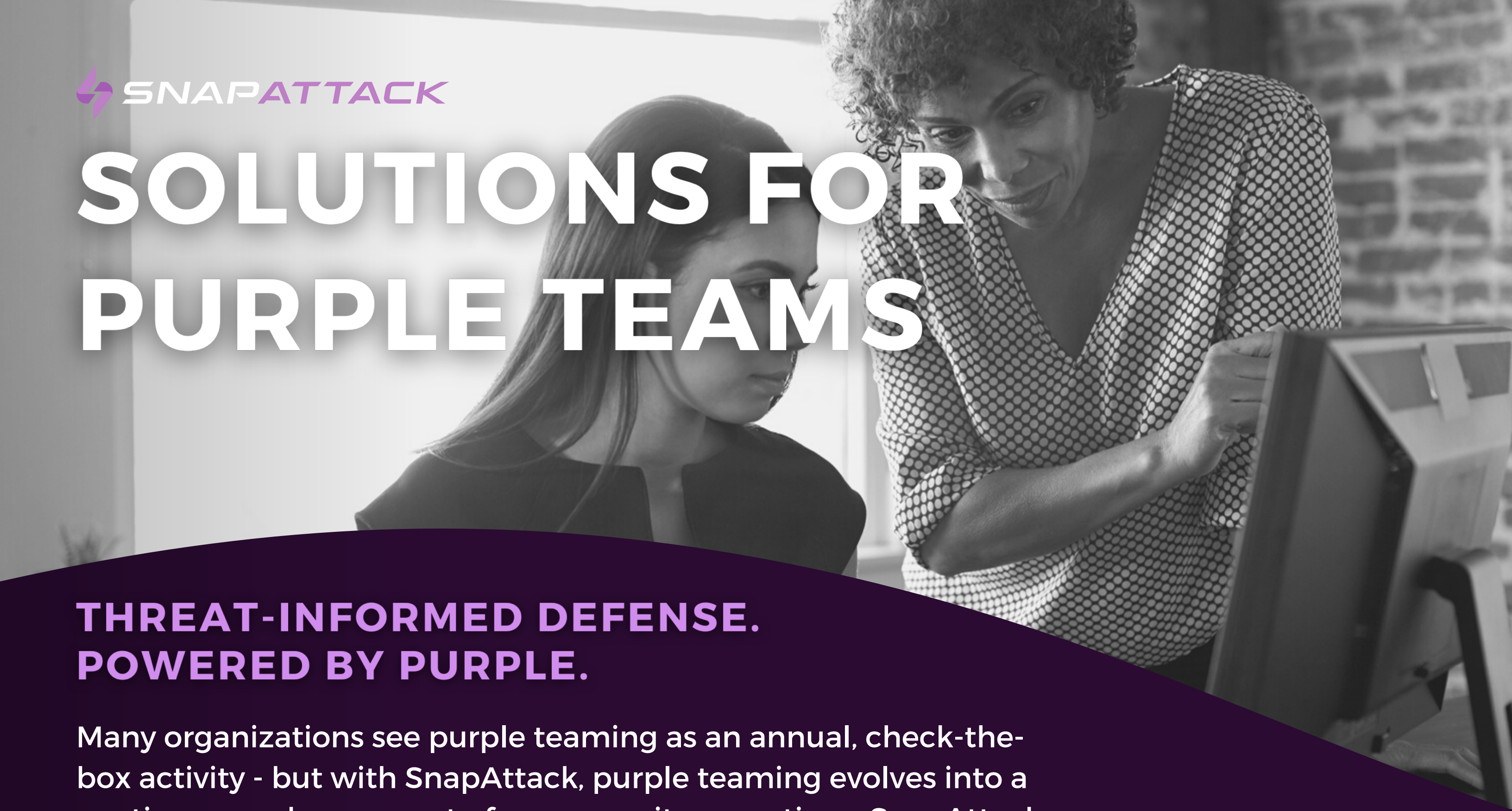

SNAPATTACK

SOLUTIONS FOR PURPLE TEAMS

THREAT-INFORMED DEFENSE. POWERED BY PURPLE.

Many organizations see purple teaming as an annual, check-the-box activity - but with SnapAttack, purple teaming evolves into a continuous enhancement of your security operations. SnapAttack is the world's first purple teaming platform and offers a single source of truth for offensive and defensive activities, enabling you to get more from your tools and more from your teams.

Red and blue teams turn to SnapAttack when...

The blue team lacks **visibility** into the red team's processes, and the red team lacks the **time** to **share relevant information**.

They're driven apart by a **siloed dynamic** and **competing goals**.

They're **unable to effectively collaborate** because they're **buried** in work and **underresourced**.

Purple teaming is conducted to **check a box**, not to provide **continuous insight** into the threat landscape.

reduced time-to-detect

5-10 minutes

before snapattack: 1-2 weeks
after snapattack: 5-10 minutes

confidence that scales

<5% false positive

rate for highest quality detections

visualize coverage

MITRE ATT&CK

measure visibility against the mitre att&ck matrix

Operationalize purple teaming in a collaborative environment to drive security operations forward.

Get ahead of incoming and emerging threats.

ATTACK CAPTURE LAB

Research threats in our portable sandbox, then spin up local attacks in the Attack Capture Lab to understand relevant forensic artifacts.

NO-CODE DETECTION BUILDER

Quickly build quality detections with built-in logic and error checking and a simple, point-and-click interface – with or without any coding knowledge.

Centralize operations, improve collaboration.

ATTACK LIBRARY

Visualize an attack from start-to-finish in real-time with all the telemetry you need at your fingertips.

DETECTION REPO

Browse our library of thousands of validated TTP-oriented detections validated to work against the latest attacks, with one-click deployment in your existing SIEM or EDR.

Align goals between red and blue teams.

CONFIDENCE SCORING

Leverage our data-science driven detection confidence scoring to hunt with the precision and speed you need.

MITRE ATT&CK

Know exactly where you stand by mapping your coverage and environment against the MITRE ATT&CK matrix.

Remove barriers to continuous testing.

VALIDATE YOUR WORK

Automate the validation of new detection logic, and leverage our data science-driven approach to score your detections for confidence and false positive performance in advance.

30+ INTEGRATIONS

Pivot from tool-to-tool with 30+ direct integrations that empower both teams to streamline communications and collaboration.