

eSec Threat Manager powered by Alert Logic

Cloud-Powered Threat & Vulnerability Management

With Alert Logic's cloud-powered Threat Manager™, you can now cost-effectively defend and protect your enterprise against internal and external threats, no matter how fragmented your IT world has become. Using Alert Logic's patented 7-Factor Threat Scenario Modeling and our purpose-built grid computing infrastructure, you can now automatically identify anomalous behavior patterns, track threats on a global scale, and drive remediation and mitigation of risk factors, all from a simple browser window.

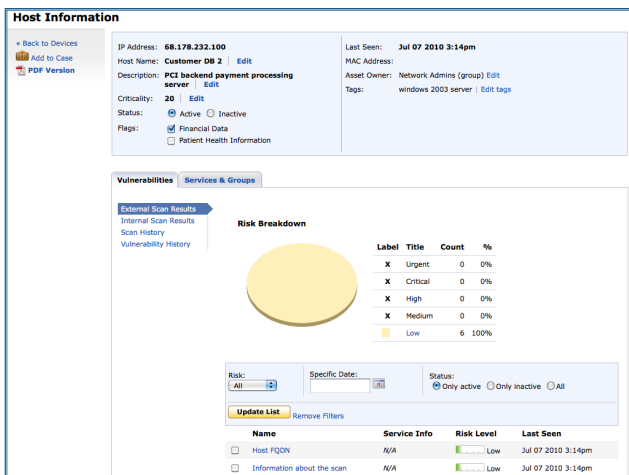
Threat Manager brings clarity across both the enterprise and the fractured data center by extending its reach into your hosting provider environments giving you complete threat visibility through a single interface. Now you can audit, remediate and document security across multiple sets of requirements; internal policies and external industry legislative mandates. This includes asset discovery, asset grouping and risk weighing, remediation prioritization, vulnerability assessment reporting and remediation tracking allowing you to proactively manage business risk. As a Software-as-a-Service (SaaS) solution, there is no infrastructure to deploy or manage, saving valuable time in deployment, management and on-going maintenance.

Benefits

- **Detect & Defend** - Identify and stop attacks that put your organization at risk.
- **Assess Vulnerabilities** - Unlimited scanning and correlation of vulnerability and threat information.
- **Maintain Compliance** - Regularly test systems and processes and generate audit-ready reports.
- **Trend & Report** - Out-of-box and customizable reports that can be scheduled to arrive via email
- **24x7 Monitoring** - ActiveWatch service provides 24x7 monitoring to increase accuracy of threat detection.

Features

- Alert Logic is a PCI Security Standards Council Approved Scanning Vendor (ASV)
- Patented 7-Factor Threat Scenario Modeling reduces false positives and improves threat detection
- Global threat visibility incorporates thousands of sensors into the patented intrusion detection decision process.
- 45 dashboards and hundreds of reports to manage effectiveness of security and compliance programs.
- 24x7 Security Operations Center (SOC) staffed with GIAC analysts who handle all security incidents and provide expert guidance for remediation.



Host Information

IP Address: 66.178.232.100
 Host Name: Customer DB 2
 Description: PCI backend payment processing server
 Criticality: 20
 Status: Active
 Last Seen: Jul 07 2010 3:14pm
 MAC Address: [redacted]
 Asset Owner: Network Admins (group)
 Tags: windows 2003 server

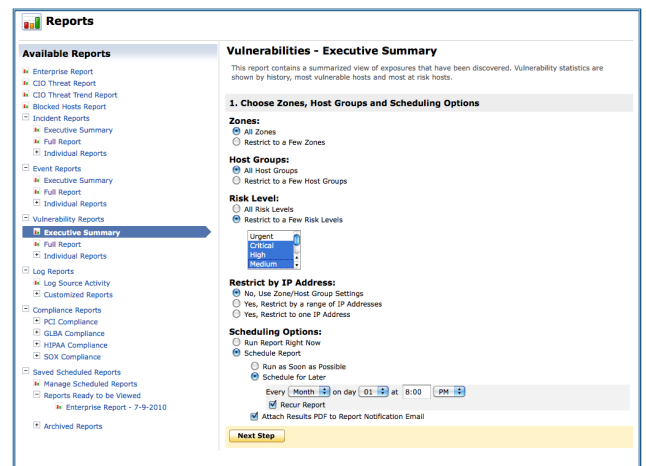
Vulnerabilities

Risk Breakdown

| Label | Title | Count | % |
|-------|----------|-------|------|
| X | Urgent | 0 | 0% |
| X | Critical | 0 | 0% |
| X | High | 0 | 0% |
| X | Medium | 0 | 0% |
| ■ | Low | 6 | 100% |

| Name | Service Info | Risk Level | Last Seen |
|----------------------------|--------------|------------|--------------------|
| Host FQDN | N/A | Low | Jul 07 2010 3:14pm |
| Information about the scan | N/A | Low | Jul 07 2010 3:14pm |

Easily prioritize hosts for remediation



Reports

Available Reports

- Enterprise Report
- CID Threat Report
- CID Threat Trend Report
- Blocked Hosts Report
- Incident Reports
- Executive Summary
- Full Report
- Individual Reports
- Event Reports
- Compliance Reports
- Log Reports
- Log Source Activity
- Customized Reports
- Compliance Reports
 - PCI Compliance
 - GLBA Compliance
 - HIPAA Compliance
 - SOX Compliance
- Saved Scheduled Reports
 - Manage Scheduled Reports
 - Reports Ready to be Viewed
 - Enterprise Report - 7-9-2010
- Archived Reports

Vulnerabilities - Executive Summary

This report contains a summarized view of exposures that have been discovered. Vulnerability statistics are shown by history, most vulnerable hosts and most at risk hosts.

1. Choose Zones, Host Groups and Scheduling Options

Zones:
 All Zones
 Restrict to a Few Zones

Host Groups:
 All Host Groups
 Restrict to a Few Host Groups

Risk Level:
 All Risk Levels
 Restrict to a Few Risk Levels

Restrict by IP Address:
 Yes, Restrict by a range of IP Addresses
 Yes, Restrict to one IP Address

Scheduling Options:
 Run Report Right Now
 Schedule Report
 Run as Soon as Possible
 Schedule for Later
 Every [Month] on day [01] at [0:00] PM
 Attach Results PDF to Report Notification Email

Next Step

Quickly view highlights from compliance dashboards

IT Security & Compliance

Patented Software

Alert Logic Threat Manager and Log Manager utilize a combination of a patented grid-based technology and cutting edge 7-factor threat scenario modeling to accurately identify and prioritize threats in your environment.

Security Operations Center

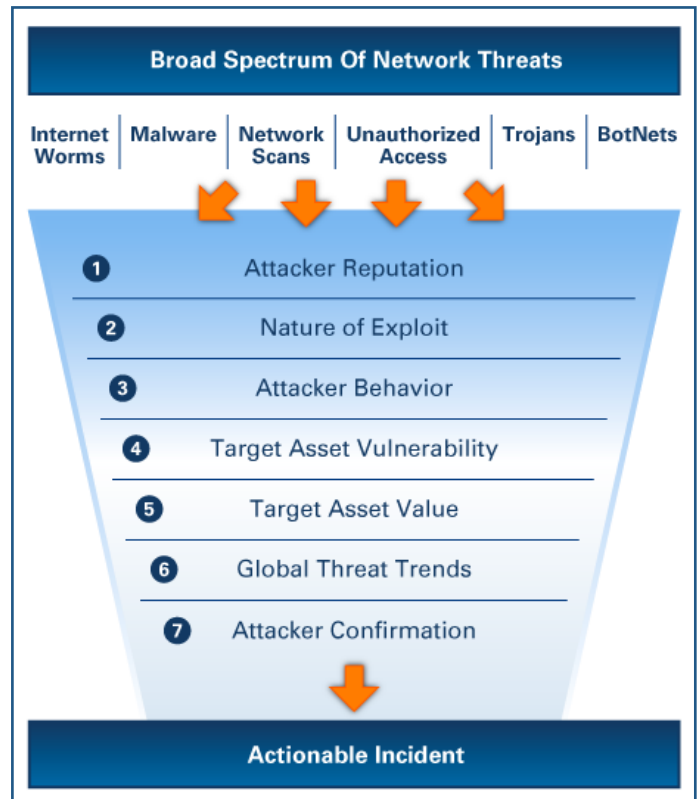
Alert Logic's Security Operations Center is staffed by highly skilled security professionals with Global Information Assurance Certification (GIAC) by the SANS Institute, who, through the ActiveWatch and LogReview services, provide 24x7 monitoring and incident response at a fraction of the cost of employing these skills in-house.

Complete Threat Visibility

Alert Logic uniquely sits at the nexus of threat, vulnerability and log data within your network and across our global sensor footprint of over 1,000 customers and hosting service providers. This gives us unparalleled visibility to identify and prioritize security incidents based on a complete picture and is not matched by off-the-shelf software.

Powered by the Cloud

Alert Logic takes the difficulty out of obtaining, achieving and affording security and compliance solutions by offering Threat Manager and Log Manager in a service-based delivery model. This cloud-based model means you don't have to buy, implement or maintain the expensive and complicated hardware and software usually associated with intrusion detection, vulnerability assessment, and log management.



7-Factor Threat Scenario Modeling



eSec Managed Security

Bagsværdvej 70B
DK-2800 Lyngby
tlf. +45 7020 5585

www.esec.dk

For more information

Tlf. +45 7020 5585

Email: os@esec.dk

Web: www.alertlogic.com