InfoSight®
Bringing the Future into Focus®

305-828-1003
info@infosightinc.com
www.infosightinc.com

Security Operations Center as a Serivce (SOCaaS)

Overview - The Challenge

The challenge for many Security Operations (SecOps) teams today is the requirement for measurable outcomes that are driven by metrics based upon Key Performance Indicators (KPIs). Most Security Operations Centers (SOC) have metrics at some level, but not detailed enough to gain the visibility needed to reach an optimized state.

InfoSight's Security Operations Center as a Service (SOCaaS) detects cyber threats quickly and provides containment, incident response services to deliver SecOps at velocity 24x7x365. Our results are measurable at a granular level to facilitate an environment of continuous improvement and delivery optimization.

How We Do It

InfoSight's SOCaaS combines XDR, SOAR, AI along with Threat Intelligence and highly trained human actors to deliver a positive outcome. Our decades of experience-based knowledge provides what you need to guard against cyber threats and simplify risk management. We take a "co-managed" approach to SecOps that can raise your organization's cyber maturity level rapidly.

Do You Know Your Metric & Key Performance Indicators (KPI's)?

Mean Time to Detect
The time it takes your team to discover a potential security incident

Mean Time to Respond
The time it takes to control, remediate and/or eradicate a threat once it has been discovered

Alarm Time to Triage
Date/Time Alarm Inspection - Date/Time of Alarm Creation

Alarm Time to Qualify
Date/Time of Alarm Closure or Addition to Case - Date/Time of Alarm Creation

Mean Time to Contain
The average time taken by security teams to detect, acknowledge, and minimize the probability of further spread of an incident

Threat Time to Investigate
Date/Time of Case Closed or Elevated to Incident - Date/Time of Case Creation (MITRE)

Time to Mitigate
Date/Time Incident Mitigated - Date/Time Incident Determination (MITRE)

Time to Recover
Date/Time of Recovery from Incident - Date/Time of Incident Mitigation (MITRE)

Incident Time to Detect
Date/Time Threat Qualified for Investigation/Case Creation - Date/Time of Initial Indicator of Threat (MITRE)

Incident Time to Response
Date/Time of Incident Mitigation - Date/Time Initiated of Investigation (MITRE)

InfoSight
Bringing the Future into Focus
305-828-1003
info@infosightinc.com
www.infosightinc.com

Security Operations Center as a Serivce (SOCaaS)

A Deeper Dive into InfoSight's Services

24x7 Comprehensive Security Monitoring - InfoSight's SOC monitors all your assets in the Data Center and the Cloud regardless of data source 24x7x365.

Containment & Triage - InfoSight's SOC can contain an incident from spreading and perform triage to reduce the negative impact.

Incident Response & Triage - InfoSight's SOC can act on your behalf to stop attacks within the kill chain to minimize risk.

Mitigation & Remediation - We mitigate attacks and can harden systems to prevent incidents from recurring.

Notification & Alerting - Our SOC analysts can immediately notify your 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.

Threat Hunting - Ongoing hunts search for unknown vulnerabilities and threats that may already exist.

Why InfoSight

- 24x7x365 US-Based SOC
- SOC 2 Certified
- 25+ years of proven outcomes
- Offering full threat lifecycle services from Detection and Response to Mitigation and Remediation
- Flexible pricing models that can be 24x7, 8x5, or off-peak 7pm to 7am only coverage
- Solutions are Regulatory Compliance driven (GLBA, PCI, HIPAA, NERC, AWWA, etc.)
- Offering Services for the Data Center, Cloud and Hybrid environments
- Certified Experts (CISSP, CISA, CEH, OSCP, AWS, AWWA, etc.)