

Autonomous proactive cyber defense

Emerging threats assessed, hunted, and hardened against
across your enterprise stack, in minutes, not days.

BACKED BY

Austrade & Global Victoria
global partnerships

BUILT FOR

Cyber teams in mid-to-
large enterprise
organizations

GET STARTED

[Book a demo →](#)

Meet Sol

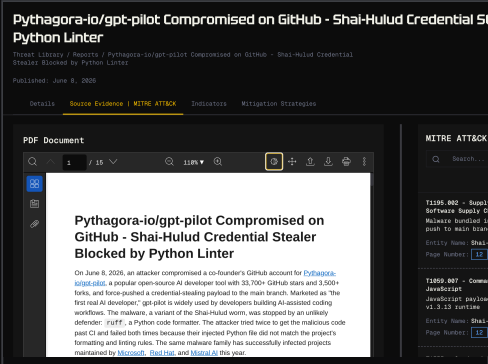
Sol collects intelligence, prioritizes the threats that matter to you, and orchestrates the defenses that close the gap, end to end.



Emerging relevant threat

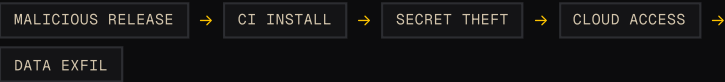
Shai-Hulud · self-propagating npm worm, steals CI & cloud secrets

T1195.001 · T1552.001 · Matched to you



Sol orchestrates and improves defenses

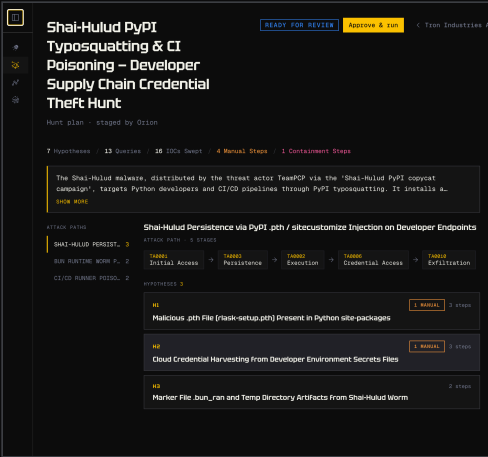
Dependency scan · 1,284 packages · 1 finding



HUNT	Compromised packages & secret theft
HARDEN	Pin lockfile, revert infected packages
REMEDiate	Rotate exposed CI token

ACROSS GitHub SIEM AWS

~90 seconds, start to finish



Sol notifies & informs

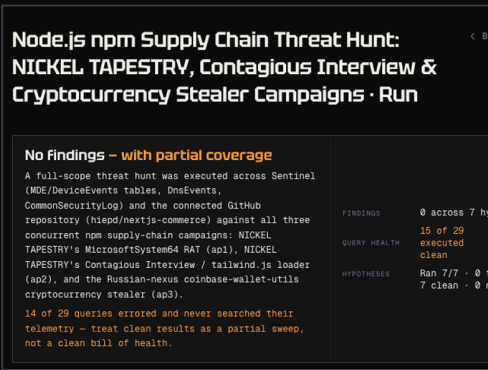
Mitigation plan posted to Slack #security-ops

3 repos pinned · 1 token rotated · Awaiting approval



Ready for the threat

- ✓ 3 repos pinned to safe version
 - ✓ Exposed CI token rotated & scoped
 - ✓ Validated SIEM & AWS for impact
- Intel to hardened



■ Human approval on every execution, or fully automated. Your call.

HOW IT WORKS

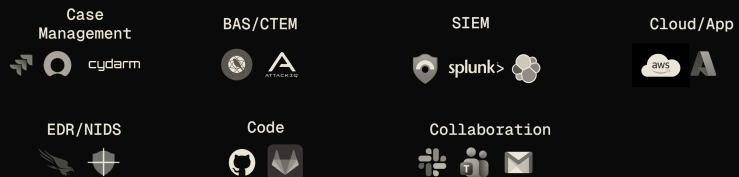
Built for **autonomous** workflows,
across your existing stack.

Sol

Proactive actions



Integrations



Outcomes



Close the gap in **minutes**, not days

ENABLE AUTOMATION

Configure once. Sol does the rest.

You define what Sol watches, the playbooks it runs, where they run, and how much autonomy to grant. From then on Sol acts on every matching threat, day and night.

01



Create a threat profile

Tell Sol what to watch: a sector, a campaign, or a line of defense.

THREAT PROFILE

- Healthcare Sector

Live

Sector · Healthcare

Region · ANZ

02



Configure playbooks

Choose which playbooks Sol runs against the profile, and their scope.

PLAYBOOKS

- Threat Hunting
- Cyber Threat Intelligence
- Detection Engineering
- Threat Mitigation
- Executive
- Attack Simulation

90 days

03



Configure integrations

Connect the tools Sol runs in. No new console to live in.

RUN TARGETS · 2 SELECTED

- ☒ Microsoft Sentinel
- ☒ GitHub

CONNECTED

CONNECTED

04



Configure the workflow

Set how much autonomy Sol has, and how your team gets notified.

MODE

Manual

Semi-automated

Fully automated

☒ Notified via Slack

INSIDE SOL

AsyncRAT CDN Steganography & Bulletproof Infrastructure Hunt - US Defense Sector

REAL

Hunt plan · staged by Orion

6 Hypotheses / 14 Queries / 30 IOCs Swept / 4 Manual Steps / 1 Containment Step

The threat actor 'gigajew' (tracked on HackForums) is operating an AsyncRAT campaign that weaponizes Cloudinary CDN-hosted steganographic images to

[SHOW MORE](#)

ATTACK PATHS

CDN STEGANOGRAPHY ... 5

ASYNCRAT PERSISTEN... 3

CDN Steganography Stager → JScript Dropper → A .NET Implant

ATTACK PATH · 7 STAGES

TA0001
Initial
Access

→

TA0002
Execution

→

TA0005
Defense
Evasion

→

TA0011
Command
and
Control

HYPOTHESES 5

H1

Cloudinary CDN Image Fetch Used to Deliver Steganographic AsyncRAT Stager

1 MANU...

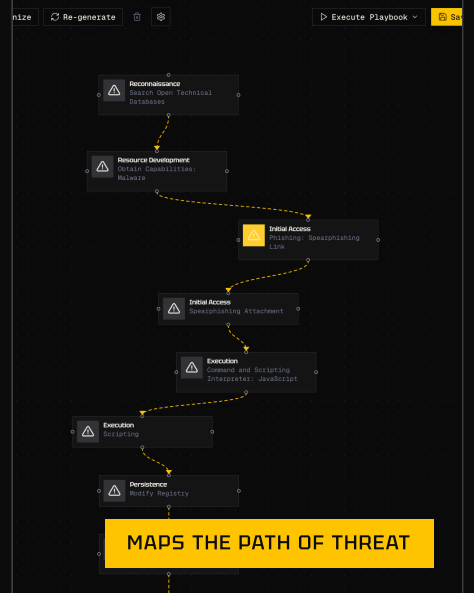
H2

WScript / CScript Spawning (~7500-line Junk-Injection) on

1 MANU...

AUTONOMOUS PLAYBOOKS

PT Overlapping TTPs - 16 Key Groups

Relationships Heatmap Overlap **Attack Path**

MAPS THE PATH OF THREAT

give me a workbench with their overlapping TTPs

I want all of them

ORION

Now let me fetch the MITRE profiles for the most significant active Iranian threat actors in parallel:

Now I have enough data to synthesize the key overlapping TTPs and build the workbench. Let me identify the highest-frequency cross-entity technique clusters before calling the workbench tool.

Iranian APT Overlapping TTPs - 16 Key Groups [Open in workbench](#)

Cross-actor TTP overlap analysis across the most active Iranian state-sponsored threat actors, revealing shared tradecraft between IRGC and MOIS-linked clusters.

16 Actors · 17 connections

Across the 16 Iranian actors profiled, the TTP overlap is striking and analytically revealing - the ecosystem effectively shares a common playbook with differentiated objectives rather than differentiated methods.

The universal spearphishing (T1589.001) and persistence (T1567.001), and HTTP/HTTPS C2 (T1071.001). This means attribution purely from initial access or persistence artifacts is

ASK IN PLAIN LANGUAGE

HackForums Actor gigajew Caught Red-Handed: AsyncRAT Campaign Uses Cloudinary CDN Infrastructure

Threat Library / Reports / HackForums Actor gigajew Caught Red-Handed: AsyncRAT Campaign Uses Cloudinary CDN Steganography and 7-Month-Old Bulletproof Infrastructure

Published: March 16, 2025

Details Source Evidence MITRE ATTACK Indicators Mitigation Strategies

PDF Document

HackForums Actor "gigajew" Caught Red-Handed: AsyncRAT Campaign Uses Cloudinary CDN Steganography and 7-Month-Old Bulletproof Infrastructure

intel.breakglass.tech/post/hackforums-actor-gigajew-caught-red-handed-asyncrat-campaign-uses-cloudinary-cdn-steganography-and-7-month-old-bulletproof-infrastructure

Breakglass Intelligence

March 16, 2026

Breakglass Intelligence

intel.breakglass.tech

HackForums Actor "gigajew" Caught Red-Handed: AsyncRAT Campaign Uses Cloudinary CDN Steganography and 7-Month-Old Bulletproof Infrastructure

INTELLIGENCE DRIVEN

Threat Library / Threat Actors / Scattered Spider

Scattered Spider

Details MITRE ATTACK Reports

TA0043 - Reconnaissance	TA0042 - Resource Development	TA0001 - Initial Access	TA0027 - Initial Access
T1589 - Gather Victim Identity Information	T1583 - Acquire Infrastructure	T1078 - Valid Accounts	T1451 - SIM Card Swap
T1589.001 - Gather Victim Identity Information: Credentials	T1583.001 - Acquire Infrastructure: Domains	T1078.002 - Valid Accounts: Domain Accounts	T1600 - Phishing
T1589.002 - Gather Victim Identity Information: Email Addresses	T1583.003 - Acquire Infrastructure: Virtual Private Server	T1078.004 - Valid Accounts: Cloud Accounts	
T1580 - Gather Victim Network Information	T1585 - Establish Accounts	T1133 - External Remote Services	
T1580.005 - Gather Victim Network Information: IP Addresses	T1585.001 - Establish Accounts: Social Media Accounts	T1190 - Exploit Public-Facing Application	
T1593 - Search Open Websites/Domains	T1586 - Compromise Accounts	T1159 - Trusted Relationship	
T1593.001 - Search Open Websites/Domains: Social Media	T1586.002 - Compromise Accounts: Email Accounts	T1566 - Phishing	
T1594 - Search Victim-Owned Websites		T1566.001 - Phishing: Spearphishing	
T1597 - Search Closed Sources		T1566.002 - Spearphishing Link	
		T1566.003 - Phishing: Spearphishing Link	

PROVEN COVERAGE

FEATURES

Continuously prepare your defense.



Threat context

TTPs, victimology and behaviors, structured for agents to reason over.



Living threat profile

Who is likely to target what you run, updated as the landscape moves.



Attack path mapping

How a technique actually reaches your crown jewels, ranked.



Threat hunting

Pursues what slips past alerts, before it becomes an incident.



Attack simulation

Replays real adversary tradecraft to find what your defenses miss.



Detection engineering

Writes and tunes detections that fire on what matters.



Mitigation & remediation

Closes the gaps it finds, then verifies the fix held.



Autonomous & continuous

Runs every cycle without tasking, day and night.



Human-in-the-loop

Approvals in Slack, Teams or Jira. One click, full audit trail.



Sol AI ✦

Research any threat in plain language, then manually orchestrate hunts, simulations, detections and briefings across the whole platform.

WHERE WE FIT

Where Sol fits.

Sol orchestrates based on emerging threat behavior across the tools you already run, turning your existing stack into one proactive defense.

INPUT · THREAT INTELLIGENCE

Emerging threat intelligence

Reports · TTPs · victimology · OSINT



SOL

AUTONOMOUS PROACTIVE DEFENSE

Threat behavior / Orchestration / Execution

ORCHESTRATE & EXECUTE PROACTIVE DEFENSES BASED ON YOUR THREATS



Attack
Simulation



Endpoint



Network



Cloud



Application



SecOps /
SIEM



YOUR EXISTING STACK

POSITIONING

AI SOC helps you clean up. Sol helps you avoid the mess.

BEFORE THE BREACH

BREACH HAPPENS

AFTER THE BREACH



An attack slips through defenses

Sol

Proactively defends **before** the breach.

- Proactive and threat-informed
- Triggered by new intelligence and which adversaries & TTPs matter to you
- Intel → hunts, simulation, detection, execution, defensive uplift
- Answers the 3 questions CISOs ask:
 - ? Does it affect us?
 - ? Have we been impacted?
 - ? Are we prepared?

AI SOC

Detects it and reacts faster.

- Reactive and alert-driven
- Triggered by what's firing right now
- Alert → triage → investigate → respond
- Faster containment during the incident



Ready before the **breach.**

Book a demo

EMAIL

info@elezar.io

WEBSITE

elezar.io

LOCATION

Melbourne, Australia