CASE STUDY

Microland minimized risks and secured an S&P 500 global hospitality & entertainment company with ServiceNow integrated automated vulnerability management

Overview

Our client is a US-based hospitality and entertainment company operating over 35 hotels, casinos, resorts, and golf courses across the country with 50,000+ employees catering to millions of customers annually.

Challenge

The client was operating in the travel and hospitality industry and handled sensitive customer information of thousands of its customers. The client was concerned about the risks from unidentified and unmitigated vulnerabilities in its IT environment which could impact its day-to-day operations or lead to a breach of customers' sensitive and financial information.

The customer wanted to revamp its security operations by integrating its cybersecurity tools with ServiceNow to address the below challenges:

Lack of visibility into risk posture:

The client was leveraging multiple platforms for vulnerability management without real-time visibility or insights into the risk posture of the organization

Delayed response mitigation:

Increased risk of threats to the IT environment due to delayed response and mitigation of vulnerabilities exposing critical assets in the organization

Ineffective and unstable CMDB:

Lack of configuration management database (CMDB) maturity in terms of data completeness, correctness, and compliance
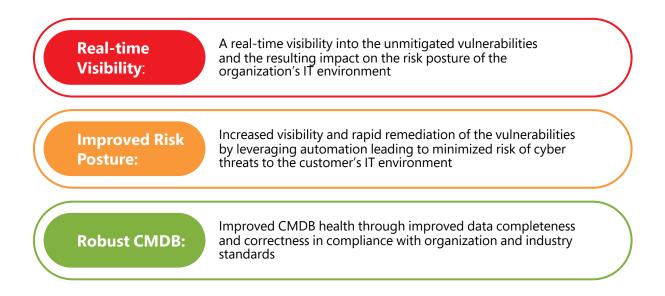
Solution

Based on the inefficiencies identified during the assessment of the security operations and CMDB management, Microland designed and implemented the below solution in ServiceNow to remediate the gaps identified.

• Automate Integrating enterprise vulnerability management tools like Rapid7 InsightVM and Microsoft TVM with ServiceNow to provide end-to-end visibility across the attack surface of the IT infrastructure. Integration with ServiceNow provided real-time insights into the IT risk posture of the client's organization with periodic comprehensive reports on unmitigated vulnerabilities.

• **Improved CMDB:** Comprehensive analysis of over 4 million CIs in the CMDB for data completeness and correctness and maturing CMBD based on the gaps identified and recommendations of the assessment. Implemented the industry best practices to improve CMDB maturity and compliance with organization and industry standards.

Business Benefits Delivered

Based on the assessment of the customer's security operations and CMDB management and the remediation changes implemented based on the recommendations, the customer achieved the following:

| **Real-time Visibility**: | A real-time visibility into the unmitigated vulnerabilities and the resulting impact on the risk posture of the organization's IT environment |

| **Improved Risk Posture:** | Increased visibility and rapid remediation of the vulnerabilities by leveraging automation leading to minimized risk of cyber threats to the customer's IT environment |

| **Robust CMDB:** | Improved CMDB health through improved data completeness and correctness in compliance with organization and industry standards |