ManageEngine
Log360

CASE STUDY

# Tigloo quickly identifies and mitigates a DDoS attack on its client with Log360

**Company:** Tigloo | **Industry:** IT services and IT consulting | **Location:** Spain

## About Tigloo:

Tigloo is an IT service organization with 26 years of experience working in services related to ICT infrastructures. Tigloo manages critical infrastructure of their clients, ensuring they are always operational, allowing them to focus on their business with a peace of mind that their IT service management is in good hands. Tigloo also offers security against global security threats with the latest technological advances.

## Challenges faced by Tigloo:

Tigloo has encountered a variety of challenges while working as a IT service provider, that have tested the robustness of their security infrastructure. Among the multiple threats and issues, a few have stood out.

- **Account compromise**

  Account compromises have been a notable threat to Tigloo's clients. Cybercriminals use tactics such as phishing and exploiting vulnerabilities to gain unauthorized access to user accounts. Once access is gained, they can steal data, disrupt operations, or deploy malicious software, jeopardizing the company's digital assets.

- **Misuse of user privileges**

  Misuse of user privileges has posed a significant internal threat. Instances where employees or associates exploit their access to sensitive information or systems have been concerning. Such actions can risk the exposure of confidential data and potentially pave the way for external threats if the misused privileges lead to weakened security.

- **Failed logons or failed authentication**

  Failed logons or authentication attempts have been a concern for Tigloo's clients. These could be indicative of brute force attacks, where attackers attempt different username and password combinations to gain unauthorized access. This threat can result in potential system lockouts, disrupting workflow and productivity.

- **Suspicious changes to sensitive files**

  Tigloo has also dealt with incidents involving suspicious changes to sensitive files. Modifications, deletions, or access to critical data files without explanation could indicate a breach, where an unauthorized entity is manipulating the company's digital assets. This compromises the data and can impact decision-making processes that rely on the accuracy of this information.

  To address these challenges of its clients, Tigloo wanted a SIEM solution that would provide them a consolidated view of their client's security landscape, enabling real-time analysis of events and alerts.

## The Solution: Log360

Log360 provided a structured approach to address these security challenges through its powerful features:

**Mitigating account compromise:**

Real-time alerting: Log360 provided immediate alerts for any unauthorized access or suspicious login attempts, enabling the IT team to act swiftly in preventing potential breaches.

User Entity Behavior Analytics (UEBA): By employing UEBA, Log360 was able to detect anomalous user behaviors, such as unusual login times or access patterns, which could indicate a compromised account.

**Curbing misuse of user privileges:**

Privilege auditing: Log360 helped with auditing user privileges, ensuring that only authorized personnel had access to sensitive data and systems.

Role-based access control: Implementing role-based access control, Log360 ensured that users could only access data and systems required to their role, thereby minimizing the risk of internal threats.

**Addressing failed logons and authentication issues:**

Privilege auditing: Log360 helped with auditing user privileges, ensuring that only authorized personnel had access to sensitive data and systems.

Role-based access control: Implementing role-based access control, Log360 ensured that users could only access data and systems required to their role, thereby minimizing the risk of internal threats.

**Monitoring suspicious changes to sensitive files:**

File integrity monitoring: Log360's file integrity monitoring ensured that any unauthorized changes to sensitive files were instantly detected and reported.

Real-time file auditing: The solution offered real-time auditing of file accesses, modifications, and deletions, ensuring that Tigloo could swiftly identify and investigate any suspicious activity.

With this, Tigloo was able to enhance their client's security posture significantly, ensuring robust protection against both internal and external threats.

## Impact:

In a critical instance that underscored the effectiveness of Log360, Tigloo was able to successfully thwart a potential Distributed Denial of Service (DDoS) attack targeted at one of their clients, showcasing the platform's capability in real-time threat detection and mitigation.

**Timeline:**

Upon detecting an unusual surge in traffic and multiple requests to the client's server, which are indicative of a DDoS attack, Log360 immediately triggered an alert to Tigloo's security team. The alert was based on predefined parameters and anomaly detection algorithms that identified the irregularities in the network traffic patterns.

Within a remarkably short time frame, Eduard Florin, cybersecurity specialist at Tigloo was able to:

- **Swiftly analyze the threat:**
  Utilizing Log360's intuitive dashboard and analytical tools, Florin quickly analyzed the incoming traffic, identifying the malicious IP addresses and patterns associated with the attack.

- **Implement defensive measures:**
  Armed with this information, he formulated and deployed a rule within Log360 to block the identified malicious IP addresses and connections, effectively mitigating the DDoS attack.

- **Preserve client operations:**
  By promptly neutralizing the threat, Tigloo ensured that the client's operations remained uninterrupted, safeguarding their digital assets and maintaining the integrity of their services.

- **Post-incident analysis:**
  Following the incident, Florin utilized Log360's forensic capabilities to conduct a thorough analysis of the attack, ensuring that all potential vulnerabilities were identified and secured against future threats.

This incident not only exemplifies Log360's robust threat detection and rapid response capabilities but also underscores its important role in empowering Tigloo to safeguard their clients against sophisticated cyber threats and saving valuable time, money and resources for the organization.

To help organizations fully understand its potential cost savings, Log360 offers an ROI calculator. This tool allows users to estimate their potential ROI by considering the reductions across all the SIEM cost components. Try it out now!

## 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