SOLUTION BRIEF

Alert Logic for HIPAA Compliance

AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE

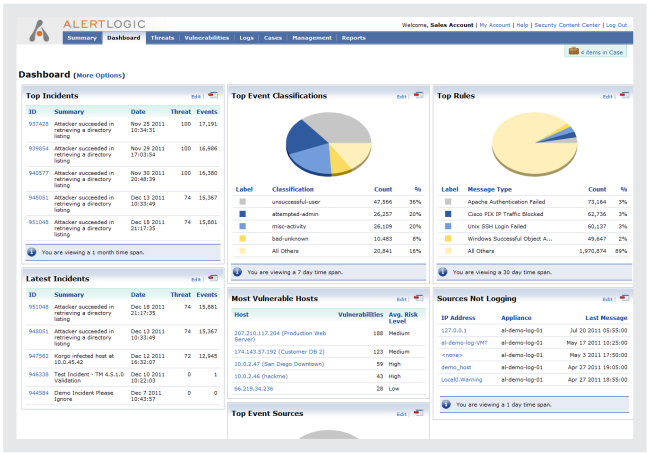
Making personal health information (PHI) more easily accessible to medical professionals is also creating opportunities for identity theft and medical claim fraud. According to Experian, 1.4 million Americans were victims of medical identity theft in 2009. The Health Insurance Portability and Accountability Act (HIPAA) outlines a number of preventive measures that create a proactive approach to discovering and addressing suspicious network activity and vulnerabilities. In order to comply with HIPAA, healthcare organizations and their business partners need to review log data, implement intrusion detection solutions and conduct regular vulnerability scans to help strengthen their security programs and protect PHI. And with the passage of the HITECH Act in 2009, cleaning up after a breach will often be more expensive and damaging than preventing one, making compliance with HIPAA all that much more important.

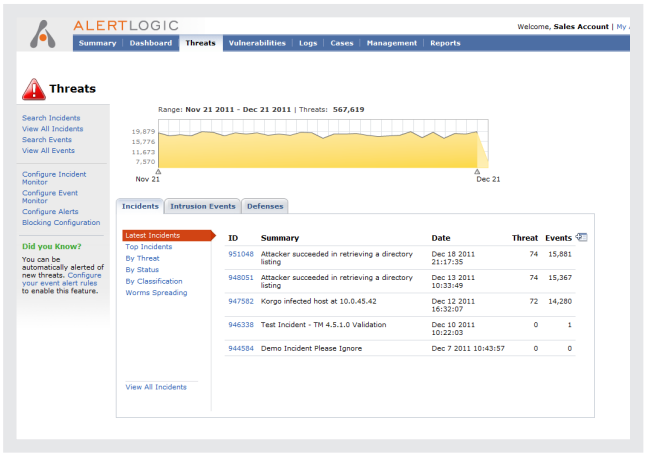
- Alert Logic Log Manager provides the means for the effective log review and forensic analysis needed to comply with HIPAA.
- Alert Logic Threat Manager uses patented technology to remove noisy network traffic and zero in on the activity that is most threatening to your environment, as well as provide unlimited vulnerability scanning.
- Alert Logic Web Security Manager provides proactive defense against Web application attacks.

Delivered as Software-as-a-Service (SaaS), Alert Logic's services provide a comprehensive security and compliance solution so you can be more proactive in the defense against cyber crime.

DETAILED VULNERABILITY ASSESSMENT & REMEDIATION GUIDANCE

To achieve HIPAA compliance, you must identify and remediate all critical vulnerabilities. Threat Manager streamlines this process by providing simple, actionable reports that detail vulnerabilities and recommendations. The Web interface provides easy-to-use dashboards and drill-down capabilities to quickly investigate any discrepancies. There is also a Dispute Wizard that helps document compensating controls that are in place to remediate specific vulnerabilities.





Threat Manager contains over 45 dashboards and 100 reports to help you manage compliance

HIPAA/HITECH SOLUTIONS MAPPING

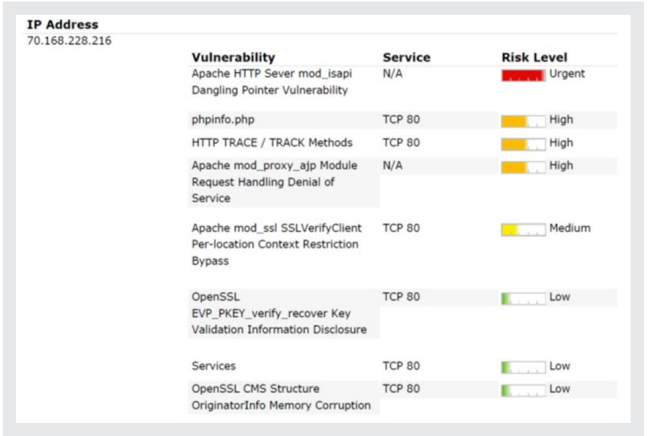
THREAT MANAGER & ACTIVEWATCH	> **164.308 (a)(1)(ii)(A):** Risk Analysis—Conducts vulnerability assessment > **164.308 (a))1)(ii)(B):** Risk Management—Implements security measures to reduce risk of security breaches > **164.308 (a)(5)(ii)(B):** Protection from Malicious Software—Procedures to guard against malicious software host/network IPS > **164.308(a)(6)(iii):** Response & Reporting—Mitigates and documents security incidents
LOG MANAGER & LOGREVIEW	> **164.308 (a)(1)(ii)(D):** Information System Activity Review—Procedures to review system activity > **164.308 (a)(6)(i):** Log-in Monitoring—Procedures and monitoring log for log-in attempts on host IDS > **164.312 (b):** Audit Controls—Procedures and mechanisms for monitoring system activity
WEB SECURITY MANAGER & ACTIVEWATCH	> **164.308 (a)(1):** Security management process—Implement policies and procedures to prevent, detect, contain and correct security violations > **164.308 (a)(6):** Incident Procedures (R)—Implement policies and procedures to address security incidents

PRODUCTS & SERVICES

Alert Logic Threat Manager	– Threat Manager is a vulnerability assessment and intrusion detection solution that is delivered using a Software-as-a-Service (SaaS) model. With Alert Logic's Threat Manager and ActiveWatch solutions, you can now cost-effectively defend and protect your network against internal and external threats across centralized and distributed environments. – Threat Manager leverages Alert Logic's patented expert system, which includes Threat Scenario Modeling, purpose-built grid computing infrastructure, and the ability to automatically aggregate and correlate anomalous behavior patterns to quickly identify threats and attacks to your network
Alert Logic Log Manager	– Effective log management is imperative in maintaining compliance, but is also a powerful security tool that can prevent intrusion and security breaches. Log Manager automates log collection, aggregation and normalization, simplifying log searches, forensic analysis and report creation through real-time or scheduled analysis. Once logs are transferred to Alert Logic's secure cloud, Log Manager protects and stores the data to preserve against unauthorized loss, access or modification.
Alert Logic Web Security Manager	– Web Security Manager provides active protection against Web application attacks, one of the more prevalent threats to business-critical applications. Proactively blocking unauthorized activity, Web Security Manager effectively protects against the most dangerous attacks, such as SQL Injection and Cross-Site Scripting.
ActiveWatch and LogReview Services	– ActiveWatch is integrated with Threat Manager to provide 24x7 network monitoring, expert analysis and guidance on security events and incidents. This service increases the accuracy of threat detection, reduces false positives and allows you to stay focused on your business. – ActiveWatch for Web Security Manager provides 24x7 monitoring and ongoing tuning of your web application firewall, along with escalation for inappropriately blocked requests. – LogReview provides daily event log monitoring and review, and is designed to help you meet PCI DSS requirement 10.6. A team of certified security analysts acts as an extension of your team to expertly review your log data daily and alert you whenever suspicious activity or possible security breaches are detected. – These services are managed from Alert Logic's state-of-the-art, 24x7 Security Operations Center (SOC), which is staffed by security professionals with Global Information Assurance Certification (GIAC) from the SANS Institute.

HOST VULNERABILITY REPORT

For each host, Threat Manager will produce a report that details the vulnerabilities and associated risk levels that are exposed. In this example report, you can see that there is a range of urgent to low-level vulnerabilities on the host.

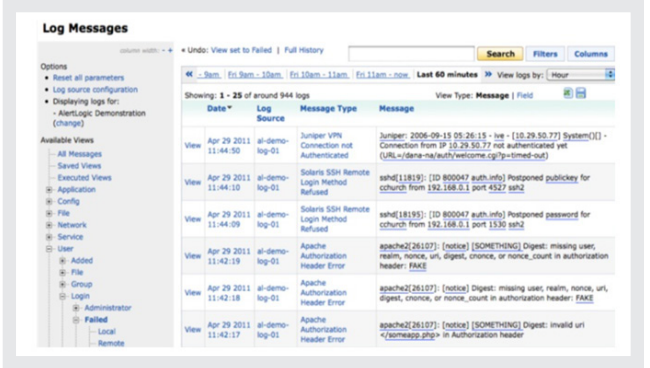


IP Address
70.168.228.216

Vulnerability	Service	Risk Level
Apache HTTP Sever mod_isapi Dangling Pointer Vulnerability	N/A	Urgent
phpinfo.php	TCP 80	High
HTTP TRACE / TRACK Methods	TCP 80	High
Apache mod_proxy_ajp Module Request Handling Denial of Service	N/A	High
Apache mod_ssl SSLVerifyClient Per-location Context Restriction Bypass	TCP 80	Medium
OpenSSL EVP_PKEY_verify_recover Key Validation Information Disclosure	TCP 80	Low
Services	TCP 80	Low
OpenSSL CMS Structure OriginatorInfo Memory Corruption	TCP 80	Low

FAILED LOGIN ATTEMPTS REPORT

This report can be scheduled to run on a daily basis to ensure that attacks such as brute force attacks are not occurring. Many companies use this report to determine if contractors or onsite vendors are trying to gain access to sensitive information.



Log Messages

ABOUT ALERT LOGIC

Alert Logic, the leading provider of Security-as-a-Service solutions for the cloud, provides advanced security tools coupled with 24×7 Security Operations Center expertise, allowing customers to defend against security threats and address compliance mandates. By leveraging an "as-a-Service" delivery model, Alert Logic solutions include day-to-day management of security infrastructure, security experts translating complex data into actionable insight, and flexible deployment options to address customer security needs in any computing environment. Built from the ground up to address the unique challenges of public and private cloud environments, Alert Logic partners with over half of the largest cloud and hosting service providers to provide Security-as-a-Service solutions, such as intrusion protection, vulnerability assessment and log management for over 1,800 enterprise customers. Alert Logic is based in Houston, Texas, and was founded in 2002. For more information, please visit www.alertlogic.com.