The McGill University Health Centre (MUHC)

Strengthening its security posture with in-depth global intelligence

Centre universitaire de santé McGill — McGill University Health Centre

Overview

The need

MUHC security staff wanted to more quickly identify and assess potential threats and security exposures.

The solution

A security intelligence solution based on IBM and Trend Micro software helps MUHC rapidly detect and respond to attacks, and offers a platform to reduce the time and cost of vulnerability management.

The benefit

The platform currently analyzes 700 events per second, correlating network noise into a coherent story that helps staff uncover and stop approximately five major security attacks annually.

The McGill University Health Centre (MUHC) is one of the world's foremost academic health centers. Each year, the MUHC treats almost 40,000 inpatients and realizes more than 700,000 ambulatory visits while performing almost 35,000 surgeries. Its Research Institute is the second largest medical and life sciences research facility of its kind in Canada.

Detecting security threats early

Health records are a valuable commodity on the black market as cybercriminals seek social security numbers and other personal information that can be used in identity theft. At the MUHC, work began several years ago to implement a global surveillance platform that would help security personnel more quickly identify and respond to potential threats, and better protect electronic patient information and network operations.

A priority for the MUHC is finding security weaknesses and minimizing potential risks across its network. "Vulnerability management and manual scanning can be extremely time consuming—primarily in terms of resolution, but also in terms of identification," says a senior security analyst with the MUHC Center of Surveillance and Security (CSS). "The key for us is to focus on the issues that have 'pertinent applicability' in which the combination of exposure and threat exists in the context of a teaching hospital. With QRadar software, we can gain that visibility instantly and be more proactive to address security weaknesses rapidly."

IBM

Solution components

Software

- IBM® QRadar® Security Intelligence Platform
  - IBM Security QRadar SIEM
  - IBM Security QRadar Risk Manager
  - IBM Security QRadar Vulnerability Manager
- Trend Micro Deep Discovery

IBM Business Partner

- Trend Micro

The open source tools that the MUHC previously used required a lot of time in terms of management and lacked the intelligence of an enterprise-level correlation system, which the security team required to efficiently monitor a health organization that is comprised of six hospitals.

"Global visibility and fast response across our network are critical to protecting our infrastructure," says a senior security analyst with the MUHC Center of Surveillance and Security (CSS). "It can cost millions to get back into operation if systems are infected, so early detection is critical."

Applying advanced analytics and anomaly detection

Working with IBM and Trend Micro, the MUHC implemented a sophisticated, integrated security intelligence platform that helps it detect and respond to attacks that could otherwise get lost in the "noise."

"Upper management supported our vision to increase network visibility using IBM QRadar and Trend Micro software," says a CSS senior security analyst.

IBM® Security QRadar® software provides advanced analytics and anomaly detection capabilities to help turn event data from roughly 3,000 network assets, including servers, network devices, and security devices and applications, into actionable insight. The organization also plans to incorporate activity from clinical applications.

Security staff can quickly determine if seemingly disparate incidents are somehow related and whether the issue is an operational one (for example, a network outage can be caused by a non-validated configuration) or a security threat.

The team also has more visibility into custom-systems that can't run virus protection software due to vendors' guidelines.

"We can identify threats as they emerge, and act quickly so we can stop them very early on, before they can do any damage."

—A Senior Security Analyst, Center of Surveillance and Security, The McGill University Health Centre

"We have exceptions on our network that can't follow our standards," says a CSS senior security analyst. "With this solution, we can monitor these systems and act quickly if any performs an action that is a threat to itself or to other machines on the network."

Detecting zero-day attacks and known malware

Malware-based threats are common to all organizations, especially to the MUHC, which has a heterogeneous environment consisting of students, executives, clinicians, researchers, contractors, suppliers and more. In a new era of BYOD (bring your own device), the spread vectors are constantly increasing and require security teams to be on a constant watch for known and unknown threats that can only be recognized through abnormal behavior or specialized detection systems.

According to a CSS senior security analyst at the MUHC, by integrating Trend Micro Deep Discovery with the QRadar platform, the security team is better able to uncover malware-driven attacks that may be designed to steal sensitive information or employee credentials, or to interrupt operations.

The software inspects network traffic for evasive threats, such as zero-day malware, and feeds the information into the QRadar platform, to enable rapid response.

"Before, it could take days to analyze something that was behaving abnormally on the network and recognize the cause as a malicious piece of software," says a CSS senior security analyst. "Now, we can do that in a few minutes and see if, and where, an infection is propagating so we can respond immediately."

Thwarting potential attacks

The platform currently analyzes 700 events per second, correlating millions of events into a coherent "story" that has helped the MUHC security personnel reduce incident response time and thwart attacks.

"We typically uncover approximately five serious cases a year," says a CSS senior security analyst. "We can identify threats as they emerge, and act quickly so we can stop them very early on, before they can do any damage."

The organization's short-term priority is to include context into events by working with IBM to integrate vulnerability and risk-related information with the existing protection measures in place. This work will increase the level of intelligence in high-priority risk identification to help MUHC reduce the time and effort required in prioritizing actionable events, which, in turn, helps security staff to reduce the organization's overall risk.

"By combining asset vulnerability information based on the network with application data that provides the actual degree of exposure to an identified threat, we can more quickly see if we have potential holes in our network that require imminent attention, and we can understand the risk, so we can concentrate on the riskiest issues first," says a CSS senior security analyst.

Teaming with IT to improve operations

A side benefit, according to the MUHC, has been improved network performance and availability.

"We've been able to identify and help our IT staff in validating configurations that might affect network or system availability and create noise on the wire, which can reduce the security visibility," says a CSS senior security analyst. "We have shown in numerous cases the value of the platform to both business and IT executives, and QRadar is now part of organizational processes, such as troubleshooting, forensics, monitoring and alerting. A quick demo caught our executives' attention and won them over quickly."

He concludes, "The load of information that we have to treat from infrastructure IT systems, administrative systems, clinical applications and biomedical systems is overwhelming for any security team in a similar context. QRadar helps clear the noise on the wire and enables us to gain the clarity we need to evaluate the threats efficiently. In a world of interconnectivity and network convergence, QRadar also brings value to the business. Monitoring biomedical equipment critical to human life and confirming its availability is a clear example of how security becomes a business enabler and not just an IT 'toy.'"

Take the next step

To learn more about IBM Security software, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/security

For more information about Trend Micro, visit: http://www.trendmicro.com/deepdiscovery

For more information about the McGill University Health Centre, visit: www.muhc.ca

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
July 2015

This document is current as of the initial date of publication and may be changed by IBM at any time. 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.

Trend Micro Deep Discovery is not an IBM product or offering. Deep Discovery is sold or licensed, as the case may be, to users under Trend Micro's terms and conditions, which are provided with the product or offering. Availability, and any and all warranties, services and support for Deep Discovery is the direct responsibility of, and is provided directly to users by, Trend Micro.

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.

Please Recycle

Facts provided by: Youssef Jad, Senior Security Analyst, Surveillance and Security Center, The McGill University Health Centre

WGC12384-USEN-01