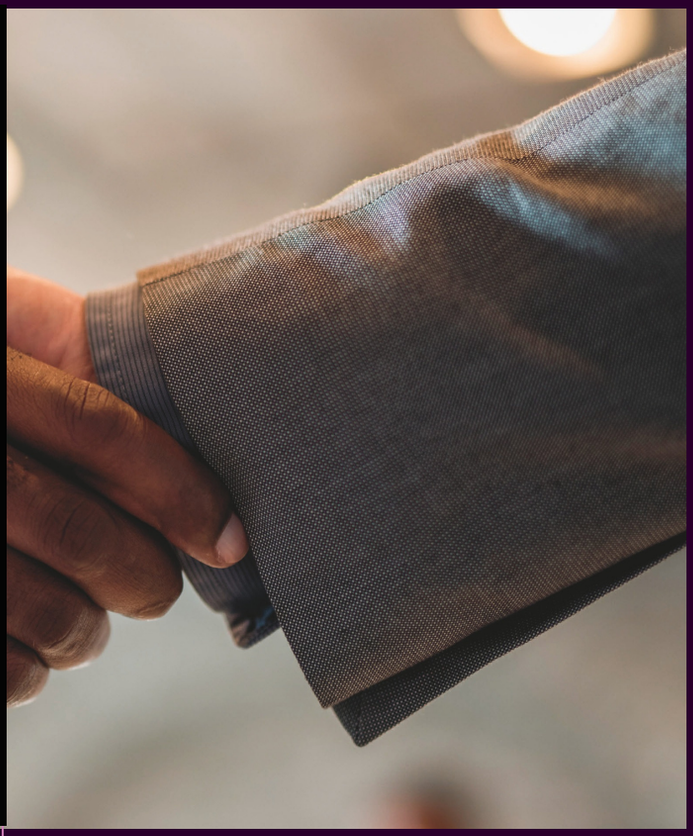
SNAPATTACK + CROWDSTRIKE

A STRONGER DEFENSE

Accelerate threat hunting through adversary emulation and detection-as-code, hardening defenses with the CrowdStrike Falcon® platform.



About the partnership >

SNAPATTACK + CROWDSTRIKE FALCON

Stay on top of today's most critical threats with world-leading threat intelligence that includes tactics, techniques and procedures (TTPs), behavioral analytics, indicators of compromise (IOCs) and a thorough description of each individual actor, with captured attacks in SnapAttack enriching your understanding of any given threat.

SNAPATTACK + CROWDSTRIKE ACCELERATED THREAT HUNTING & SECURITY VALIDATION

Validate your security posture by launching attacks against your infrastructure to identify operational weaknesses for prioritized remediation. View or create validated detection content to enable greatly accelerated hunts, empowering even Junior SOC Analysts, and measure your security posture through the MITRE ATT&CK matrix.

About the platform >

SNAPATTACK

Utilize a library of thousands of validated detections to power security operations. **Build, validate and deploy new detection content to CrowdStrike Falcon or any Popular SIEM, or XDR.** No matter where your customers' security data is, we've got you covered with...

CROWDSTRIKE

Transform threat intelligence into actionable detection content and hunt packages faster, more easily, and at global scale.

Use world-leading threat intelligence

Leverage a constantly growing library of threat intelligence, including front-line research from trusted global partner organizations, available for all SnapAttack users.

Enriched with our Attack Library

Identify specific artifacts left behind by adversary techniques to gain clearer insight into threat intelligence and impacts on victim machines.

Enabling detection at scale

Drive velocity by leveraging our Detection Repo containing thousands of validated detections benchmarked for high confidence and false positive performance. When custom detections are required, streamline the traditional detection development life cycle (DDLC), creating detections 98% faster with SnapAttack's no-code detection builder.

Deployable to any SIEM or XDR

Push button deployment to The Falcon Platform and 30+ other direct integrations, immediately deploy vendor-agnostic, validated detections, queries, and hunt packages into your existing security stack.

Validated in BAS / adversary emulation

Validate your security posture with SnapAttack and CrowdStrike to prioritize remediation and historical threat hunts by minimizing risk from exposed assets.

Why companies turn to SnapAttack >

- They need industry-leading threat intelligence to bring context into their security.
- They have the threat intelligence, but it's too challenging to rapidly action the latest intelligence relevant to them.
- They need a library of detections built upon threat intelligence, immediately deployable into their tools of choice.
- They need to build custom detection content to support threat hunting and security operations at scale.
- They need to validate their security posture through adversary emulation and breach and attack simulation.
- They identified weaknesses in their attack surface through adversary simulation and need to hunt down potential incidents with targeted detections.