SNAPATTACK

SOLUTIONS FOR THREAT HUNTERS

CUT THROUGH THE NOISE. GET BACK TO THE HUNT.

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.

Threat hunters turn to SnapAttack when...

They lack the **clarity** they need to accurately **prioritize relevant threats**.

They have disparate **tools** and **data sources**, and struggle to hunt across all of them.

They're sifting through the **noise** in an attempt to understand which threats are actually **legitimate**.

Their **limited time** is spent triaging **false positives and incidents** rather than actually hunting.

accelerate hunt programs

5-10 minutes

before snapattack: 1-2 weeks
after snapattack: 5-10 minutes

scale threat hunting

98% faster

threat hunts

enhance confidence

< 24 hours

< 24 hours to add new threat intel

Operationalize threat hunts with centralized intelligence, integrated tooling, and a streamlined workflow.

Focus on what matters.

THREAT INTEL FEED

Get up to speed on the latest threats through SnapAttack's Threat Intelligence Library, and we'll sift through the noise to help you prioritize hunts.

IOC + TTP HUNTER

Hunt for both IOCs and TTPs using threat intel from anywhere and get automatic feedback regarding what is and isn't relevant to your environment.

Connect the disconnected.

ATTACK LIBRARY

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

DETECTION REPO

Rapidly hunt with thousands of validated TTP-oriented detections validated to work against the latest attacks in your existing SIEM or EDR.

Gain clarity, get proactive.

CONFIDENCE SCORING

Leverage our data-science driven detection confidence scoring to hunt with the precision and speed you need.

MITRE ATT&CK MATRIX

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

Get back to the hunt.

NO-CODE DETECTION BUILDER

Quickly build quality detections with built-in logic and error checking and a simple, point-and-click interface – all without requiring any coding knowledge.

VALIDATE YOUR WORK

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