CASE STUDY

FinTech Gets 24/7 Coverage, Detections, & Immediate ROI with Binary Defense's MDR & Co-Managed SIEM Solution

Customer Profile

As a Fintech company serving thousands of customers and employing hundreds of staff, their organization managed substantial volumes of sensitive personally identifiable information (PII) from major banks and financial institutions. Recognized as the besttechnology worldwide for fighting enterprise fraud and financial crime, this organization is on a mission to the world a safer place to transact.

Challenges

As a fintech company serving thousands of customers and employing hundreds, they handled large volumes of sensitive PII from major banks and financial institutions. Due to strict regulations, the company struggled to meet client expectations for advanced security measures. Limited resources and expertise challenged the security team in managing SIEM and SOC operations, including recruiting qualified staff for 24x7x365 operations. The team of inexperienced analysts lacked the skills to develop a robust detection strategy and optimize SIEM, resulting in excessive logs that wasted time and resources. There was no SOC coverage after 5 PM or during holidays, creating security risks. Despite customer expectations for stringent security, the fintech's internal team was illequipped. To comply with regulations and meet expectations, the company outsourced its SOC to an MDR provider to address security gaps and improve its security posture.

Solution

Managed Detection & Response (MDR)

Co-Managed SIEM

Sumo Logic

Results

- Implemented the CSE module within SumoLogic, enabling Binary Defense analysts to efficiently execute swift TDIR actions on their behalf
- Enhanced visibility and coverage into their threat landscape
- Immediate ROI on SumoLogic due to full optimization
- Instant access to security experts and proven detection strategies

Challenges

As a fintech company serving thousands of customers and employing hundreds of staff, their organization managed substantial volumes of sensitive personally identifiable information (PII) from major banks and financial institutions. Due to strict regulations surrounding financial institutions, the Fintech Company struggled to meet the expectations of its clients, who had a more advanced security posture than their own. Due to limited resources and expertise, the security team faced considerable challenges in managing their security operations. Key challenges included recruiting qualified staff for 24x7x365 operations, no detection strategy in place with minimal alerts, and the need for outside expertise to implement the CSE (Cloud SIEM Enterprise) module within SumoLogic. The security team consisted of young analysts who lacked the skills needed to develop a robust detection strategy and fully optimize their SIEM. This led to a noisy SIEM due to the ingestion of excessive and unnecessary logs, which consumed valuable time and resources.

Furthermore, there was no SOC coverage after 5 PM or during holidays, creating significant security risks and opportunities for threats to inflict considerable damage. Although customers expected stringent security measures, the fintech's internal team was ill-equipped to meet these demands. To comply with regulations and satisfy customer expectations, the Fintech Company decided to outsource its SOC to an MDR provider, who could address its security gaps and enhance its security posture.

Solution

Binary Defense emerged as the perfect MDR partner due to our attacker's perspective to safeguard clients' businesses while developing a personalized, human-driven, tech-enabled approach for each client, no matter their industry or environment. This personalized approach resulted in a combination of a Managed Detection and Response (MDR) service and a Co-Managed SIEM solution that utilized the Fintech Company's existing security tools. Acting as an extension of the Fintech Company's security team, Binary Defense's expert security analysts provided around-the-clock monitoring of their environment to reduce the risk of attackers breaching their environment and gaining access to valuable customer

data. Binary Defense leveraged its extensive expertise and proven detection methods to implement a standard rule set, complemented by a customized detection strategy. This included tailored playbooks, detections, and use cases, all designed to align with the specific needs and nuances of the Fintech Company's industry.

Results

Implementing Binary Defense's solution produced significant results within just a month. The Fintech Company's security program advanced considerably, gaining enhanced visibility into potential threats and 24x7x365 coverage without adding any additional headcount. When partnering with Binary Defense, the onboarding process included a health check to identify security gaps and ensure that only essential logs were ingested into SumoLogic, minimizing alert fatigue. Expert detection engineers aided the security team by automating manual processes, such as logging into SumoLogic to check alerts and helped centralized and streamlined tasks, saving the internal team precious time and resources. Additionally, Binary Defense detection engineers worked alongside the internal security to deploy the CSE (Cloud SIEM Enterprise) module and configured it to be available for SOC to conduct TDIR actions on their behalf. The Fintech Company experienced immediate ROI with SumoLogic due to the detection engineers creating customized detections, use cases, playbooks and deploying standard rulesets. This proactive approach ensured the fintech's security measures consistently stayed ahead of potential threats

24x7x365
expert coverage without adding a single employee headcount

In Conclusion

The Fintech Company and Binary Defense partnership highlights the importance of a tailored MDR solution with a personalized approach. By leveraging Binary Defense's MDR and Co-Managed SIEM solution, the Fintech Company achieved a mature and robust security program that meets the high standards of their large banking clients. The collaboration addressed the immediate challenges and set the foundation for ongoing security improvements.

Binary Defense is a trusted leader in Managed Detection and Response (MDR), helping organizations across industries stay ahead of modern cyber threats. Our team of SOC analysts, threat hunters, detection engineers, and researchers works around the clock to deliver outcomes that matter: earlier threat detection, faster response, and stronger long-term security.

We take an attacker's mindset to defense, combining deep expertise with proactive tradecraft to protect what matters most.

Learn more at binarydefense.com, explore our blog for the latest insights, or follow us on LinkedIn.

600 Alpha Parkway, Stow OH 44224
sales@binarydefense.com

FORRESTER
WAVE STRONG PERFORMER 2025
Managed Detection And Response Services

BINARY DEFENSE