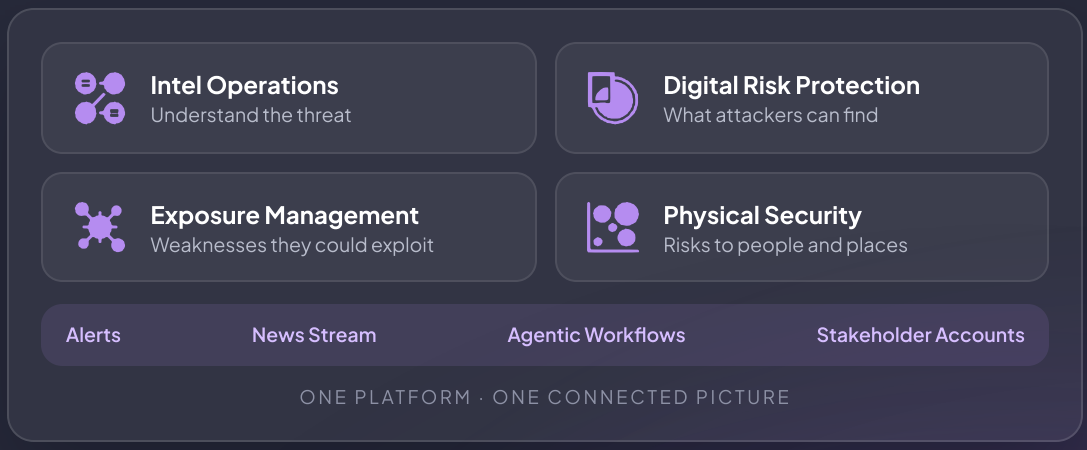
MORADO · THREAT INTELLIGENCE PLATFORM

See what attackers see. Act before they do.

How Morado connects threat intelligence, digital risk, exposure management and physical security in one platform, and turns what it finds into action.

Security teams | CTI and SOC | Exposure management | MSSPs and partners



Knowing about a threat is only the beginning.

Security teams are not short of threat data. Feeds, alerts, reports and dark web findings arrive from more tools than most teams can watch. What they are short of is answers: whether a threat affects their organization, whether their defenses would stop it, and who needs to act.

Are we affected?

A supplier is breached. Credentials are exposed. A threat actor targets your industry. What does it mean for you?

Are we protected?

An alert doesn't say whether you can detect the attacker's techniques or whether your weaknesses are exploitable.

What happens next?

Findings need to become action: hunts, response workflows and the teams responsible for protecting you.

Why it's hard today

Too many disconnected tools. Threat intelligence, dark web monitoring, brand protection, attack surface and vulnerability data usually live in separate products. Each produces useful signals, but analysts have to stitch them together by hand, and the connections between them get missed.

Intelligence without a path to action. Most tools surface data and stop there. Checking whether a threat applies to your environment, hunting for it and coordinating a response all happen somewhere else.

Disconnected from requirements. Intelligence requirements, RFIs and stakeholder questions are tracked in spreadsheets and email, so it is hard to direct collection or show that the program answers what the business needs to know.

> Morado is built to close those gaps: one platform that finds what attackers could use against you, connects it with the threats that matter, tests it against your environment and carries it through to the people who act.

A connected intelligence program, from discovery to decision.

Morado produces its own intelligence and exposure findings and brings in your existing intelligence feeds, security tools and internal data. Prioritization is one outcome. The bigger one is a program that supports discovery, investigation, defense, collaboration and decision-making.

01	02	03	04
Find exposure	**Know the threat**	**Take action**	**Keep improving**
Leaked credentials, impersonation, exposed infrastructure and location-specific risks.	Connect findings with attacker activity, your intelligence requirements and evidence from your environment.	Launch hunts, assess detection coverage, check exposure, protect accounts and coordinate remediation.	Share intelligence, collect stakeholder feedback, answer RFIs and track program maturity.

How the platform works

COLLECT
Your data and ours

- Your tools: SIEM, EDR, vulnerability scanners and intelligence feeds
- Brand, executive and third-party monitoring
- Threat feeds and news, collecting from day one
- Morado's scans: attack surface, vulnerability validation and dark web
- Physical locations and travel
- 30+ integrations with the tools you already run

UNDERSTAND
One pipeline

- **Process:** normalize every source
- **Correlate:** link threats to your exposures
- **Prioritize:** what deserves attention, and who needs to act
- **Enrich:** add attacker context
- **Test:** hunts, coverage and exposure checks

DELIVER
To the people who act

- Alerts and investigations for your analysts
- IOCs pushed to your SIEM
- Agentic workflows for repeatable response
- Tasks in your ticketing or ServiceNow
- Reports, briefings and answers to RFIs
- Stakeholder accounts for decision-makers

A FULL TIP, AND THE PROGRAM AROUND IT.

Intel Operations

Everything you expect from a Threat Intelligence Platform, connected to the rest of your intelligence program: stakeholder requirements, investigations, hunts, coverage analysis, detections, reporting and feedback.

Threat Intelligence Platform

Intelligence from feeds, reports, communities, partners and your own findings in one record, with the full indicator lifecycle.

- Standardized, deduplicated and enriched, with source and handling kept
- Decide whether to research, monitor, hunt, alert or block
- Distributed to SIEM, endpoint, network, DNS, web and email controls; STIX 2.1 in and out

Stakeholders & requirements

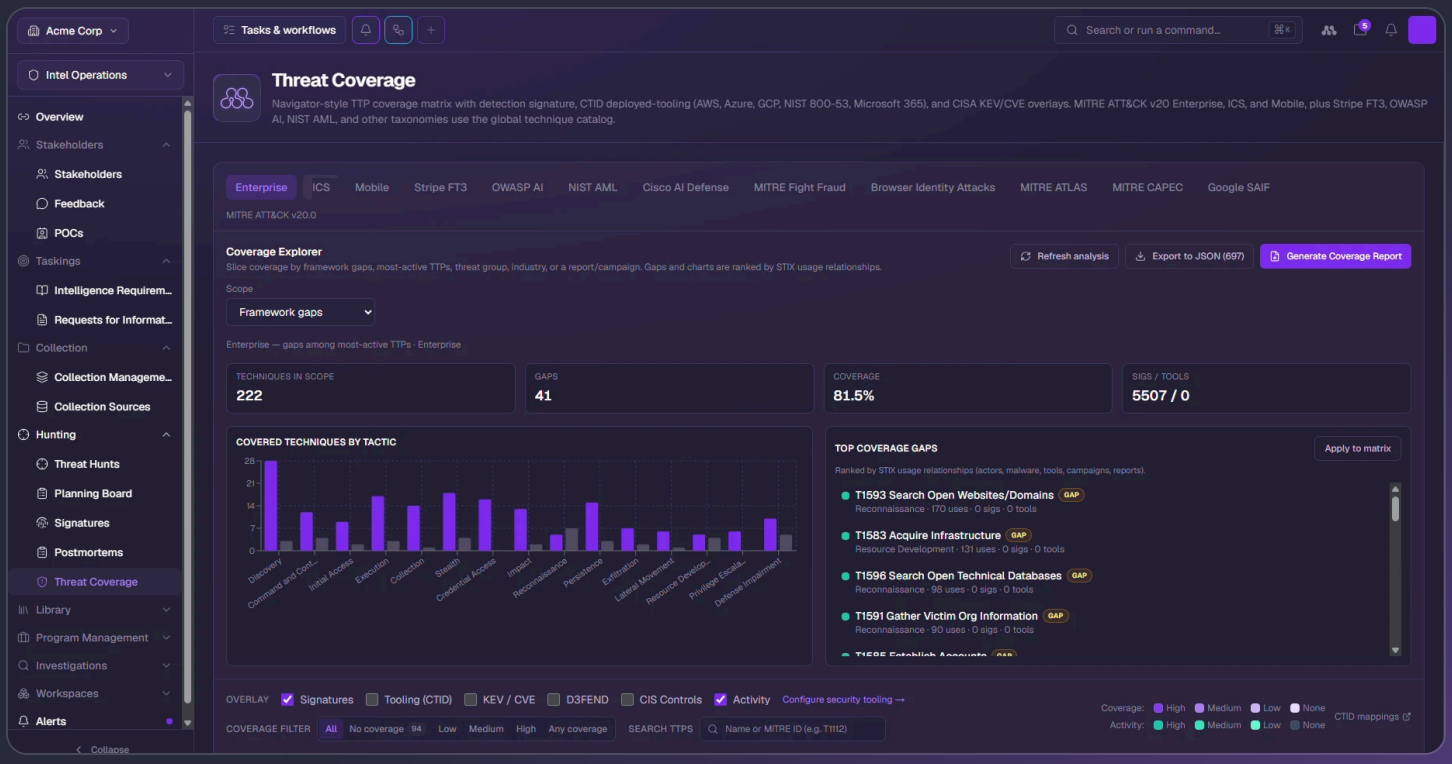
Stakeholder functions aligned to Priority Intelligence Requirements, so the CTI team knows who needs a finding and who to escalate to. RFIs keep questions and answers on record.

Threat coverage across frameworks

Map relevant actor behavior across ATT&CK, ATLAS, CAPEC, fraud and AI security frameworks against your telemetry and detections, then turn gaps into detection work your team reviews.

Investigations, hunts & reporting

Hypothesis-driven investigations, retrospective hunts in your SIEM, and reports tailored to each audience, with stakeholder feedback that becomes follow-up work.



Threat coverage in Intel Operations. Example data.

DISCOVER WHAT ATTACKERS CAN FIND ABOUT YOU.

Digital Risk Protection

External threats and exposures affecting your organization, people, brand and business relationships, connected with investigation and remediation so every finding keeps its evidence and leads to a documented decision.

Brand protection

Lookalike domains, impersonating apps and social profiles, with screenshots, evidence and takedown support.

Compromised credentials & stealer logs

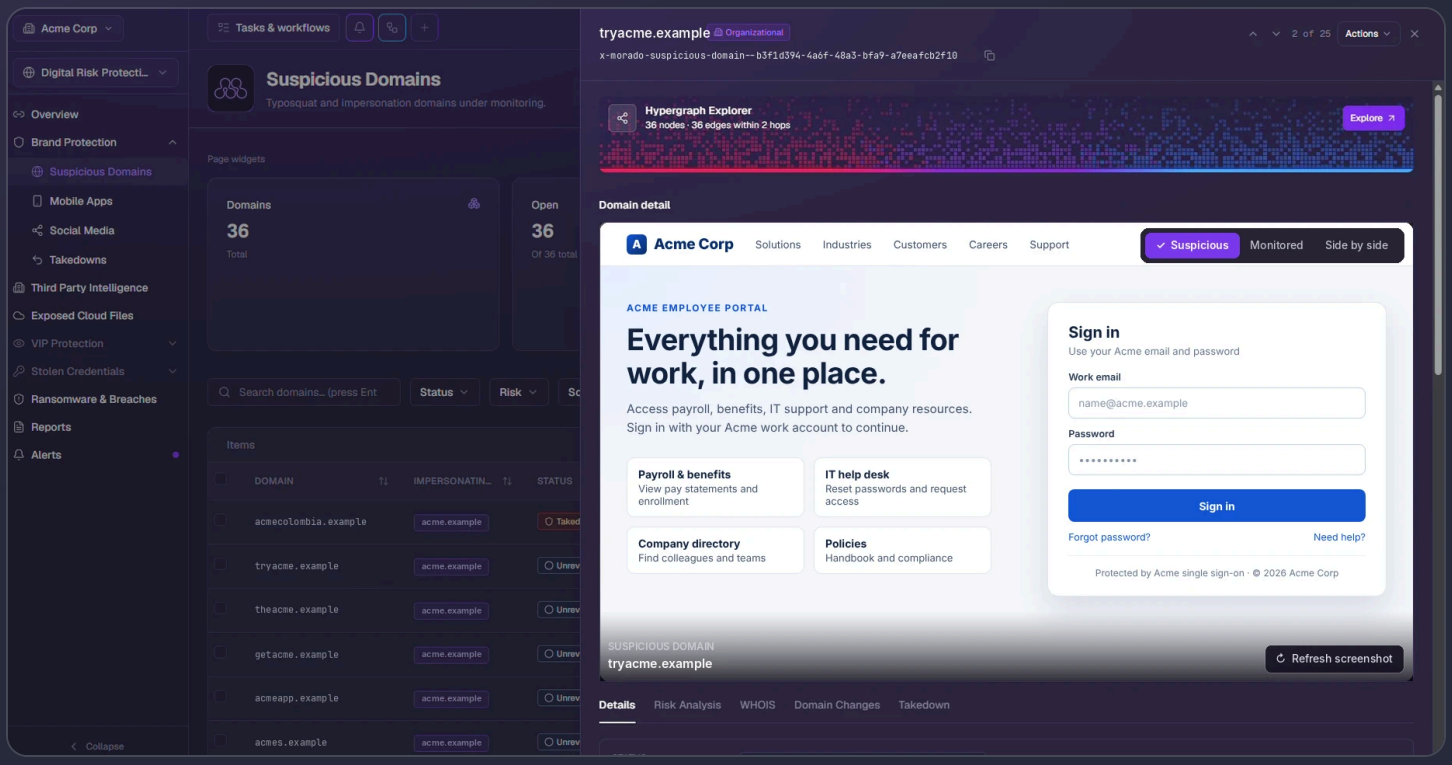
Credentials from breach data, combo lists and stealer logs, prioritized with password-policy filtering and validated through Microsoft Entra workflows.

Executives, exposed files & third parties

Executive exposure and impersonation, publicly exposed cloud files, and ongoing intelligence on suppliers and partners.

Ransomware & breach intelligence

Claims that name you, and your files appearing in a supplier's breach. A claim is a lead, assessed against the evidence.



A lookalike domain hosting a copy of an Acme sign-in page. Example data.

FIND THE WEAKNESSES ATTACKERS COULD EXPLOIT. PROVE WHICH ONES THEY CAN.

Exposure Management

Discover exposed assets, validate exploitability and prioritize remediation by the threats that matter to you, in a full Continuous Threat Exposure Management (CTEM) program.

Scope & discovery

Domains, IPs and CIDR ranges, or assets imported read-only from your cloud accounts, scanned for exposures, misconfigurations, certificate issues and vulnerabilities.

Live exploitability validation

For supported vulnerabilities, proprietary live testing shows whether a weakness is actually exploitable, with a focus on edge devices.

Drift & prioritization

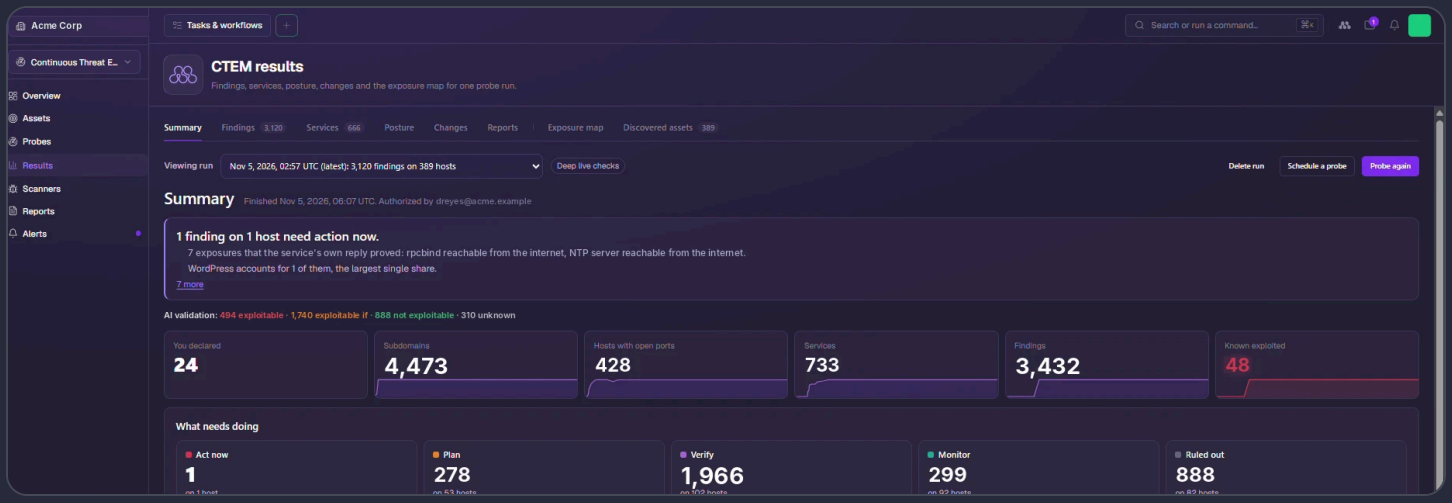
Each assessment compared with the last, so you see what is new, persistent or returning, prioritized with Morado vulnerability intelligence.

Notify, rescan & verify

Findings go to the teams who fix them, with the evidence behind each request, then a rapid rescan confirms the fix worked.

The CTEM cycle

01	02	03	04	05
Scope	**Discover**	**Prioritize**	**Validate**	**Mobilize**
Domains, IPs, ranges and cloud accounts.	Exposures and internal scanner findings.	Intelligence, impact and drift.	Live testing of exploitability.	Notify, then rescan to verify.



CTEM results in Exposure Management. Example data.

UNDERSTAND RISKS AROUND YOUR PEOPLE AND LOCATIONS.

Physical Security

Monitor physical threats to employees, travelling executives and VIPs, and the places people work, with location-based monitoring, travel risk, camera integration and geopolitical intelligence.

Sites & the Operations Map

A risk score for every office and plant, with incidents, news and satellite imagery around each area of interest.

Camera integration

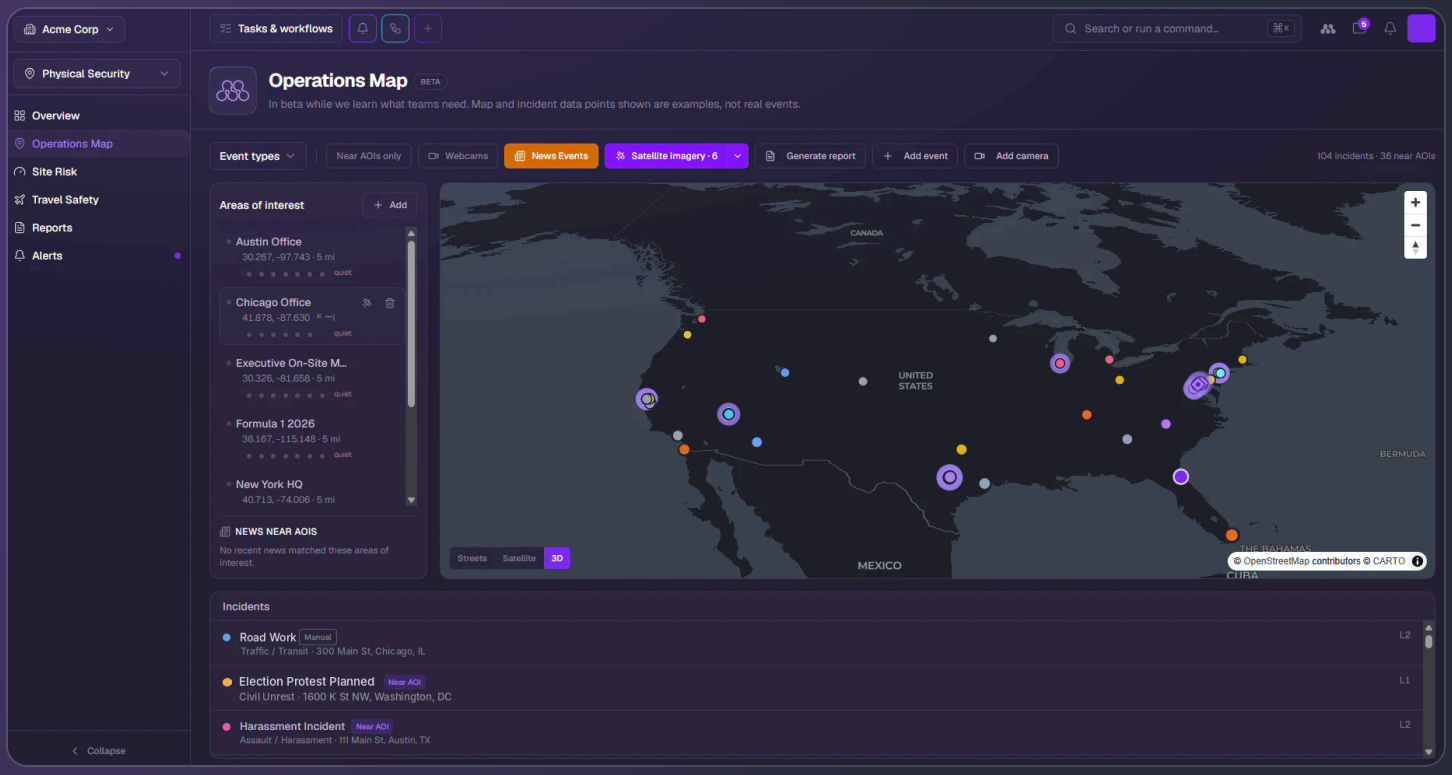
Supported customer camera systems give authorized security staff a view of conditions while they assess an event.

Executive & VIP travel

A risk brief for every trip, with warnings before departure, in transit and at the destination.

Geopolitical intelligence

Regional developments connected to the sites and trips they could affect, so plans are reviewed before an incident.



The Operations Map in Physical Security. Example data.

Across every module

These capabilities work across all four modules, so a finding in one place can be triaged, investigated, automated and shared from anywhere.

Alerts

One command center for everything that comes in. Every module feeds one prioritized queue, with AI analysis in every alert doing the first pass while your analysts make the call.

News Stream

Reporting matched to your Priority Intelligence Requirements. Stories group coverage of a topic across sources, and the intelligence in each article is extracted into STIX.

Agentic Workflows

Describe a process in plain language and Morado builds the automation, no code required. Approval steps keep a human in the loop before the actions that matter.

Stakeholder Accounts

A simple view for executives and business leaders: read reports, give feedback and open RFIs, connected to your intelligence team.

Workspaces

Bring other organizations into a shared environment to share intelligence, upload reports and discuss findings, for customer communities, partners and ISACs.

Program maturity

A built-in CTI-CMM assessment shows where your program stands, where to improve and how it is progressing.

How it connects: two examples

A compromised credential

- Digital Risk Protection finds an exposed credential.
- A workflow checks it against your password policy and validates it in Microsoft Entra.
- If it is live, the configured protection runs: password reset and session revocation.
- The user and your analysts are notified, and the alert closes.

A third-party breach

- Third-party monitoring identifies an incident at a supplier.
- A workflow investigates the actor, hunts for its indicators and checks TTP coverage.
- Exposure Management checks for the vulnerabilities involved.
- Relevant findings are escalated to the teams responsible.

Built for the way you work

Security leaders
Understand threats to your organization and where your defenses need attention. Give leadership clear assessments and track program maturity.

CTI, SOC and detection teams
Turn threat reporting into investigations, automated hunts and detection improvements.

Exposure and physical security teams
Validate vulnerabilities, investigate digital exposure and assess risks to people and locations.

MSSPs and partners
Fully multi-tenant across all four modules, co-branded or powered by Morado, with customer users inside their own tenants.

Run it your way

Self-service
Your team, or your provider, operates the platform.

Analyst-supported
Morado analysts add research, investigations, reporting, RFIs and dark web retrieval.

Managed program
Morado runs ongoing intelligence operations within an agreed scope.

Partner delivery
MSSPs and consultancies deliver across customer tenants.

Security and trust

SaaS, with strict separation
Morado is delivered as a SaaS platform. Each organization and each MSSP customer has its own tenant, with its data kept separate.

Trust Center
Security, privacy and compliance documentation is available in our Trust Center, and our SOC 2 Type II report is shared on request.

About Morado. Morado is a veteran-owned cyber threat intelligence company headquartered in San Diego, California. Morado combines a threat intelligence platform with analyst services, so security teams and the providers who serve them can see what attackers see and act before they do.

501 W Broadway, Suite 800, San Diego, CA 92101

See Morado in action.

Book a demo, or start a free 2-week trial.

sales@morado.io
morado.io/demo