Business challenge

With the introduction of a comprehensive new security regulation, the insurer needed a fast path to implementing security information and event management (SIEM) across the enterprise.

Transformation

To meet New York State compliance deadlines for its new security regulation and rapidly achieve operational sophistication, this property and casualty insurer engaged IBM Business Partner Sirius to architect, install and remotely manage an enterprise-wide IBM® QRadar® SIEM solution.

Results

Scalable solution
supports up to 40,000 EPS
and more than 5,100 devices

24x7x365
remote monitoring and management
delivers operational maturity

Rapid implementation
helped the company meet
New York State compliance deadlines

Property & casualty insurance company

Addressing new security regulatory mandates with a managed IBM QRadar SIEM solution from Sirius

This property and casualty insurance company is headquartered in the southeast US and is licensed in multiple states across the country.

"Step one was selecting the SIEM tool that would meet this client's current needs and provide a strategic platform for the future."

—Brian Reichart, Managed Security and Infrastructure Specialist, Sirius

Share this

Facing a short runway for addressing new security regulations

When the New York state Department of Financial Services (NYDFS) announced 23 New York Code Rules and Regulations 500 (23 NYCRR 500), a cybersecurity regulation for all financial institutions doing business in New York, it gave covered organizations a staggered set of implementation deadlines to meet.

Addressing the regulation's requirements fit within the plans of this property and casualty insurance company that does business in New York and several other states. It had determined that security management is a strategic business function for the company—only now it had a firm deadline with a short runway for addressing compliance.

A critical component of the compliance effort was to get an organization-wide security information and event management (SIEM) system in place and fully operational prior to the September 2018 implementation deadline for 23 NYCRR 500. The company did have SIEM tools deployed in different parts of its infrastructure, but that left devices and entities uncovered. Moreover, even with those gaps, the tools were generating more events than the current staff could handle effectively. Company leadership was not getting the detailed view it needed across the entire enterprise.

Selecting a strategic platform that supports business growth

Rather than tackling the task of choosing and implementing an enterprise-wide SIEM solution on its own, the insurance company turned to IBM Platinum Business Partner Sirius for help. The company had an existing relationship with Sirius, and Sirius was already approved to work within its IT environment—both factors that positioned the IT solutions provider to help address the company's need for speed.

> ***"Considering the company's expected 10% to 15% year-over-year growth, we really felt that a dedicated on-premises QRadar solution was correct for this client."***
>
> —Brian Reichart, Managed Services Solutions Sales Specialist, Sirius

"Step one was selecting the SIEM tool that would meet this client's current needs and, more importantly, provide a strategic platform for taking the company into the future," says Brian Reichart, Sirius Managed Services Solutions Sales Specialist, who led the engagement. Sirius recommended IBM® QRadar® SIEM, which was one of the tools already in use at the company.

"The newly appointed CISO did grill us very intensively as to why we thought QRadar was the product to go with. We also had a long discussion about the value of an on-premises deployment versus the cloud. After working through their strategic imperatives around security, and considering the company's expected 10% to 15% year-over-year growth, we really felt that a dedicated on-premises QRadar solution was correct for this client."

Among the differentiating features that contributed to the selection of QRadar over other SIEM platforms under consideration is the extensive set of standard reports included as well as the flexibility of reporting. That means little customization was required to set up the security software. The log manager platform provides fast access to data for operational review and enables analysis of activity in subsets of the environment.

The insurance company's CISO also appreciated the opportunity to add functionality through the IBM Security App Exchange, an ecosystem of developers offering apps and add-ons for QRadar and other security solutions.

With just over six months until the company's "go live" target date, Sirius went to work architecting the scalable QRadar solution and installing collectors and consoles across the insurer's three major data centers plus several remote locations. The Sirius solution includes correlation rules that filter out false positives and are critical to the efficiency of any SIEM solution, notes Reichart: "In addition to the correlation rules recommended by IBM, Sirius has developed its own set of correlations that we add. This tuning helps to significantly reduce the number of alerts that the system generates."

Achieving operational maturity with managed services

Today the insurance company's QRadar SIEM installation covers more than 5,100 devices, with new log sources being added continuously as the business grows. The solution supports the company's current workload at 24,000 events per second (EPS) with the capability to scale up to 40,000 EPS.

Monitoring and ongoing management are provided by Sirius via the Business Partner's SOC, which enabled the insurer to meet its tight deadline for achieving operational sophistication without having to build and staff its own operations center. This positioned the company to avoid potential fines and penalties from 23 NYCRR 500 while giving the insurer time it needs to staff up and equip their own SOC in the future.

> ***"Right now, we are 24x7x365 eyes on glass and hands on keyboards supporting QRadar."***
>
> —Brian Reichart, Managed Services Solutions Sales Specialist, Sirius

"Right now, we are 24x7x365 eyes on glass and hands on keyboards supporting QRadar," says Reichart. Ongoing support includes adding new correlation rules to fine tune the system, meeting with the client weekly and continuing to implement new log sources as the company adds new resources to its IT environment.

"This company has not slowed down their growth," says Reichart. "They are continuing to deploy new tools, new hardware and new servers in the environment. Those are all new log sources that we are pulling for them as we go."

Solution component

- IBM® QRadar® SIEM

Take the next step

To learn more about the IBM solutions featured in this story, please contact your IBM representative or IBM Business Partner.

About Sirius

Sirius, an IBM Platinum Business Partner, is a national integrator of technology-based business solutions that span the enterprise, including the data center and lines of business. Since its founding in 1980, Sirius has grown to be one of the largest IT solutions integrators in North America. Today, Sirius offers integrated, multivendor technology solutions that meet the requirements of the full range oforganizations, from small businesses with fewer than 500 employees to large enterprises with thousands of employees and hundreds of locations. To learn more about Sirius, visit: www.siriuscom.com

Please Recycle

86022886-USEN-01