ACALVIO

Acalvio ShadowPlex Honeytoken Accounts and Honeytokens for CrowdStrike Falcon® Identity Protection

Challenges:

Identity threats are involved in over 80% of all cyberattacks (including APT threats, Ransomware attacks, and Advanced malware). Attackers harvest identities from endpoints, applications, and identity stores in the enterprise. Attackers target Privileged Identities (human users, service accounts, and application credentials) to perform Lateral Movement and Privilege Escalation. When the threat actors obtain access to valid enterprise identities, their activities and movement within the network are masked as legitimate traffic. In any organization, the identity attack surface can be large, and eliminating all the entry points for attackers is very challenging for the security teams.

Solution:

ShadowPlex Honeytoken Accounts and Honeytokens for CrowdStrike Falcon® Identity Protection provide a new layer of Deception Technology-based Defense-in-depth for Identity Protection.

Honeytoken accounts and Honeytokens are a class of Deception Technology techniques that are proven to be extremely powerful and efficient in detecting a variety of identity threats. Honeytoken accounts are deceptive accounts (representing human and service accounts) created in Active Directory (AD) that are specifically designed to lure attackers and deflect them away from real identities. Honeytokens are deceptive credentials and data that are embedded in legitimate assets such as Falcon endpoints and cloud workloads. Any usage or manipulation of these deception artifacts is a very reliable indicator of an identity threat.

Acalvio ShadowPlex leverages Falcon® Identity Protection Honeytoken Account monitoring and containment policy to provide a scalable and effective deception-based identity threat detection solution.

Use Cases / Business Value:

Use Case / Challenges	Solution Description	Benefits
Customers are looking to operationalize the CrowdStrike Falcon® Identity Protection Honeytokens capability	ShadowPlex Honeytoken Accounts and Honeytokens provide a rich and mature set of capabilities for enterprises. The pre-integrated solution is completely automated for Honeytoken Account recommendation, creation, and deployment of Honeytokens at scale	• High-fidelity Identity threat detection based on Deception Technology • Built-in attacker containment • Generation of rich Identity Threat Intelligence
Deception-based detection of Identity threats on Falcon endpoints and unmanaged endpoints	ShadowPlex Honeytoken Accounts enable identity threat detection on unmanaged endpoints and Honeytoken Accounts with Honeytokens enable detection on managed Falcon endpoints	Identity threats can originate from any endpoint, including unmanaged endpoints. It is important to have visibility into these threats for analysis and timely responses to arrest the attack progression. Additionally, deceptions are very effective in luring the attackers and deflect them away from real identities.
Ability to extend Identity protection across the enterprise network	Acalvio ShadowPlex is a scalable offering that enables deployment across a large enterprise network with multiple Active Directory domains and a large number of endpoints	Attackers can target any domain or endpoint and use it to pivot to other domains and endpoints. Comprehensive coverage across domains and endpoints is essential to avoid detection gaps and blind spots for the defense teams.

Technical Solution:

CrowdStrike Falcon® Identity Protection has built-in support for monitoring honeytoken accounts and a policy-based identity threat containment and response mechanism. Any access or alterations of honeytoken accounts trigger a dedicated detection, giving the SOC analysts visibility into the adversary attack path.

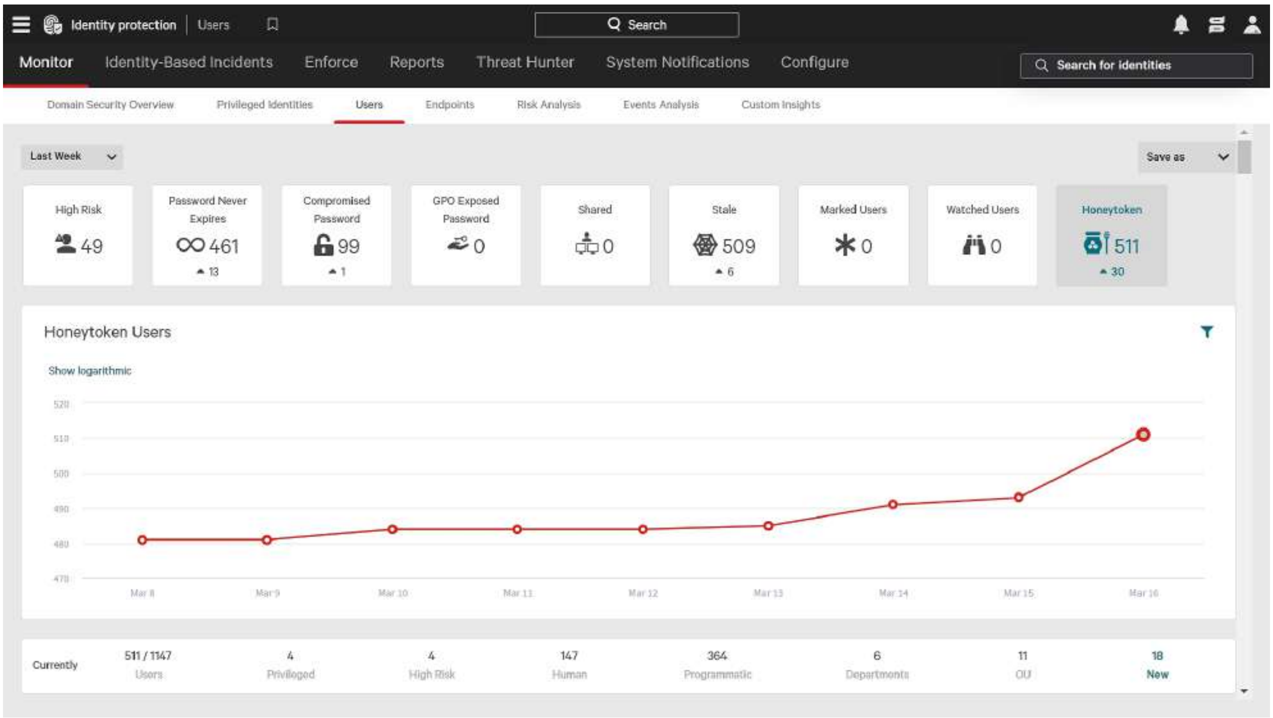
Manually creating Honeytoken Accounts and Honeytokens is a laborious process and it is extremely challenging to make them attractive to attackers. Acalvio ShadowPlex brings the power of deception technology coupled with advanced AI to provide the following direct benefits:

- Advanced deception technology for sophisticated, fingerprint-resistant deceptive artifacts
- Automated recommendation of effective and attractive Honeytoken Accounts
- Automated creation and seamless deployment of Honeytokens on endpoints
- Automated Honeytoken lifecycle management, including periodic refresh.

Acalvio ShadowPlex platform brings years of domain expertise in Deception Technology. Acalvio's platform is tightly pre-integrated with the Falcon® platform to enable CrowdStrike customers to easily and quickly leverage the power of the new Falcon® Honeytoken Accounts capabilities to protect critical assets.

Key Solution Capabilities:

- **Advanced Deception Technology:** Acalvio ShadowPlex Honeytoken Accounts and Honeytokens, a class of advanced deceptions that provide a new layer of Defense-in-depth for Identity Protection.
- **Advanced AI-based Honeytoken Accounts Recommendation:** Honeytoken Accounts are deceptive user accounts, service accounts, and application identities added to identity repositories.
- **Automated Creation and Deployment of Honeytokens:** Deceptive credential profiles deployed on Falcon endpoints.



High Risk	Password Never Expires	Compromised Password	GPO Exposed Password	Shared	Stale	Marked Users	Watched Users	Honeytoken
49	461	99	0	0	509	0	0	511
	▲ 13	▲ 1			▲ 6			▲ 30

Currently	511 / 1147	4	4	147	364	6	11	18
	Users	Privileged	High Risk	Human	Programmatic	Departments	OU	New

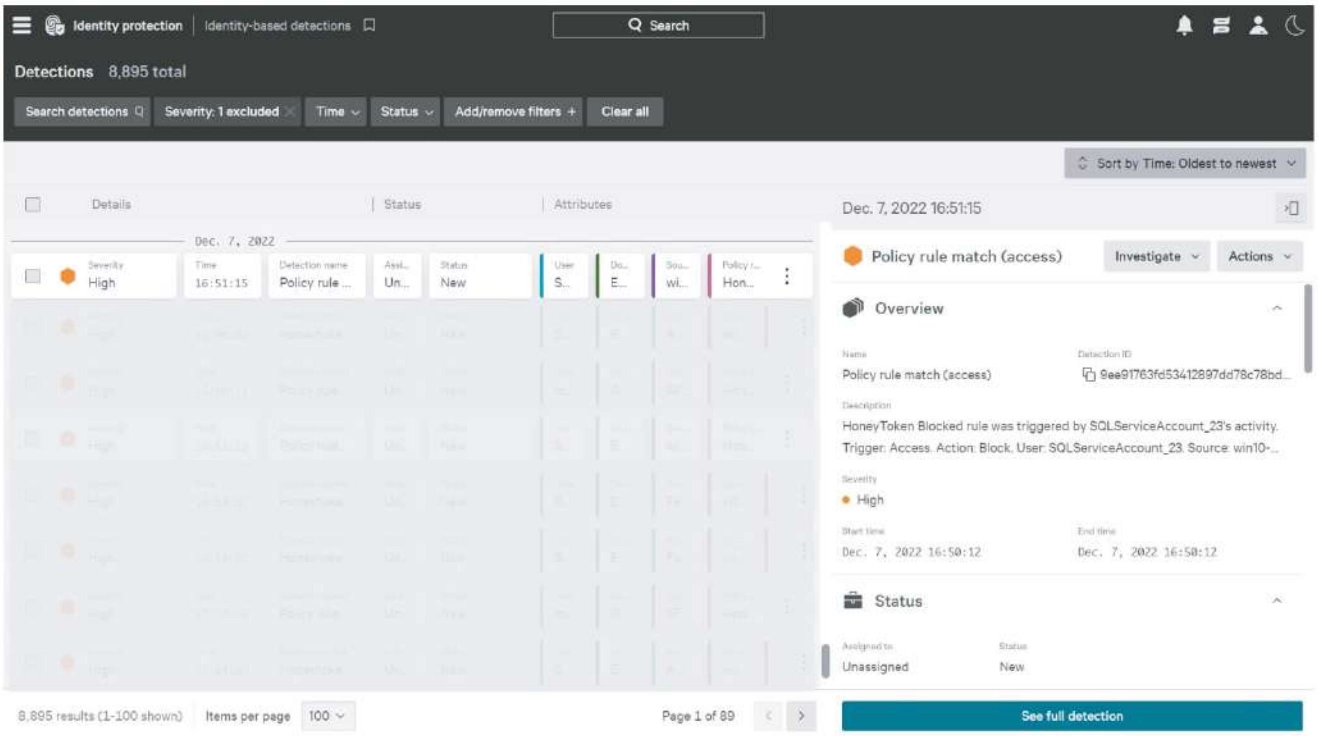
Figure1: ShadowPlex recommended Honeytoken Accounts in Falcon® Identity Protection console

CrowdStrike Falcon® Identity Protection has built-in support for monitoring honey accounts and a policy-based identity threat containment and response mechanism. Any access or alterations of honey accounts trigger a dedicated high-fidelity detection, giving SOC analysts visibility into the adversary attack path.

Automated Deployment and Maintenance

If security administrators were to manually create honey accounts in AD, it would be an involved and challenging process, given the various design dimensions to consider in making honey accounts effective and attractive to attackers. Acalvio ShadowPlex abstracts away these challenges by bringing in years of domain expertise in Deception Technology. Acalvio's platform is seamlessly pre-integrated with the CrowdStrike Falcon® platform to enable CrowdStrike customers to leverage the power of honey accounts and honeytokens easily and quickly.

Honeytokens created by the Acalvio ShadowPlex platform blend well with existing identity caches on endpoints. Honeytokens extend the power of honey accounts to Falcon-managed endpoints and even unmanaged endpoints.



Detections 8,895 total

Details			Status		Attributes			
Severity High	Time 16:51:15	Detection name Policy rule ...	Assi... Un...	Status New	User S...	Do... E...	Sou... wi...	Policy r... Hon...

Dec. 7, 2022

8,895 results (1-100 shown) Items per page 100

Page 1 of 89

Dec. 7, 2022 16:51:15

Policy rule match (access)

Overview

Name: Policy rule match (access)

Detection ID: 9ee91763fd53412897dd78c78bd...

Description: HoneyToken Blocked rule was triggered by SQLServiceAccount_23's activity. Trigger: Access. Action: Block. User: SQLServiceAccount_23. Source: win10-...

Severity: ● High

Start time: Dec. 7, 2022 16:50:12

End time: Dec. 7, 2022 16:50:12

Status

Assigned to: Unassigned

Status: New

Figure2: Honeytoken activity blocked using policy settings

The Honeytokens fulfillment capability from Acalvio is a completely automated solution, pre-integrated into the Falcon® platform, and does not require any additional Acalvio software to be installed. Acalvio provides a single console solution to CrowdStrike Falcon® customers.

Key Solution Benefits:

- A fully automated, robust platform for operationalizing honeytoken accounts for Identity Protection.
- Honeytokens capability seamlessly extended to Falcon endpoints, including deployment and refresh lifecycles.
- Advanced AI-based recommendation engine for Honeytoken Accounts
- Pre-integration with CrowdStrike Falcon® Identity Protection and no additional software to install on enterprise networks.
- Complete control on types and counts of honeytoken accounts being created for customers.
- Powerful capability to detect identity threats from managed and unmanaged endpoints including in Zero Trust environments.

About Acalvio Technologies

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 for IT and OT networks, 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 from the Cloud, on-premises or via marquee managed service providers.

Active Defense with Cyber Deception Technology | Acalvio