

Alert Logic Threat Manager™ and ActiveWatch

Advanced Advanced Network Protection, Delivered as a Service

With Alert Logic's Threat Manager and ActiveWatch solutions, you can now cost-effectively defend and protect your network against internal and external threats, no matter how fragmented your IT world has become.

Threat Manager is a cloud-powered vulnerability assessment and intrusion detection solution that is delivered using a Software-as-a-Service (SaaS) model. Threat Manager leverages Alert Logic's patented expert system, which includes 7-Factor 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. Integrated with Threat Manager, ActiveWatch provides 24x7 monitoring and expert guidance services from Alert Logic's state-of-the-art Security Operations Center (SOC).

Staffed by GIAC-certified analysts and security experts, ActiveWatch allows you to meet PCI compliance requirements at a fraction of the cost of staffing your own team of analysts.



Advanced Features for an Evolving Threat Landscape

With the rapid growth of online commerce, Web applications have become the primary target for cyber-criminals. Malicious hackers now leverage protocol or application vulnerabilities to commit data theft, cause denial of service or deface websites. As a result, the challenge to secure and monitor internal and customer-facing websites, card processing systems and other critical infrastructure continues to grow every day.

The latest release of Alert Logic Threat Manager helps customers solve these challenges by delivering unparalleled intrusion detection and visibility into critical Web-based infrastructure vulnerabilities, including the handling of Ajax and SQL injection technologies. Threat Manager also includes an optional SSL decryptor module that actively decrypts SSL traffic and enables customers to detect attacks that may be injected over encrypted SSL channels.

PCI Compliance

Alert Logic continues to maintain their PCI Security Standards Council Approved Scanning Vendor (ASV) and Level 2 Audited Vendor status. Threat Manager now supports the latest PCI DSS 2.0 requirements and has been enhanced to include advanced risk reporting capabilities, including CVSS risk scoring and "audit-ready" reports for PCI-QSAs.



Key Benefits

Detect & Defend

- Patented 7-Factor Threat Scenario Modeling reduces false positives and improves threat detection
- Optional SSL Decryption Module provides visibility into encrypted SSL-based intrusion traffic

Assess Vulnerabilities

- Regularly scan internal and external networks — whenever and as often as you choose
- Global threat visibility incorporates thousands of sensors into the expert system's decision process

Maintain Compliance

- Comply with a wide range of regulatory mandates (PCI DSS, SOX, HIPAA, GLBA, etc.) with audit-ready reports
- 24x7 Security Operations Center (SOC) staffed with GIAC analysts provide around-the-clock monitoring services

Trend & Report

- Use custom reports or leverage the dozens of out-of-the box dashboards and reports to effectively track and manage security incident activity
- Easy-to-use Web console to view reports, run queries and perform drilldown analysis from any browser

Lower Costs

- SaaS delivery model means quick deployment with minimal capital investment
- All software and appliance maintenance, upgrades and patches are included with your subscription — no hidden costs
- Integrated ActiveWatch services provides shared SOC monitoring services at a fraction of the cost



Threat Manager & ActiveWatch Features

Threat Signatures and Rules

- 45,000+ IDS Signature Database; New Signatures Updated Weekly
- Rule Set Consolidated from Multiple Sources
 - Alert Logic Security Research Team
 - Emerging Threats
 - Open Source, Third-Party Collaboration
- Real-time Signature Updates to Alert Logic Expert System
- Custom Rule Creation and Editing

Vulnerability Assessment and Intrusion Detection

- Unlimited Internal and External Scans
- Broad Scanning and Detection Visibility
 - Network Infrastructure
 - Server Infrastructure
 - Business-Critical Applications
 - Web Technologies (IPv6, Ajax, SQL Injection, etc.)
 - SSL-Based Intrusion Traffic
- Signature and Activity-Based Correlation
- Patented 7-Factor Threat Scenario Modeling

Integrated Managed Security Services

- GIAC-Certified Security Analysts and Researchers
- 24x7 State-of-the-Art Security Operations Center
- Trained Experts in Alert Logic Solutions
- Monitoring, Analysis and Expert Guidance Capabilities
- Customized Alerting and Escalation Procedures

Analysis and Reporting

- Dozens of Dashboards and Reports Available Out-of-the-Box
- Custom Reporting Capabilities
- Common Vulnerability Scoring System (CVSS) to Assess Risks
- Audit-Ready Reports
- Single Web-Based Console for Entire Environment
 - User Management and Administration
 - Dashboards and Drilldown Analysis
 - Report Scheduling, Creation and Review
 - Scan Scheduling and Results Review

Compliance Support

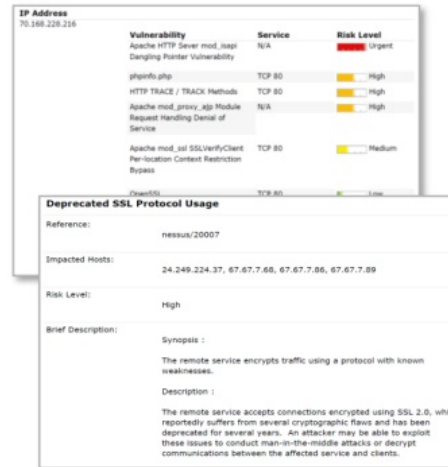
- PCI Approved Scanning Vendor (ASV)
- PCI Level 2 Audited Vendor
- Support for Multiple Compliance Mandates
 - PCI DSS 2.0, HIPAA, SOX, GLBA, CoBIT, etc.
- 6-Month Storage of All Raw IDS Event Data
- SAS 70 Type II Audited Data Centers
- Indefinite Storage and Archival of Incident Analysis and Cases

Security-as-a-Service Delivery

- Rapidly Deploy and Scale as Needed
- Pay-as-You-Go; Minimal Capital Expenditure
- Always Utilize Latest Software and Signature Database
- No Hidden Costs – Subscription Includes:
 - Software and Hardware Upgrades, Maintenance and Patches
- Architected for Multi-Tenant Support
- Easily Deploy in On-Premise, Off-Premise or Hybrid Environments

Detailed Vulnerability Reports

Detailed vulnerability and host reports are produced to provide detailed descriptions and lists of impacted hosts, risk levels and remediation tips.



IP Address	Vulnerability	Service	Risk Level
76.546.228.216	Apache HTTP Server mod_ssl: Missing Header Vulnerability	N/A	Urgent
	phpinfo.php	TCP 80	High
	HTTP TRACE / TRACE Methods	TCP 80	High
	Apache mod_proxy: Xp Module Request Handling Denial of Service	N/A	High
	Apache mod_ssl SSLVerifyClient: Per-location Context Restriction Bypass	TCP 80	Medium
	OpenSSL: CVE-2015-3566	TCP 80	Low

Deprecated SSL Protocol Usage	
Reference:	nessus/20007
Impacted Hosts:	24.249.224.37, 67.67.7.66, 67.67.7.86, 67.67.7.89
Risk Level:	High
Brief Description:	<p>Synopsis : The remote service encrypts traffic using a protocol with known weaknesses.</p> <p>Description : The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.</p>

Expert Security Services with ActiveWatch

The ActiveWatch team augments your existing IT team to ensure rapid detection and response to network incidents. In addition to monitoring the network traffic flows for incidents, the SOC team reviews suspicious network traffic to identify zero-day attacks that might not otherwise trigger an alert. This intelligent review and response by industry professionals not only increases the overall visibility into your network, it reduces the potential for false positive alarms and helps identify zero-day attacks that may have slipped by or gone unnoticed.

When an incident or suspicious network activity is detected, the ActiveWatch team will conduct an analysis of the situation and notify your staff based on predetermined escalation procedures. They will work with your team to perform in-depth analysis and assessment of the incident and recommend containment and mitigation actions.

ActiveWatch also includes integrated incident and case management capabilities that allow customers to track and report on incident trends across their entire enterprise, including the services hosted outside of the internal perimeter. This capability provides an audit trail of suspicious findings and gives a historical record of the response and actions from start to finish.

