OBSIDIAN

Community Software Development Kit (SDK)

Solution brief

SDK 2.0

Foundational SaaS coverage through broad app connectors is essential for delivering turn-key SaaS security, giving organizations the visibility needed to enforce policies, detect anomalies, and respond quickly. With this foundation, security teams gain a clear map of access across their environment: knowing which users and service accounts exist, who created and operate them, and what their permissions allow. This context helps anticipate AI agent interactions, reduce over-permissioned risk, and contain the blast radius of agentic AI breaches.

To further advance this foundation, Obsidian's enhanced SDK 2.0 significantly expands integration depth by ingesting richer posture data beyond accounts, including tickets, assets, and other SaaS entities. Restore control over SaaS by closing the gap between detection and resolution using action policies built on richer posture rules.

Use Case: Complete Custom Configuration Protection

> **Challenge**
>
> Some apps have critical settings (e.g., unverified domains) not covered by Obsidian's default schemas, leaving gaps in security and compliance.

> **Solution**
>
> Security teams can build or extend custom schemas in Python or YAML, then upload them to enforce tailored posture rules. This centralizes monitoring, ensures compliance, and provides complete visibility into critical configurations while extending Obsidian's coverage.

Feature Benefits

Tailored Security and Compliance:

Create custom security policies to cover every part of your SaaS environment and meet all compliance requirements.

Easy, Guided Deployment:

Accelerate your time to value with guided onboarding and new Command-Line Interface (CLI) tools for fast, automated management, eliminating the need to write custom scripts or depend on developer assistance.

The Obsidian SDK

The SDK integrates niche, custom, and third-party applications into the Obsidian platform, giving security teams granular control over their SaaS environment. Its key advantage is the ability to capture custom posture data, delivering deep visibility into unique configurations and user activity that standard integrations often miss. By extracting telemetry directly from these apps, teams can build unlimited schemas and uncover risks, thereby extending coverage to non-native apps and accelerating incident response.

Unified SaaS Posture Monitoring

Continuously track authentication, access, and configuration changes with real-time data. Generate custom reports to track security improvements.

Reduce False Positives

Create app-aware detection rules and prioritize alerts to reduce noise and speed up your response.

Endpoint Data Flow Monitoring

Track the status of data sent to storage endpoints, including the number of records sent and any errors.

Standardized Data

The SDK normalizes third-party app data into a standard, human-readable format for easy analysis with other security tools.

Expanded CLI Tools

These tools empower teams with flexible customization, allowing you to build a security posture tailored to your needs.

Posture Rules Import/Export CLI

Create custom rules based on posture data, with the ability to easily move them between platforms.

Schema Upload CLI

Upload custom data schemas to capture any SaaS configuration and use it within Obsidian.

Activity Data Upload CLI

Bulk upload and standardize activity events to power searches and security policies.

Custom Posture Data Upload

Define and upload customizable posture data schemas and rules in Python or YAML to match your unique platform requirements.

High-Volume Performance

Process up to 10 MB compressed data from a single service, ensuring high-volume data ingestion without compromising performance.

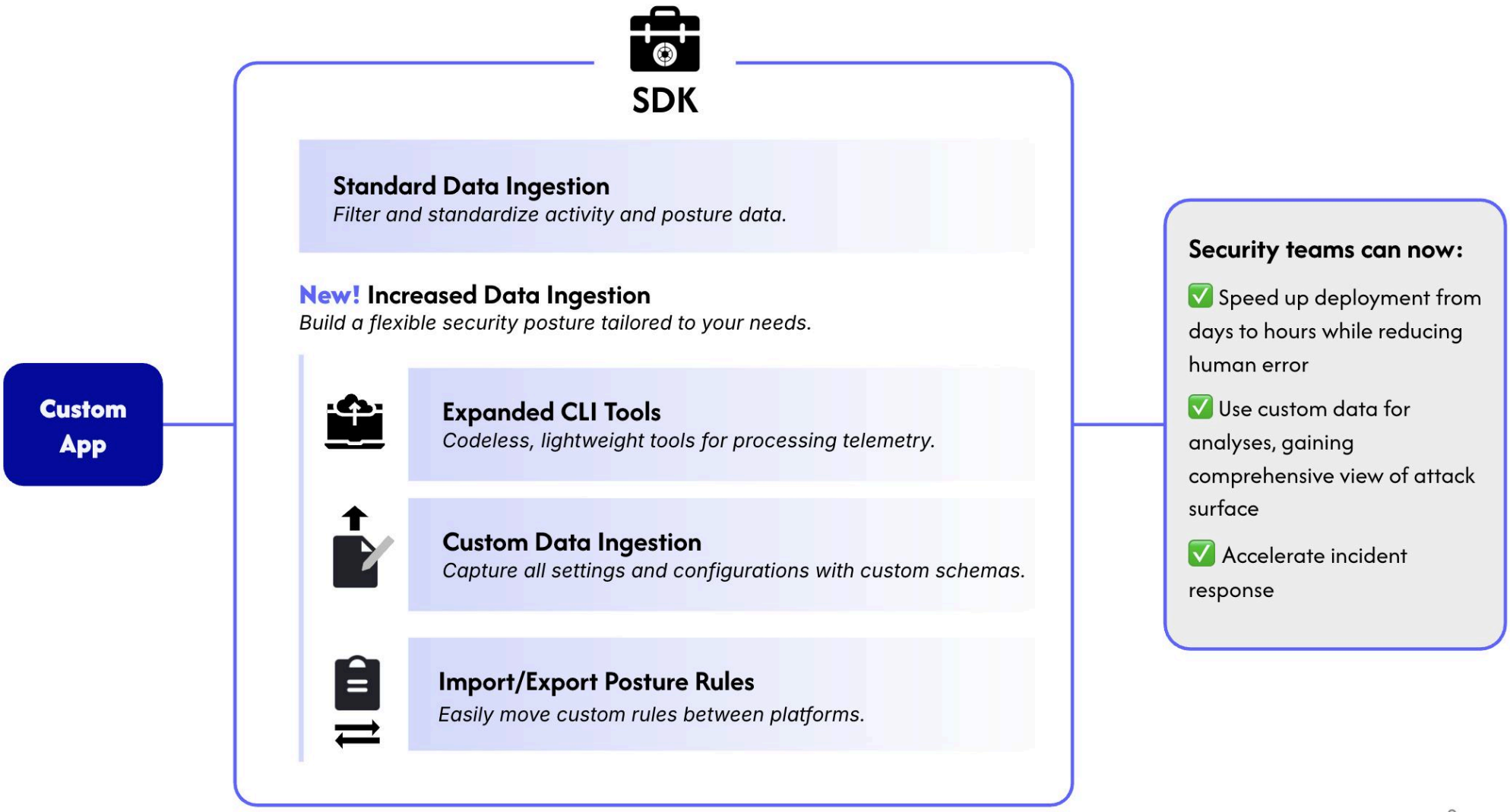

Fig. 1: The new SDK streamlines the integration of custom applications, empowering the SOC to build unlimited schemas, create app-aware detection rules, and accelerate incident response.