Pioneer Telephone Uses Rapid7 InsightIDR and Nexpose to Unite Disparate Departments and Networks

Pioneer Telephone has operated in the telecom space for over 60 years, with traditional telephone service, broadband, and wireless covering large portions of Oklahoma and Kansas. Chad Kliewer, in turn, joined the company two years ago and became its Information Security Officer shortly thereafter. He was tasked with implementing an overall security plan for the business, as well as ensuring compliance standards were being met.

To do that, he needed to bring together multiple groups across the organization, including corporate, the telephone business, and broadband, to build one cohesive infrastructure. One additional hurdle? This needed to be done without a centralized IT group in place.

"I'm a security team of one," Chad says. "In addition to implementing a program, I'm also the one keeping an eye on it. I don't have a team available to set things up and monitor it all day. I need the analytics to bring to light what's important and what's not."

For Chad, that's where Rapid7 InsightIDR and Nexpose come in.

"They bring all those areas together and provide one big view all at once," he says.

Connecting the network

Chad laid the foundation for Pioneer's infosec program based on the NIST Cybersecurity Framework for Critical Infrastructure. The first step was determining the assets he was working with.

"You can't protect what you don't know you have," Chad explains. "With the number of different groups Pioneer has, there are numerous types of devices connecting to our network. It's been a huge undertaking."

Before Chad, there wasn't a formalized scanning process. Chad brought on Nexpose, Rapid7's leading vulnerability management solution, and discovered around 6,000 total network assets and a slew of vulnerabilities, some of which even the manufacturers didn't know existed.

When prioritizing where to start and what to fix, Chad saves time with dynamic asset groups within Nexpose. Unlike trying to get next steps implemented at a corporate level, which can take time, Nexpose allows Chad to go in, create his own groups, and say "okay, I want to see everything that has a risk score of over 800,000 and we're going to start whittling down on those." From there, Chad sends the results over to the desktop team to start

Industry:	Telecommunications
Company Size:	570 employees
Products:	Nexpose, InsightIDR

> "I don't have a team available to set things up and monitor it all day. I need the analytics to bring to light what's important and what's not."

knocking off the machines listed in the automated Top 10 Remediations Report.

For example, Pioneer is in the process of rolling out Office 365. "We created an asset group and could see that we had 33 Office

2007 installations and 124 Office 2010s, that needed to be updated," he says. "Now we know exactly what needs to be updated, whereas before we were just guessing."

An added benefit Nexpose provides Chad is the ability to see which vulnerabilities have Metasploit modules available, so he can validate if those vulnerabilities pose a real risk in their network context. As some may already have compensating controls in place, such as firewalls or antivirus, Chad can prioritize fixing vulnerabilities that pose real risk. Overall, Chad says Nexpose has opened some eyes at Pioneer, giving visibility into problems they didn't know they had, and assigning numbers to the problems they did know they had. Now, they're able to judge and value them against each other, and set up a plan of attack to tangibly reduce their attack surface with confidence.

Getting real-time insight

Beyond vulnerability management, Chad loves that Nexpose scan results integrate right into InsightIDR, Rapid7's technology for incident detection and response. InsightIDR automatically detects the top attack vectors behind breaches and combines SIEM, UBA, and EDR capabilities to leave attackers with nowhere to hide. In the months Chad has been using InsightIDR, they gained visibility into users not adhering to set security policies.

"When I saw I had 30 some odd users that showed they were in Oregon, when they're not, I started digging," Chad explains. He found that several employees were using an unapproved email application on their mobile devices, which meant emails and credentials were being stored in an unknown environment. InsightIDR provided the information needed to contact the individuals and remediate the situation quickly.

As for the included endpoint detection and visibility, Chad's continuing to roll out the Insight Agent.

"I like that it can communicate directly with the platform, so I have visibility into my machines even when they're not connected to the corporate network. It's one of my favorite things," he says.

This is essential for Pioneer, which has a lot of technicians working in the field. An added bonus is that the Insight Agent can also pull vulnerability data for Nexpose, so only one agent is needed for both use cases.

To do his job effectively, Chad relies on having the analytics he needs, when he needs them. As a team of one, he doesn't have time to wade through false-positive alerts or parse through raw logs across his environment. InsightIDR serves up high-fidelity, low-volume alerts on important network happenings. During investigations, Chad can bring together real-time user behavior, log search, and endpoint data to find answers fast.

"I like the log search and the ability to bring in logs from anywhere. Not just from supported sources, but from any source," he says.

A more unified future

As Pioneer's ISO, Chad is expected to show value and metrics regarding the company's networks and overall security, and he's confident these tools will help him do that. He has also started playing around with Nexpose Now, the cloud-based Nexpose dashboard that provides real-time scanning and analytics. Chad says that while he's just started adjusting his dashboards, he thinks Nexpose Now gives an even better view into his assets.

Overall, Chad says that Pioneer has historically operated as three or four separate companies, groups that previously had little visibility into each other. But that's starting to change.

"Bringing everything together from different departments and networks into one view has been a challenge. Using Rapid7 InsightIDR and Nexpose however, has definitely made the process easier."

About Pioneer Telephone

Pioneer Telephone Cooperative, Inc., an industry leader in rural telecommunications services, is a multi-service telecommunications corporation providing communications products and services to more than 150,000 subscribers/customers in 76 communities encompassing 30 Oklahoma counties in Western Oklahoma. Pioneer provides an array of telecommunications products and services, including Local Telephone Service, High-Speed Internet, Ethernet Transport Service (ETS), Digital TV, Cellular, Long Distance, Wireless Broadband, Security Systems, Business Solutions and Yellow Pages Advertisement. This institution is an equal opportunity provider and employer. For more information about Pioneer, please call 1.888.782.2667 or visit our website, www.ptci.com.