Case Study

BINARY DEFENSE

Binary Defense Helps Law Firm Improve Cybersecurity by Implementing New SIEM

Business

One of the top 10 largest law firms, specializing in manufacturing, energy, utility, healthcare, banking, private equity and technology

Challenges

Current SIEM did not meet security standards due to poor and unresponsive incident detection

Internal team not equipped for 24/7 support

Results

Binary Defense implemented new SIEM for law firm

Internal staff was trained on how to respond to alerts

Binary Defense SOC monitoring for alerts 24/7

"Binary Defense is 100% better than our previous partner and gives us good insights of the threat landscape." -CISO at global top 10 law firm

The legal industry faces complicated cybersecurity challenges
Law firms continue to be a highly-coveted target for cybercriminals looking to gain access to business capital, trade secrets and intellectual property.

The biggest cybersecurity risks for law firms include:
- Phishing
- Ransomware
- Leaks of sensitive data
- The risk of malpractice allegations due to poor cybersecurity

Cybercrime continues to evolve at an alarming pace. If these threats are not contained and stopped, firms can lose assets, highly-sensitive, confidential information, and incur millions of dollars in damages. Add to that the public relations nightmare of the backlash from clients whose information was compromised. After a breach, customer trust is eroded, leading them to seek legal counsel elsewhere. The entire business suffers.

The American Bar Association has issued a formal opinion[1] on attorneys' ethical obligations to avoid cybersecurity breaches. Lawyers are expected to make reasonable efforts when communicating confidential information using the Internet. In addition, depending on the industry of law firms' clients, they may be subject to comply with regulations such as HIPAA (healthcare). However, some firms might not have a security staff that can tackle security issues around the clock.

A Security Information & Event Monitoring System (SIEM) is a useful tool for monitoring data across a law firm's network

A SIEM helps keep an organization safe by centralizing data from various network devices, including servers, firewalls, etc., and correlating that data to provide a holistic overview of an organization's security environment. Alerts are generated if abnormal activity is detected. These alerts need to be reviewed by a person to determine if a threat is present, and then acted on if necessary. To fully respond to SIEM alarms, an organization needs to be staffed for 24-hour support or outsource this work to a Security Operations Center (SOC).

Binary Defense customer was searching for SIEM replacement

One of the top 10 global law firms, with clients spanning across industries including manufacturing, energy, utility, healthcare, banking, private equity and technology, had a SIEM in place but wasn't satisfied with their current technology partner. In addition, the firm wanted to upgrade their internal team's skillset and capacity.

1 https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf

Partner Spotlight: AT&T Cybersecurity United Security Management (USM)

AT&T Cybersecurity offers an all-in-one platform that responds, detects, assesses, responds to and reports necessary threats.

Key features include:

- Network asset discovery
- SIEM event correlation, auto-prioritized
- Dark web monitoring for stolen credentials
- 24/7 monitoring

Binary Defense SIEM

Binary Defense SIEM services protect your company's most valuable assets with network monitoring that is human-driven and technology-assisted. Our platform uses advanced detection technology and a team of dedicated security analysts that integrate seamlessly into your team to provide protection around the clock.

Specifically, the law firm felt that the provider wasn't meeting cybersecurity standards due to poor incident detection and an unresponsive support team. The firm knew they needed a higher level of security with 24/7 monitoring that was quick to address alarms, as well as provide crucial information about the alarm so their team could respond. The law firm selected Binary Defense to replace the existing SIEM technology.

New SIEM replacement helps law firm achieve its goals

Binary Defense recommended AT&T Cybersecurity Unified Security Management (USM) as the replacement SIEM. In 2018 and 2019, Binary Defense was AT&T Cybersecurity's Global Partner of the Year, recognized as the top Managed Security Service Provider partner using the USM solution. (However, Binary Defense works with most of the industry's top SIEMS). The Binary Defense onboarding team did a standard "rip and replace" with the old technology, and then conducted customized training with the law firm's staff on how to respond to malicious attacks, and finally created a decision tree of whom in the firm would respond if an alarm occurred.

AT&T USM is monitored by the Binary Defense Security Operations Center (SOC), which is a team of cybersecurity experts who keep watch over their clients' SIEMs 24/7/365.

As the Chief Information Security Officer at the firm stated, "The Binary Defense SOC experts truly act as an extension of our security team. They provide timely communication on alerts, as well as fully-detailed reports that contain actionable and valuable information."

Learn more about the SIEM service at BinaryDefense.com/SIEM.