



# Establishing a State-of-the-Art Security Operations Center (SOC) for an 80+ Year-Old Midwestern Insurance Firm

**Industry:** Insurance

**Client:** Leading US Insurance Company

## Challenge

The client, a prominent US insurance company, was facing increasing cybersecurity challenges as their IT infrastructure expanded across multiple environments, including Azure, AWS, and on-premises systems. They required a comprehensive Security Operations Center (SOC) to provide real-time threat monitoring, detection, and response. In addition, they needed to migrate their existing security workloads to a more advanced and scalable Security Information and Event Management (SIEM) platform to consolidate log data from various sources and enhance their threat detection capabilities.

# Key Challenges



Expanding infrastructure with security needs across hybrid environments (Azure, AWS, on-premises, third party cloud solutions).



The need for a centralized SOC for real-time threat monitoring and incident response.



Migrating to a more robust SIEM platform capable of integrating diverse log sources and environments.



Ensuring seamless SOC operations and empowering internal teams to maintain and scale security operations.

## Activities

NETSOL was selected as the trusted partner to build the SOC from the ground up, delivering the following services:

### 1 | **SOC Establishment:**

Built a centralized SOC infrastructure to continuously monitor security events, detect incidents in real time, and coordinate responses across cloud and on-premises environments.

### 2 | **IBM QRadar Deployment:**

Built a centralized SOC infrastructure to continuously monitor security events, detect incidents in real time, and coordinate responses across cloud and on-premises environments.

- ✔ Successfully migrated the client's existing security workloads to IBM QRadar, a leading SIEM platform known for its scalability, advanced threat detection, and efficient log management capabilities. This has allowed for centralized log management, real-time security event monitoring, and automated threat response, significantly enhancing the company's ability to detect and address security incidents efficiently.
- ✔ Configured QRadar in both distributed and high-availability (HA) modes, ensuring seamless, continuous monitoring across all environments, even during peak loads or unexpected failures.
- ✔ Deployed QRadar with integrated behavioral analytics, machine learning (ML), and artificial intelligence (AI) to continuously monitor and analyze network traffic and system activities. This proactive approach enabled the early detection of anomalies, suspicious behavior, and emerging threats, allowing for rapid interception of potential attacks before escalation.
- ✔ Optimized use cases through continuous fine-tuning, ensuring QRadar effectively generates relevant offenses in response to the latest and evolving security threats, improving incident response and reducing false positives.

### **3 | Log Source Integration:**

Integrated log data from all critical sources, including Azure, AWS, on-premises systems, and third-party cloud services, into IBM QRadar for comprehensive security coverage.

### **4 | Policy and Procedure Development:**

Developed and documented standardized SOC policies and procedures to streamline operations and ensure efficient, organized responses to security incidents.

## 5 | **User Training:**

Provided in-depth training to the client's internal teams on SOC operations, security best practices, and the effective use of IBM QRadar, empowering them to independently manage and scale their SOC.

## **The Solution**

NETSOL delivered a cutting-edge SOC designed to centralize security monitoring across the client's hybrid cloud and on-premises environments. With IBM QRadar SIEM at the core, the SOC provided real-time threat detection, analysis, and response capabilities. The seamless integration of log sources from Azure, AWS, on-premises systems, and third-party services offered the client a holistic view of their security posture.

Additionally, NETSOL developed a set of comprehensive SOC policies and procedures, ensuring structured, efficient, and scalable operations. Extensive user training further empowered the client's teams to maintain the SOC independently, reducing their reliance on external support while enhancing their ability to manage and mitigate security threats proactively.

## **Achievements**

The deployment of the SOC and migration to IBM QRadar resulted in significant improvements to the client's cybersecurity posture:

### **Faster Threat Detection and Response:**

The consolidation of log data from diverse environments (Azure, AWS, on-premises) within QRadar significantly reduced the detection-to-response time for potential threats. This minimized security weaknesses and helped prevent the escalation of security incidents.

### **Empowered Teams:**

The in-depth training provided by NETSOL enabled the client's teams to manage SOC operations independently. This not only enhanced their operational capabilities but also fostered a culture of proactive threat mitigation.

### **Streamlined Operations:**

The newly established SOC policies and procedures ensured structured and efficient incident handling, enabling the client's internal teams to respond more effectively to potential breaches.

### **Enhanced Security Visibility:**

Centralized monitoring across the entire infrastructure gave the client real-time insights into security activities, allowing for quicker identification and mitigation of suspicious activities across cloud and on-premises environments.

## **Conclusion**

NETSOL's expertise in SOC development and the deployment of IBM QRadar enabled the leading US insurance company to significantly strengthen their cybersecurity defenses. The migration to a robust SIEM platform, combined with the seamless integration of multi-cloud log data and comprehensive training, resulted in faster threat detection, increased security visibility, and a more empowered internal security team.

This case study highlights NETSOL's ability to deliver customized, state-of-the-art cybersecurity solutions tailored to complex, multi-cloud environments. By partnering with NETSOL, organizations can confidently safeguard their operations and data, ensuring resilient and scalable security management.

# About NETSOL

NETSOL Technologies is a trusted global partner, renowned for its deep industry expertise, customer-centric approach, and commitment to excellence. Delivering cutting-edge IT solutions with a strong emphasis on cloud technology and professional services, NETSOL ensures client success across 30+ countries, solidifying its position as a leading global IT solutions provider.

## PARTNERSHIP



## CERTIFICATIONS



## COMPLIANCE POSTURE



Information Security Management Standard



System and Organization Controls



System and Organization Controls



System Management System Standard



Quality Management System Standard



**Get in touch!**

**NETSOL Technologies Inc.  
(Headquarters)**

16000 Ventura Blvd.,  
Suite 770 Encino, CA 91436

**Phone: +1 818 222 9195**

**Schedule a Meeting**

**Website:**  
[www.netsoltech.com](http://www.netsoltech.com)