

InfoSight's Managed Extended Detection & Response

InfoSight's Managed Extended Detection & Response (XDR) Services can detect and respond to incidents 24x7x365 regardless of the source. Most organizations find it difficult to find the right staff to monitor and manage their own detection and response systems 24x7x365. InfoSight's XDR services consolidates your on-premise, hybrid and/or Cloud environments into one cohesive overview to monitor and manage vulnerabilities.

Overview - The Challenge

Having many different types of devices and data sources to monitor can put your organization at higher risk for a security incident. It can be overwhelming to monitor, analyze and respond to thousands of alerts each day. The threat analysis is a full-time job within itself and InfoSight wants to make it easier on you.

How We Solve It

InfoSight's Managed XDR services, we take your data sources where our experts to monitor them from a "single pane of glass" 24x7x365. Additionally, Security Orchestration and Automation (SOAR) helps automate and speed up incident response and recovery in the instance of a breach. When data sources are normalized and no threats are apparent, our SOC analyst conduct threat hunting exercises to proactive look for threats.

The Outcome

You can be at ease 24x7x365 that InfoSight's Managed XDR services are at work even when you're not! Our Managed XDR can make response times quicker, smarter, more efficient, and more cost effective. Leveraging our XDR resources will allow you to experience better cybersecurity and act quickly on any threats that come your way!

Key Service Features

- 24x7 Threat Monitoring
- Cyber Incident Response
- Proactive Threat Hunting
- Threat Intelligence
- Behavior Monitoring
- Policy Creation & Management
- Full Scope Services on Software, Firewall and/or Devices

InfoSight's Managed Extended Detection & Response

Service Descriptions



24x7 Threat Monitoring: Continuously scan inbound and outbound traffic across your environment



Cyber Incident Response: Evaluate alerts and data coming from network endpoints & help remediate and secure networks against future attacks



Threat Intelligence: Use custom tools to identify threats & thereby automate searches focused on thwarting



Behavior Monitoring: Looking for patterns and similarities in system's behavior along with suspicious activity



Policy Creation & Management: Withhold compliance and industry specific standards, ensure your organization is up to date on policies and procedures



Proactive Threat Hunting: Searching for indicators of compromise in an IT environment for the potential presence of malicious activity, usually before any alerts are generated by security devices or systems.

Why InfoSight

- 24x7x365 US-Based SOC/NOC
- SOC 2 Certified
- Complete MSSP Services that include Monitoring, Real-Time Threat Analysis, Mitigation/Remediation, Alerting, Reporting and Device Management
- Flexible pricing models that can be 24x7, 8x5, or off-peak 7pm to 7am only coverage
- 22+ years Regulatory Compliance experience (GLBA, PCI, HIPAA, NERC, AWWA, etc.)
- Certified Experts (CISSP, CISA, CEH, OSCP, AWS, AWWA, etc.)
- Managed Services for On-premise Data center, Cloud and Hybrid environments