splunk>

CASE STUDY

Cal Poly Drives Resilience While Training Tomorrow's Security Leaders

Key Challenges

To better protect its campus and data, Cal Poly needed a unified security platform that would give them visibility into the university's complex, hybrid infrastructure while also centering students' experiential learning.

Key Results

With Splunk, Cal Poly gained the visibility they needed to strengthen their security posture, which has increased resilience and provided students with more real-world learning opportunities.

CAL POLY

Industry: Education

Solutions: Security

Products: Splunk Cloud Platform, Splunk Enterprise Security

Cal Poly students learn by doing.

That's not by chance; it's been a core tenet of the California Polytechnic State University's founding philosophy since it was formed in 1901. In Cal Poly's Security Operations Center (SOC), which is tasked with providing round-the-clock protection from cyber threats, "it's students who provide the first, tier-one incident response," says Doug Lomsdalen, chief information security officer for Cal Poly.

But as the university began to migrate to the cloud, its security environment became exponentially more complex. Lomsdalen and his team needed more visibility into the university's distributed systems so they could quickly detect security incidents — an ability that proved especially important during the pandemic. Now Splunk Cloud Platform and Splunk Enterprise Security (ES) provide unprecedented visibility into Cal Poly's security environment and offer its students critical skills that will serve them (and their future employers) well — long after they graduate.

Staying resilient when the world changed overnight

Wanting to meet ever-increasing cybersecurity threats with expanded security capabilities, Cal Poly began its cloud journey in 2016. Though the university began to benefit from the agility that the cloud provides, its infrastructure also became more complex, limiting the ability to see into systems and fix issues quickly. Now with the Splunk platform, the university has visibility into its systems, correlating over 105GB of data from disparate sources each day to fight threats and strengthen Cal Poly's security posture. "Data is instrumental in our day-to-day business of security. If we didn't have that visibility that Splunk provides us on a daily basis, we would just be flying blind," Lomsdalen says.

This visibility was especially critical during the pandemic, when the university was forced remote virtually overnight and any blindspots could have proved catastrophic. With Splunk's tools, the team quickly and seamlessly went remote, and each staff member still had critical, real-time visibility into Cal Poly's security posture.

Outcomes

1M+
threats thwarted each day

<5 min
to respond to incidents thanks to programmatic alerts that provide 24/7 visibility

2-4
students per quarter given real-world cybersecurity experience

Student learning remains front and center at Cal Poly — pandemic or not — and student employees, under the supervision of senior staff engineers, play a key role in the university's security operations by designing, building and monitoring the Splunk dashboards that pull in critical information about the university's security posture. When the university went remote, it was vital the students continued to have access to the data they needed, whether they were in their dorm or at their kitchen table. With Splunk, the data remained at their fingertips. "Because the data never really left campus, students could still access all the tools and log sources to operate a secure environment," says Lomsdalen. During this challenging time, students experienced the importance of cybersecurity first-hand — and protected the university at the same time.

> Data is instrumental in our day-to-day business of security. If we didn't have that visibility that Splunk provides us on a daily basis, we would just be flying blind."
>
> **Doug Lomsdalen**, CISO, Cal Poly

Splunk makes the grade with best-in-class protection

Universities are notorious for being vulnerable to phishing attacks, and Cal Poly receives over a million hits a day that they consider attacks on the university. "I know the number of threats against the university is higher and the complexity greater than ever before," says Bill Britton, chief information officer for Cal Poly, who had witnessed the power of Splunk while working with the U.S. Department of Defense community. "But I also know that we're protecting the university at a level we've never had before."

Splunk Cloud Platform and Splunk ES have transformed the university's ability to detect security incidents. Since it standardizes the retention period for security-related events, Splunk ES is flexible enough to allow modifications with no interruptions in detecting security events — helping the university adapt to increasingly complex cyber threats. "Splunk allows us to be more proactive through the visibility it has given us," says Doug Lomsdalen. "By giving us that visibility, we can quickly respond to potential threats and better protect the campus."

The Splunk platform has also simplified how the security team assigns and keeps track of incident handling. "We have 10 staff and students looking at security events," Britton says, "and Splunk makes it easy to keep track of who's handling which alerts."

From campus to companies around the world

The students working in Cal Poly's SOC keep busy. But thanks to the Splunk platform's ease of use, they can spend their time doing meaningful work, not just onboarding. "Our student assistants have been incredible at getting up and running with Splunk after two weeks of training," Britton says. "We frequently assign them to add or modify Splunk dashboards, reports and alerts, as well as to enable more Splunk Enterprise Security features as we add new security event sources to Splunk."

When they're not thwarting would-be attacks on the university's environment, Cal Poly students are assisting with educational and training programs on campus and at the California Cybersecurity Institute (CCI). There, they help guide the next generation of cybersecurity professionals and set themselves up for successful careers in IT after they graduate. In fact, every recent student summer hire in cybersecurity studied for and passed the Splunk Core Certified User exam through an early adoption of Splunk's Academic Alliance Program — just another way Cal Poly delivers on its promise of real-world learning to its students.

Looking forward, Cal Poly plans to almost double the amount of data processed on the Splunk platform to stay resilient and proactive as the cyber threat landscape continues to grow in complexity and size. Students will be engaged in the effort every step of the way.

24-543931-Splunk-CalPoly-CS-102