opentext™

Case Study

Security Fusion Center

Security Fusion Center safeguards global resources every minute, every day with Security Solutions.

Challenge

When OpenText™ and HPE Software combined into one of the world's largest pure-play software companies, Brian Hanson, Chief Information Security Officer (CISO) of the combined company, found himself tasked with protecting a new business footprint and infrastructure. The protection needs were beyond those of the historical Micro Focus (now part of OpenText™) that had approximately 4,000 employees, but smaller in scale than the historical HPE solution that served over 300,000 employees.

Brian knew that for the combined OpenText™, a leading software company and the steward of product innovation and sensitive customer and employee data, he needed a world-class solution for monitoring security events that was right-sized for an organization 5% the size of legacy HPE.

Solution

Brian's team had leveraged the Cyber Security Services Security Intelligence & Operations Consulting (SIOC) group to establish the Cyber Defense Center around the ArcSight technology. Through thousands of cyber security projects across hundreds of organizations worldwide, the SIOC team had the experience, mature methodology, and best practices that ensured success for that project. As he prepared for the merger with OpenText™, Brian was able to turn to the same consulting team with a new set of requirements, and leverage a capability recently added to the OpenText™ services portfolio: ArcSight Solution Management Services by OpenText™.

These services combine SIOC and ArcSight consulting best practices with a solution for managing the ArcSight platform and providing security analysis to protect OpenText's assets, becoming the heart of OpenText Cybersecurity's new Security Fusion Center (SFC).

Rather than just integrating security products for the new organization, OpenText has systematically worked to centralize relevant event feeds from thousands of systems, servers, users, commercial and open-source products, and custom tools into security solutions with a clear business purpose in mind: to empower the SFC to perform advanced, complex analytics and relevant alerting on the threats to processes, systems, users, and data enabling its business.

OpenText IT's global footprint provides an added benefit to our product and services organizations with access to a real-world environment that enables the development, testing,

MICRO FOCUS®

At a Glance

- **Industry**
  Software & Technology
- **Location**
  United Kingdom
- **Challenge**
  Protect worldwide enterprise resources and serve as an operational best practices environment for innovation in enterprise security.
- **Products and Services**
  Solution Management Services
- **Success Highlights**
  + Protected data on a global scale for approximately 18,000 employees
  + Served as a showcase for enterprise security innovation, protecting the company's most important assets: our business processes, systems, users, and data.
  + Kept customers steps ahead of cyber threats.

and refinement of the ArcSight and NetIQ solutions by OpenText™ brings to market to help customers stay steps ahead of cyber-attacks and seamlessly conduct their business. The SFC demonstrates not only OpenText's ability to gain a collective view of the entire enterprise, but it also serves as a showcase for the enterprise security innovation protecting the company's most important assets: our business processes, systems, users, and data.

The SFC provides a forum to showcase OpenText's services expertise and the value of mature integrations of OpenText products to customers and partners.

Correlating Data across Dozens of Platforms

Security solutions that are deployed and locally managed at OpenText locations worldwide send data to the SFC to provide proactive threat detection across the enterprise.

According to Brian Hanson, Vice President of Cyber Security and CISO for OpenText IT, "At Micro Focus (now part of OpenText™), approximately six hundred million security events are actively detected per day. When a serious threat is detected, our security teams mobilize with the SFC to proactively determine the breadth, depth, and impact of a potential threat. All of the relevant information to begin a complete incident response process is at our fingertips in real time."

ArcSight Enterprise Security Manager (ESM) by OpenText™ and ArcSight Data Platform by OpenText™ work together to create a powerful, cyber defense system that is the backbone of the SFC. Each element plays a critical role in ensuring the security of OpenText's valuable information assets, which include enterprise applications, customer information systems, intellectual property assets, and all of the critical information resources available on the OpenText enterprise network.

ArcSight enables the proactive monitoring of events from dozens of platforms from a single console and performs advanced correlation of events from multiple sources including Microsoft Windows Server Active Directory, *nix, VMware, Microsoft.net, VPNs, firewalls, IPS, network devices, web proxies, open source solutions, and databases. OpenText IT is able to capture logs from most of the sources using ArcSight's out-of-thebox connectors and use the OpenText™ FlexConnector framework to build collection logic and contextualize logs for any others.

ArcSight ESM aggregates, filters, and correlates the data, arming analysts with the robust, high-quality alerts they need to perform effective security intrusion and intelligence analysis. Implementation of our security products followed the OpenText Cybersecurity Services deployment methodology, and incorporates best practices for correlation content, continuous health monitoring, and workflow operations.

Detecting Attacks

An enterprise the size of OpenText receives probes and attempts to exploit vulnerabilities hundreds of times per second. The ArcSight solution processes an average of six hundred million events daily and reduces the event flow to a volume that can be managed by the handful of analysts who are active during each SFC shift. Those analysts further refine the alerts to 10-20 incidents that are referred for follow-up and remediation action. It would take an army of analysts in the tens of thousands to perform an equivalent function manually. Without ArcSight in place, that analysis would not be performed and those events would be collected yet left unexamined, leaving attacks in progress to remain undetected.

The SFC leverages the ArcSight Activate development framework, a modular content development method designed to quickly deploy actionable use cases. The benefits of following Activate include a common development methodology that provides OpenText Cybersecurity continuity as security requirements grow and change over time, as well as detection capability for specific products and emerging threats impacting security teams each day.

ArcSight ESM provides the SFC with a centralized platform to conduct security investigations and workflow. The SFC leverages ArcSight to detect threats in real time so they can be mitigated quickly, and uses ArcSight to collect and correlate vast amounts of security data, which greatly improves the ability of analysts to pinpoint and thwart genuine threats. "The ArcSight solution provides Micro Focus (now part of OpenText™) Cyber Security comprehensive threat detection and triaging that allows us to correlate and detect real threats faster and spend valuable resources responding versus chasing false positives," says Hanson.

Partnering Internally with Professional Services

Merging two companies is no small feat. The ability to partner internally with the world-class Cyber Security Services SIOC team has allowed OpenText Cybersecurity to deploy the SFC on schedule and see value early and continuously. Brian had a need to continue monitoring the security, risks, and compliance of existing business assets while simultaneously building the capability to protect the assets of the new post-merge OpenText.

OpenText Cybersecurity Services' SIOC enabled Hanson and his team to meet these objectives on an aggressive schedule by building the SFC using ArcSight Solution Management Services (SMS). The alignment of OpenText IT objectives and ArcSight SMS capabilities were clear and provided OpenText IT with instant acquisition and ongoing retention of expertise, standardized operational processes

> **"Working with our Cyber Security consultants allowed my team to rely on experts for daily solution management and targeted response leveraging mature processes and to focus on developing orchestration capability so that I can achieve increased value with significantly less investment …"**
>
> **BRIAN HANSON**
> Vice President of Cyber Security and CISO
> Micro Focus

Connect with Us
OpenText CEO Mark Barrenechea's blog

and deliverables, and resulted in value with a single point of contact for platform management and security analysis and operations. ArcSight SMS eliminated repetitive tasks and manual handoffs through automation and allowed the OpenText Cybersecurity team to transition maintenance and operations to an experienced partner and focus on advanced security detection and risk mitigation. "Working with our Cyber Security consultants allowed my team to rely on experts for daily solution management and targeted response leveraging mature processes, and to focus on developing orchestration capability so that I can achieve increased value with significantly less investment …" says Hanson.

Matthew Shriner, Vice President of Cyber Security Services, agrees. "ArcSight SMS addressed an immediate need for OpenText™ IT. Our services are designed to help ArcSight customers who are struggling to realize the full value of their security solutions because of rapid organizational change and global shortages in cyber security talent. My team consists of hundreds of experienced security and ArcSight experts ready to help customers overcome those challenges and unlock the power of Micro Focus (now part of OpenText™) software in their environment."

Results

Preparing for the Future

For Hanson, mature operations are the constant objective for OpenText Cybersecurity and the SFC as his teams are in charge of detection of emerging threats and the effective management of the security solutions protecting the business.

Like most IT organizations, OpenText IT is responsible for managing a heterogeneous environment that provides defense-in-depth for the enterprise. Hanson expects to partner with Cybersecurity once again for one of the post-merge projects on the horizon: integration of NetIQ Sentinel by OpenText™, NetIQ Identity Governance by OpenText™ and NetIQ Access Manager by OpenText™ solutions into the SFC. By partnering with OpenText™ Professional Services, Hanson anticipates the development of a strategy that allows the IAS suite to perform what it does best and leverage the day-today operational capability of the SFC.

As OpenText continues to perform additional post-merge activities, Hanson's teams are prepared to tackle the expected increase in data sources and volume; the sophisticated, multi-stage attacks that run under the radar; and the competition for security expertise impacting all industries.

By leveraging market-leading solutions within internal operations, OpenText is extracting even more value from each security dollar so that innovations that protect its business can be passed onto its customers. The use of OpenText products and Cybersecurity Services solutions within the SFC drive a culture of continuous improvement within a real-world environment that enables the development, testing, and refinement of the solutions that OpenText brings to its customers.

Learn more at
www.microfocus.com/opentext

opentext™