ACALVIO SHADOWPLEX

AUTONOMOUS DECEPTION
Deception as a Strategic Imperative

"We must move away from trying to achieve the impossible perfect protection and instead invest in detection and response.”

Peter Sondergaard, Head of Research, Gartner
Deception is **NOT** just Honeypots

**Decoys**
- IP addressable false targets
- Respond and interact with an adversary
- Designed to look and feel like legitimate systems

**Lures**
- Deliberately placed vulnerabilities
- Application, OS and protocol CVEs (Common Vulnerabilities and Exploits)
- Weak configuration and permissions
- Fake Service Accounts

**Baits**
- Deception objects on legitimate endpoints
- Trigger Alert independent from decoys
- Examples include Ransomware Detonation and Beaconing Documents

**Breadcrumbs**
- Fake info on legitimate systems
- Diverts adversary away from real systems and towards your decoys
- Agentless, Non-finger-printable
- Only discoverable by advanced attackers (end-user not affected)
How Deception Works: Creating an Attacker’s Challenge

Initial Foothold
• Attacker has remote command & control

Establish Additional Beachheads
• Redundancy
• Sacrificial lambs

Lateral move towards Mission Objective(s)
• Data exfiltration
• Disruption

Workstation & Server Decoys
• Dense Minefield
• Detect Adversary as Beachheads Established

Breadcrumbs
• Present False Trail
• Deceive Adversary During Recon
• Divert Away from Mission Objective to Decoy

Baits
• Data decoys on endpoints
• Carefully placed tripwires that alert when accessed
ShadowPlex – A Comprehensive Platform

Detect Threats
- With Precision & Speed
- Leverage InSights & Autonomous Deceptions

Protect
- Enterprise Assets
- Cloud Workloads
- IoT & ICS

Investigate Threats & Attacks
- Threat Confirmation
- Hypothesis Testing
- Threat Hunting – Ferret Latent Threats

Respond to Threats
- Automated real-time Response
- Threat Containment, Diversion

Respond

Investigate

SHADOWPLEX
Acalvio ShadowPlex Unique Features

Deception Farms Architecture
- Cloud-based Deception projected across distributed enterprise, on-premises and in Cloud
- Just-in-time decoys minimize 3rd-party licensing costs

Enterprise Scale with Interaction Depth
- Patented FluidDeception® technology enables thousands of decoys
- Dynamically increases the interactivity of the decoy under attack to gather full TTPs

Complete Deception Palette
- Decoys, Breadcrumbs, Baits & Lures
- 100+ built-in deception types, customizable and extensible

Autonomous Deception
- Ease of use
- Configuration, deployment and management of deception is completely driven by AI

Effective Deception
- Non fingerprintable deception – completely blended into each neighborhood
- Deception customized by AI for every subnet and host
- Agent-less

Attack Containment by Design
- Decoys cannot be used as base for pivot-back attacks

Built on 25 Issued Patents
Deception – Complementary Dimension to EDR

Deception-based Detection adds to CrowdStrike EDR

❖ Detects both known and unknown threats
❖ No false positives - any activity against Deception is suspect
❖ Ability to introduce new types of resources to attract latent threats
❖ Ability to detect threats against resources where agents cannot be installed
  ➢ E.g. Printers, Routers / Switches, IoT Cameras
  ➢ Legacy systems, e.g. Windows 95
❖ Active - not just observe but *Engage* and *Delay* attacks
Acalvio + CrowdStrike Integration Architecture

Deception Deployment
1. ShadowPlex requires only sensors (physical or virtual) to be deployed in enterprise network
2. Endpoint telemetry data from CrowdStrike used to automatically configure decoys
3. CrowdStrike API to deploy breadcrumbs on enterprise hosts – Optional Integration

Investigation
4. CrowdStrike telemetry to
   a) Trace attack back thru’ n/w
   b) Threat hunting using Deception

Response
5. CrowdStrike API to quarantine infected host – Optional Integration