Stairwell

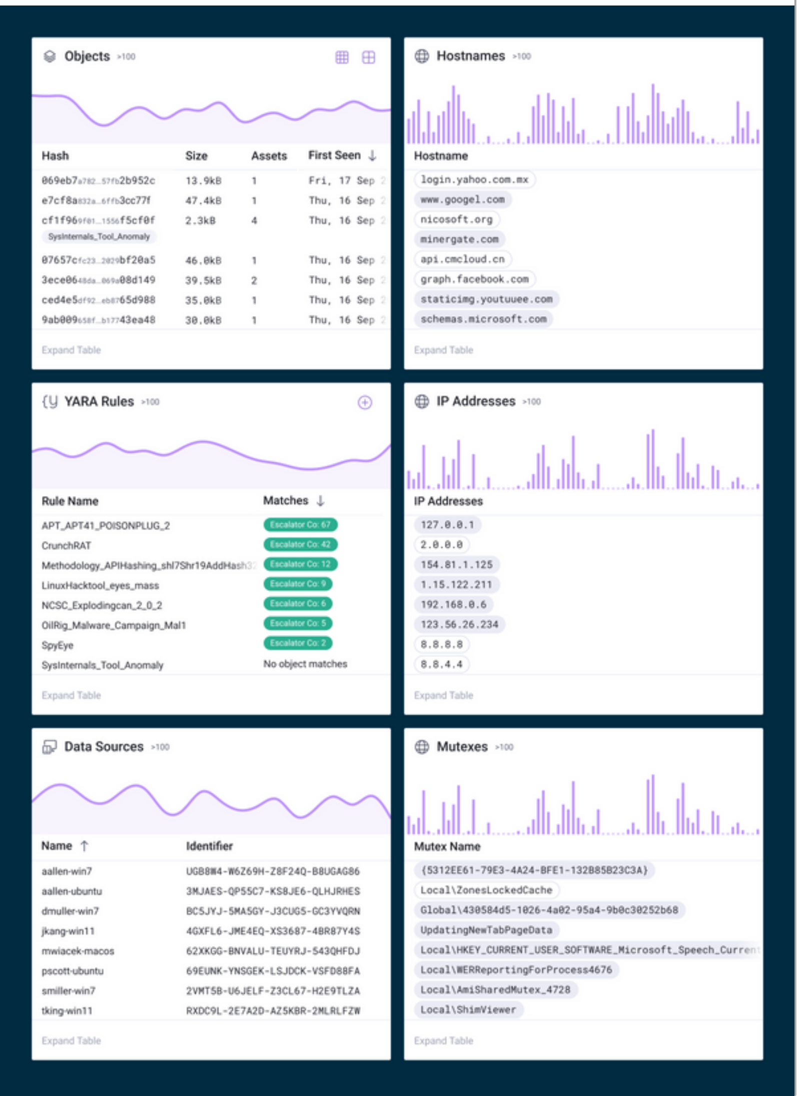
Outsmart any attacker

Inception platform

Data sheet

The Inception™ platform creates tailored, constantly adapting threat defenses for your organization that are imperceptible to even the most sophisticated attackers.

We start with what's unique to your environment and contextualize it at scale so security teams can easily understand and act on novel discoveries.



Objects >100

Hash	Size	Assets	First Seen ↓
069eb7a782…57fb2b952c	13.9kB	1	Fri, 17 Sep 2
e7cf8a832a…6ffb3cc77f	47.4kB	1	Thu, 16 Sep 2
cf1f969f01…1556f5cf0f SysInternals_Tool_Anomaly	2.3kB	4	Thu, 16 Sep 2
07657cfc23…2029bf20a5	46.0kB	1	Thu, 16 Sep 2
3ece0648da…069a08d149	39.5kB	2	Thu, 16 Sep 2
ced4e5df92…eb8765d988	35.0kB	1	Thu, 16 Sep 2
9ab009658f…b17743ea48	30.0kB	1	Thu, 16 Sep 2

Hostnames >100

Hostname
login.yahoo.com.mx
www.googel.com
nicosoft.org
minergate.com
api.cmcloud.cn
graph.facebook.com
staticimg.youtuuee.com
schemas.microsoft.com

YARA Rules >100

Rule Name	Matches ↓
APT_APT41_POISONPLUG_2	Escalator Co: 67
CrunchRAT	Escalator Co: 42
Methodology_APIHashing_shl7Shr19AddHash32	Escalator Co: 12
LinuxHacktool_eyes_mass	Escalator Co: 9
NCSC_Explodingcan_2_0_2	Escalator Co: 6
OilRig_Malware_Campaign_Mal1	Escalator Co: 5
SpyEye	Escalator Co: 2
SysInternals_Tool_Anomaly	No object matches

IP Addresses >100

IP Addresses
127.0.0.1
2.0.0.0
154.81.1.125
1.15.122.211
192.168.0.6
123.56.26.234
8.8.8.8
8.8.4.4

Data Sources >100

Name ↑	Identifier
aallen-win7	UGB8W4-W6Z69H-Z8F24Q-B8UGAG86
aallen-ubuntu	3MJAES-QP55C7-KS8JE6-QLHJRHES
dmuller-win7	BC5JYJ-5MA5GY-J3CUG5-GC3YVQRN
jkang-win11	4GXFL6-JME4EQ-XS3687-4BR87Y4S
mwiacek-macos	62XKGG-BNVALU-TEUYRJ-543QHFDJ
pscott-ubuntu	69EUNK-YNSGEK-LSJDCK-VSFD88FA
smiller-win7	2VMT5B-U6JELF-Z3CL67-H2E9TLZA
tking-win11	RXDC9L-2E7A2D-AZ5KBR-2MLRLFZW

Mutexes >100

Mutex Name
{5312EE61-79E3-4A24-BFE1-132B85B23C3A}
Local\ZonesLockedCache
Global\430584d5-1026-4a02-95a4-9b0c30252b68
UpdatingNewTabPageData
Local\HKEY_CURRENT_USER_SOFTWARE_Microsoft_Speech_Current
Local\WERReportingForProcess4676
Local\AmiSharedMutex_4728
Local\ShimViewer

Key benefits of Inception

Inception is your trusted partner, guiding you through threat analysis, detection, and response. It automates processes that have traditionally made detecting compromise tedious and time consuming. And the platform offers a rich set of investigation tools to help you outsmart attackers.

Detects compromise across past, present, and future states

Inception treats all files as suspicious and pre-preserves them as evidence to speed detection and uncover previously unknown compromises. By continuously evaluating the entirety of evidence in light of emerging insights, we unlock time. You can detect compromise across the past, present, and future states of your organization's environment, denying attackers places to hide.

Produces contextual threat intelligence

With its inside-out approach, Inception uncovers what's most important to your organization. The platform starts by analyzing your files to produce intelligence and then enriches it with external information to deliver actionable insights for detection and response teams. Inception amplifies the novel activity and interesting relationships between files in your environment. It helps you identify malware variants and uncover low-prevalence artifacts that indicate nefarious activity.

Keeps you out of attackers' reach

Inception helps you outsmart even the most sophisticated attackers with unique threat detection for your organization that is imperceptible to attackers. It does this by giving you a platform for creating tailored defenses and intelligence that the attackers can't test against or reverse engineer.

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

1. Collect

It's easy to collect any file within your environment for recursive investigation.

Safely collect, preserve, and keep files active for continuous analysis:

- Ingest any file and keep it for continuous analysis
- Pull files from wherever they are
- Store your own malware samples or enable feeds of malware
- Continuously scan all stored files

2. Analyze

It automatically analyzes all collected files–past and present–to create tailored intelligence and enrich it with external information. Inception:

- Evaluates every file continuously, based on emerging intelligence
- Scans every file with 32+ AV engines and returns the tally and signatures of suspicious files
- Continually analyzes your tagged IOC queries and notifies you as new information comes in
- Does pattern-matching against files and feeds
- Enables efficient management of thousands of YARA rules: pre-loaded, feeds, custom, new
- Provides syntax guidance for your YARA rules

3. Investigate

Use 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.

- Hunt for signal across your centrally stored files with our powerful query language
- Re-investigate IOCs as new information comes in to eliminate false negatives
- Uncover anomalies, variants, unique relationships, and low-prevalence files
- Detonate files to generate more signal

4. Connect

Inception is designed to integrate with your security workflow. You can use pre-built integrations or use the Inception API to build a custom integration.
You can:

- Get notified about alerts in Inception in your ticketing system, inbox, or chat update
- Log Inception events and alerts to your SIEM
- Plug directly into your security infrastructure and integrate with SOAR or other applications
- Identify false negatives from your auto-triaged events by integrating enriched IOC data in your SOAR

Stairwell

Inception Platform

Use Cases

Gain visibility, customize defenses, analyze suspicious files, and triage more effectively

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

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. Even your investigations of suspicious activity are preserved for ongoing analysis by the platform. When you identify malware-led attacks, 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

The Inception platform extracts IoCs and observables from suspicious files in your environment. This inside-out approach ensures that the identified IoCs are applicable to 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 the protection tools (Firewalls, EDR, etc. used for enrichment of detection and response information. Inception prioritizes threats inside your environment, while continuously analyzing your files against the latest threat intelligence from multiple sources.

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. You can begin looking for its traces in your environment because the Inception platform collects all of your file corpus and pre-preserves it as evidence. It extracts features out of these files – including files that may have been deleted – and continuously analyzes them against the latest threat intelligence.

Triage every alert with research-grade understanding

Inception provides your team a one-stop-shop for static and dynamic analysis of potential malware and presents all of the information in an easy-to-use interface. Inception also provides file enrichment APIs that can pull information directly into your SIEM and/or SOAR. 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. Inception can also compare the features of the convicted files against the overall file corpus of your organization and highlight any files that look similar to the bad one. You can also use the Inception platform to analyze files from systems that you believe were infected on an ad hoc basis.

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. 051022

Stairwell