ALERT LOGIC™

WHITEPAPER

Constant Vigilance Is Key for Effective Security

Monitoring for Suspicious Activity and Emerging Threats 24/7 for Better Cybersecurity

Cybercrime is big business. Bad actors around the world are constantly developing new technologies and techniques to streamline the process of finding and compromising vulnerable systems to carry out nefarious activity. Systems exposed to the internet are under constant attack by both automated and targeted attacks. Attacks are also being commoditized—enabling less technical people to mount effective attacks as well. According to security experts:

- Internet-connected systems are attacked every 39 seconds on average—nearly 2,250 attacks per day.[1]
- It takes 206 days on average to identify a breach, and 314 days to contain or remediate it.[2]
- Attackers are leveraging artificial intelligence for targeted and automated attacks.[3]

Cloud Adoption Increases Attack Surface

The pool of targets to compromise increases due to cloud adoption. Experts predict that 94% of all workloads will run in the cloud by 20214 and organizations that move to the cloud typically use two or more cloud providers5.

The security from on-premise to cloud is different, as is security between cloud providers. Security professionals are finding traditional point security products inadequate to extend proper security protection to the cloud. Common cybersecurity tools like firewalls, endpoint protection, and intrusion detection systems provide some measure of defense against these attacks, but inevitably some attacks will slip through. Conducting periodic scans or sporadically reviewing logs means attacks that get past your defenses may remain undetected for long periods and provide cybercriminals with time to linger on your network, conduct reconnaissance to identify other vulnerable and high value targets, and inflict damage.

To detect and defend against continuous attacks, organizations need to monitor 24/7 to identify critical security incidents to be remediated.

94%

of all workloads will run in the cloud by 2021

Better Security with Constant Vigilance

Continuous monitoring is an essential component for effective cybersecurity. However, there are a variety of factors that make it challenging for most organizations to accomplish on their own to achieve round-the-clock security monitoring.

Consider the following figures from recent studies:

- Proper staffing will require 15 - 20 security experts.
- There are 4 million cybersecurity jobs unfilled resulting in a significant shortage of candidates6
- The candidate pool will need to widen to include mid-level to entry level candidates.
- Salary for a junior level security analyst is ~$75,000 USD.
- Ongoing training and professional certifications can be as much as ~$20,000 USD per person.
- There is an estimated $100,000 USD per year for tooling stack.
- Total annual costs amount to $1.5M - $2M USD.

There will also be a ramp period, constant tuning required for the tool stack, and the risk of people leaving once they have been trained which means a constant vigilance program is unattainable for many organizations. Fortunately, there is another way to achieve better security with constant vigilance provided by highly-skilled cybersecurity professionals. Organizations should look at managed detection and response (MDR) providers.

Constant Vigilance with a "Tools + People Approach"

It's crucial to have the right platform, intelligence, and expertise to deliver effective security. Alert Logic has built a managed detection and response (MDR) platform that provides comprehensive security for your workloads across your environment. We also have dozens of security researchers and data scientists working to identify emerging threats and over 150 highly skilled security analysts monitoring client networks from our security operations centers (SOCs) around the clock.

Our experts provide the constant vigilance you need. They filter out the noise and investigate and respond to security incidents 24 hours a day, 365 days a year. We alert customers only to security incidents that need attention, so they can stay focused on their core business and developing innovative products and services for their customers, while having peace of mind that their network and data are being watched.

Learn how you can get more effective security and better cybersecurity outcomes with constant vigilance.

Stories from the Soc

Vigilance Reduces Exposure to Risk

Attackers often use current events as a catalyst or cover for their attacks. During these times vigilance reduces exposure to risk and it's not uncommon to see a spike in scans from nation states and other third-party attackers. However, most of these attacks are correlated, not coordinated — meaning they are automated and somewhat random until they identify vulnerable targets.

During a recent geopolitical event, Alert Logic security analysts noticed a rise in traffic polling systems on a client network. Certain services use specific TCP/IP ports, and the system is designed to respond to queries with information about the platform and version to facilitate connection. However, that information can also be used to identify and target vulnerable systems. The analyst contacted the customer about the activity with remediation guidance of a configuration change to prevent systems from responding to requests from unknown external sources. The result was a dramatic drop in scanning activity.

The combination of data feeds across multiple compute environments, analytics, and experienced people filter out noise to recognize correlation between activity and potentially malicious outcomes. This is how constant vigilance helps provide effective cybersecurity.

1 University of Maryland, Study: Hackers Attack Every 39 Seconds
2 IBM Security, 2019 Cost of a Data Breach
3 CNBC, Automated hacking, deepfakes are going to be major cybersecurity threats in 2020
4 Cisco Annual Internet Report (2018-2023)
5 Gartner, Why Organizations Choose a Multicloud Strategy
6 Alert Logic, Six Practical Approaches to Bridge The Cybersecurity Talent Shortage