SIEMPHONIC

Enterprise

EventTracker SIEMphonic Enterprise

Overview

SIEMphonic Enterprise is our industry-leading co-managed SIEM that optimizes your ability to predict, prevent, detect and response to security threats while streamlining regulatory compliance. This comprehensive and scalable SIEM-as-a-Service is based on Security Center, our award-winning SIEM platform, which also encompasses other critical capabilities such as intrusion detection (IDS), vulnerability scanning (VAS), threat intelligence, user and entity behavior analsysis (UEBA), and honeynet deception technology. Whether implemented on-premises or in the cloud, our 24/7 intelligence-driven SOC provides administration, analysis, compliance, and tuning expertise so you can focus on the unique requirements of your organization.

With the SIEMphonic Enterprise service, you are able to choose what functions you would like EventTracker to manage: Administration, Analysis, Compliance, Tuning, IDS and VAS options. These services will:

- **Detect and remediate 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

Features/Options

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

- System Administration
- Daily/Weekly Incident Review
- Daily/Weekly Log Review
- Incident Investigation/Forensics
- Audit Assistance
- Vulnerability Assessment/Scanning Service (VAS)
- Intrusion Detection System (IDS)
- HoneyNet
- Network Traffic Analysis
- 24x7 Monitoring, Escalation and Notification

How it Works

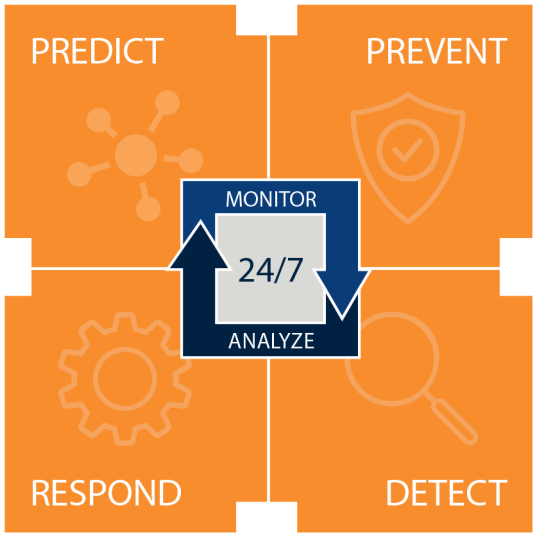
Step 1: EventTracker is installed, either on your premises or in a tier-1 data center, Amazon or Azure and configured to monitor your assets. The implementation is customized to your specific environment and requirements.

Step 2: Once the installation is complete, staff at the EventTracker Security Operations Center (SOC) are granted limited, audited access to only the EventTracker application and server. No other access to other IT assets is required or expected.

Step 3: We work with you to configure, tune, filter and refine alert rules, reports, dashboards and analytics. Incident response procedures and your operational runbook frameworks cover when, why, who and how the SOC staff should escalate incidents to your attention.

Step 4: SOC staff begin monitoring your IT assets on a 24/7 basis, and provide daily or weekly log reviews, escalating incidents per procedure and maintaining the EventTracker installation in top working order. SOC staff is also available to answer ad-hoc questions and provide support for incident review, audit assistance, etc.

Step 5: We conduct regular assessments and executive dashboard reviews of the service deliverables with key members of your team to continuously improve the process and stay abreast of any changes to your environment.



SIEMPHONIC

Enterprise

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, licensing key installation
- System health checks, storage projections and log volume/performance analysis
- Analyze changes 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, VAS

Analysis Service (Daily/Weekly)

The SOC provides expert security analytics including:

- Analysis of your alerts, incidents, anomalies and reports
- Annotation, logbook entries and escalation
- Delivery of Critical Observations Report management summary
- Delivery of monthly or quarterly management executive dashboard

Compliance Service

The SOC provides compliance report annotation and audit support services including:

- Review top level 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"

Tuning Service

The SOC provides on-demand advanced expert services on an annual retainer

- Advanced correlation and behavior analysis configuration
- Custom alerts
- Custom scripts
- 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 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. RHEL Virtual Machine platform.

Intrusion Detection System

The 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. e-mail) and/or auto-remediation actions.

The service includes the maintenance of Snort for signature, engine and platform updates. RHEL Virtual Machine platform.

24x7 Managed Service

The SOC staff will monitor alerts, notify and escalate via emails, texts and phone calls to designated client staff.

About EventTracker EventTracker delivers business critical solutions that transform high-volume cryptic log data into actionable, prioritized intelligence that will fundamentally change your perception of the utility, value and organizational potential inherent in log files. Our leading solutions offer Security Information and Event Management (SIEM), real-time Log Management, and powerful Change and Configuration Management to optimize IT operations, detect and deter costly security breaches, and comply with multiple regulatory mandates.