New insights into security

How higher education insitutions are using SIEM to prioritize threats and keep data safe

In April 2021, student and staff information from more than a half-dozen universities—including academic transcripts, medical records, research grants, employment contracts and Social Security numbers in some cases—surfaced on the dark web. One institution,the University of Colorado, received a $17 million ransom demand.[1]

The breach, which is believed to have affected at least 300 organizations, is the latest example of the mounting cybersecurity challenges faced by higher ed during the pandemic. Cyberattacks on education institutions increased by 30 percent in the six months after the pandemic shifted most courses and activities online in March 2020, compared to 6.5 percent across all sectors, according to one report. By the end of the year, another analysis found more than 60 percent of all detected malware was in the education sector.[2]

While most colleges and universities had managed some level of online programming—and the associated security challenges—before the pandemic, "the big change is the scale and acceleration of change," says Douglas Natal, General Manager for U.S. Public Sector for cloud-based security vendor Sumo Logic. "The aha moment is that they've got to get their technology up to speed."

A new environment

Colleges and universities continue to explore cloud-based learning management systems and applications to leverage the elasticity and availability of cloud infrastructure, all in an effort to afford students and staff an enriched online experience, especially after the pandemic ended in-person activity on most campuses. However, the rapid scaling of online activities and the proliferation of mobile devices has dramatically increased the attack surface, according to Pete Tseronis, Founder and CEO of Dots and Bridges and former Chief Technology Officer at the U.S. Department of Energy.

"The Internet of Things presents both opportunity and risk. More devices means more connectivity. And the connectivity is global. As such, our threat landscape has grown exponentially, with remote connectivity everywhere and anywhere via the palm of our hand," Tseronis says.

Given the growing numbers of students and staff with legitimate needs to access systems from outside the institution's networks, it's become imperative for university IT departments to create and enforce security policies, but also to understand what users are doing over time to identify potentially dangerous actors.

Institutions must determine whether access from IP addresses outside of the United States represent international students or potential bad actors. And with the interconnected nature of institutions and shared services, the activities of both people and automated processes must be monitored to determine if and when they might result in a security breach or data theft.

For example, one institution identified suspicious activity from a shared services provider with legitimate access to their servers. Closer examination found that a bad actor had set a script to repeatedly download the same large document, taxing network resources.

When it comes to network activity from individuals or automated processes, there's one question all institutions must consider, according to Natal: "Are the authorized users performing unauthorized activity, outside of their normal behavior?"

Visibility and observability

Traditional cybersecurity approaches are adept at identifying breaches. But with tens of thousands of users—both human and automated systems—accessing an institution's systems at any one time, pinpointing potentially dangerous behavior in real time and identifying shifts away from typical behavior is something even highly trained security analysts struggle with. Many suffer from "alert fatigue," with the large numbers of false positives and alerts consuming most of their time and making it more likely that the real threats are missed.

The advent of cloud SIEM (security information and event management) solutions provide greater visibility into network activity, even as the number of users explodes. Aggregating system logs and user data from many sources across different systems and cloud providers, including network hardware, security systems, servers, databases and applications, cloud SIEM solutions consolidate information to provide a complete picture of activity. They also provide security analytics to identify threats and generate insights to better secure systems, as well as generate advanced forensic data to help identify and mitigate breaches after they occur.

Through these automated activities, some cloud SIEM solutions can reduce false positives by as much as 90 percent, allowing security analysts to prioritize the most important threats to focus on. For example, examining a persistent threat coming from multiple parts of the world is likely a better use of time than chasing each suspicious attempt at access from a broad range of unrelated IP addresses. Pinpointing threats can also help speed remediation. "Being able to automatically triage and follow the path to a breach is simplified with a modern cloud SIEM that can provide insights and intelligence so humans can more effectively spend their time on solutions," Natal says.

Getting compliant with data protection

Cloud SIEM solutions also help institutions enforce and gather data for compliance around a wide range of privacy and security regulations. For colleges and universities, compliance begins with Family Educational Rights and Privacy Act (FERPA) regulations governing student education records, but can encompass a much broader range of standards, including the Health Insurance Portability and Accountability Act (HIPAA) for student health information and institutions with hospitals, Federal Risk and Authorization Management Program (FedRAMP) authorization requirements, which impact institutions receiving federal grants for research and other projects, and even the Payment Card Industry Data Security Standard (PCI DSS) for on-campus and online credit card payments.

Without these solutions, IT staff often must undertake the timeconsuming process of assembling security logs from multiple systems for audits and other compliance activities. Automating these systems can reduce the work involved in annual audit cycles by weeks and improve relationships with external auditors.

Looking ahead

A greater dependance on distance teaching and learning will last long beyond the pandemic. As our global educational community seeks to embrace a "new normal," ensuring the security, integrity and authenticity of information is paramount. Furthermore, institutions will find "no shortage of taxonomies, frameworks and methodologies to leverage," Tseronis says. He urges stakeholders to prioritize technology investments based on the alignment of technology capability to mission need, the identification of high value datasets/systems, and the mapping of organizational risk posture to aforementioned resources such as the NIST Cybersecurity Framework[3]—identify, protect, detect, respond and recover.

"At the end of the day, every organization is unique," Tseronis adds. "Technology insertion still requires old-school enterprise architecture principles emphasizing an 'architect, invest, implement' approach. Complementing an investment decision is fine. It's not always about 'ripping and replacing.' Most importantly, it is imperative to understand your needs first and foremost."

Given the rapid shift to cloud delivery and applications, it's vital to ensure cybersecurity solutions can support the collection of data logs, metrics and traces from both cloud and on-premises systems. Look for easy-to-use tools and opportunities to bring your staff up to date with the technology, as well as for systems that automate processes involved with compliance and regulations. Cloud-native solutions can automatically update to address emerging security threats. They also can easily scale as network traffic increases and provide simplified dashboards to make all staff aware of network activity and potential threats in real time. Some organizations have monitors prominently displaying these statistics in public places, but all institutions can benefit from providing students and staff with a greater awareness of cybersecurity threats.

"Allowing people to know the security posture of the organization can help make them more conscious of the risks they are taking online," Natal says.

Finally, don't minimize the human factor. A 21st-century workforce will require thinking, reasoning and teamwork, in addition to technological aptitude. Leveraging SIEM and Security Orchestration, Automation and Response (SOAR) tools offer automation, but don't discount human intuition, especially as these enterprise platforms traverse, according to Tseronis.

That's important, because eliminating rote tasks and the chase for false positives can improve retention and reduce turnover, helping build institutional knowledge across systems and applications.

And institutional knowledge begins with IT leadership, with SIEM solutions helping them remain focused on current threats.

"Today's higher ed organizations should be reskilling, retaining and recruiting individuals that maintain strategic, operational and tactical skill sets, all in an effort to mitigate risk and accelerate innovation," Tseronis says.

About Sumo Logic

Sumo Logic Inc., (NSDQ: SUMO) is the pioneer in continuous intelligence, a new category of software, which enables organizations of all sizes to address the data challenges and opportunities presented by digital transformation, modern applications, and cloud computing. The Sumo Logic Continuous Intelligence Platform™ automates the collection, ingestion, and analysis of application, infrastructure, security, and IoT data to derive actionable insights within seconds. More than 2,100 customers around the world rely on Sumo Logic to build, run, and

secure their modern applications and cloud infrastructures. Only Sumo Logic delivers its platform as a true, multi-tenant SaaS architecture, across multiple use-cases, enabling businesses to thrive in the Intelligence Economy. For more information, visit www.sumologic.com.

About Amazon Web Services

For 14 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform. AWS offers over 175 fully featured services for compute, storage, databases, networking, analytics, robotics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual and augmented reality (VR and AR), media, and application development, deployment, and management from 77 Availability Zones (AZs) within 24 geographic regions, with announced plans for 15 more Availability Zones and five more AWS Regions in India, Indonesia, Japan, Spain, and Switzerland. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—trust AWS to power their infrastructure, become more agile, and lower costs. To learn more about AWS, visit aws.amazon.com.

This piece was developed and written by the Center for Digital Education Content Studio, with information and input from Sumo Logic.

1. https://denver.cbslocal.com/2021/04/14/colorado-cu-boulder-17-million-ransom-demandaccellion-data-breach/
2. https://securityboulevard.com/2020/12/why-higher-education-is-a-prime-target-forcybercriminals/
3. https://www.nist.gov/cyberframework

CENTER FOR DIGITAL EDUCATION

Produced by The Center for Digital Education. The Center for Digital Education is a national research and advisory institute specializing in K-12 and higher education technology trends, policy and funding. The Center provides education and industry leaders with decision support and actionable insight to help effectively incorporate new technologies in the 21st century.
www.centerdigitaled.com

sumo

Toll-Free: 1.855.LOG.SUMO | **Int'l:** 1.650.810.8700
305 Main Street, Redwood City, CA 94603

www.sumologic.com