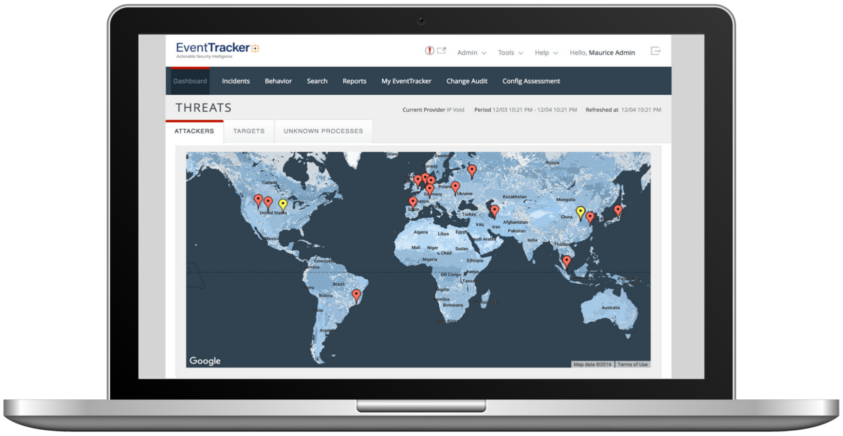
EventTracker
Actionable Security Intelligence

EventTracker Security Center

One platform for all critical SIEM capabilities



Current Provider IP Void   Period 12/03 10:21 PM - 12/04 10:21 PM   Refreshed at 12/04 10:21 PM

Overview

Security Center is a comprehensive platform for real-time security monitoring, advanced threat detection and response, and audit-ready compliance. It identifies security threats, malware, unusual behavior and suspicious network traffic and notifies you when you're under attack.

Today's network defenses are routinely penetrated as the threatscape is constantly evolving to evade detection. Firewalls, anti- virus and IDS/IPS are essential, but are not enough to prevent cyber-attacks. Further, keeping up with security at scale, 24x7, across all assets, is more than a full-time job. Whether your organization has 25 servers or 2,500, EventTracker Security Center can help by improving log analysis, awareness, detection and incident response across all your servers, workstations, network devices, locations and teams.

EventTracker Security Center ingests millions of security and log events and processes them through advanced analytics to detect and notify when changes in patterns across users and systems occur, based on unusual behavior and out-of-ordinary access. EventTracker Security Center monitors for anomalies and suspicious network activities and provides built-in response rules to block or terminate harmful activities. Integrated threat intelligence provides curated data on bad actors, locations and IP addresses, both locally and across the globe, to answer who, when and where. All your data is organized and presented in the form of dashboards and reports within EventTracker, and archived to a compressed electronic vault to meet regulatory retention requirements.

Pricing

EventTracker Security Center is available by annual or perpetual license, with pricing to fit any budget.

Monitor:

- Antivirus
- Applications
- Behavior
- CPU/Disk/Memory Threshold
- Custom applications
- Databases
- File/folder access
- IDS/IPS
- Mobile devices
- Network devices
- Pre-defined policy templates
- Routers
- Servers/Workstations
- USB and CD/DVD
- Virtual infrastructure

Supported Log File Formats:

- Windows EVT/EVTX
- SYSLOG (TCP/UDP)
- SNMP V1/V2/V3
- CHECKPOINT OPSEC LEA
- VMWARE API
- VULNERABILITY SCANNERS
- XML
- IIS/IIS W3C/ IIS MSID
- TEXT FILE
- J SON
- NETFLOW V5, V9

Features

Automatic Remediation

The EventTracker family offers automatic remediation capabilities that users can configure using scripting, Powershell, Visual Basic, and others. Based on correlated events that meet serious or critical thresholds, or that occur after hours, EventTracker Security Center can be set to take immediate, predefined action.

Behavior Analysis and Correlation

Behavior Analysis enables you to quickly detect and address changes in system and user behaviors. Automatic baseline learning or flexible rules definitions determine your thresholds for alerting on anomalies in your infrastructure. Real-time processing and correlation give you the complete picture of what's new and different.

Endpoint Threat Detection and Response

EventTracker Security Center provides enhanced end-point monitoring and security, generating an event when USB/DVD/CD removable media is inserted including the username and device serial number; all file transfers to USB devices are recorded; USB devices can be automatically disabled based on serial number.

Threat Intelligence

EventTracker easily incorporates threat intelligence from STIX/TAXII-compliant providers, commercial and open source feeds, and internal honeypots into the EventTracker Threat Center - an integration platform for commercial and open source threat feeds. The platform uses this data to reduce false-positives, detect hidden threats and prioritize your most concerning alarms.

Incident Handler's Logbook

Electronic Logbook, based on SANS Incident Handlers Guidebook, records incidents, reports, and changes with valuable context, and gives users the ability to flag interesting incidents, reports, configuration assessment or change audits that enable IT teams to escalate efficiently.

Reporting

EventTracker Security Center provides powerful and comprehensive analytics and reporting engines to allow users to easily and quickly search, analyze and report on all event data either in real-time, for compliance purposes or as part of a post-incident forensics process. EventTracker Security Center stores events in their original state and the complete contents are accessible to the user.

Real-Time Alerting

EventTracker Security Center's alerting capability enables the user to generate alerts when critical events occur such as security breaches or performance problems. The EventTracker Security Center Alert Console provides a web-based centralized user interface to define and view all alerts. Alerts can be prioritized and ordered via a user- configurable risk-scoring algorithm so important alerts are always given the attention they require.

Search and Forensic Analysis

EventTracker Security Center offers the most comprehensive and flexible search options in the SIEM/Log Management industry. Period! We have spent more than 10 years working with hundreds of security and sys admin users to address numerous log search scenarios and use cases.

Options Available

There are options for modules including Change Audit - File Integrity Monitoring, Configuration Assessment/ SCAP, FIPS 140-2 compliant data transmission, and the availability to have multiple collection points and collection masters. EventTracker HoneyNet is also available as part of its managed security service and enables an enterprise to add a deception network layer to its cybersecurity defenses.

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.