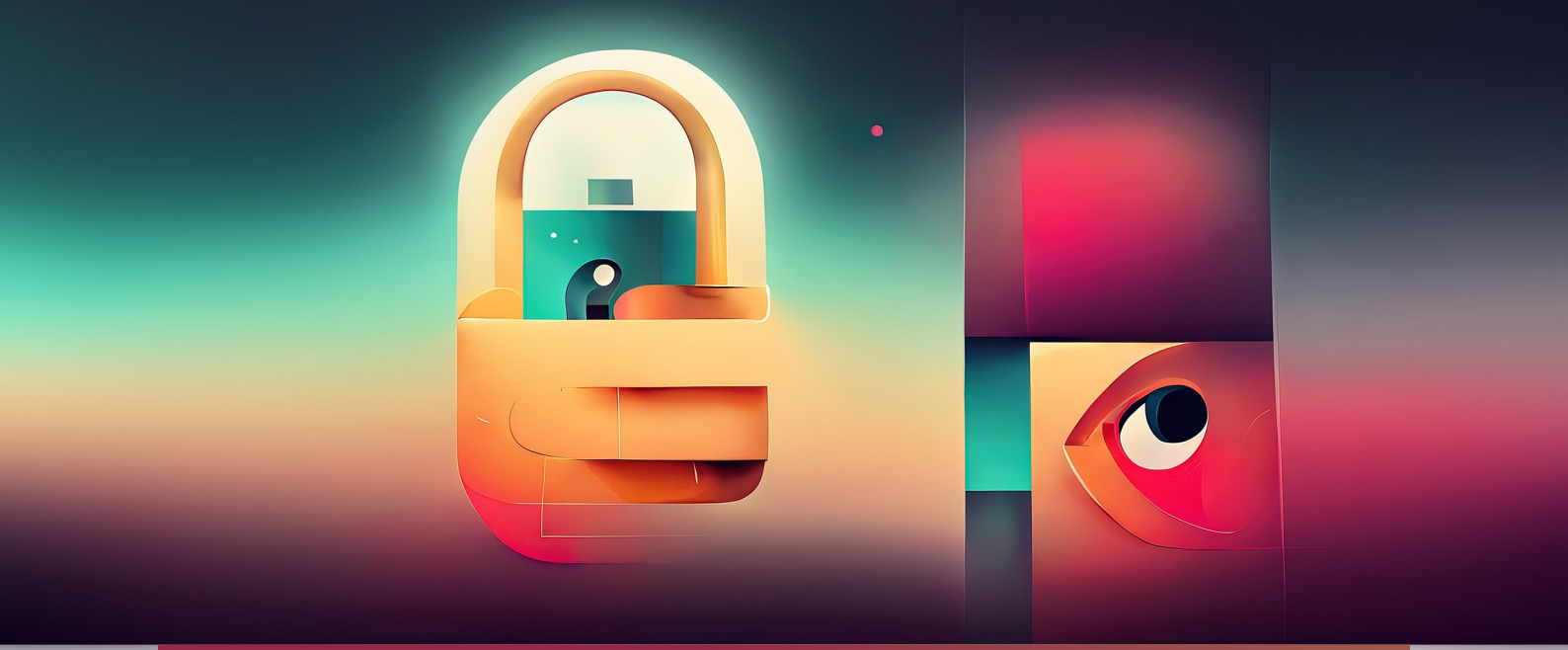
ManageEngine
Log360

CASE STUDY

Detecting and mitigating cyberthreats with Log360:

A case study on Teague's security success



COMPANY: **Teague Inc.** | INDUSTRY: **Design** | LOCATION: **United States**

About Teague:

Teague is a design and innovation company that combines technological expertise with a deep understanding of human behavior to make futuristic designs in the automotive, aviation, retail, smart city, and telecommunication industries. Teague has designed some of the iconic designs that have shaped the world we live in and the culture we experience every day. Some of its designs include the NASA space station, the Microsoft Xbox, the Boeing 787, and the Virgin Hyperloop pod.

Challenges:

The design and innovation industry is known for its cutting-edge ideas, forward-thinking approach, and commitment to pushing the boundaries of creativity. However, this industry is not immune to various challenges, particularly when it comes to ensuring the security and integrity of digital assets and sensitive information. Teague, like other companies in this industry, faces several threats that can have significant implications on its operations and reputation. Some of them include:

Account compromise: Unauthorized access to employee accounts can lead to theft or manipulation of valuable intellectual property and sensitive client information, resulting in financial losses, business operations disruptions, and reputational damage.

Failed logons or failed authentication: Failed logons or authentication attempts can indicate unauthorized access attempts or weak security practices, potentially leading to the disclosure of confidential design information and disruption of projects.

Frank Avendano, senior security and systems administrator at Teague, wanted a solution to solve these challenges and secure the organization's IT infrastructure.

The solution: ManageEngine Log360

To effectively address Teague's security challenges, Avendano chose Log360 since it offered several valuable features tailored to the company's needs.

The following features stood out as particularly beneficial for Teague:

Analyzing log data through a graphical dashboard:
Log360 provides a graphical dashboard that allowed Teague to analyze log data visually. This feature enabled the company to identify and monitor suspicious behaviors, anomalies, and trends in real time, and to prioritize high-risk security events.

Detecting insider threats using user and entity behavior analytics:
By monitoring user activities, access patterns, and behavior, Log360 can detect anomalous actions or deviations from normal behavior. This empowered Teague to identify potential insider threats, such as unauthorized access attempts or data exfiltration, and take appropriate measures to mitigate them.

Blocking malicious sources through threat intelligence feeds:
Log360 integrates with threat intelligence feeds, which enabled Teague to receive real-time alerts and updates regarding known malicious IP addresses, domains, and URLs. By leveraging this feature, Teague could proactively block access to malicious external resources, reducing the likelihood of successful phishing attacks and more.

By implementing Log360 and leveraging its powerful features, Teague was able to bolster its security posture, enhance incident response capabilities, and proactively protect its valuable digital assets from account compromise and failed logons or authentication.

Impact:

With the implementation of Log360, Avendano was able to spot and prevent a brute-force SSH attack targeting a host in a demilitarized zone (DMZ).

Utilizing Log360's real-time monitoring and event correlation capabilities, Avendano detected a suspicious pattern of repeated login attempts on a host in the DMZ. By analyzing the insights on security events and leveraging Log360's event correlation engine, he identified the indicators of a brute-force SSH attack. With this information, he was able to mitigate the attack successfully.

Avendano recognized Log360 as an integral part of Teague's cybersecurity operation, stating that it played a vital role in identifying security threats that his organization faces. With the solution's real-time monitoring and incident management capabilities, Log360 enabled Avendano to stay ahead of threats and protect Teague's systems and data effectively.