Acalvio ShadowPlex and CrowdStrike Falcon Integration

Introduction

Acalvio and CrowdStrike have built a strategic partnership to offer the best-in-class **Identity Security** solution on the CrowdStrike platform. A key part of this partnership between Acalvio and CrowdStrike is the **tight integration** between Acalvio's ShadowPlex and CrowdStrike's Falcon platforms. **Acalvio App on the CrowdStrike (CS) Store** allows CrowdStrike customers to try-and-buy the Acalvio ShadowPlex solution.

Acalvio App on CrowdStrike Store: High-level Overview

The Acalvio app combines the power of Acalvio's Deception Technology with CrowdStrike capabilities for **rapid and precise detection** of identity attacks, including advanced threats, which enables **automated real-time response** to mitigate cyber threats.

Acalvio uses CrowdStrike detections and vulnerability assessments as some of the inputs in generating Identity Attack Paths. In addition, the Acalvio app offers novel **threat investigation, threat confirmation, and threat hunting** capabilities by combining Acalvio's dynamic deception platform capabilities with CrowdStrike's endpoint telemetry, agents on endpoints and sandbox capabilities.

Integration Overview

This document briefly describes the tight integration between ShadowPlex and CrowdStrike Falcon platforms.

1. **Rich Telemetry Data (FDR) streamed by CrowdStrike**

   The rich telemetry of endpoint activities is streamed by the CrowdStrike service for use by the Acalvio Managed Service.

   This telemetry data is leveraged for **Threat Confirmation and to confirm activity against ShadowPlex deception** deployed on the endpoints.

2. **Endpoint Discovery Data**

   The Acalvio app leverages CrowdStrike APIs to discover all endpoints with the CrowdStrike sensor installed on them.

   This neighbourhood discovery data is used by ShadowPlex for the **auto-blending of deceptions** in every subnet.

3. **CrowdStrike Detections**

   The CrowdStrike detection events and incidents are read by ShadowPlex using the CrowdStrike-SIEM connector. This integration requires explicit access approval by the customer.

   ShadowPlex uses these detection events for discovering **Identity Attack Paths**.

4. **Deployment of Deceptions**

   ShadowPlex leverages the CrowdStrike agent on endpoints to deploy and manage endpoint deception autonomously. This feature requires the customer to explicitly grant access to the RTR APIs via the CrowdStrike console.

5. **Falcon Spotlight Endpoint Vulnerability Assessment Data**

   ShadowPlex is integrated to fetch and use endpoint vulnerability assessment data from CrowdStrike Falcon Spotlight. This integration requires explicit access approval by the customer.

   The vulnerability data from Falcon Spotlight is used for discovering **Identity Attack Paths**.

6. **EDR Response functionality**

   ShadowPlex is integrated with CrowdStrike to enable **automated responses**.

   If the customer configures automated response policy in ShadowPlex, this integration is used to quarantine automatically and in real time an endpoint on a detection event.

7. **FalconX Sandbox integration**

   ShadowPlex is integrated with CrowdStrike FalconX sandbox as well as CrowdStrike's Hybrid Analysis (https://www.hybrid-analysis.com/) engine.

   ShadowPlex High Interaction Decoys capture multiple artifacts including the tools, files, and scripts downloaded by the attacker onto the decoy. ShadowPlex integration with the CrowdStrike sandbox enables the defense to **optionally detonate any collected malware in a sandbox.**