HORIZON3.ai

~~TRUST BUT~~ VERIFY

CASE STUDY

Higher Education Institution Finds Easier, Better Scanning with NodeZero

Higher Education Institution Finds

Easier, Better Scanning with NodeZero

When the Desert Research Institute (DRI) of Reno, NV, a higher education organization focusing on applied environmental research, needed a way to run penetration testing and vulnerability scanning at an affordable cost, they found NodeZero.

“DRI is a soft money funded organization, so we are always budget focused, and what drew us to [Horizon3.ai] was the ability to get a full featured, easy to use pentest program at a price we can afford. The fact that NodeZero is autonomous makes things significantly easier,” says Ryan Coots, Information Security Officer with DRI. “We don’t have to pay a red team to do an expensive, in-person comb-through of our security controls.”

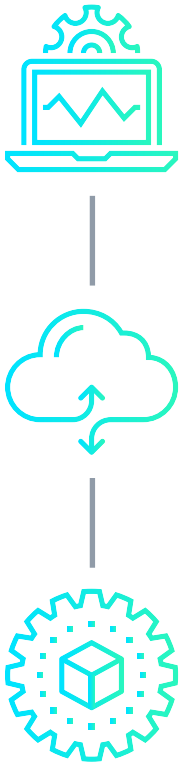
DRI had used other products before, but found that after a one-year deal, the price would jump to an unaffordable price point.

“And then we’d have to start over with a new tool,” says Coots.

DRI has a highly segmented environment with approximately 100 different subnets, giving them about 5,000 IP addresses across all their networks and campuses. NodeZero has helped with keeping their network secure, as well as improving visibility across the board.

“We have a couple of non-centrally managed IT groups at DRI that have the ability to spin up their own network servers, and we don’t always have deep visibility on those machines. Where NodeZero helps us here is we can now scan those servers, find exploitable vulnerabilities and misconfigurations, and work with those groups to remediate them,” says Coots.

Where NodeZero Excelled



DRI looked at several competing products, all of which were strictly vulnerability scanners.

"NodeZero is more of a pentest tool that uses vulnerabilities to try and exploit actual gaps that exist in systems," says Coots. "The difference is NodeZero takes it one step further to try to actually carry out an attack in a safe manner. As this is all done via A.I. and an easy-to-use dashboard, this serves our needs well."

Other products simply scan against a database of vulnerabilities, he says.

"Additionally, NodeZero looks for weak credentials and other holes, vulnerabilities, or misconfigurations an attacker could use to break into the system," says Coots, whereas NodeZero has a more complete process.

"It's very easy to set up and use, very affordable, and has very few issues with penetration testing and scanning," he says.

Another benefit to NodeZero: while it runs an intense test, it doesn't tax resources or interrupt the workflow of the end users, which DRI had found with other products.

"Other scans are very aggressive and in-depth and can knock out a system or cause a disruption – we haven't had that with NodeZero," says Coots.

The Benefits of External Pentesting

DRI was quick to make use of NodeZero's external pentesting option when released in early 2022.

"That was a huge help," says Coots. "Previously we had to coordinate with an outside group or even pay to have our public subnets externally scanned. The ability to launch my own external pentest has been extremely useful to us. We've already run one with great results, remediated any issues and then verified the remediations worked. That ability to verify a fix is one of the biggest features for us."

As a Design Partner, Coots had shared the desire for external pentesting with the Horizon3.ai team previously, who he says is always responsive and open to suggestions and feedback.

How DRI uses NodeZero

Coots has enabled a small, junior team to run NodeZero pentests, but all of IT has read-only access so they can review the hosts, operations, and remediation options. This fosters relationships between the IT staff and helps them focus on security.

> **They can see: Here's a vulnerability, here are the remediation options, and here's why we should go fix it,** says Coots.

One-click verification of remediation has been a significant benefit for ensuring when something is fixed, it truly is fixed, explains Coots.

"There is no more 'I think I've fixed this issue' – now we run a 1-click verify op and confirm that it's fixed," he says.

The short learning curve to use NodeZero has helped make it a success for DRI, Coots explains.

"It's pretty much; you have a Docker instance, you give it an IP range to scan, and off it goes – the automation is critical when you have a small staff," he says.

This has enabled DRI to run pentests more often. They've been running 40-plus tests monthly at this point, and Coots is working on a recurring quarterly schedule.

"I scan 100 different network segments a quarter, when the scans are complete, we then combine the results into a spreadsheet and sort by severity which is based on how NodeZero classifies them. We're able to start from the top down and remediate," says Coots.

Coots uses NodeZero to improve the scanning process for DRI's highly segmented environments. Since NodeZero is fully containerized, it is portable and easy to configure for multiple network segments. This allows Coots to scan segments as if there were no protections in place in each segment.

"With the setup now, I take the firewall out of the equation," says Coots. "I put the NodeZero container in the same subnet I am scanning, and because the scan is contained within the same network segment, it doesn't trigger the firewall which would normally limit the results of any vulnerability or pentest scan. The result is a much more in-depth scan and a real look at vulnerabilities and exploits within a network segment. We're able to get significantly more information out of each operation."

How NodeZero Can Help

- For more information on NodeZero's functionalities through continuous autonomous penetration testing, visit

www.horizon3.ai/nodezero