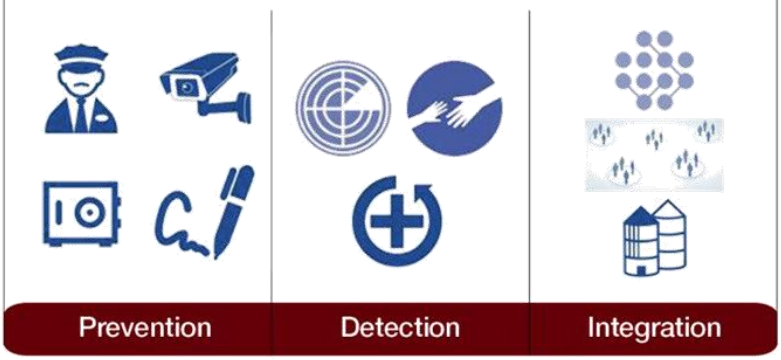
INGRAM MICRO SECURITY

Solution Architecture – Cisco & AlienVault

Multi-vendor intelligence based solution

Threat Landscape Today

Cyber Security Landscape Today



The Solution…

Vendors Involved

Umbrella
Threat Intelligence Director (TID)
Firepower Devices (NGFW, NGIPS, Firepower Services)

USM Anywhere
Open Threat Exchange (OTX)

Cisco Umbrella

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet wherever users go.
Cisco Umbrella uses the internet's infrastructure to block malicious destinations before a connection is ever established. Umbrella uses DNS to stop threats over all ports and protocols - even direct-to-IP connections.
Stop malware before it reaches your endpoints or network. Instead of proxying all web traffic, Umbrella routes requests to risky domains for deeper URL and file inspection

AlienVault USM Anywhere

AlienVault USM Anywhere delivers powerful threat detection, incident response, and compliance management across cloud, on-premises, and hybrid environments. Unlike any other security solution on the market today, USM Anywhere combines multiple essential security capabilities in one unified platform: asset discovery, vulnerability management, intrusion detection, behavioral monitoring, SIEM, and log management, as well as continuous threat intelligence.

USM Anywhere
Open Threat Exchange (OTX)

Cisco Threat Intelligence Director (TID)

The Cisco Threat Intelligence Director (TID) operationalizes threat intelligence data, helping you aggregate intelligence data, configure defensive actions, and analyze threats in your environment.

When installed and configured on your hosting platform, TID ingests data from threat intelligence sources and publishes the data to all configured Cisco Firepower Devices (NGFW, NGIPS, Firepower Services).

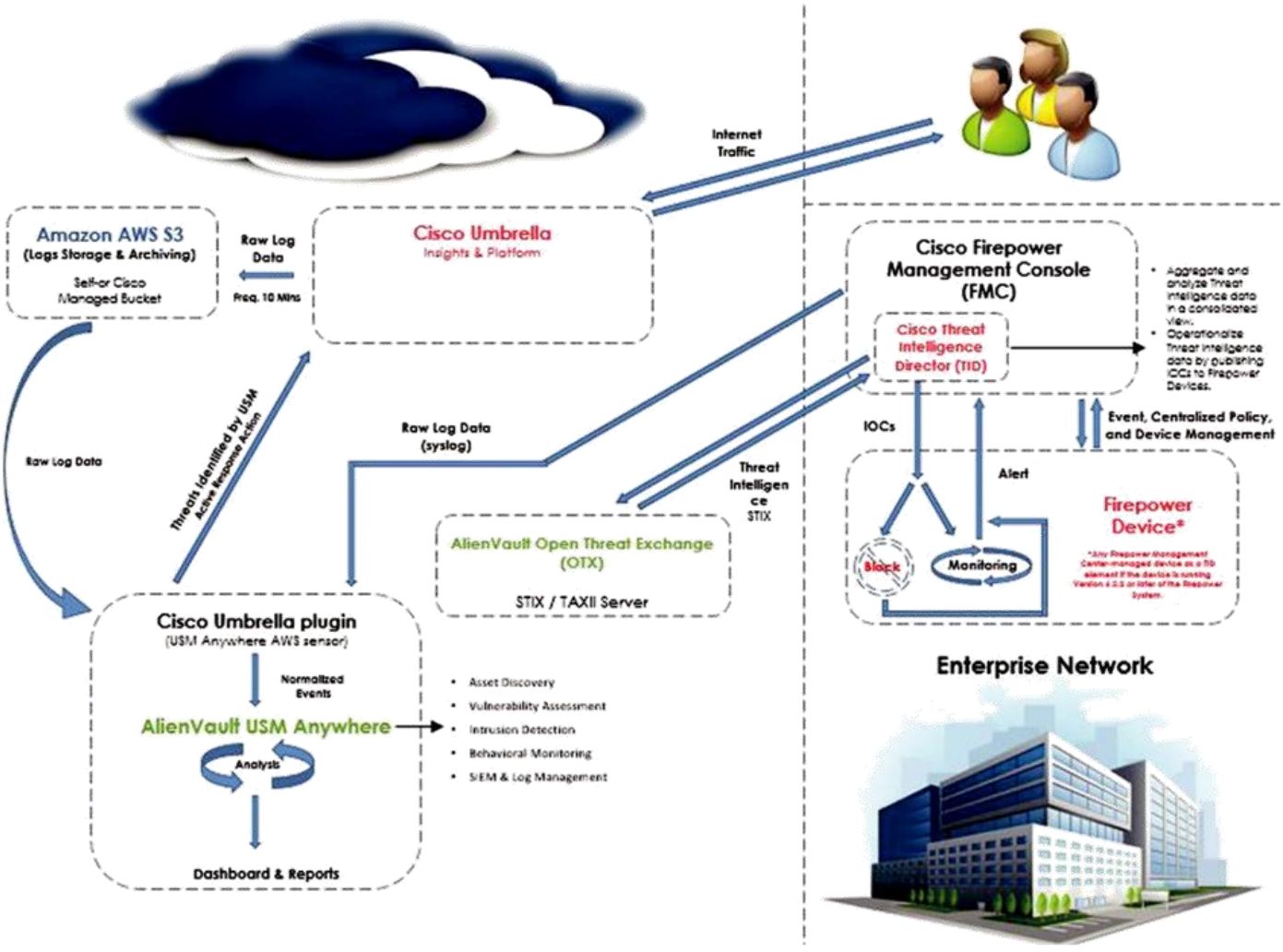
AlienVault Open Threat Exchange (OTX)

AlienVault OTX is an open threat intelligence community that enables collaborative defense with actionable, community-powered threat data.

AlienVault OTX provides open access to a global community of threat researchers and security professionals. It now has more than 65,000 participants in 140 countries, who contribute over 14 million threat indicators daily.

Integration Relationships

1. Umbrella ----Log----> AlienVault USM
2. AlienVault USM ----Threats (Malicious Domains)----> Umbrella
3. Firepower Devices ----Log----> AlienVault USM
4. AlienVault OTX ----Threat Intelligence----> Cisco TID ----IOCs----> Firepower Devices ----Observations----> AlienVault USM



About the Integration

AlienVault and Cisco deliver a full package of security essentials for threat detection, taking your threat detection and response capabilities to new levels. With the integration of these products, you can add Umbrella logs to USM Anywhere to gain visibility into all internet activity and automated alerting, and you can send malicious domains detected within USM Anywhere to Umbrella for automated blocking.

Cisco Threat Intelligence Director (TID) aims to tap into resources that help you corroborate evidence of suspicious behavior and then automatically act to contain the threat. By ingesting threat intelligence from AlienVault OTX threat feeds, TID correlates enriched observations from Cisco security sensors to detect and alert on security incidents. By converting intelligence into actionable indicators of compromise, your network defenses can block or monitor more threats, reduce the number of alerts to review, and improve your overall security posture.

Integration Benefits

Save Time & Money

- SaaS-delivered threat detection eliminates hidden costs and saves time.
- Affordable subscription-based pricing for USM Anywhere and Cisco Umbrella; buy what you need, add as you need.
- Unify visibility across cloud and on-premises environments, reducing time and expense of integrating and managing multiple products.
- Focus on threat response and not writing complex security analytics rules

Reduce Time to Detection & Response

- Get prioritized, contextual alarms with AlienVault OTX and the Cisco Talos backbone for robust threat intelligence
- Automate policy enforcement between the platforms for rapid response.
- Enhance threat visibility and reduced mean time to detection & response.

Operationalize Intelligence

- Ingest threat intelligence using open industry standard interfaces.
- Augment network sensor effectiveness with third-party intelligence.
- Stream indicators of compromise to Cisco security sensors to automatically block or monitor suspicious activity.
- Correlate observations from network sensors and send alerts on incidents
- Improve your security posture based on enhanced security intelligence.