splunk> a CISCO company

CASE STUDY

UNLV Hits the Jackpot with Student SOC and Splunk

Key Challenges

With a limited cybersecurity staff and resources, UNLV needed a creative solution to keep its campus community secure while providing an exceptional educational experience for its students.

Key Results

Trained through the Splunk Academic Alliance, students in UNLV's SOC are gaining hands-on security experience while remediating critical vulnerabilities in the university's digital environment.

UNLV

Industry: Higher education, Public sector

Solutions: Security, Platform

Products: Splunk Cloud Platform, Splunk Enterprise Security, Splunk Academic Alliance

Viva the University of Nevada, Las Vegas!

The University of Nevada, Las Vegas (UNLV) is a premier research institution and oasis of knowledge in the heart of the Mojave Desert. With a security team of only four full-time security operations center (SOC) analysts, UNLV needed additional support safeguarding its complex digital environment for its 35,000 students, faculty, and staff.

"We want to do everything we can to keep the school secure," says Jason Griffin, senior information security analyst for UNLV Information Technology. "And from an academic standpoint, we also want to provide opportunities for cybersecurity students to gain essential knowledge and experience for when they enter the workforce." With the help of Splunk Enterprise Security, Splunk Cloud Platform, and Splunk Academic Alliance, UNLV is doing just that.

Outcomes

600+
vulnerabilities remediated in first 6 months

Significant
visibility increase into their hybrid environment

100%
job placement post-graduation

SIEM City

Launched in 2022, UNLV's SOC program gives cybersecurity students real-world SOC experience and essential workforce development skills, including responding to alerts, correlating tickets, prioritizing incidents, and resolving critical vulnerabilities. And their efforts are paying off. "We've substantially increased visibility in our vulnerability management program through Splunk dashboarding and alerting," says Griffin. "Since May of 2024, the students have remediated over 600 vulnerabilities, with nearly 100 of them critical." So while UNLV students get smarter, the school gets safer.

"When we started, this was a manual process of logging into multiple platforms, manually examining the data or results of the scan, and then creating the ticket, hoping there wouldn't be duplicates or errors," says Griffin. Now, UNLV SOC analysts leverage Splunk Enterprise Security to ingest and correlate data for various operational use cases. Any suspicious activity in their network triggers a notable event, which initiates further investigation. Griffin and his team are working toward having Splunk automate this process by ingesting the data from multiple sources, correlating it, and using workflow actions to connect to their ticketing system. "Those vulnerabilities used to take twice as long to remediate as they do now," continues Griffin. "And when we fully implement the automation, it will cut that time to one-tenth."

Built-in features like adaptive response have also been game-changers since using them for additional drill-down searching enables the student analysts to get more granular. Having preconfigured options and the ability to access external sites also streamline processes.

"Splunk Enterprise Security has significantly increased our visibility," says Griffin. "We went from knowing things were happening in our environment to being able to see everything and address them as they come up. We've entered a world where detection is now possible."

"With Splunk Enterprise Security, not only has our university's security posture improved, but the academic experience has as well," says UNLV Chief Information Security Officer Vito Rocco. "Providing students with hands-on experience in a real SOC broadens their horizons and opportunities once they enter the workforce."

UNLV Chief Information Officer Kivanc Oner, who works with Rocco seeking grants and approvals from the state, agrees, adding: "Not only does this program empower our students with cutting-edge skills, but it also strengthens Nevada's cybersecurity landscape as a whole. By training the next generation of cybersecurity leaders, we're ensuring the state's digital future is in capable hands. Splunk is a critical partner in this mission, helping us bridge education and real-world application."

> With Splunk Enterprise Security, not only has our university's security posture improved, but the academic experience has as well. Providing students with hands-on experience in a real SOC broadens their horizons and opportunities once they enter the workforce."

Vito Rocco, Chief Information Security Officer, UNLV

It goes without saying that these students are hard at work, earning up to 1000 hours of hands-on SOC experience over the course of a single year. Not surprisingly, UNLV's SOC program boasts a 100% job placement rate post-graduation. According to Griffin, the vast majority of students continue to work in cybersecurity — from major retail companies to the U.S. military — and all of them leave with their Splunk Core Certified Power User certification. "The students and their drive as a part of this program and their desire to use Splunk and understand what a great tool it is culminates in this exceptional opportunity," he says.

UNLV Rebels make it happen

In addition to running and overseeing Splunk Enterprise Security for the UNLV campus community, Griffin teaches graduate-level security data analytics courses through the Splunk Academic Alliance. "I was introduced to the program and the opportunities Splunk provides for students at .conf2021," says Griffin. Initially offering the Academic Alliance training as an optional, extended portion of his curriculum, Griffin made it a core part of his syllabus the following year. "I teach analytics on Mondays and Splunk on Wednesdays," he continues. "I always pull concepts from what I discuss in analytics and relate them to the Splunk lesson."

And it's not only UNLV students who reap the benefits of the Academic Alliance program. University employees are also getting schooled in Splunk. "Right now, we're actually training our cybersecurity team through the program," says Griffin. "I stay very refreshed in the material because I want to stay current, as well. It's twofold."

Ahead in the cloud

The campus cybersecurity team isn't the only one benefiting from Splunk. UNLV Information Technology Senior 2 IT Operations Analyst and Supervisor Jeremiah McClain has been a Splunk on-prem user since 2010. During that time, McClain witnessed the UNLV network grow from a single server to a clustered system and needed a solution to scale alongside it. That's why he recently transitioned to Splunk Cloud Platform.

> With Splunk, we discovered fire."
>
> **Jeremiah McClain,** Senior 2 IT Operations Analyst and Supervisor, UNLV Information Technology

"Splunk Cloud Platform makes it very easy to separate data based on use case, access requirements, and retention," says McClain. "Sometimes, we can even have a customer viewing basic dashboards within minutes." But that's not all.

"Not only will the switch to the cloud be much cheaper in the long run," says Director of IT Operations Center at UNLV Information Technology Paul Trinidad, who is the business-side facilitator of all things Splunk. "It's made it far easier for the team to focus on delivering value to the organization rather than spend a lot of time doing administrative work."

McClain agrees, adding that this value includes building dashboards and supporting Griffin's cybersecurity efforts. "We have rich visibility into the entire environment so our teams are able to work hand-in-hand," he says.

And since moving to the cloud, McClain has seen uptime improve significantly. "There's been a great increase in reliability," he says. "And it's easier to run a service that people depend on, especially our security team. We need the most robust and resilient platform we can get."

UNLV is taking care of business

Griffin and McClain hope to expand the UNLV SOC program across the state of Nevada, helping different campus communities. In the meantime, they're working hard to broaden Splunk use cases in their own backyard. From managing lines at the wellness center to prioritizing maintenance requests and ingesting research data from lab instruments, the duo sees a use for Splunk in just about everything.

"With Splunk, we discovered fire," says McClain. "What comes next?"

"We invent the wheel," Griffin responds.