Co-Managed SIEM Service

A CTI Managed Security Service

CTI's 12x7 or 24x7 Co-Managed SIEM service gathers logs and events from key hosts within the network, aggregates the logs together and provides alerting on events or series of events that match pre-determined criteria. Through a combination of Management and Monitoring of the customer SIEM Environment, CTI is able to provide the following key features to customers.

- Data Aggregation - Logs from the customer's environment are gathered into one central location and displayed together to provide full context to host activity.
- Data Correlation - Logs are inspected to look for relationships, patterns, and trends across all log hosts to identify activity that may be malicious in origin.
- Alerting - CTI works with our customers to create relevant useful alerts so that in the event of issue, security or operational, the relevant parties will be notified.
- Log Retention - CTI works to meet your log retention requirements by identifying the solution that will meet your needs and keep your data secure but accessible if needed.
- Compliance Reports - Depending on compliance or audit requirements, CTI will work with the customer to build the reports and views needed for various levels of user.

SIEM MONITORING & MANAGEMENT

CTI SIEM Management consists of health and performance, availability and outage notifications, patch and software updates and tuning and configuration. Our SIEM Monitoring includes the following.

- Event Review - CTI's Security Operations staff will perform a review of events generated from the logs received from data sources. Actionable events will be escalated via ticketing system to the customer.
- Automated Alerting - CTI will work with the customer on the creation of automated alerting. Automated Alerts are generated when the SIEM has identified activity as suspicious or problematic based on signatures or behavior patterns. Automated alerts arrive via email.
- Integrated Ticketing System - When actionable events are identified by the SIEM Solution an Automated Alert is generated, all information is submitted into our ticketing system for investigation, tracking, and auditing purposes. The ticketing system is available through our customer user portal and email.
- Log Queries & Investigation - In the event that suspicious activity has been detected or an investigation of the activity of a host is a required, CTI can perform custom queries in the SIEM Log Database to retrieve event information from a designated date and time.
- Data Correlation - On-demand reports are available to the customer detailing statistics and analysis of the activity of the hosts reporting in to the service. Many of the reports available are tailored to security or compliance requirements.

CTI

Your Data is Our Passion

SIEM SERVICES

We provide the following features:

- Data Aggregation
- Data Correlation
- Alerting
- Log Retention
- Compliance Reports

Monitoring & Management includes:

- Event Review
- Automated Alerting
- Integrated Ticketing System
- Log Queries & Investigation
- Data Correlation

OUR CLIENTS

We understand that our clients have choices and we partner with them to provide high quality services at a fair value. Their success is our success.

FINANCIAL SERVICES	NATIXIS BROWN BROTHERS HARRIMAN	INSURANCE	Lincoln Financial Group TRAVELERS Amica AUTO HOME LIFE
HEALTHCARE	PARTNERS HEALTHCARE healthdialog BOSTON MEDICAL CENTER HealthNet Plan	LIFE SCIENCES & PHARMA	moderna messenger therapeutics Shire Biogen
HIGHER EDUCATION	Tufts UNIVERSITY HARVARD UNIVERSITY COLUMBIA UNIVERSITY College of Physicians and Surgeons	RETAIL	Kenneth Cole NEW YORK macy's CLARUS

ABOUT CTI

CTI solves business problems by providing services spanning business advisory, technology, and advanced analytics. We help companies envision, design, implement and manage complex data-centric business solutions. Our approach is to understand your business strategy before evaluating how data can strengthen your goals. We focus on producing meaningful insights from your data asset. We expose those insights, embedding them into your business processes while guiding user adoption for a more data-driven culture.

CONTACT US

CTI is a provider of security, platform and analytic solutions located in Burlington, Mass., serving customers in New England, Metro New York, Metro Atlanta, and beyond.

Corporate Office:

78 Blanchard Road
Suite 304
Burlington, MA 01803
Tel: 781-273-4100
800-932-4249
Fax: 781-273-7351