DATA SHEET

CYPHORT™

GUIDE TO INCIDENT RESPONSE TIME/COST AVOIDANCE

Cyphort Anti-SIEM

The Anti-SIEM Overview

The Anti-SIEM solution combines Advanced Threat Detection, Advanced Threat Analytics, and One-Touch Threat Mitigation into a distributed software platform that integrates with your existing security architecture and is centrally managed through an intuitive UI.

The Anti-SIEM addresses two critical requirements facing security teams:

1. **Productivity.** Security teams are typically flooded each day with hundreds of security alerts that must be triaged to determine which should be ignored and which need investigation. Incident responders require both automation and analytics capabilities that streamline their workflows and reduce the manual effort required for incident analysis and response.
2. **Security.** The alerts, logs, and events presented to security analysts typically indicate symptoms of potentially malicious activity in the network. What's missing is detailed visibility into the specific advanced threat itself. Security analysts require a platform that combines strong threat detection with advanced analytics to deliver comprehensive, actionable information on these threats. In addition, one-touch threat mitigation is needed to immediately contain the threat and update existing security infrastructure to block future occurrences. Download the Anti-SIEM Data Sheet.

How Anti-SIEM Streamlines Incident Response and Lowers Costs

- Integrates with Active Directory to pinpoint the targeted host and user by name
- Ingests logs from security devices such as Antivirus, Endpoint Detection and Response, Next Generation Firewall, and Secure Web Gateways
- Identifies relevant event and log data and extracts key parameters such as filename, threat source, hash, signature, and the action taken by the security device
- Correlates Cyphort-identified advanced threats with relevant event data from other security devices
- Presents a security incident timeline that combines all events targeting the compromised user/host
- Allows a variable time horizon to view past events that targeted the host over months or years
- Prioritizes alerts based on risk, calculated using threat severity, asset value, and threat progression
- Automatically updates blocking rules to a wide range of inline security devices such as Cisco, Juniper, Checkpoint, Palo Alto Networks, Blue Coat, and many others
- Integrates with Network Access Control devices to restrict and isolate the movement of infected hosts

Tier 1 Incident Activities the Anti-SIEM Automates to Enhance Productivity

Without advanced security analytics and automation, Tier 1 analysts are required to manually combine information from an array of data sources to get the actionable information required to assess the risk of each security incident. This is a time-consuming process and is a productivity drag on incident response teams. The Anti-SIEM's advanced analytics engine automates seven key steps in the process and provides the actionable information required by security teams. These steps include:

- Triage
- Identify
- Collect
- Analyze
- Correlate
- Assess
- Mitigate

Average Number of Incidents Triaged Per Day

The Anti-SIEM Time/Cost Avoidance Calculator uses default values for the average number of customer incidents triaged per day. The defaults are relative to the number of endpoints selected and are as follows:

- 5 incidents — for less than 1,000 endpoints
- 10 incidents — for 1,000 to 10,000 endpoints
- 25 incidents — for greater than 10, 000 endpoints

The number of customer incidents triaged per day is derived from a research report by the Osterman Group. The research report survey respondents were categorized into company size based on endpoints and asked to choose the average number of threat incidents they triaged each day. However, users of the calculator can modify the values based on their unique environment. | Download the Osterman Research Report.

About Cyphort

Cyphort, Inc. is a security software company providing mid- and large-size enterprise customers with innovative security analytics for advanced threat defense. The solution is built with an open architecture that integrates with existing security tools to discover and contain the advanced threats that bypass the first line of security defense in an organization. Based in Santa Clara, California, the company was founded in 2011, is privately-held, and distributes its software through direct sales and channel partners across North America and international markets. Learn more at www.cyphort.com.