ALERT LOGIC®

SOLUTION OVERVIEW:

ALERT LOGIC® THREAT MANAGER™ WITH ACTIVEWATCH

EXPERT BACKED, DETECTION AND THREAT RESPONSE

Protecting your business assets and sensitive data requires regular vulnerability assessment, continuous threat detection and 24-hour monitoring for quick responses to threats — in your own environment, a hosted environment or the cloud. This is challenging for IT professionals in charge of security at fast growing businesses. Management and employees are pushing adoption of public cloud migration while your shorthanded security staff is trying to avoid being the next public headline.

ALERT LOGIC® THREAT MANAGER™ a cloud-based managed network intrusion detection and vulnerability assessment solution delivered as a service that works in any datacenter environment, from on-premises to the cloud. It works the same way in every environment, so you keep costs down without having to learn multiple systems and hire additional staff.

ALERT LOGIC® ACTIVEWATCH™ our GIAC expert analysts are a 24x7 extension to your team constantly looking for suspicious activity. Experts investigate and respond to Threat Manager™ events and scan data as they are analyzed by Alert Logic® ActiveAnalytics™.

HOW THREAT MANAGER WORKS

Threat Manager™ detects suspicious activity in network environments, quickly identifying threats to your assets so that you can respond. We monitor network traffic and analyze billions of events with our patented ActiveAnalytics.

BENEFITS

- Provides comprehensive protection with an extensive IDS signature database, continual updates, and unlimited vulnerability scanning
- Delivers emerging threat protection based on insight gained from thousands of global customers
- Reduces costs compared against the costs of using multiple traditional solutions
- Provides the latest security technology managed by GIAC-certified analysts
- Addresses compliance requirements of PCI DSS, HIPAA/HITECH, Sarbanes-Oxley, and other mandates
- Significantly reduce costs by augmenting in-house security team with Alert Logic ActiveWatch experts - freeing up internal resources to focus on other tasks

Using intelligent multifactor correlation, we identify security events requiring attention. After validation by a SOC analyst, we notify you with recommended actions/responses within 15 minutes for critical issues. 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.

COMPLIANCE

We help you meet compliance challenges. Threat Manager™ 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).

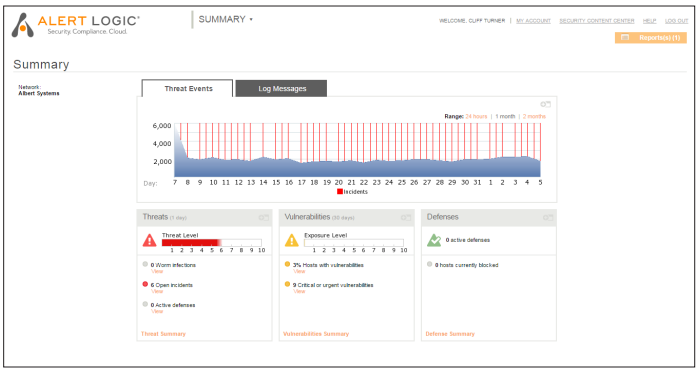
EXPERT ONBOARDING AND OPERATIONALIZATION

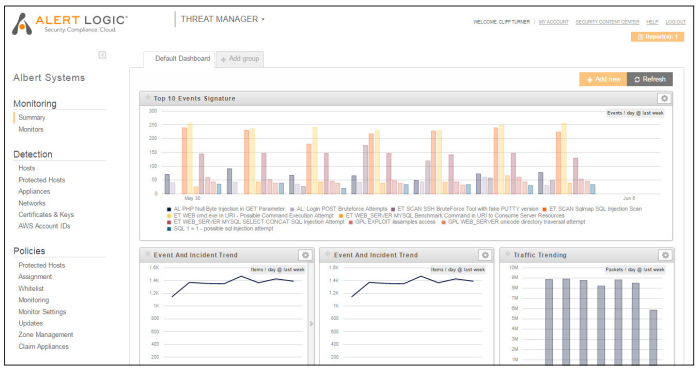
Security investments often go unused or are deployed with partial or default settings – placing businesses at risk while never fully realizing their investments. Our security professionals ensure proper deployment, configuration, tuning and optimization of Alert Logic® Threat Manager™.

Every customer is assigned an Alert Logic onboarding project manager (OPM) to manage the entire process and onboarding team of 20+ specialist including: Project Managers, Onboarding Engineers, NOC Technicians, Network & System Administrators, Security Analysts and Product Trainers.

THE RIGHT SECURITY APPROACH MEANS BETTER SECURITY OUTCOMES

The Alert Logic® approach is fundamentally different from traditional security vendors, who sell single purpose security technologies that require their customers to staff, train, implement and monitor which constantly increases costs and seldom fully addresses the full scope of your security issues. If you've ever seen complex implementation and large investments 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 achieve your security goals. In the age of fast-changing threats and distributed infrastructure, Security-as-a-Service gives you the outcomes you need.

You get all these benefits without a large investment, staff burden or distractions from your strategic IT initiatives. Security-as-a-Service delivery provides 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.

THREAT MANAGER DEPLOYMENT

1

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

- Physical or Virtual Appliances
- Agents with virtual tap

2

Events are analyzed by Alert Logic ActiveAnalytics.

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 your requirements, and analysts work to help you remediate threats and attacks.

ALERT LOGIC SECURITY RESEARCH TEAM

Alert Logic 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, correlation rules, and best practices for resolving incidents.

RESEARCH	CONTENT DEVELOPMENT	EXPERT SYSTEM
• Real-time customer data from more than 3,800 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 • Scanning performance and IDS rule optimization	• Patented correlation engine based on global view of threat data • Continuously analyzes millions of data points into meaningful intelligence

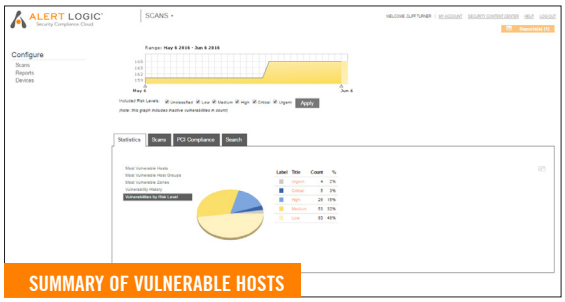
ACTIVEWATCH: EXPERT SECURITY SERVICES FOR THREAT MANAGER

MONITOR – 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.

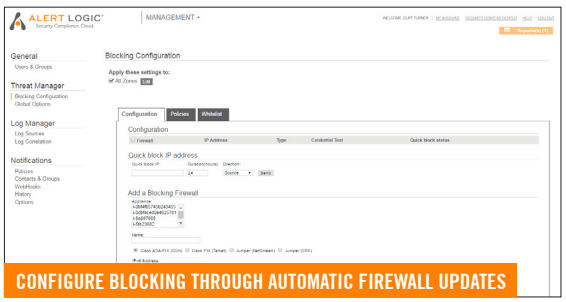
ALERT – when an incident or suspicious network activity is detected, the ActiveWatch™ team will conduct an analysis of the situation and notify your staff based on predetermined escalation procedures. They will work with your team to perform in-depth analysis and assessment of the incident and recommend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

REPORT – 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 – called ActiveWatch Premier are available which include daily summary review by a senior security analyst, weekly reporting on security posture based on business goals, and review of NetFlow for anomaly detection, 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	• 68,000+ 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

ENVIRONMENTS WE PROTECT

Alert Logic delivers Security-as-a-Service, protecting your critical data across public cloud, private cloud, on-premises, managed hosting/co-lo and hybrid environments.

Alert Logic has built deep integrations into the leading public cloud platforms including Amazon Web Services and Microsoft Azure.

amazon web services

Microsoft Azure

PRIVATE CLOUD

HOSTED

PUBLIC CLOUD

ON-PREMISES

ALERT LOGIC®