CASE STUDY

University Hires Pratum Testing Team to Take Its Best Shot

Even with best-in-class policies in place, this major university knows that cybersecurity never rests. So they asked Pratum's penetration testers to prepare them for the toughest attacks that determined hackers may dream up.

Tough Targets Need Better Testers

Years ago, the chancellor of Troy University gave the school's IT team clear marching orders: "I never want to see us in the news over a cybersecurity breach. Tell me what you need in order to keep us safe."

With that kind of executive buy-in, the Troy, Alabama, university has created an enviable cybersecurity posture. After years of investing in annual evaluations and creating an in-house Security Operations Center, the university has hardened into a tough target for hackers.

Company: Troy University
Industry: Education
Established: 1889
Student/Faculty: 18,329
Pratum Services: Penetration Testing

But Greg Price, Troy's CSO/CTO, didn't create this best-in-class security program by getting comfortable. "We don't want to view security as a one-and-done operation," he says. "It's continually changing and ever-evolving." So when it was time for his latest penetration test, Greg decided to level up to a cybersecurity vendor who could truly simulate the best shot that sophisticated, determined hackers would take at Troy's system.

> With Pratum, we not only had a cordial, professional engagement, but I felt we were working with a group that was truly concerned with our posture from a security perspective. Everything was very well -planned, orchestrated and executed.
>
> **Greg Price, CSO/CTO, Troy University**

Finding a Next-Level Partner

Troy University's complex environment includes four campuses in Alabama, 20-plus support sites outside the state, 75,000 student accounts spread across the world, and partnerships with multiple organizations in Asia. As keepers of large amounts of personally identifiable information (PII), the university faces numerous compliance frameworks, including the Gramm-Leach-Bliley Act (GLBA).

With so much to protect, Troy has implemented a wide array of cybersecurity best practices. Along the way, Troy's team realized it needed to upgrade to a cybersecurity consultant who could deliver more than basic, off-the-shelf attacks. "We were getting templated reports that didn't give us many productive things to do," Greg says. "We needed someone who would take a very critical and professional look and try to break it."

After a referral from a colleague, Greg interviewed Pratum and hired the team to do a comprehensive risk assessment. Pratum's assessment won Greg's confidence—and found few holes in the university's policies and controls. Next up was the penetration test.

Pen Testers Square Off with the Security Team

During the scoping phrase, Greg asked Pratum to test several IP addresses and web apps in a black-box format. The pen testers got almost no information about the environment they faced, and Troy's security team got no warnings that would help them prepare their defenses. Greg told Pratum's team to focus heavily on network exploitation and the critical web apps exposed to the general public.

Pratum's team used automated scans to identify vulnerabilities, then tried to manually exploit weaknesses and pivot into the larger system. Typical of a heavyweight fight, the early rounds were a stalemate. The university's artificial intelligence tools blocked much of the common reconnaissance hackers try. "Things you'd expect to see on 99% of web apps in the recon stage were pretty much knocked away initially," Pratum Senior Penetration Tester Jason Moulder says.

Moving past the scans, Pratum's testers entered the real chess match against Troy's security team. The testers customized their manual attacks with the kind of intel gathering that hackers would do. For example, Jason looked for news about research happening at Troy University labs, knowing that hackers love to target cutting-edge intellectual property.

When he started attacking the system, Jason quickly found "honeypots" that Troy's team left as soft targets to bait hackers into revealing their methods. Sidestepping the traps, Pratum went after the real targets—and found Troy's human analysts waiting. Spotting anomalous activities, Troy's team quickly isolated networks to prevent pivots. "Tools do a lot," Jason says, "but not everything. That's where the human aspect comes in. They were proactive, not reactive."

Pratum's team accessed some information they could use to target users through their Google accounts or other outside vectors. But Troy's system was mostly locked up tight. "Troy is a hard target because of the mitigations they have in place," Jason says. "Stuff would start to work, but then they would pick up on the activity and shut it down. It's good to know that they're on top of things."

But What About the End Users?

Cybersecurity conventional wisdom holds that it's easier to hack a person than a server. But what about in an organization that provides constant security training? To find out, Troy University included a Pratum phishing campaign designed to test the savviest users.

"When I described what I wanted to see, Pratum said, 'Are you sure?'" Greg says. "I told them that we bombard these users with things to enhance their awareness. Just throwing misspelled messages and a few odd logos at them isn't going to work. Go after them, and we'll see if they're behaving properly."

The phishing campaign went to more than 1,100 employees, including spear phishing messages targeted specifically at 30 high-ranking employees. The fake messages included Greg's signature block and Troy University's actual logo. One message asked users to click a link to a spreadsheet on SharePoint. The link led to a page that looked exactly like Troy's login page. After the user input their credentials, the page blinked and loaded the actual IT service page. Most users would enter their credentials again, thinking the page had experienced a blip. The second login took them to their actual account, leaving users unaware that they'd given their credentials to an outside source.

Proving people still represent a soft target, Pratum's testers got the login credentials from 33 people in the main test and one person in the spear phishing test. "It only takes one to fail," say Pratum's Tanner Klinge, who ran the phishing campaigns. "I have yet to see a campaign where no one gives up their credentials."

Again, though, Troy's strong cybersecurity program blocked any real damage. Most of the compromised Troy users quickly changed their passwords to block further action by the testers. And even with the other credentials in hand, Pratum's testers couldn't pivot into broader attacks thanks to Troy's use of network segmentation and multifactor authentication (MFA).

Make the Best Even Better

But like an all-star who keeps drilling on the fundamentals, Greg took the phishing campaign results as a kickstart for more training. "Despite all the substantial things we have going on, some users still fell for it," he says. "We take that as an opportunity to address some training weaknesses."

That kind of actionable information further validated Troy's selection of Pratum. "We got exactly what we expected," Greg says. "It was not a boilerplate, templated report that anyone could've produced. It was very insightful. The tools were not off the shelf, and Pratum used some very clever approaches just like the real bad guys do."

1551 SW Prairie Trail Pkwy
Ankeny, Iowa 50023

pratum.com
515.965.3756

Pratum
An HBS Brand