ManageEngine
Log360

CASE STUDY

Crusader Community Health uses Log360 to detect and mitigate cyberattacks

Company	Industry	Location
Crusader Community Health	Healthcare	United States

About Crusader Community Health

Crusader Community Health was established in 1972 as a community-based, nonprofit community health center to serve the Rock River Valley region of Illinois with excellent primary healthcare for all people in need. It is a federally qualified health center that provides complete medical, dental, and behavioral care and also includes specialized care for chronic diseases like diabetes, asthma, congestive heart failure, and chronic lung disease.

> Log360 is an essential component in our organization that made our job hassle-free, and I would definitely recommend it to other healthcare organizations that are seeking a SIEM solution.

Lonnie Lehman,

Director of IT and cybersecurity operations at Crusader

Challenges

As a healthcare organization, Crusader's primary requirement is to adhere to the HIPAA compliance mandate. Meeting the compliance requirements is a continuous process. It involves not only meeting the rules stated in the mandate but also enhancing the security posture of the enterprise.

Crusader wanted to enhance its security posture by analyzing its users' behavior. The company also wanted to audit all its network devices and applications to proactively hunt for any threats. Crusader was looking for a unified security solution that could give it the visibility it needed and help ease compliance audits.

The solution: Log360

Implementing ManageEngine Log360 has helped Crusader Community Health identify security threats and improve its security posture. The solution has aided Crusader with:

- **Network device monitoring:** Log360's security analytics plays an important role in detecting and preventing security breaches by continuously surveilling, collecting logs, and analyzing the devices, like firewalls, switches, and routers. With Log360, Crusader's threat hunters have gained complete visibility into raw log data, so they are now able to monitor the network for threats proactively and resolve them before they get out of hand.

- **Compliance requirements:** Log360's audit-ready HIPAA compliance reports and compliance violation alerts have helped ease the HIPAA audit process for Crusader.

- **Event correlation for attack detection:** Log360's predefined correlation rules have helped Crusader's IT admins detect cyberattacks, like ransomware, privilege escalation, and file integrity threats. The threat hunters get alerted through real-time alert notifications, either via SMS or email, about any malicious security events or compliance-specific events detected across the network.

- **User and entity behavior analytics (UEBA):** Log360 establishes a standard baseline of behavior for all users in the network and assigns the users risk scores. With the help of this feature, Crusader's threat hunters have been able to detect suspicious activities like anomalous logins or deleted event logs. Therefore, it is now easier for the IT admins to keep tabs on unauthorized activities.

- **Dashboard metrics:** With Log360's dashboard, Crusader's threat hunters can take a quick glance at all the major security events taking place in the network or the Active Directory infrastructure. The graphical data has made it easy for them to gain valuable insights so they can develop incident response plans.

Impact

Crusader Community Health is completely satisfied in choosing Log360 as its SIEM solution. The company has found the product to be user-friendly and is mainly impressed by the alert features that help detect critical security events.

Lonnie Lehman, director of IT and cybersecurity operations at Crusader, was able to identify account compromise with the help of Log360's UEBA as he detected and sorted out suspicious changes made to sensitive files in less than a week. Crusader also appreciated the customer service that was provided by Log360's support team and how the team helped resolve all issues.