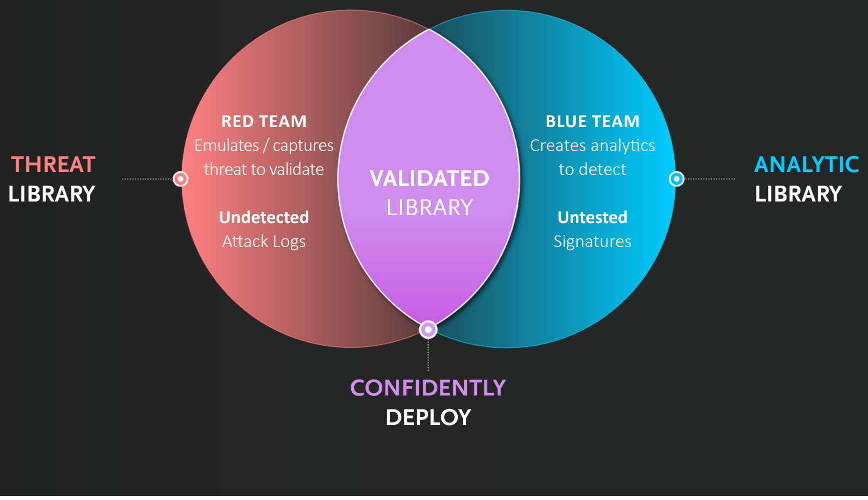
SNAPATTACK®

THE PLATFORM FOR PROACTIVE AND THREAT-CENTRIC SECURITY, BUILT ON REAL-WORLD ATTACKER TRADECRAFT

OVERVIEW

SnapAttack is the security industry's first purple teaming platform. It is a cloud-based software solution that helps accelerate existing threat intelligence, threat hunting, and purple teaming capabilities to help translate IOCs to behavioral analytics, validate true-positive attack behavior, and minimize false positives to drive more focus and efficiency on cyber defense teams.



THREAT LIBRARY

RED TEAM
Emulates / captures threat to validate

Undetected
Attack Logs

VALIDATED LIBRARY

BLUE TEAM
Creates analytics to detect

Untested
Signatures

ANALYTIC LIBRARY

CONFIDENTLY DEPLOY

APPROACH

SnapAttack accelerates your security analytic development and helps measure and proactively reduce cybersecurity risk. Our novel approach involves 3 main steps:

Capturing Adversary Tradecraft:
Organize red team/CTI knowledge in an easily digestible and usable way, enabling your security staff to stay ahead of threats by collaborating in real time

Simplifying Analytic Creation:
An intuitive interface that lowers the barrier to entry to creating high confidence behavioral analytics for your existing security, manage your detection backlog, and gain quantifiable evidence of your program's effectiveness

Reducing Risk:
Using the MITRE ATT&CK framework, track detection coverage and gaps, manage your detection backlog, and gain quantifiable evidence of your program's effectiveness

USE CASE EXAMPLES

SolarWinds and Darkside Ransomware attacks provided a critical example of how scaling and sharing your behavioral detections is needed with advanced actors. SnapAttack helps store threat intel, emulate the kill chain of events, create behavioral analytics, and establish ongoing protection against future attacks.

√ ***Manage and keep up with detections***

√ ***Share information quickly and seamlessly***

√ ***Deploy detections across your tech stack***

√ ***Measure your control gaps and coverage***

DIFFERENTIATORS

SnapAttack is different than what is currently offered as it is an all-in-one purple teaming platform offering an environment for collaboration across red, blue, and threat intelligence teams. The platform evolves your security detections, creates robust behavioral analytics, and optimizes your threat detection.

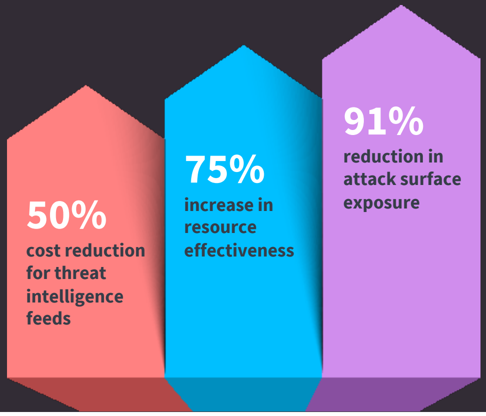
SnapAttack manages the full analytics lifecycle (Identify, Develop, Validate, Deploy, Maintain) and helps automate the deployment process for quick time time to value

SnapAttack creates robust behavioral analytics by validating them against true positive attacks, then testing and tuning in your environment.

SnapAttack optimizes your threat detection and empowers teams to create high-quality behavioral analytics faster, increase analyst productivity, and deliver measured threat and detection

- **Accelerate your analytic creation:** Easy analytic builder and on-going subscription to add 1000+ analytics out of the box
- **Memorialize offensive tradecraft:** Start with over 1,000 captured attack sessions and grow your library
- **Optimize and reduce risk:** Measure MITRE ATT&CK detection coverage and stop threats across the cyber kill chain

	Before		After
VULNERABILITY EXPOSURE:	**7** days	→	**1** day
ANALYTIC TESTING & DEPLOYMENT:	**12** hours	→	**1** hour
THREAT INTEL CURATION:	**75** hrs/wk	→	**20** hrs/wk



If you want to advance your security team's capabilities and improve your enterprise protection, get a demo of the industry's first purple teaming platform, SnapAttack.

For more information please contact: info@snapattack.com

Visit our website: https://www.snapattack.com