GETTING OUT OF THE CYBERSECURITY BUSINESS IS THE SMARTEST DECISION A CISO CAN MAKE

With an estimated 3.5 million cybersecurity positions going unfilled by 2021, **according to recent research from Cybersecurity Ventures[1],** it's near impossible to hire and retain the experts needed to keep up with increasingly sophisticated cybersecurity threats 24x7. This leaves many organizations desperately trying to ward off threats with a patch-work of DIY solutions that all fall short.

In 2019, the College of Southern Nevada (CSN), a public college with 37,000+ students on multiple campuses, found itself in a dilemma. Its efforts to bolster security had resulted in spiraling costs and an unmanageable technology stack.

> **With the Open Systems solution, we no longer need to be in the tactical day-to-day security business.**
>
> **Mugunth Vaithylingam,** CSN CDxO

WHY CHANGE?

- Difficulty hiring security staff
- Budget stress from point solutions
- DIY security not cutting it

THE NEW REALITY

- Unified solution: SASE SD-WAN + Microsoft Azure Sentinel + MDR
- 24x7 SOC

WHY IT'S BETTER

- Direct 24x7 detection, investigation, and remediation of threats
- Consistent costs reduce budget stress
- Ability to focus on student, faculty, and staff technology experience

"Due to the complexity of all the cybersecurity solutions we were using, it had become hard to hire, train, and keep security professionals. We were in firefighting mode," says Mugunth Vaithylingam, Chief Digital Experience Officer (CDxO) at CSN. "I routinely had to ask our CFO for additional funds to buy new security products I was assured were needed urgently to prevent breaches."

Yet when Vaithylingam inventoried the CSN technology stack, he found some of the security gear had never been implemented, configured optimally, or updated. Worse yet, many items were reaching end of life. "It was a budgeting nightmare, and I wasn't confident that we were as secure as we should be."

Allowing this situation to continue was not an option. With ever-tightening budgets, a wealth of personal and research information, and countless unsecured personal devices, higher education is a top target for cybercrime.

Vaithylingam knew things had to change. It was time to get out of the security business.

GOODBYE DIY, HELLO SECURITY-AS-A-SERVICE

Choosing to outsource his security operations was not an easy decision, but Vaithylingam knew he had made the right call after learning about Open Systems' Managed Detection and Response (MDR) service. Its combination of continuous 24x7 monitoring, AI automation and veteran security engineers made it the ideal solution to CSN's security issues.

"With the Open Systems solution, we no longer need to be in the tactical day-to-day security business," says Vaithylingam. "Instead, we manage the partner and focus on strategic security issues, like setting up the proper governance and educating the CSN community on best practices."

VIRTUAL IMPLEMENTATION, IMMEDIATE RESULTS

CSN signed its contract with Open Systems in March 2020, at the height of COVID-19 quarantines. Working together, the teams were able to conduct a fully remote implementation, including Secure SD-WAN as part of CSN's shift to a SASE architecture. Within a few months, all hardware had been replaced, solutions baselined, and the entire setup nearly ready to launch as a full managed security operations center (SOC).

With Open Systems helming the full SASE architecture, which includes Secure SD-WAN and MDR, engineers have unparalleled access to help CSN discover, investigate, and thwart threats. Rather than simply alerting Vaithylingam's busy team to suspicious activity – which wastes time and can open the door to

> "It was [an] intelligent decision. We have one dashboard where we can see the threats that are coming through. There were a couple of different incidents that were detected that we wouldn't have found any other way. When we were alerted by Open Systems, our team dug in and figured out what was going on."
>
> **Mugunth Vaithylingam,** CSN CDxO

increased damage – Open Systems can remediate threats immediately, based upon a preapproved incident response plan.

"If anything goes wrong, they can triage it immediately or co-manage it with our CSN team," says Vaithylingam.

For example, in the early stages of implementation, they prioritized Endpoint Detection and Response (EDR), given the plethora of student, staff, and faculty devices on unsecured networks due to remote learning and working during the pandemic. The Open Systems team found network activity that called for a deeper investigation by their team. Previously, the activity may have not been found or investigated quickly, due to the stream of alerts that CSN's small IT staff had to keep up with on top of its other work.

With the MDR service up-and-running, Vaithylingam has found peace of mind, confident that CSN's security needs are in good hands. Adding to his newfound calm is the predictable cost of the service and the knowledge that he won't need to ask his CFO for more funds each quarter.

Open Systems' ability to detect and respond to threats 24x7 is even more critical as the CSN IT staff turns its focus to create an excellent online learning and working environment for its community, as well as security governance and best practices.

"As we prepare to fully engage with Open Systems, we look forward to focusing on a long-term security strategy, knowing that Open Systems' technology and engineers are there to keep noise to a minimum, identify real threats, and work with us on response," says Vaithylingam.

[1] **"Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021," Cybercrime Magazine, October 2019, https://cybersecurityventures.com/jobs?mc_phishing_protection_id=45427-c079ptuuab2voeh0q2d0.**