At a glance

Industry

- Government Office

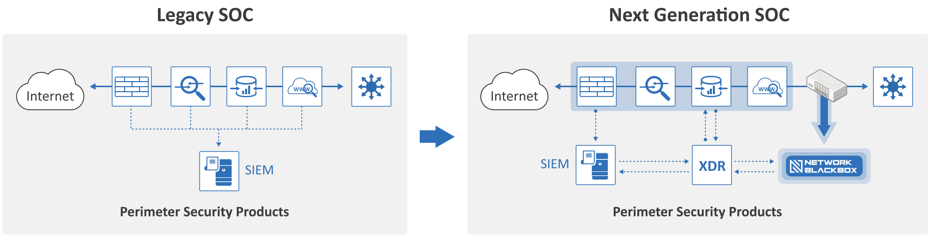
Challenge

- Only focusing on monitoring on detected and generated security events
- Siloized security event analysis system
- Inability to determine the risk and impact of detected security events on the system or experiencing delays

Outcome

- Advanced security operating systemization
- Immediately determine the risk and impact of an attack based on to securing evidence
- Reduce MTTD and MTTR
- Identify the possibility of the government strengthening internal traffic security and making secondary projects

Case of Implementing Advanced Security Operating System for Reducing Response Time



This case study focuses on the successful implementation of an advanced security operating system at a government office to reduce response time related to security breaches. As security threats continue to evolve and become more sophisticated, it is essential for government offices to have a robust security infrastructure in place to protect sensitive information and systems.

The government office in question recognized the need for a comprehensive security solution that could quickly detect and respond to security incidents. After a thorough evaluation process, the office selected Quad Miners' Network Detection and Response (NDR) solution to enhance their security posture and reduce response time.

In this case study, we will examine the challenges faced by the government office, the solution implemented by Quad Miners, and the outcomes achieved through the adoption of advanced security operating systems.

Background

The global government agency operates an integrated internet network that spans multiple boundaries with a complex security configuration. With the diversity of systems, agencies, departments, and personnel under its protection, ensuring effective cybersecurity measures is critical. The agency's focus on accelerating digitalization adds to the complexity of the security challenge, requiring an advanced security operating system that can keep pace with evolving threats. To achieve this goal, the agency has implemented a centralized, integrated security operation to provide comprehensive cybersecurity coverage. However, with the increase in frequency and sophistication of security breaches, the agency recognizes the need to reduce response time and improve its incident response capabilities. In response, the agency has turned to Quad Miners and its NDR solution to enhance its security posture and reduce the risk of cyber threats.

Challenge

The government office faced several challenges when it came to their security operations. Their integrated internet network had multiple boundary security configurations, making it difficult to monitor and detect security events. Additionally, their security event analysis system was siloed, which hindered their ability to determine the risk and impact of detected security events on the victim system.

The office had previously relied on traditional security event management systems that often produced too many alerts, making it difficult for security teams to prioritize and respond to incidents in a timely manner. This led to delays in response times, which in turn increased the risk of a security breach occurring.

Furthermore, the government office was looking to accelerate their digitalization efforts, which meant that their security systems needed to be agile and able to adapt to new technologies and threats. This required a more advanced security operating system that could integrate multiple security solutions and provide a centralized view of the entire security landscape.

Solution

Quad Miners' NDR solution Network BlackBox was able to address the challenges faced by the government office through the implementation of a comprehensive and integrated security operating system. The solution aimed to reduce response time related to security breaches and to provide a centralized, integrated security operation.

Firstly, the NDR solution collected definitive evidence of the breach on the network through collecting rich dataset and metadata which can be only extracted with rebuilt packet streams from captured full packets. This allowed for the detailed analysis of network traffic and helped in identifying the source of the breach.

Next, the solution automated the analysis process through the integration of Stellar Cyber (XDR) and the existing SIEMs and Quad Miner’s Network Blackbox. This allowed for faster identification of security events and their respective risk and impact on the victim system. The integration of multiple security systems also ensured a more comprehensive and holistic view of the network security posture. Quad Miner Network Blackbox and Stellar Cyber initially integrated using Syslog. Quad Miners Network Blackbox sends session with details including metadata which are useful for investigation. It provides concrete evidence for impaction and effectiveness of detected attack events which have been alarmed by other security devices. Also, it provides contents and files includes raw packet analysis through API integration.

Finally, the solution aimed to minimize network configuration changes, which could potentially introduce vulnerabilities and increase the risk of security breaches. By implementing a system that can monitor and detect changes to the network configuration, the government office can ensure that only authorized changes are made and that these changes do not pose a risk to the security of the network.

Outcome

After implementing Network BlackBox, the government office achieved the following outcomes:

- Advanced security operating systemization: The NDR solution helped the government office to establish a more advanced security operating system that could detect and respond to security incidents in real-time. This helped to improve the overall security posture of the organization.

- Immediate determination of the risk and impact of an attack: The NDR solution enabled the government office to immediately determine the risk and impact of an attack based on securing evidence. This helped the organization to quickly respond to security incidents and minimize the potential impact of such incidents.

- Reduced MTTD and MTTR: With the NDR solution, the government office was able to reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to security incidents. This was achieved through the automation of security incident analysis and response, which helped to minimize delays and improve the overall efficiency of the security operations center.

- Identification of the possibility of strengthening internal traffic security and making secondary projects: The NDR solution provided the government office with insights into its internal traffic security. This helped the organization to identify areas of improvement and prioritize secondary projects to strengthen its overall security posture.

Overall, the government office was able to improve its security operations with Network BlackBox. The organization now has a more advanced and efficient security system in place that can respond to security incidents in real-time, reducing the risk and impact of such incidents.