

How Secure is Your Network?

Find and Remediate Exposures with Vulnerability Scanning

Vulnerability Scanning with Threat Manager™

Alert Logic Threat Manager delivers actionable intelligence to protect and secure networks. First, the Threat Manager intrusion detection engine is used to detect the attempts by hackers, viruses and other malicious agents' behavior to compromise critical systems. In addition, Threat Manager includes a fully integrated vulnerability scan engine. This engine performs in-depth inspections of systems to identify security weaknesses and vulnerabilities that a hacker may use to steal data, install backdoors, corrupt systems or commit other malicious activities. With each scan, Threat Manager will automatically test every system and report its findings to reveal security issues in equipment, operating systems and applications.

Threat Manager is designed to scan customer networks seamlessly and generate detailed reports specifying network security weaknesses. The Threat Manager database, which includes thousands of known vulnerabilities, is updated continuously with the most recently discovered security vulnerabilities, including discoveries by our own team of security experts and those discovered by corporate and private security teams around the world.

Why Alert Logic?

Security and Compliance Automation

Alert Logic Threat Manager utilizes a combination of patented grid-based technology and cutting-edge 7-Factor Threat Scenario Modeling expert system to accurately identify and prioritize threats in your environment. All this is delivered through a seamless "as-a-Service" delivery model with flexible deployment options to address customer security needs anywhere they have IT infrastructure. To complement this, Alert Logic offers hands-on active management of your security infrastructure with its ActiveWatch service. ActiveWatch security experts translate complex attack data into actionable insight.

Complete Threat Visibility

Alert Logic serves as the nexus of threat, vulnerability and log data within your network. Our global sensor network spans more than 1,500 customers and partners across four continents. This gives Alert Logic unparalleled visibility to accurately identify and prioritize security incidents, delivering a broad threat picture that is unmatched by traditional, self-managed on-premise solutions. Alert Logic's in-house security research team investigates the newest vulnerabilities and exploits, develops the threat correlation rules and vulnerability checks, and tunes the expert system to ensure accurate, automated security analysis.

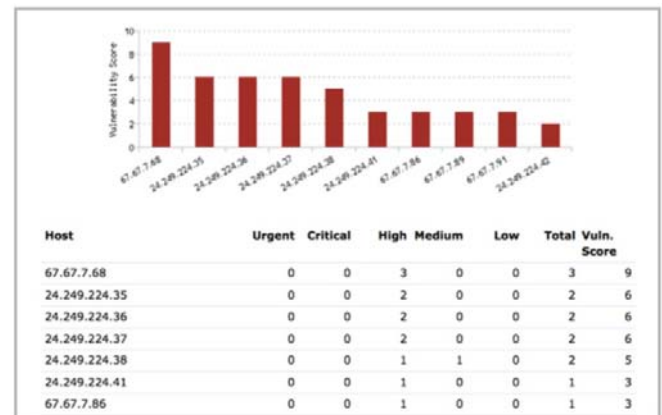
PCI Compliance

Alert Logic continues to maintain their PCI Security Standards Council Approved Scanning Vendor (ASV) and Level 2 Audited Vendor status. Threat Manager 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.



Real Examples, Real Vulnerabilities

In the example below, Threat Manger scanned part of a customer's environment. These scans were executed from Alert Logic's secure cloud. The scans can be executed from the internal network or from the Alert Logic cloud to assess Internet-facing servers and devices. This allows customers to get the perspective on their system's security that a hacker would gain while looking for opportunities to exploit or penetrate their environment.



Summary Report

This summary report provides a snapshot of the number and criticality of vulnerabilities found at each host. Of these hosts with vulnerabilities, those with urgent or critical vulnerabilities may have already been exploited, as these vulnerabilities only require basic expertise or skill to gain access to a system. High- and medium-level vulnerabilities are issues where there may be an exploit proof of concept in existence, or where the vulnerability combined with another low or medium vulnerability may create a compromise. Low vulnerabilities, which have been excluded from this report, are mostly informational and are typically used to learn more about the systems and services that are running.

Vulnerability Assessment

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.

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

Detailed Vulnerability Report

Threat Manager also provides a detailed report that shows specific information about the nature of each detected vulnerability. This report includes an explanation of the vulnerability, the impacted hosts, risk level, external research sources and remediation steps. Below is an example for the Deprecated SSL Protocol Usage vulnerability.

Deprecated SSL Protocol Usage	
Reference:	nessus/20007
Impacted Hosts:	24.249.224.37, 67.67.7.68, 67.67.7.86, 67.67.7.89
Risk Level:	High
Brief Description:	<p>Synopsis :</p> <p>The remote service encrypts traffic using a protocol with known weaknesses.</p> <p>Description :</p> <p>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> <p>See also :</p> <p>http://www.schneier.com/paper-ssl.pdf</p> <p>Solution :</p> <p>Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead.</p>

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 dashboard KPIs 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 round-the-clock SOC monitoring services at a fraction of the cost

