BINARY DEFENSE

Threat Hunters Identify Outdated Software And Bridge Security Gaps For Government Entity

Customer Profile

A Government Entity that collects and stores sensitive information, encompassing government security secrets, citizen data, and critical infrastructure details. Ensuring business continuity and safeguarding citizens' data are vital for delivering essential services, maintaining public trust, and upholding national security.

Challenges

As a Government Entity it frequently faces cyber threats, including ransomware, business email compromise (BEC), and phishing attacks. These threats can lead to severe repercussions, such as the closure of schools and government offices, and can hinder residents' access to essential services. The security team lacked the resources and time to prioritize Hypothesis-Based Threat Hunts and needed a provider who could identify and alert them to emerging threats to their environment.

Solution

Managed Detection & Response

Hypothesis-Based Threat Hunting

Results

- Over 18,000 alerts were triaged, with only 25 requiring escalation to the client
- Threat hunts reduced the dwell time of attackers in the client's environment
- Successfully uncovered hidden, advanced threats missed by automated, preventative, and detective controls
- Enhanced the detection strategy through a continuous feedback loop informed by threat hunt findings

Challenges

This Government Entity is frequently targeted due to its extensive repository of sensitive information, encompassing government security secrets, citizen data, and critical infrastructure details. These attributes render it highly attractive to threat actors and groups for espionage, disruption, and political influence operations. The Government Entity's security team faced many challenges. Limited resources and competing priorities hindered their ability to dedicate time to proactive threat hunts that would focus on emerging threats. Concerns about potential threats, worsened by political events, highlighted the necessity for proactive threat detection and mitigation. Without hypothesis-driven threat hunts, their security strategy had gaps, increasing the risk of prolonged attacker presence and vulnerabilities across their environment. While implementing new security tools, their team recognized the importance of partnering with someone who could maximize the value of both new and existing security tools during threat hunts.

Solution

Binary Defense addressed these challenges by implementing a custom solution combining **Managed Detection & Response (MDR)** and a **Hypothesis-Based Threat Hunting** solution. Binary Defense expert detection engineers crafted a tailored detection strategy to minimize alert noise and deliver high-fidelity alerts. Security Operations Center (SOC) analysts provide around-the-clock monitoring to protect organizations from threats, offering in-depth investigations and remediation recommendations. In collaboration with SOC analysts and detection engineers, skilled Threat Hunters use a blend of threat intelligence, intuition, and expertise to identify anomalies and track patterns of threat activity over time, revealing hidden threats. Clients benefit from this human-driven process to uncover hidden, advanced threats missed by automated, preventative, and detective controls. Binary Defense Threat Hunters conduct regular threat hunts that are carried out using the client's existing security tools, with automated queries scheduled as frequently as necessary. This vigilant monitoring detects covert attacks that AI tools or standard security methods often miss. Complete transparency between Binary Defense Threat Hunters and the client is maintained by providing comprehensive reports on ongoing and new threat hunting activities.

The Binary Defense team provides reports, which detail the origins of queries from threat intelligence or independent research and are accessible to the client's team on demand for quick access. Binary Defense is committed to transparency and open communication with clients by conducting regular updates and monthly activity summaries; this approach keeps the client informed, enabling strategic decisions based on current threat intelligence.

In Action

Binary Defense's expert Threat Hunters identified applications using outdated and vulnerable versions of log4j on their endpoints. Further investigation revealed that the Java application "Techline Connect" loaded two outdated versions of log4j, both over 10 years old, that were susceptible to log4shell RCE exploits. After completing a thorough investigation, a detailed report was provided to the Government Entity's security team, outlining the findings and offering remediation recommendations. This empowered the team to address the vulnerability and prevent adversaries from exploiting the security gap. With Binary Defense's expert Threat Hunters, the Government Entity enhanced its threat response capabilities, shortening attacker dwell times and mitigating potential damage. This partnership allowed Binary Defense's Threat Hunter to integrate seamlessly with the team, conduct hypothesis-driven threat hunts, and align their security strategy with industry best practices, effectively closing security gaps.

Results

After deploying a tailored detection package specifically designed for the client's unique environment, the Binary Defense team delivered a comprehensive detection and response solution, acknowledging that every environment is unique. This customized approach enabled the Government Entity to stay ahead of emerging threats with precision and agility, ultimately enhancing security effectiveness while minimizing the risk of overlooked threats. Alongside the dedicated work of detection engineers, SOC analysts provided around-the-clock monitoring and triaged over 18,000 alerts in three months, with only 25 requiring escalation to clients. This not only resulted in substantial time savings for the client by eliminating the need to sift through thousands of alerts but also facilitated the creation and ongoing tuning of detections. To enhance defense capabilities, the Threat Hunting team conducted multiple operations to minimize blind spots and counter elusive threats targeting the client's environment and industry. This effort highlights the power of collaboration in proactively addressing threats and fortifying defenses against emerging adversaries.

18,000+

alerts were triaged by Binary Defense analysts, with only 25 requiring escalation to the client

In Conclusion

The collaboration between the Government Entity and Binary Defense highlights the strength of strategic partnerships in bolstering defenses against adversaries. By utilizing Binary Defense's expertise and advanced threat-hunting techniques, the Government Entity has strengthened its defenses, mitigated risks, and reduced the dwell time of threats within its environment. This alliance underscores the significance of regular threat hunts, proactive security measures, and transparent communication in effectively identifying and addressing emerging threats.