CASE STUDY

Insurance Company Expands Threat Detection & Response Coverage with Binary Defense's MDR Solution

Customer Profile

This Insurance Company is dedicated to safeguarding families and businesses by offering financial protection. With a robust team of employees, the company has earned accolades from top insurance analysts for its prudent investment strategies and strong performance, serving hundreds of clients effectively.

Challenges

The Insurance Company lacked an internal SOC and sought a MDR provider capable of vendor consolidation and diverse services to enhance its security posture. The internal security team also wanted a trustworthy partner that could provide transparent communication. The environment required expertise in a number of security tools due to it being comprised of telemetry from various cloud and identity sources, all feeding into their SIEM.

Solution

Managed Detection & Response (MDR)
Co-Managed SIEM

Results

- 3 health checks were conducted to close security gaps and reduce blind spots
- Binary Defense SOC achieved a 97.4% triage efficiency and 42.1% investigation efficiency
- 2 Defense Validation tests were carried out on the Insurance Company's environment to identify security gaps
- With an average triage time of 1 minute, a total of 70.7 hours of triage time was completed over the course of 3 months Detection engineers created over 40 new custom detections

Challenges

This Insurance Company focuses on helping protect families and businesses. With hundreds of employees, the Insurance Company has been recognized by leading insurance analysts for its sound investment policies and performance, serving hundreds of subscribers.

The Insurance Company lacked a dedicated internal SOC and sought a MDR provider capable of vendor consolidation through diverse services to enhance its security posture. Additionally, the Insurance Company needed a trustworthy partner with transparent leadership communication. Without an inhouse SOC, they experienced coverage gaps and felt the pressure of potential threats, especially during holidays when they were the most vulnerable to attacks. With only five team members juggling multiple roles and responsibilities, these challenges were particularly pressing. The Insurance Company's environment was comprised of telemetry from various sources, including cloud, identity, two EDRs, and a Vulnerability Management System, all feeding into their SIEM. The team wanted to add an additional layer of defense by bringing in deception technology alongside their existing EDR. They needed an MDR partner to scale and advance their security program while aiding in the transition between SIEM systems. The Insurance Company selected Binary Defense as its MDR provider due to its strong collaboration with its sister company, TrustedSec.

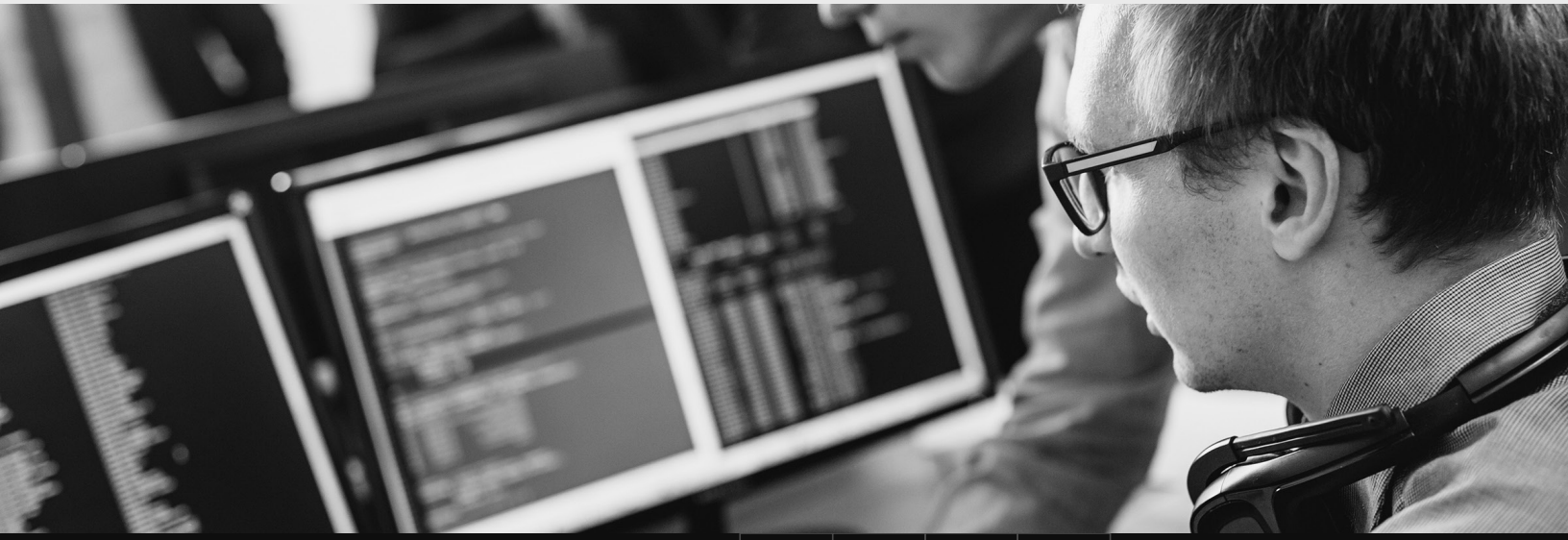
The Insurance Company highlighted the significance of fostering a genuine partnership with its MDR provider, emphasizing the need for open communication channels and transparency from Binary Defense's leadership.

Solution

Binary Defense utilized the Insurance Company's existing security tool investments while offering expert guidance as their organization grew and required a more sophisticated security program. By working closely with the Insurance Company's security team, Binary Defense acted as an extension of their team, assisting with the transitioning, monitoring, and ongoing tuning of their SIEM. Binary Defense crafted a tailored Managed Detection and Response (MDR) and Co-Managed SIEM solution to address the Insurance Company's specific needs, easing the challenge of managing their security investments alone. These security investments was comprised of multiple EDRs, including BDVision for enhanced detection with deception technology, vulnerability management, cloud, and the transition from two SIEM vendors – ultimately moving to Sentinel. Binary Defense's SOAR capabilities enhanced efficiency by offering a unified view for analysts that ingested this alert data across platforms. The Insurance Company gained around-the-clock access to a fully staffed SOC, ensuring no gaps in coverage. Binary Defense employs seasoned cybersecurity experts across T1, T2, and T3 analyst levels to deliver prompt response and remediation support against emerging threats.

Beyond expanding coverage, Binary Defense's MDR solution equipped the Insurance Company with threat intelligence feeds for continuous analytical threat hunts. This offered actionable insights to help reduce Mean Time to Respond (MTTR). To maximize the value of their security tools, Binary Defense detection engineers devised a tailored detection strategy aligned with the client's industry and environment. This strategy, complemented by customized playbooks and Binary Defense's proprietary ruleset, boosted the client's ability to identify and respond to threats swiftly. After the deployment of the detection strategy to its SIEM, regular adjustments of policies and alerts help minimize false positives, ensuring the system remains effective and adaptive to emerging threats.

Ongoing improvements are also captured and discussed in recurring QBRs as one avenue for security posture improvement discussions related to trending metrics or current industry-related threats. Binary Defense's Technical Account Manager and service delivery teams regularly interact with the internal security team and share knowledge about alerts and mitigations. Through this strategic partnership, Binary Defense offers a customized MDR and Co-Managed SIEM service to resource-strapped security teams like the Insurance Company, providing comprehensive visibility and continuous monitoring, shielding it from the latest cyber threats, and maintaining a mature security posture.



Results

Implementing Binary Defense's MDR solution brought significant improvements and measurable results for the Insurance Company by continuously enhancing detection methodologies, threat intelligence, and response strategies. By facilitating the transition of not one but two SIEMs, Binary Defense provided expertise for tool optimization that resulted in the reduction of log ingestion costs.

To ensure a tailored detection strategy, Binary Defense's Detection Engineers identified critical log and event sources, deployed a proprietary Binary Defense ruleset, optimized log ingestion and costs, implemented multiple watchlists, and integrated the Binary Defense Threat Intel Feed to anticipate evolving threats. Additionally, the Detection Engineering team developed several custom playbooks, creating over 40 new detections, and conducted three health checks on the Insurance Company's environment. Through ongoing tuning efforts, the Binary Defense SOC achieved a 97.4% triage efficiency and 42.1% investigation efficiency. With an average triage time of 1 minute, a total of 70.7 hours of triage time was completed over the course of 3 months, allowing the Insurance Company security team to focus on strategic initiatives and core business activities rather than being burdened by operational security tasks.

To further enhance the Insurance Company's threat detection capabilities, Binary Defense conducted two Defense Validation tests on their environment. The first test aimed to identify gaps in coverage by performing adversary simulation on endpoints, carrying out common threat actor tactics for device and domain discovery, attempting to exfiltrate files, and attempting to steal passwords leveraging several tools. The second test emulated Darkside Ransomware threat actions, including checking the language settings of the computer, device discovery, creating a scheduled task for persistence, exfiltrating Excel XLS files and encrypting XLS files in a folder on the desktop.

Upon completing the tests, Binary Defense compiled detailed reports highlighting key findings and offering actionable recommendations to enhance the company's security posture. They also provided tailored threat hunting queries to strengthen the overall threat detection strategy. By partnering with Binary Defense, the insurance company has significantly advanced its security program, fortifying its environment against increasingly sophisticated attackers.

2 Defense Validation tests were performed on the Insurance Company's environment to identify any coverage gaps

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