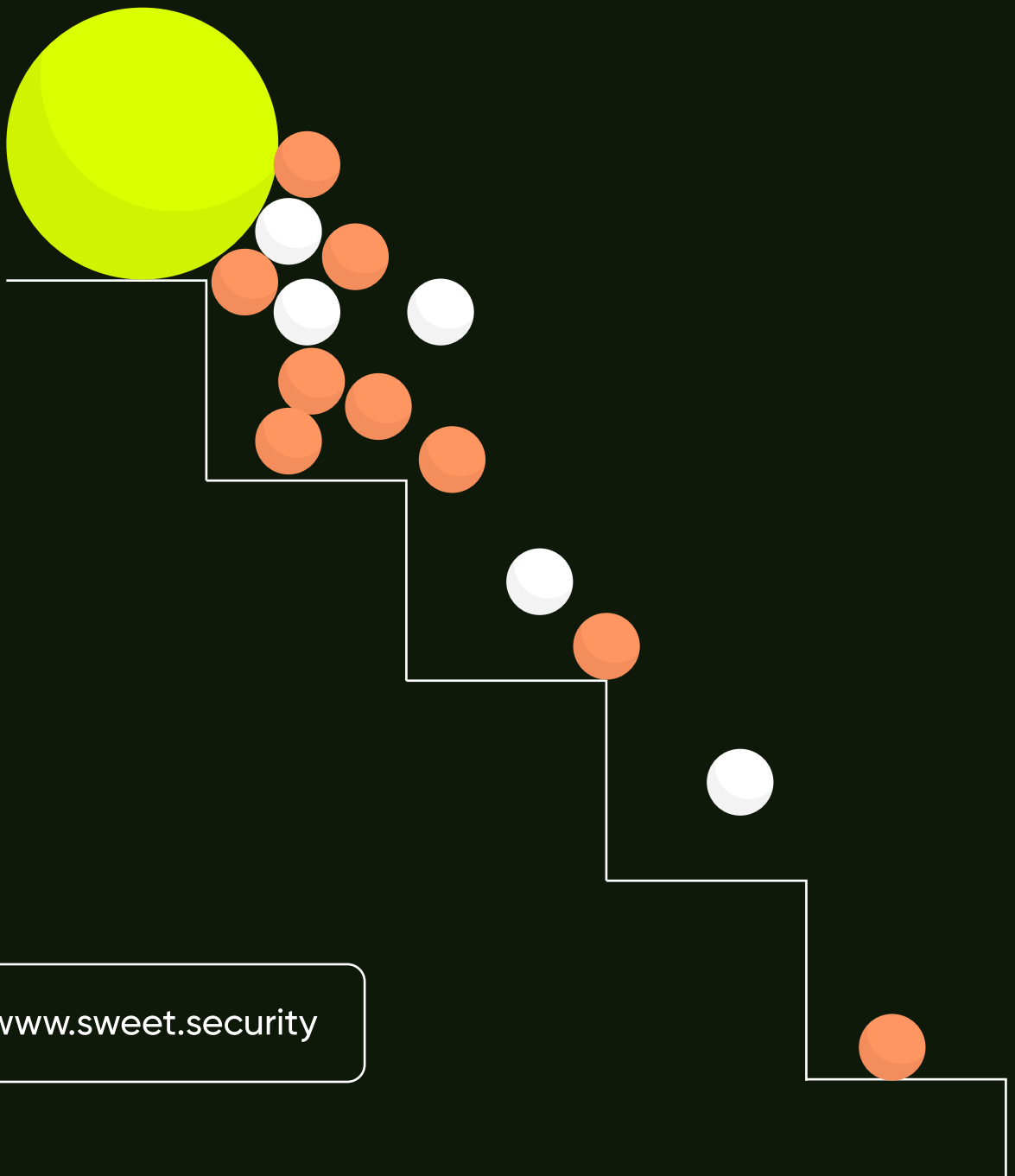
sweet.

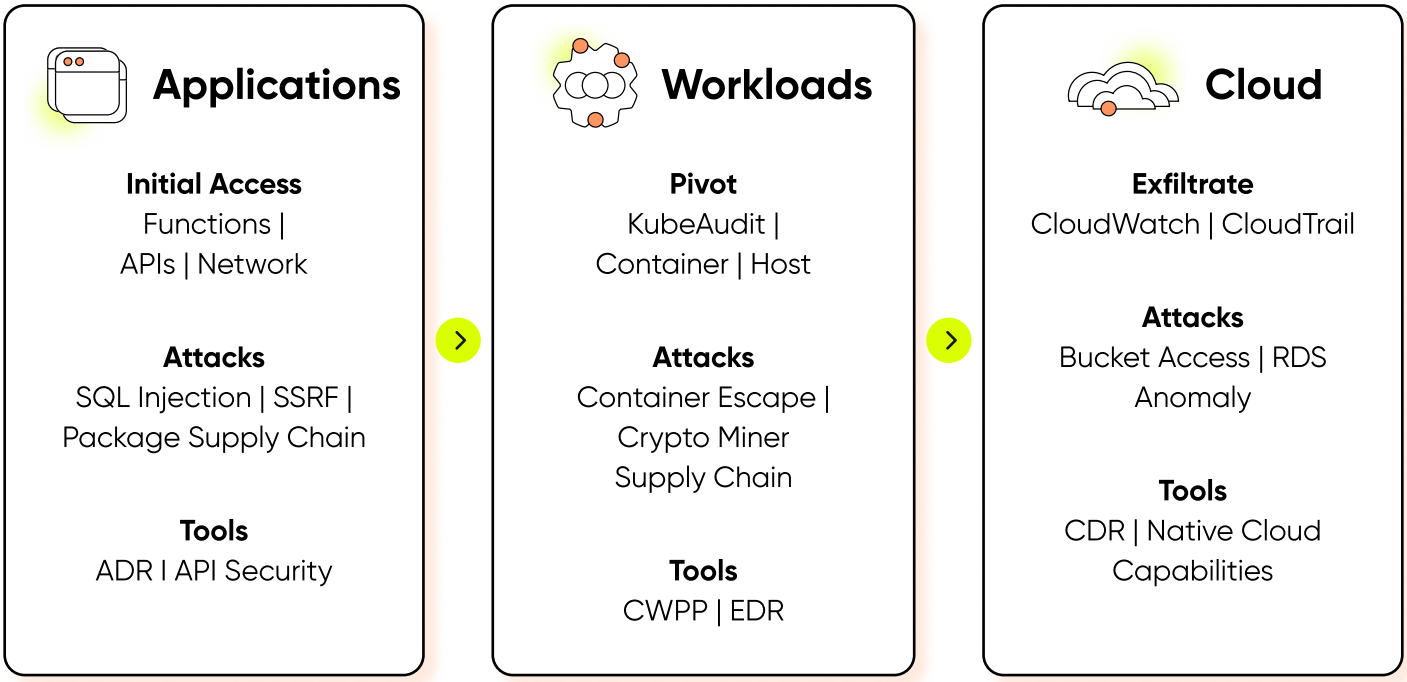
5 Steps to Boost Detection and Response in a Multi-Layered Cloud



www.sweet.security

5 Steps to Boost Detection and Response in a Multi-Layered Cloud

The link between detection and response (DR) practices and cloud security has historically been weak. As global organizations increasingly adopt cloud environments, security strategies have largely focused on "shift-left" practices—securing code, ensuring proper cloud posture, and fixing misconfigurations. However, this approach has led to an over-reliance on a multitude of DR tools spanning cloud infrastructure, workloads, and even applications. Despite these advanced tools, organizations often take weeks or even months to identify and resolve incidents.



Add to this the challenges of tool sprawl, soaring cloud security costs, and overwhelming volumes of false positives, and it becomes clear that security teams are stretched thin. Many are forced to make hard decisions about which cloud breaches they can realistically defend against.

By following these five targeted steps, security teams can greatly improve their real-time detection and response capabilities for cloud attacks.

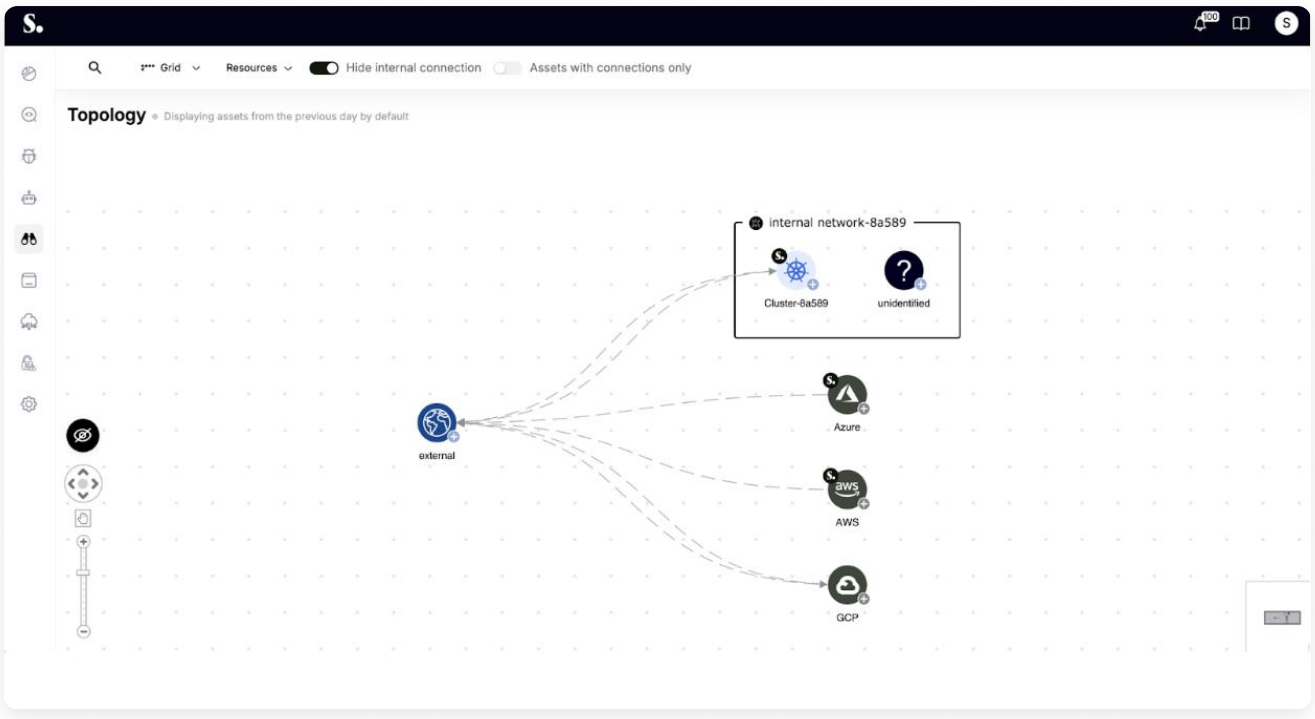
Step 1 Add runtime visibility and protection

When security teams lack real-time visibility, they're essentially operating blind, unable to respond effectively to threats. While cloud-native monitoring tools, container security solutions, and EDR systems offer valuable insights, they tend to focus on specific layers of the environment. A more comprehensive approach is achieved by using eBPF (Extended Berkeley Packet Filter) sensors.

eBPF enables deep, real-time observability across the entire stack—network, infrastructure, workloads, and applications—without disrupting production environments. By operating at the kernel level, it delivers visibility without adding performance overhead, making it a powerful solution for runtime security.

Here are some key capabilities to leverage for this step:

- **Topology Graphs:** Displays how hybrid or multi-cloud assets communicate and connect.
- **Full Asset Visibility:** Showcases every asset in the environment, including clusters, networks, databases, secrets, and operating systems, all in one place.
- **External Connectivity Insights:** Identifies connections to external entities, including details about the country of origin and DNS information.
- **Risk Assessments:** Evaluates the risk level of each asset, alongside its impact on the business.

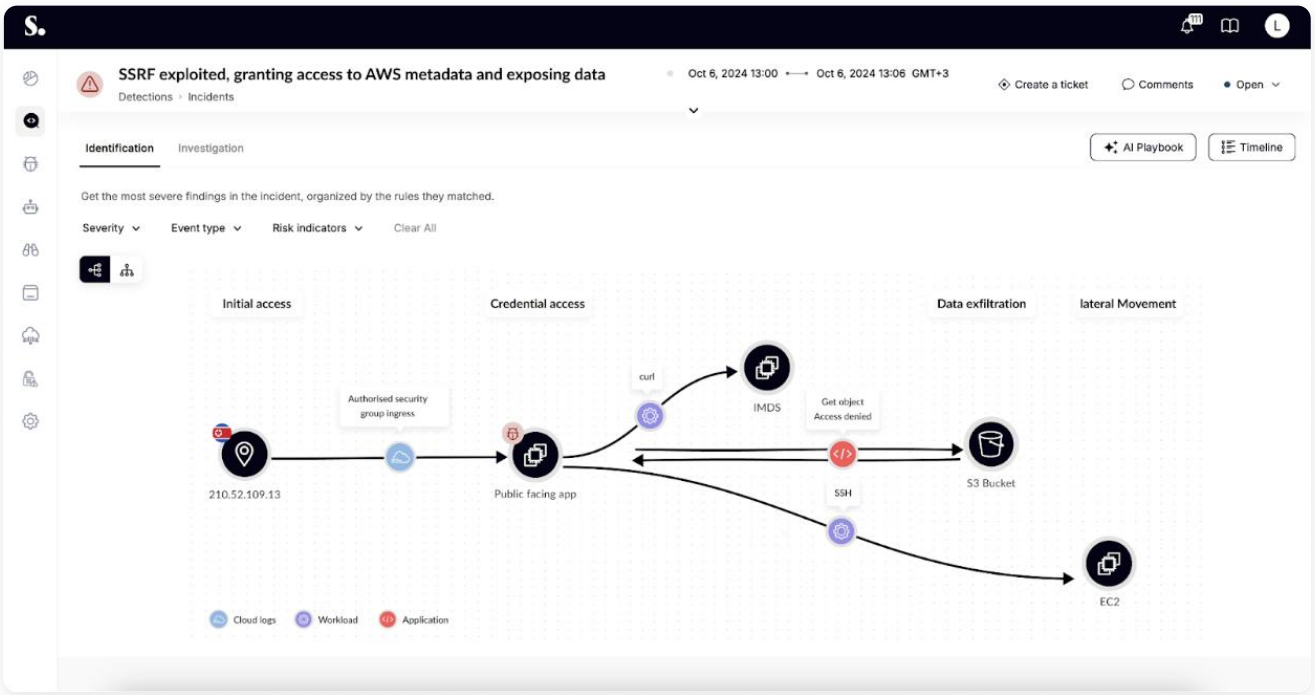


Step 2

Use a multi-layered detection strategy

As attackers continue to evolve and evade detection, it becomes harder to find and stop breaches before they unfold. The biggest challenge in doing so lies in detecting cloud attack attempts where adversaries are stealth and exploit multiple attack surfaces– from network exploitation to data injection within a managed service – all while evading detection by cloud detection and response (CDR), cloud workload detection and response (CWPP/EDR), and application detection and response (ADR) solutions. This fragmented strategy has proven inadequate, allowing attackers to exploit gaps between layers to go unnoticed.

Monitoring cloud, workloads and application layers in a single platform provides the widest coverage and protection. It makes it possible to correlate application activity with infrastructure changes in real-time, ensuring attacks no longer slip through the cracks.



Here are some key capabilities to leverage for this step:

- **Full-Stack Detection:** Detects incidents from multiple sources across cloud, applications, workloads, network, and APIs.
- **Anomaly Detection:** Utilizes machine learning and behavioral analysis to identify deviations from normal activity patterns that may indicate a threat.

- **Detects Known and Unknown Threats:** Pinpoints events according to signatures, IoCs, TTPs, and MITRE known tactics.
- **Incident Correlation:** Correlates security events and alerts across different sources to identify patterns and potential threats.

Get started with multi-layered detection and response today.

Step 3 View vulnerabilities in the same pane as your incidents

When vulnerabilities are isolated from incident data, the potential for delayed responses and oversight increases. This is because security teams end up lacking the context they need to understand how vulnerabilities are being exploited or the urgency of patching them in relation to ongoing incidents

In addition, when detection and response efforts leverage runtime monitoring (as explained above), vulnerability management becomes much more effective, focusing on active and critical risks to reduce noise by more than 90%.

Here are some key capabilities to leverage for this step:

- **Risk Prioritization:** Evaluates vulnerabilities according to critical criteria—such as whether they are loaded into the applications memory, are executed, public-facing, exploitable, or fixable—to focus on threats that actually matter.
- **Root Cause Discovery:** Finds the root cause for each vulnerability (in as deep as the image layer) in order to tackle the root as soon as possible and fix multiple vulnerabilities at once.
- **Validation of Fixes:** Leverages ad-hoc scanning of images before they are deployed to ensure all vulnerabilities were addressed.
- **Regulation Adherence:** Lists out all active vulnerabilities as an SBOM to adhere to compliance and regional regulations.

Step 4

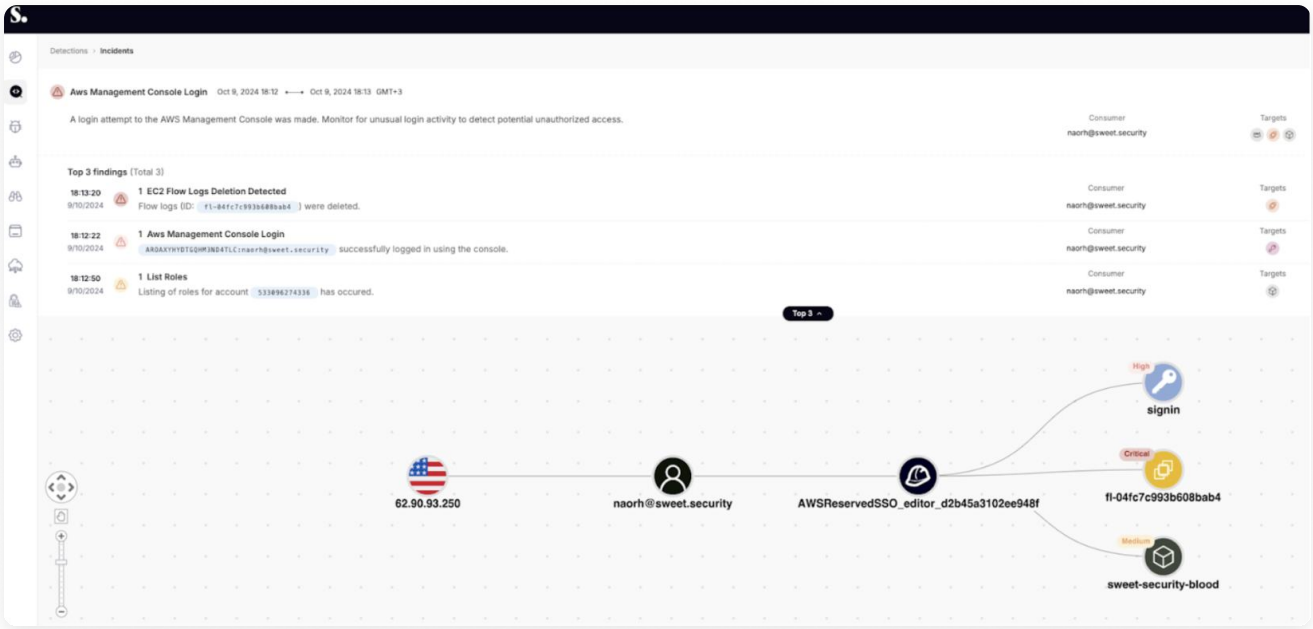
Incorporate identities to understand the “who”, “when”, and “how”

Threat actors often leverage compromised credentials to execute their attacks, engaging in credential theft, account takeovers, and more. This allows them to masquerade as legitimate users within the environment and go unnoticed for hours or even days.

The key is to be able to detect this impersonation and the most effective way to do so is by establishing a baseline for each identity, human or otherwise. Once the typical access pattern of an identity is understood, detecting unusual behavior is easy.

Here are some key capabilities to leverage for this step:

- **Baseline Monitoring:** Implements monitoring tools that capture and analyze baseline behavior for both users and applications. These tools should track access patterns, resource usage, and interaction with data.
- **Human Identities Security:** Integrates with identity providers for visibility into human identity usage, including login times, locations, devices, and behaviors, enabling quick detection of unusual or unauthorized access attempts.
- **Non-Human Identities Security:** Tracks the usage of non-human identities, providing insights into their interactions with cloud resources and highlighting any anomalies that could signal a security threat.
- **Secrets Security:** Identifies every secret across your cloud environment, tracks how it’s used at runtime, and highlights whether they’re securely managed or at risk of exposure.



Step 5

Have a multitude of response actions available for contextual intervention

Each breach attempt has its own unique challenges to overcome, which is why it's essential to have a flexible response strategy that adapts to the specific situation. For example, an attacker might deploy a malicious process that requires immediate termination, while a different cloud event might involve a compromised workload that needs to be quarantined to prevent further damage.

Once an incident is detected, security teams also need the context in order to investigate fast, such as comprehensive attack stories, damage assessments, and response playbooks.

Here are some key capabilities to leverage for this step:

- **Playbooks:** Provides play-by-play responses for every incident detected to confidently intervene and terminate the threat.
- **Tailored Attack Intervention:** Offers the ability to isolate compromised workloads, block unauthorized network traffic, or terminate malicious processes.
- **Root Cause Analysis:** Determines the underlying cause of the incident to prevent recurrence. This involves analyzing the attack vector, vulnerabilities exploited, and weaknesses in defenses.
- **Integration with SIEM:** Integrates with Security Information and Event Management (SIEM) systems to enhance threat detection with contextual data.

By implementing these five steps, security teams can boost their detection and response capabilities and effectively stop cloud breaches in real-time with complete precision. The time to act is now – Get started today with Sweet Security.

sweet.

The time to act is **now**

Get started with multi-layered detection and response today.