CASE STUDY:

Tocumen International Airport Chooses RidgeBot Automated Pentesting for More Secure, Agile, and Resilient Security Operations

Ridge Security Technology Inc. www.ridgesecurity.ai

The Customer

In Panama City, Panama, Tocumen International Airport is the region's primary airport and manages four regional airports, serving as a crucial hub for domestic and international flights. With approximately 1,700 employees, the airport ensures efficient operational management.

The airport's sprawling aviation complex is pivotal in air travel and cargo transportation. Its significance is underscored by its service to 17,820,000 passengers, 31 airlines, and the annual transport of 208,000 metric tons of cargo.

The Challenges

The airport encountered significant security challenges deploying new systems into production and changing existing systems. With dozens of critical applications, Tocumen absorbed cyberattacks daily. It needed a solution to prioritize hundreds of vulnerabilities by identifying the most critical so the team could focus on eliminating the highest risks first and then address the less severe ones.

To address these challenges, Tocumen engaged a manual penetration testing firm to test its systems. This manual process led to significant delays and a lack of agility in service delivery. Implementing a single penetration test took three months for the contract, six weeks for testing, and a month for the final report. Tocumen needed to reduce this timeframe significantly, lower the cost of testing, and enable more flexibility in the testing process. The yearly fee for manual penetration tests was over $130,000. Tocumen wanted to cut that cost in half.

Tocumen's aspiration to conduct pentesting in-house and at any time required an automated, user-friendly solution. The aim was to eliminate production delays and establish a more agile and consistent security posture.

A critical issue was the infrequency of their penetration testing, which was conducted only once a year. Without more frequent testing, the escalation of cyber threats posed a significant operational risk.

Improving infrastructure coverage was essential. Manual pentesting was limited to servers and workstations. The airport needed broader protection coverage with a solution that could test anything with an IP address. This included web servers, CCTV equipment, access control systems, firewalls, printers, IP phones, flight information display systems, communication, and security devices.

The Solution

The airport chose RidgeBot, an AI-Powered security validation platform that proactively discovers and eliminates threats with frequent and continuous automated penetration testing. Unlike manual testing, RidgeBot operates tirelessly and can regularly conduct pentesting weekly or even daily and provide historical trending reports for analysis.

Ridgebot safeguards all of Tocumen's applications, which are crucial for maintaining operational efficiency, security, and passenger experience. Three apps are at the top of their critical list.

Baggage Handling System: The system is 4 kilometers long and has potential attack surfaces along its path. RidgeBot tests the entire system to find any vulnerabilities that can be exploited.

Closed-Circuit Television Surveillance System: Vital for airport and national security, this system employs facial recognition and aids in counterterrorism efforts. RidgeBot tests the CCTV cameras using their IP addresses and the servers that run the system. During the ethical hacking process, RidgeBot uses the camera's web interface to simulate a hacker taking over control. This enables Tocumen staff to understand vulnerabilities and fix them quickly.

Total Airport Management System: This is mission-critical for coordinating all airport operations and activities and ensuring seamless functioning across the airport. Every week, RidgeBot tests dozens of servers supporting the system for vulnerabilities to ensure its availability.

The airport leverages RidgeBot's clear reporting and visual aids like the KillChain for remediation. This provides the Tocumen team with a graphical representation and a logical view of all the steps RidgeBot took to exploit a system vulnerability. For example, if a server was successfully compromised during a test, other systems may have been used to access it. RidgeBot pinpoints vulnerabilities on those systems without interrupting the server supporting airport operations.

Additionally, Tocumen utilizes security assessments against ransomware, information leakage assessments, Active Directory security validation, and weak password usage validation. These features are vital in enhancing the airport's security posture and ensuring robust protection.

The Benefits

RidgeBot has proven instrumental in identifying exploitable vulnerabilities in systems often overlooked, such as printers, CCTV equipment, and IoT devices. Compared to manual testing by experts, RidgeBot is significantly faster and more precise in its findings, enhancing the airport's ability to address security vulnerabilities more effectively.

The airport significantly enhanced its security posture by minimizing exposure periods for newly exploitable vulnerabilities. Additionally, it now promptly deploys new services into production. RidgeBot has improved the productivity of the airport's security personnel, allowing them to focus on exploitable vulnerabilities and prioritizing the most critical vulnerabilities and potential risks.

Other pentesting vendors were evaluated. However, the other solutions required server agents, adding complexity to installation and operations. Furthermore, no other product performed well for web pages, and none tested web servers. They also lacked intuitive interfaces, making them challenging to navigate and understand. Ultimately, these factors led Tocumen to choose RidgeBot.

> “We particularly appreciate Ridgebot's zero false positives, it identifies exploitable vulnerabilities, validates, and provides evidence to substantiate those risks. Additionally, RidgeBots' real-time reporting means instant results rather than waiting weeks”.
>
> *Abdy Sanjur, Innovation Manager within the Technology Vice Presidency for Tocumen International Airport*

Other insights reflect positive staff experiences and benefits that Tocumen has derived from using RidgeBot.

User-friendly interface simplifies pentesting and enhances overall usability.

Real-time reporting provides immediate insights into security vulnerabilities, enabling prompt remediation.

Significant time-savings and increased efficiency compared to manual pentesting.

Continuous monitoring maintains security resilience and prevents breaches.

Automated pentesting accuracy and effectiveness in identifying vulnerabilities enhance Tocumen's security posture.

Agentless approach distinguishes it from other solutions.

Excels in pentesting for web services.

Integral to Tocumen's comprehensive multi-layered security, RidgeBot enables the airport to test the security of its entire IT infrastructure. It is more confident, knowing its IT infrastructure is proactively tested, validated, and secured before anything can be exploited.

Tocumen plans to use RidgeBot in a new security operations center, acting as a red team, to conduct ethical attacks and test the internal team's ability to respond to incidents.

About Ridge Security

Ridge Security is a leader in exposure management and is dedicated to developing innovative cybersecurity products that benefit CISOs and security teams by reducing risk through validation and using automation to improve efficiencies. Ridge Security's products incorporate advanced artificial intelligence to deliver comprehensive security validation, powerful workload protection and cloud security monitoring.

Request a Demo