opentext™ | Cybersecurity

Case Study

PwC Canada

ArcSight steps up to detect advanced threats on critical infrastructure clients in North America with scalable and flexible threat hunting.

Who is PwC Canada?

PwC Canada's Partners and staff are located coast to coast and bring their expertise to provide quality services and products that help solve important problems. PwC's Cybersecurity team helps its clients unite existing lines of defense against modern-day threats. PwC brings together a multidisciplinary team that includes professionals in the areas of cybersecurity, financial crime and industrial systems, to help develop strategies that will cut across the vertical and functional silos.

Globally, PwC has offices in 152 countries and employs more than 328,000 people. PwC is among the leading advisory and professional services networks of firms in the world.

"The ArcSight out-of-the-box capabilities of world-class SOAR, great threat hunting, and rapid reporting and analytics functions make it a great end-to-end solution for our utilities clients."

Umang Handa
Partner, National Lead, Managed Security Services, Cybersecurity and Privacy
PwC Canada

Next-Level Security Solution to Protect National Critical Infrastructures

When the PwC Canada team is approached by utilities clients who provide national critical infrastructure such as power generation and transmission, substation distribution systems, and water treatment—many things need to be considered, as Umang Handa, Partner, National Lead, Managed Security Services, Cybersecurity and Privacy, PwC Canada, explains: "We have to remember that these companies are heavily regulated and need to comply with the standards of North American Electric Reliability Corporation (NERC), whose mission it is to ensure the reliability of the North American bulk power system. On a practical level, the nature of these clients often means that we need to monitor and manage remote sites in low-bandwidth locations, which may have performance implications as we pull data from them. In short, finding a cybersecurity solution to manage these complex and sensitive environments is a challenge."

Looking for a flexible and scalable solution able to provide leading threat detection and response, as well as automation capabilities, the team found ArcSight Enterprise Security Manager (ESM) by OpenText™. ArcSight is designed to reduce threat exposure by

pwc

At a Glance

Industry

Services

Location

Canada

Challenge

Protect national critical infrastructure clients who are subject to strict NERC regulations and typically operate complex and sensitive environments

Products and Services

ArcSight Enterprise Security Manager
ArcSight SOAR
Galaxy

Success Highlights

- Built-in SOAR solution saves time and improves efficiency
- Secure multi-tenancy provides cost-effective hosting opportunities
- Advanced out-of-the-box capabilities enable easy and fast deployment
- Full NERC compliance through sophisticated threat hunting
- CyDNA to detect the threat actors that are targeting PwC clients

> **"We appreciate that ArcSight ESM includes a powerful SOAR engine. This accelerates effective incident response with intelligent automation. It saves our clients time and improves their operational efficiency."**
>
> **Umang Handa**
> Partner, National Lead, Managed Security Services, Cybersecurity and Privacy
> PwC Canada

Connect with Us
www.opentext.com

detecting threats in real time with powerful and adaptable security information and event management (SIEM) correlation analytics with a native security orchestration, automation and response (SOAR) solution.

ArcSight Has Versatility for Clients of Different Sizes

"One of our key requirements was automation," recalls Handa. "We appreciate that ArcSight ESM includes a powerful SOAR engine. This accelerates effective incident response with intelligent automation. It saves our clients time and improves their operational efficiency. We also found that ArcSight ESM was easy to deploy, even within complex hybrid or multi-cloud environments."

Not all of PwC's clients are large enterprises, and the PwC Canada team sees value in hosting ArcSight ESM in a secure multi-tenanted environment. Many companies understand the benefits of a SIEM, but assume they are too expensive. By using PwC's ArcSight ESM hosting and event monitoring to PwC Canada in a multi-tenanted fashion, they are pleasantly surprised to find that this is an affordable proposition after all. ArcSight ESM includes a threat modeling engine to get them up and running quickly. This is enhanced by PwC Canada's own threat hunting models.

A Winning Team: Advanced Threat Hunting Combined with PwC Cybersecurity Expertise

PwC Canada appreciates the ongoing efforts of the Cybersecurity team by OpenText™ to enhance the ArcSight offering. One such effort is the launch of the new Galaxy solution, which integrates with ArcSight. Galaxy is an immersive cyberthreat experience that provides actionable and business-centric intelligence for security executives, enabling them to quickly gain visibility into the most pressing threats to their business and help secure the value chain. This community-based platform accelerates executive understanding of cyber risk, drives faster business risk decisions, and reduces the cost to deploy proactive cyber resiliency measures.

"This is an exciting development," notes Handa. "With the major digital transformation that is happening on an unprecedented scale, the importance of cybersecurity and cyber resilience continues to grow for organizations, no matter their industry or region. Galaxy provides a platform where CISOs, SecOps, ITOps, and internal auditing teams can get a full view of the latest threats, together with an insightful action plan to harden their organization's overall cyber defense."

He concludes: "The ArcSight out-of-the-box capabilities of world-class SOAR, great threat hunting, and rapid reporting and analytics functions make it a great end-to-end solution for our utilities clients. In this modern day and age with advanced threat actors, our clients need an open and transparent view into their threat detection and automated response, and this is exactly what we deliver with ArcSight, combined with our own services and cybersecurity expertise."

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.