



Security Monitoring Service for Network-Based IDS

A Total Outsourced Security Solution for Your Business

Axxera, a premier managed security services provider, offers Security Monitoring Service for Network-Based IDSs. Axxera's Intrusion Detection solution provides comprehensive, outsourced monitoring for your organization's Network-Based IDSs, helping to detect and respond to the most sophisticated and malicious hacker attacks. The service is based on Central Intelligence's, Axxera's proprietary, next-generation security management and monitoring platform.

Central Intelligence offers the only true real-time monitoring service in the Managed Security Services industry to protect your company's mission-critical information assets.

Redefining Security Monitoring

Holistic approach

Unlike our competitors, Central Intelligence (CI) takes a holistic approach to security monitoring:

Aggregation of Data, the CI technology platform aggregates log data and alerts through VPN connections to your security devices, including the leading commercially available firewalls, network-based IDSs, host-based IDSs, and other security applications.

Data Normalization, the data is then normalized across a distributed database architecture at Security Operations Centers (SOCs) where Security Analysts see an uninterrupted view of network activity.

Data Mining and Correlation, the CI technology platform then mines the data for suspicious events using a variety of expert systems and anomaly-based advanced query sets, correlates them to other signs of attack, and presents them to Security Analysts.

• Achieve Real Time Security

- o Real-time security monitoring and actions that combat the most sophisticated and malicious hacker attacks
- o Real-time ticket information and status
- o Real-time security device log and alert data
- o Real-time analysis, commentary and recommendations by Security Analysts of Security Events

• Easily scale as per your organization's security requirements

• Secure communication between your IDS management console and the Axxera SOC.

• Store 1 GB of online log data storage per monitored host. Option to purchase additional online storage space on demand.

• Use Advanced Reporting features to view

- o Performance of security devices
- o Status of changes, upgrades, patches and other related system maintenance to the IDS management console
- o Details of malicious activity directed at the client site
- o Analysis and interpretation of significant events

• Need not share administrative access privileges to your IDS sensors with Axxera.

• Integrate with the market leading IDS vendors

- o Cisco Secure IDS Appliances
- o The Enterasys Dragon IDS Appliance and Enterasys Dragon Sensor on select Intel platforms
- o ISS RealSecure on select Nokia Appliances and Sun-manufactured Solaris platforms

Expert Analysis

Security Analysts in the SOCs interpret this data in real-time, using advanced query and analysis tools. Analysts then categorize attacks by analyzing malicious activity according to many different criteria, including source, destination, direction and distinguishing factors. They then prioritize the results according to a constantly evolving threat model, customized to your needs.

Fast, Professional Response

Working closely with the client, Security Analysts take action to help defend against intrusions before a crippling loss of information can occur.

Security Monitoring Service for Network-Based IDS Package

Security Monitoring Service for Network-Based IDS includes:

Gold

The Central Intelligence Gold Service level includes the following features:

- 24x7 Support center coverage
- Next-generation security monitoring
- Standard configuration management, emergency configuration management and security support available 24x7x365
- Monitoring and management of infrastructure firewalls 24x7x365
- Real-time automated proactive protection against attacks
- Predictive protection based on real-time global IP reputation (botnets) intelligence
- Forensic investigation of attacker for trending and analysis
- 4.5 GB of online log data storage per device with the option to purchase additional online storage
- Access to the Axxera central intelligence portal for real-time security analysis

Platinum

The Central Intelligence Platinum Service level includes the following features:

- 24x7 Support center coverage
- Next-generation security monitoring
- Standard configuration management, emergency configuration management and security support available 24x7x365
- Monitoring and management of infrastructure firewalls 24x7x365
- Real-time automated firewall proactive protection against attacks
- Predictive protection based on real-time global IP reputation intelligence
- Forensic investigation of attacker for trending and analysis
- Primary Security Analyst assigned to your account to analyze repetitive cyber attacks
- Proactive security incident management with root cause analysis
- Proactive security architecture problem review
- Proactive firewall patch management based on current exploits
- 30 standard policy changes per month and 12 emergency policy changes per year per device
- 4.5 GB of online log data storage per device with the option to purchase additional online storage
- Access to the Axxera Central Intelligence portal for real-time security analysis

Axxera Service Description	Gold	Platinum
→ 24x7 Support Center coverage	✓	✓
→ Event correlation and validation with Central Intelligence technology	✓	✓
→ Central Intelligence portal (system health, forensic investigation, security reporting)	✓	✓
→ Ticket tracking, communication, notification and escalation management	✓	✓
→ Operational Steps with validation and notification steps	✓	✓
→ Security Incident management (detection, classification, notification, recording, and closure)	✓	✓
→ Project management for installation	✓	✓
→ Provide real-time proactive security incident response	✓	✓
→ Provide real-time proactive security incident mitigation	✓	✓
→ Provide real-time forensic investigation on attacker for pattern analysis	✓	✓
→ Provide real-time Intelligence based Protection from bad reputation ip address	✓	✓
→ Provide real-time security incident dashboard graphs	✓	✓
→ Provide real-time security forensic investigation dashboard graphs	✓	✓
→ Monitor availability and response for firewall and IDS	✓	✓
→ Operational Steps with validation, troubleshooting, resolution and escalation steps	✓	✓
→ Incident resolution based on manual or automated procedures (blocking attacks, ports, or internal hosts)	✓	✓
→ Primary Security Analyst assigned to every account for incident investigation, diagnosis, and control		✓
→ Proactive security architecture problem identification		✓
→ Configuration identification, status, verification and audit		✓
→ Patch analysis and management		✓
→ Analyze repetitive critical cyber attacks and suggest corrective actions		✓
→ Update and manage IDS signatures for the latest attack patterns		✓
→ Analyze IDS signature updates and suggest classification changes		✓
→ Suggest changes to optimize security for new applications		✓
→ Analyze digital evidence and suggest forwarding to law enforcement		✓
→ Project management resource assigned for installation and on-going account maintenance		✓
→ Complete security problem management with incident root cause analysis, when appropriate		✓
→ Enterprise account management with complete understanding of architecture		✓
→ Change management coordination, review, risk assessment and justification		✓
→ Release management planning, deployment and acceptance		✓
→ Monitor ticket activity (24 hour report) and work to reduce false-positive and non-critical items		✓
→ Streamline resolution procedures to reduce resolution times of security tickets		✓
→ Configuration management (identification, planning, control and optimization)		✓
→ Perform changes to optimize firewall and IDS		✓
→ Install and apply fixes to security vulnerabilities according to industry standards		✓
→ Install latest anti-virus data files (any applicable software fees to be paid by customer)		✓

Service Enhancements

The following enhancements to the Central Intelligence Security Monitoring Service are available:

Security Help Desk

Central Intelligence offers 24x7x365 Security Help Desk support for your security devices. Clients can directly interface with the SOCs to address security device configuration and management issues through the client-designated single point of contact. The Central Intelligence Security Help Desk functions on a token redemption basis. One token provides for a single Security Help Desk support call of up to one hour in length.

Online Data Storage

All Managed and Monitored IDS packages include a fixed amount of online data storage per device. This amount of data storage represents 3 to 6 months of IDS alert data for a typical client. If a client's device generates a greater-than-average amount of data, Central Intelligence recommends that the client purchase additional online data storage. While all data is backed up on tape, once the amount of online data storage is exceeded, the oldest material is purged from the online data store. Clients can purchase additional storage at their discretion for a one-time setup fee and an incremental monthly fee.

Network Deployment

IDS monitoring requires deployment and management of an IDS Management Console on the customer's premises.

Central Intelligence-Managed IDS Management Console, Client Managed IDS Sensors

The Network-Based IDS Monitoring Service is designed to allow Central Intelligence to manage and monitor the IDS management console and monitor the Network-Based IDS sensors. The client installs and manages the Network-Based IDS sensors themselves. IDS console management allows Central Intelligence to update attack signatures via the console. The sensors report back to the management console and the management console reports the logging information to Central Intelligence securely through encrypted communication. The management of the Network-Based IDS sensors is left to the client.

Design Advantages

This design avoids the need for Central Intelligence to have root or administrative access to the Network-Based IDS sensors. The client maintains administrative control over the sensors and is responsible for patches and updates on those sensors. This combination of central and distributed management yields a highly scalable architecture while minimizing impact to the client's system performance.

Service Level Agreements

Central Intelligence provides industry-leading Service Level Agreements (SLAs) in support of the Security Monitoring Service for Network-Based IDS. The SLAs include uptime, service guarantees and penalties if guarantees are not met.

Additional Security Offerings

Central Intelligence offers a full suite of information security services to suit your needs. For additional information about Central Intelligence's Real-Time Managed Security Services, see the following documents:

- Managed and Monitored Firewall Service
- Host-Based IDS Monitoring Service
- Digital Evidence
- Predictive/Proactive Services
- Enterprise Security Reporting

Protect Your Network with the Central Intelligence Security Monitoring Service

With real-time information protection and industry-leading security professional services, Central Intelligence provides the most advanced information security available today. Find out how Central Intelligence's Security Monitoring Service can give your network the security you need.

About Axxera

Founded in 2007, Axxera is uniquely positioned to safeguard the electronic presence of today's corporations. Our founders pioneered the security industry by designing, and building security infrastructure worldwide. Axxera has helped secure hundreds of global organizations, and e-businesses.

Axxera Managed Security Services delivers the expertise, tools and infrastructure you need to secure your information assets from Internet attacks 24/7/365, often at a fraction of the cost of in-house security resources. Access to the Axxera Portal a secure Web-based management tool, provides a single interface to easily monitor the security of your overall infrastructure of managed and unmanaged security devices.

Axxera's proprietary technology platform enables detailed processing of every event on your network. Our processing model gives expert analysts at Axxera's Security Operations Centers the advanced tools they need to provide real-time analysis and protection.

Axxera Headquarters

2 Park Plaza	Phone: 949.502.4930
Suite 200	Fax: 949.861.9229
Irvine, CA. 92614	Email: info@axxera.com
	Web: www.axxera.com

Sales Offices

3109 Colebrook Lane	590 Madison Avenue
Dublin, CA. 94568	New York City, NY. 10022

Axxera International Center

1st Floor, Lakshmi Towers - B
Plot No. 17, Nagarjuna Hills
Hyderabad, Andhra Pradesh, India.
Pin - 500082