilitate lateral movement or privilege escalation within the cloud environment.

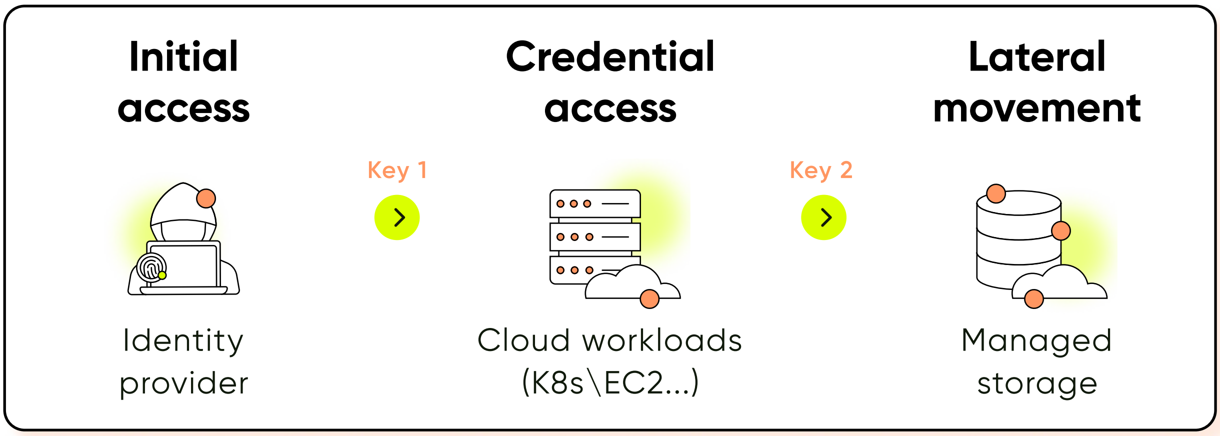


Attacker's Steps:

1. **Initial Compromise:** The attacker breaches a machine using phishing or exploiting a vulnerability.
2. **Secret Search:** They hunt for secrets stored on disk, within configuration files, or exposed in environment variables.
3. **Using Stolen Secrets:** The attacker uses these discovered secrets to move laterally within the environment or escalate privileges.
4. **Broader Network Access:** With the acquired access, they attempt further infiltration, such as with code injection, which changes the operation of the environment.

Attack 4: Exploited Vulnerability in an Identity Management Solution

Overview: Credential theft combined with lateral movement can lead to further breaches, as seen with successful credential stuffing attacks or in the example of Okta's customer support system breach. The diagram below showcases how an attacker can easily impersonate an employee via credential theft from the SaaS ID provider and move laterally within the environment using authorized tokens.



Attacker's Steps:

1. **Initial access:** The attacker exploited a vulnerability in the identity provider (e.g., Okta) to gain initial access to the environment of the identity provider's customer.
2. **Lateral Movement:** Using the stolen employee credentials, the attacker moved laterally within the environment to access critical workloads, which allowed them to navigate through the network and find further opportunities for exploitation.
3. **Exfiltration:** After gaining sufficient access and moving laterally, the attacker accessed the company's database and exfiltrated sensitive data.

Strengthen Your Cloud Security with Sweet Security

Sweet Security's Cloud Native Detection & Response platform offers a robust solution for enhancing cloud security through the mixture of identities management and cloud detection and response. By providing a full inventory of secrets and identities, monitoring for insecure practices and anomalies, and integrating with leading identity and secret management solutions, Sweet Security enables organizations to protect their cloud environments against sophisticated identity-based threats through cutting-edge Identity Threat Detection and Response (ITDR).

Enhancing Security with Identity and Secret Integrationst

Sweet Security integrates seamlessly with leading identity providers (OIDC) offering comprehensive visibility into human identity usage.

Our platform also integrates with secret management systems, such as AWS Secrets Manager, Azure Key Vault, and CyberArk Conjur, to manage secrets more securely and onboard with one click unmanaged secrets. By identifying unmanaged secrets and facilitating their onboarding into secure management systems, Sweet Security reduces exposure risks and ensures that all sensitive information is handled correctly.

Ready to secure your cloud environment like never before?
Contact us today for a demo and discover how Sweet Security can provide the attack detection you need to stay one step ahead of adversaries.

Secure your cloud with **sweet.**

Get a demo