sysdig

The 555 Benchmark for Cloud Detection and Response

10 MIN TO PAIN

Cloud attacks are fast. After finding an exploitable asset, malicious actors need less than 10 minutes on average to execute an attack. Although identity and access management, vulnerability management, and other preventive controls are common in cloud environments, no organization can stay safe without a threat detection and response program for addressing zero-day exploits, insider threats, and other malicious behavior.

Operating in the cloud securely requires a new mindset. Cloud-native development and release processes pose unique challenges for threat detection and response. DevOps workflows — including code committed, built, and delivered for applications — involve new teams and roles as key players in the security program. Rather than the exploitation of traditional remote code execution vulnerabilities, cloud attacks focus more heavily on software supply chain compromise and identity abuse, both human and machine. Ephemeral workloads require augmented approaches to incident response and forensics.

Cloud security programs need a new benchmark. The 555 benchmark — 5 seconds to detect, 5 minutes to triage, 5 minutes to respond — challenges organizations to acknowledge the realities of modern attacks and to push their cloud security programs forward. The benchmark is described in the context of challenges and opportunities that cloud environments present to defenders. Achieving 555 requires the ability to detect and respond to cloud attacks faster than the attackers can complete them.

5 Seconds to Detect Threats

Challenge

The initial stages of cloud attacks are heavily automated due to the uniformity of a cloud provider's APIs and architectures. Detection at this speed requires telemetry from compute instances, orchestrators, and other workloads, which is often unavailable or incomplete. Effective detection requires granular visibility across many environments, including multicloud deployments, connected SaaS applications, and other data sources.

Opportunity

The uniformity of the cloud provider infrastructure and known schemas of API endpoints also make it easier to get data from the cloud. The proliferation of third-party cloud-detection technologies like eBPF have made it possible to gain deep and timely visibility into IaaS instances, containers, clusters, and serverless functions.

Collect detection signals from the cloud service provider and cloud security tools within 5 seconds to ensure visibility into ephemeral assets.

5 Minutes to Correlate and Triage

Challenge

Even within the context of a single cloud service provider, correlation across components and services is challenging. The overwhelming amount of data available in the cloud often lacks security context, leaving users with the responsibility for analysis. In isolation, it is impossible to fully understand the security implications of any given signal. The cloud control plane, orchestration systems, and deployed workloads are tightly intertwined, making it easy for attackers to pivot between them.

Opportunity

Combining data points from within and across your environments provides actionable insights to your threat detection team. Identity is a key control in the cloud that enables the attribution of activity across environment boundaries. The difference between "alert on a signal" and "detection of a real attack" lies in the ability to quickly connect the dots, requiring as little manual effort by security operations teams as possible.

Automate triage by gathering full context for all correlated signals within 5 minutes of receiving the first relevant alert.

5 Minutes to Initiate Response

Challenge

Cloud applications are often designed using serverless functions and containers, which live less than 5 minutes on average. Traditional security tools expect long-lived and readily available systems for forensic investigation. The complexity of modern environments makes it difficult to identify the full scope of affected systems and data and to determine appropriate response actions across cloud service providers, SaaS providers, and partners and suppliers.

Opportunity

Cloud architecture allows us to embrace automation. API- and infrastructure-as-code-based mechanisms for the definition and deployment of assets enable rapid response and remediation actions. It is possible to quickly destroy and replace compromised assets with clean versions, minimizing business disruption. Organizations typically require additional security tools to automate response and perform forensic investigations.

Use the flexibility of the cloud to initiate tactical response actions within 5 minutes of a high-fidelity detection.

Conclusion

555 is a benchmark for mature threat detection capabilities in the cloud. Performing at this level requires mindsets, tooling, and processes designed for the cloud. Challenging organizational security operations functions to meet 555 for key use cases will substantially improve your threat detection and response program.

sysdig

PB-030 REV. B 7/24