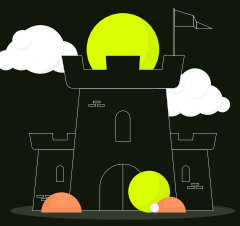
sweet.

Solutions for SOC & IR Teams



Investigate fast. Cut noise. Respond with context.

You don't need more alerts. You need to understand which ones matter — and why. Sweet Security gives SOC and Incident Response teams a complete picture of incidents across the cloud, workload, and application layers, with the context to act and the clarity to reduce MTTR across the board.

Runtime Event Collection

Captures processes, file accesses, network traffic, and memory usage.

Baseline and Deviation Analysis

Establishes normal behavior and identifies anomalies.

MITRE Classification

Tags events using MITRE ATT&CK framework for standardized threat analysis.

IOC and TTP Detection

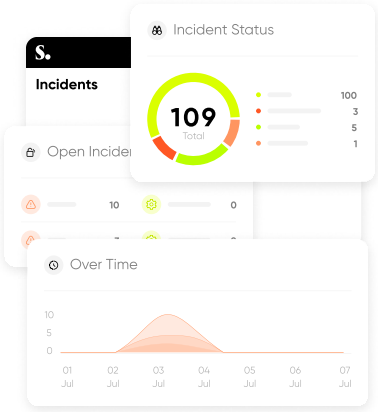
Continuously updated from external security vendors.

Detect Threats in 30 Seconds or Less — Across the Entire Cloud Stack

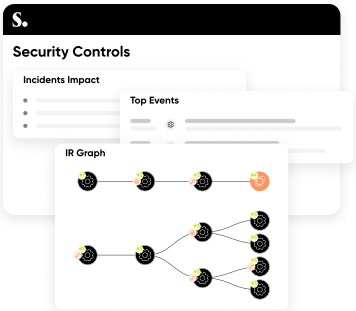
Sweet detects threats in real time, including zero-day exploits, misused identities, or known attack signatures. We monitor activity across:

- **Cloud Infrastructure** (IAM events, session anomalies, policy changes)
- **Workloads** (container behavior, file access, network connections)
- **Cloud-Native Applications** (API calls, external communications, sensitive data flows)

Our engine correlates signals from every layer into a single incident, showing how an attacker moves across your environment — from initial access to lateral movement to the crown jewels.



From Detection to Investigations and Forensics — Instantly



Detection is just the start. Sweet guides analysts through deep investigation:

- LLM-powered detection engine pinpoints root cause and "smoking guns"
- Indications on a true threat or false positive — with clear reasoning
- Identification of the responsible developer or team for fast resolution
- Every incident is shown as a narrative timeline — attacker steps, success/failure, and impact

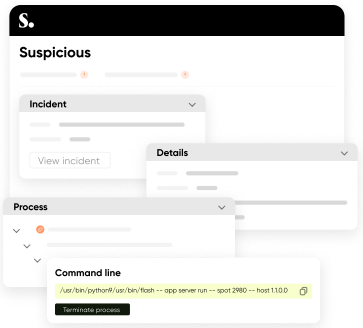
Teams using Sweet reduce MTTR by over 90% — from hours to 2–5 minutes to fully understand and resolve incidents.

Respond and Stop the Attack — Automatically

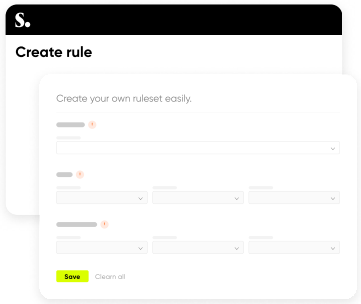
Once you've identified the threat, Sweet helps you shut it down:

- Terminate malicious processes instantly (manually or automatically)
- Send alerts via Slack, Jira, ServiceNow, or custom webhooks
- Integrate with SOAR tools like Torq to automate full incident containment

Whether you respond manually or via automation, Sweet gives you the power to kick the attacker out in real time — not just alert on it.



Tune Your Detections. Not Just Your Alerts.



Every environment behaves differently.
Sweet gives you the control to adapt:

- Build custom detections using signals from cloud logs, workload data, or L7
- Apply workload-specific baselines — by cluster, namespace, or label
- Suppress or tag noisy behaviors without losing visibility
- Enrich findings with context, labels, and team ownership

It's easy to create high-fidelity alerts for your environment, not just generic ones.

Fits Into Your Workflow

Sweet helps SOC teams reduce alert fatigue, investigate with confidence, and respond faster — without switching tools or stitching data together.

Learn more