

## Customer: Large Health Insurance Company

**Target Application:** Perimeter Monitoring / Server Log Collection

**Compliance Applicability:** HIPAA Compliance

### Overview:

Customer is a large health insurance agency with a number of offices, partners, and vendors with external access to their internal network. This Customer expressed concern about the strength of perimeter security configurations in remote branches, and was looking to implement a SIM solution for centralized operational security monitoring. Due to recent successful attacks on similar companies and the emergence of new viruses and worms, the Customer wanted to monitor their perimeter to ensure that only authorized traffic was making it through the firewall. Additionally, they wanted to correlate firewall data with Intrusion Detection System (IDS) logs to identify threats that were breaching their perimeter. Due to the Health Insurance Portability and Accountability Act (HIPAA), the Customer also needed to collect logs from all HIPAA regulated servers. The Customer had implemented several application silos for security and compliance monitoring, but was looking to build a central monitoring solution for all events with one, integrated real-time dashboard. Goals of this project included:

- Monitoring of Internet-facing firewalls and Virtual Private Network (VPN) devices
- Monitoring of internal IDS logs
- Detection of Worm and Virus breakouts within the internal customer networks
- Notification and incident tracking for all access to HIPAA servers housing client-specific information.

### Environment:

The Customer uses Cisco PIX and Checkpoint Firewalls in addition to Cisco VPN devices on the perimeter. For Intrusion Detection, they have deployed ISS Real Secure sensors throughout the global network, while the server environment is a heterogeneous mix of Windows, Linux, AIX, and Solaris. The Customer has zoned their network according to the list below.

#### Zones:

Internet – Any IP address or range not identified as being internal

Extranet – Remote Customer offices, partners and vendors with direct connections

External – Remote Customer offices, partners and vendors connected by VPN

Bastion – Area between DMZ and Internal networks

DMZ – Area between Firewalls and Bastion

### Solution:

Vigilant worked with the Customer to create a list of use-cases derived from examination of network traffic across each zone. By mapping appropriate and suspicious traffic patterns across the network zones, Vigilant created a series of custom correlation rules to meet the Customer's requirements.

#### Custom Rules:

- **Internet Zone to Internal Network** – Any event where the Source IP has been determined to be a non-Customer IP and the Target IP is internal.
- **Internal Zone Monitoring** – Monitoring events in the various zones for suspicious activity.

- **SQL Slammer Monitoring** – Monitor IDS logs and notify appropriate personnel when the Slammer Worm variants are detected.
- **Excessive Windows Access Error Monitoring** – Monitor IDS logs and look for a high rate of Windows Access Error events coming from a single host. This activity is indicative of an internal worm or virus.
- **Privileged Login Failure** - An authentication event to an IDS sensor where a privileged account unsuccessfully performs a login attempt.
- **High Rate of SMB Service Sweep Monitoring** – Monitor IDS logs looking for a high rate of SMB Service Sweep events coming from a single host. This activity is indicative of an internal worm or virus.
- **High Rate of Email Signature Monitoring** – Monitor IDS logs looking for high rates of Suspicious Zip Files and Executable Email Extension events coming from a single host.
- **High Rate of TCP Probe Signature Monitoring** – Monitor IDS logs looking for a high rate of TCP Probe MSRPC events coming from a single host.

#### Custom Reports:

- Executive Summary Report – (High level bar/pie chart)
- HIPAA Server User Activity Violations
- All Violations by User ID
- All Violations by Source IP / Source Hostname

#### **Summary:**

The customer's specific requirements for centralized security and IT control monitoring were met by instituting a single SIM solution for perimeter and internal surveillance, and by leveraging Vigilant's consulting team to design and build tailored rules. The customer now monitors their network infrastructure with one, integrated dashboard, and reacts to security or policy violations in real time. In addition, the customer is able to easily demonstrate that they are compliant with HIPAA regulations.