



Speed: faster detection and targeted mitigation reduces the mean time to respond



Focus: higher fidelity reduces false positives and ensures proper containment and actionable recommendations for remediation



Accuracy: continuous monitoring and investigation plus full packet capture illuminates security blind spots

Cisco Active Threat Analytics

A secure network is a powerful tool for achieving growth and stability. Safeguarding your business and customer data is critical for protecting your employees, customers, and reputation in an environment built on trust. Yet maintaining the integrity of your network is difficult to accomplish as you expand your capabilities. Furthermore, changing business models designed around mobility and cloud resources add new layers of intricacy to corporate networks. This creates a dynamic threat landscape that evolves quickly to find gaps in protection. An increasingly complex market for information security leads to fragmented security efforts. To innovate and disrupt, your business needs a balanced security solution capable of providing both proactive protection and adaptable expansion.

Overview

Cisco Active Threat Analytics (ATA) integrates deep expertise with cutting-edge technology, leading intelligence, and advanced analytics to detect and investigate threats with great speed, accuracy, and focus. Our expert investigators monitor customer networks 24x7 from our global network of state-of-the-art security operations centers, providing constant vigilance and in-depth analysis as a comprehensive security solution.

Features

	Enhanced	Premier
24x7 Threat Analysis and Incident Monitoring	✓	✓
Cisco Collective Security Intelligence Enrichment	✓	✓
Log and Telemetry Collection	✓	✓
Customer Portal	✓	✓
Metadata Extraction	✓	✓
Rules-Based Analytics	✓	✓
Advanced Analytics	✓	✓
High Touch Incident Support	✓	✓
Full Packet Capture		✓
Proactive Threat Hunting		✓
Security Device Management (Cisco and Third Party)	Add-on	Add-on

PEOPLE



24 x 7 Threat Analysis and Incident Monitoring: A global network of security operations centers with highly trained and certified experts who provide constant vigilance and on-demand analysis of your networks

High Touch Incident Support: A designated investigation manager with deep incident analysis and investigation skills who stays current with your environment and specific network goals in order to provide incident management focused on your specific needs

Proactive Threat Hunting: Activities involving seeking out malicious activity not identified by traditional alerting mechanisms. Hunting methods are documented in a living play-book that is continuously updated as threats and malicious campaigns evolve



INTELLIGENCE

Cisco Collective Security Intelligence Enrichment: Cisco proprietary and third party threat information used to provide situational and environment awareness of the latest threats



Email + Endpoints + Web + Networks + IPS + Devices

Active Threat Analytics leverages security knowledge from Cisco TALOS and Cisco Collective Security Intelligence to deliver global insights and context

TECHNOLOGY



Metadata Extraction: Drawing out and storing packet header and key payload information from network taps in order to provide additional data and context during incident investigation in order to increase incident fidelity

Full Packet Capture: Collecting and storing raw full packet information in order to conduct in-depth analysis and forensics that can confirm attack behavior and answer questions such as: who the true attacker was, what malicious activities were performed and what data was breached

Log and Telemetry Collection: Collecting telemetry from various network elements in order to identify relationships among the data, thereby enabling rapid analysis during incident investigation



ANALYTICS

Rule based Analytics: Analysis methods based on predetermined rule matching to detect known attack patterns or behaviors

Advanced Analytics: Machine learning techniques and proprietary algorithms used to detect malicious behavior based patterns and statistical anomalies. This is driven by an extensible big data architecture for processing, storing, and analyzing large amounts of unstructured security telemetry for greater visibility and context

www.cisco.com/go/securityservices