Healthcare IT Company Achieves Compliance through Co-Managed SIEM Services

The stakes are high: maintain the security and compliance of patient records or risk losing customer trust and credibility.

A technology company that provides services to healthcare organizations is trusted with sensitive information on a daily basis, including millions of patient records. Maintaining this trust with customers is paramount to business success, and any sort of breach could be catastrophic.

For the company's security team, monitoring information 24x7x365 and maintaining system updates required administrative work that took up too much time. After implementing a new SIEM device, the company turned to Optiv as its managed security services provider.

What was the best way to approach this challenge?

- Meet strict compliance requirements from sources such as Payment Card Industry Data Security Standards (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA) and the Federal Information Security Management Act (FISMA).
- Ensure solution includes logging security data and validating that customer information is being monitored 24x7x365.
- Allow client to offload monitoring and maintenance with a co-managed, locally hosted solution.
- Onboard client for 24x7x365 co-managed SIEM services, allowing the client to retain physical control and ownership of the SIEM device while reallocating internal resources away from hours of daily security administrative work.

PROJECT OVERVIEW

Organization Size:
2,500 employeess

Organization Industry:
A large IT company focused on healthcare

Challenge:
To remain compliant with strict customer regulatory requirements and to monitor and retain logs on a 24x7x365 basis for possible threats.

IMPACT

- Reallocated security team to other high value tasks
- Centralized security logs, monitored 24x7x365 by Optiv
- Met requirements and continued to maintain compliance for PCI, HIPPA and FISMA standards

CO-MANAGED SIEM SERVICES:
Reviewing Process and Answering Requirements

Planning
Optiv assigned a dedicated service delivery manager to serve as a point of contact throughout the project, as well as creating a process and guiding onboarding.

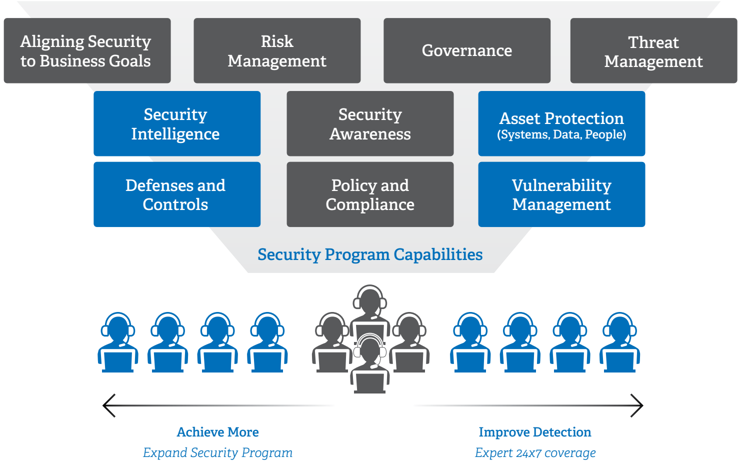
Onboarding
Optiv onboarded the SIEM device, creating alerts and notifications for client-specified events around possible security incidents, ranging from firewall denial and outbreak alerts to virus or spyware detection.

Monitoring
Once the device was onboarded, Optiv began monitoring the environment 24x7x365, alerting the client to critical events and providing remediation steps as needed.

Optimizing
To further support the client, Optiv continually monitors the health of devices, including configuration management, tuning and customization.

Reporting
To meet the client's business needs, Optiv set up on-demand and scheduled reporting of defined security events.

Optiv Managed Security Services



Aligning Security to Business Goals

Risk Management

Governance

Threat Management

Security Intelligence

Security Awareness

Asset Protection (Systems, Data, People)

Defenses and Controls

Policy and Compliance

Vulnerability Management

Security Program Capabilities

Achieve More
Expand Security Program

Improve Detection
Expert 24x7 coverage

Maintaining Credibility and Compliance

The ability to meet and remain compliant with strict requirements represents a huge part of this healthcare IT company's credibility. Without that, the company could not retain customers or remain successful as a business.

Optiv continues to provide this company with peace of mind in knowing that its system is stable, healthy and monitored 24 hours-a-day. As a result:

- The client no longer has to monitor logs in each system during core business hours or perform maintenance.
- Engineers can focus on other high value tasks, rather than time consuming system administration.
- There is much less risk in missing a security threat due to the sheer number of daily logs.
- Maintained compliance for customer requirements.
- Improved efficiency and a decreased risk of data breaches.

Optiv's co-managed SIEM services provides this client with many benefits, including:
System stability:
Optiv implements the daily management of system updates for required devices

View the Client Spotlight Infographic at www.optiv.com/resources/library

OPTIV

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

1125 17th Street, Suite 1700 | Denver, CO 80202 | 800.574.0896 | www.optiv.com

2.16 F1