A World-Class Pediatric Medical Center

Centralizing security and compliance management with IBM QRadar SIEM

Overview

The need

As the number of patients served is expected to increase, this world-class pediatric medical center needed a solution that would help centralize its security and compliance programs, and that could scale security operations for comprehensive visibility into the network architecture.

The solution

An advanced security information and event management solution that centralizes and correlates logs and events to provide staff with integrated security intelligence.

The benefit

Provided deep insight into network environment; detected malware that previously hadn't been identified; saved administrators time.

With incredible growth across hospital information systems, this medical center's security administration team realized it had a challenge with managing data for compliance, as well as maintaining a secure environment. With limited staff and resources, the team needed to find a way of better managing the dramatically growing logs of data.

The organization recognized that centralizing its log collection without a unifying solution was becoming burdensome in the quest to identify potential offenses on its network. With so many log sources producing disparate silos of information, the security team struggled with correlating meaningful alert information and effectively identifying potential offenses in real time.

"Prior to implementing QRadar® [now an IBM® security solution], we were filtering logs from multiple sources through SysLog, which wasn't ideal," says a security administrator for this world-class medical center. "We understood the capabilities a next-generation SIEM [security information and event management] product would provide, but we needed to educate ourselves and the management team on the solutions that would make sense for us."

"The biggest benefit to deploying QRadar was that after the initial implementation, we were up and running immediately."

—Security Administrator, A World-Class Pediatric Medical Center

Extracting intelligence and helping the Security Administration team scale

With the data environment growing daily, it was clear that scale would play an enormous factor in the decision to deploy QRadar, now an IBM security solution, especially where the number of logs was escalating to millions every day. What the team at the medical center found was that QRadar offered robust integration with so many of today's network and security components so that it could correlate data from all the log-producing sources already deployed.

"Part of the decision to deploy the solution was that our team believed we would extract more intelligence from more components with QRadar, as compared with other market solutions," says the security administrator. "Our goal was to centralize the location for where we could correlate logs and events so we could run reports out of one solution to provide us with the integrated intelligence we have been looking for."

Flow data delivers real-time intelligence

By leveraging flow data from QRadar, now an IBM security solution, this medical center can gain deep insight into its network environment that it was unable to with any solution it previously used, or was considering.

"As we deployed QRadar, I wasn't even aware of the behavioral analysis capabilities in the product," says the security administrator. "QRadar's behavioral anomaly detection functionality enables us to correlate misconfigured systems and detect malware that we weren't previously identifying. For example, this provided us with the ability to detect whether a specific machine is infected by something like a botnet."

Solution components

Software
- IBM® QRadar® SIEM

"Part of the decision to deploy the solution was that our team believed we would extract more intelligence from more components with QRadar, as compared with other market solutions."

—Security Administrator, A World-Class Pediatric Medical Center

As the team continues to scale up security operations with IBM QRadar, it is able to effectively streamline overall security process so staff can use the solution to pull the actionable information necessary from logs and events. Centralizing its program through IBM QRadar helps save the time it took pulling logs from multiple sources, as well as event information that a small team could not afford to spend the manual time analyzing.

"With a SIEM deployment, being able to collect logs upon deployment was unheard of with any other solution," says the security administrator. "I didn't have to spend a lot of time or money on professional services to start getting results, and I didn't have to coordinate extensive training for my staff because QRadar is intuitive and is easy to use."

For more information

To learn more about IBM security solutions, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/security

To increase the business value of your IBM security solutions, participate in an online community. Join the IBM security community at: http://instituteforadvancedsecurity.com

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
October 2012

This document is current as of the initial date of publication and may be changed by IBM at any time.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

Please Recycle

WGC12347-USEN-00