tenable

LCE™

Tenable provides continuous monitoring that empowers you to transform your security program with continuous visibility and critical context, enabling decisive action.

Product Overview

Tenable Log Correlation Engine® (LCE®) is a critical component of Tenable SecurityCenter Continuous View® (SecurityCenter CV™), and is able to aggregate, normalize, correlate and analyze event log data from raw network traffic, intrusion detection data, system and application logs, and user activity within your infrastructure.

Benefits of Using LCE

- Normalize, correlate and analyze user and network activity from log data generated by nearly any device or application across the enterprise in a central portal.
- Store, compress and perform full-text search on any log generated by thousands of network devices and applications.
- Demonstrate compliance with internal policies and regulatory requirements by maintaining an auditable infrastructure.
- Monitor files and directories for unauthorized changes and deletions.
- Detect malware and malicious system processes running in your environment.
- Capture user access logs and behavior for insider threat profiling to determine exactly where your employees surf on the Internet, what systems they access and what programs they run.
- Categorize and store logs not matching existing rules for further analysis, providing insight on activities that previously would be overlooked.
- Monitor local and remote Windows systems for USB devices, CD-ROM and DVD activity.
- Detect deviations from baseline activity for any log source automatically, including firewall spikes, changes in web application error rates and denial of service attacks.

Log Correlation Engine as a Component of SecurityCenter CV

Tenable's continuous monitoring platform is Tenable SecurityCenter CV, which allows for the most comprehensive and integrated view of network health.

SecurityCenter CV can manage multiple Nessus® scanners, multiple Nessus Network Monitor instances and Log Correlation Engine servers and provides a correlation of real-time threat detection, critical log/event monitoring and custom compliance monitoring capabilities in a single, role-based interface for users to evaluate, communicate and report results for effective decision making.

SecurityCenter organizes network assets into categories through a combination of network scanning, passive network monitoring and integration with existing asset and network management data tools, then correlates all this information with enterprise-wide log data to provide a comprehensive view of system and network activity.

Key Features

Anomaly Detection & Event Correlation

As events are collected, LCE uses statistical profiling of each device to identify changes in expected behavior. Alerts are generated if abnormal activity is detected, such as increases in event types, increased connections or changes in the client or server behavior.

LCE contains advanced correlation rules that look for worm outbreaks, network anomalies, compliance violations, data breaches, advanced security threats, misused wireless access points and more. These rules are written in the Tenable Application Scripting Language (TASL), so the definitions can be augmented or modified as the need arises.

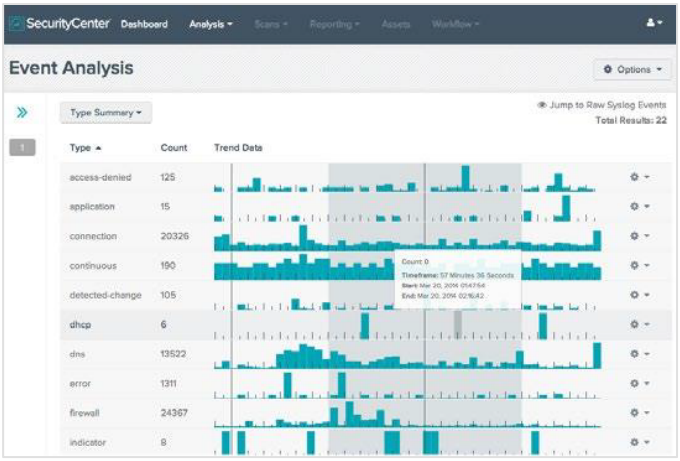
Reporting & Analysis

The forensic analysis and incident response capabilities of SecurityCenter CV and its extensive library of security apps draws on the entire integrated data store of vulnerabilities, threats and intrusions all from one web interface, including:

- **Log Retention** – All logs sent to the Log Correlation Engine can be stored on the same hard disk, relayed to a SYSLOG server or written to a storage area network to aid in regulatory compliance efforts or to support forensic investigations. Log data may be rotated and archived or can be saved in a compressed format on the Log Correlation Engine and can be searched from the Log Correlation Engine interface or the SecurityCenter console.
- **Log Correlation Engine Clients** – Each Log Correlation Engine can be connected to thousands of Log Correlation Engine Clients that are designed to gather Windows logs, web logs, system commands, syslog, network traffic and file integrity information. Additionally, the LCE web query client can import events from Amazon Web Services (AWS) to monitor cloud applications, and it can import successful logins, failed logins and user change events from Salesforce.

Centralized Management

Significantly reduce deployment and administration time with centralized Log Correlation Engine Client administration and management functions. This allows for efficient deployment and real-time configuration modifications.



For More Information: Please visit tenable.com
Contact Us: Please email us at subscriptionsales@tenable.com or visit tenable.com/contact