ManageEngine
Log360

The basics of auditing and **securing your network perimeter** with **SIEM**

www.manageengine.com/log-management

Introduction

To thwart network attacks, you first need to be on top of critical security events occurring in your network. While monitoring network performance is important for troubleshooting and ensuring smooth operations, auditing log data generated by your network devices is crucial for identifying security events of interest. But due to the high volume of events generated by your network perimeter devices, auditing these events in real time can be challenging, if not impossible.

In this handbook, you'll learn about the basics of auditing and securing your network perimeter by leveraging a security information and event management (SIEM) solution.

Extract valuable security insights from network device syslogs

Any activity occurring along your network perimeter is recorded as a log. Firewalls, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), routers, and switches all generate large volumes of syslog data that contain valuable information about every event occurring in your network. These are the logs that security administrators need to audit in order to ensure their network is secure. Collecting and analyzing logs from your network devices comes down to three steps:

- **Enable logging:** Log in to the network device's GUI as an administrator and enable system logging. The device will then generate log entries for a specified set of events and forward the data to the specified remote server.
- **Centrally collect logs:** Deploy a SIEM solution to centrally aggregate log data from all your network devices. Centrally storing log data is essential because it helps you connect the dots and discover attack patterns by correlating events from different sources.
- **Analyze log data to detect attacks:** Set up report and alert profiles on your SIEM solution for critical security incidents. These will help you continuously monitor security events occurring in your network to ensure no potential threat goes unnoticed.

Gain complete network visibility with audit reports

Security teams can periodically review network activity by running reports using a SIEM solution. Audit reports provide a clear visualization of important security events that have occurred over a given time frame. This will give you total visibility of your network perimeter and help you furnish reports for both internal audits as well as compliance audits.

Detect security threats with alerts

To detect threats in real time, configure alerts for events that are a security concern. Depending on your requirements, select which events you need alerts for and which events you can periodically review in reports. When an alert is triggered, you can quickly investigate related events that have occurred by leveraging the search functionality of your SIEM solution. Go one step further and automate threat response by configuring a customized script that will be executed when an alert is triggered.

How event correlation can improve threat detection

Individual events by themselves might not give enough context to help you identify a potential security threat, and manually identifying anomalous patterns is nearly impossible given the volume of event data. This is where the event correlation engine in your SIEM solution comes into play, associating different events occurring on your network, and identifying any pattern of events that could pose a threat to your network's security. This will not only reduce the alert noise, but also help you discover threats that might be missed otherwise.

Detect malicious traffic instantly with threat intelligence

In the field of threat detection and response, threat intelligence (TI) helps mitigate attacks from known malicious sources. Integrating your SIEM solution with a TI feed processor will boost your security team's threat detection and mitigation capability. With an augmented TI feed, a SIEM solution can correlate the network log data with the feed to instantly identify traffic from known malicious sources.

How ManageEngine Log360 helps audit network device logs

Log360 is a comprehensive SIEM solution that helps secure your network perimeter. Log360 collects and analyzes syslogs from network devices in real-time to help detect security threats at the earliest possible stage.

How User and Entity Behaviour Analytics (UEBA) can protect your network from unusual threats

UEBA uses machine learning to create behavior profiles of users and systems in your network. With this security baseline in place, it spots all anomalous activities of users and systems. Any suspicious activity is associated with an increase in risk scores, and this helps prioritize your attention. By monitoring risk scores, you can mitigate potential security threats in your network.

Ready-made reports and alerts

Log360 comes packed with out-of-the-box reports and alert profiles for a wide range of network device vendors. This way, security teams can start running reports and triggering alerts from day one. Schedule reports to periodically review important security events occurring in the network. Large-scale enterprises can easily create environment-specific custom reports and alerting conditions to meet their diverse auditing requirements.

Log360's advanced correlation engine can associate network device logs with event information from other machines to detect advanced attacks. For example, it can correlate VPN client activity with logon and other server activity to detect the installation of suspicious software and services.

USE CASES

Auditing firewall traffic

With Log360, you can audit firewall traffic in real time, including accepted and denied connections. Audit traffic based on the source, destination, protocol, and port to thoroughly analyze trends in firewall traffic.

Detecting network attacks

Log360 processes IDS and IPS logs and alerts you in real time of attacks on your network. You can monitor possible network attack activity based on the source, destination, and severity to detect and mitigate attacks at the earliest possible stage.

Tracking configuration changes

Allowing network device configuration changes to go unchecked can jeopardize your network's security. With Log360, you can audit router configuration changes and firewall rule changes. Ensure security and compliance by continuously monitoring all the firewall rules that have been added, deleted, and modified,

Detecting malicious traffic with threat intelligence

Log360's built-in STIX/TAXII feeds processor and augmented global IP threat database ensures you are dynamically updated with the latest threat data. This will help you immediately detect and block malicious traffic interacting with your network.

Network device vendors supported by Log360

Log360 supports the following network device vendors out-of-the-box:

Please contact support for more details at **log360-support@manageengine.com**