ALERT LOGIC®

SOLUTION OVERVIEW:

ALERT LOGIC® THREAT MANAGER™ WITH ACTIVEWATCH

DETECT AND RESPOND TO THREATS – FROM THE DATA CENTER TO THE CLOUD

Protecting your infrastructure requires you to detect threats, identify suspicious network traffic, and respond quickly – whether the problem is in your own data center, a hosted environment or the cloud. How do you get a global view of the threats impacting all of your infrastructure, day or night, without massive investments in multiple solutions and additional staff?

Alert Logic Threat Manager with ActiveWatch Services gives you 24x7 network threat detection, monitored by Alert Logic's Security Operations Center (SOC), for the entire IT environment. Our patented expert system, driven by global threat data, identifies potential problems for our analysts to investigate – acting as an extension of your team, day and night, keeping an eye on suspicious activity.

HOW THREAT MANAGER WORKS

Threat Manager identifies suspicious activity in network traffic, quickly identifying threats to your IT assets so that you can respond. We monitor network traffic and analyze billions of events with a patented expert system. Using intelligent multifactor correlation, we identify security events requiring attention. After validation by a Level 1 SOC analyst, we notify you with recommended actions/responses. When needed, senior specialist teams are engaged to assist you. You can also implement automated blocking through integration with your network firewalls.

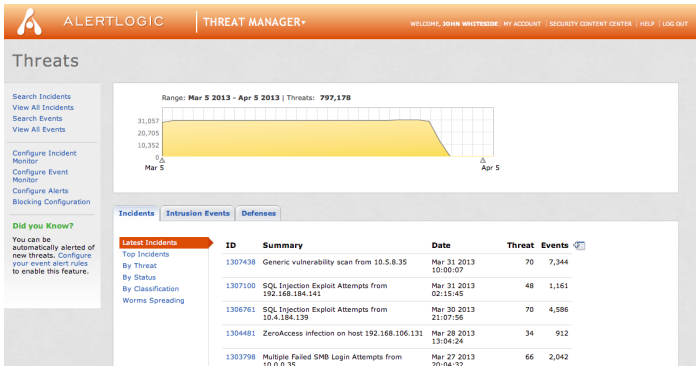
We give you insight into the real threats in your environments, helping you make more informed security investment and resource decisions. When the security program is driven by a clear understanding of the real threats affecting your network, your efforts and investments will provide more benefit and significantly enhance your security posture.

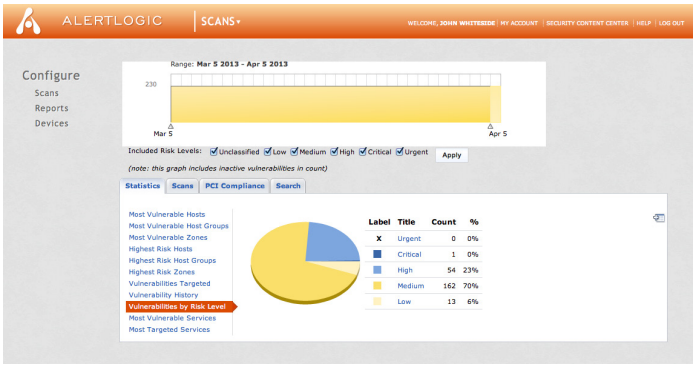
We help you meet compliance challenges. Threat Manager's intrusion detection and vulnerability scanning capabilities provide key elements to address the requirements of PCI DSS, HIPAA/HITECH, GLBA, Sarbanes-Oxley, and other mandates. Compliance-specific reporting makes it easy to evaluate and document your compliance stance. Alert Logic is a PCI-Approved Scanning Vendor (ASV).

You get these benefits without a large investment, staff burden or distractions from your strategic IT initiatives. Security-as-a-Service delivery gives you Threat Manager with ActiveWatch for a fixed monthly fee, including all monitoring, software and our 24x7 Security Operations Center (SOC) to validate incidents and provide support. You access your Threat Manager data through a web interface – the very same one used by our analysts. There's no complex integration or implementation, no upgrades – just the latest security technology and the sharpest analysts, working for you 24 hours a day, 7 days a week.

THE RIGHT SECURITY APPROACH MEANS BETTER SECURITY OUTCOMES

Alert Logic's approach is fundamentally different from traditional security vendors, who sell powerful technology that you need to implement and support – until it's time to replace it. If you've ever seen complex implementation and large investment produce disappointing results, you know the challenges. With Alert Logic, you pay for specific security capabilities and our expertise in delivering them, and you don't make a capital investment to get it. In the age of fast-changing threats and distributed infrastructure, Security-as-a-Service gives you the outcomes you need





THREAT MANAGER DEPLOYMENT

1

In the protected environment, Threat Manager passively collects network traffic data and transports it to Alert Logic through SSL channels

- Physical appliance
- Virtual Appliance
- Agents with virtual tap

2

Events are analyzed by Alert Logic's expert system. Intelligent multifactor correlation identifies suspicious patterns of events, and creates actionable incidents.

3

Alert Logic security analysts investigate incidents and check for false positives.

- Valid incidents are escalated according to the customer's requirements, and analysts work with customers to help remediate threats and attacks.

ALERT LOGIC SECURITY RESEARCH TEAM

Alert Logic's security researchers provide the expertise and leading-edge threat intelligence that makes Threat Manager so effective. Studying emerging threats, data from our global customer base, and third-party sources, the research team drives development of security content for Threat Manager's expert system, correlation rules, and best practices for resolving incidents.

RESEARCH	CONTENT DEVELOPMENT	EXPERT SYSTEM
• Real-time customer data from more than 2,500 customers • Alert Logic security and emerging threat research • Third-party security information sources and feeds	• IDS and vulnerability signatures • Correlation rules • Remediation and resolution documentation • Performance and accuracy tools	• Patented correlation engine based on global view of threat data • Continuously analyzes millions of data points into meaningful intelligence

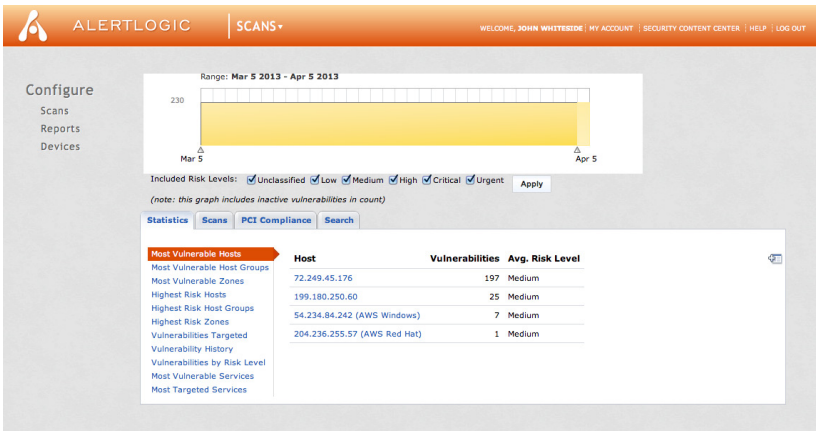
ACTIVEWATCH: EXPERT SECURITY SERVICES FOR THREAT MANAGER

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.

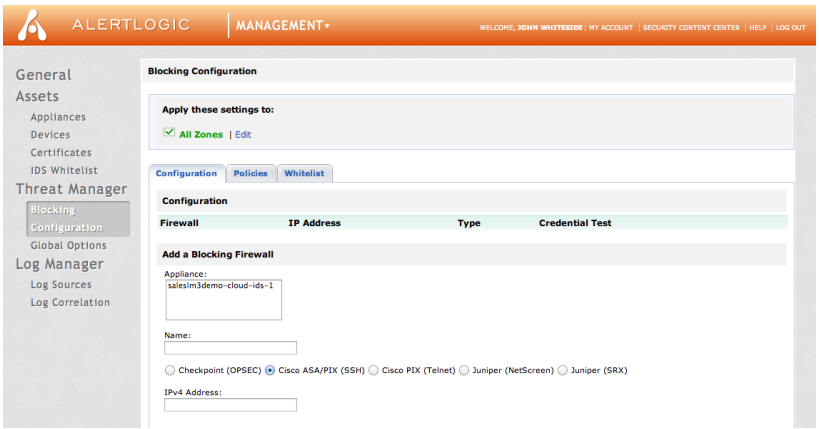
When an incident or suspicious network activity is detected, the ActiveWatch team will conduct an analysis of the situation and notify your staff based on predetermined escalation procedures. They will work with your team to perform in-depth analysis and assessment of the incident and recommend containment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

Additional services, including daily review by a senior security analyst, weekly reporting on security posture based on business goals, and review of NetFlow for enhanced detection of malware and advanced persistent threats are also available.



SUMMARY OF VULNERABLE HOSTS



CONFIGURE BLOCKING THROUGH AUTOMATIC FIREWALL UPDATES

THREAT MANAGER & ACTIVEWATCH FEATURES

DESIGNED FOR DEPLOYMENT IN ANY ENVIRONMENT	• Deploys in public and private clouds and supports elastic scaling • Provides a single view into cloud, hosted and on-premises infrastructure • Usage-based pricing to match your cloud consumption model

THREAT SIGNATURES AND RULES	• 52,000+ IDS signature database; new signatures updated weekly
	• Rule set consolidated from multiple sources
	  o Alert Logic security research team
	  o Emerging threats
	  o 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

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
	• Detailed vulnerability and host reports provide detailed descriptions and lists of impacted hosts, risk levels and remediation tips
	• Single web-based console for entire environment
	  o User management and administration
	  o Dashboards and drill-down analysis
	  o Report scheduling, creation and review
	  o Scan scheduling and results review

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 • Daily review by senior analyst and weekly reporting available • Review of NetFlow data for enhanced malware and APT detection available
COMPLIANCE SUPPORT	• PCI Approved Scanning Vendor (ASV) • PCI Level 2 Audited Vendor • Support for multiple compliance mandates o PCI DSS, HIPAA, SOX, GLBA, CoBIT, etc. • 6-month storage of all raw IDS event data • SSAE 16 Type II Verified 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 public cloud, private cloud, managed hosting, enterprise data center or hybrid environments

ABOUT ALERT LOGIC

Alert Logic, the leader in security and compliance solutions for the cloud, provides Security-as-a-Service for on-premises, cloud, and hybrid infrastructures, delivering deep security insight and continuous protection for customers at a lower cost than traditional security solutions. Fully managed by a team of experts, the Alert Logic Security-as-a-Service solution provides network, system and web application protection immediately, wherever your IT infrastructure resides. Alert Logic partners with the leading cloud platforms and hosting providers to protect over 3,000 organizations worldwide. Built for cloud scale, our patented platform stores petabytes of data, analyses over 400 million events and identifies over 50,000 security incidents each month, which are managed by our 24×7 Security Operations Center. Alert Logic, founded in 2002, is headquartered in Houston, Texas, with offices in Seattle, Dallas, Cardiff, Belfast and London. For more information, please visit www.alertlogic.com.

ALERT LOGIC®