SNAPATTACK

SOLUTIONS FOR DETECTION ENGINEERS

FASTER, STRONGER DETECTIONS. WHENEVER AND WHEREVER YOU NEED THEM.

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

Companies turn to SnapAttack when...

They need to apply detections across **several tools, languages, and environments**

They need to **build, validate, and deploy** detections **faster**

They're bogged down by **false positives** and **alert fatigue**

They need a **streamlined, standardized** detection development process

enhance confidence

< 5% false positive
rate gives you the highest confidence detections

get back to the hunt

98% faster
threat hunts

accelerate scale

80-90%
less time spent building detections

SNAPATTACK

Remove barriers to researching, building, testing, and deploying high quality, validated detections.

Write once, run many.

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.

UNIVERSAL DETECTION TRANSLATOR

Translate detections into any SIEM or EDR query language for seamless deployment.

Cut time to deployment.

VALIDATE YOUR WORK

Automate the validation of new detection logic, and leverage our data science-driven approach to score your detections for confidence, false positive performance in advance

ATTACK CAPTURE LAB

Spin up both attacker and victim machines to detonate malware, test attack techniques and automatically see the detections to use.

Build confidence in your coverage.

MITRE ATT&CK MATRIX

Know exactly where you stand by mapping your coverage and environment against the MITRE ATT&CK matrix.

SNAPSCORE

Evaluate accuracy and confidence through SnapScore to drastically reduce false positives.

Hone your craft.

ATTACK LIBRARY

Visualize an attack from start-to-finish in real-time with all the telemetry you need at your fingertips.

DETECTION REPO

View or contribute threat intelligence, attack sessions, and validated behavioral detections to build stronger, higher-confidence detections.