At a glance

Industry

- Energy

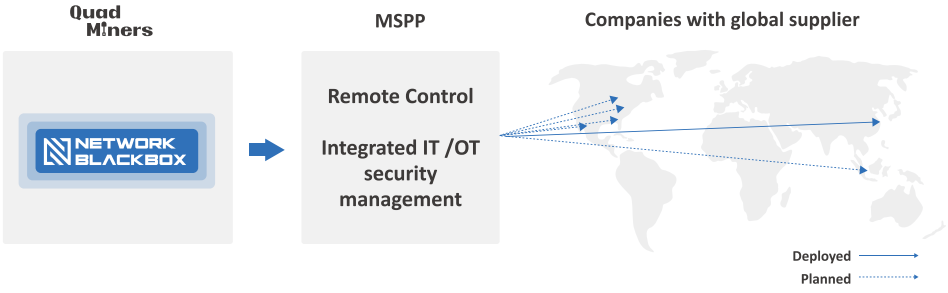
Challenge

- Unable to analyze detected security threats directly from the SOC
- Threat Identification and Threat Response Time Delay
- Limited visibility for both IT and OT in each location
- Inconsistent monitor and response against threat
- Lack of IT staff to operate threat management

Outcome

- Reduced MTTD and MTTR by utilizing conclusive evidence based on Full Packet
- Established an efficient and consistent security threat response that can operate with a small number of securities personnel
- Visibility into IT and OT areas

Full-Packet NDR Solution – Management of advanced SOC



Background

Quad Miners recently implemented its Network Detection and Response (NDR) solution for a leading energy company in the global battery industry. The energy company has been driving the globalization of its production facilities, with operations located both overseas and in Korea. To ensure the security of its critical infrastructure and operations, the company relies on domestic Managed Security Service Provider (MSSP) companies to provide Security Operations Center (SOC) services for its overseas production facilities.

However, with the growing complexity and sophistication of cybersecurity threats, the company has been reviewing a variety of solutions to enhance the security of its Industrial Automation and Control Systems (IACS). They needed a strategy for the implementation of cyber security infrastructure for both IT and OT area with Zero Trust Architecture perspective. The prevailing trend in Industrial Automation and Control System (IACS) networking is the convergence of technology, specifically IACS operational technology (OT) with information technology (IT). Quad Miners' NDR solution Network BlackBox was selected as the preferred solution due to its covers both IT and OT regarding real-time visibility, threat detection capabilities, and incident response capabilities, enabling the company to enhance its cybersecurity posture and protect its critical infrastructure.

Problem

The leading energy company in the global battery industry faced several challenges related to its security operations. The company relied on domestic Managed Security Service Provider (MSSP) companies to provide Security Operations Center (SOC) services for its overseas production facilities, but was unable to analyze detected security threats directly from the SOC. This led to a delay in threat identification and response time, which increased the risk of potential security incidents. Additionally, there was limited visibility for both IT and Operational Technology (OT) teams in each location, making it difficult to monitor and respond to threats consistently.

Furthermore, the company faced a lack of IT staff to operate threat management, which hindered its ability to effectively manage its security operations. These challenges prompted the company to seek out a solution that could provide real-time visibility, threat detection, and incident response capabilities to enhance its cybersecurity posture and protect its critical infrastructure.

Solution

Network BlackBox proved to be the ideal solution for the leading energy company in the global battery industry's security challenges. With the implementation of Network BlackBox, the company became able to detect and analyze all threats in the network directly from the SOC, reducing the time to identify and respond to potential threats. By deploying Full Packet-based NDR, the company also gained network visibility across both IT and OT domains, reducing threat response times, and enhancing its overall security posture. Quad Miners identified ICS Industry Standard Protocol as Modbus; including a custom protocol through customization and development after analyzing full packet data. Additionally, Network BlackBox provided the company with definitive evidence of threats and a single pane of threat analysis, enabling it to save threat response time and reduce daily security operations. Overall, Network BlackBox helped the energy company address its security challenges and enhance its security operations by providing real-time visibility, threat detection, and incident response capabilities to protect its critical infrastructure.

Outcome

The implementation of Network BlackBox resulted in a significant improvement in the cybersecurity posture of the leading energy company in the global battery industry. By utilizing conclusive evidence based on Full Packet, the company was able to reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) for potential threats. The solution also helped establish an efficient and consistent security threat response process for global production facilities that could operate with a small number of security personnel. The Full Packet-based NDR deployment improved network visibility for both IT and OT, minimizing Blind Spots and reducing threat response times. With Network BlackBox in place, the company was better equipped to detect and respond to security incidents promptly, enhancing its overall security posture and protecting its critical infrastructure. Ultimately, the implementation of Network BlackBox resulted in reduced cybersecurity risks and increased operational efficiency for the energy company.

Overall, Quad Miners' solution proved to be an effective and efficient solution for the energy company's security needs, enabling them to detect and respond to threats quickly and effectively.

Why NDR for Energy Companies?

Energy companies rely on their IT networks to operate their critical infrastructure, which can be complex and span multiple locations, making it difficult to identify potential threats and respond to incidents. NDR solutions provide real-time visibility into network activity, detect potential threats, and respond to incidents quickly and effectively. NDR solutions are essential for energy companies to protect their networks against cybersecurity threats, comply with regulations, gain comprehensive visibility into their networks, optimize network performance, and respond to incidents efficiently.

Quad Miners

Quad Miners is a leading NDR software vendor that provides advanced threat detection and response capabilities to organizations worldwide. Our unique selling point is their full-packet capture feature, which allows admins to see more details of network traffic from payloads and provides more depth to security. This feature enables organizations to detect threats that may go undetected by other security solutions, and it provides definitive evidence of threats to help organizations respond quickly and efficiently. Network BlackBox also offer network visibility across IT and OT environments, helping organizations to minimize blind spots and reduce threat response times. With a strong commitment to innovation and customer satisfaction, Quad Miners has established itself as a trusted partner for organizations looking to enhance their network security. Quad Miners Network Blackbox is positioned not only to make additional detections, but is ideally placed to leverage and advance the existing security infrastructure and process.