INDUSTRY: Higher Education

CASE STUDY

A Large US University Finds More Exposed Credentials 10X Faster with SpyCloud

CHALLENGE

With few resources to dedicate to account takeover prevention, this large US university was settling for a mediocre security solution that required too much manual effort.

SOLUTION

The university leverages SpyCloud's seamless integration with Splunk to automate its account takeover prevention strategy, enabling the institution to strengthen its security stance.

RESULT

Using SpyCloud automation and data, the university consistently discovers more account exposures and remediates in a fraction of the time as before and with fewer resources.

CHALLENGE: KEEPING INFORMATION ACCESSIBLE WHILE PROTECTING ACCOUNTS

This featured university takes cyber security seriously and is aware of the constant threats to its students, faculty and staff. Like many higher education institutions, however, this university has few dedicated security professionals on staff to implement and manage technologies and processes.

For security professionals at higher education institutions, there is often an identity access management dilemma. On the one hand, they want to restrict account access to only authorized individuals, yet they also want to remain "open" for students and staff to get any information they may need. This transparent framework fosters self-reliance and efficiency, but it makes it challenging to limit and control security.

The university understands account takeover is a pervasive problem throughout the college systems that is growing exponentially. They believed they were addressing threats with a product, but it failed to live up to its sales pitch, leaving them to perform additional work to get the most from the solution. "We had to do so many manual tasks after finding any issues and knew we might be missing other ATO threats. These efforts took time away from performing other necessary tasks in our security cycles," says a manager in the Office of Information Technology at the university. "We were introduced to SpyCloud and were eager to compare credential matches. Even more so, we wanted to see how the integrations would speed remediation with fewer resources."

SOLUTION: INTEGRATE SPYCLOUD AND SPLUNK FOR AUTOMATION EFFICIENCIES

The institution chose SpyCloud for several reasons, including the fact that the SpyCloud API could dump their robust breach data into its Splunk instance. According to the manager, integration into Splunk was key. "Our previous tool lacked Splunk integration, forcing us to use up resources to investigate suspicious accounts and take manual action in Splunk," he says. "Splunk scripts pull in the SpyCloud data automatically to provide instant visibility into which of student's or staff's credentials have been exposed. The quantity and quality of their data is amazing, we've never seen anything like it."

The Splunk integration means developers no longer have to take extra manual steps to consume the SpyCloud data. The SpyCloud API provides an efficient and reliable way for the Office of IT to access their exposed credentials that are being traded in underground communities. Many other account takeover prevention solutions and tools find exposed credentials only

EXPOSURES FOUND

10 TIMES FASTER

THAN WITH PREVIOUS TOOLS

after they are on public forums, much too late for remediation efforts to secure accounts.

"As a higher education institution with students, faculty and staff using school emails to access everything from financial aid to housing data to meal plans, we have a responsibility to protect those accounts as best we can from cyber criminals who hope to gain access to those accounts," says the manager. "With SpyCloud, we feel like our security staff finally have the tool they require to know the who, what, when and where as it relates to compromised accounts."

RESULTS: FASTER, MORE RELIABLE RESULTS WITH FEWER RESOURCES

Since implementing SpyCloud, the school finds more exposed credentials than ever before. Thanks to the seamless API integration with Splunk, they are finding those exposures and taking action ten times faster than in the past.

"We have to do more with fewer resources every year," says the manager. "SpyCloud digs deeper into the dark web and cyber underground than other tools and finds more stolen credentials sooner. We have more hits than we did with the other system because SpyCloud data is fresher and more complete."

> *"Splunk scripts pull in the SpyCloud data automatically to provide instant visibility into which students' or staffs' credentials have been exposed. The quantity and quality of their data is amazing, we've never seen anything like it.*