Netsurion | EventTracker®

Case Study

Co-Managed SIEM - Local Government

GOVERNMENT

About the City:

This Canadian city of 100,000 has been serving its citizens for over 80 years as part of a one million-plus greater metropolitan region that includes a Canadian Forces military installation. Protecting its citizen and employee data and privacy is crucial to avoid cyber threats like costly ransomware attacks and downtime of city services. The city sought a cybersecurity solution that would augment their IT team while also reducing complexity and cost.

"Netsurion provides 24/7 coverage and reduces false positives. Our small IT and security staff are too busy to chase after log data manually. It's a huge time saver to have all the actionable intelligence and remediation recommendations in one place."

-Cybersecurity Manager, Canadian City

The Challenge

Cyber crime is an area of rising concern for enterprises and government entities alike. Always-on connectivity and internet-driven citizen services have improved local government efficiency and effectiveness but have also increased risk. The sophistication and volume of threats against local government entities have increased in recent years, resulting in data breaches like those that have plagued larger enterprise organizations. While the city had anti-virus software and next-gen firewalls, they knew that advanced threats were evading these basic security tools. They needed the real-time visibility and monitoring that a Security Information and Event Management (SIEM) platform provides. Technology alone, however, is difficult to operationalize and maintain. A co-managed SIEM service with a comprehensive SOC would provide early detection of targeted threats as well as rapid identification of anomalous activity.

Without a co-managed SIEM, their team experienced:

- A lack of IT and security staff to address emerging threats
- Limited visibility into comprehensive cybersecurity activities
- Manual log collection and correlation that was prone to false positives

The city was looking for a solution that could deliver and orchestrate all the critical cybersecurity capabilities needed to predict, prevent, detect, and respond to potential security incidents.

Solution - Why Netsurion's Co-Managed SIEM

The Canadian city evaluated SOC-as-a-Service (SOCaaS) providers in a structured procurement process that involved Netsurion and two other vendors. During the vendor selection process, Netsurion analyzed the municipality's IT requirements and cybersecurity maturity to propose a SIEM solution that reduced cost and complexity. "Netsurion was the most comprehensive and had the best follow-through to our requirements. It was a painless process, and they answered all of our business and technology questions quickly," stated the IT Manager for the Canadian city.

Protection Against Advanced Threats

As a mid-sized municipality, the city was concerned that they were "low-hanging fruit" for threat actors looking to monetize data or make a political statement. While perfect prevention is not possible, speedy detection of threats and rapid remediation minimize damage. "Ransomware risks are front and center with our small IT team. Canada has seen attacks where data was held for ransom increase significantly in recent years, with incidents regularly in the news media," summarized the cybersecurity manager. "We knew we needed to take action to better protect citizen data."

Comprehensive 24/7/365 Monitoring

The IT team has been able to prioritize incidents and alerts based on Netsurion's co-managed SIEM recommendations and mitigation priorities. Previously, the IT team was merely reacting to the noise of millions of events and incidents, many of which are false positives that waste the municipality's time. The User & Event Behavior Analytics (UEBA) built into Netsurion's EventTracker SOC-as-a-Service pinpoints suspicious activity that varies from the baseline and identifies unknown attacks. "Netsurion's EventTracker SOC is our eyes and ears with proactive visibility 24/7 that enables our team to focus on other strategic priorities and projects," stated the IT manager.

SOC-as-a-Service from Netsurion met all their needs:

- Uphold the trust of citizens and supply-chain partners
- Detect threats that traditional anti-malware and firewalls overlook
- Simplify cybersecurity monitoring and alerting
- Prioritize remediation recommendation with dashboards and reports

Reports Accelerate Time-to-Value

Netsurion provides comprehensive reports and dashboards that improve security and early threat detection for the growing city. Highly-trained experts in the EventTracker SOC further analyze log data from disparate sources to eliminate false positives and reduce alert fatigue with easy-to-interpret reports for technical users and executive decision makers. According to the Canadian city team, one of the most important benefits of using Netsurion's EventTracker is prioritizing anomalous activity that is worth investigation and follow up. "We thoroughly review the reports from Netsurion. For example, we were notified of devices with no activity to perform forensic analysis to determine if the device was lost, compromised, or if the user merely on an extended vacation. Netsurion has been very agile and flexible to work with," noted the city's security expert.

Results

Netsurion offers one of the most advanced solutions for resource-constrained government entities to enhance security, simplify IT operations, and protect sensitive data. We help organizations predict, prevent, and detect threats while the SOC analysts enable organizations to respond quickly and efficiently without alert fatigue. Netsurion ensures a comprehensive approach with SOC-as-a-Service that prioritizes areas to devote finite resources. We combine people, processes, and technology to remain vigilant given the rising volume of advanced cybersecurity attacks targeting government entities.

With Netsurion, the city can:

- Achieve 24/7/365 SOC monitoring
- Deliver advanced threat protection against internal and external threats
- Enhance IT efficiency and effectiveness
- Reduce cybersecurity risk with prioritized remediation recommendations.

"Netsurion helps us sleep better at night with increased visibility and continuous insights that we can't produce on our own with our large volume of log files."