Seneca

Seneca Scores High on Security With Threat Intelligence From Recorded Future

Overview

Combining career and professional skills training with theoretical knowledge, Seneca's expert faculty provide a polytechnic education to 30,000 full-time and 60,000 part-time students. With campuses in Toronto, York Region, and Peterborough, and education partners around the world, Seneca offers degrees, graduate certificates, diplomas, and certificates in more than 300 full-time, part-time, and online programs. Seneca's credentials are renowned for their quality and respected by employers. Co-op and work placements, applied research projects, entrepreneurial opportunities, and the latest technology ensure that Seneca graduates are highly skilled and ready to work.

Challenge

The higher education sector is increasingly attracting cybercriminals. In fact, it is three times more susceptible to phishing attacks than the retail sector. To combat these risks, Seneca College looked for an intelligence solution that could help them reduce threat research time, better understand relevant risk, and make confident decisions faster.

Solution

Seneca turned to the Recorded Future® Platform to streamline and accelerate threat detection and response, while gaining a more comprehensive, real-world view of risk.

Results

With Recorded Future, the Seneca team was able to:

- Scale their investigation efforts and access the information they need, when they need it, to make risk-prioritized decisions
- Free up time, resulting in more robust cybersecurity measures
- Enrich their security response to more proactively block malicious IP addresses as well as addresses that might pose a risk in the future

> “Recorded Future automatically pulls from a huge range of sources, enabling us to scale our investigation efforts and access the information we need, when we need it, to make risk-prioritized decisions.”

Challenge

Chock-full of personal information on employees and students along with valuable research material, the higher education sector is increasingly attracting cybercriminals. In fact, the latest Verizon 2019 Data Breach Investigations Report reveals that the education industry is three times more susceptible to phishing attacks than the retail sector. Seneca’s security team is responsible for a wide range of initiatives that prioritize data breach prevention, detection, and response. Led by Joseph Lee, manager of security and compliance, the team sought a threat intelligence solution that could help them reduce threat research time, better understand relevant risk, and make confident decisions faster.

Historically, the team had relied on a number of tools like Pastebin alerts to track keywords of interest, as well as an on-premises solution that identified threats inside the network. But these disparate sources of threat information didn’t paint a full picture, and required quite a bit of detective work. Says Lee, “We would identify a potential phishing email coming in and have to do a lot of manual work to figure out if the URL was indeed malicious, and if so, what it was trying to do. Or, we’d see an IP address trying to poke into our servers and we’d have to manually run them against various external sources to see if it was really a malicious IP.”

In addition to spending valuable time trying to decode and operationalize in-network threat data, the team lacked visibility into external threat indicators. “We had limited visibility into what was going on outside our organization. If someone was working against us on the dark web, for example, we had no way of seeing it,” says Lee.

Solution

Lee and his team turned to the Recorded Future® Platform to streamline and accelerate threat detection and response, while gaining a more comprehensive, real-world view of risk. "With Recorded Future, we can automatically cross-reference malicious IPs and URLs and get meaningful, up-to-date context on each threat — from Risk Scores to timelines of suspicious behavior to information on associated campaigns," says Lee.

Recorded Future's machine intelligence also helps the team rapidly connect the dots across the broadest set of external threat data sources. By setting up alerts to track keyword mentions across technical, open web, and closed/dark sources, the team can pinpoint previously unidentifiable threats. For example, shortly after deploying Recorded Future, the team identified a landing page in a foreign country and in a foreign language that was selling counterfeit Seneca diplomas. Recorded Future translated and analyzed this information, enabling the security team to quickly address the issue with Seneca executives. "That incident was particularly eye-opening for our leadership team and helped us clearly demonstrate the value of Recorded Future in reducing risk and positively impacting the organization."

The Seneca team was particularly impressed with Recorded Future's seamless integration into Palo Alto's MineMeld, a threat aggregation tool they use at Seneca. Recorded Future's contextualized threat intelligence helps to rapidly identify and prioritize cyber threats such as malicious IPs, which are then fed to MineMeld and that in turn triggered a dynamic block by the Palo Alto firewall.

Recorded Future also adds valuable insight into Seneca's existing threat feeds from Sumo Logic and CrowdStrike. "With Recorded Future, we're able to automatically assign Risk Scores to IP addresses, domains, hashes, and vulnerabilities, which are based on a set of risk rules that trigger based on specific evidence. We now have the ability to fine-tune whether we want to aggressively block everything that is suspicious out there, or if we want to selectively block things with suspicious ratings over a certain threshold," says Lee.

Results

After deploying the Recorded Future solution, the Seneca security team began realizing productivity gains almost immediately. "With limited resources and a tight timeline, we'd previously only be able to research threat events on one or two internet sources before moving on. Recorded Future automatically pulls from a huge range of sources, enabling us to scale our investigation efforts and access the information we need, when we need it, to make risk-prioritized decisions."

This automation has resulted in additional time for the Seneca team to implement more proactive cybersecurity measures. Says Lee, "Before, when we'd see a malicious IP address or URL coming in, we'd block it — and that would be the end of it. Recorded Future has helped to enrich our security response so that we now not only block that IP or URL, but we can also block associated ones that may be targeting us soon."

Encouraged by these early successes, Lee plans to extend Recorded Future use cases to his newly inherited data privacy division. "By automating manual investigation, streamlining workflows, and greatly enhancing our threat data, Recorded Future is helping us take a more proactive stance to cybersecurity across the organization."

Recorded Future®

www.recordedfuture.com

@RecordedFuture

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.