SNAPATTACK

MODERNIZE
THREAT
INTELLIGENCE

THREAT INTELLIGENCE
BEFORE AND AFTER SNAPATTACK:

BEFORE

✕ You're approaching threat intelligence like a box you have to tick.

✕ You struggle to determine which intelligence is relevant and important.

✕ You're limited to hunting IOCs like IP addresses, hashes and domain names.

✕ You're paying for multiple threat intelligence services, but they're really just IOC feeds - and you're still missing actual incidents.

✕ Your hand-off from intelligence to detection engineering is cumbersome, limited, and lacking the detail needed for real action.

AFTER

✓ **Behavioral threat intelligence** is a key piece of your detection strategy.

✓ Your **priority threats** are known and documented, and you know exactly how you'd stand up against them.

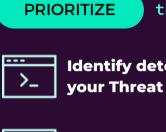✓ You can **quickly hunt for TTPs** (and IOCs) directly in your detection tools, without deep technical expertise.

✓ You can **report** upon and improve coverage against the threats that matter to **strategic stakeholders.**

✓ Threat intelligence hand-offs to **detection engineering** are seamless, efficient, and quick to action, creating a **united front** against the threats that matter.

SNAPATTACK

Threat intelligence built for detection engineers and threat hunters, custom-fit to your environment and your priorities.
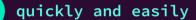
PRIORITIZE the threats that matter

Identify detection blindspots with your Threat Profile.

Speed up threat research with centralized Threat Dossiers.

MOBILIZE quickly and easily

Map your threat priorities to the MITRE ATT&CK Matrix.

Action TTPs and IOCs across your detection stack.

MATURE your threat intelligence program

Accelerate your next steps.

Easily report to internal stakeholders.

65x
faster threat research

93%
reduction in mean-time-to-detect

75%
reduction in false positives and negatives

Uncover how SnapAttack can help you modernize your threat intelligence program: