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 →

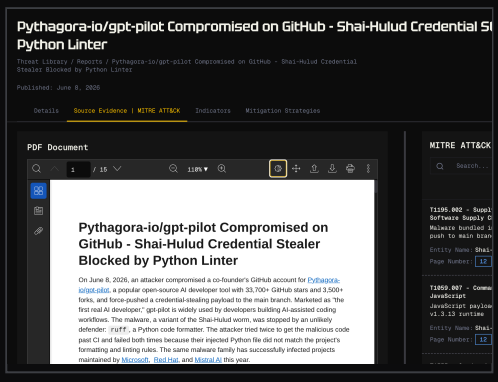
Meet Sol

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

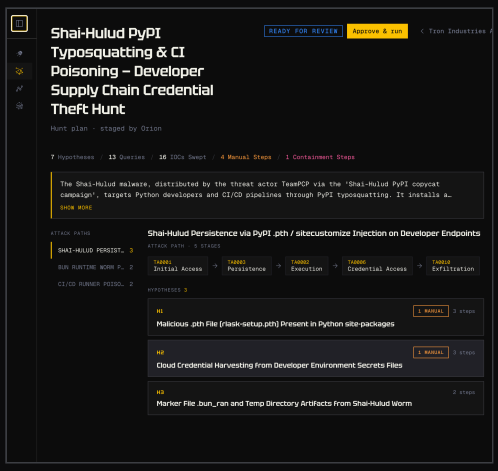
Dependency scan · 1,284 packages · 1 finding

MALICIOUS RELEASE → CI INSTALL → SECRET THEFT → CLOUD ACCESS → DATA EXFIL

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

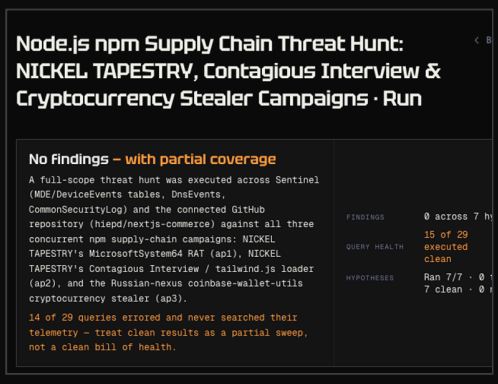
Mitigation plan posted to Slack #security-ops

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

- Contextualizes new intelligence
- Prioritizes threat
- Plans defensive actions
- Orchestrates & executes
- Closes gap in environment

Proactive actions

- Update threat profile
- Simulate attack
- Hunt for compromise
- Uplift detection
- Update security policies

Integrations

- Case Management: cydarm
- BAS/CTEM
- SIEM: splunk>
- Cloud/App: aws
- EDR/NIDS
- Code
- Collaboration

Outcomes

Relevance resolved
Only threats relevant to your organization

Coverage proven
Hunted, simulated, detections written

Readiness automated
Gaps closed and verified, evidence for the board

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 — 90 days
- Cyber Threat Intelligence
- Detection Engineering
- Threat Mitigation
- Executive
- Attack Simulation

03

Configure integrations

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

RUN TARGETS · 2 SELECTED

- ✓ Microsoft Sentinel — CONNECTED
- ✓ GitHub — 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

REA

Hunt plan · staged by Orion

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

The threat actor 'gigajew' (tracked on HackForums) is operating an Async 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

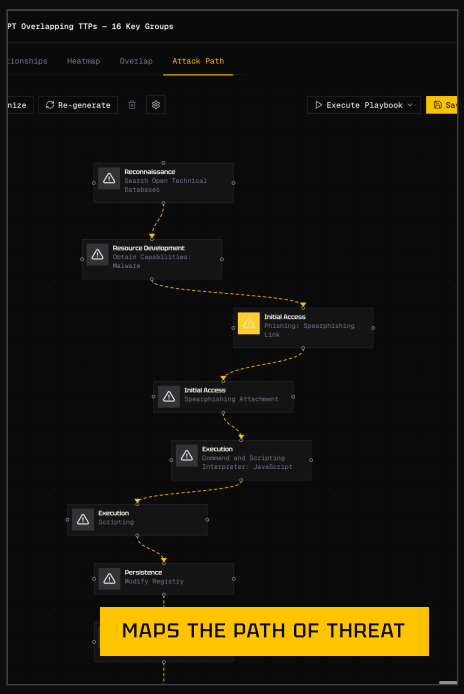
H1 1 MANU

Cloudinary CDN Image Fetch Used to Deliver Steganog AsyncRAT Stager

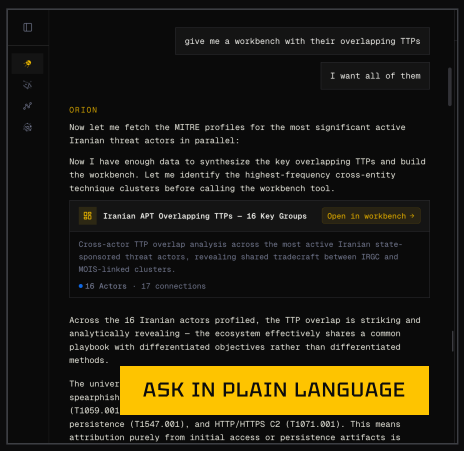
H2 1 MANU

WScript / CScript Spa on (~7500-line Junk-Inje

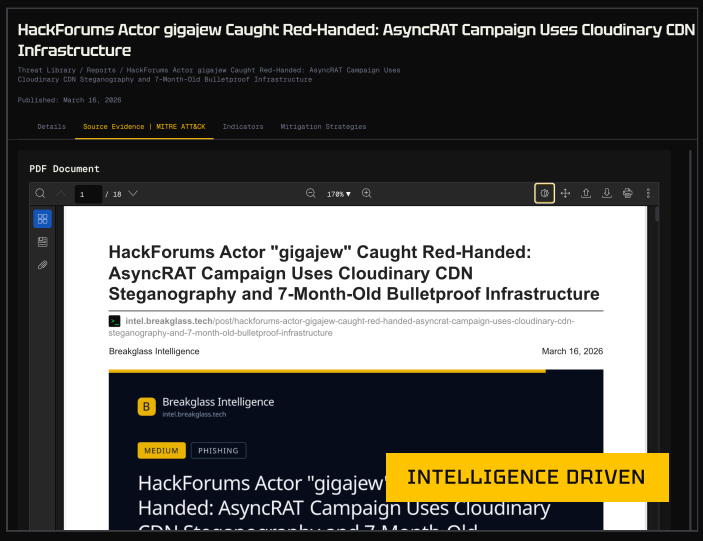
AUTONOMOUS PLAYBOOKS



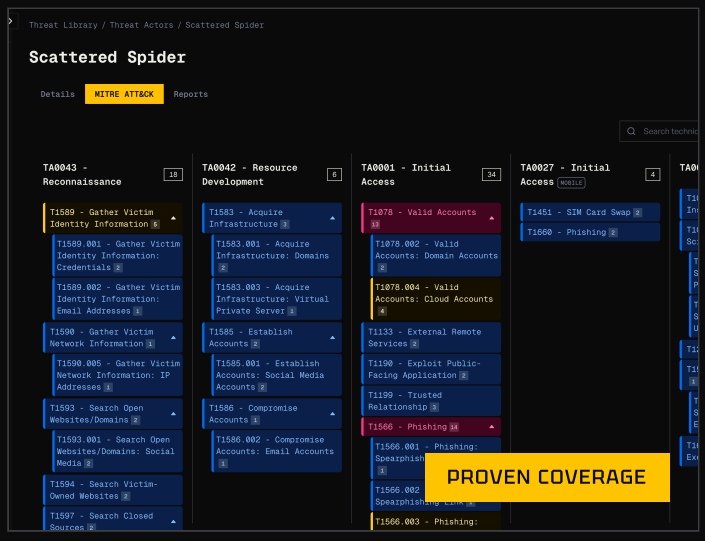
MAPS THE PATH OF THREAT



ASK IN PLAIN LANGUAGE



INTELLIGENCE DRIVEN



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

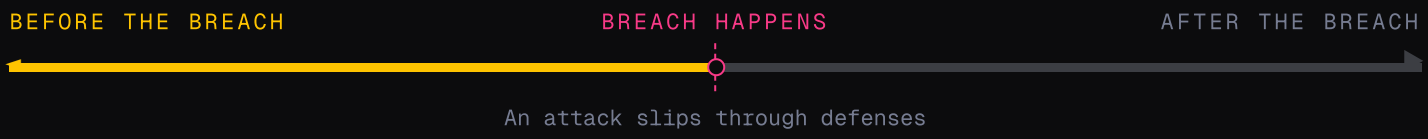
ORCHESTRATE & EXECUTE PROACTIVE DEFENSES BASED ON YOUR THREATS

Attack Simulation	Endpoint	Network	Cloud	Application	SecOps / SIEM

YOUR EXISTING STACK

POSITIONING

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



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