INFOSIGHT®

STAY AHEAD OF CYBERCRIMINALS. PARTNER WITH INFOSIGHT INC.

MANAGED SECURITY SERVICES

Effectively Monitor, Detect and Respond to Cyber Threats

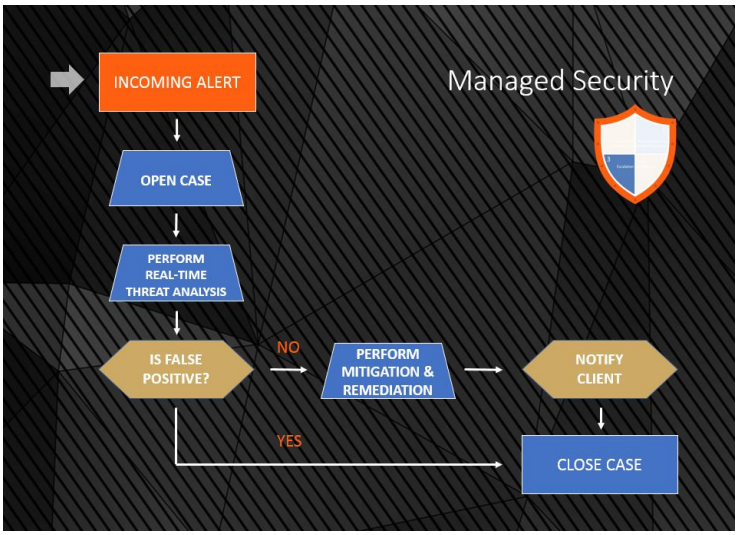
Research shows that Enterprise IT & Security departments only review less than 40% of security alerts. The is due to the fact that with hundreds of devices generating thousands of events every day, resources are stretched to the breaking point, and more resources are needed.

With our **co-managed approach to security monitoring**, we work in collaboration with IT staff. We monitor the most critical devices that require 24x7 attention, and in-house IT staff monitor internal devices and endpoints.

Our SOC leverages sound and repeatable processes to mitigate threats in a systematic approach. **Threats are analyzed in real time by InfoSight® Security Operations Center (SOC) analysts** and individual cases are created for all threat analysis performed. Device management and monitoring of *Firewalls, Intrusion Detections/Prevention Appliances, Host IPS, Active Directory and Endpoint Security* platforms can all be included in an affordable service offering. Additionally, incident-based reporting is included for all threats analyzed and mitigated during the month.

With cyber threats rising in both volume and sophistication, traditional in-house 8x5 security monitoring is good for compliance but ineffective against newer forms of cyber attacks. Due to the cost and complexity, building 24x7 in-house monitoring capabilities is not feasible for most organizations. We can help bridge the gap by bringing in complementary technologies and **services that deliver advanced security monitoring, detection, analytics, reporting and response services around the clock**.

With our systematic approach, we help organizations handle threats and vulnerabilities effectively, and alleviate the pressures they face related to cyber security threats, skills shortages and resource constraints.



Security & Infrastructure Monitoring services ensure **your network is safe 24 hours a day, 7 days a week**. Our managed security services fit into any budget with minimal upfront cost or capital outlay. Our consolidated real-time alerts and Security Compliance Summary Report help alleviate the painful process of executive management and board reporting required by numerous regulatory agencies.

InfoSight's Managed Information Security service enables efficient and cost-effective deployment of a broad defense and response strategy and is enhanced through faster provisioning and implementation of instant global updates.

Experience the difference with InfoSight® and see how quickly you can detect, prioritize and respond to threats. To get started, call or email us today.

MANAGED SECURITY SERVICES

24x7 Monitoring & Threat Analysis

The InfoSight SOC monitors and performs validated threat analysis 24x7 for the following events:

- Suspicious activity
- Unauthorized access attempts
- Malware
- Ransomware
- DDoS
- User events
- Port scans
- Logon attempts
- Researches & evidence/data collection
    - Log and timeline analysis
    - Media (e.g. file system) analysis
    - Data recovery
    - Artifact (malware) analysis

Alerting & Notification Options

Client notification can be customized to include multiple response scenarios.

- If threat analysis determines this is a false positive alert, there will be no notification.
- If threat analysis determines this is a “low or informational” alert, there will be no notification, but logging will occur.
- If threat analysis determines this is a “medium” alert, if requested, an email can be sent and logging will occur.
- If analysis determines this is a “high” alert, there will be an email or phone call made to the customer per the call escalation procedure and logging will occur.

Reporting

- **Alarms** - Reports on top alarms, top attackers, top attacked hosts, and top destination ports.
- **Assets** - Reports on assets, including asset properties, vulnerabilities, events, alarms, and raw logs for selected assets.
- **Compliance** - Reports on various compliance regulations, including FISMA, HIPAA, ISO 27001, PCI 2.0, PCI 3.0, PCI DSS 3.1, and SOX. These reports display information such as events, alarms, and asset, and map them to compliance requirements.
- **Raw Logs** - Reports on raw logs from different sources, such as firewalls, IDS/IPS systems, mail security devices, and anti-virus applications.
- **Security Events** - Reports on security events from different sources, such as events coming from firewalls, IDS/IPS systems, mail security devices, and anti-virus applications.
- **Security Operations** - Reports on security operations including tickets, top alarms, and top security events.
- **Custom Reports** - User customized reports including cloned reports and the custom security events or custom raw logs reports.

Incident Response & Mitigation

Once an incident is confirmed InfoSight will/may take the following actions:

- Prevent attackers from further damaging internal systems
- Ensure appropriate personnel are informed
- Remove compromised accounts
- Revoke compromised credential
- Remove malware/artifact left over by the attackers
- Restore from most recent clean backup
- Harden systems to prevent incident from re-occurring

Device Management

Our management platform allows us to optimize and administer your perimeter/internet security and provide detailed incident and access reporting. Below are some key elements that are delivered via our services.

- 24x7 Monitoring
- Incident response
- Multi-threat analysis
- Centralized signature & firmware updates
- Centralized logging
- Patch management, update and upgrade support
- Policy management
- Change management
- Device configuration backup
- Policy replication from device to group of devices
- Provisioning & update management
- Troubleshooting & diagnostic tools
- Attack intelligence

Threat Intelligence & Tools

- Vulnerability scanner
- Troubleshooting & diagnostic tools
- Attack intelligence

INFOSIGHT®
www.InfoSightInc.com