Nominee: Alert Logic

Nomination title: Alert Logic Cloud Defender

Alert Logic delivers Security-as-a-Service solutions that combine cloud-based software and innovative analytics with expert services to assess, detect and block threats to applications and workload in on-premises, hosted, hybrid and cloud environments, including AWS, Microsoft Azure and Google Cloud Platform. The company also helps businesses comply with mandates like PCI, GDPR, HIPAA and SOX. Alert Logic protects full application and infrastructure stack against attacks to network components, OS, database, and application layers, including hard-to-detect web application attacks and OWASP Top 10 threats. With better web application protection at a fraction of the total cost and time required of traditional security tools, Alert Logic helps reduce risk while accelerating growth of customers' businesses.

Alert Logic Cloud Defender

The first fully managed cloud security and compliance suite, delivers the functionality, security content and actionable intelligence that organisations need to uncover and remediate active threats and secure their data. It delivers four critical detection and protection capabilities – intrusion detection, vulnerability scanning, web application threat detection and log and security event analysis – combined with 'experts included' – security operations center analysts, threat intelligence researchers, data scientists, and signature developers - resulting in the strongest protection.

Supervised machine learning is delivered with Cloud Defender as part of a fully-managed service, enabling Alert Logic to achieve unprecedented accuracy rates in detecting advanced, multi-stage SQL Injection attacks. It combines the required elements of data scientists, threat researchers and Security Operations Center (SOC) analysts who use event telemetry – standardised network, log and application security data – from Alert Logic's more than 4,000 customers to quickly and continually train algorithms which learn by example. This differs vastly from machine learning simply offered as a feature or one that incorporates security data from a single customer only.

Alert Logic's Security-as-a-Service

- **Vulnerability Management (All Environments): Alert Logic provides SaaS solutions to run internal and external vulnerability scans and reports for on-premises, hosted and cloud environments with continuous updates to more than 92,000 Common Vulnerabilities and Exposures (CVEs) in software and certain network components. Alert Logic is a PCI Approved Scanning Vendor (ASV) for conducting external scans for PCI DSS attestation as well as reporting for other compliance mandates.**

- **Automatic Asset Discovery and Scanning of New Instances (AWS Environments) within minutes of being added to the environment – helping the customer understand where to take action by maintaining a current visual map of their topology that they can pivot by AMI, Instance ID & Type, IP Range, Availability Zone, tags and keywords. Configuration auditing of customer AWS environments alerts them to exposures such as overly permissive security groups or IAM policies, ELBs using insecure ciphers and S3 buckets that allow unauthenticated access**

- **Advanced Detection for Cloud-Relevant Threats – in addition to common threats affecting workloads including malware, brute force, system level attacks, and privilege escalations, Alert Logic provides detection of threats specific to web applications such as:**

  - **Exploits against known vulnerabilities in popular web application frameworks and other app stack components such as WordPress, Magento, PHP, Apache, ASP.Net, MongoDB and Hadoop**

  - **Web application attack methods, including OWASP Top 10 such SQL injection, cross-site scripting, cross-site request forgery, information lead/disclosure, path traversal, code inspection, input validation and authentication issues.**

- **Assists organisations with meeting compliance mandates without disrupting their business activities**

- **Identifies vulnerabilities across an organisation's IT infrastructure in real-time**

- **Defends web applications from attacks to ensure availability and prevent data loss**

- **Analyses logs across the application stack to identify malicious or anomalistic behaviour**

Alert Logic's differences to their competitors include:

CENTRALISED SECURITY MANAGEMENT

Cloud Defender protects all infrastructure types and provides a single user experience, eliminating the need for a security solution for each type of environment and protects data at several layers of the application stack - network, system, and web application. It provides around-the-clock 24x7 monitoring.

SCALABLE THREAT DETECTION AND RESPONSE MANAGEMENT

Cloud Defender provides the benefits of traditional security solutions without the cost and complexity of internal deployment and management. It combines advanced technology and security expertise to deliver the features, security content, threat investigation, and a call from their security experts to walk customer through remediation process when a high priority incident is detected environment - unlike traditional solutions requiring hardware purchase, implementation of complex software, correlation rule configuration and internally generated security content.

NATIVE PUBLIC CLOUD SECURITY

Cloud Defender is delivered from the cloud, providing customers with a solution that is easy to get up and running quickly – first results can be observed within minutes.

EXPERT ONBOARDING

Alert Logic's security professionals ensure proper deployment, configuration, tuning and optimisation of Cloud Defender. Every customer is assigned an Alert Logic onboarding project manager (OPM) to manage the process and onboarding team of 20+ specialist.

Funky Pigeon commended Alert Logic's products, and excellent customer service, including their ability to 'scale up' during the highest points of traffic. Brett King, Service Delivery Manager at Funky Pigeon said: "The Alert Logic service is enabling us to tick the box for security. It's enabled us to put all our logs into one place for both the AWS environment and the production environments, so we were able to look at the whole thing from end to end rather than little bits in isolation. Because we're a small team, we can concentrate now on the business growth, the new products, the development, improving the site, and not worry about security."

Hillary's Blinds two IT staff members tasked with security management spend a mere 5% of their time reacting to only the high priority security incidents Alert Logic brings to their attention. Julian Bond, Head of ICT at Hillary's said: "We saved thousands of dollars and many hours every week by choosing this cost-effective technology with experts included. Alert Logic ensures that our cloud security extends being the reactive to a truly proactive stance allowing us to continue successfully growing the Hillary's brand."

Many global brands have also taken their security standards to the next level with Alert Logic's solutions – i.e. Time Inc, Steinhoff, Rosetta Stone, The Garrigan Lyman Group.

Why nominee should win

1. Security-as-a-Service solutions that combine cloud-based software and innovative analytics with expert services to assess, detect and block threats to applications and workload in on-premises, hosted, hybrid and cloud environments.

2. The company also helps businesses comply with mandates like PCI, GDPR, HIPAA and SOX.

3. Alert Logic protects full application and infrastructure stack against attacks to network components, OS, database, and application layers, including hard-to-detect web application attacks and OWASP Top 10 threats.

3. Alert Logic helps reduce risk while accelerating growth of customers' businesses.