St. Elizabeth Healthcare

A holistic view of cyber health with SecurityCenter Continuous View

Challenge

St. Elizabeth Healthcare wanted to implement a more robust security platform that could deliver relevant, on-demand analytics to upper management. They also needed a framework for prioritizing risk assessments and vulnerability remediation. SecurityCenter Continuous View™ fulfilled both their immediate needs and future growth areas:

- Flexible templates and dashboards for easily customized reports
- Passive scanning to complement active vulnerability scanning
- Compliance audits for HIPAA and PCI
- Log analysis of IDS feeds

About St. Elizabeth Healthcare

St. Elizabeth Healthcare is one of the oldest and most respected medical providers in the Greater Cincinnati area, serving Northern Kentucky for over 150 years. St. Elizabeth Healthcare includes five main campuses, 60+ remote facilities, over 314 physicians and more than 7,300 associates. They are also a member of the Mayo Clinic Care Network. Sponsored by the Diocese of Covington, they provide comprehensive and compassionate care, including over $100 million annually in uncompensated care. The St. Elizabeth mission is supported by state-of the-art technology, a secure, internal electronic medical records system and an innovative mobile app.

The Problem

The primary reason for the St. Elizabeth team to upgrade their security program was the need to access comprehensive information quickly and efficiently. That included analytics for reporting up to executives in easy to understand reports and dashboards, insight into high priority remediation needs such as outdated applications running old versions of Java or Flash, visibility into sensitive medical devices, and watching for potential intrusions all without compromising the care and health of patients.

"The support was phenomenal, the training was excellent, and the tool is very efficient."

Harold Eder

The Tenable Solution

St. Elizabeth acquired a 20,000 IP address license for SecurityCenter CV in 2014. Since St. Elizabeth had been using Nessus® Professional for vulnerability scanning for several years, HealthGuard Security (HGS), Tenable's partner in the Midwest, recommended SecurityCenter CV for its familiar and friendly user interface. With the help of Tenable, St. Elizabeth was up and running in a few short hours. "It was a pleasant surprise to get up and running in almost no time," said Harold Eder, Director of IT Infrastructure and Security. "The support was phenomenal, the training was excellent, and the tool is very efficient."

"We spend a lot less time identifying problems and more time fixing them."

Gene Rouse

Key Benefits

- Information on demand
- Flexible templates and reports
- Trend analysis of scans over time
- Efficient operations, saving staff time
- A holistic view of vulnerabilities and the highest remediation priorities
- Risk analysis on the retention of outdated devices
- A do not actively scan list for IP addresses that identify sensitive equipment
- Automatic feed for daily updates
- Passive scanning on transient devices
- Continuous compliance audits for HIPAA and PCI
- Log analysis of IDS feeds

Currently, they are actively scanning 9,600 IPs and passively scanning 500-600 devices, with the infrastructure growing every day. Flexibility in configuring new scans and reports provides a quick and efficient route for growth.

The Results

Eder recognizes that cybersecurity is an enterprise-wide issue and not just an IT matter. He believes that the business value of SecurityCenter benefits the entire organization, not just the security team.

"SecurityCenter gives us a very holistic view into our vulnerabilities and our highest remediation priorities," he explained. "We can determine where we can have the greatest impact when remediating specific deficiencies across all our systems." And SecurityCenter goes well beyond vulnerability management to risk assessment. "It also helps in risk analysis of our systems," continued Eder. "For example, to assess if an outdated medical device is worth the risk of retention."

While SecurityCenter provides these daily benefits, Eder sees a larger benefit in the solution. "We don't just get a single point in time visibility. We can analyze scans over the course of several months for trending data."

And Eder is very pleased with the operational benefits for the IT department. "SecurityCenter is much more efficient than most of the other security solutions we have seen. For a small team of three security professionals, central management and time savings are critical to our 365/24/7 operations."

Passive scanning

In healthcare and clinical settings, so many devices are sensitive in nature and cannot be actively scanned. When such equipment is being used for patient care, active scanning cannot be reliably scheduled. Gene Rouse, Network Engineer for Security at St. Elizabeth, explained how passive scanning provides a new capability that enforced their security posture: "We monitor for anything that can't be actively scanned. The Passive Vulnerability Scanner (PVS) can listen for those devices and provide visibility into equipment that is off limits for active scanning. For example, IV pumps, CT scanners, or MRIs cannot be actively scanned when in service for patients. We went from zero visibility to complete insight into our clinical devices."

Configuration auditing

Configuration auditing also helped St. Elizabeth identify outdated applications. "Java is a real problem in hospitals," said Rouse. "We have outdated versions of Java running simply because they are required by older applications. SecurityCenter helps us identify patching and reconfiguration needs. Adobe Flash was another issue; the results of an early vulnerability scan helped us prioritize the need to push out Flash updates to reduce our risk considerably. We spend a lot less time identifying problems and more time fixing them."

Metrics reporting

The St. Elizabeth security team agrees that the metrics reporting capabilities of SecurityCenter provide a huge benefit. Rouse extolls the ease and flexibility of aggregating data from several template reports into one custom, repeatable report. Eder is impressed with the ability to provide on-demand information that is easy for top level executives to understand: "It takes a lot less effort for superior results."

> *"I can do a whole lot more in a lot less time."*
>
> ***Gene Rouse***

Top 3 features

As the power user of SecurityCenter CV, Rouse highlights three technical features that have made his life much easier:

- A do not scan list – "I discovered a place in SecurityCenter where I can define IPs of devices or hosts that should never be actively scanned. The Blackout Window provides peace of mind for sensitive equipment."
- Flexible reporting and templates – "I can use information from 20 different canned reports and build a single report without having to create custom reports from scratch. Then, I can automatically distribute a dozen monthly reports to the appropriate stakeholders. I can do a whole lot more in a lot less time."
- Automatic feed for current updates – "SecurityCenter updates itself daily; I don't have to initiate a download or install anything. The automatic feed is a great feature for staying up to date with the latest enhancements."

> *"SecurityCenter is truly a solution we can grow with as we take advantage of additional features."*
>
> ***Harold Eder***

Future Roadmap/Next Steps

SecurityCenter is a work in progress at St. Elizabeth. With just under a year of use, Rouse knows there is a lot more he can do with SecurityCenter. Plans for the immediate future involve expanding their use of the Log Correlation Engine™ (LCE®). "LCE is getting feeds from our IDS system. We want to correlate outside attacks against internal vulnerabilities," explained Rouse.

They will also be expanding their use of HIPAA and PCI compliance audits, including that data in a risk assessment program with Tenable partner HGS.

"SecurityCenter is truly a solution we can grow with as we take advantage of additional features," concluded Eder. "There is a lot of value in SecurityCenter; I couldn't ask for more."