Solution Brief

Attack Detective:
Next-Gen Automated Threat Hunting

Attack Detective: Overview

With Attack Detective, you have the complete attack surface visibility in real time by querying data exactly where it lives. By connecting to the API of your SIEM or EDR, Attack Detective runs detection content from SOC Prime's platform against the entire pool of data available in the cyber defense system and presents the outcomes to provide cybersecurity professionals with a holistic view of the organization's cybersecurity posture. With Attack Detective, teams are equipped with better tooling to perform daily security operations more precisely and efficiently and 100x times faster than before to focus on what matters most.

Highlights

- **Amplify Security Operations**
  - Stay ahead of emerging threats with a dataset of 10K+ Sigma rules against any TTPs
  - Reduce manual effort on auditing all your data across the entire infrastructure from weeks or months to just a few hours
- **Gain Complete Data Visibility**
  - Identify data source gaps to prioritize areas to primarily focus on
  - Gain extended visibility into ATT&CK coverage based on organization-specific log sources
- **Advance Attack Surface Visibility**
  - Scan data across all security assets, services, tenants, and hosts
  - Gain a holistic view of your environment
- **Refine detection content prioritization**
  - Automate content selection and customization matching the organization's current needs and threat profiles
  - Check the scan results by running instant hunts directly in the selected SIEM or EDR environment

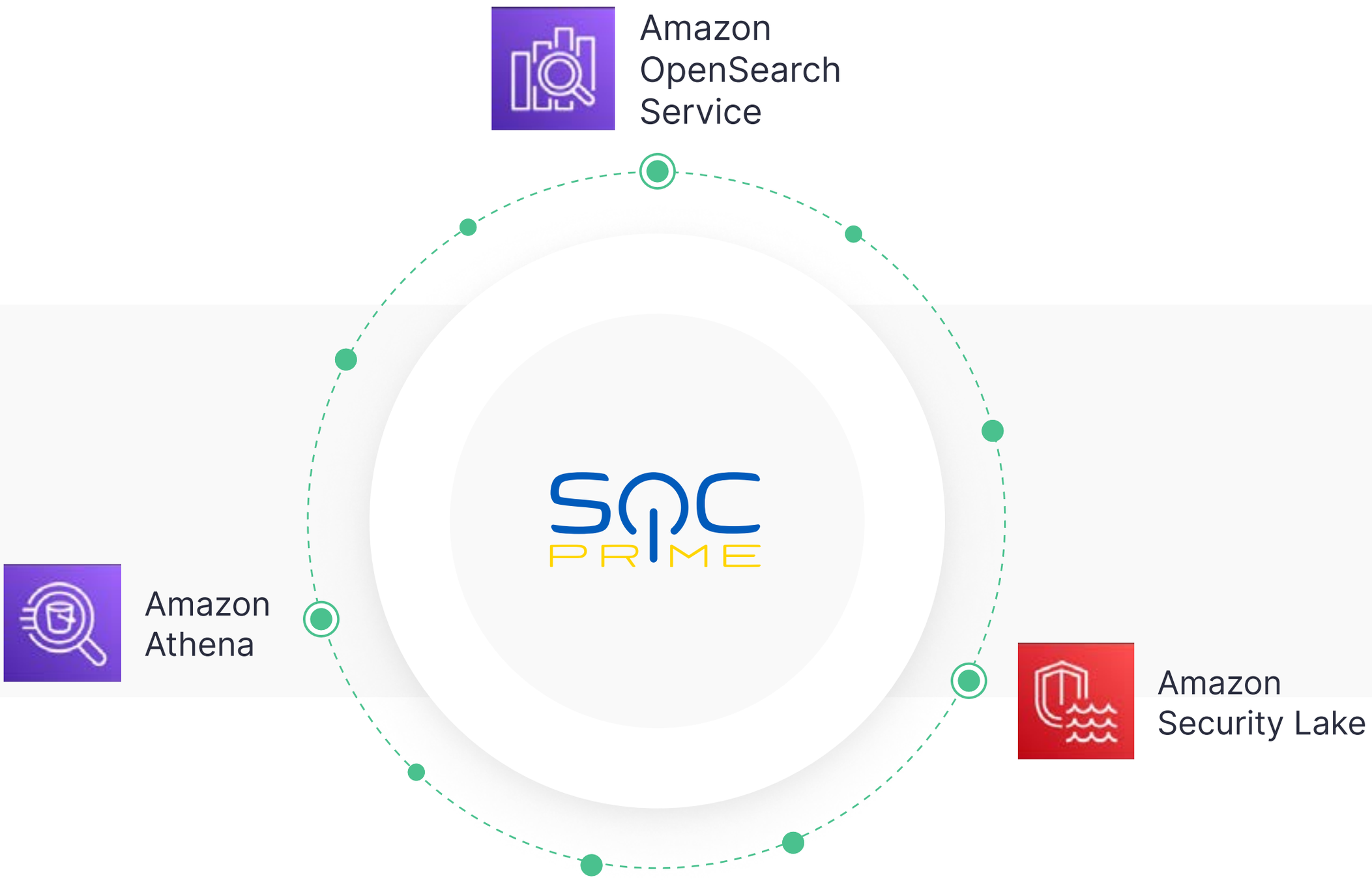
Zero-Trust

Attack Detective provides an enterprise ZTA (Zero Trust Architecture) with the ability to avoid risks of vendor lock-in. Gain comprehensive data visibility based on all your organization-specific logs while keeping all your data where it lives. We do not ask for any of your potentially sensitive data back.

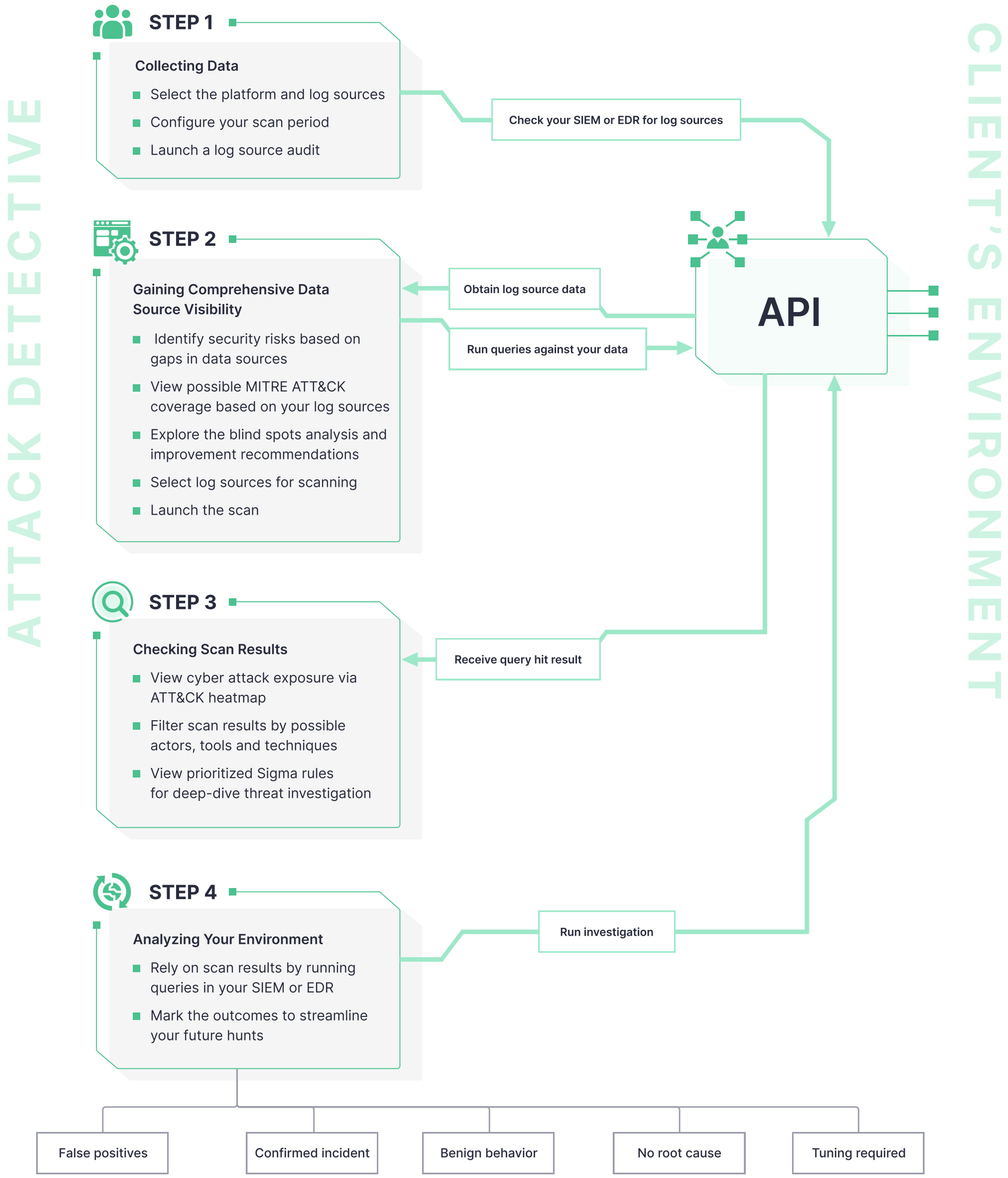
Attack Detective fully supports control plane and data plane segregation. Different accounts are used for the Attack Detective policy configuration and for data storage access in different tenants. No data transfer between control plane and data plane.

Multi-Cloud

Attack Detective connects multiple technologies in a single place to enable real-time attack surface visibility across the organization-specific cloud environments and streamline threat investigation.



Attack Detective Workflow



Capabilities

1 Gain a Comprehensive Visibility into Your Data

- Track your overall detection coverage based on organization-specific log sources as benchmarked against ATT&CK
- Identify log source gaps and blind spots in your detection coverage along with recommendations how to fill these gaps

2 Launch the Scan Customized to Your Security Needs

- Set the scan to your security needs by selecting the platform and log source
- Run the scan to match your data with Detection-as-Code content from SOC Prime's platform

3 Gain a Snapshot of Your Attack Coverage in Real Time

- Explore the outcomes consolidated into detected ATT&CK techniques along with the impacted assets, services, and accounts
- Analyze potential threat actors and adversary tools in use

4 Delve into the Scan Details Mapped to ATT&CK

- Instantly visualize a heatmap over a selected time period with triggered ATT&CK tactics and techniques
- Check if the visualized data can be attributed to a relevant attack

5 Deep Dive into Threat Context Without Alert Generation

- Go through the list of relevant Sigma rules with stats of behavior hits along with affected accounts and assets
- Rely on the Global Action Loop by leveraging feedback from your peers on the rule outcomes

6 Drill Down into Your SIEM or EDR for In-Depth Investigation

- Run prioritized queries in your SIEM or EDR to validate the risks
- Mark the triggered rule according to the displayed behavior to prioritize your detection procedures

Explore SOC Prime to defend against attacks easier, faster, and more efficiently than ever before.

LEARN MORE