MCPHS University Saves Time and Effort with Nexpose

About MCPHS University

One of the oldest Universities in the city of Boston, Massachusetts, the MCPHS University has a legacy of valuable education and continues to grow to meet the ever-evolving needs of medical sciences and the medical community. In addition to its online campus, the University runs three physical campuses in New England: Boston, MA; Worcester, MA; and Manchester, NH.

Allen Basey, Senior Security Analyst at the MCPHS University, manages the security for all campuses from his office in Manchester, where he also provides IT support. While Allen and his team must make sure they are compliant with standards like HIPAA/HITECH, FERPA, and Mass 201 CMR 17, it's crucial that they secure the sensitive data of the University's students, faculty, and staff all while monitoring security controls at the University to keep incidents and risks low, and efficiency high. ▸▸▸

Challenge: Increasing Effectiveness of Scanning

When Basey came on board at the University more than two and a half years ago, he was tasked to develop new security procedures and policies at the University, including comprehensive vulnerability scanning. But as the only person dedicated to maintaining security, he needed to be able to improve the University's overall security posture without being overburdened. "My job was to integrate and improve security, as well as monitoring," says Allen. "I do what I can, soup to nuts."

His first move was to bring in a vulnerability scanner as inexpensively as possible, so he opted to use Tenable's Nessus. "I looked at different solutions, and I got the cheapest that I could get," says Allen. Using Nessus was very hands-on and required Allen to conduct his scans manually. "I started by doing quarterly scans, but when I looked at the risk scores, Nessus really only gave me the highs, mediums, and lows. There was no way to determine what the priority was—what they were finding was as far as we were behind, it was hard to get people to take action." Allen also found that Nessus had difficulties keeping up with a larger amount of assets, which meant that he had to do some hand-holding, breaking scans into smaller chunks to get the product to scan all of his assets.

> "The big difference [compared to Nessus] was in the prioritization of vulnerability remediation, which **saves me almost 140 hours of work.**

Not only did Nessus not give Allen critical context into what issues really needed attention, but that lack of context made it even more difficult to get the IT support teams to take action and patch vulnerable systems. According to Allen, IT was "skeptical of patching everything, they didn't know what would break." It became increasingly difficult to demonstrate the need to patch one system over another, especially since Nessus didn't provide any guidance on specifically how to patch certain issues to fix found vulnerabilities. Researching how to patch these vulnerabilities cost the University's IT team's precious time, and inevitably, crucial patches began to fall by the wayside.

It didn't take long for Allen to realize that Nessus's cheap upfront cost didn't outweigh the inconvenience and impact of having to do everything manually: from manual scans to prioritization and patch research. "I don't have time, being just one person, to go out and manually scan everything. I needed something that would do automated reporting and our systems support team needed something to help them prioritize—that's why I started looking at Rapid7."

BENEFITS

TIME SAVED OUTWEIGHS LOW COST

The benefits of Nexpose's vulnerability prioritization automatic scanning far outweighed the cost advantage of Nessus.

AUTOMATED PRIORITIZATION

140 hours saved with automated prioritizing

Solution: Making the Business Case for Nexpose

The first time Allen asked to purchase Nexpose over Nessus, his boss, the CIO, turned him down. But he didn't give up—a year later, in order to justify purchasing Nexpose, Allen says he had to build out a comprehensive business case and present it to the CIO. First he identified key needs that any vulnerability scanner would need to address:

- Ever-growing security compliance and protection standards
- Automatic periodic scans of all assets in the University's infrastructure
- Ad hoc scans of new equipment, like a new server, before it is introduced to the network to make sure they're free of vulnerabilities
- Ability to look for specific critical or news-making vulnerabilities within the infrastructure and find out if they are definitively present or not
- Easy vulnerability prioritization, as hands-off as possible, reducing overhead and manpower requirements

His next step was to recreate and quantify the steps that he'd need to take to emulate what Rapid7 Nexpose does automatically. He mapped out his process for discovering assets he wanted to scan, how he'd set up the scan, and then review and prioritize the scan's results.

"The big difference was in the prioritization of vulnerability remediation. Nexpose's prioritization is automatic, which saves me almost 140 hours of work compared to prioritizing it manually," says Allen. "Rapid7 security solutions allow me to automate the scanning and reporting features, which saves me at least 10 hours in asset discovery and reporting."

With these numbers in hand as his proof of concept, making the switch from Nessus to Rapid7 Nexpose was an easy sell to the CIO.

Results: Increasing Productivity with Nexpose

With Rapid7 Nexpose up and running at the University, Allen is seeing the benefits of automation that he mapped out in his business case.

Allen found that the time-saving automated capabilities within Nexpose had a cascading effect—not only was he able to benefit from the new efficiencies, but other teams did as well. "This prioritization and remediation reporting also saves our system support group hours of work in research on completing patches."

He has Nexpose set to continuously discover assets—including virtual assets—and prioritize discovered vulnerabilities. With this information in hand, he's had a much easier time asking the University's system support groups to implement key fixes.

Allen is happy with his decision to switch to Nexpose and has had positive interactions with Rapid7 staff and support: "Support from Rapid7 has been great, they are the first to make contact and are ready to assist at a moment's notice," he says. "Rapid7 has been very helpful in all that I have asked them for—so far they have shown true professionalism and have pushed me along in a very positive manner."

About Rapid7

Rapid7 (Nasdaq:RPD) powers the practice of SecOps by delivering shared visibility, analytics, and automation so that Security, IT, and Development teams can work together more effectively. The Rapid7 Insight platform empowers these teams to jointly manage and reduce risk, detect and contain attackers, and analyze and optimize operations. Rapid7 technology, services, and research drive vulnerability management, application security, incident detection and response (SIEM), orchestration and automation, and log management for more than 7,200 organizations across more than 120 countries, including 54% of the Fortune 100.

Our cloud-based vulnerability management solution, InsightVM, combines the power of Rapid7's Insight platform along with the core capabilities of Nexpose to provide a fully available, scalable, and efficient way to collect your vulnerability data, turn it into answers, and minimize your risk.

Get started with Rapid7 vulnerability management solutions at www.rapid7.com/vuln-management.