SNAPATTACK

SOLUTIONS FOR SOC MANAGERS

STREAMLINE YOUR SOC TEAM WITH CONFIDENCE, CLARITY, AND EFFICIENCY.

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 **scale** their security program

They need to be **more proactive** in their approach

They need to **get more** from their existing teams and tools

They want to **drive collaboration** across red and blue teams

enhance confidence

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

accelerate scale

98% faster
threat hunts

drive collaboration

80-90%
less time spent building detections

Give your SOC the tools, context, skills, and confidence to not only respond to threats, but stay ahead of them.

Make your existing SIEM and EDR tools work for you, not against you.

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.

Accelerate scale within Security Operations (SecOps).

SNAPATTACK FEED

View and equip threat intelligence, attack sessions, and validated detections all from one place to streamline the hunt process.

ATTACK CAPTURE LAB

Spin up both attacker and victim machines in a portable sandbox that allows you to capture adversary tradecraft.

Drive collaboration and prioritization across teams.

HORIZONTALLY INTEGRATED WORKFLOW

Give teams a platform to collaborate, share intel, and build detections with efficiency and clarity.

Visualize your coverage against every threat.

MITRE ATT&CK MATRIX

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