Aviation Industry International Airport Case Study

Background

Officially opened in the mid-1990s, this busy international state airport is the largest in North America with over 35,000 employees working from its Western United States location. It handles traffic from 23 different airlines from North America, Latin America, Europe and Asia, providing non-stop flights to 215 destinations and taking travelers around the globe.

Like many international airports, at any given time this airport's IT system will process vast amounts of information for purposes ranging from ensuring people get from A to B safely to maintaining the highest airport security standards. Therefore, the international airport was searching for a trusted and experienced external partner to help review and bolster its cybersecurity.

Challenge

Given the nature of an international airport's activities, the security of data is of paramount importance to ensure passenger and staff safety. If an airport's operations were ever infiltrated the impact could be catastrophic.

It is not surprising, then, that international airports must adhere to meticulous standards set and monitored by government agencies and non-compliance with data protection regulations can result in hefty fines.

However, many security auditing solutions focus on network scanning alone, rarely extending their focus beyond firewalls, and many are prohibitively expensive.

The airport wanted a durable solution that would underpin their cybersecurity set up, help them quickly identify any weaknesses throughout their complex network and recommend clear steps to remedy each one and ultimately ensure compliance.

The Solution

The IT team at the airport decided to implement Titania Nipper, saying it "takes a refreshingly new approach to security auditing, supporting an impressive range of firewalls, switches and routers from all the major players".

Nipper supports devices from Cisco, Brocade, Check Point, Fortinet, HP, Juniper, Watchguard, and many others and can provide up-to-the-minute reports on vulnerabilities, making it an obvious choice for this US-based international airport's complex network.

With extremely busy day-to-day operations at play, the virtual modeling aspect of Nipper, which reduces false positives and identifies fixes to ensure security and compliance, was another attractive feature for the airport's team who decided to implement the software.

"Nipper takes a refreshingly new approach to security auditing, supporting an impressive range of firewalls, switches and routers from all the major players."

Aviation Industry International Airport Case Study

Technical know-how

For busy IT teams like the one at this airport, another key benefit of Nipper was that installation is complete within minutes, and auditing is a straight-forward, two-step process.

Nipper is easy to set up and implement - 'straight out of the box' it makes regulatory compliance a clear and efficient process.

Those responsible for cybersecurity can simply download the configuration file from the device to be interrogated and point Nipper at the file location and Nipper will identify the device from its contents. Or they can specify a directory where multiple files are stored and create a single report on all of them. Designed to suit all organizational requirements, four levels of auditing and reporting are available to choose from.

The security audit covers more than 20 key areas, including administrative access, authentication, IDS/IPS, SNMP, port configurations and software vulnerabilities. For maximum flexibility, the IT team can enable or disable each as required and also apply filters to fine-tune the information they want to see.

Another valuable feature of Nipper is support for v2 of the CVSS (Common Vulnerability Scanning System) open framework. Prior to generating reports, cybersecurity professionals can select CVSS and also configure other associated environmental metrics if they wish to do so. These include settings for CDP (Collateral Damage Potential), target distribution, as well as confidentiality requirements, enabling users to define and prioritize which areas are most important to them.

"Nipper is easy to set up and implement - 'straight out of the box' it makes regulatory compliance a clear and efficient process."

Reporting and visibility

For the international airport's IT team one of the most appealing aspects of Nipper was its reporting capabilities, giving them the tools to communicate with people at all different levels and in a variety of roles. Reports can be quickly produced to include raw data if required by the technical team, as well as more top-line information for the wider audience beyond the IT team, with summaries, graphs and other visual breakdowns to aid the reader in digesting its contents.

Describing the level of information in the reports as "remarkable" the airport team say they can clearly and succinctly highlight security issues within their network, provide an impact assessment and expose any potential security breaches and recommendations for remedial actions. Any other areas for concern are clearly highlighted and each is graded for overall impact and ease of remediation, empowering the team to quickly prioritize tasks. Where a problem can be fixed through the command-line interface for a device, a list of all the relevant commands is provided, so that the team can fix the issue without having to rummage through the device's user manual. The team can also generate comparison reports to see whether unauthorized changes have been made to critical devices.

"The level of information in the reports were remarkable."

Aviation Industry
International Airport Case Study

Results

The level of automation and efficiency Nipper can provide enables the IT team to focus on more strategic, higher-level issues rather than wasting time investigating every false positive or manually complying with regulations.

The ease and clarity of reporting also means that the IT team can now spend less time identifying any potential issues and can easily prioritize what needs to be done. The visual breakdowns in the reports also enable better communication with senior colleagues and non-IT staff.

As well as the benefits at an organizational level and of adhering to government regulations, having robust cybersecurity processes in place signals to other stakeholders that the international airport takes data protection extremely seriously. Customers are increasingly sophisticated when it comes to the safety of their data and want to know that they are in safe hands, particularly when it comes to something as important as international travel.

In an increasingly competitive and tough environment for the travel sector, being able to provide customers with this peace of mind is a key element of maintaining commercial success.

Why we chose Titania Nipper

- **It supports an impressive range of firewalls, switches and routers**
- **Installation takes minutes**
- **Auditing is a straightforward two-step process**
- **The security audit covers more than 20 key areas, including administrative access, authentication, IDS/IPS, SNMP, port configurations and software vulnerabilities**
- **The sophisticated reporting makes regulatory compliance easier and more efficient**
- **Reports are well structured and clear**
- **It's an informative, valuable and cost-effective solution.**

"The level of information in the reports is quite remarkable. Not only do they clearly highlight security issues with firewalls, but also provide an impact assessment, potential security breaches and recommendations for remedial actions".

For more information about how Titania Nipper can support you and your organization, access your free trial today.

"Reports provide an impact assessment, potential security breaches and recommendations for remedial actions."

Try it now for 30 days titania.com/register/trial