SNAPATTACK

PLATFORM INTEGRATIONS

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

Translation Compatibility

SnapAttack can translate queries to the following platforms and languages. This means that, at a minimum, users can copy and paste functional queries over to the target SIEM/EDR.

Microsoft Azure | Carbon Black. | Chronicle | CROWDSTRIKE | DEVO

elasticsearch | humio | LimaCharlie | Microsoft Defender | OpenSearch

Radar | securonix | SentinelOne | splunk> | Trellix

Integration

Users can leverage SnapAttack to execute threat hunts, deploy detection rules, and launch queries across the following platforms through API integrations.

Microsoft Azure | Carbon Black. | Chronicle | CROWDSTRIKE

elasticsearch | humio | Microsoft Defender | OpenSearch

SentinelOne | splunk>