CASE STUDY

The University of Lethbridge

// The Modern SOC Company

JASK

CASE STUDY

The University of Lethbridge Leverages JASK's Cloud-Native SIEM to Better Secure Complex Environment

"We embarked on a mission to find a platform that would give us complete and actionable visibility into our potential attack surface."

Manager of Information Management and Security

About University of Lethbridge

The University of Lethbridge (U of L) is one of Canada's top-ranked universities and leading research institutions. With campuses in Lethbridge and Calgary, Alberta, the U of L attracts more than 8,700 undergraduate and graduate students from around the world each year. It offers more than 150 undergraduate and 60 graduate programs across seven different schools: Arts & Science, Education, Fine Arts, Health Services, Liberal Education, Graduate Studies and the Dhillon School of Business.

The Challenge

Due to the wealth of sensitive information higher education institutions are responsible for, EDUCAUSE named information security as the top IT issue the education sector needs to address. Coupled with evidence that financially-motivated attacks against higher education are on the rise, it's clear that universities remain a prime target of online criminals and nation state attackers. To ensure it remains secure in the face of these growing threats, the University of Lethbridge set out to strengthen its security posture. The first step? Creating a next-generation security operations center (SOC).

"We embarked on a mission to find a platform that would give us complete and actionable visibility into our potential attack surface," said Kevin Vadnais, manager of information management and security at the University of Lethbridge. "It is difficult to scale cybersecurity resources with escalating demands, so we focused on finding a tool that would make our team vastly more efficient and better equipped to rapidly respond to threats."

"The JASK ASOC platform provides our team with the visibility and automation needed to increase our agility, while allowing us to get more out of our existing tools and remain flexible as we scale."

Manager of Information Management and Security

With a small team of only two full-time security staff, the U of L needed a solution to effectively automate the work of the tier-1 security analyst. Working to secure two different college campuses and thousands of students, the University also required a tool that would provide them with the visibility across its digital assets that support multiple locations and thousands of students.

"We had to find the right technology to automatically correlate security alerts coming in, rather than trying to have our small team analyze the vast amount of data we receive on a daily basis," said Vadnais. "It would be unreasonable to expect my team to adequately protect the entire digital footprint of our campuses without adding advanced technology into the mix."

Open, Flexible Architecture Leads to Immediate Benefits

To address these challenges, the University of Lethbridge implemented the JASK Autonomous Security Operations Center (ASOC) platform. As a cloud-native, advanced Security Information and Event Management (SIEM) platform, JASK ASOC allowed the U of L to immediately gain the desired visibility into its data without the need for maintenance of a complex infrastructure. In addition, the open nature of the platform will enable the University to seamlessly integrate its existing security solutions with JASK ASOC, further increasing its ability to quickly and efficiently identify interesting events that should be investigated.

"We have an incredible amount of data to analyze, and it's essential for us to be able to identify the events that matter as quickly as possible," said Vadnais. "The JASK ASOC platform provides our team with the visibility and automation needed to increase our agility, while allowing us to get more out of our existing tools and remain flexible as we scale."

For example, the University has a corporate firewall from Checkpoint in place to establish a defense perimeter. JASK was able to work with the Lethbridge security team to create an environment with a more transparent view of all traffic entering and leaving its network.

"Due to the openness of JASK, we were able to place collectors within our ecosystem to monitor all incoming and outgoing traffic from behind our firewall," said Vadnais. "These sensors allow us to analyze the type of activity occurring beyond our outside defense strategies, enabling us to quickly identify the events occuring past our perimeter. This setup has been crucial to our ability to spot and eliminate threats effectively."

Advanced Insights: From Reactive to Proactive

By fusing data from security tools and applying AI and machine learning to automate the correlation and analysis of threats, the JASK ASOC platform provides actionable information via JASK Insights that allows the U of L's security team to be more proactive and get ahead of potential threats.

"Before we deployed JASK into our environment, we had to be reactionary, often waiting until a threat was uncovered before we could clean up the mess," said Vadnais. "With JASK, we're much more proactive, identifying attacks before they become catastrophic. We're able to see abnormal behavior when it first emerges and take steps to eliminate the risks, rather than waiting for the damage to be done and move forward with recovery efforts."

Intelligence in BYOD Environments

The University's IT team uses Microsoft's Active Directory to manage the vast amounts of devices across its networks. Deploying JASK has increased the team's ability to manage this multifaceted ecosystem.

"In a complex environment with a BYOD culture, we have to be able to see what users are bringing in and monitor the related activities for abnormal traffic patterns," said Vadnais. "With JASK, we're able to analyze the plethora of device and network information directly in the ASOC platform, providing clear visibility into all of the assets we need to monitor through a single interface."

Moving Forward: Improved Security Posture

Beyond the technical benefits, JASK has provided the University of Lethbridge with unparalleled customer support. With a dedicated customer service team, JASK ensures a high level of personalized assistance as the customer's security environment evolves.

"In addition to eliminating the stress of having to manually analyze every security alert across our networks, JASK has been stellar from a customer support perspective," said Vadnais. "The team is hands-on, and we view them more as an extension of our team than an outside vendor."

As the University builds out its SOC, it plans to leverage JASK's open, flexible architecture more as well.

"As we add technologies to our security toolbelt, the flexibility that JASK provides will be incredibly valuable. We look forward to adding data sources for JASK to correlate for us in the future, and continuing to reap the benefits of its powerful automation abilities."