ManageEngine Log360 | CASE STUDY

Revealing the invisible: How Log360 transformed Globitech's cybersecurity landscape

Organization: **GW-Globitech** | Industry: **Manufacturing** | Country: **USA**

About GW-Globitech:

GW-Globitech (GlobalWafers-Globitech) is a world-renowned, IATF 16949:2016-certified provider of silicon epitaxy products and services, catering to the semiconductor industry globally. As one of the largest silicon-epitaxy foundries, Globitech is dedicated to offering a diverse array of epi products, including image sensor epi, buried layer epi, and discrete epi. Utilizing advanced processes and equipment, the company ensures exceptional quality and uniformity across its product offerings.

A subsidiary of GlobalWafers Co., Ltd., Globitech is committed to delivering innovative technology solutions throughout the world. The company operates out of a 125,000-square-foot facility equipped with state-of-the-art infrastructure, supporting a high-quality production process. Established in 1999, Globitech has a rich history of dedication, professionalism, and teamwork that drives its continuous innovations in techniques, strategies, and management.

Unmasking network blind spots:
Identifying the challenges and business requirements

Before implementing ManageEngine Log360, Katie Dell, the IT system administrator at Globitech, was primarily seeking to gain better insights into the network activities of the organization.

In her own words: "The solution was to have more insight into activities happening on the network, and have a way of actively alerting, notifying, and recording any problems, anomalies, or potential threats so that we can resolve these before they get out of hand."

The main challenge was the lack of visibility into the network, which led to a reactive approach to problem-solving, and limited knowledge of potential threats.

"We didn't know there was a problem until the problem had already occurred and had been escalated," Dell said.

From cyberattack to cybersecure: The need for better security

A cyberattack on Globitech's environment highlighted the importance of cybersecurity and the need for a comprehensive approach to protect the organization. The attack prompted Globitech's IT team to take every available approach to understand and address potential vulnerabilities. Overcoming these challenges involved investing resources into becoming more cyber-aware, and adopting a security-focused mindset.

Before choosing Log360, Dell and her team evaluated other solutions, including Perch, Stealthwatch, and SolarWinds. However, they found these alternatives were costly, less intuitive, and not user-friendly for this small team.

> *"We're a small group and having some abilities to plug and play almost without having to take a two-month course on how to use the application was the largest piece of the puzzle for us."*
>
> **Katie Dell,** IT system administrator, Globitech.

Log360's features: A security administrator's dream come true

Log360 played a significant role in improving cybersecurity at Globitech. With the implementation of Log360, the team gained better visibility into user activities and network vulnerabilities which enabled them to implement up-to-date security standards efficiently and quickly.

"Before Log360, our users had a lot of operational freedoms that we didn't know about, and this left our network open to a lot of vulnerabilities," Dell noted.

Some of the most valuable features of Log360, Dell notes, include the capabilities the company leverages utilizing other ManageEngine solutions, such as AD monitoring with ADAudit Plus, and the intuitive dashboards in EventLog Analyzer. Globitech also benefits from analytics, UEBA, and real-time incident response capabilities. These features are crucial for providing better insights into Globitech's network and addressing potential threats to its environment.

Tailoring Log360:
Customizing for effective security threat detection

With the help of implementation through ManageEngine's Onboarding program, Globitech's IT team is able to fine-tune the solution's real-time alerting system to its IT environment without false positives which ensures the accurate timing of events. Moreover, Log360 has helped Globitech's IT team resolve security threats more efficiently, with Dell reporting, "About 30 minutes. It reported that data really quickly!"

Log360 to the rescue: Intercepting a cyberattack

In a particular incident, Dell was alerted to suspicious activity involving repeated logon attempts from a single account. With the assistance of Log360, she delved deeper into the issue, identifying the user account that was the source of the attempts, and the IT team further tracked down the specific computer that was being targeted for access. It was discovered that the Active Directory (AD) account in question was inactive, but hadn't been disabled or deleted. This raised concerns for the IT team about other possible security loopholes that could be exploited.

Most alarming was the detection of an attempt from an external source to utilize the inactive account's credentials in what appeared to be a brute-force attack. Upon recognizing this potential threat, Dell’s team deployed Log360 to swiftly act by implementing measures to secure the AD. Thoroughly cleaning it and ensuring the inactive accounts were removed was their first step. The profile was also removed from computers it was trying to gain access to, thereby blocking any such future threats.

Utilizing Log360, the Globitech IT team has realized substantial time and cost savings along with improvements in productivity and efficiency. Moreover, Dell reported a remarkable 400% improvement in resolving IT tickets related to AD issues. The insightful incident detection and immediate remedial action serve as a testament to the invaluable role of Log360 in reinforcing the company's cybersecurity infrastructure.

Implementation Made Easy: The Benefits of Log360 with Onboarding

Dell's experience with Log360's implementation with the Onboarding service was positive, thanks to the strong partnership and customized setup offered by the product team. She highly recommends taking advantage of Log360's onboarding services for other organizations, stating, "It makes it much less stressful and saves so much time getting it accomplished in just a few sessions that could have taken our IT team months."

During the implementation process, Globitech team faced a few unexpected challenges, including issues with licensing changes and the need for infrastructure adjustments. However, the Log360 team was quick to respond and provide the necessary support.

"Our Log360 liaison was able to pull the appropriate teams needed to quickly resolve the issue so that we lost, maybe, like half a day in the setup. He knew who to get on the phone to get it resolved," Dell observed.

Satisfaction Guaranteed:
How Log360 Exceeded Our Expectations

When asked to describe her team's experience with Log360 in one word, Dell had difficulty choosing just one to state her satisfaction.

> *"Satisfied. Everything was beyond my satisfaction. So happy, relieved.*
> *I just can't pick one."*
>
> **Katie Dell,** IT system administrator, Globitech.

This sentiment showcases the overall success of Log360 in addressing the IT system administrator's needs, overcoming challenges, and providing positive outcomes. Furthermore, Globitech team rated Log360 as a five out of five in terms of ease of use, indicating a high level of user-friendliness.

This case study highlights the pivotal role Log360 plays as a unified SIEM solution to meet the intricate needs of organizations like Globitech. The implementation of Log360 led to substantial enhancements in cybersecurity and operational efficiency. The tool provides a unique amalgamation of enhanced network visibility, efficient threat detection, and streamlined security operations. The potent combination of the Log360 Onboarding service, superior support, and smooth integration with existing infrastructure have made this solution cost-effective and user-friendly.

Globitech has reported impressive gains, with a 400% rise in the efficiency of resolving IT tickets, indicative of the value provided by Log360. The success of Log360 in this scenario is a testament to its ongoing relevance in the evolving cybersecurity landscape. Its demonstrated capabilities and commitment to exceptional service indicate that Log360 is primed to assist organizations in fortifying their digital fortresses, thereby ensuring their success in this digitally driven era.

About Onboarding

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