INDUSTRY:
Telecommunications

SIZE:
600 employees

PRODUCTS:
InsightVM
InsightIDR
Metasploit Pro
AppSpider Pro

Pioneer Telephone Leverages the Rapid7 Insight Agent to Ease Management, Improve Visibility

CHALLENGE

- The ISO was tasked with monitoring a large, mobile workforce with over 5,000 endpoints and historically siloed business groups.

- There was a lack of visibility into network devices, coupled with an FCC mandate to provide evidence of running a security and risk program.

SOLUTION

- Rapid7's Insight Agent automatically collects data from all endpoints in InsightVM and InsightIDR to maximize visibility and control.

- The live dashboards in InsightVM enable the ISO to visualize remediation and asset risk scores over time, ultimately tracking their security progress.

Pioneer Telephone Cooperative, Inc. is a rural communications provider with a 60+ year history. It offers telephone, internet, DSL, and carrier ethernet, alongside digital TV and cellular services to businesses and residential customers in Western and Southwestern Oklahoma and Southern Kansas. The company continues to grow to this day, with over 150,000 subscribers/customers and 600 workers across 27 locations.

Chad Kliewer, the information security officer (ISO) at Pioneer, has a role complicated by a large mobile workforce, 5,000+ endpoints to manage and secure, ongoing compliance requirements, and a corporate structure comprising multiple siloed business groups.

Telcos under fire

As a telecommunications provider, Pioneer is part of US critical infrastructure, which is increasingly being probed by organized cybercrime gangs and nation states. In addition to these attacks, is the constant threat of customer data theft and ransomware that many organizations face today.

That's partly why industry regulators have been tightening their requirements of late. The FCC issued an order demanding that all telecoms and broadband companies provide evidence of running a security and risk program. There was just one problem for Kliewer: before Rapid7 he had little visibility into any network devices. First using Nexpose, Rapid7's on-premise vulnerability management solution, and now InsightVM, the cloud-based version that leverages the power of the Insight platform, has helped him to compile an accurate inventory of assets and then manage risk on those assets.

As mentioned, Kliewer also had the challenge of gaining visibility and control of endpoints in a company still segmented into various groups, across a large remote workforce. He's also in the process of improving the incident response and disaster recovery plan, which requires the documenting and managing of key assets.

> "With the [Insight Agent] ... I can still assess threats on machines even when employees are outside the corporate network."

Why InsightVM?

Kliewer already had InsightIDR, Rapid7's incident detection and response solution built on the Insight platform, working alongside Nexpose, so the upgrade to InsightVM was a no-brainer. InsightVM provides real-time data and remediation capabilities to help organizations better manage, prioritize, and mitigate risk. Having a single Insight Agent to manage both InsightVM and InsightIDR has eased management considerably—an important point considering Kliewer works in a security team of one, so anything that can boost productivity is a bonus.

The Insight Agent automatically collects data from all endpoints, even ones that can't actively be scanned. That's significantly improved visibility and control for Kliewer, who says at least 20 percent of the workforce are out in the field at any given time, and may not connect to the corporate network for a month.

"With the [Insight Agent] … I can still assess threats on machines even when employees are outside the corporate network," he says.

Cutting complexity, delivering insight

Even more importantly for Pioneer, InsightVM has finally helped Kliewer gain a full picture of all his network assets and their risk profile.

"We have a lot of different equipment; it's not like I can look at a CVE listing and know exactly what I've got," he explains. "That's what InsightVM helps me with: to be able to nail that stuff down, know what assets I have out there, and whether any of those new vulnerabilities actually apply to me, without having to dig around or rely on someone else."

Two other key features Kliewer has been putting to good use are the threat feeds and dynamic asset groups:

- **Threat feeds** allow Kliewer to work more efficiently. "Threat feeds help me know what is exposed to the outside world and is being exploited, so I know where to prioritize," he explains.

- By setting up **asset groups**, Kliewer has also been able to expedite the remediation of endpoints by other groups within the business, ultimately streamlining a process previously done via spreadsheets which he admits were "always out of date."

"One thing I've been able to do is set up an asset group to target exactly what I want fixed, and I can give the team a direct link to that asset group and say 'this is what I expect you to fix, this needs to be zero,'" says Kliewer. "That way we're not going back and forth with spreadsheets trying to figure out what's going on."

Reducing risk

Another reason for choosing Rapid7 was its support for two key security control frameworks used by Pioneer: the NIST Cybersecurity Framework and CIS Top 20.

"InsightVM helps to trend over time and show that vulnerabilities are being addressed and remediated with a clear goal, showing an active security framework without the 'check box' mentality of a compliance program," says Kliewer.

Detailed dashboards have helped him visualize this progress. Although Kliewer hasn't used any bespoke reports to measure the success of the program thus far, he's been able to track the risk score versus number of assets via these high-level graphical displays. From there, InsightVM enables Kliewer to go in and tell each business group what areas they need to prioritize. He's also using the product to scan and harden any new devices before they're deployed, further reducing the company's risk exposure.

With InsightVM, Pioneer was able to measure a milestone: a risk score lower than the total number of corporate networked assets. With InsightVM and InsightIDR leading the charge, the telco will be looking to hit many more key goals going forward, as it gets smarter and more effective at managing endpoint risk.

"InsightVM helps to trend over time and show that vulnerabilities are being addressed and remediated with a clear goal."