RAPID7

CASE STUDY | Essentia Health

Essentia Health Reduces Risk with Nexpose and Metasploit

Securing the Essentia Health network is no mean feat. The multi-billion dollar integrated health system spans multiple states and roughly one hundred facilities in the Midwest, and boasts a network that includes fifty thousand IPs – from facilities to medical device equipment. Faced with safeguarding patient data and other critical information, Essentia's security team must locate and resolve high-risk vulnerabilities before they are discovered and exploited by attackers with malicious intent.

In an industry where compliance is key, HIPAA, HITECH and PCI DSS requirements add another layer of complexity to the security puzzle. But "compliance does not equal security," Scott Erven, Manager, Information Security at Essentia Health, points out, "hackers don't usually read policies and procedures before they try to break in. People make mistakes – just because you can check a box doesn't mean you're always following proper procedure. You won't see variance from a compliance check or external audit unless you're proactively scanning."

> *"We reduced risk by more than 98%. That's particularly impressive when you consider that we brought on five new hospitals in that timeframe."*
>
> **Scott Erven**
> Manager, Information Security
> Essentia Health

Selecting a Vulnerability Management Offering

According to Scott, "Due to the size and growth of the organization, security holes such as weak credentials and improper patches were an unfortunate reality." With this awareness in mind, he and his team began to search for a solution that would perform thorough testing against all active systems.

"We collaborated with the internal audit group and with the board, and ultimately decided to bring in an external third party to do a penetration test," says Scott. The end goal was to find a way to demonstrate that risk was present, and then secure the necessary resources to get a vulnerability management program off the ground. Essentia pushes regular medical record rollouts and maintains a steady cadence of acquisitions, so one of Scott's primary concerns was being able to do due diligence up front before integrating new systems with Essentia's network. The security team wanted the ability to run a full penetration test on an environment to remediate existing issues prior to taking on a third party network.

"That was a hugely important part of our process," recalls Scott. "Previously Essentia had undergone rapid growth and bought out huge health systems without doing any security testing on them, so we highlighted that as an area for improvement. Now, our board has allowed us to require penetration testing as part of our due diligence around an acquisition, before anyone can have a conversation about connecting to our network and using our services."

As a starting point, the security team looked at various Gartner market leaders and then whittled the playing field down to three: Tenable, Core Security, and Rapid7. One of the key differentiators Tenable promised was passive scanning, which seemed appealing on paper. However, during the evaluation process, Scott and his team quickly realized that it would be a hindrance rather than a help.

Key Stats

Sector
Healthcare

Products
Nexpose Enterprise Edition

Metasploit Pro

Key Benefits

98.5% reduction in risk exposure after 8 months of using Metasploit and Nexpose

Detailed insight into medical device vulnerabilities and prioritized mitigation to address them quickly

“We uncovered several things about passive scanning,” says Scott. “In theory it sounds like a good idea, but the execution is often very poor and simply results in more logs and alerts to look at, which just end up getting ignored due to lack of resources. Secondly, if there’s any type of application or legacy system that isn’t actively communicating on the network, you’ll never be able to identify that system with passive scanning. Even though as a legacy system, it likely poses a risk! With passive scanning, you can’t see the risk associated with those systems if traffic isn’t going back and forth.”

The drawbacks of passive scanning were a major weakness that Scott and his team could not overlook. Instead they focused on finding a solution that would enable them to validate risk and remediation.

“We didn’t want to start a vulnerability management program based solely on vulnerability scanning,” says Scott. “It came down to Tenable Security Center and Core Insight. We wanted another product in the offering that complemented vulnerability scanning, and we wanted to have vulnerability validation for prioritization and progress. Tenable then went out the window, because the tool didn’t have a good penetration testing platform to use. The team was familiar with Core, having used it previously in their careers, but during the bake-off it became apparent that the Core Insight platform was very immature. There was no easy way to do a proof of concept with them – Core would have had to bring systems on-site for a two-week period.”

After an in-depth vendor evaluation, Rapid7 quickly emerged as the standout, beating out both Tenable and Core Security. Scott’s team opted for Rapid7 Nexpose Enterprise and Rapid7 Metasploit Pro.

Seeing the Benefits of Nexpose and Metasploit

“After eight months of running Nexpose and Metasploit, we had a follow-up compliance audit,” says Scott. “In comparison with the previous year, we had reduced risk exposure by more than 98%. That’s particularly impressive when you consider the fact that we brought on five new hospitals in that timeframe – it proved that using Metasploit prior to an acquisition made a significant impact. Our current goal is to use Metasploit on all assets on a quarterly basis.”

The acquisition process is now much smoother from a network integration point of view. In the past, this had been fraught with security headaches, but now the team can be proactive in identifying and addressing potential issues before merging systems.

“We also gained a lot of insight into the risks associated with medical devices and are able to take the necessary actions, working with the manufacturers to find solutions where possible,” adds Scott. With Nexpose and Metasploit, medical device exploits or weak passwords were a weekly discovery. “As far as admin-level vulnerabilities, we continue to find things probably monthly on the medical device side, thanks to process improvements.

“Security is very ingrained in our selection process. Our biomedical team has recently been integrated into the Information Services organization, meaning we have buy-in to get devices remediated, so that we have user awareness while vendors are on-site doing an implementation. We’ve also got them in our project planning program. That’s definitely a big win.”

This is not the only cross-team collaboration that has improved with the deployment of Nexpose and Metasploit. The security team has also seen increasing buy-in and support from other departments: “The ability to prioritize vulnerability reporting to the IT team was another great feature; we’re now able to do that much more efficiently, whereas before we had to give them a hundred-page report on every system.”

Strong Product Support

“Whenever we need to speak to Rapid7, the response is always quick,” says Scott. “They’re very good at listening to what our priorities are. It’s allowed us to scan medical devices in a stable way, without bringing them down. We’re big fans of the solution – it’s really the only product out there that can deliver.”