Fourteen universities using student-run SOCs to strengthen cybersecurity skills

For all the cybersecurity challenges higher education leaders are contending with today—too many attacks with too few people to detect them, a shortage of cybersecurity skills, and too many potential open doors for cyberattackers to enter—a promising answer has coalesced to help overcome them.

That answer can be summed up in one word: students.

In at least 14 higher education institutions (see list below), a relatively new and increasingly effective type of program called student powered security operations centers (SOCs) is now being established with more likely to follow. In these on-campus, engine-room-like central hubs of cybersecurity, students are gaining real-world, hands-on experiences performing various cybersecurity tasks such as monitoring, analyzing, and responding to security incidents.

Students are not only bolstering campus cybersecurity—they're catapulting their cybersecurity career opportunities.

Student-powered SOCs also deliver much-needed cost advantages. Universities get more people detecting and preventing threats without having to spend a lot more money to strengthen their professional cybersecurity teams.

Furthermore, veteran professionals can also be unshackled from routine threat hunting to focus on more advanced cybersecurity threats and strategies.

UNIVERSITY HIGHLIGHTS STUDENTS' CYBERSECURITY ACHIEVEMENTS

Here's an example of one such program that shows this trend's momentum. When you go to the website of the **University of North Florida's** cybersecurity team, you see something new and different and actually a bit surprising. The website shows that the group has handled over 16,000 threat alerts and resolved more than 11,900 incidents.

But these cybersecurity achievements aren't credited to the cybersecurity professionals on that team as you might expect. The credit goes to student interns.

CYBERSECURITY TASKS STUDENTS DO

Within these SOCs, students are being guided by cybersecurity pros. They're tackling a range of important cybersecurity projects:

- Evaluating and prioritizing security alerts or incidents based on their severity and potential impact
- Reviewing security log-in attempts and detecting anomalies
- Identifying false positive cases (not real threats despite being identified as such)
- Detecting malware
- Patching software flaws and other security vulnerabilities

CASE STUDY
Fourteen universities using student-run SOCs to strengthen cybersecurity skills

WHY ARE HIGHER EDUCATION SOCS EMPLOYING STUDENTS?

What's driving this trend? Intense need is the answer.

Cybercriminals continue to unleash attacks against higher education institutes because of the valuable and sensitive research and intellectual property on campuses, the relatively open information-sharing cultures, and disaggregated systems and networks that open plenty of doors to go through and steal data.

In research reports tracking cyberattacks by industry, education ranks high on the bull's-eye list. An example came forth in the **Verizon 2024 Data Breach Investigations Report**. Of all breaches that took place between November 1, 2022 and October 31, 2023 across 21 industries, the highest number was recorded for the education services industry—a dubious number one ranking: 1,537 out a total of 10,626.

Being frequently targeted and the availability of limited resources are two main reasons why bringing aboard students to help higher education SOCs is becoming more widespread.

> "Higher education provides the talent, training, and staffing at a much lower cost, while the public sector provides the digital infrastructure, data centers, and funding,"
>
> LaLisha Hurt, a Splunk industry advisor in a **Splunk** article.

While most tasks that need to be performed are similar and focus on the fundamentals of cyberattack detection, there are slight differences based on the university.

California Polytechnic and State University

Working alongside cybersecurity professionals, up to eight students learn theories behind different types of cyberattacks and get educated on industry-standard data security.

> "In an article in **eCampus News**, the university's Chief Information Security Officer Doug Lomsdalen said:
>
> We do lots of over-the-shoulder training with them. We walk them through how to address specific alerts and emails, and then give them the keyboard and go from there. They're always being monitored by full-time staff—our students are never working by themselves."

Fairfield University

Up to four students work in this school's SOC to extract data from information technology tools and format that information in concise ways for the team's cybersecurity pros.

Maryville University

This university takes a slightly different approach. Students provide cybersecurity consulting services to external local clients.

TIPS FOR A SUCCESSFUL STUDENT-RUN SOC PROGRAM

Higher education leaders may want to consider the following steps to maximize program effectiveness.

Define the "why"

From the outset, write down the most important reasons for bringing aboard students to help strengthen SOC cybersecurity. Do you want to give them career opportunities more than anything else? Do you want to buttress campus cybersecurity because it'll cost you less than hiring more cybersecurity pros? Whatever your reasons, make sure you clarify them before moving ahead.

14 UNIVERSITIES BENEFITTING FROM STUDENT-POWERED SOCS

1. Auburn University
2. California Polytechnic and State University
3. Carnegie Mellon
4. Fairfield University
5. Louisiana State University
6. Maryville University (Missouri)
7. North Carolina A&T University
8. Oregon State University
9. University of Cincinnati
10. University of Maryland College Park
11. University of North Florida
12. University of Oklahoma
13. University of South Carolina Aiken
14. University of Southern Indiana

Define priorities

Identify specific tasks you need students to perform and how those will be measured. Do you want them identifying false positives more than anything else? Do you want them looking for AI-powered deepfakes? Is it most important they detect anomalies? Rank these in order of importance. Set numerical goals to track how well they execute them.

Assign a program leader

A member of the university's cybersecurity professional team should be designated as the students' leader. This person should take responsibility for ensuring students are assigned appropriate tasks, stay on track, and have a single person to depend on to ask questions and express ideas and concerns.

Do background checks and onboard training

Students will be exposed to sensitive personal and university information. As such, they need to be checked in advance for any background history that poses a risk in allowing them to see this information. The sensitivity of the data needs to be made clear to students. They need to be taught about and appreciate the seriousness of the risks associated with them using it in ways not allowed or missing cyberattack red flags that cause it to be stolen.

Make experiences realistic

Students want to gain skills that help them get ahead in their professional careers. Make sure work they do involves realistic and actual cybersecurity situations. The more you expose them to what they encounter in the world of professional cybersecurity, the more skills they'll develop and knowledge they'll gain.

The extra horsepower they bring will ease the workload on cyber professionals while protecting the university better from cyberattacks.

Set up space for students

It's a good idea to create a section within the SOC for students to work together. In close proximity, they can conveniently ask each other questions and learn from one another while also accelerating learning.

Allocate appropriate amount of resources

A key question is how many students to bring into your SOC operation. It may be wise to start small, say, five people. See how that goes. Refine the program as you learn what's most effective. There may be space limitations that would preclude taking on a few dozen students at once. Bringing aboard too many might create extra work for the cyber pros that they don't have time to oversee.