Solution Brief

Risk-Optimize Your Cybersecurity Posture with SOC Prime and Amazon Security Lake

Driving zero-trust & multi-cloud transformation to boost SOC efficiency and optimize security investments

Pain Points

- **Lack of visibility & high data storage costs.** With large amounts of data coming from multiple organizations' assets and growing exponentially, security teams are constantly challenged with gaining complete visibility into their data and affording the high costs of its storage.
- **Vendor lock-in risks.** Organizations maintaining a complex multi-tenant environment need advanced solutions allowing them to achieve more flexibility and ensure risk control through the existing diverse technology stack.
- **Costly and resource-intensive migration.** Organizations relying on complex infrastructure face the challenges of timely log source & detection content migration that results in a long time to value for a new deployment and exposes assets to multiple security risks.
- **Data security and compliance risks.** With cloud migration being the top digital transformation priority, organizations are looking for ways to mitigate related security hurdles and risk-optimize the cybersecurity posture by applying more robust compliance with privacy regulations and securing mission-critical data.

Our Solution

SOC Prime drives a transformational change in cybersecurity, relying on a zero-trust & multi-cloud approach to empower security teams with smart data orchestration, dynamic attack surface visibility, and cost-efficient threat hunting. Backed by its advanced cybersecurity solutions, Uncoder AI, Attack Detective, and The Prime Hunt, SOC Prime enables organizations to boost their cyber defense capabilities at scale, unleashing the power of Amazon Security Lake.

UNCODER AI: Unleashing the Power of AI for Advanced Detection Engineering

Leveraging Uncoder AI, an Augmented Intelligence framework that fuses cyber threat intelligence, indicators of attacks, 10,000+ Sigma rules mapped to MITRE ATT&CK® and backed by collective cybersecurity expertise and generative AI engines, customers can be timely notified of emerging threats, proactively develop and update detection algorithms, and gain aggregated context on any cyber attack.

With Uncoder AI, security teams can save development time and migration costs by re-using threat hunting queries & rules and automatically translating them to Amazon Athena and Amazon OpenSearch in the OSCF format.

ATTACK DETECTIVE: Enabling Smart Data Orchestration and Automated Threat Hunting

SOC Prime's Attack Detective tool intelligently and automatically queries security logs in the customer's Amazon Security Lake account via Amazon Athena and Amazon OpenSearch to identify data sources and then scan them in real time based on over 10,000 Sigma rules.

The Benefits of Using SOC Prime's Attack Detective with Amazon Security Lake

- **Run an alertless SOC**
  — Act smarter by focusing on what matters most
  — Investigate incidents rather than overwhelming volumes of alerts
- **Enable smart data orchestration**
  — Identify missing data and reduce blind spots in your cyber defense
  — Continuously improve visibility into the latest threats, CVEs, and behaviors
- **Accelerate hunting efficiency**
  — Automatically partition Amazon Security Lake to boost resource efficiency
  — Reduce costs on hunts and IOC matching
- **Improve data observability**
  — Link and correlate with EDR and on-prem SIEM data to gain a holistic view of your environment
  — Automatically calculate cost savings without moving data to the cloud

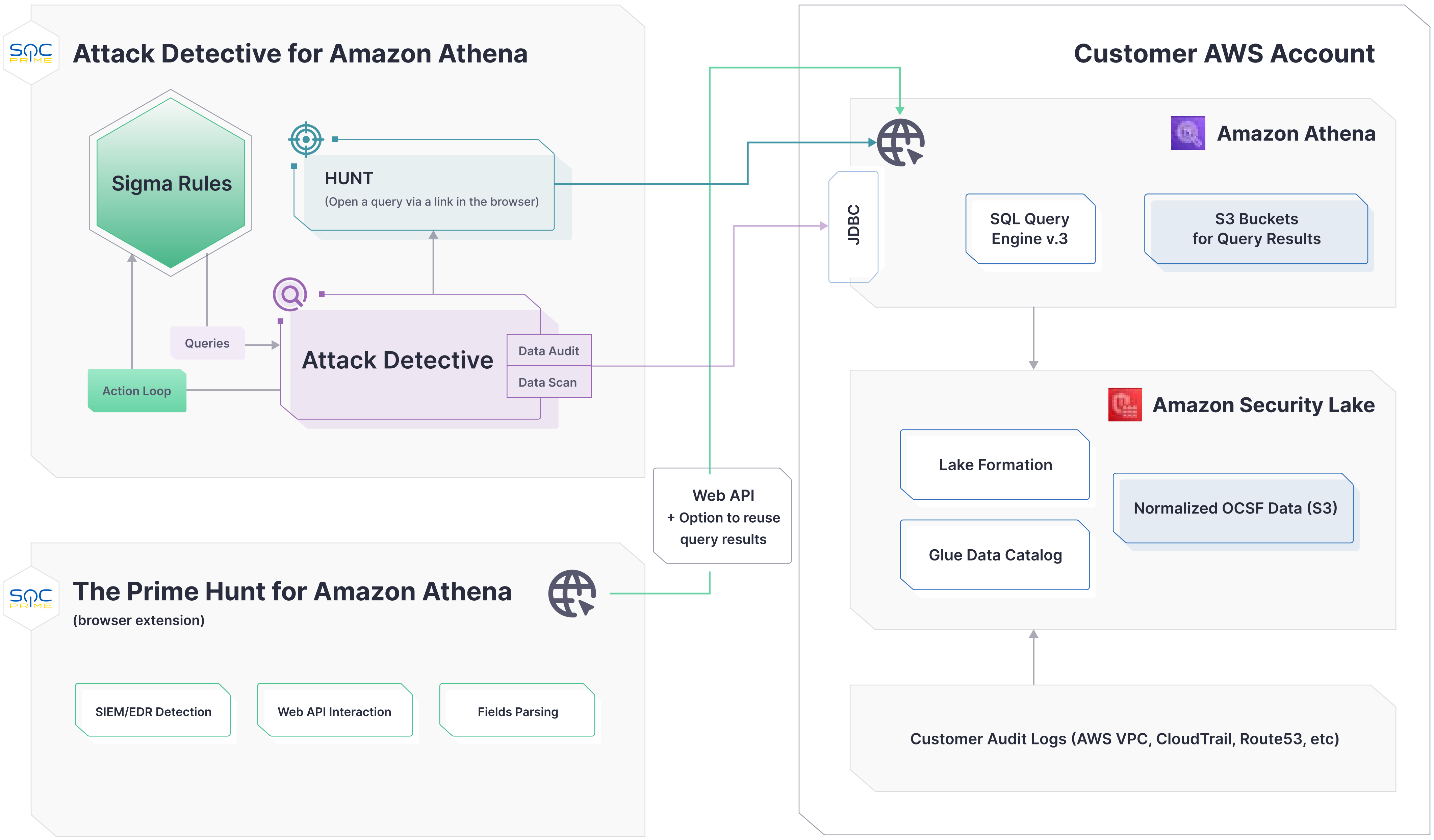
THE PRIME HUNT: One UI for Platform-Agnostic Threat Hunting

The Prime Hunt open-source browser add-on enables security professionals to extract valuable data from large datasets at a lower cost. Users can seamlessly run threat hunting queries on security logs within the Amazon Security Lake account via a web browser in both Athena and OpenSearch and automatically identify accounts and assets affected by the suspected activity.

SOC Prime’s Integration with Amazon Security Lake

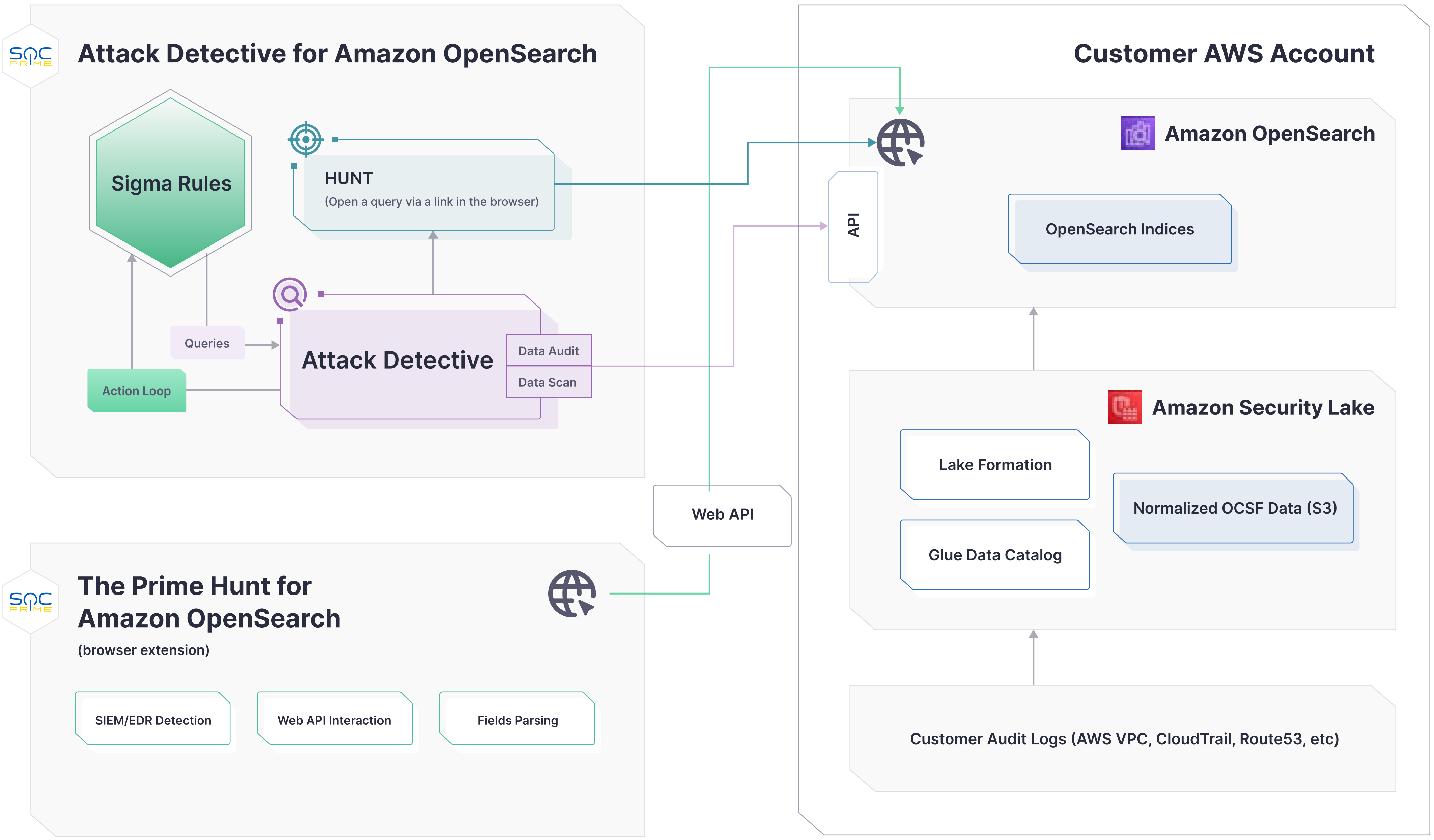
SOC Prime integrates with Amazon Security Lake leveraging the query access to the security data lake via Amazon Athena and Amazon OpenSearch services.

Attack Detective queries security logs in the customer's Amazon Security Lake account via JDBC (in Athena integration) and via API (in OpenSearch integration) to identify data sources and then scan them with a curated set of threat hunting queries.



Amazon Security Lake integration with SOC Prime’s Attack Detective and The Prime Hunt solutions via Amazon Athena

The Prime Hunt integrates with Amazon Security Lake via both Amazon Athena and OpenSearch, depending on the user environment, using the web API. Security engineers can run queries on security logs in the customer's Amazon Security Lake account directly from their browser in either Athena or OpenSearch environments and automatically identify accounts and assets affected by the suspected activity.



Amazon Security Lake integration with SOC Prime's Attack Detective and The Prime Hunt solutions via Amazon OpenSearch Service

Explore how SOC Prime can empower your organization with a zero-trust & multi-cloud cybersecurity approach backed by collective industry expertise to always stay ahead of the curve.

LEARN MORE ↗