Quad Miners

At a glance

Industry

- Military

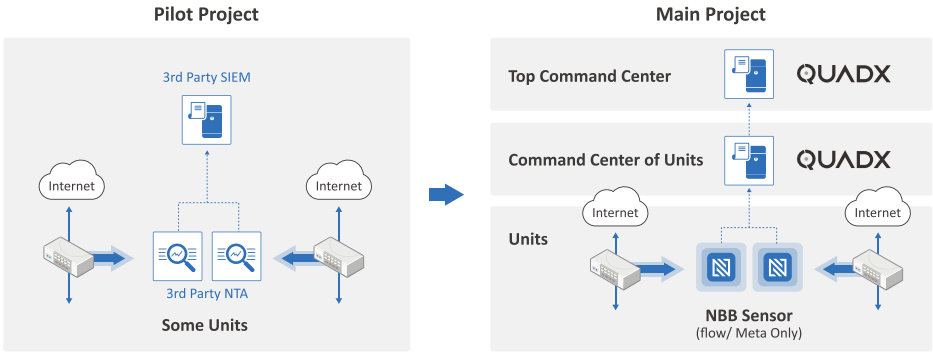
Challenge

- Integrate threat events from nationwide security solutions with integrated analytics
- Systematization of stable network traffic collection for military forces across the country
- Collection of lossless traffic information for all network communications at Army units
- Essential data analytics capabilities to instantly support existing security operating systems

Outcome

- Systematization of meta- and flow-based data analysis across the entire military system
- Integration of traffic monitoring and analysis systems in the Army Security Center
- Supports Cyber Warfare readiness for all military

MILITARY CASE STUDY



In today's digital age, military organizations face an ever-growing number of cyber threats that pose significant risks to national security. Cyber warfare has become an increasingly important part of current warfare strategies, as militaries recognize the strategic value of digital operations. Cyber-attacks can be conducted quickly and anonymously and can often cause significant damage with relatively little investment. To counter these threats, military organizations require robust and advanced cybersecurity solutions that can help detect and respond to security incidents quickly and effectively. Quad Miners, a leading provider of network detection and response (NDR) solutions, has been working closely with a military organization to establish a traffic analysis system based on full-packet flow and metadata. In this case study, we will explore the challenges faced by the military organization and how Quad Miners' NDR solution Network BlackBox helped address these challenges by providing full packet-based traffic inspection.

Background

In recent years, specific military user networks (Internet, intranet) have piloted flow/meta-based analysis systems, which have been effective to some extent. However, in order to establish a comprehensive security posture, it is necessary to collect all traffic from distributed Army networks for full visibility. Additionally, there is a need to build an integrated analysis system related to security threats, which can validate the operational effectiveness between existing security infrastructure and network traffic analysis (NTA) solutions.

Challenge

The military requires an integrated analysis system to effectively protect against security threats across the entire military system. This requires the integration of threat events from nationwide security solutions with integrated analytics. However, due to the distributed nature of military forces across the country, there is a need for stable network traffic collection and the collection of lossless traffic information for all network communications at Army units.

In addition, the NDR solution needs to provide essential data analytics capabilities that can instantly support existing security operating systems. This requires the solution to cover the whole military bases, which have a large surface area, making it challenging to collect and analyze network traffic data from all endpoints and infrastructure.

Furthermore, the military required detailed information which can be used deep investigation against security alerts and events, but the existing NTA product just provided network visibility and known threat detection only. This means the solution must be able to capture all network traffic for analysis, including the metadata associated with the traffic, to enable complete threat visibility.

Finally, the military requires a solution that can keep up with the rapidly evolving threat landscape, which requires constant updates and enhancements to the NDR solution. The solution should be able to adapt to new and emerging threats and be flexible enough to integrate with existing security infrastructure.

Solution

Network BlackBox was able to provide a comprehensive solution for the challenges faced by the military. Quad Miners proved a reliable and effective solution for deep investigation against anomaly and various threats with rich dataset as metadata which can be only extracted with analysis of rebuilt packet streams from fully captured traffic although not store the packet data. Their solution included the integration support through threat event parsing of security solutions, collection of all communication traffic through sensors in each region, and the ability to detect anomalies, threats, and content to suit military characteristics.

Quad Miners also ensured the composition of the shortest security analysis system across the nation by providing vendor data analyst dispatch support. The dispatch support was able to provide timely response to security threats, reducing the analysis and response times.

Overall, Quad Miners' solution provided a comprehensive and effective way for the military to achieve its security goals. The solution integrated seamlessly with the existing security infrastructure and provided the necessary data analytics capabilities to instantly support the existing security operating systems. The NDR solution also covered the whole military bases, which was a significant surface area, ensuring a comprehensive approach to network security.

Outcome

The implementation of Network BlackBox enabled the systematization of meta- and flow-based data analysis across the entire military, providing integrated threat detection and data analysis capabilities. The integration of traffic monitoring and analysis systems in the Army Security Center allowed for efficient centralized monitoring and management of security threats.

The NDR solution significantly improved the military's readiness for cyber warfare by providing enhanced visibility into network traffic and enabling timely detection and response to security threats. Additionally, the legitimacy of the need to migrate to a full-packet capture-based traffic enforcement systematization was recognized, and the NDR solution provided a viable solution to meet this need.

With the support of vendor data analyst dispatch, the shortest security analysis system across the nation was achieved, reducing analysis and response times for security incidents. Overall, Network BlackBox provided the military with a comprehensive and effective network security solution that significantly enhanced its cybersecurity posture.

Why does the military need NDR solution?

The military needs an NDR (Network Detection and Response) solution to enhance their cybersecurity posture and protect against potential cyber threats. With the increasing use of technology and connectivity in the military, there is a higher risk of cyberattacks and potential data breaches. An NDR solution can provide real-time visibility and threat detection across the entire network, allowing security teams to quickly identify and respond to any security incidents. Additionally, an NDR solution can provide the military with the ability to analyze network traffic data for insights and patterns that could help identify potential vulnerabilities in their network. Overall, an NDR solution can significantly improve the military's ability to detect, prevent, and respond to cyber threats.