Stairwell

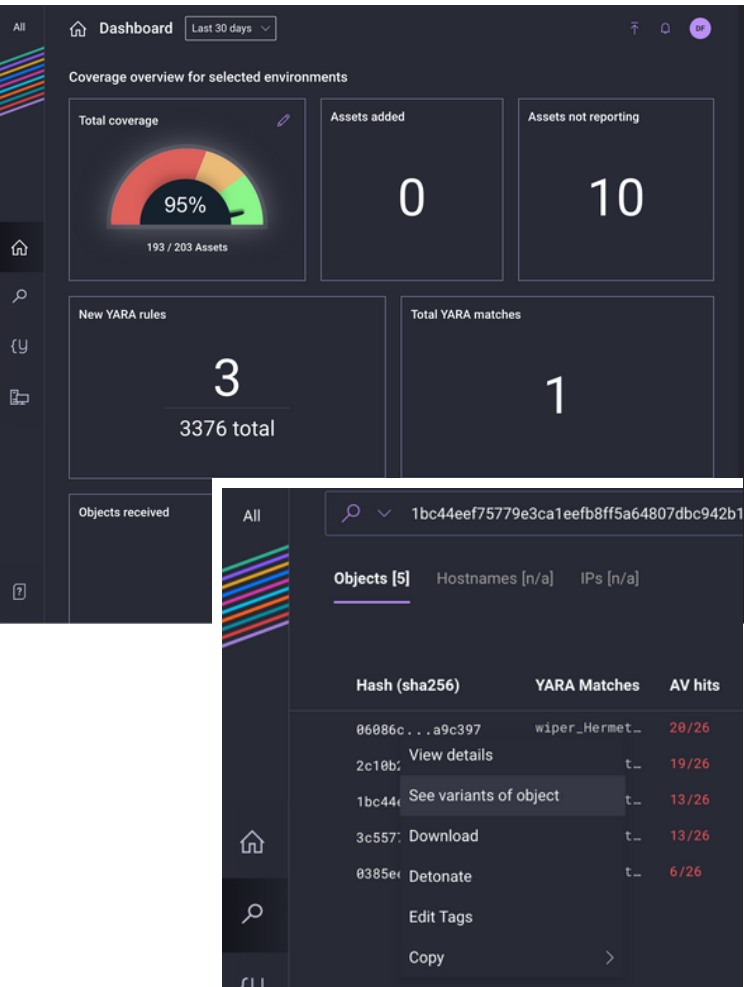
Outsmart any attacker

# Inception platform

Data sheet

Stairwell Inception™ is a SaaS platform that uplevels the capabilities of your security team and automatically detects malicious and suspicious activity that your existing cybersecurity solutions miss. These blind spots include emerging threats, malicious activity that passes through traditional "point-in-time" threat detection defenses, malware variants, and siloed information sources.

Inception increases your ability to protect your organization from the gaps exploited by advanced attacks by automating continuous intelligence, detection, and response in a collaborative workflow.




## Key benefits of Inception

Unique in the marketplace, Inception continuously captures, stores, and analyzes all the executable files in your environment. Its virtual storage locker preserves primary security artifacts for ongoing analysis as new threat intelligence becomes available. In this way, Inception creates tailored, constantly adapting threat defenses for your organization across all time horizons that are imperceptible to even the most sophisticated attackers.

**Improves the performance of your team and your tools**
Inception breaks your team out of unproductive and redundant silos and uplevels the capabilities of all your security team members. Even entry-level team members extract meaningful results from Inception's rich set of automated investigation tools. For example, with the click of a button, a SOC analyst can perform automated variant discovery, identifying malware variants in seconds with a fidelity that would take hours or days for an experienced threat researcher to do.

The intuitive Inception platform is highly responsive from the UI to the integrations with other tools in your tech stack, including SIEM, SOAR, and endpoint tools. The information flow and data enrichment capabilities reduce redundancies and foster collaboration between security subgroups.

**Detects compromise across all time horizons**
Inception treats all files as suspicious and pre-preserves the executables as evidence to uncover previously unknown compromises in your environment. By continuously evaluating your corpus of file data in light of emerging insights, it unlocks time. When new malware is identified, you can efficiently search for it — and variants of it — to determine whether your organization is impacted now or was in the past. That's because Inception is examining the primary security artifacts for meaningful results, not abstracted log data.

**Produces contextual and undetectable threat intel**
With our inside-out approach, Inception uncovers what's most important to your organization and delivers tailored defenses and intelligence that attackers can't test against or reverse engineer. Inception starts with what's unique to your environment and contextualizes it at scale so your security team can easily understand and act on novel discoveries such as malware variants and low-prevalence artifacts that indicate nefarious activity.

Inception allows your threat intelligence, incident response, and SOC teams to collaborate and iterate on unique defenses.

## 1. Collects

Collects primary security artifacts in your environment for continuous investigation.

Safely collects, preserves, and keeps files active for continuous analysis:

- Ingests file executables and stores them for retrospective analysis
- Pulls files from wherever they are
- Stores your malware samples or enables feeds of malware
- Continuously scans all stored files

## 2. Analyzes

Automatically analyzes all collected evidence — past and present — to create tailored intelligence and enrich it with external information as it arises:

- Evaluates every file continuously
- Identifies malware variants in minutes
- Scans with 32+ AV engines and returns verdicts
- Notifies you about new info for IOC queries
- Performs pattern-matching for files and feeds
- Helps you manage thousands of YARA rules: pre-loaded, feeds, custom, new
- Provides syntax guidance for your YARA rules

## 3. Investigates

Uses the holistic, pre-preserved view of your environment to separate the signal from the noise, understand relationships between the malicious and the suspicious, identify previous compromises, and prevent future threats.

- Hunts for signal across your centrally stored files with our powerful query language
- Re-investigates IOCs as new information comes in to eliminate false negatives
- Delivers research-grade insights with variants, anomalies, unique relationships, and low-prevalence files
- Detonates files to generate more signal

## 4. Connects

Integrates easily with your security workflow with pre-built integrations or the Inception API for custom integrations. You can:

- Plug directly into your existing security infrastructure: SIEM, SOAR, and endpoint tools
- Discover variants and enrich threat intelligence data between applications, such as enriched IOC data in your SOAR to identify false negatives
- Get notified about Inception alerts in your ticketing system, inbox, or chat
- Log Inception events and alerts to your SIEM of choice

Stairwell

Inception Platform

# Use Cases

## Detect missed threats and streamline your workflow

Organizations and security teams in all industries find value in the Inception platform. Here are some key use cases.

### Detect hidden threats with visibility into malicious activity that traditional defenses miss

The Inception platform enables you to efficiently identify suspicious artifacts and malware that have evaded your detection and prevention security controls. Inception continuously analyzes your environment against the latest threat intelligence from multiple sources and uncovers threats that would otherwise remain undetected. When you identify malware-led attacks and response time is critical, the Inception platform improves the efficiency and effectiveness of your team by quickly identifying related malware variants that exist in your environment. Inception helps you streamline your triage, investigation, and remediation process, and create tailored defenses that attackers cannot test against.

### Create customized defenses with contextual threat intel, from external and your own

Inception prioritizes threats inside your environment, while continuously analyzing your files against the latest threat intelligence from multiple sources. This provides you with a tailored defense system based on the unification of external and internal threat intel. The Inception platform extracts IoCs and observables from suspicious files — and variants of those files — in your environment. This keeps the volume low while providing important context to your analysts about where each IoC came from and how your team can best defend your organization against it. These low-volume targeted IoCs can be used to block adversary access via integration with your protection tools (Firewalls, EDR, etc.) or used for enrichment of your detection and response information.

### Make the attack-of-the-day a non-event for your business

When a new form of ransomware or nation-state attack hits the news, your team doesn't have to wait for threat intel feeds to be updated or your security vendors to roll out updates. Your team can simply copy the new threat report or the blog page into the Inception UI. Inception will extract any IoCs from this text and run a search of these IoCs (IP, Domain, YARA, Hashes) against your entire file corpus (past and present) to identify any matches. When matches are found, that's a confirmation of the presence of the threat in your environment. Once Inception identifies the IoC, you can use your normal incident response process to remedy it. Inception also expedites your deep-dive analysis of malware, including efficient identification of any variants so you can root the adversary out of your environment.

### Triage every alert with research-grade understanding

Inception provides your team with a one-stop-shop for static and dynamic analysis of potential malware, including variants, and presents all of the information in an easy-to-use interface. Once your files are loaded into Inception via the lightweight file forwarder, they are continuously evaluated against the latest threat intelligence that includes the Inception platform's shared corpus of hundreds of millions of malware samples. When Inception identifies malware in your environment, your SOC analysts can discover variants of it with the click of a button. You can also use the Inception platform to analyze files from systems that you believe were infected on an ad hoc basis. Inception also provides file enrichment APIs, including an Inception Variants API, that can pull information directly into your SIEM and/or SOAR.

Contact us to learn more about how the Inception platform can help your security team outsmart any attacker.

## About Stairwell

Stairwell helps organizations take back the cybersecurity high ground with solutions that attackers can't evade. Its flagship product, the Inception platform, enables security teams to outsmart any attacker. Visit stairwell.com and connect with us on Twitter, LinkedIn, and Facebook.


Data Sheet - Rev. 092122

Stairwell