Hewlett Packard Enterprise

Case Study

Zayo Group builds world-class security operations center for cyber defense

Protects clients with HPE Security ArcSight

Objective
Launch new global security operations center to enhance managed security services to proactively defend government and commercial clients against cyber threats

Approach
Engage HPE Security Intelligence and Operations Consulting (SIOC) to design global security operations center (GSOC) and build HPE Security ArcSight framework

IT Matters
- Monitors up to 1,000+ devices per client
- Enables real-time correlation
- Shrinks remediation time
- Meet FIPS 140-2/SSAE-16 requirements
- Boosts stability with certified connectors to leading security products

Business Matters
- Shrinks time-to-launch
- Delivers lower ownership costs than competitive platforms
- Ensures scale for global SOCs
- Accommodates dedicated and multi-tenant commercial clients
- Builds revenue from high-value services

The launch of an expanded Managed Security Service Provider (MSSP) practice promised to be a win-win opportunity for communications infrastructure company, Zayo Group and its customers. But delivering the highest level of security and controls meant building a state-of-the-art global security operations center (GSOC)—from the ground up and on an accelerated schedule driven by revenue goals and emerging market opportunities.

In just six months, working with experts from HPE Security Intelligence and Operations Consulting (SIOC) services, the Zayo team built a multi-zone, Public Works and Government Services Canada (PWGSC)-certified GSOC for delivering services to both enterprise and government clients. This world-class facility from Zayo Group helps clients proactively defend against cyber threats. Through Zayo's Advanced Threat Management Security portfolio that integrates the HPE Security ArcSight security information and event management (SIEM) platform, clients gain access to usable incident data and GSOC services, including advanced analytics and threat hunting technologies that reduce risk landscapes and optimize protection.

The challenge

Build a world-class GSOC, from the ground up

The project began in early 2015 within the communications infrastructure group at Allstream, Inc., a leading Canadian communications provider, prior to its acquisition by Zayo Group in Q1 2016. Mike Vamvakaris, Vice President of Managed Cyber Security at Zayo Group, was there from the beginning. "We were competing for the opportunity to build a secure WAN for a major government client. To win the business, we had to prove the security of our backbone and the network endpoints from which we

"We evaluated numerous competitive offerings, but ArcSight offered multiple unique advantages, including support for FIPS 140-2 encryption, multi-tenancy, and the ArcSight Connector library for out-of-the-box integration with commercial security products."

– Mike Vamvakaris, Vice President, Managed Cyber Security, Zayo Group

would provision and support the WAN. As a long-time, in-house user of an HPE Security ArcSight Enterprise Security Management system, we knew the platform would meet our security management requirements for this client, including providing continuous monitoring of WAN endpoints and operating/business support systems, as well as support for FIPS 140-2 encryption."

Vamvakaris says that the bigger challenge was building a state-of-the-art global SOC to meet the zone-based access control and other stringent requirements of this client. "Although we fully understood the level of effort that would be required to win this business, we also recognized that the opportunity could serve as a springboard for an expansion of our MSSP practice. The challenge was building out a GSOC with all of the critical elements—including the full triad of technology, people, and processes—to deliver managed security services not only to this client, but to multiple high-end financial services, healthcare, retail, and government organizations from our existing customer base and adjacent market verticals. We needed to move quickly to take advantage of immediate opportunities and to achieve our aggressive first-year revenue objectives."

The solution

HPE SIOC expertise and the HPE Security ArcSight SIEM platform

Working with HPE SIOC, the Zayo Group team completed the physical GSOC in six months and launched its expanded MSSP offering just 12 months later. "The HPE SIOC team was instrumental to our success," continues Vamvakaris. "They provided the best security practices to build out our infrastructure, our global SOC facility with five-zone access controls, and incident workflow processes."

Today, HPE ArcSight serves as the MSSP SIEM platform and is packaged with the Zayo Group Advanced Threat Management Security portfolio. Services include threat-feed monitoring and correlation, threat mitigation, security forensics, and other related professional services. The MSSP practice provides services to both Zayo Group and external clients.

The HPE ArcSight platform aggregates data for centralized monitoring and rapid response to threats. ArcSight provides granular, real-time correlation rules that allow Zayo to create use cases against very specific customer requirements. Current use cases

include role-based access control, unidentified and unauthorized changes, traffic to/from malicious sites (utilizing HPE Reputation Security Monitor), unexpected process aborts, file integrity monitoring, and unauthorized device additions.

> "The HPE SIOC team provided invaluable assistance in helping us find, onboard, and train analysts in preparation for launch. Their expertise was invaluable, start to finish."
>
> –Mike Vamvakaris, Vice President, Managed Cyber Security, Zayo Group

HPE SIOC experts assisted the Zayo team throughout the GSOC project, from design and blueprinting of the physical GSOC to onboarding talent, training security analysts, and providing expertise for proposal responses. The SIOC team worked with Zayo to expand its ArcSight footprint to support the expanded MSSP business, providing the framework to ensure Zayo could effectively utilize ArcSight's integrated case management system to perform best-of-breed security analysis on correlated events, track the progress of security cases, and report on their open and resolved status. This process included wrapping all critical information, from nomenclature and remediation actions, into a custom wiki platform that drives Zayo's best practices.

Zayo's ArcSight Management Console currently ingests data from more than 30 vendor applications. Nine logger appliances provide long-term data retention.

Results

World-class global SOC services

"Our new GSOC went live in 2016," reports Romona James, Senior Manager, Product Marketing, Zayo Group. "The facility is PWGSC certified and SSAE 16 certified and audited. The center features dual fiber network and power feeds, multi-zone security, including zones that require secret security clearance and two-factor biometric physical security, and other GSOC functionality. The commercial GSOC helps position Zayo Group as a leading MSSP in Canada and will provide a new stream of security-services revenues for the company. Designed for government entities and enterprises that demand the highest level of security measures and control, the GSOC offers advanced threat detection and mitigation services to help customers protect against attacks, including data loss that can cost millions of dollars and reputational value."

Case study
Zayo Group

Industry
Telecommunications

Customer at a glance

Application
Advanced Threat Management for MSSP practice

Software
- HPE Security ArcSight Enterprise Security Manager
- HPE Security ArcSight Data Platform
- HPE Security ArcSight Compliance Insight Package
- HPE Reputation Security Monitor

HPE services
- HPE Security Intelligence and Operations Consulting (SIOC)

Vamvakaris adds that HPE Security ArcSight delivers critical functionality, including the ability to integrate with third-party hunting and analytics tools. "We evaluated numerous competitive offerings, but ArcSight offered multiple unique advantages, including support for FIPS 140-2 encryption, multi-tenancy, and the ArcSight Connector library for out-of-the-box integration with commercial security products. Validated solutions simplify deployment and administration and ensure greater stability for large-scale log collection. Another important benefit that ArcSight offers is the ability to correlate multiple sources of attacks under a single pane of view—that up-levels investigative efforts, helps shrink remediation time, and boosts the productivity and effectiveness of our security analysts."

The HPE Security ArcSight SIEM platform enables an MSSP practice that can scale according to customer needs. For a single client, Zayo can monitor from five to 1,000+ devices from multiple sources and overall can provide services to nearly every size business, from mid-market companies to the largest enterprise and government clients. Vamvakaris states, "We chose this platform because it provides a complete set of SIEM solution capabilities—including a fully customizable incident investigation and management workflow—for supporting a MSSP GSOC. Every incident, ticket, threat feed, anything that we correlate plugs into ArcSight."

Global scale, cost savings, accelerated launch

"ArcSight enables cost-effective scale—none of the other products we reviewed offered scalability at a comparably low cost of ownership," notes Vamvakaris. "The ArcSight licensing model also helps reduce expenses with modular and transferrable customer licenses that minimize administrative costs. We expect to expand our practice into the United States and Europe. Of the products we evaluated, ArcSight's SIEM platform allowed us to build out Zayo's global MSSP practice quickly and cost-effectively."

Vamvakaris estimates that engaging HPE SIOC experts accelerated GSOC time-to-launch by at least 50 percent. SIOC assistance with staffing also enabled the Zayo team to rapidly build out its security team, more than doubling the number of analysts within just months. Approximately 75 percent of the team is comprised of Level 1 and 2 analysts, with the remaining 25 percent dedicated to Level 3 support.

"The HPE SIOC team provided invaluable assistance in helping us find, onboard, and train analysts in preparation for launch," comments Vamvakaris. "Their expertise was invaluable, start to finish, from GSOC design guidance to assistance in the development of our wiki and use cases that are easily tailorable to specific client requirements, to best practices, incident workflow, response management, staffing, training, and more. We could not have delivered this world-class global SOC and MSSP practice without the HPE partnership."

A partnership for customer value

"Our mission with Zayo Group's MSSP practice is to offer customers true value by helping safeguard their data and keeping pace with their rapidly evolving security needs," summarizes James. "With the HPE Security ArcSight platform and the partnership of the HPE SIOC team, we believe we have the right technology, processes, and tools to deliver that value to the enterprise market."

Learn more at
hpe.com/Software/ArcSight

Sign up for updates

Hewlett Packard Enterprise

4AA6-7468ENW, August 2016