



PLATFORM INTEGRATIONS

SnapAttack was built to power not just one tool, but to help you get the most out of any security tool.

SIEMs

splunk>



Microsoft Azure



⇔ DEVO



elasticsearch



NETWITNESS



sumo logic

/logpoint



securonix

Radar

ArcSight≰ graylog

_

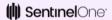
LOGIO

Secureworks

▼ FortiSIEM

EDRs

*∕*CROWDSTRIKE







Carbon Black.

OTHERS











«FIND



insightIDR









ABOUT OUR INTEGRATIONS

Our integrations empower SnapAttack users to transform any piece of threat intelligence into detection content that can be validated through adversary emulation and BAS and deployed into any SIEM, EDR or XDR. With 30+ direct integrations*, it doesn't matter where you've sourced your threat intel, if you bring your own, or if you use ours – it takes one click to deploy the SnapAttack detections into any environment, regardless of your SIEM, EDR or XDR.

*We continuously expand our integrations. If you don't see your product here, let's chat.

BENEFITS

Scale your defenses

SnapAttack's threat researchers amplify your security posture through our massive Detection Repo containing thousands of validated detections that we score for false positive and false negative performance. Be confident in your coverage by deploying SnapAttack's latest content to your existing tools.

Streamline Hunting

The clunkiest parts of threat hunting, the ones that keep you away from the hunt - research, writing, and validation - are streamlined through SnapAttack, making it easy for you to develop new content based on adversary emulations from our Attack Library

Consistency in Coverage

Our API integrations ensure you can manage your detection coverage across all of your tools, with at-a-glance measurability and reporting against the MITRE ATT&CK Matrix.



Simplify coverage across environments – regardless of tooling.

stay ahead of the threat

[<u>7</u>	Scale SecOps across your attack surface efficiently.	Our integrated view across disparate enterprise data sources offers context and the ability to consistently detect threats across the entire technology estate, regardless of tooling
	Accelerate your ability to respond to the latest threat intelligence	Our Detection Repo is continuously updated with the latest threat, enabling your blue team to immediately action on new intelligence and hunt priorities
	Improve resource effectiveness and detection outcomes	Our Attack Library, Detection Repo, Attack Range and Detection Builder reduce the need to scale headcount by making your existing teams and tools more effective, and integrated.
	Streamline and standardize your detection content across all of your tools	Give teams the ability to create, translate, deploy, validate detections across their stack without having to know a syntax for a myriad of security tools, enabling them to collaborate seamlessly.
Ø€.	Level up junior analysts while they're on the job.	Enable your teams to quickly understand any given attack technique by observing the adversary, their victim, and the true positive evidence left behind.
□0∆ <u>±</u>	Know you have your attack surface covered.	Visually quantify your MITRE ATT&CK coverage for a specific actor or threat to deployed detections and gain immediate perspective on your actual detection coverage mapped against ATT&CK.