ManageEngine
Log360

CASE STUDY

Log360 helps Citizens Bank & Trust Co. of Grainger County Automate Log Management and Threat Detection

About the Organization

Citizens Bank & Trust Co. of Grainger County is a state-chartered bank with a rich legacy. The bank recently celebrated 100 years of successful operations in December of 2019. Citizens has offices in five locations across the county, fulfilling the banking needs of over 13,000 customers.

It offers various services to its customers ranging from checking accounts, loan products, notary services, safe deposit boxes, and more. The organization has a compact two-member IT team with Daniel Fast, information security and technology officer, overseeing its IT security operations.

> “
>
> *The automation of log management across AD and the entire network saves me a ton of time and gives me the confidence that my network is secure. I know that no threats are present on my network.*
>
> **Daniel Fast,**
> Information security and technology officer.

Challenges

Being a financial services organization, managing events from all devices connected to the network is one of the primary requirements for Federal Financial Institutions Examination Council (FFIEC) compliance. The logs had to be manually reviewed on an ad hoc basis to spot issues.

Since this process was repetitive and time-consuming, often times, only logs from servers that were deemed critical were audited. Going through logs from all the connected workstations and devices manually wasn't practically possible with such a small IT team. They had to constantly look through hundreds of emails from numerous threat feeds to identify potential risks.

The Solution

Fast was looking for a security information and event management (SIEM) solution to automate the process of log monitoring and threat detection. The out-of-the-box features, unbeatable price, and positive reviews on Gartner and other reputed forums led him to ManageEngine Log360. With Log360, Fast was able to improve the cybersecurity posture of the Citizens Bank & Trust Co. by:

- Automatically monitoring logs from all the components connected to the network rather than a few critical servers.

- Monitoring sensitive servers to detect any anomalous activities.

- Generating several built-in reports by collecting, parsing, and analyzing logs or creating custom reports based on the requirement.

- Leveraging Log360's threat intelligence capabilities. The threat intelligence module spontaneously correlates information from various threat feeds and assists the IT team in protecting the network from the latest known threats.

- Monitoring Active Directory and network devices to enable treat intelligence, which helps the organization fulfill banking compliance requirements.

- Utilizing Log360's flexible, custom functionalities for all the bank's specific SIEM needs.

Impact

Citizens Bank is glad to have chosen Log360 as its SIEM solution especially due to the return on investment. It also appreciates the manner in which feature requests are handled and the support extended in customizing the product to suit the bank's requirements.