EventTracker
Actionable Security Intelligence

SIEMPHONIC
Essentials
powered by EventTracker

EventTracker SIEMphonic Essentials

Overview

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

Here are some of the benefits you will realize with SIEMphonic Essentials:

- **Detect and Remediate Threats:** Realize faster detection and response to threats that evade anti-virus and firewalls with the help of our SOC
- **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 a variety of compliance regulations (HIPAA, PCI DSS, SOX 404, FISMA, and more)
- **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 (IDS)

Technical Specifications

- Windows 7 and higher
- Windows 2008 R2, 2012 R2, 2016
- EmbeddedPOSReady 2009
- Firewalls: Cisco, Juniper, WatchGuard, Fortigate, Palo Alto, Checkpoint, Sophos, Meraki, McAfee, SonicWall

HOW IT 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.

Monitor Systems and User Behavior

- User behavior and activity analysis
- Event correlation
- 400-day searchable log retention
- Monitor file and app changes
- Threat dashboard

Detect Cyber Attacks Instantly

- Removable media inserts and file copying
- Group security policy changes
- Abnormal network or system activity
- Abnormal user activity or remote access
- Application installs

Automate Responses

- Terminate processes with Blacklisted Hash
- Terminate connections to bad reputed IPs
- Propagate action across all endpoints

HAYCOR
COMPUTER SOLUTIONS INC.

Haycor Computer Solutions Inc.
info@haycorsolutions.ca
www.haycorsolutions.ca

EventTracker
Actionable Security Intelligence

SIEMPHONIC
Essentials
powered by EventTracker

Wide Range of Real-Time Incident Alerts

EventTracker 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

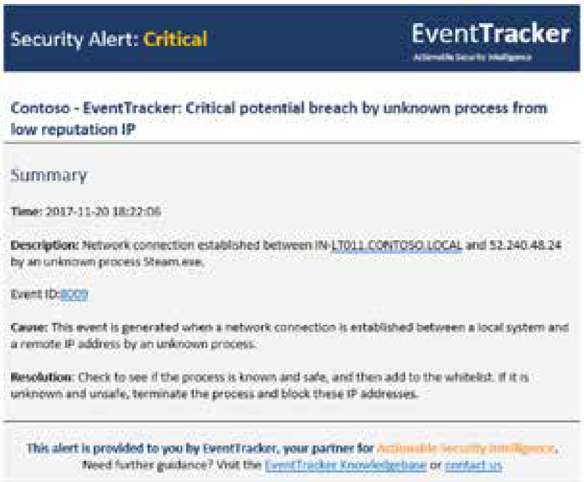
- Administrative logon success
- New Windows User Location Affinity Activity
- Excessive logon failures due to bad password/ username
- Removable media (i.e. USB drive) inserted
- User account disabled
- User added or deleted
- Users added to Domain Admin or local Admin group
- Users password set to 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
- Out of ordinary IP Address Activity
- Out of ordinary Windows process activity



Security Alert: Critical

EventTracker
Actionable Security Intelligence

Contoso - EventTracker: Critical potential breach by unknown process from low reputation IP

Summary

Time: 2017-11-20 18:22:06

Description: Network connection established between IN-LT011.CONTOSO.LOCAL and 52.240.48.24 by an unknown process Steam.exe.

Event ID:8009

Cause: This event is generated when a network connection is established between a local system and a remote IP address by an unknown process.

Resolution: Check to see if the process is known and safe, and then add to the whitelist. If it is unknown and unsafe, terminate the process and block these IP addresses.

This alert is provided to you by EventTracker, your partner for Actionable Security Intelligence.
Need further guidance? Visit the EventTracker Knowledgebase or contact us

Clearly defined and actionable critical incident alerts

EventTracker, a Netsurion company, 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.

HAYCOR
COMPUTER SOLUTIONS INC.

Haycor Computer Solutions Inc.
info@haycorsolutions.ca
www.haycorsolutions.ca