HORIZON3.ai

~~TRUST BUT~~ VERIFY

CASE STUDY

Public University Uses NodeZero to Close Gaps, Prove Value of Cybersecurity

@Horizon3ai info@horizon3.ai www.horizon3.ai

Public University Uses NodeZero to Close Gaps, Prove Value of Cybersecurity

One of our customers, a public university in Victoria, British Columbia, is constantly looking for ways to improve their overall cybersecurity posture – and has started using NodeZero's autonomous pentesting capabilities to keep their students, faculty, and data safe.

Speaking with us was the University's Senior IT Security and Risk Specialist, a role that didn't exist until 2017. Like many organizations, the importance of cybersecurity needed a champion in-house to bring it to the top of mind.

"Before that, there wasn't someone dedicated to security, and virtually no policies for cybersecurity at all," he mentioned. "My role as the sole security person here touches all areas from proposing and drafting policies, to firing up the Zeek server to look at the logs, look for strange traffic, and everything in between."

Since joining, he has been working on aligning the university's cybersecurity policies with industry best practices in a number of areas, and instituted a handful of programs to address vulnerability management and user management.

A while back, the organization ran into a situation where there were an abundance of minor account compromises that cumulatively turned into a hassle for everyone involved. Taking the lead, the risk specialist started building out awareness training, advocating basic policies and building an expectation of some basic cyber hygiene.

> **We started to reduce the number of those kinds of incidents, which also worked out well as that was right around the time we had a few minor ransomware incidents**," he said.

"But because I'd done that work with the business units (developing better awareness and preparedness), we were able to resolve those incidents quickly."

This also led to the university realizing it needed someone in that security role full-time.

NodeZero as a Difference Maker

The university wanted to do some penetration testing to get confirmation that the changes they'd been implementing were working and to identify any security gaps that might remain.

"I took advantage of some pre-negotiated contracts in place by our being a public body, and asked vendors for some quotes. After my heart restarted after seeing the quotes, I just happened to get an email from the Horizon.3ai sales team and said, 'ok let's take a look at it'," said the risk specialist. "I saw the ability of NodeZero to do what I needed to do at a similar cost, but also with the ability to repeat that find, fix, verify process and customize the testing the way I wanted it done."

That flexibility and the find, fix, verify loop really drew him in during the initial test.

"That's really what we wanted to do," he said. "The way Horizon3.ai is set up allows for that. It shows where problems are and provides guidance on what we need to do to fix it. It has the right philosophy, as opposed to just asking: what can we break into? I can get a kid from high school to hack away at our network, but the question is, how do we fix it?'

He also found that the ability to do multiple pentests is a huge benefit.

"It was a breath of fresh air. I can repeat this!" he said. "When one network segment showed some interesting vulnerabilities, I was able to fix them and repeat the test to verify that things were much better."

This was the difference from traditional pentesting options, where it would cost thousands of dollars and take weeks, if not months, to bring a team in to test and assess every time.

Improving Credentials Hygiene and Beyond

NodeZero was particularly helpful in addressing the common struggles associated with credentials hygiene and patching.

"We have people who felt that having a nice, long password meant nobody would ever guess it. We're now able to show that's not true," said the risk specialist. Character count matters, but is ineffective when it's reused from a previous breach or is a simple string. NodeZero provides password analytics from the NTDS database in their domain, pinpointing exactly where their credential policy is effective.

NodeZero was also able to help with vulnerabilities that were consistently getting flagged as weaknesses in scans.

"Those vulnerabilities became a pivot point – we now have proof that there's a vulnerability, here's what happens when it exists, now let's fix it," he said.

It helps minimize pushback and enabled him to offer proof to higher-ups. By reporting on vulnerabilities or other cybersecurity issues so that everyone in a leadership role is seeing it at the same time, everyone knows what needs to be fixed – which helps foster cooperation to help those improvements move forward quickly and easily.

Deciding on NodeZero

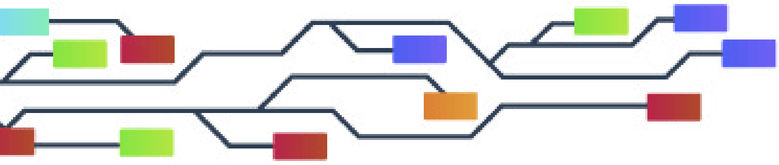
The University did look at other, traditional pentesting options as well as NodeZero before signing on.

"Typically, they were security companies that had a standing contract with our provincial government," said the specialist. "I didn't look at anyone doing it autonomously the way NodeZero does it. I saw the chance to spend the same money but gain more capabilities."

Coincidentally, the opportunity for a trial run came up at the end of the fiscal year and there was some budget left which enabled him to show leadership of the value of NodeZero.

"The reports enabled my CIO to show the executive team that we're being proactive and taking the steps our board wants us to take, and we can demonstrate we're taking positive action to secure our environment," he said.

The IT and Risk Specialist has been very impressed not just with NodeZero as a tool, but also by the team behind it.



"I'll tell you, the support is phenomenal," he told us. "I can't tell you how many times I've been in the middle of an op and the chat bubble pops up because someone is there and concerned that I'm having an issue. It takes customer service to the next level."

The team's proactive approach has made a big difference.

> **I've come in to work in the morning and found an email from someone at Horizon3.ai letting me know they'd reviewed our ops, found a vulnerability, and let me know how to fix it,**
>
> he said.

And then there's the overall ease of use NodeZero offers.

"Setting up an op is simple. It's so easy an old guy like me can do it, and it not only tells me what's broken but how to fix it," he remarked. "It shows the attack chain, how it got in, how to fix it, and then I can use that to demonstrate to others what needs to happen. We get the attack chain, proof, and how to fix it, all in one package."

If you'd like to see how NodeZero works with your organization, have our experts walk you through a demo

https://www.horizon3.ai/demo

HORIZON3.ai

~~TRUST BUT~~ VERIFY