ManageEngine Log360 | CASE STUDY

U.S. Geological Survey combats Log4j security threat with Log360

Company: **U.S. Geological Survey** | Industry: **Government** | Location: **United States**

About the organization

The U.S. Geological Survey is the primary federal source of information on ecosystems, land use, mineral resources, water use, and availability. The U.S. Geological survey provides vital earth, water, biological and mapping data to help in the decision-making process on environmental, resource, and public safety issues. Providing updated maps and images of Earth are among its many public services.

Challenges

The U.S. Geological Survey faces the challenge of dealing with an ever-evolving security threat landscape. Kelvin Chung, the system administrator at the U.S. Geological Survey, said that one of the significant security threats faced by his team is the compromise of user accounts. Malicious actors often target user credentials through phishing attacks or other social engineering techniques.

If successful, these attacks can lead to unauthorized access to sensitive systems, data breaches, or further network exploitation. They also have to protect the organization from failed logons or authentication.

The U.S. Geological Survey needed a way to detect, mitigate, and pre-empt cyberattacks, including identifying various attack vectors such as malware, ransomware, distributed denial-of-service (DDoS) attacks, and zero-day exploits.

Overall, the organization faced significant challenges in securing its network, detecting and mitigating cyberattacks, meeting compliance mandates, and proactively managing threats. Addressing these challenges required robust security measures, continuous monitoring, advanced threat detection technologies, and a proactive approach to cybersecurity.

The Solution: Log360

Log360 was the ideal solution for addressing the network security and threat management challenges faced by the U.S. Geological Survey. With its powerful features and capabilities, Log360 offers a comprehensive approach to ensure the organization's data and infrastructure are protected from evolving security threats. Here are some of the ways Log360 has helped solve the challenges faced by the U.S. Geological Survey.

Spotting suspicious user behavior: Log360 provides an intuitive graphical dashboard that enables the U.S. Geological Survey to analyze log data effectively. This visual representation helps identify suspicious behaviors and anomalies within the network.

Identifying security threats through event correlation: Log360 utilizes an advanced event correlation engine to identify security threats. By correlating different security events from various sources, Log360 can detect complex attack patterns that may otherwise go unnoticed.

Meeting compliance demands through audit-ready reports: Log360 simplifies the process of meeting compliance mandates for the U.S. Geological Survey. It generates audit-ready reports that demonstrate adherence to regulatory standards such as NIST, HIPAA, and FISMA.

With Log360, the U.S. Geological Survey is able to proactively detect and mitigate security threats, ensure regulatory compliance, and maintain the integrity and confidentiality of its network infrastructure.

Impact

Within just two weeks of implementing Log360, the team at the U.S. Geological Survey successfully spotted a critical incident related to the Log4j vulnerability. By leveraging Log360's device application monitoring capabilities, Chung and his team was alerted to suspicious activities associated with Log4j. This early detection allowed them to mitigate the potential risks promptly and prevent any exploitation of the vulnerability, thereby safeguarding their sensitive data and infrastructure.

Chung also customized the product to create specialized reports to aid in identifying threats and vulnerabilities within the environment. By utilizing these reports, the team can proactively assess their security posture, identify potential risks, and take necessary actions to mitigate them.