BINARY DEFENSE™ | AON

CASE STUDY

Company Strengthens Incident Response Through MDR Integration

Customer Profile

A mid-sized institution faced a significant security incident when they detected unusual network activity. Despite having some security measures in place, they lacked the internal resources to investigate and respond to alerts effectively. Aon's Stroz Friedberg DFIR Team was engaged through counsel to conduct a digital forensic investigation into the incident and to conduct containment, response, recovery, and restoration services.

Challenges

- Limited Internal Resources
- Lack of Continuous Monitoring
- Shift from Current SIEM Provider
- Need for Long-Term Incident Management

Solutions

- Aon Digital Forensics and Incident Response
- Binary Defense Managed Detection and Response

Results

During the incident response effort, it became clear that although the client had an EDR solution in place, the client was experiencing challenges with monitoring and keeping up with alerts, both prior to the incident and during the response. To help, Aon brought in Binary Defense to assist with containment in the short term and with building cyber resilience through enhanced detection, monitoring and response thereafter. Binary Defense was engaged to provide 24/7/365 monitoring and detection, portal access to their SIEM with hours of implementation and initial tuning, SIEM management, existing EDR solution support and ongoing detection engineering and tuning including custom detection creation to ensure best possible oversight and visibility.

Challenges

The internal team at this company faced limitations in both bandwidth and expertise, preventing them from thoroughly investigating and addressing security incidents as they arose. The internal security team also did not have the resources to monitor 24/7/365. This prompted Aon to contact Binary Defense and collaborate to ensure the client was receiving security coverage every hour of the day.

As a result of the incident and the need for a proactive threat detection and response strategy, Aon partnered with Binary Defense to enable Managed Detection and Response (MDR) to establish comprehensive, continuous monitoring. Following the initial response, the company required a comprehensive solution to detect and mitigate future threats proactively. Leveraging the expertise of Binary Defense and Aon, the team successfully integrated reactive and proactive cybersecurity strategies. This collaboration enhanced security of the client's environment, dramatically improving effective detection and response to potential threats.

In response to the incident, the company decided to transition to a more advanced SIEM, necessitating additional monitoring during the transition. This measure was vital to ensure nothing was overlooked during the the SIEM migration.

Solution

DFIR Engagement

Aon deployed Velociraptor for digital forensic investigation and leveraged the client's existing EDR solution in support of the review. Using these and other tools, Aon's Stroz Friedberg DFIR Team determined that a threat actor known as Rapture gained access to the client's network via compromised VPN credentials. Following initial access, the threat actor was able to escalate privileges, install backdoors, move laterally, exfiltrate data and deploy ransomware malware in furtherance of encryption. The attack caused significant business disruption requiring immediate assistance and support.

MDR Integration

Recognizing the need for ongoing protection, Aon recommended bringing in Binary Defense. Binary Defense deployed monitoring solutions across the organization's IT infrastructure, enabling 24/7/365 detection and response capabilities.

Binary Defense MDR offered real-time alerts, allowing the client to respond to suspicious activity immediately. Binary Defense detection tools helped reduce false positives, while the SOC team provided human expertise combined with actionable threat intelligence to validate threats and offer guidance on incident management.

Collaboration Between DFIR and MDR Teams

Aon worked closely with the Binary Defense team, ensuring that the monitoring systems were fine-tuned to the client environment. By integrating investigation, response and monitoring solutions, the client was able to maintain a state of readiness against ongoing threats while reducing the likelihood of similar incidents recurring.

Results

- **Improved Threat Detection:** During the incident response effort, it became clear that although the client had an EDR solution in place, the client was experiencing challenges with monitoring and keeping up with alerts, both prior to the incident and during the response. To help, Aon brought in Binary Defense to assist with containment in the short term and with building cyber resilience through enhanced detection, monitoring and response thereafter. Binary Defense was engaged to provide 24/7/365 monitoring and detection, portal access to their SIEM with hours of implementation and initial tuning, SIEM management, existing EDR solution support and ongoing detection engineering and tuning including custom detection creation to ensure best possible oversight and visibility.
- **Proactive Security Posture:** Continuous monitoring has empowered the client to proactively detect and neutralize potential threats, improving their security posture.
- **Enhanced Security Collaboration:** The combined expertise of Aon and Binary Defense fostered a holistic approach to security, ensuring both reactive and proactive measures were in place to safeguard their environment.

In Conclusion

This company significantly enhanced its security capabilities by integrating Binary Defense's Managed Detection and Response (MDR) solution with Aon's advanced Digital Forensics and Incident Response (DFIR) services.

The integration of these services allowed the company to return to operations more quickly with enhanced and heighted detection and response capabilities. The company was able to turn the page on the incident, address its regulatory and compliance obligations and, importantly, ensure stakeholders that with remediation measures enacted and Binary Defense MDR in place, the company's security posture post incident had been greatly enhanced.

About Binary Defense

Binary Defense is a trusted leader in security operations, supporting companies of all sizes and industries to proactively monitor, detect and respond to cyberattacks. The company personalizes a Managed Detection and Response solution, including advanced Threat Hunting, Digital Risk Protection, Phishing Response, and Incident Response services, helping customers mature their security program with confidence.

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

About Aon
Aon's Cyber Solutions offers holistic cyber risk management, unsurpassed investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.