COLLEGES IN THE CROSSHAIRS: AFFORDABLE PROTECTION THAT DETECTS AND RESPONDS

Each day at the College of Southern Nevada (CSN), the state's largest college with 37,000+ students and multiple campuses, Chief Digital Experience Officer (CDxO) Mugunth Vaithylingam acknowledges that cybersecurity incidents are not just a threat, but an inevitability.

He has to be this candid. In the 2019–2020 academic year, education was the top target for Trojan malware and adware, and the second-most desired target for ransomware[1].

> Due to the complexity of the cyber-security solutions we were using, it had become hard to hire, train, and keep qualified security professionals.

Mugunth Vaithylingam, CSN CDxO

WHY CHANGE?

- Unable to keep up with threat alerts
- Difficult to hire qualified security staff
- DIY security solutions not optimized well
- Needed 24x7 threat coverage

THE NEW REALITY

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

WHY IT'S BETTER

- Unified solution provides access for immediate, 24x7 threat remediation
- Human-powered threat investigation augments Azure Sentinel data
- Customized incident response plan

Cybercriminals are opportunistic and educational institutions have valuable PII and research data, often run on outdated technology and with countless, often unsecured endpoints. This reality made his job nearly impossible until he found the right security services partner.

“Our team was spending a lot of time and focus in a firefighting mode to keep the CSN community safe and secure,” says Vaithylingam. “Due to the complexity of the cybersecurity solutions we were using, it had become hard to hire, train, and keep qualified security professionals. Additionally, DIY had become costly and difficult to manage.”

During a technology evaluation, Vaithylingam found some security products hadn’t been fully implemented, optimally configured, or updated. Many of these were reaching their end-of-life. Worse yet, visibility and detection of potential threats couldn’t be relied upon – especially not at the level of best-in-class security operations centers (SOC) that combine automation with the intuition of veteran security engineers for comprehensive 24x7 monitoring.

“I was never confident that we were as secure as we should be,” Vaithylingam said, acknowledging that the IT team had no way to tell what was slipping through the cracks.

RAPID RESPONSE WITHOUT A RAPIDLY INCREASING BUDGET

With the college’s data and reputation on the line, Vaithylingam wasted no time in searching for a solution to the college’s security management and cost issues. He found a savior in Open Systems. In addition to providing threat detection, the company offered a full SASE solution and the ability to respond to threats – at a price that fit his budget.

By stacking Open Systems’ Managed Detection and Response (MDR) service with its Secure SD-WAN, CSN was able to outsource an entire SOC to Open Systems for far less than it would cost to build one internally. Because Open Systems also provides the Secure SD-WAN, its engineers can directly access it for immediate threat response, based upon a preapproved incident response plan. This saves time and, potentially, damage. Open Systems’ MDR is also built on the Microsoft Azure Sentinel SIEM, which helps customers like CSN optimize their investments.

“Open Systems comes in and replaces all the hardware and manages it. Their ‘eyes on glass’ are level-3 engineers with a collective 500+ years of experience. If anything goes wrong, they can triage it immediately and/or co-manage it with the CSN team,” says Vaithylingam. “I strongly believe that no educational institutions should be managing their own security operations centers or data centers.”

> “Open Systems comes in and replaces all the hardware and manages it. Their ‘eyes on glass‘ are level-3 engineers with a collective 500+ years of experience. If anything goes wrong, they can triage it immediately and/or co-manage it with the CSN team.”
>
> **Mugunth Vaithylingam,** CSN CDxO

[1] Malwarebytes Labs, “Trojans, ransomware dominate 2018-2019 education threat landscape,” August 14, 2019

GOOD-BYE TACTICAL RESPONSE, HELLO MORE STRATEGIC SECURITY

CSN signed its contract with Open Systems in March 2020, at the height of the COVID-19 quarantine. Working together, CSN and Open Systems conducted a fully remote implementation, including the new SD-WAN. Within a few months, all hardware was replaced.

Different solutions, such as Network Detection and Response (NDR) and Endpoint Direction and Response (EDR), were baselined, a preliminary step that allows the Open Systems team to separate signal from noise so that only legitimate threats are escalated. Some previously undetected threats were even found at this stage.

The teams are currently working on incident response plans, so that CSN can determine the exact level at which it wants its IT personnel to be involved. With the triple implementation of moving to an SASE architecture that includes Secure SD-WAN, MDR, and Azure Sentinel, Open Systems can provide 24x7 service far beyond threat recognition and alerts. Its security analysts research threat alerts, provide reports that augment the raw Azure Sentinel SIEM data, and can immediately remediate network threats – even if they originate outside of the network.

Vaithylingam is happy with the results. By getting out of the tactical side of security and simplifying management of network and cybersecurity operations through one partner, his team can focus on other ways to reduce threats, such as governance and educating the CSN community on best practices. Says Vaithylingam, “Now we have one partner with global operations to monitor our network and stop attacks in real time.”

Open Systems is a groundbreaking cybersecurity company delivering an experience way beyond expectations. Our obsessive care for our clients' businesses has led us to reinvent how cybersecurity is delivered to fit today's mobile, cloud-based world. Our team, based in North America, Europe, and Asia, consistently provides crazy good cybersecurity to leading organizations all over the world.

Learn more at **open-systems.com** |