Stream.Security

CDR Essentials:

a guide for overwhelmed cloud teams.

INTRODUCING

The rapid adoption of cloud technology has presented new security challenges that many teams were unprepared to face. The dynamic nature of cloud environments and the pace of change have created significant blind spots in cloud architecture, leading to a lack of confidence in their security. To mitigate risks, security teams must assess and minimize their exposure without impacting operational functionality.

Security Lift and Shift

Traditionally, organizations have relied on Vulnerability Management (VM) solutions to scan their environment and patch vulnerable assets based on their severity. However, the dynamic nature of the cloud has made it challenging for security teams to manage the increasing number of vulnerabilities based on their impact on the business.

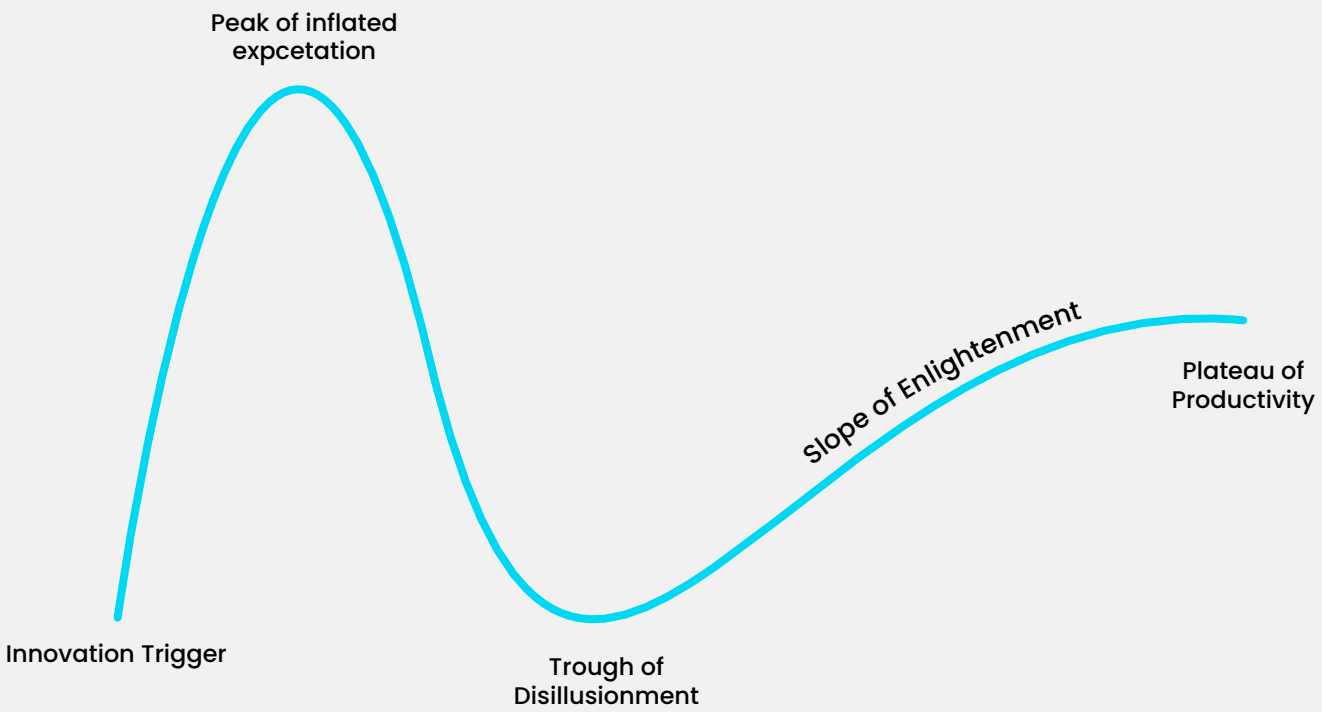
Determining exposure in cloud environments can be particularly ambiguous. Security teams often find themselves blind to the potential impact of vulnerabilities, making it crucial to have an initial "pair of eyes" to get a glimpse of their exposure based on the specific properties of their environment. This initial visibility is the first step in prioritizing fixes based on their potential business impact, ensuring that the most critical vulnerabilities are addressed promptly and effectively.

Initially, DevOps teams adopted a "lift and shift" approach, moving everything from on-premises to the cloud, only to realize that the cloud required a new paradigm—a cloud-native architecture. Similarly, traditional VM solutions have reached their limits once applied to cloud environments since they require a cloud-native approach to managing exposure.

The Golden Age of CSPM

Cloud Security Posture Management (CSPM) was conceptualized around 2019, coined by Gartner. CSPM gives security practitioners a daily view of their cloud exposure, allowing them to prioritize remediation efforts effectively. By 2024, CSPM has become a standard deployment in most enterprises, marking the completion of the initial step in securing cloud environments.

A proper CSPM deployment includes running scans of the cloud environment every day (or even more often), finding any weak spots, and figuring out how to fix them. CSPM has made a big difference for their security teams by periodically checking for issues and making it easier to resolve them quickly.



Cloud Security for Everyone?

Security teams have evolved significantly, developing unique functions to cover different phases of risk and creating a layered defensive system. For simplicity, let's divide the responsibilities into two main categories:

1. Preventive Teams:

These teams focus on hardening the environment to minimize exposure and deter risks. They include vulnerability management teams, governance, risk, and compliance (GRC) teams, and identity and access management (IAM) teams.

2. Responsive Teams:

These teams aim to respond fast to mitigate threats. They analyze behaviors within the environment and investigate and respond to suspicious activities. This group includes Security Operations Centers (SOC), Incident Response (IR) teams, and blue teams.

Responsive teams and preventive teams tackle security from different angles. Preventive teams are all about Hardening the environment to stop threats before they start. They run regular scans, find weak spots, and fix them to keep things secure. Responsive teams, on the other hand, operate with the mindset that breaches will happen. They focus on quickly spotting, investigating, and dealing with threats as they come up.

Understanding a threat isn't just about knowing it's there, it's about grasping the full picture of its impact. This involves looking at the blast radius, which is how much damage a threat could cause, like what data it can access or systems it can affect. It also means assessing exploitability or how easily the threat can take advantage of vulnerabilities. By understanding these aspects, responsive teams can prioritize their actions, contain threats effectively, and minimize overall damage.

Unfortunately, responsive teams are still in the "lift and shift" phase of cloud security, applying on-premises practices to handle cloud threats. They mainly rely on logs from the SIEM to manage these threats, which can be insufficient for the dynamic and complex nature of cloud environments.

The Role of SIEM

Security Information and Event Management (SIEM) systems first emerged in the early 2000s to monitor on-premises environments. As organizations transitioned to the cloud, many extended their SIEM systems to include cloud events. However, the dynamic nature of cloud environments presents unique challenges, such as an overwhelming number of alerts and difficulty assessing alert severity based on business context.

REAL-WORLD SCENARIO

A Breach

Consider a scenario where an attacker uses stolen credentials to log in as a legitimate user, triggering a "new geo location" alert on the SIEM, indicating an unusual login from a different geographical location compared to the legitimate user's typical activity. Next, the attacker clones the organization's most sensitive database (DB), creating a new snapshot of the RDS, which triggers an alert for "a new RDS snapshot created." Following this, the attacker creates a new instance using the cloned database, generating a "new instance creation" alert on the SIEM. Finally, to facilitate data exfiltration, the attacker assigns a new security group to the cloned database that allows internet access, which triggers a "new security group for RDS" alert.

Event	SIEM alert
Attacker logs in using stolen credentials	New geo location
Cloning of the sensitive RDS database	A new RDS snapshot created
Creation of a new instance using the cloned DB	New instance creation
Assign a security group that allows internet access to the snapshotted DB	A new RDS snapshot created

In this situation, the attacker is within the environment with all necessary access to start exfiltrating data. To outpace the adversary, the security team must assess the impact associated with each activity, which is based purely on raw logs from the cloud-native feeds, understand the new attack path, and ultimately, be able to correlate these events and understand that this is the same attack storyline.

CSPM is the answer? Not exactly

CSPM was designed primarily for preventive teams. However, when CSPM tools are used by responsive teams to address ongoing threats, they reveal a significant limitation: they "reverse blink." Each scan provides only a snapshot in time, leaving responsive teams practically blind between scans. The momentary visibility provided by CSPM is inadequate for real-time threat observation and response.

Assuming the responsive team has access to a CSPM tool, a typical workflow would be as follows: upon receiving an alert, the team reviews the most recent scan results and assesses all changes from the last scan to the current state, including alerts like "A new RDS snapshot created" and "New security group for RDS." This process involves manually evaluating new exposures, analyzing the likelihood of damage based on environmental properties (exploitability), and assessing potential damage based on compromised user privileges and accessibility (blast radius). Alternatively, the team can initiate a new scan, wait a few hours, and then handle the threat based on the more updated cloud state.

Both options pose significant time risks: either manually investigating the current state, which may require internal effort or assistance from other teams, or waiting hours for the next scan results to complete. This delay can be critical in fast-paced threat scenarios where immediate action is necessary to mitigate potential damage.

The Cloud Paradigm Shift

Responsive teams must respond fast, requiring real-time cloud state observability to assess threat exploitability and blast radius. This real-time insight could allow them to track the adversary's previous actions and intent, enabling them to outpace the attacker.

The Rise of Cloud Detection and Response

Cloud Detection and Response (CDR) has become a critical component of modern cybersecurity strategies. CDR provides the necessary visibility and real-time monitoring required to detect and respond to threats effectively. It ensures that responsive teams have continuous access to the latest information about their cloud environments, enabling them to act immediately and decisively against potential threats. Additionally, CDR ensures that responsive teams have all relevant contexts for each alert, including the business impact, allowing for more informed and effective responses.

The Four Steps of CDR

Cloud Detection and Response (CDR) involves four main steps for each attack. If any step results in identifying a false positive, meaning there is no risk to the environment and the activity is expected, the process stops at that point. The team will then wait for the next event to investigate, avoiding unnecessary escalation and focusing on real threats.

1. Detection

Identifying behavioral anomalies is the first step in the security process. Various tools and technologies are used to monitor and flag suspicious activities. For example, User and Entity Behavior Analytics (UEBA) tools analyze user behavior to establish baselines of normal activity and flag any deviations as potential threats. These tools must also provide all the necessary context to address a threat, alongside the threat itself. It is crucial to offer this context during the detection phase to equip responsive teams with the information they need to outpace adversaries. This context includes correlating activities and revealing exploitability and blast radius. When anomalies are detected, alerts are sent to the SIEM system for centralized monitoring and response, along with the associated context.

2. Triage

Once an alert is generated, it must be assessed to determine its severity and potential impact. Triage involves evaluating the alert's origin, whether it is an expected behavior or an anomaly. Security teams assess the exploitability of the alert by considering factors such as the presence of vulnerabilities, exposure, the status of multi-factor authentication (MFA), and potential attack paths to sensitive assets. Effective triage helps prioritize alerts based on their likelihood of causing damage, ensuring that security teams focus on the most critical threats.

3. Investigation

After triaging an alert, further investigation is needed to understand the full scope of the potential threat. This involves examining related activities to determine if the alert is part of a broader attack. For example, if a user logs in from a new geo-location and the user is unaware of this activity, security teams need to check if the user has accessed other assets, attempted privilege escalation, or changed configurations. The investigation process helps map out the attack storyline and assess the threat's impact on the environment, ensuring a comprehensive understanding of the potential risk.

4. Mitigation and Remediation

Security teams must take appropriate actions to address the threat following the investigation findings. They have to choose between these two options based on their business needs:

- Mitigation involves immediate steps to reduce the threat's impact, such as isolating affected systems or blocking malicious activities.
- Remediation involves more permanent solutions to eliminate the threat, including patching vulnerabilities, restoring compromised systems, and ensuring no persistence points remain for the attacker.

This stage often requires collaboration with R&D and DevOps teams to assess the

impact on business operations and ensure that remediation efforts do not jeopardize the organization's functionality. Effective collaboration demands that security teams provide context on the remediation's impact and help other teams respond quickly.

Responsive teams must react quickly, requiring real-time access to the cloud state to assess exploitability and blast radius. This need gave rise to Cloud Detection and Response (CDR), providing continuous monitoring and analysis of cloud environments. Unlike traditional CSPM, CDR solutions keep the "eyes" of responsive teams constantly open, ensuring they can outpace adversaries.

Conclusion

Integrating Cloud Detection and Response (CDR) represents the next big step for the cybersecurity industry. As cloud environments continue to evolve, the need for real-time visibility and continuous monitoring becomes increasingly critical. CDR provides the tools and context to protect their cloud environments against ever-evolving threats. Embracing CDR technology will empower cybersecurity teams to enhance their detection, triage, investigation, and remediation processes within their business impact context.

About Stream Security

Stream Security is a leader in Cloud Detection and Response (CDR), leveraging its innovative CloudTwin technology. CloudTwin is a real-time simulative model that maps all cloud activities, configurations, and identities onto a dynamic graph. This advanced model reveals the impact of every activity, helping security teams instantly uncover exploitability, blast radius, and the entire attack storyline. By providing this level of visibility, CloudTwin enables security teams to understand the nature of attacks at the speed of the cloud and outpace the adversary.

Ready to dive deeper?

We hope you found our insights valuable.

If you're curious to explore Cloud Detection and Response further and see a live view of your cloud environment, let's talk.