CASE STUDY

HITACHI
Inspire the Next

MANAGED SECURITY SERVICES FOR MUNICIPALITIES

QUICK FACTS

Industry: Public Sector

Company Type: Municipality

Location: Canada

Employees: 10,000+

Needs & Requirements:

- Secure corporate IT assets against vulnerabilities and intrusions
- Meet annual PCI DSS compliance requirements
- Report findings to executive team
- Monitor infrastructure on a 24/7 basis and liberate in-house IT team

THE CHALLENGE

The City has experienced explosive growth due to major migration flows in the last few years. It managed to keep up the pace serving its growing number of citizens by gaining efficiencies with the implementation of various e-services. The City provides over 250 distinct services from 15 business units to over 1 million citizens. Many of these services are supported by the City's Information Technology (IT) Computing Infrastructure, which consists of a geographically widespread network and contains multiple categories of sensitive and public data. Some segmented portions of the computing environment are subject to rigorous compliance requirements, such as the Payment Card Industry Data Security Standard (PCI DSS), or have extremely high availability requirements, such as the Police and Fire Department communications environment with a required uptime of 99.999%.

Similar to many other Information Security teams within municipal governments, the City's team consisted of a small number of analysts providing reactive services during normal week days. Evenings, graveyard shifts and weekends were covered by pager rotation for critical incidents. With successful security breach times being measured in minutes but an organization's ability to react to a breach measured in days, weeks, or months, time is on the attacker's side based on the traditional security "best of breed" investment model.

Also, the City's Security Information Event Management (SIEM) solution came to end-of-life status and did not bring any value because IT staff simply lacked the time to maintain the solution and keep the business rules up to date.

THE SOLUTION

Struggling to recruit and retain the specialized resources required for proactive 24/7 security monitoring, the City decided to engage a Canadian Managed Security Services Provider (MSSP) to complement its internal team and manage alerts generated by the tools already deployed in its environment.

Hitachi Systems Security Inc. deployed its Threat Monitoring Service, which consists of continuous real-time monitoring and management of internal and external threats to the City's network environment. Supported by Hitachi Systems Security Inc.'s certified Information Security Analysts, a tailored event correlation and incident handling workflow was customized to the City's threat management requirements and processes. Now every threat event, data loss, or malicious activity is identified and validated by the Hitachi Systems Security Inc. team who then escalates the potential threat to the City's IT staff so that corrective action can be taken.

Log management services were also deployed to extend threat management capabilities, providing vital referential data via access to historical log information collected and processed. This service is critical to proper investigation of breaches, can support auditing and is a required component of many compliance programs such as PCI DSS. All of those services are offered from any of Hitachi Systems Security Inc.'s global network of Security Operations Centers (SOCs).

MAIN BENEFITS

Thanks to Hitachi Systems Security Inc.'s managed security services, the City benefits from a 24/7 incident response team – an organizational necessity in today's world of insider and advanced targeted threats – and was able to:

- ✓ Gain real-time visibility of the threats affecting the City's IT environment in a prioritized fashion
- ✓ Facilitate PCI DSS annual audits thanks to the audit trail left by the threat monitoring console
- ✓ Achieve far superior reaction time to security incidents
- ✓ Increase signal to noise ratio so City staff could be involved only when their precious time was needed
- ✓ Improve management reporting with monthly executive reports, generated by Hitachi Systems Security Inc.'s certified Information Security Analysts
- ✓ Harden the City's overall security posture
- ✓ Achieve consistency and efficiencies across the organization, leaving the City's IT security staff more time to engage in value-added activities
- ✓ Utilize the $100,000 annual license and maintenance fees related to the complex SIEM solution in a more cost effective fashion, with 24/7 proactive, managed security services from independent experts

SERVICES PROVIDED

A team of Hitachi Systems Security Inc.'s Senior Cyber Security Experts collaborated with the City's IT security resources on this engagement to:

- Perform continuous 24/7/365 Cyber Security Monitoring of its IT infrastructure
- Deploy a large sensor, intended as replacement for the end-of-life SIEM solution
- Configure the service and personalize the correlation engine, driving endless iterative increases in effectiveness
- Escalate all threat activity within 15 minutes
- Offer self-serve Vulnerability Scanning
- Provide on-site Data Archival for historical log investigations and meeting compliance requirements

Hitachi Systems Security Inc.
955 boul. Michèle-Bohec, Suite 244, Blainville (Québec) J7C 5J6 Canada
Tel: +1 450-430-8166   Fax: +1 450-430-1858
www.hitachi-systems-security.com