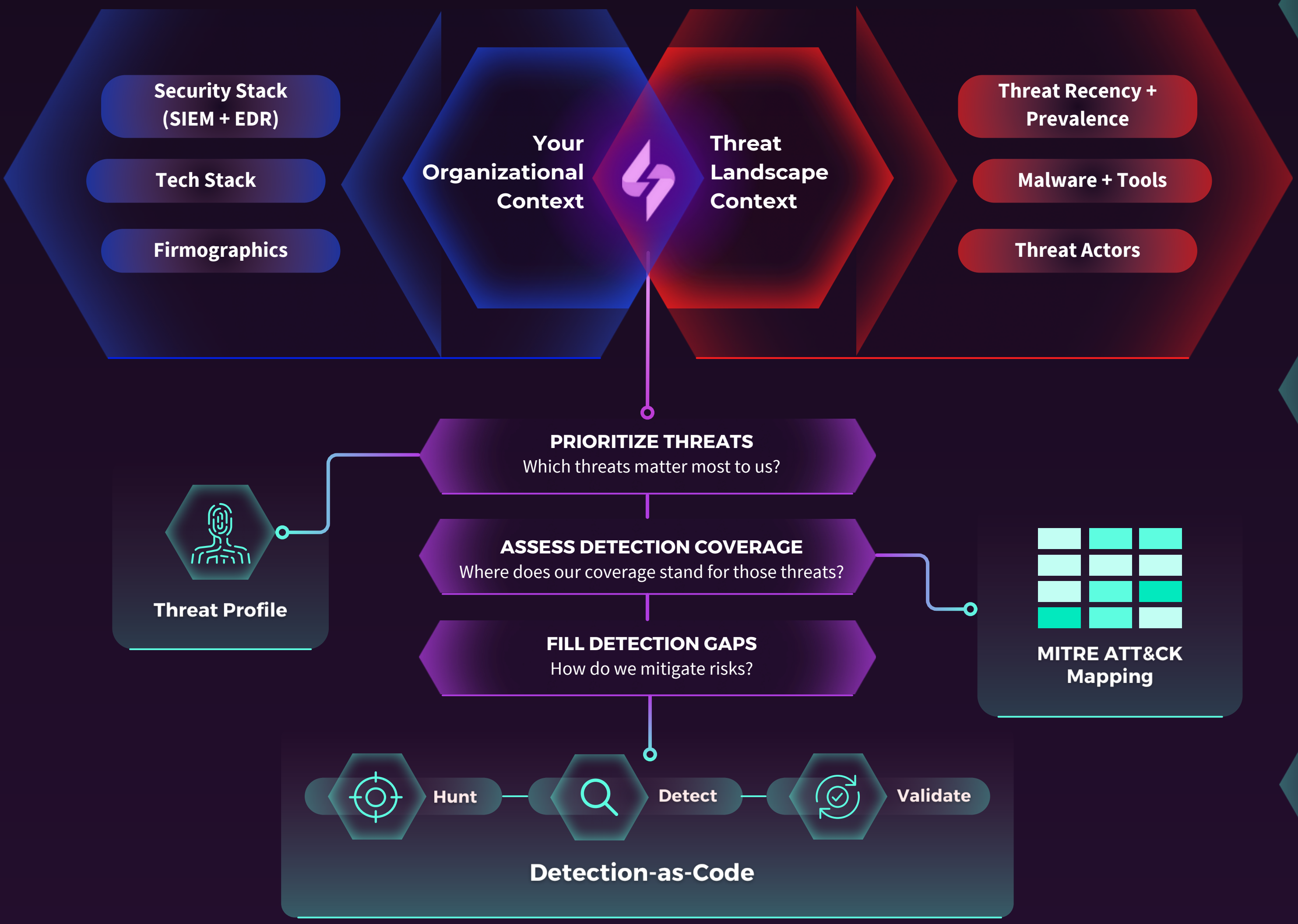
SNAPATTACK The Threat Hunting and Detection-as-Code Platform

Detect the threats that matter, **faster**, in Chronicle.

SnapAttack is an **intelligence-driven threat detection platform** that provides threat-specific detection rules and hunting searches, recommended based off of an organization's unique threat profile, for teams to quickly and easily implement in Chronicle.



Security Stack (SIEM + EDR)

Tech Stack

Firmographics

Your Organizational Context

Threat Landscape Context

Threat Recency + Prevalence

Malware + Tools

Threat Actors

Threat Profile

PRIORITIZE THREATS
Which threats matter most to us?

ASSESS DETECTION COVERAGE
Where does our coverage stand for those threats?

FILL DETECTION GAPS
How do we mitigate risks?

MITRE ATT&CK Mapping

Hunt — Detect — Validate

Detection-as-Code

Backed by industry-leading Mandiant threat intelligence

4k+ **Thousands of high-quality pre-built detections**

86% **86% MITRE ATT&CK coverage for Chronicle**

SNAPATTACK

Translate intelligence into meaningful threat detection outcomes with an end-to-end workflow.

Uncover and prioritize the threats that matter most.

Align detection coverage with threat priorities.

Address detection gaps with ease and precision.

1. What are the threats, and which threats matter?

SnapAttack uses key information like your industry, tech stack and region to automatically build a **Threat Profile** and help you understand which Threat Actors, Malware, Tools, and Techniques actually matter using industry-leading threat intelligence.

2. What is our detection coverage? How do those gaps relate to the threats that matter?

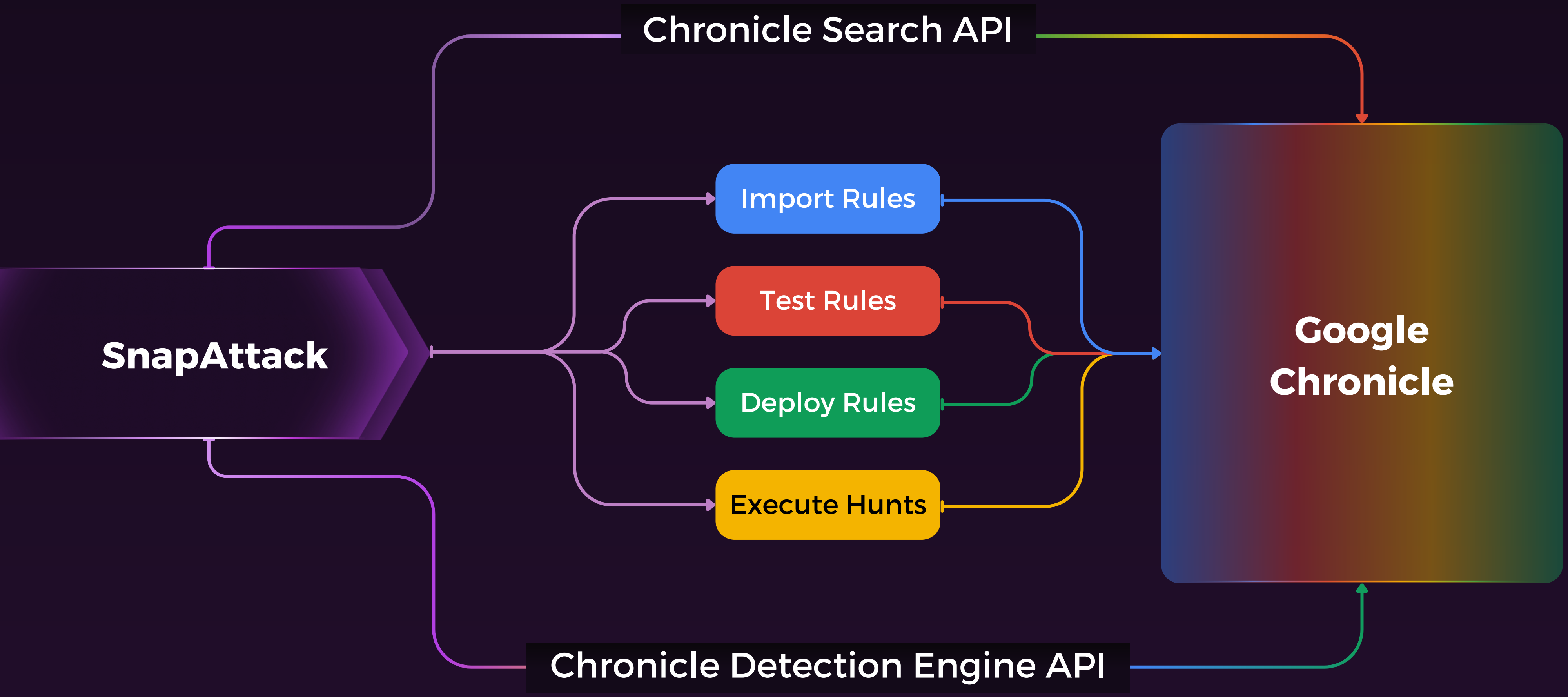
Pull in your existing YARA-L rules and leverage **MITRE ATT&CK™** to visualize coverage against prioritized threats and drive strategic growth by focusing on commonly used Techniques & Sub-Techniques, leveraged by Threat Actors that actually target you.

3. How do we fill our detection gaps?

The **Detection Library** provides over 4,500 YARA-L Rules and 3,000+ UDM Searches that are continuously validated against real threats in SnapAttack, automatically tested in your environment, and can be easily deployed in Chronicle.

SNAPATTACK

Integrate directly into Chronicle and start improving detection coverage in a matter of minutes*.



* Users must first obtain the correct API credentials and permission from their Chronicle representative.

SNAPATTACK

Make the most of your Chronicle investment with SnapAttack.

TRY OUT OUR COMPLIMENTARY POV >

www.snapattack.com