Top-Tier Airline Carrier

Case Study

Top-tier Airline

Enhancing Security Operations for a rich legacy carrier with NetWitness Platform

Customer Overview

A renowned national/ international airline carrier with a lot of legacy and history, who is dedicated to providing safe and comfortable air travel to millions of passengers was faced with a unique challenge. With a complex and expansive IT infrastructure to manage flight operations, reservations, customer service, and more, the airline recognized the critical importance of robust cybersecurity measures to protect sensitive passenger data and maintain operational integrity.

Problem Statement

The customer faced a significant challenge in managing its diverse and distributed logging points across various IT systems. The absence of centralized log management led to inefficiencies in monitoring, detecting, and responding to potential security threats. The customer needed a solution to consolidate these siloed logging points into a centralized location, which would facilitate better control, correlation, and visibility of security events and incidents.

Key Customer Expectations:

The Customer had the following key expectations from the solution:
1. **Centralized Log Management:** The customer sought to consolidate all logging points into a single, centralized location to streamline security operations and improve efficiency.
2. **Enhanced Visibility:** The Carrier aimed to gain a comprehensive view of its IT environment's security posture by aggregating and correlating security data from various sources.
3. **Enhanced Visibility:** The customer wanted an advanced solution that could detect and alert them about potential security threats in real-time, allowing for swift remediation.

Solution Proposed: NetWitness Platform

After careful evaluation of multiple options and the expectations of the customer, the proposed solution was the implementation of the NetWitness Platform. NetWitness Platform is an evolved Security Information and Event Management (SIEM) system and threat detection solution. It offers the following features to fulfill customer's requirements:

1. **Centralized Log Management:** NetWitness Platform provides the ability to collect, normalize & store logs from various sources in a centralized repository. This consolidation enables Customer's security team to efficiently analyze security events from a single location.

2. Correlation and Visibility: The platform's advanced correlation engine allows for the detection of complex threats by analyzing security events across the entire IT infrastructure. It helps identify patterns & relationships that might indicate a potential security incident.

3. Real-time Threat Detection and Response: NetWitness Platform's real-time monitoring and alerting capabilities empower customer's security analysts to detect and respond to security incidents promptly. This reduces the time between threat identification and mitigation.

4. Advanced Analyst Workbench: The solution offers an analyst workbench equipped with advanced tools for investigating and triaging alerts and incidents. This feature enables customer's security team to quickly assess the severity of alerts and take appropriate actions.

5. Security Operations Orchestration: NetWitness Platform supports end-to-end security operations programs, allowing customer to streamline and automate incident response processes for improved efficiency.

Conclusion

By partnering with Techjockey, This renowned national/international carrier successfully addressed its challenge of consolidating logging points and gained improved control, correlation, and visibility across its security operations. The solution's capabilities led to enhanced threat detection, streamlined incident response, and a fortified cybersecurity posture for the airline's critical IT infrastructure.

Benefits and Outcomes:

By implementing the NetWitness Platform, the customer achieved the following benefits:

Efficient Operations

Centralized logging and advanced correlation improved the efficiency of security operations, reducing the time and effort required to manage security events.

Enhanced Threat Detection

The platform's real-time threat detection capabilities enabled customer to identify and respond to security incidents more effectively, bolstering their overall cybersecurity posture.

Improved Incident Response

The advanced analyst workbench and orchestration capabilities allowed customer's security team to respond to incidents promptly and effectively, minimizing potential damage.

Comprehensive Visibility

The consolidated view of security events provided a holistic understanding of the airline's security landscape, facilitating better decision-making.