



InfoSight®

Bringing the Future into Focus™

24x7 Managed Detection & Response

Overview - The Challenge

The most daunting challenge for information security teams today is the requirement for threat monitoring and incident response 24x7x365 with internal resources that are available only 8x5. Additionally, limited IT staffing and tight cybersecurity budgets make holistic information security seem impossible. All too often, teams are asked to extend beyond basic security operations and are requested to actively threat hunt and research zero-day attacks. This can easily exhaust personnel and create unnecessary risk for most organizations.

InfoSight's Security Operations Center (SOC) leverages sound and repeatable processes to mitigate threats in a systematic approach delivering superior outcomes...

We guarantee no alert fatigue EVER and protect companies operating within an on-premise Datacenter, the Cloud or Hybrid!

How We Do It

Our "Co-managed" approach provides security monitoring by becoming an extension of your IT team to monitor your most critical devices 24x7x365, while your team focuses on other assets. We offer a hosted SIEM in a layered security model where all assets can be viewed in a "single pane of glass" by both your IT team and ours at the same time. Additionally, we can also complement your existing SOC team with "off-peak only" (7pm to 7am) coverage to give you real 24x7 threat visibility.

We also focus on:

- **Being proactive by making recommendations to improve security**
- **Deploying active threat hunting options**
- **Proving full threat lifecycle services: Monitoring > Incident Response > Containment > Remediation > Reporting**
- **Leveraging your Cloud toolsets where possible to save budget resources**

Key Service Features

- **24x7 Device & Data Source Monitoring**
- **Threat Detection & Analysis**
- **Incident Response**
- **Mitigation & Remediation**
- **Notification & Alerting**
- **Reporting & Analytics**
- **Attack Intelligence**
- **Vulnerability Management**
- **Troubleshooting & Diagnostic Tools**













InfoSight®

Bringing the Future into Focus™

24x7 Managed Detection & Response

A Deeper Dive into InfoSight's Services

-  **24x7 Device & Data Source Monitoring** - InfoSight's SNOC monitors all your assets in the Data Center and the Cloud regardless of data source 24x7x365.
-  **Threat Detection & Analysis** - 24x7 InfoSight SNOC Analysts monitor your assets and applications against attack by tuning out the noise and acting on validated events.
-  **Incident Response** - InfoSight's SNOC Analysts can take action in your behalf to stop attacks, contain incidents and minimize risk.
-  **Mitigation & Remediation** - We mitigate attacks and can harden systems to prevent incidents from recurring.
-  **Notification & Alerting** - Our SNOC analysts can immediately notify you team using a variety of methods around the clock providing recommendations for corrective actions.
-  **Reporting of Analytics** - Our comprehensive reporting and detailed analytics ensure compliance with ease.
-  **Attack Intelligence** - We leverage intelligence resources and threat vectors that are gathered from global sources.
-  **Vulnerability Management** - Scanning your network regularly to make sure no unnecessary or unknown vulnerabilities exist and ensure all patches are in place.

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