INTEGRATE. COLLABORATE. VALIDATE.

SnapAttack is the only comprehensive solution in the market that rolls detection engineering, adversary emulation, purple teaming, and threat hunting into a single, easy-to-use product that enables you to use your existing SIEM, EDR and security technology more effectively and streamline collaboration across teams.

01. research
Understand the art of an attack. Operationalize threat intelligence.
- Threat Intel
- Attack Library
- Detection Repo

02. write
Combat attacks with a systematic, scientific approach.
- Attack Capture Lab
- No-Code Detection Builder

03. validate
Put your new defenses to the test.
- Adversary Emulation
- Breach Attack Simulation

04. deploy
Deploy to your existing tools with confidence.
- One-Click Deploy
- Universal Detection Translator

Continuous validation with MITRE ATT&CK coverage mapping

maximize ROI
50% cost reduction for threat intelligence feeds

75% increase in resource effectiveness

< 5% false positive rate as the highest confidence analytics

at a glance view of protection
Enhance your maturity, unlock the potential of your team and tools, and bring the fight to the adversary.

**stay ahead of the threats**

| Scale security. | SnapAttack Feed (Intelligence, Detections, + Attack Sessions): Master their craft by browsing threat intelligence, 1000s of attack sessions, and 1000s of validated detections. |
| Drive team collaboration. | Attack Capture Lab: Spin up both attacker and victim machines in a portable sandbox that allows you to capture tradecraft from anywhere and deploy them into any environment. |
| | Horizontally Integrated Workflow: Integrates intelligence, attacks, and detections enabling each team to tackle key threats with common information in one place. |
| | Built-In Logic and Error Checking: Reduce alert fatigue by validating every analytic for accuracy and precision against our library of known true positive attacks. |
| Up-level your analysts. | No Code Detection Builder: Build quality detections with built-in logic and error checking and a simple, point-and-click interface – all without requiring any coding knowledge. |
| | True Positives: Enable your analysts to easily triage alerts from the field by comparing to known true-positive attack telemetry. |
| Know you're protected. | MITRE ATT&CK Matrix: Identify gaps in coverage for any given attack using the MITRE ATT&CK coverage matrix. |
| | Attack Replay: Deploy real attacks to your environment to prove that your coverage works. |
| Power up your tools. | Universal Detection Translator: Translate detections into any SIEM or EDR query language for seamless deployment. |
| Give your data context. | Detection Repo + Real-Time Tuning: Reduce alert fatigue AND false negatives by validating every analytic for accuracy and precision against our library of known true positive attacks. |
| Maximize ROI. | 30+ Direct Integrations: Get more from the tools you already have with our continuously updated partnerships and integrations. |