tenable network security

Clemson University

Overview

Clemson University, recognized by U.S. News and World Report as the 25th best college in the U.S., is a major, land-grant, science- and engineering-oriented research university which maintains a strong commitment to teaching and student success. The university has nearly 20,000 students enrolled and employs almost 1,200 faculty and staff.

Clemson's IT security team falls within the university's security organization and is responsible for the compliance, policy setting, and information protection of more than 80,000 registered devices connected to its network, which spans 46 counties statewide.

Business Needs

Clemson needed a new approach to its existing IT security and auditing process that would reduce costs, streamline compliance reporting, and improve security through automation and integration with existing software and systems.

Backlogged

Clemson University has a small IT security team which is tasked with the security and compliance of Clemson's large and complex network — including tens-of-thousands of registered IPs. In addition to housing sensitive student, faculty, and financial transaction information, the university serves as the data hub for a crucial state medical service. Needless to say, the security of this information is critical for Clemson.

The IT security team at Clemson manages approximately five full audits per year and works very closely with its auditing team to ensure it is meeting all compliance initiatives, especially PCI and HIPAA. During one of these audits, the team discovered it needed to make some changes.

> "Our network generates mountains of log data, and our current security process was working, but not as efficiently as we would have liked it to," said David Buckley, Director of Security Infrastructure, Clemson University. "We needed to create a system where we were shipping our log data to a separate dedicated log server that had limited access and would create some separation of duties between our security team and system administrators."

Buckley added that audits were taking longer than they needed to because the team had to tap the system administrators, who were already strapped for time, to gain access to the log data our security auditors needed.

> "Most organizations like ours face a barrage of attacks every day. The majority of them are unsuccessful, but the sheer volume can be a distraction that makes it difficult to determine if something has slipped by our defenses. With our new additional tools, we are able to better identify the threats and respond accordingly."
>
> ***David Buckley***
>
> Director of Security Infrastructure,
>
> Clemson University

Creating the Security Curriculum

To get its security process back on track, Clemson University planned to introduce several new security strategies and tools with three key business goals:

- Strengthen security by creating a centralized log data repository with limited access that would ensure network and server activity from privileged users, like system administrators, was being actively monitored for suspicious behavior.
- Reduce costs with new systems which would cut administrative overhead and shrink security resource requirements across multiple business units, including the security, server, and monitoring teams. This new process would provide opportunities to reallocate tight staffing resources to alternate high-priority projects and tasks.

> "We have three security pros to manage, monitor, and protect all the sensitive information that flows through Clemson's network, so making efficient use of our already limited staffing resources was an essential requirement for our revamped security process," added Buckley.

- Streamline compliance and reporting by automating several pieces of the audit process and delivering fast, accurate, and easy-to-understand reports without burdening the server team. Clemson's IT security team works very closely year-round with its auditors to ensure it's meeting core compliance requirements, like HIPAA and PCI. Improving its compliance process was critical to its success and its ability to continue to expand.

The Tenable Solution

The Building Blocks of Strong Security and Compliance

To meet these business needs, Clemson University began several new security processes and deployed new technology solutions, including Tenable's SecurityCenter™, Nessus®, and Log Correlation Engine™.

By leveraging this new security process, Clemson University was able to:

- Tighten its grip on network activity by building a new, separate log repository with limited access to members of the security team and leveraging log correlation technology to monitor, correlate, and identify abnormal system events in real time. This new security approach also gave Buckley's team a single console where they could access all the information needed and become more responsive to system outages through increased visibility and alerts.
- Transform and reduce the length of its audit process by half with increased automation, clear understandable network status reports, and integrated systems that could provide near-instant insight into vulnerability and patch status across its vast network — with the right amount of detail its auditors needed.

> "Audits used to be a multi-day process for us, and now we can deliver audit results in the same day, which is saying a lot when your network is as complex as ours is," said Buckley. "We now have packaged scans and reports that make it turnkey to get an up-to-date snapshot of the compliance status of the network, without having to reinvent the wheel every time and without having to get multiple business units involved."

- Keep auditing and security costs in check by giving Buckley and his team an opportunity to reallocate resources to alternate high-priority projects like building a Data Analysis Network, which would also allow Clemson to consolidate traffic data in order to perform passive vulnerability scanning.

Business Needs

New approach to existing IT security and auditing process that:

- Reduces costs
- Streamlines compliance reporting
- Improves security through automation and integration with existing software and systems

"Keeping our network safe, particularly the hundreds-of-thousands of medical records we store for the state of South Carolina, is the top priority of our department," said Buckley. "It's what keeps me up at night, and it was the key goal for revamping our process."

"We considered several different approaches, but we saw an opportunity to combine existing resources and systems along with new technology to gain better security through integration, correlation, and increased network visibility. The integration also offered cost and compliance benefits, and we were able to build on top of our existing Nessus deployment — making it quick and easy to implement this new strategy."

David Buckley

Director of Security Infrastructure,

Clemson University

Next Steps and Bottom Line

Security: An Ongoing Process Not a Product

Clemson University continues to find new ways to improve, automate, and optimize its security process through technology and industry best practices. The university runs on a 30-day patch deployment schedule and recently automated its patch management and reporting system to improve efficiency and results. By leveraging several new solutions, including Tenable's Nessus vulnerability scanner, Clemson's new process now automatically scans critical systems every 30 days for vulnerabilities, identifies unpatched systems, and sends a report to system administrators and members of the security team — highlighting which systems are missing critical patches and what kind of progress has been made over the past 30 days.

> "The speed at which we're able to scan our network is pretty remarkable, but these new automated systems are light years ahead of what we were doing before," said Buckley. "It's nice that this new process has made our day-to-day more manageable, but the real ROI is that we're more proactive about our security and compliance initiatives and we're keeping our network safe."

"It used to take us days to gain access to server log data, and now we can get the visibility we need within a matter of minutes," added Buckley. "We have a responsibility to the state of South Carolina, our students, and faculty to actively protect their sensitive data, and this new process keeps us ahead of attacks by helping us understand potential gaps and connect the dots between certain types of network events."

David Buckley

Director of Security Infrastructure,

Clemson University

For More Information

Questions, purchasing, or evaluation:

sales@tenable.com or 410.872.0555, x500

Twitter: @TenableSecurity

YouTube: youtube.com/tenablesecurity

Tenable Blog: blog.tenable.com

Tenable Discussions: discussions.nessus.org

www.tenable.com

tenable™ network security