ACALVIO
AI-POWERED DECEPTION

ShadowPlex Threat Intel

Targeted Threat Intelligence for Preemptive Cyber Security

What is Targeted Threat Intelligence

Threat intelligence is a collection of data that helps organizations understand and respond to cyber threats. It is used to identify potential risks, understand the motivations of attackers, and develop long-term security strategies.

Generic threat intelligence provides broad insights about emerging attack vectors and threat trends across industries, while "targeted threat intelligence" focuses on specific information about a particular organization or threat actor, tailored to their unique vulnerabilities and potential attack methods, allowing for more proactive defense strategies against imminent threats.

Advanced attackers such as the Midnight Blizzard APT threat group leverage password spraying against a limited number of accounts to gain initial access. Generic threat intelligence is less effective against such precise attacks, requiring targeted threat intelligence to identify the threat activity and enable proactive response actions.

ShadowPlex Threat Intel

ShadowPlex Threat Intel deploys a number of external-facing decoys for web applications and other services that are typical of the services exposed for an organization. ShadowPlex TI is a managed service that includes customization, deployment and management of all the decoy services. ShadowPlex TI filters the noise and generates specific intelligence on the threats targeting the enterprise. The threat intel is shared using standard STIX format so that the organization can automatically consume and react on the intelligence.

Targeted intelligence provides actionable insights to directly address specific threats against an organization and includes detailed indicators of compromise (IoCs) like IP addresses, compromised credentials, geolocation and specific TTPs used, such as password spraying, brute force, credential stuffing attacks.

Gartner defines preemptive cyber security as “an emerging category of cybersecurity technologies that are designed to prevent, stop or deter cyberattacks from achieving their objectives” and highlighted Acalvio as the innovator in Advanced Cyber Deception. ShadowPlex TI is a key pillar of preemptive cyber security by providing early threat detection, enabling security teams to proactively build appropriate security measures.

KEY BENEFITS

- Detailed and actionable threat intelligence on the attacks specifically targeting an organization
- Alerts on even zero-day exploits
- Immediate notification, enabling quick proactive strengthening of the security posture
- Identification of stolen credentials, addressing one of the biggest threat vectors
- Detailed TTPs enable threat hunting
- Key pert of preemptive cyber security

FEATURES

- Easy and quick deployment
- Completely managed service
- Standard STIX based notification
- Periodic report generation

WHAT DOES THE SERVICE INCLUDE

Decoy Customization

Customer can choose from a wide variety of decoy types and Acalvio will customize the decoys as appropriate for the customer. Additional decoy types can also be created.

Hosting the Decoys

Acalvio will host and manage all the decoys in our own cloud infrastructure. This also removes all attacks against the decoys completely away from the customer's network.

Threat Intel

All threat intelligence generated by the decoys is shared immediately using STIX format. In addition, periodic reports can be scheduled.

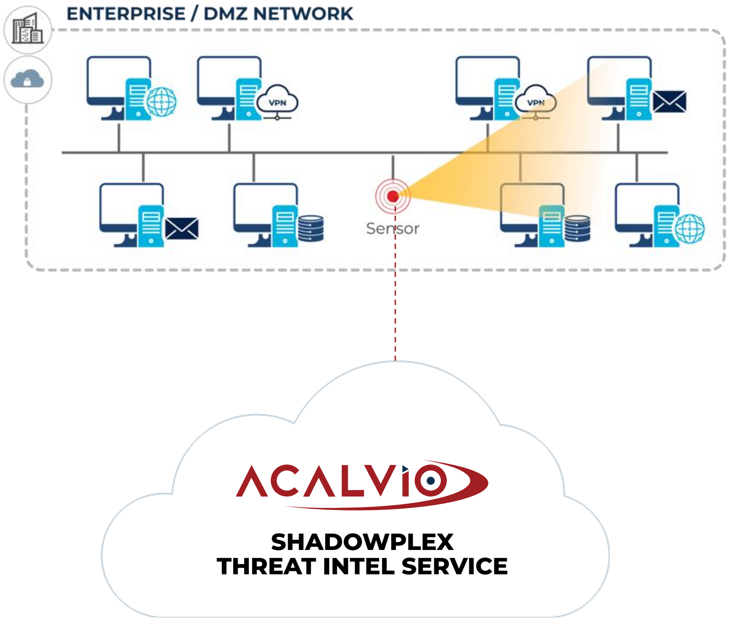
Management Console

Customers can use the management console to view threat intel data, schedule reports, configure integrations etc.

ARCHITECTURE

ShadowPlex Threat Intel is a managed SaaS solution that generates intelligence on threats specifically targeting an enterprise.

The architecture enables easy deployment. Only a ShadowPlex sensor (a small virtual appliance) is deployed in the customer's DMZ. All the decoys are hosted and managed in Acalvio cloud infrastructure, keeping the attacks completely isolated from the customer's enterprise network.



Acalvio is the leader in autonomous cyber deception technologies, arming enterprises against sophisticated cyber threats including APTs, insider threats and ransomware. Its AI-powered Active Defense Platform, backed by 25 patents, enables advanced threat defense across IT, OT, and Cloud environments. Additionally, the Identity Threat Detection and Response (ITDR) solutions with Honeytokens enable Zero Trust security models. Based in Silicon Valley, Acalvio serves midsize to Fortune 500 companies and government agencies, offering flexible deployment from Cloud, on-premises, or through managed service providers. **www.acalvio.com**