ALERT LOGIC®

SOLUTION OVERVIEW:

ALERT LOGIC® SECURITY OPERATIONS CENTER-AS-A-SERVICE

THREAT INTELLIGENCE. EXPERT DEFENDERS. WE'VE GOT YOUR BACK.

HIGHLIGHTS:

- Expert defenders in the Security Operations Center (SOC) protecting you 24/7, and turning complexity into actionable information
- Cutting-edge threat intelligence based on industry data and expert research
- Real-time alerting, incident verification, and remediation guidance from experts
- SIEMlessly connecting platform, intelligence, and experts to provide the best security for your business

Alert Logic researchers and SOC analysts stay on the cutting edge of threat intelligence and use machine-learning that builds on data from our customers to enable ever-smarter, ever-stronger security coverage. It's part of our SIEMless Threat Management approach: our threat intelligence researchers acquire and analyze cutting-edge security data, and then our expert defenders take action on that data to detect and defeat malicious actors.

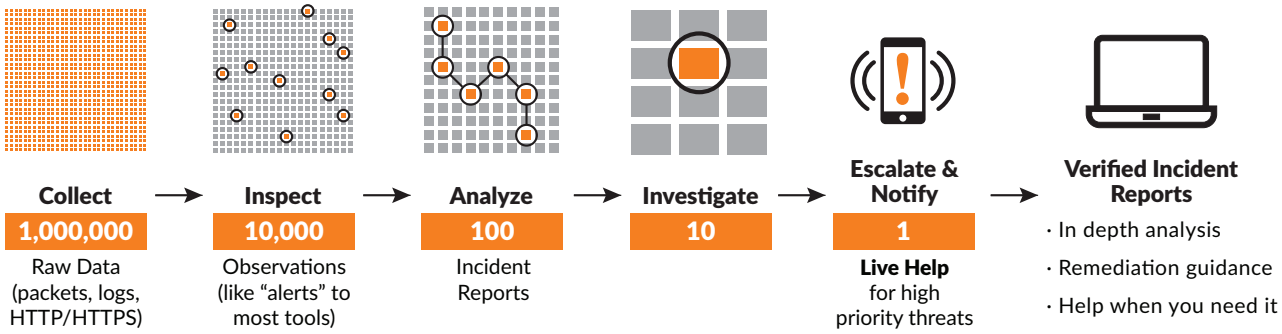
THREAT INTELLIGENCE KEEPS YOU ONE STEP AHEAD

Attackers innovate, and so do we! Our threat researchers are constantly creating security detection methods to stay ahead. The Alert Logic threat intelligence team has an army of researchers on your side, creating the cutting-edge security data necessary to protect your organization against the latest threats.

- Data scientists develop and train algorithms to detect advanced, multi-stage threats
- Security researchers replicate attacks to test how to better prevent, detect and remediate
- Security content developers test, implement and continuously improve detection and blocking logic such as signatures and rules
- Threat intelligence analysts look for changes in attack landscape and to understand the latest trends in how adversaries are operating.

THEN OUR RELENTLESSLY VIGILANT EXPERT DEFENDERS GO TO WORK

The Alert Logic Security Operations Center continuously monitors, triages, and escalates the most relevant threats. They proactively alert you when there are verified incidents that you need to pay attention to and provide remediation advice.



BIG DATA POWERS AND "HERD IMMUNITY" PROVIDE MORE INSIGHT TO PROTECT YOU

Our researchers, data scientists and developers sit atop a curated set of content to help inform our data decisions, including: petabytes of network, log and HTTP session data. It is consistently and continuously collected from cloud and on-premises data centers and thousands of companies worldwide, giving our experts more insight into your adversaries and how to detect and disrupt them.

We also leverage industry-recognized threat intelligence sources containing information about IP/Domain reputation, malware communications, command-and-control servers etc. to provide customers with robust threat detection intelligence.

YOUR OWN ASSIGNED ANALYST

Many customers decide to add Alert Logic Active Watch Enterprise, an optional service which provides an assigned security analyst. Your assigned analyst provides ongoing securing posture reviews, and gets in the "trenches" with you to respond to incidents.

"Tango immediately saw the benefits after the Alert Logic team of experts detected attack patterns coming from China and made recommendations to our Tango team on how to address them. We implemented those recommendations immediately to ensure none of the traffic coming from that area could have access to our system."

Bill Thornton, Vice President, Tango

TANGO

ALERT LOGIC®