InfoSight®
www.infosightinc.com

SECURITY OPERATIONS CENTER AS A SERVICE (SoCaaS)

305-828-1003 info@infosightinc.com

Overview

InfoSight's Security Operations Center (SOC) operates as your own trusted cybersecurity team providing you with real time 24x7 threat monitoring, analysis, containment, triage, remediation, escalation, and reporting. All with no alert fatigue ever! Additionally, we can leverage your cloud native toolsets or ours, the choice is yours!

The Challenge

Attackers work 24x7, while most organizations IT departments don't... Additionally, tight cybersecurity budgets and the effort required to analyze all security events can be exhausting leading to employee fatigue and turnover. Recruiting and retaining cybersecurity analysts is probably the most challenging it has been in decades. Your team should be focused on more strategic objectives that support business goals and not fighting cybersecurity fires.

How We Deliver It

InfoSight brings a co-managed approach to security monitoring by becoming an extension to your IT team to monitor your most critical assets and data sources 24x7x365. We deliver enterprise threat management through a layered security model where all assets in the datacenter or the cloud can be viewed in a "single pane of glass" by both your IT team and our SOC simultaneously. This allows your team to focus on day-to-day concerns thereby improving overall efficiency and operational effectiveness.

We Solve Five Major Issues:

Alert Fatigue

With so many data sources and devices, along with the growing threat landscape all creating thousands or even millions of alerts per second, alert fatigue will set in even for a 24x7 shop.

Tool Overload

Adding tools for specific components across the data center and the cloud leads to tool overload, and in many cases many of the tools are not fully implemented.

Untuned Data Sources

Data Sources must be tuned to eliminate information, unnecessary and false positive events/alarms. Doing this allows for only actionable alerts and easier visibility to spot trends. And it saves money when on ingestion-based cloud platforms!

Blind Spots

We architect a security environment that eliminates blind spots!

Cloud Services Spend

Ingestion-based pricing models can get out of control fast! We can assist in saving significant budget dollars on your cloud spend.

Bringing the Future into Focus

www.infosightinc.com

InfoSight®
www.infosightinc.com

SECURITY OPERATIONS CENTER AS A SERVICE (SoCaaS)

We accomplish our tasks by:

Monitoring & Threat Detection – We provide 24x7x365 continuous and proactive monitoring of your environment.

Incident Response & Remediation – Our Analysts adhere to the SLA's runbooks to remediate issues or to triage and escalate to your team.

Incident/Problem Management – We own incident/problem management from creation to closure.

Ownership of runbook maintenance – We will work closely with your team to leverage any existing runbook collaterals and IT Teams knowledge as we build, manage, and maintain the runbook.

Monthly Reporting – We provide monthly incident-based reporting.

Ongoing monitoring enhancements – We are responsible for managing the monitoring tools to ensure tools remain updated, tuned, and deliver the monitoring outputs desired by the client.

Incident Case Management – Case Management Tickets are automatically created by the monitoring tools or manually created by authorized InfoSight, Client or Client staff to track incident investigations to closure.

Global Threat Intelligence – Threat Intelligence helps gain insights into real threats in your attack surface, helping you make more informed security decisions.

Incident Communications – We alert the client of incidents via escalation protocols based on environment and the severity of the incident. All incident creation, documentation and closure will be maintained in InfoSight's ITSM via automated or manual updates.

24x7 MDR & SOCaaS

	SMB	Professional	Enterprise	What Makes Us Different?
Security Operations Center (SOC) Services				
24x7x365 SOC Threat Monitoring, Detection and Response (MDR) -US-based SOC2 Certified	X	X	X	
Fully Managed Cloud-based SIEM/XDR	X	X	X	
US-based SOC 2 Type 2 Certified Security Operations Center	X	X	X	
24x7x365 Endpoint Detection & Response (EDR)	X	X	X	
Complete Run/Playbook Maintenance	X	X	X	✓
24x7x365 Managed Network Intrusion Detection Systems (NIDS)	ADD-ON	X	X	
Incident Based Monthly Reporting including Executive Reporting for the C-Suite	X	X	X	
Internal Vulnerability Scanning[1]	X	X	X	
Proactive Threat Hunting	ADD-ON	X	X	
Active Directory Auditing/Alerting	ADD-ON	ADD-ON	X	
Global Threat Intelligence Feed	X	X	X	
Dark Web Scanning	ADD-ON	X	X	
API & Application Security Monitoring	ADD-ON	ADD-ON	X	✓
Per device or consumption-based pricing	X	X	X	✓
Customized Incident Response - offering full "Mitigation and Remediation", or just "Monitoring, Triage &/or Containment" and Escalation to your team.	ADD-ON	X	X	✓
Monitoring of OT Industrial Control assets	ADD-ON	ADD-ON	ADD-ON	✓
Network Operations Center (NOC) Services				
Includes 24x7 NOC Performance Monitoring & Alerting for Servers Network/Cloud Assets and Services for Windows/Linux/Azure/AWS environments. Also includes Response and Remediation , or just Monitoring and Escalation to your team.	ADD-ON	X	X	✓
Endpoint Patch & Vulnerability Management - Management of the approval and deployment of supported Endpoint Operating System "Security patch(s)", "Critical Update(s)" and supported "Third-party" application patches.	ADD-ON	ADD-ON	X	✓
CISO & Risk Management Services				
$1mil Cyber Insurance[2]	ADD-ON	ADD-ON	X	✓
Mitigator Vulnerability & Threat Manager™	ADD-ON	X	X	✓
Virtual Information Security Officer (vISO) Program access on scheduled cadences	ADD-ON	ADD-ON	X	✓
Cyber Controls Assessment	ADD-ON	ADD-ON	X	✓
Incident Response Paybook	X	X	X	✓
Security Awareness Services				
Employee Security Awareness Training and Learning Management System (LMS) Access	ADD-ON	ADD-ON	X	
Full featured Email Phishing Platform with prebuilt templates	ADD-ON	X	X	
Online Banking Customer Cybersecurity Awareness Training Program (CSAP)3	ADD-ON	ADD-ON	X	✓
Operational & Technology				
Leverage your XDR/SIEM or ours - the choice is yours!	N/A	X	X	✓
Co-managed delivery	X	X	X	✓
Full-access to our SIEM/XDR as a tool for your team	X	X	X	
Cloud Spend Evaluation & Recommendations	ADD-ON	X	X	✓
Data Source tuning	ADD-ON	X	X	✓
XDR & SIEM Solutions Agnostic Delivery (MS Sentinel, Splunk, USM, etc.)	N/A	X	X	✓
Offering 7 PM to 7 AM "off-peak" and weekend-only monitoring to provide savings where staffing resources overlap	X	X	X	✓
Service Delivery Manager	X	X	X	
15min response SLA	X	X	X	✓

1 SIEM/XDR Platform dependent *2 Subject to Application approval* *3 For Financial Institutions only*