ALERT LOGIC®

ALERT LOGIC® PROFESSIONAL

Intrusion detection and log management, backed by 24/7 monitoring and threat analysis from certified security experts

ATTACKERS INNOVATE. WE DO, TOO.

Addressing threats is a moving target. Monitoring around the clock requires a 24/7 Security Operation Center (SOC), but creating your own can take years. High costs and staffing challenges mean that organizations struggle to identify, prioritize and respond to threats. Security approaches like Security Information and Event Management (SIEM) and traditional outsourcing are expensive and often fail. There is a better way.

Alert Logic Professional provides visibility into your environments (cloud, on-premises, or hybrid), and helps you identify the remediation steps required to reduce exposures. You get an intrusion detection system that includes security monitoring and threat analysis from certified security experts to help you detect threats and eliminate vulnerabilities.

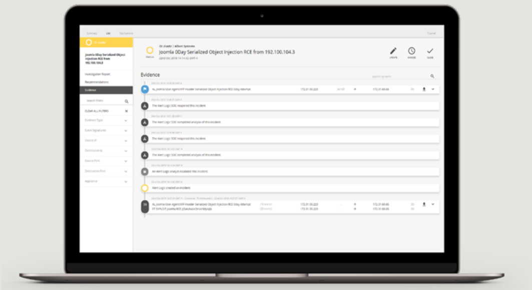
Alert Logic delivers the platform, intelligence, and expertise to help you build a mature security program and meet compliance mandates at a lower total cost than other approaches. That's the benefit of SIEMless Threat Management. Only from Alert Logic.

ALERT LOGIC PROFESSIONAL INCLUDES THE FOLLOWING:

- SOC 24/7 incident management and response support
- Security Posture Report
- Always-updated threat intelligence feeds
- Threat content and emerging threat details
- Asset visibility
- Anti-virus scanning
- Vulnerability scanning
- Vulnerability and remediation intelligence
- Extended Endpoint protection
- Machine learning and behavioral analytics
- Threat risk intelligence – summary and trends
- PCI scanning ASV support
- Log file analytics

WITH ALERT LOGIC PROFESSIONAL, YOU GET:

- Better threat visibility with our award-winning platform
- Security content and intelligence to place threats in context
- Escalation support for vulnerabilities and intelligent notifications
- Endpoint protection to break attacks at the earliest opportunity
- Help to validate, triage and respond to incidents
- Tactical and structural handling recommendations to make you more secure
- Receive notification of critical issues within 15 minutes of verified incidents



> *"We chose Alert Logic because we can be safe in the knowledge that we've got experts looking at our network activity 24/7 when we're not able to do it."*
>
> Richard Marshall
> Head of Platform, Wealth Wizards

Wealth Wizards

	Es ALERT LOGIC® **ESSENTIALS** Vulnerability & Asset Visibility with Extended Endpoint Protection	Pr ALERT LOGIC® **PROFESSIONAL** *Essentials* + Threat Detection & Incident Management	En ALERT LOGIC® **ENTERPRISE** *Professional* + Managed WAF & Assigned SOC Analyst options
SECURITY PLATFORM	• Asset discovery • Vulnerability scanning • Extended endpoint protection • Cloud configuration checks • Compliance	• Threat monitoring and visibility • Intrusion detection • Security analytics • Log collection and monitoring • Extensive log search capabilities • Anti-virus and Cloud vendor security integrations	• Always-on WAF defense against web attacks (e.g. OWASP Top 10, emerging threats, zero-day vulnerabilities) • Protection from SQL Injection, DoS attacks, URL tampering, cross-site scripting attacks & more
THREAT INTELLIGENCE	• Threat Risk Index • Remediation guidance • Prioritization and next steps • Comprehensive vulnerability library	• Event insights and analysis • User behavior anomaly detection • Threat frequency, severity, and status intelligence • Attack protection capabilities	• Verified testing against more than 2.1 million web application attacks • Advanced detection capabilities to spot and block malicious activity • Dark Web scanning
EXPERT DEFENDERS	• 24/7 email and phone support • PCI Scanning and ASV support • Service health monitoring	**ACTIVEWATCH PROFESSIONAL** • 24/7 SOC with incident management, escalation, and response support	**ACTIVEWATCH ENTERPRISE** • Security Posture Review • Incident response assistance • Threat hunting • Help with tuning strategies, customized policies, and best practices

ALERT LOGIC®