SIEMPHONIC
Essentials
powered by EventTracker

SIEMphonic Essentials

Overview

SIEMphonic Essentials is based on the award-winning EventTracker platform, scaled and simplified to meet the security and compliance needs of small- and medium-size businesses (SMBs) in a single, affordable solution. We designed SIEMphonic Essentials to address the growing need for affordable, 24/7 threat monitoring to combat the evolving threat landscape, and help businesses meet multiple compliance regulations.

Some benefits include:

- **Detect and Remediate Threats:** Realize faster detection and response to threats that evade anti-virus and firewalls
- **Increase Operational Efficiency:** Have more time to focus on your core business without having to divert resources to SIEM
- **Simplified Compliance:** Improve your audit process by providing pre-defined reports on compliance regulations PCI DSS, HIPAA, and NIST 800-171.
- **Cut Costs:** Reduce the costs to deploy, configure, and operate enterprise-level SIEM technologies

Features/Options

Components of this service include:

- 24/7/365 monitoring and alerting
- Automatic threat remediation
- Daily security/compliance reporting
- Pre-defined alerts
- Pre-defined compliance reports
- Host-based Intrusion Detection System

Technical Specifications

- Windows 7 and higher
- Windows 2008 R2, 2012 R2, 2016
- EmbeddedPOSReady 2009
- Firewalls: Cisco ASA, Cisco Meraki, CyberOAM, FortiGate, MikroTik, SonicWALL, SOPHOS XG, Untangle, WatchGuard

Log Sources

- Windows
- Active Directory
- Firewall
- O365

HOW ESSENTIALS WORKS

With a light-weight sensor deployed to your critical endpoints, EventTracker alerts you immediately of any anomalies or suspicious activities. SIEMphonic Essentials listens to you as you tune the solution to what events you consider threats, as well as those you do not, allowing you to also automate responses to specific events.

SIEMPHONIC

Essentials

powered by EventTracker

Wide Range of Real-Time Incident Alerts

SIEMphonic Essentials uses advanced log analysis to trigger a number of out-of-the box alerts that notify your organization at the first sign of a security, compliance, or operational issue. Alerts are delivered in real-time, and depending upon the criticality, some will generate an automatic remediation response to make sure that your environment is immediately protected from advanced cyber threats. If the alert does not require automatic remediation, EventTracker will provide remediation recommendations. A sample of available alerts are below.

Security Alerts Triggering Remediation

- Terminate processes with Blacklisted Hash
- Terminate connections to bad reputed IPs
- Critical potential breach by unknown process from low reputation IP
- Critical potential breach from low reputation IP
- Unsafe MD5 hash detected

Firewall Events

- Virus detected
- Attack detected
- Configuration changed
- Authentication failed
- IDS intrusion detected
- URL filtered
- VPN authentication success

Abnormal User Behavior

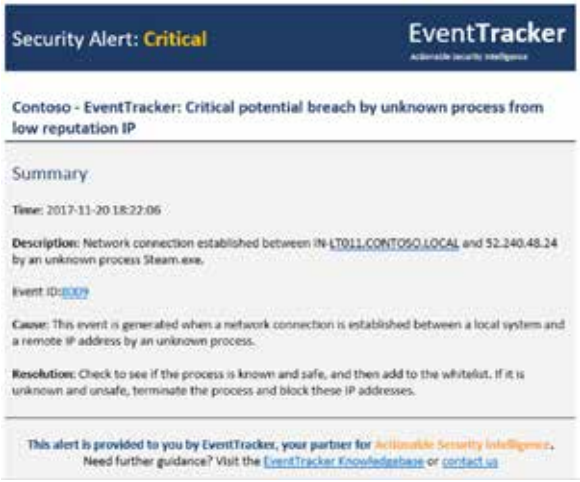
- Administrative logon success
- New Windows User Location Affinity Activity
- Excessive logon failures due to bad password/user name
- Removable media (i.e. USB drive) inserted
- User account disabled
- User added or deleted
- Users added to Domain Admin or local Admin group
- Users password set to never expire
- Windows audit log cleared
- Excessive logon (id 4625) failures from an IP Address

Operational Events

- Critical service is not running
- Disk space is critically low
- A process consuming high CPU
- A system consuming high CPU
- A process is taking too much memory
- A system is taking too much memory

Abnormal Process or System Behavior

- A new TCP port started listening
- New Windows Software Install Activity



Clearly defined and actionable critical incident alerts.

EventTracker, a Netsurion company, empowers organizations to successfully predict, prevent, detect, and respond to cybersecurity threats. The EventTracker SIEM platform unifies machine learning, behavior analytics, and security orchestration, and has been recognized for 10 straight years by Gartner on the Magic Quadrant for SIEM. EventTracker offers a suite of SIEM solutions built for any size company or budget. More and more organizations are seeking SIEM-as-a-Service to realize optimal security results. SIEMphonic builds on the EventTracker platform by delivering a Co-Managed SIEM service complete with 24/7 global Security Operations Center (SOC), powered by threat intelligence.

Recognized for 10 consecutive years on the Gartner Magic Quadrant for SIEM.

www.eventtracker.com

Netsurion EventTracker
Actionable Security Intelligence