Cisco Classified Network Services: Advanced Threat Analytics for Government

Benefits

- Avoid the cost of new, specialized staff or equipment
- Focus on your strategic mission priorities
- Improve network availability and performance

Features

- Largest threat intelligence database outside the U.S. federal government
- Cross-industry partnership for threat detection and remediation
- Proactive safeguards against a wide range of advanced threats
- Rapid detection, characterization, and quarantine of threats
- Threat remnant search, identification, and remediation
- Security policy optimization
- Ongoing management and monitoring of security appliances

Today's information security landscape grows more complex and challenging every day. This is especially true for government and other public sector organizations that are regular targets of increasingly sophisticated cyber attacks. Locked in a race they can't win alone, many chief information security officers (CISOs) turn to managed security service providers to help safeguard their networks. This ensures that their security posture is always up to date, without the cost of building and staffing their own evolving capabilities. But for U.S. customers with special security, data protection, or classification requirements, there's only one place to turn.

Cisco Classified Network Services

Formed in response to the attacks of September 11, 2001, the Cisco Classified Network Services team delivers a portfolio of advanced services and support specially designed to meet the data protection and regulatory requirements of the U.S. public sector. Our new Managed Security Services provide the advanced threat prevention, detection, and mitigation capabilities you'd expect from Cisco. They are delivered from our highly secure and cleared U.S.-based facilities, staffed by U.S. citizens on U.S. soil–all at the appropriate security classifications for your organization.

Protection Before, During, and After an Attack

Our services combine industry-leading technology, expert security investigators, machine learning, and predictive analytics. We protect your network, endpoints, and sensitive data before, during, and after an attack. In addition to seeing that your security appliances are up to date, our analysts monitor your network to make sure that threats are not already hiding there.

Service components include:

- Classified remote managed services
- Data collection and analysis
- Data enrichment
- Device management
- Collective security intelligence
- Event correlation
- Full packet capture
- Hadoop/big data analytics
- Log analysis
- Machine learning
- NetFlow generation
- Protocol metadata extraction
- Rule-based analytics
- Security device management
- Sourcefire and Threat Grid technologies

During an attack, our advanced threat analytics solution rapidly detects and quarantines the threat. After the attack, we'll continue searching for remnants, analyze the root cause, and fix the vulnerability that enabled the attack to occur.

Active Threat Analytics for Government offers two tiers of service: Essentials and Premier.

Active Threat Analytics Essentials (ATAE-G)

This managed solution for 24x7 security monitoring, threat detection, analysis, and device management:

- Aggregates, monitors, analyzes, and reports data from a variety of network sources. It then identifies and contains threats and provides recommendations for remediation
- Is designed for customers seeking external security operations solutions. It manages and monitors customer-owned security products or basic security information and event management (SIEM) solutions
- Helps to improve your security strategy and threat coverage as your organization grows, so you can adopt disruptive technologies with confidence
- Identifies incidents quickly and provides actionable recommendations for remediating risks and security events

Active Threat Analytics Premier (ATAP-G)

This managed detection and response solution focuses on threat detection. It reduces the time to detect and the time to respond for advanced threats. Expert security investigators monitor network activity around the clock from a Cisco security operations center (SOC). The service:

- Analyzes a wide variety of telemetry available within your network instead of focusing on security devices
- Seeks out and uncovers threats, including those that may have bypassed perimeter defenses
- Detects advanced threats rapidly by combining analytics, people, intelligence, and technology
- Applies rule-based, statistical, machine learning, big data, and predictive analytics methods to detect anomalous activity and validate potential threats
- Hunts down unknown threats proactively
- Identifies incidents quickly, dramatically reducing the number of false positives
- Provides actionable recommendations for remediating risks and security events and confirms successful threat eradication
- Frees in-house security resources to focus on core initiatives

Trusted Partner of the People Who Trust No One

Classified Network Services began delivering high-touch technical support to the U.S. intelligence community and Department of Defense. Today, we offer a broad and expanding portfolio of high-touch technical support and managed services for the intelligence community, Department of Defense, civilian agencies, state and local government, and educational institutions. We can help support anyone with special security, data protection, or classification requirements.

Next Steps

For more information on Cisco Active Threat Analytics for Government, contact your Cisco account manager.