Digital Defense, Inc. helps Tulane University Bolster Information Security

DIGITAL DEFENSE® INCORPORATED

www.DigitalDefense.com

In higher education, we work hard to protect the sensitive data and intellectual property of students, faculty and staff. Hackers are realizing that universities are a treasure trove of valuable data and we are a growing target for cyber-criminals.

—Hunter Ely, Assistant Vice President, Information Security and Policy Officer at Tulane University.

About Tulane University

Tulane University is one of the foremost independent national universities in the South, located in New Orleans, LA. With ten schools and colleges that range from the liberal arts and sciences through a full spectrum of professional schools, Tulane provides its students with a breadth of choice. Tulane University's ten academic divisions enroll approximately 8,000 undergraduates and about 5,000 graduate and professional students. The schools of Architecture, Business, Liberal Arts, Public Health and Tropical Medicine, and Science and Engineering offer both undergraduate and graduate programs. Other divisions include the Schools of Law, Medicine, Social Work and Continuing Studies.

SITUATION:

Higher Education Institutions Face Unique Security Challenges

Universities and other higher education institutions face a unique and complex set of cybersecurity challenges not experienced by other industries. As Hunter Ely, Assistant Vice President, Information Security and Policy Officer at Tulane University, explains, higher education institutions have to walk a fine line between making sure the students, faculty and staff connecting to the university's networks are kept safe and secure, while also being careful not to become the internet police. "We never want to prevent people from accessing the data they need for projects and research," states Ely. "Every time a student, faculty or staff member goes online, the university has to consider if our security policies and procedures are properly protecting them without blocking them from accessing useful information."

Since universities often do not have direct access to the majority of the endpoints of their network, the complexity of the problem increases. Students, faculty and staff are connecting to the network multiple times a day through multiple endpoints such as laptops, phones and other personal devices, which can potentially open doors for a cyber-criminal and put sensitive data at risk, leaving the university vulnerable to a devastating breach.

In the wake of these challenges, along with the increasing number of attacks universities are facing, Tulane is continuing to further its commitment to cybersecurity. With more than 16,000 students, faculty and staff and the increase in potential vulnerabilities that could put the network at risk, having a strong vulnerability management program in place is crucial.

SOLUTION:

Vulnerability Management Platform Unlike Others – Frontline™ Vulnerability Manager (Frontline VM)

In order to help manage ongoing threats and meet data protection requirements and compliance mandates, Tulane turned to Digital Defense, Inc. (DDI) for a vulnerability management solution. Leveraging DDI's Frontline VM, Tulane is streamlining processes and improving data security by effectively identifying internal and external vulnerabilities that can be exploited by cyber-criminals and hacktivists.

Previously, Tulane was using another popular network scanning tool to assist with vulnerability management, but was struggling with reports that provided large amounts of static and extraneous data, which then had to be distilled into something actionable. Rather than continuing to hound their previous provider for insight and assistance, they decided to look for a new solution. This brought them to DDI.

The Tulane Security Team discovered that DDI's Frontline VM is able to provide a better solution that is customizable and easy to use.

Frontline VM is advanced, intuitive and cost effective. Underpinned by cutting-edge technology, Frontline VM quickly identifies weaknesses within a network and prioritizes assets to ensure remediation efforts reduce security risk as rapidly as possible. Role-based reports present the necessary intelligence to the users, executive leadership and auditors. Frontline VM is an instinctive console supported by a cloud-based architecture, which eliminates ongoing capital expenditure and frees the client from concerns about technology obsolescence and the burden of performing software and hardware updates.

Tulane has found that reports generated and delivered via Frontline VM are actionable, allowing the team to move quickly on issues and streamline remediation efforts. Tulane experiences fewer false positives, which saves time, and Frontline VM does not take weeks of training to get new people up and running. This means more members of the Tulane Security Team can use it and have role-based access to the data. "The data from Frontline VM is distinct without having to go into a lengthy description, and the critical issues are very clear – the big things do not get lost in the shuffle," says Mark Liggett, Senior Security Analyst, Tulane University.

Tulane's team also appreciates that, after they fix an issue, they can immediately re- scan, and find out almost in real-time if their fix effectively remediated the problem.

"We can use Frontline VM to easily tease out the problems in our network, which is more important to us than in other organizations because we do not have direct access to the endpoint," Ely says.

The vulnerability reports we receive from DDI are easy for the various schools and departments that we work with to understand and provide concise data and actionable intelligence for my team.

—Mark Liggett, Senior Security Analyst, Tulane University

Cutting Edge Technology

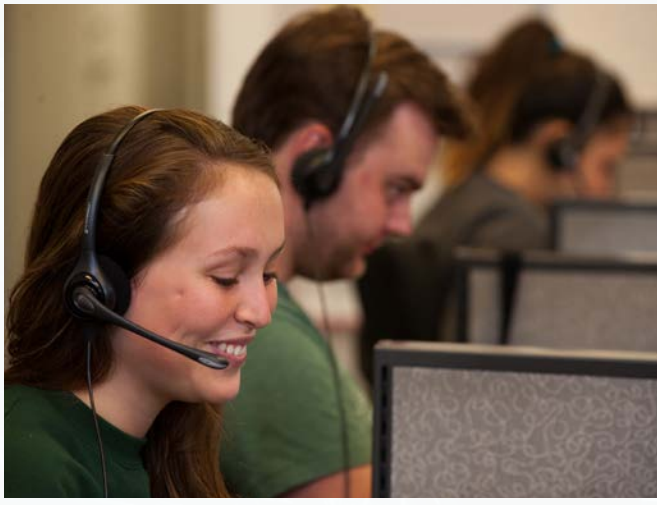
DDI is a long standing innovator in vulnerability management. The powerful patented scanning technology, complemented by a patent-pending advanced network host correlation algorithm, produces highly accurate results. Unlike premise-based tools previously used by the university that silo data, DDI's technology helps identify trends and outliers through the analysis of aggregated data. This allows DDI to quickly generate more accurate and complete results and to alert Tulane swiftly to any potential vulnerabilities that could threaten their security.

Having a proven scanning technology in place has become even more valuable for Tulane when thinking about the issue of unknown endpoints (hosts) faced by institutions of higher education. In any network, assets don't always stay in place. DDI's network host correlation tracks and reconciles assets and their data, even when their IP addresses change, providing unparalleled vulnerability management. Other tools only provide a one-time static snapshot of risk, resulting in an inaccurate view of the entire security posture. With so many different and changing endpoints on their network, Tulane can use DDI's vulnerability management solution to unravel any problems.

The People Factor: Support We Need When We Need It

Tulane has also found that, with DDI, they have access to experts who can be an extension of their organization, with a white glove approach to support. DDI's on-demand Personal Security Analyst team is available to help define requirements, craft strategy and effectively execute a vulnerability management program tailored to their organization.

While set up is simple and the platform is intuitive, when questions do come up, assigned client support helps make day-to-day issues easier to manage, including remediation prioritization and assignments.



DIGITAL DEFENSE® INCORPORATED

www.DigitalDefense.com