Fidelis Security

CASE STUDY

A University Children’s Hospital Strengthens Security with Fidelis Security’s Intelligent Deception Platform

The Organization

Part of a leading North American university, the hospital is exclusively dedicated to pediatric and obstetric care, offering multiple specialty locations, pediatric practices, and partner hospital locations across a large metropolitan are. The hospital has nearly 5,000 staff members and volunteers and handles over 500,000 patient visits a year.

The hospital’s sprawling and distributed information systems comprise of approximately 7,000 endpoints and servers used daily by thousands of users. Secure collaboration within the hospital systems — which contain critical organizational, financial, and Protected Health Information (PHI) — is facilitated with a HIPAA-compliant BOX service.

The Threat and the Challenge

Like many large healthcare organizations, the hospital was no stranger to high profile cyber-attacks, breaches, and the rigid network security and data security requirements dictated by HIPAA (the Health Insurance Portability and Accountability Act) and other regulations.

With the understanding that no prevention technology can guarantee complete protection against breaches, especially in the age of sophisticated Advanced Persistent Threats (APTs), the hospital’s IT security staff were looking to add a new and proactive weapon to their network security arsenal — one that would detect suspicious activity from within the network.

The hospital was seeking a solution that could be rapidly deployed and would not impact network performance or burden security staff with masses of false positives or data logs. They needed a solution that would enable them to maximize security resources by focusing solely on actual threats.

Benefits

- Network traffic visibility
- Enhanced threat analytics
- Zero impact on network/endpoint performance
- Leveraging user and web access behavior for business analytics

Benefits

After evaluating a number of tools, including some based on UBA (User Behavioral Analysis), the hospital’s IT security experts selected Fidelis Deception*. Within a few hours, Fidelis Deception was installed and set up, and had already conducted an automatic analysis of the hospital’s network. Out-of-line and agentless, this solution had zero impact on the hospital’s network performance.

After learning the hospitals’ network topography, Fidelis Deception began creating decoys and distributing the breadcrumbs which form the basis of its deception approach. Fidelis Deception’s intelligent decoys publicize themselves throughout the organization, generating traffic that attracts attackers — who believe they are accessing real applications, files, and data assets but are in fact attacking the decoy network.

Fidelis Deception then closely monitored the hospital’s network activity, analyzing communication between assets and remote locations, and watching for communication with command and control (C&C) servers. The system continued to gather intelligence combining analytical activities, informing IT security staff when an attack was in progress, and providing a complete forensic trail of attacker activities.

*formerly Topspin DECOYnet

Successful Implementation

"Within just hours of deployment, Fidelis Deception had already identified and pinpointed suspicious activities that had apparently bypassed our existing security infrastructure," said the hospital's IT Security Architect. "This enabled our IT security teams to promptly address and neutralize the threats."

By way of example, Fidelis Deception found scanners from an associate organization that were going through the file directories. As a result, the staff was able to properly block this activity. Providing unique visibility into network activity, Fidelis Deception also identified the usage of unauthorized tools and uploads that violated security policy.

"Automating the process of network and system analysis helped our security staff reduce noise and highlight actionable incidents, providing a clear story of potential attacks in each of their phases," said the hospital's IT Security Architect. "Moreover, Fidelis Deception provided a uniquely granular view into attacker activities and communication channels, delivering excellent visibility of internal and egress traffic and network usage analysis by decoupling human and machine processes."

> "Fidelis Deception takes our network security to the next level. Its main advantage is that it solves a security problem with a whole new approach and provides visibility with real business analytics. This was a key differentiator for us — and has proven itself by delivering immediate ROI."
>
> *~ The Hospital's, IT Security Architect*

Today, Fidelis Deception continues working round-the-clock at the hospital, maintaining the privacy of PHI and other sensitive data by leveraging advanced offensive deception technology, threat analysis, and visibility.

"Fidelis takes our network security to the next level. Fidelis Deception's main advantage is that it solves a security problem with a whole new approach and provides visibility with real business analytics. This was a key differentiator for us — and has proven itself by delivering immediate ROI.", the hospital's IT Security Architect concluded.

Contact Us Today to Learn More About Fidelis

Fidelis Security | 800.652.4020 | info@fidelissecurity.com

Fidelis Security® is the industry innovator in proactive cyber defense, safeguarding modern IT for global enterprises with proactive XDR and CNAPP platforms. Fidelis Security consolidates IT security operations to shrink attack surfaces, automate threat detection, and accelerate analysis, forensics, and response so that organizations remain resilient through cyber-attacks and emerge stronger and more secure. Fidelis Security is trusted by top commercial, enterprise, and government agencies worldwide.