ALERT LOGIC®

PATHMAKER GROUP

SOLUTION BRIEF:

THREAT & RESPONSE EXPERTISE

Qualified security staff are hard to find and difficult to retain. And, operating a dedicated 24/7 security operations center (SOC) can be expensive. Plus, a mix of security tools makes it nearly impossible to understand attack data holistically, requires expensive and difficult-to-find skilled resources, and requires substantial effort to get to value.

As a result, security and IT directors spend far too much time and money on breach prevention and threat detection, and it takes significant efforts, filter through the noise, chase down false positives and focus on actual attack data.

With over 82% of breaches1 caused by malware, user misuse, or social attacks, there must be a better way.

82%

of breaches[1] caused by malware, user misuse, or social attacks

With nearly two decades of experience providing Security Operations to thousands of organizations Alert Logic has been built to ensure these demands can be met by our customers without the expense of building and maintaining their own teams or needing to source security detection technologies from multiple third parties.

PLATFORM + INTELLIGENCE + EXPERTS = PEACE OF MIND

24/7

expertise to identify threats and respond more quickly

Alert Logic SIEMless Threat Management provides the expertise you need to identify threats and respond more quickly.

- Cutting-edge threat intelligence and research maintain pace with the threat landscape.
- Expert security specialists place threats into context and verify incidents so that you can focus on what really matters to your business
- Access to an industry-leading and always up-to-date security platform
- Security guidance and recommendations 24/7

[1] *2019 Data Breach Investigations Report (DBIR)*

> *"WE SAVE A LOT OF TIME AND RESOURCES WITH ALERT LOGIC IN THAT THEY TAKE A LOT OF OUR SECURITY DATA AND DO GREAT CORRELATION ON IT, SO WE DON'T CHASE DOWN GHOSTS. WE SPEND TIME FOCUSED ON THE SECURITY ISSUES THAT MATTER."*
>
> - Zach Vinduska, Vice President, Infrastructure, Security & Compliance, ClubCorp

24/7 Incident Monitoring and Management

Get insights and remediation steps to help you respond to threats and address vulnerabilities. Our expert SOC analysts validate issues and provide support whenever you need it.

Remediation Intelligence

Get clear risk reduction remediation actions based on network and application vulnerability scanning on internal and external assets though a PCI level scanning solution supported 24/7 by scanning experts.

Security Analytics

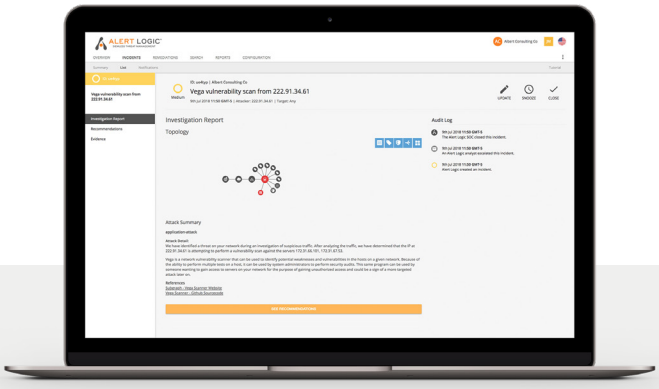
Get a topology view of your environment and in-depth insights into activity, events and potential incidents. This enables you to better understand threats and vulnerabilities with contextual enrichment/enhancement.

Threat Risk Index

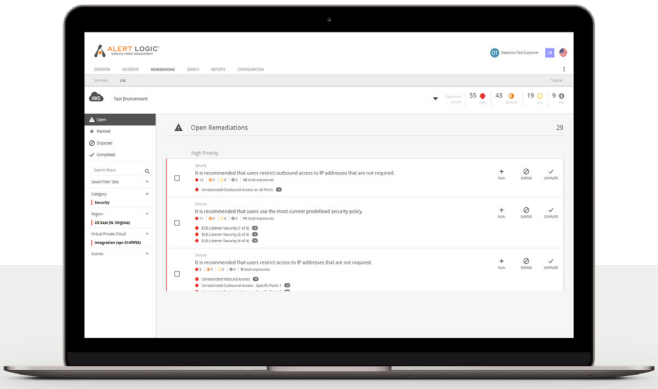
The Threat Risk Index is a personalized score across assets, networks, and deployments which allows you to track improvements over time. Leverage Alert Logic's security intelligence and public vulnerability severity data to gain insights into potential attack risk.

Support for Multiple Environments

Alert Logic solutions work the same way in every environment with only one security solution to deploy, learn and manage. We present security incidents within one console to give you a single view of your security posture. Plus, simple-to-use deployment tools make it easy to quickly extend security into new environments.



- Single view to benchmark your status
- Modern UX
- All your assets in a single dashboard



- Continuously scan for vulnerabilities
- Detect configuration problems
- Manage remediation workflows

ALERT LOGIC®