Morado

THREAT INTELLIGENCE THAT LEADS TO ACTION

See what attackers see. Act before they do.

Morado is one connected platform for threat intelligence, digital risk, exposure management and physical security. It shows what attackers can see about your organization, tells you what's relevant, and helps your team respond, with software and analysts working together.

01
Find exposure
Leaked credentials, impersonation, exposed assets and location risks.

02
Know the threat
Connect findings with attackers, your requirements and your environment.

03
Take action
Hunts, detection coverage, exposure checks, account protection and remediation.

04
Keep improving
Share intelligence, answer RFIs, collect feedback and track program maturity.

Four modules, one platform

Intel Operations
A full TIP, and the program around it.
- Full TIP: indicator lifecycle, STIX 2.1, push to your tools
- Stakeholders, PIRs and RFIs aligned to who acts
- Coverage across ATT&CK, fraud and AI frameworks
- Investigations, SIEM hunts, detections and reporting

Digital Risk Protection
Discover what attackers can find about you.
- Brand impersonation: domains, apps and social, with takedowns
- Stolen credentials and stealer logs, validated in Entra
- Executive exposure, exposed files and third parties
- Ransomware and breach intelligence

Exposure Management
Find and prove the weaknesses attackers could exploit.
- Discovery from domains, ranges and cloud accounts
- Live validation of exploitability, focused on edge devices
- Drift tracking, threat context and internal scanner data
- Notify the teams who fix it, then rescan to verify

Physical Security
Understand risks around your people and locations.
- Site risk and the Operations Map for offices and plants
- Executive and VIP travel risk briefs
- Camera integration, imagery and local news
- Geopolitical intelligence tied to sites and trips

Across every module — Alerts · News Stream · Agentic Workflows · Stakeholder Accounts

Why teams choose Morado

One connected program
Requirements, digital risk, exposure, physical risk and reporting in one place, so findings connect.

Tested against your environment
Hunt in your SIEM, compare actor TTPs with your detections and validate exploitability. 30+ integrations.

Agentic workflows
Describe a process in plain language and Morado builds it. No code, with a human in the loop.

Proof of progress
Built-in CTI-CMM assessment and stakeholder feedback show where your program stands and how it improves.

Who it's for

Security leaders · CTI · SOC & detection · Exposure teams · Physical security · MSSPs & partners

Run it your way

Self-service, **analyst-supported** or a **managed program**. Morado analysts add research, investigations, reporting, RFIs and dark web support when you need them. MSSPs deliver across fully multi-tenant customer tenants, under their own brand.

in /morado-intelligence
web morado.io
email sales@morado.io