Crystal Morin is a Cyber Security Strategist at Sysdig tasked with bridging the gap between business and security through cloud and container-focused webinars and papers for everyone from executives to technical practitioners.

A speedy response is imperative for cloud security

STRATEGY AND SPEED

Crystal Morin *reports on the security demands of the cloud*

Organisations are using more cloud services every year. According to analyst firm IDC, spending on cloud computing will reach $1.37-trillion by 2027. However, while the technology to build and run in the cloud is pushing ahead, security models and processes have to keep up.

Cloud computing is valued because it is faster and more flexible than traditional IT. However, traditional IT security processes don't work at the same speed. According to Mandiant's M-Trends 2023 report, the average amount of time that an attacker is present in traditional IT networks before being detected is 16 days. In the cloud, the time between an attacker's initial access to an environment and an attack being carried out is only 10 minutes on average, according to Sysdig's 2023 Global Cloud Threat Report. That difference – between days of access in traditional networks and minutes to attack in the cloud – proves that a speedy response is imperative for cloud security.

In order to deliver the most effective approach to cloud security posture, we must consider how IT security is organised and the tools that are available. For example, server or host security has historically been an ownership gray zone, where the protection approach varies based on organisational preferences. Security teams typically focused on the protection of the host itself, while DevSecOps teams prioritised the protection of their applications against attack. Today, these applications can include many different components, such as containers, Kubernetes, virtual machines, serverless instances and other workloads that are connected to them. Rather than long-running implementations that would exist in one place for years, these instances can be created on demand and then removed when they are no longer required.

Correlating and contextualising events is both a time-intensive and time-sensitive task. Traditional security tools like Endpoint Detection and Response (EDR) maintain their strength in Windows workstations. The foundational endpoint roots and immature Linux capabilities of EDR result in critical shortcomings during incident response spanning multiple environments; they simply cannot stitch them together. The only way for security teams to truly secure the cloud is with tools and platforms that are purpose-built for the cloud.

In cloud attacks, threat actors typically try to escalate their account permissions and find more credentials that they can test to access other cloud instances. Cloud security tools deliver better visibility of lateral movement by alerting on the misuse of user identities and entitlements. Cloud logs and recorded API calls provide better visibility compared with traditional on-premise workloads, where lateral movement may only be inferred and tracked down.

Security teams with traditional EDR must manually stitch isolated events together, slowing their ability to effectively respond. Cloud incident investigations require the correlation and contextualisation of multiple domains into a single view, so security teams can quickly trace and build on an event across containers, hosts and cloud activity.

All of this has to be done in real time in order to stop attacks in ten minutes or less. Cloud security teams should be enabled with the tools they need to proactively mitigate threats and risks across their cloud estate. This includes automated prevention of malware processes, pause, stop and kill options for containers, and auto-generated forensic captures. After detecting a risk, security teams should be able to jump into the impacted host to carry out triage, surgical remediation actions and root-cause analysis.

Alongside your tooling, you should look at your collaboration between teams. Rather than working in isolation, your cloud security and developer teams must collaborate on how to prioritise issues and stop exploits together. This requires more insight into each other's goals and working practices so that both teams can help each other be more effective ●