ALERT LOGIC®

SOLUTION BRIEF:

24/7 SECURITY MONITORING

Monitoring threats in motion is a continuous process but staffing a 24/7 Security Operations Center (SOC) is expensive and difficult to accomplish. Most organizations simply cannot afford this level of staffing. And, even if they could, a dramatic cybersecurity skills shortage means that it is incredibly difficult to hire and train an internal team. Therefore, many organizations opt to go without 24/7 security monitoring, hoping to catch what they can during business hours and react to threats the next morning or weekday.

SECURITY IS A "ROUND-THE-CLOCK" REQUIREMENT

Bad actors don't adhere to business hours, and your security efforts can't afford to either. Alert Logic's ActiveWatch SOC Team found that over 60% of the most severe incidents happen during nights and weekends. Since most compromises happen within seconds of launching an exploit, by the time business hours roll around, it's already too late.

Attackers don't adhere to business hours. Over

60%

of high and critical incidents occur during nights & weekends.

STOPPING ATTACKS AND ELIMINATING DWELL TIME

Delays in responding to threats increases potential attacker dwell time and can result in breaches, data exfiltration, increased remediation complexity, and potentially dramatic financial losses. In a recent "Cost of a Data Breach" report research, the Ponemon Institute found that there is a "direct correlation between how quickly an organization can identify and contain a data breach, and the financial consequences that may result.[1]"

BUILDING YOUR OWN SOC IS COMPLICATED (AND EXPENSIVE)

Building your own 24/7 SOC can cost anywhere between $2M and $5M per year between staffing, security tools, and physical space. The cybersecurity skills shortage makes hiring the 15-20 security experts required to staff an around-the-clock SOC even more challenging. Yet, despite this massive investment, nearly 75% of all SOCs fail to meet business goals and/or achieve recommended maturity levels.[2] Many of these organizations end up turning to a security partner like Alert Logic to give them the benefit of a 24/7 SOC without the hassle and expense.

[1] *Dark Reading "With Data Breach Costs, Time is Money", July 24, 2019*
https://www.darkreading.com/attacks-breaches/with-data-breach-costs-time-is-money/d/d-id/1335336
[2] *Dark Reading "SOCs Use Automation to Compensate for Training, Technology Issues", July 13, 2018*
https://www.darkreading.com/threat-intelligence/socs-use-automation-to-compensate-for-training-technology-issues/d/d-id/1332292

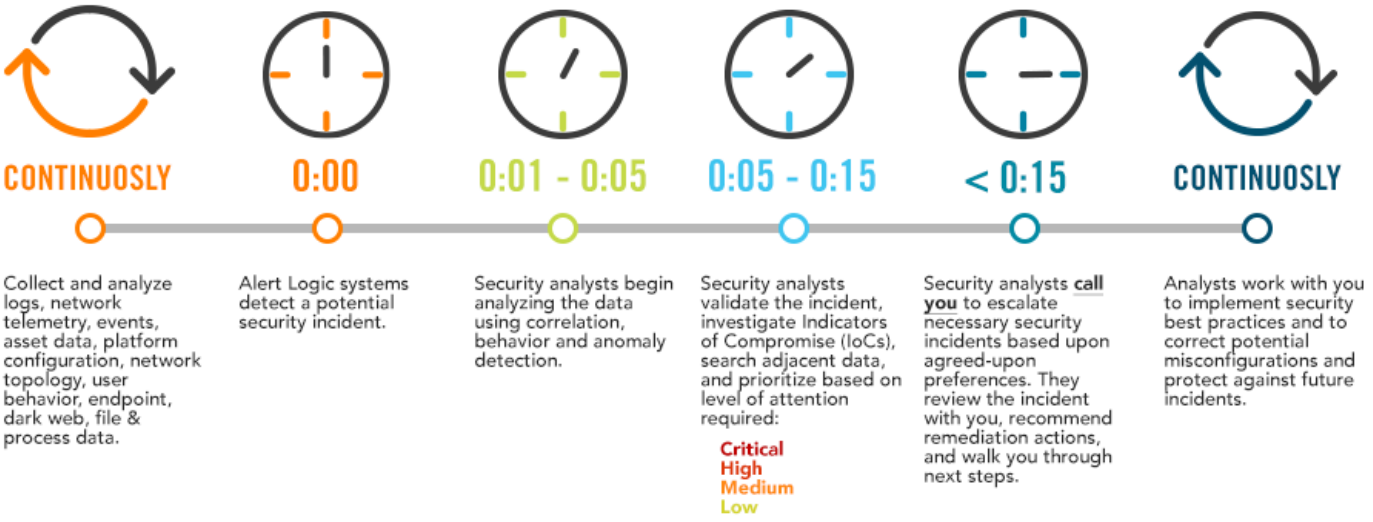
24/7

round-the-clock expertise to identify threats and respond more quickly.

PLATFORM + INTELLIGENCE + EXPERTS = PEACE OF MIND

With nearly two decades of experience providing Security Operations to thousands of organizations, Alert Logic provides 24/7 peace of mind to our customers. Alert Logic SIEMless Threat Management provides the expertise our customers 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 matters to your business
- Access to an industry-leading and always up-to-date security platform
- Security guidance and recommendations 24/7



SERVICES AND OPTIONS AVAILABLE

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.

15 MINUTE SLA FOR HIGH & CRITICAL INCIDENTS: The Alert Logic SOC works with you to determine how you want to be contacted in the event of an incident. However, our standard protocol is to pick up the phone and contact you within 15 minutes of a high or critical incident.

REMEDIATION INTELLIGENCE: Get clear risk reduction remediation actions based on network and application vulnerability scanning on internal and external assets.

THREAT INTELLIGENCE: Gain insight into real threats in your environments, helping you make more informed security investment and resource decisions faster. Our threat intelligence reduces network threats and delivers verified security incidents.

DARK WEB SCANNING: Know when executive credentials are found on the dark web – at any hour. Dark web scanning uncovers potential risks of attack due to hacked email accounts, spear phishing, or other targeted social engineering efforts. This option is available in the Alert Logic Enterprise – Active Watch Option.

MANAGED WAF DEFENSE: Protect your enterprise with an always-on, fully-managed WAF defense against web attacks including the OWASP Top 10, emerging threats, and zero-day vulnerabilities. This option is available in the Alert Logic Enterprise – WAF Option.

ALERT LOGIC®