Netsurion™
Powering Secure and Agile Networks

EventTracker SIEMphonic

Overview

Keeping up with cyber threats and compliance requirements are tough tasks for any IT team, large or small. Every day you may experience a flood of alert warnings, emails, advisories, and threat data – plus you never have enough time, staff, or budget.

You don't have to do this alone – get EventTracker SIEMphonic and get back to business.

EventTracker SIEMphonic is a Co-Managed SIEM that functions as an extension of your team to strengthen defenses, respond in real-time, control costs, and optimize your teams' abilities. Also known as SOC-as-a-Service, our Co-Managed SIEM is built on our own award-winning platform and has been on the Gartner Magic Quadrant for SIEM for 11 consecutive years.

Whether on-premises or in the cloud, our 24/7 intelligence-driven ISO/IEC 27001-certified Security Operations Center (SOC) provides expertise so you can focus on the unique requirements of your organization.

- **Protect against cyber threats:** Realize faster and more accurate analysis, detection, and response to threats and vulnerabilities
- **Increase operational efficiency:** Have more time to focus on your core business without having to divert resources to SIEM
- **Simplify compliance:** Spend less time with on-site auditors and simplify the audit process with analyst log review, documentation of findings, and response to coverage or process deficiencies
- **Cut costs:** Reduce the internal costs to deploy, configure, and operate SIEM technologies as our experts will RUN and WATCH it for you

Features/Options

Components of these services can be customized:

- System Administration
- Daily/Weekly Incident Review
- Daily/Weekly Log Review
- Incident Investigation/Forensics
- Anomalous Login Detection and Blocking
- Vulnerability Assessment/Scanning Service (VAS)
- Intrusion Detection System (IDS)
- Honeynet
- Network Traffic Analysis
- 24/7 Monitoring, Escalation, and Notification

How it Works

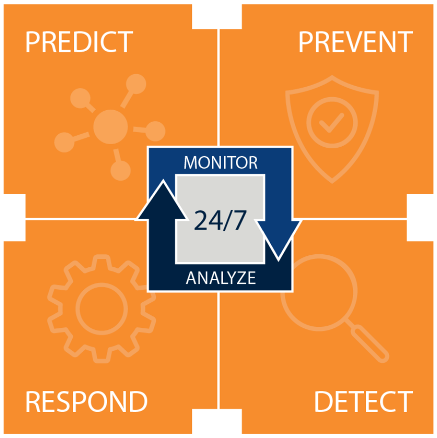
Step 1: EventTracker Security Center SIEM software is installed either on premises, hosted, co-located, or in the cloud (Amazon, Google, Azure, etc.), and configured to monitor your assets. The implementation is customized to your specific environment and requirements. We manage every engagement focused on your desired outcomes.

Step 2: Once the installation phase is complete, our dedicated team of SOC analysts securely access the EventTracker applications and servers. No other access to other IT assets is required or expected, and no data leaves your network.

Step 3: We configure, tune, filter, and refine alert rules, reports, dashboards, and analytics based on your environment and priorities on an ongoing basis. Incident response procedures and your specific operational runbook frameworks cover when, why, who, and how our SOC staff should escalate incidents and remediation recommendations to your attention.

Step 4: Our SOC staff monitors your IT assets on a 24/7 basis, and provides daily or weekly summaries called Critical Observation Reports, escalating incidents per procedure and maintaining the EventTracker installation in top-working order. Our SOC staff is also available to answer questions and provide support for incident review and forensics, audit assistance, etc.

Step 5: We conduct regular assessments and planning sessions of the service deliverables with key members of your team through Executive Dashboard Reviews. We continuously improve the process based on your objectives and stay abreast of any changes in your environment.



Administration Service

Components of these services are customized to meet your requirements and options include:

- EventTracker software updates, service and knowledge packs, new release upgrades, and licensing key installation
- System health checks, storage projections, and log volume/performance analysis
- Change analysis in log collection for new systems and non-reporting systems
- EventTracker administration and configuration for users, standardized reports, dashboards, and alerts
- Generate weekly system status report
- Confirm external/third party integrations are functioning normally: threat intelligence feeds, IDS, Honeynet, and VAS

Analysis Service (Daily, Weekly, or 24/7)

The SOC provides expert security analytics including:

- Analysis of your alerts, incidents, anomalies, and reports
- Annotation, casebook entries, and escalation
- Delivery of Core Observation Report (COR) management summary
- Delivery of monthly Executive Dashboard management summary

Compliance Support

EventTracker SIEMphonic includes frameworks for compliance needs such as PCI DSS, HIPAA, GDPR, NIST, ISO-27001, etc., enabling you to:

- Review summary reports for relevant frameworks
- Review detailed reports as necessary
- Annotate findings as needed
- Maintain auditor-ready artifacts – always be ready for an IT audit

Advanced Customization

The SOC can also provide expert services:

- Advanced correlation and behavior analysis configuration
- Custom alerts
- Custom scripts and dashboards
- Configuring FLEX reports and top-level summaries

Vulnerability Assessment Service

The SOC staff will work with clients to identify and group assets, schedule scanning, and attempt to detect vulnerabilities on a monthly or quarterly basis. Detailed results, including remediation recommendations are integrated into the EventTracker Reports Dashboard for review. Common Vulnerability Scoring System (CVSS) results are integrated with EventTracker Incidents (alerts) for asset prioritization. Trend reports showing new, remediated, or unchanged vulnerabilities are provided. For dynamic networks, discovery scans precede vulnerability scans. Both authenticated and unauthenticated scans are supported. The service includes the maintenance of the scanner system for signature, engine, and platform updates.

Intrusion Detection System

Our SOC staff will install Snort Community Edition, configure, tune, and maintain available rules to monitor your network. Alerts are integrated into the EventTracker Incidents Module which can launch notifications (e.g. email) and/or auto-remediation actions. The service includes the maintenance of Snort for signature, engine, and platform updates.

Honeynet

Comprised of multiple virtualized decoys strategically scattered throughout the network to lure bad actors, Honeynets can provide intelligence about malicious activity against the network. EventTracker Honeynet is integrated with the EventTracker Console and alerts network administrators of suspicious activity, and provides them with situational awareness view of their network.

Recognized for 11 consecutive years on the Gartner Magic Quadrant for SIEM.

Netsurion™
Powering Secure and Agile Networks

netsurion.com/eventtracker