EventTracker Network Security

EventTracker Network Security is the most comprehensive solution for businesses that need to meet critical compliance requirements. It utilizes industry-leading SIEM technology to collect, analyze and correlate information from network devices, endpoint logs and threat intelligence feeds. This enables you to provide alerting, reporting and log retention to SMBs that need to meet common regulatory requirements.

Key Features

THREAT INTELLIGENCE SUPPORT

The SOC works together with you to identify threats on servers and firewalls, while supporting compliance guidelines through a fully integrated range of response capabilities available 24x7 - keeping client data and environments safe.

ULTIMATE SIEM TECHNOLOGY

Network Security powered by EventTracker, an established SIEM platform present on the Gartner Magic Quadrant for 10 consecutive years. Continuum combined this innovative technology, with our experienced SOC, delivering the best solution for SMBs that need to meet compliance requirements while keeping their businesses secure, in a cost-effective way.

MONITORING AND ANALYSIS

Monitor key log files to identify and correlate events that could be malicious, while providing additional security and adherence to regulatory guidelines.

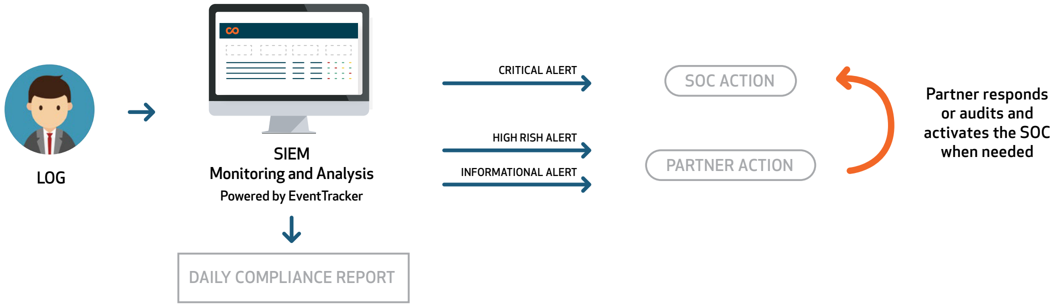
COMPLIANCE REPORTING

Generate daily reports and threat analysis outlines for three regulatory standards: PCI, HIPAA and NIST 800.

Working Together With The SOC

Alerts are designed to meet the continuous log monitoring requirement specified by PCI, HIPAA and NIST 800 compliance regimes. Those alerts are divided into two classes: SOC Action Alerts and Partner Action Alerts. The SOC has complimentary responsibilities with you to guarantee the ideal efficiency of the solution (see table below for more details on the alert description).

ALERT TYPE	DESCRIPTION	SOC ACTION	PARTNER ACTION
CRITICAL	Actions that can be commonly indicative of an active attack should be investigated and responded to immediately	●	
HIGH RISK	Actions that are commonly associated with normal business activity that are also used by attackers to maintain a foothold in the environment.		**Immediate Response**
INFORMATIONAL	Actions that are generally associated with normal business activity that should be reviewed on a periodic basis for signs of malicious activity ***If the action is unexpected, it should be investigated immediately***		**Audit**



Security & Compliance

Regulation is a standardized rule by governing bodies to ensure organizations and proprietary information are secure Organizations that are highly security conscious or subject to these regulations need to ensure their MSP has the ability to meet this high standard of security. Here's how Continuum ensures you meet SMBs expectations around security and compliance.

LOG RETENTION

Most compliance regimes require some level of retention of log data and security best practices and also dictate retaining logs to assist in incident response. Continuum Fortify for Network Security retains 90 days of logs online that are available in the console and provide MSPs the ability to retrieve logs as old as 400 days upon request.

COMPLIANCE REPORTING

EventTracker Network Security generates daily compliance reports based on the SMBs regulation needs, and they can be downloaded and saved as required. The three supported compliance reports are PCI, NIST 800 and HIPAA.

888.676.1228 | info@systnet.com

SystemsNet
Keep it up