ALERT LOGIC™

SOLUTION OVERVIEW

Alert Logic MDR Enterprise

Designated security expert for individualized protection

Purpose-Built To Protect Your Highest Risk Assets

Security professionals responsible for the security posture of their organizations are well aware of the challenges in finding highly qualified and skilled people. Recent studies show the shortage of skilled security people to be in the millions which means these highly skilled people will be in high demand and difficult to retain. This puts an organization in a difficult situation because they need the security expertise in order to protect their IT estate.

Alert Logic MDR Enterprise consists of a designated security expert who becomes an extension of your staff. This person provides in depth individualized evaluation, protection, and customized response services, leveraging the Alert Logic Professional service.

ALERT LOGIC MDR ENTERPRISE INCLUDES:

- Continuous Threat Hunting
- Pro-Active Tuning and Sensor Optimization
- Extended Security Investigations
- Custom Response Processes
- Weekly Security Review
- Annual On-Site Visits

With Alert Logic MDR Enterprise, You Receive

DESIGNATED SECURITY EXPERT

Get access to a veteran security expert in the Alert Logic Security Operations Center (SOC). Focused on your security and business requirements, your designated security expert works as a member of your team to level up your security maturity. In-depth individualized evaluation, protection, and customized response services enhance the other Alert Logic MDR services for greater insight into data exfiltration and discovery of advanced persistent threats.

CONTINUOUS THREAT HUNTING

Continuous threat hunting is a proactive approach to threat detection that identifies and disrupts cyber threats that target your business. Multiple teams enable Alert Logic to deliver complex threat analysis. Informed by research and intelligence and based on known attack methods, and unusual activity indicators, experts in our security operations centers work to identify persistent threats. Network telemetry, logs from security devices, applications, and systems are all analyzed using custom methods and purpose-built tools to find indicators that our hunters follow to identify threats. They then collect more data to rapidly uncover time-sensitive insights about active threats to reduce dwell time and stop attacks before they start.

REPORTING AND CONSULTATION

Your assigned security expert performs proactive daily security reviews to identify incident and threat trends unique to your environment. Recurring reports detail key findings and recommendations, threat trends, and risk analysis. Weekly meetings with IT and security employees in your organization are utilized to learn, understand, and advise on what is critical to your business to help guide and prioritize your operations and delivery programs.

PROACTIVE TUNING AND SENSOR OPTIMIZATION

Thanks to their intimate knowledge of your organization, systems, and security controls, your designated security expert can act as an extension of your team, working in the background to configure, tune, and optimize the Alert Logic technologies and processes based on your unique profile and change programs. Through continual analysis of threat indicators and behavioral data, we identify false positives and events of no relevance to you, which feed into the tuning procedure.

	MDR ESSENTIALS	MDR PROFESSIONAL	MDR ENTERPRISE†
SERVICE ELEMENTS			
Implementation Support	●	●	●
24/7 Platform Support	●	●	●
Vulnerability Insight Support	●	●	●
PCI Dispute & PCI DSS & ASV Program Support	●	●	●
MDR CONCIERGE		●	●
24/7 Threat Management		●	●
15-minute Escalation SLA		●	●
Emerging Threat Response		●	●
On-Demand Tuning & Sensor Optimization		●	●
Machine Learning Log Review		●	●
DESIGNATED SECURITY EXPERT			●
Continuous Threat Hunting			●
Pro-Active Tuning & Sensor Optimization			●
Extended Security Investigations			●
Weekly Security Review			●
Annual On-site			●
FEATURES			
Hybrid Asset Discovery	●	●	●
Internal & External Vulnerability Scanning	●	●	●
Cloud Configuration Checks/CIS Benchmarks	●	●	●
Endpoint Detection	●	●	●
PCI Scanning	●	●	●
File Integrity Monitoring		●	●
Network Monitoring		●	●
Log Data Monitoring		●	●
Log Collection & Search with 12 Month Retention*		●	●
Web Log Analytics		●	●
Real-time Reporting & Dashboards	●	●	●
Cloud Security Service Integration		●	●
Cloud Change Monitoring		●	●
User Behavior Monitoring		●	●

† Alert Logic MDR Enterprise requires Alert Logic MDR Professional licences for protected assets included in the Alert Logic MDR Enterprise service
* Log retention is always on-line, no restriction on search window exists and more than 12 months retention is available on-request

Contact us to learn more: www.alertlogic.com/mdr