Acalvio ShadowPlex for OT/ICS

How operational technology defends against cyber threats through a non-intrusive solution based on cyber deception

Why OT cybersecurity is different than IT

OT environments have unique characteristics. OT environments have purpose-built hardware and software with specialized form factors, designed for industrial and manufacturing processes. The form factor of OT equipment makes it challenging to deploy agent-based security solutions.

Outdated devices with little security as OT devices typically have longer lifetimes

- Weak or no authentication
- Lack of encryption

Patch application is challenging

- Patches are not always available as devices are not supported or purpose built
- The need for uninterrupted business operations makes patch application difficult

Limited security tooling

- Agent-based security solutions are not compatible with assets in the OT environment
- Network Detect and Respond (NDR) solutions are not inline, making the detection slow

Attack surface in OT environments

OT environments have a significant attack surface that is being exploited by threat actors. The threats originate from multiple factors, including:

Increased convergence of IT with OT: Adversaries leverage the trusted pathways between IT and OT to pivot from IT to OT. These pathways include shared Active Directory (AD) environments, jump servers and similar equipment that is common to IT and OT.

OT equipment is increasingly connected to the public internet: Equipment in OT environments is increasingly connected to the public internet, to enable remote administration and monitoring. Internet connectivity creates a significant attack surface, attackers exploit the public facing OT assets to gain a foothold into the OT environment.

Legacy IT equipment in OT: OT environments often have legacy IT equipment, such as workstations that run on legacy operating system versions. This creates a significant attack surface, with attackers gaining the ability to perform vulnerability exploits that target this legacy equipment.

OT protocols do not support encryption and authentication: Multiple OT protocols are unencrypted and do not support authentication. This enables an attack surface where attackers can sniff and perform man in the middle attacks to intercept and transform communication between the assets.

Threats targeting OT environments

Ransomware: Ransomware is one of the primary threat vectors targeting OT environments. The critical nature of ICS systems make ransomware a particularly challenging threat. The Colonial Pipeline attack was a high-profile attack in recent times. Ransomware attacks continue to escalate in intensity and frequency in OT environments, with groups such as Lockbit and BlackBasta specifically targeting OT environments..

APTs: Advanced Persistent Threats (APTs) are increasingly targeting OT environments, with nation-state threat actors looking to perform espionage or data theft from industrial environments. APT groups specialize in targeting specific verticals within ICS, leveraging deep knowledge of the equipment characteristics to perform stealthy attacks.

OT specific malware: OT environments are being targeted with specific malware variants that exploit the lack of encryption and authentication in OT protocols to conduct exploits. From the original malware such as Stuxnet and Havex to more recent malware versions such as CosmicEnergy, custom OT specific malware creates significant damage to OT environments.

Insider threats that target OT assets: Insider threats are important threat vectors, with insiders leveraging the trusted access to perform exploits against OT assets.

Supply chain attacks: Supply chain attacks are increasing rapidly with the increased adoption of open-source software as part of the software supply chain. The Log4j exploit is an example of an exploit that can be propagated through a supply chain compromise and can target OT assets.

Acalvio ShadowPlex

Traditional approaches to OT security have limitations

OT security approaches have been divided into preventive controls and passive detection.

Prevention controls for OT have traditionally been focused on air gapping. The increased connectivity between OT and IT has reduced the effectiveness of air gapping as a security control. Attackers exploit the pathways between IT and OT to pivot from IT environments to OT.

OT threat detection is primarily based on passive detection. Passive detection solutions typically connect to a SPAN port, analyze the mirrored traffic to identify threats based on anomaly detection, signature, and log analytics. These solutions are useful to detect a set of known attacks with known attacker TTPs. These solutions have a challenge with false positives that are associated with anomaly-based detection approaches.

Equipment in OT environments has special form factors, with low computing resource requirements and special purpose hardware and software. OT equipment such as Programmable Logic Controllers (PLCs) is not compatible with agent-based security controls such as endpoint detection and response (EDR) and Antivirus (AV).

Modern adversaries are bypassing traditional detection approaches in OT through novel offensive techniques, living off the land (LotL) exploits, zero days.

With the wide variety of threats targeting OT environments, it is essential for OT security to adopt a defense in depth approach, by combining a set of independent and interlocked detection layers for comprehensive detection coverage. Adding a detection layer that can detect evolving threats, zero days and can detect threats against identity architecture and endpoints is essential.

Cyber deception provides a necessary detection layer for OT security

Deception technology involves deploying a set of deceptive elements that serve as traps for the adversary. This includes decoys that represent OT and IT assets and endpoint deceptions deployed on the assets. Deceptions do not impact the OT environment and are not used in existing OT workflows. Any usage of the deceptions is an immediate indicator of malicious activity.

Deception is an effective approach to OT threat defense, providing early and precise detection of OT threats. Deceptions are characterized by:

- Deception is non-intrusive and low-risk. Deception does not sit inline, does not scan and does not disrupt normal OT operations.
- ShadowPlex Deception does not require any resources from the customer
  - All decoys are physically generated and managed completely inside the ShadowPlex service. Decoys do not require any resources from the enterprise network. Decoys are only "projected" into the network.
  - ShadowPlex is agentless
  - ShadowPlex does not generate any network traffic
  - Autonomous deception makes deception easy to deploy and manage

ShadowPlex protection for OT environments

ShadowPlex provides an extensive palette of deceptions for OT environments. This includes decoys that represent assets across the levels of the Purdue OT/ICS reference architecture. ShadowPlex decoys support multiple interaction levels - low, medium, and high interaction. ShadowPlex decoys represent OT assets including HMIs, PLCs, Controllers and support multiple OT protocols, such as Modbus, Ethernet/IP, Siemens S7, BACnet.

ShadowPlex deceptions detect multiple adversary tactics targeting assets in OT and enable SOC and IR teams to gain actionable intelligence to OT environment threats. The detections include the early stages of the attack lifecycle such as Discovery, Lateral Movement and includes advanced tactics such as Impair Process Control and Inhibit Response Function.

Discovery/asset visibility for OT environments

ShadowPlex provides support for multiple approaches for performing discovery of assets in OT environments. The discovery data enables blended deceptions to be deployed in the OT environment.

ShadowPlex leverages a combination of pre-built integrations for discovery in OT environments. ShadowPlex gains visibility into the production endpoints through integrations with EDR, Active Directory.

Native support for OT deceptions in deception palette

ShadowPlex offers IT and OT deceptions to represent assets in the OT environment. ShadowPlex provides a rich combination of OT decoys, IT decoys, endpoint deceptions (breadcrumbs and baits) to detect threats in the OT environment. **ShadowPlex has 350+ pre-built deceptions for OT and IT assets.** ShadowPlex also provides extensibility, enabling the deployment of custom deception that represent specific types of assets in the OT environment.

OT Decoys

ShadowPlex provides support for OT decoys. The decoys are deployed adjacent to the real OT assets and enable detection of threats targeting the OT environment.

Examples of OT decoys include

- PLCs (Programmable Logic Controllers)
- HMIs (Human Machine Interfaces)
- Controllers
- IoT Assets such as IoT cameras, DVMs, NVRs, and printers.

ShadowPlex has native support for OT/ICS protocols, including Modbus, BACnet, Ethernet/IP, and S7. This enables defense teams to gain visibility to the attacker TTPs beyond the initial connection to the OT decoy. For example, ShadowPlex can deploy PLC decoys that support Modbus protocol and detect attacker actions such as Read Coil or Write Coil.

The OT decoys represent assets from multiple OEM vendors in OT, such as Honeywell, Rockwell Automation, Schneider Electric, Siemens etc.

Support for multiple OT protocols and equipment types provide comprehensive threat detection for threats targeting OT assets.

IT Decoys

ShadowPlex provides decoys representing IT assets within the OT environment, such as engineering workstations and jump servers. This enables early detection of threats that target the IT assets in the OT environment

ShadowPlex also provides support for deploying decoys that represent legacy IT assets in the OT environment. Patching/upgrading assets in the OT environment can be challenging and IT assets are often deployed with legacy OS and application versions. ShadowPlex decoys can represent legacy IT assets to detect attackers attempting to exploit vulnerability against legacy IT equipment in the OT environment.

Endpoint Deceptions

ShadowPlex provides a comprehensive set of endpoint deceptions (breadcrumbs and baits) deployed on production endpoints.

ShadowPlex endpoint deception deployment is agentless. This avoids the management challenges associated with the deployment of additional agents and avoids an increase in the attack surface when additional agents are deployed.

ShadowPlex offers pre-built breadcrumbs with credential profiles that can guide potential attackers to IT and OT decoys in the OT environment. These breadcrumbs include:

- Browser profile breadcrumbs leading to the web interfaces of OT/IoT decoys.
- Breadcrumbs deployed in the operating system cache, such as ARP (Address Resolution Protocol), memory cache, and RDP (Remote Desktop Protocol) cache.

ShadowPlex also allows for custom breadcrumb profiles, enabling the deployment of additional breadcrumb types leading to OT decoys. Breadcrumbs are deployed on engineering workstations and similar IT assets within the OT environment.

ShadowPlex provides baits that are deployed on IT assets in the OT environment and enable the defense to detect threats such as data exfiltration.

Extensible deception palette

ShadowPlex provides an extensible deception palette, with the ability to customize the out of box deceptions to represent OT assets in specific verticals. The decoys, breadcrumbs and baits can be customized at multiple levels, from custom content associated with the deceptions to deploying a custom decoy based on a Golden VM image that is provided by the administrator.

The extensible deception palette enables OT deceptions to be deployed across the set of OT verticals and industry focus.

OT threat detections/incidents

ShadowPlex deceptions enable early and precise threat detection. ShadowPlex has a built-in threat analytics engine that performs automated summarization, enrichment and correlation of the deception events to generate actionable, high-fidelity incidents. ShadowPlex incidents are automatically enriched using the integration with threat intelligence reputation services such as VirusTotal. ShadowPlex incidents are mapped to the MITRE ATT&CK for ICS framework and the corresponding Tactics and Techniques are surfaced in the incidents.

ShadowPlex incidents surface vulnerability exploit attempts made by attackers against OT and IT assets. The detections include tactics corresponding to attacker actions early in the attack lifecycle such as Discovery, Lateral Movement. Advanced attacker tactics such as Impair Process Control and Inhibit Response function can be detected.

The incidents are sent to the SIEM and SOAR through native ShadowPlex integrations. This enables SOC and IR teams to perform investigation and response actions from the existing SOC platforms.

Response

ShadowPlex provides response capabilities to isolate a compromised endpoint. ShadowPlex supports automated response options for automated isolation of the compromised endpoint after a detection. The response actions are performed based on pre-built integrations in ShadowPlex.

Out of the Box Deception Palette for OT Environments

ShadowPlex provides Deception Playbooks that deploy packaged solutions for assets in OT environments. ShadowPlex Deception Playbooks for OT environments include deceptions for OT verticals, including:

- Oil and Gas
- Water Treatment
- Electricity
- Manufacturing
- Industrial Process Automation

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**