

## The first continuous red-team agent that combines Mythos-grade models with a whiteboxed adversarial approach - built from within production, powered by Sweet's runtime data

Organizations face a new generation of AI-driven attackers operating at machine speed, while most security tools still cannot validate which vulnerabilities are actually exploitable in real production environments.

- ✗ Most AI red-team tools still operate like external attackers - blind to the internal relationships that determine exploitability
- ✗ Traditional red teams are periodic, manual, and limited in coverage and speed
- ✗ Most security tools generate isolated findings that teams struggle to prioritize into real breach risk

### With Sweet Attack, you can:

#### Close Every Security Gap

Identify and exploit attack paths across your entire runtime environment.

#### Maintain Continuous Coverage

Adopt a continuous, always-on security posture.

#### Shift the Conversation

Focus all teams on exploitable attack paths.

#### Reduce Red Team Costs

Expand validation coverage without proportional cost increases.

## Why Sweet Attack

### • Built from Runtime Intelligence

Sweet Attack operates from inside your environment using the runtime intelligence attackers wish they had:

- Live application behavior
- API traffic
- Identity relationships
- Cloud topology
- Runtime workloads
- Source code visibility

This allows Sweet Attack to reason about attack paths the way real attackers do.

### • Continuous Adversarial Validation

Sweet Attack continuously validates exploitable attack paths across applications, APIs, identities, infrastructure, and AI systems, autonomously and at AI speed.

### • From Findings to Breach Paths

Sweet Attack validates which weaknesses can actually become compromise paths, helping teams focus on the risks that matter most.

## How it works

> 01

### Discover

Continuously map your attack surface across cloud and AI environments.

> 02

### Analyze exploitability

Mythos-grade models identify vulnerabilities that are realistically reachable and exploitable.

> 03

### Build chains iteratively

Learn how attackers could chain weaknesses into real compromise paths.

> 04

### Report + re-evaluate

Confirmed chains, mitigation + remediation guidance, always-on as env evolves.

## Sweet Attack by the numbers

0

previous installations needed



<15min

to first validated finding



100s

of validated finding types across APIs, identities, workloads and more.



All

modern cloud and AI technologies supported



"Cast & Crew has engaged tier-one offensive security firms for years. Sweet Attack surfaced exploitable attack paths in three days that prior engagements had not identified, and paired the findings with a concrete, prioritized remediation plan we were able to action immediately. The combination of depth and operational usability is what set the engagement apart."



**Tal Hornstein,**  
Chief Information Security Officer, Cast & Crew Entertainment Services



## Harnessing the Power of the Sweet Platform

Instead of focusing on singular sources of information, Sweet Attack correlates intelligence across multiple layers into a unified attack chain model. This creates a compounding effect: as visibility expands across the environment, attack-path validation becomes increasingly precise, connected, and operationally relevant. **Attackers still need to piece this intelligence together manually. Sweet Attack already has it.**

[Get a Sweet Attack Demo>>>](#)

[www.sweet.security](http://www.sweet.security)