cybereason | CASE STUDY

Seton Hall University

SETON HALL UNIVERSITY
1 8 5 6

INDUSTRY

Higher Education

THE CHALLENGE

While the university environment might pose cybersecurity challenges that may not exist in the corporate world, Seton Hall and other universities like it suffer from many of the same business and operational challenges that corporate enterprises must deal with, including:

- Small IT Security staff
- Complex, open environment
- Reliance on non-IT security staff to assist in 24/7 incident response

SOLUTIONS

- To date, the university has deployed Cybereason on all of its servers—both on-prem and cloud infrastructure—as well as all of the employee, faculty, and student worker machines.
- Seton Hall conducted a head-to-head comparison between Cybereason and Crowdstrike.

SETON HALL LEVERAGES THE MALOP FORCE MULTIPLIER

As with many universities of its size, the cybersecurity mission at Seton Hall University is a highly complex undertaking. With more than 10,000 students across multiple campuses and over one thousand staff and faculty demanding easy and open access to a network spanning three campuses, the threat of ransomware and other advanced attacks is high.

"The university is not like a corporation," said Eric Lopez, Seton Hall's Enterprise Security Architect. "It's very difficult for security to say no because there's academic freedom. All we can do is say, well, what are you trying to accomplish? Maybe I have a better solution. If I don't, I need to know what you're doing so I can put compensating controls around that. And so that's kind of the world we live in. It's not as easy as saying no and blocking everything at the firewall."

THE CHALLENGE

Lopez, who spoke to Cybereason during DefenderCon21, said the risk management approach at the university involves trying to understand what tools and technologies staff and administrators need to use and then determining if they pose any risks. If so, it's important to determine whether the university is willing to accept that risk. "And if we are willing to accept it, what are we putting in place? This is why Cybereason has been invaluable to us," Lopez said. "If we aren't familiar with what they're doing on those machines, at a minimum we're going to put Cybereason on them. If there's nothing else that we do, we have to put Cybereason on them."

Seton Hall takes a unique approach to their cybersecurity program by giving students hands-on experience with tools such as Cybereason and making them part of the university's Security Operations Center. "Our students have learned so much and they're so enthusiastic about it. I think that's really showing the value of what the student SOC does for the university and what Cybereason does for the students," said Keith Barros, Seton Hall's Senior Director of Information Security.

When Lopez joined Seton Hall, the security team was using Carbon Blackand McAfee AV (managed via ePO). But their full-time staff and student workers could not easily manage the volume of alerts coming out of these systems.

THE SOLUTION

Lopez and his team ended up conducting a head-to-head comparison between Cybereason and Crowdstrike. "We put it through the wringer," Lopez said. "We threw all types of attacks at the same known virtual machine configuration, all strains of Trojans, ransomware, you name it. The only difference was one was running Cybereason and one was running CrowdStrike. And at the end of the day, nothing got past Cybereason."

By comparison, Lopez was also able to train his non-technical student workers on how to manage MalOps in less than one week.

"If Cybereason had a more complicated interface, it would take them so much longer to get up to speed," said Barros. "And it doesn't, and that's one of the reasons we originally chose the product. It's one of the big values."

"With Cybereason, I didn't have to run all these different queries," he said. "It was all collected in the MalOp. From there I could easily pivot and determine that a particular machine made a connection to a malicious IP. Then I could easily determine how many other machines in my environment did the same thing. And I could do that with a click. And so that's when we started to say, this is very valuable."

> "We needed a platform that was really going to be very user friendly, but not lacking in features and something we were completely confident could protect us. And so far that's been Cybereason for us."
>
> **ERIC LOPEZ**
> Security Architect, Seton Hall University

THE OUTCOME

Cybereason and the student cybersecurity program now provides Seton Hall more value than just threat detection and response. "We are no longer just a cost to the university. We're actually part of what's generating revenue," said Barros. "Which is a positive because we now have students wanting to join the cybersecurity program and wanting to work for us. It's value. That's a big change for us."

"Shortly after we installed Cybereason, I was literally the only full-time security person for the entire university," Lopez said. "Being able to get my students in there and managing those MalOps, you really can't put a price on that when you're talking about securing your environment. When Cybereason generates a MalOp, I can see the entire path, I can see the entire kill chain. And then the system shows the root cause and provides recommendations for remediation.