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.

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.

InfoSight®
www.infosightinc.com

SECURITY OPERATIONS CENTER AS A SERVICE (SoCaaS)

Why InfoSight® ?

24x7x365 Staffed SOC

100% US based SOC 2 Certified Operations Center

Only US-based W2 employees

Providing both Security and Network Infrastructure Support

Support for Cloud, Datacenter or Hybrid networks

Monitoring of Applications, DBs, Security, Infrastructure, Server or Serverless

Offering Device-based or consumption-based pricing models

24x7 or off-peak 7pm-7am coverage available

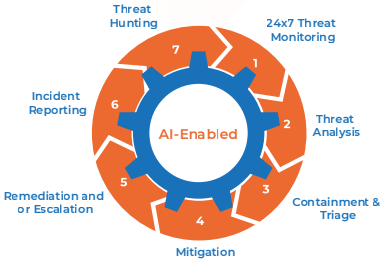
Federally regulated and critical infrastructure client experience

Cyber liability insurance coverage

24+ years of successful outcomes

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 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.

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.

Monthly Reporting – We provide monthly incident-based reporting.