Site feedback

Business challenge

Mohawk College wanted to implement an industry-leading SIEM solution to manage defenses against growing threats that might breach the already robust system protecting its complex IT environment.

Transformation story

The college worked with GlassHouse to implement the QRadar SIEM platform to help it gain

Results

Provides visibility

into threats across on-premises and cloud environments

Accelerates threat detection

with prioritized insights to address the most critical threats

Integrates seamlessly

with multiple systems across different college departments and campuses

Business challenge story

Cybercriminals target college IT systems

Higher education institutions are one of the richest and ripest targets for cybercriminals. They offer the fruit of intellectual property, research and the personal information of both students and faculty. And generally, that low-hanging fruit is easily harvested by bad actors because cybersecurity measures and technology are often implemented piecemeal, without an eye to systematic prevention and response across multiple university or college departments.

College in Hamilton, Ontario. “Typically, if you don’t have a well-thought-out security program, the technical people will do everything around protecting the environment. They’ll quickly run out and buy some anti-malware, or maybe install fancy, new, next-generation firewalls. And while those fixes are very important, they’re only part of combatting cyberattacks at a college like Mohawk.”

It’s not surprising that Mohawk takes a comprehensive approach to cybersecurity. The college focuses on applied research, with multiple lines of study that allow students to gain real-world experience with businesses in Hamilton and the Greater Toronto Area. It is known for innovation in its own operations, with LEED-certified green buildings and heating and cooling systems.

Mohawk also teaches cybersecurity and has an extensive Central IT department that oversees cybersecurity for the institution. Several years ago, it became clear that the college needed to use state-of-the-art cybersecurity tools to protect and defend against malicious attackers.

Frank recalls how the college’s cybersecurity environment evolved. “Our board was starting to ask questions about it, asking how we could build a program around protecting our critical assets,” he says. Central IT started by looking at different industry frameworks for security, including ISO 27001 and ISO 27002 standards for managing information security. It then used the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) to conduct a gap analysis and score itself across its five pillars: identify, protect, detect, respond and recover.

The college knew that it had done well in identifying the assets it needed to protect and in protecting those assets generally. However, it did not score as well in detection, so if its controls failed, it could not quickly identify the breach and move on to respond and recover from the breach. “You can put all this investment into your protection mechanisms, but there’s no silver bullet,” asserts Frank. “Eventually, there's a high risk of compromise and a complex landscape.”

Mohawk decided to focus on and invest in detection. “We wanted to make sure that if somebody got past our protection, we could quickly detect and eradicate them from our network,” Frank says. In higher education, it can sometimes take months before someone realizes that the attackers have infiltrated a system. “We didn’t want that to happen if our systems were breached,” he says.

exactly what systems were touched, to rebuild your systems after the fact and re-secure your network after a breach."

Mohawk began a search for an industry-leading detection platform. At the time, it was already working with IBM to build out its cybersecurity curriculum to include SIEM tools such as the QRadar solution. It was with this synergy in mind that Frank and his colleagues began exploring SIEM solutions for the college.

Frank outlines the college's criteria: "We wanted a tool that was easy to use, didn't require substantial amounts of training for users to be able to pivot and search through data to both see event logs and do network traffic analysis." The college needed a tool that would not only store the information for searches but also identify and prioritize incidents and offer the option to apply AI to investigate breaches faster.

QRadar quickly rose to the top of the solutions that Mohawk investigated. The tool stood out above the others under consideration because Gartner had named it a SIEM leader in its Magic Quadrant for SIEM report, it had good standing with public cloud providers and it had received strong references from other higher education institutions.

> "It's all about visibility... With QRadar, there's a layer of visibility that we previously didn't have."
>
> **— Andrew Frank, Manager of IT Security Services, Mohawk College**

Transformation story

SIEM for detection, prioritization

Mohawk decided to implement the QRadar SIEM platform to help it more quickly detect and prioritize threats on its diverse and distributed IT network. "So QRadar really checked a lot of boxes for us once we determined what tool we wanted," says Frank. "We just needed to

Mohawk selected GlassHouse, a local IBM Business Partner, to implement the QRadar solution and to provide personalized ongoing support to the college.

“We could tell from the beginning that everybody was extremely professional at GlassHouse,” says Frank. “They weren’t just there to sell us something and get in and get out. They established a relationship with us.”

GlassHouse implemented the QRadar solution, building the infrastructure across three campuses and its primary data center to help the college ingest and analyze data from multiple systems and departments. The IBM Business Partner also trained the Mohawk team and provided all the necessary documentation and diagramming.

The QRadar platform provides Mohawk with a consolidated dashboard that helps its IT security staff visualize its network security. When a breach or offense occurs, security analysts can use the offence dashboard to gain insight into how, when and where it occurred. The QRadar solution also prioritizes offenses based on their relevance, credibility and severity, so Mohawk can concentrate on responding to the highest priority offenses first.

The solution is also highly configurable to users’ specific needs. For example, the college experiences a great deal of email phishing attacks on faculty, staff and students. “We were able to create a dashboard for ourselves,” says Frank. “When a phishing attack comes in and gets through our protection barrier, we’re quickly able to pivot through the data, whether it’s subject line, senders, receivers or content of a message and quickly pick out those messages and understand how deep they got into our organization, what the spread was and how many users were impacted.”

The security team can then follow up with users to alert them to the fact that they’ve received a phishing message, and request that they let the team know if they’ve interacted with it. The Mohawk team can also remove the messages from the email server before other users engage with them.

Mohawk was also looking to the future when it chose the QRadar solution. Although not currently running QRadar in the cloud, Mohawk can take advantage of the QRadar Cloud Visibility app. “We wanted to make sure that we were picking a solution that is future-proof to be able to ingest information from the public clouds, should we end up in that position,” says Frank. “If we decide to place our instance in the cloud, as opposed to running it on site, QRadar really meets those needs for us and really differentiated itself.”

can cost-effectively collect, parse and store large volumes of security and IT operations data. With all security data in one place, Mohawk can achieve easier compliance reporting, gain more insightful results and provide teams with a more-robust data set to query. This both simplified the implementation and reduced costs for Mohawk, which was another differentiator that helped the college choose the QRadar solution.

GlassHouse worked with the security team to tune the system so that it sifts out the alerts that don't require immediate remediation. According to Jeff Wilson, Director of Cloud and Managed Services Sales at GlassHouse, "We want to get to actionable data ... the 10% that you want to focus on, figure out the root cause and remediate quickly."

Frank is pleased with the hands-on assistance from GlassHouse. "We did need professional services to be able to get to that point," he says. "We really worked with GlassHouse to work to ... make sure that we have it properly tuned for our environment. So now we know that when we do have a potential compromise in the future, we're not sifting through so much data and we have a fairly clean interface."

> "We want to get to actionable data ... the 10% that you want to focus on, figure out the root cause and remediate quickly."
>
> **— Jeff Wilson, Director of Cloud and Managed Services Sales, IBM Business Partner GlassHouse Systems**

Results story

"It's all about visibility"

Even with the best cybersecurity protection systems, some threats get through. And if the security team can't see the threat, it can't respond to it. Now, after implementing QRadar, Mohawk can quickly spot and respond to cybersecurity breaches.

"It's all about visibility," says Frank. "Being able to see what's happening on the network, being able to see how the different machines connect and communicate with each other. It's about creating alerts to be able to see if there's a potential compromise in the network

Frank contrasts the previous complexity of overseeing the Mohawk security system and the current simplicity of viewing it with the QRadar dashboard. “If you can imagine, in a large organization, you can have many different security tools and appliances,” he says. “From anti-malware on the endpoints, to the data center, to firewalls — external to the organization, and also internally in different locations — intrusion prevention sensors among others.” Previously, these elements all had all their own unique interfaces that his security team had to log into individually to view possible threats. And there were many of each element, scaled across the organization in different departments, campuses and locations.

“Now, QRadar ingests all that data into one pane of glass for us to look at,” Frank says. “And then all the alerts, warnings and potential threats that come up out of those solutions, those are really prioritized in a risk-based approach for us to investigate. So, it really does assist with sifting through information; it makes it quick and it makes sure that we’re focusing on those top risks or threats.”

Mohawk also uses QRadar Data Store to provide centralized log management, which boosts Payment Card Industry Data Security Standard (PCI DSS) compliance for the college. Centralized logging also helps the operations team, according to Frank. “When we’re troubleshooting issues in the data center that are not security related, the operations team now has access to be able to dig into the details,” he says. “They can do searches to find the information that they need quickly without having to manually go into each and every machine and try to manually review the logs. I think it speeds up a number of challenges that the average infrastructure team is going to face.”

Frank is glad that that the college chose to work with an IBM Business Partner like GlassHouse and lauds the GlassHouse team: “They not only had really high-quality, technical and knowledgeable staff around QRadar, but also cybersecurity in general. We were absolutely impressed.”

Jeff Wilson, of GlassHouse, in turn explains why having a close relationship with Mohawk has engendered success. “There’s nothing in Mohawk’s environment that has been difficult in terms of integrating into QRadar,” he says. “In security, having a tight and effective engagement with a customer — understanding their processes, understanding their infrastructure and their software environment and where their most critical data is — is really important to delivering security and finding ways to patch holes that exist. And so that

The engagement has also been successful thanks to support from the college board and buy in from other departments, such as the operations and infrastructure teams, who have already reaped benefits from the QRadar solution. “They understand what the tool is, how it works, and how in their unique departments, they can start to see benefit from the tooling itself,” says Frank. “I think that was a critical success factor as well as getting everybody to board the bus and driving it together to find the right solution internally at the college.”

The college is building synergy between its behind-the-scenes security department and its academic programs by offering courses in cybersecurity that include SIEM. Ultimately, its use of the QRadar platform may become a recruiting tool, as students who want to build skills in a high-demand arena like cybersecurity will see that the college is practicing what it teaches by implementing a state-of-the-art SIEM solution.

> “If we decide to place our incidents in the cloud as opposed to running it on site, QRadar really meets those needs for us and really differentiated itself.”
>
> **— Andrew Frank, Manager of IT Security Services, Mohawk College**

Mohawk College & GlassHouse

Founded in 1966, Mohawk, located in Hamilton, Ontario, Canada, positions itself as a postsecondary destination renowned for its innovation culture. Its mission is to educate and prepare highly skilled graduates for success and contribution to the community, Mohawk College educates more than 32,500 full-time, part-time, apprenticeship and international students, with approximately 1,000 faculty. It operates three main campuses: Fennell, Stoney Creek and the Mohawk-McMaster Institute for Applied Health Sciences at McMaster University.

their IT environments. The company has expertise in and provides solutions for cloud, managed services, enterprise security, infrastructure and more. It operates from its Canadian corporate headquarters in Toronto, and its US headquarters in Lisle, Illinois, and employs approximately 80 people.

Solution component

- QRadar Security Info and Event Management

Take the next step

To learn more about the IBM solutions featured in this story, please contact your IBM representative or IBM Business Partner.

Print

View more client stories

Produced in the United States of America, April 2021.

might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

This document is current as of the initial date of publication and may be changed by IBM at any time. IBM Business Partners set their own prices, which may vary. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.