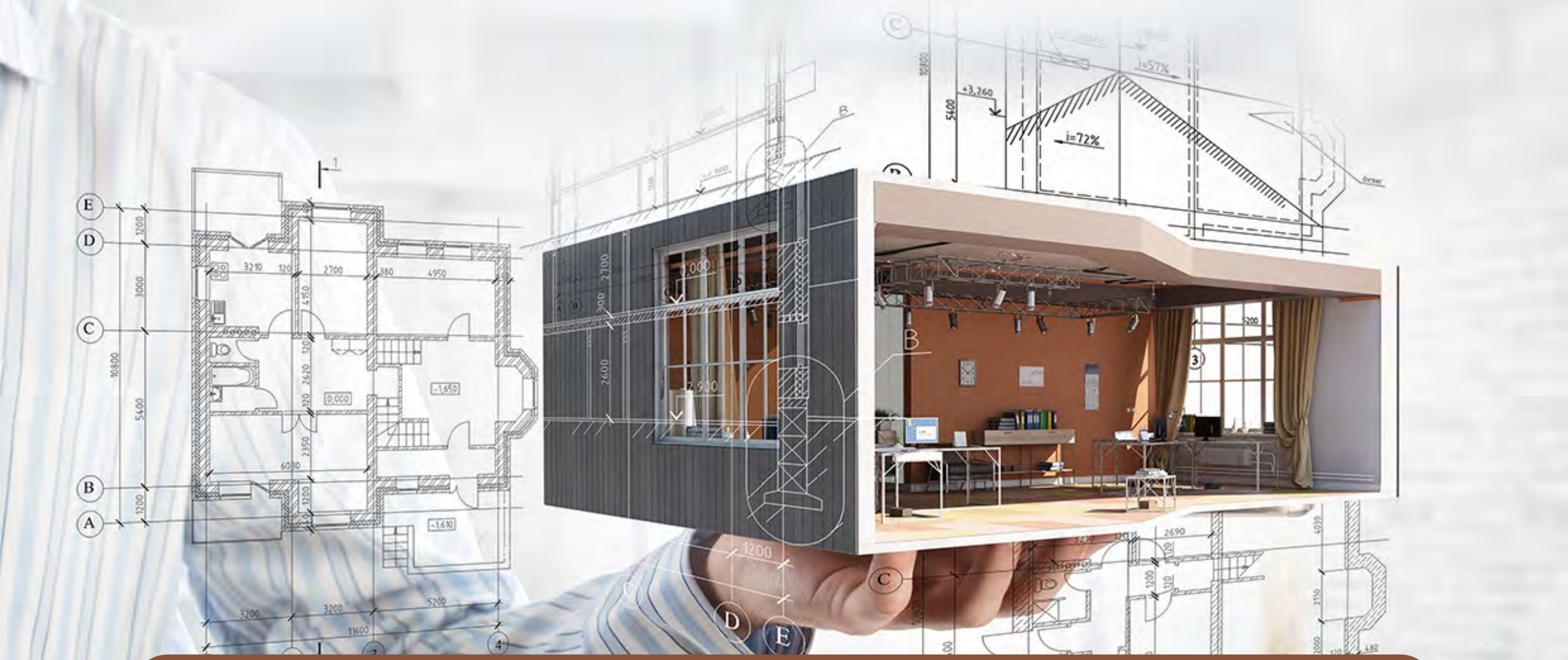
ManageEngine Log360 | CASE STUDY

LaBella leverages Log360 to **enhance its security posture**



Organization: **LaBella** | Industry: **Architecture** | Country: **USA**

About LaBella

LaBella Associates is a full-service engineering team based in Rochester, New York, with more than 1,500 architects, engineers, planners, and construction managers working in more than 30 offices. As a nationally recognized Design Professional Corporation, Labella creates structures, plans, ideas, and results. Its four key service offerings include buildings, energy, infrastructure, and environmental where its impact is seen, felt, and experienced worldwide.

The search for a logging tool

LaBella needed a log management solution to monitor its sensitive file servers, produce reports on the history of access, and utilize other vital data that help it conduct forensic analysis when there is a data breach.

Don Hess, the security operations manager of LaBella, wanted a solution to retain logs of the file system activity and monitor the logon and logoff activity of users to spot any irregularities. Previously, to monitor file system activity or logon activity, Hess needed to visit every file server and manually search for logs, a tedious task.

LaBella's logging woes

LaBella had an issue with unauthorized group policy changes made by its staff and contractors who had access to the internal network. Whenever a breach happened, LaBella's IT security team needed details about who accessed sensitive file servers to be able to perform log forensics. Before, Hess needed to log on to a large number of domain controllers and, since these logs would overwrite itself every 24 hours on the domain controller, it often wasn't possible to find the correct person efficiently or in a timely manner.

LaBella determined it needed to solve these problems and secure its network perimeter with a comprehensive and trustworthy SIEM solution.

The Solution: Log360, a trustworthy choice

LaBella shortlisted a few solutions, like Arctic Wolf and Darktrace, but after hours of research and reading reviews online, a familiar name stood out among SIEM solutions: ManageEngine Log360. Known for its robust reputation in the industry, software developer ManageEngine already earned the trust of Hess. Not only was he familiar with ManageEngine, he also had a deep appreciation of its offerings like Endpoint Central, Patch Manager Plus, and other solutions integral to LaBella's IT operations.

Hess also experienced the exceptional support provided by ManageEngine. Whenever questions arose or assistance was needed, the ManageEngine support team was just a call or message away, ready to offer guidance and resolve any issues promptly. This level of support was instrumental in maintaining LaBella's operations smoothly, earning Hess' admiration and trust, and reinforcing his choice of Log360 over other products.

A favorite Log360 feature: Generating custom reports

When asked about the Log360 feature he uses the most at LaBella, Hess cited monitoring and generating reports for the sensitive group changes. Hess generates various customized reports using Log360 daily and weekly.

Streamlining investigations and cost savings with Log360

When asked how Log360 helps the LaBella save time and money, Hess cites the previous, manual process required to find and determine who implemented group membership changes. Using Log360, Hess is able to do that quickly by performing a simple click. Automation of this process has saved valuable time and money for LaBella.

Strengthening security defenses and achieving compliance

Log360 streamlined the security posture for LaBella and prepared it to tackle any cyberattack that might come its way.

> *"It's a great product and meets all our needs, making it a worth-wile investment.*
> *I'll likely recommend Log360 to others."*
>
> **Don Hess,** security operations manager, LaBella

Hess adds that LaBella will have to be NIST compliant in a couple of years and the predefined reports of Log360 will help it achieve that.

Other key features of Log360

- Log360's UEBA capabilities lets you analyze user and entity behavior patterns to detect anomalies and identify potential insider threats, compromised accounts, and unauthorized access attempts.
- Log360 integrates with the MITRE ATT&CK framework, providing a comprehensive understanding of attack techniques and tactics, and enhancing threat detection and incident response.
- Log360 allows the creation of custom correlation rules, empowering organizations to tailor the correlation engine to their specific needs.
- Log360 generates real-time alerts for critical security events, enabling organizations to take immediate action. These alerts provide actionable information, aiding in rapid incident response and minimizing the impact of security incidents.

LaBella's seamless onboarding experience

Recognizing the importance of a properly deployed solution, Hess chose Log360's onboarding service. The Log360 onboarding support team worked closely with Hess, meticulously assessing LaBella's unique requirements and tailoring the deployment plan accordingly. Its expertise and guidance alleviated any concerns he had, and ensured a smooth and successful deployment.

Throughout the process, the Log360 onboarding deployment team showcased its commitment to customer satisfaction. It swiftly addressed any challenges or issues that arose, resolving them promptly and efficiently. Hess was particularly grateful for this proactive approach which ensured that all problems were rectified in a timely manner. This level of support gave him the peace of mind he needed; he knew that Log360 was deployed properly and that any obstacles would be promptly overcome.

The Log360 onboarding service not only saved Hess valuable time, but it also enabled him to focus on other critical tasks as he entrusted the deployment process to the experts. As a result, Log360 was up and running quickly, empowering LaBella with its robust security features without any unnecessary delays or complications. Hess highly recommends the onboarding service to save time and quickly deploy Log360.

About ManageEngine onboarding service

Onboarding is a ManageEngine service that provides solution implementation to clients upon request. This service includes the installation and customized configuration of the ManageEngine solutions. It enables clients to seamlessly begin work without worrying about the complexities of installation, deployment, and product use. Every client environment is unique and requires additional support beyond the basic installation and standard features. With Custom Onboarding, clients have the option to engage a team of product experts to manage the installation, implementation, customization and training based on the business needs.

Our Products

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus

Exchange Reporter Plus | M365 Manager Plus

ManageEngine
Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

$ Get Quote

⤓ Download