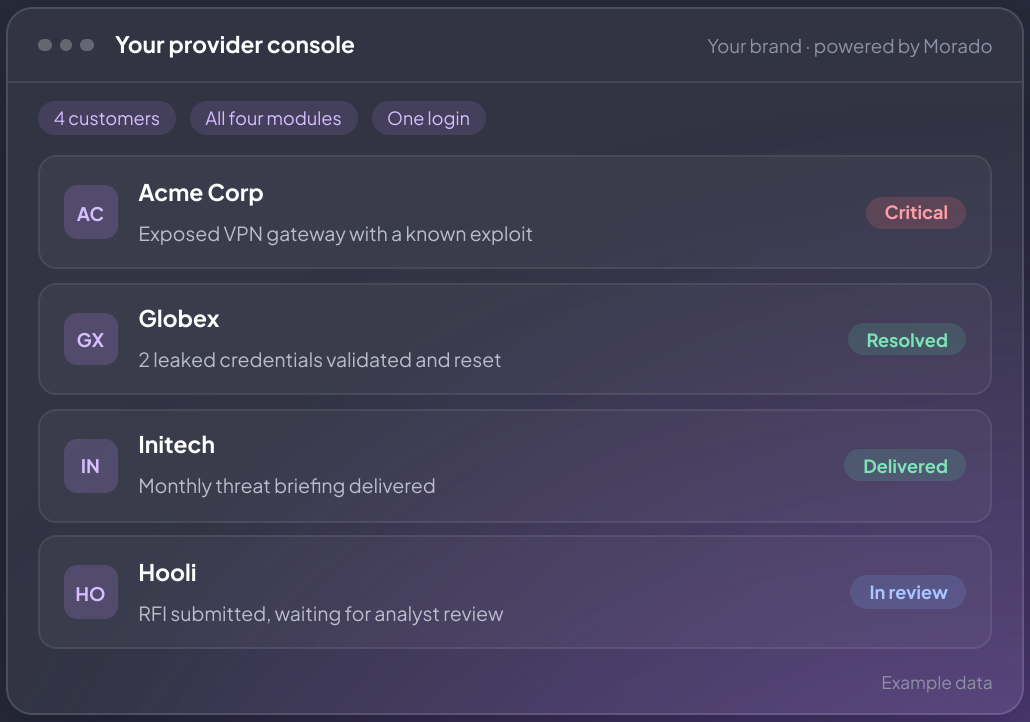
MORADO · MSSP AND PARTNER PROGRAM

Threat intelligence as a managed service.

How MSSPs and consultancies can launch, deliver and scale a cyber threat intelligence service line for every customer they serve.

MSSPs · MSPs · Consultancies · MDR providers



Every customer needs threat intelligence. Few can build it themselves.

Threat intelligence helps a security team focus on the attacks most likely to reach it: which actors target its industry, which of their techniques its defenses would miss, which exposed assets and credentials give them a way in. Customers increasingly expect it. But when they ask about it, they rarely want a feed. They want answers.

Are we affected?

A supplier is breached. Credentials are exposed. An actor targets our industry. What does it mean for us?

Are we protected?

Can we detect the attacker's techniques? Are the vulnerabilities they exploit present and exploitable here?

What happens next?

Who needs to act, what should they do, and how do we know it got done?

Why most organizations can't do this alone

Specialist skills. Intelligence analysis is its own discipline. Handing it to an already busy SOC as a part-time task dilutes both jobs and burns people out.

Tools and data. A working program needs a threat intelligence platform, collection across the open, deep and dark web, attack surface visibility and integration with the security stack. Assembling and maintaining that is expensive.

Time. Recruiting, hiring and training analysts takes months before they produce intelligence that is specific to the organization and ready to act on.

Why providers are positioned to deliver it

MSSPs, MSPs and consultancies already hold the relationship, the context and often the telemetry. Adding threat intelligence turns that position into a differentiated, recurring service line: one that answers the questions customers are already asking, connects to the monitoring and response you already provide, and gives every renewal a clear story of progress.

> The challenge is delivering it at scale. Every customer has different assets, exposures, stakeholders and requirements. A managed CTI service only works if one team can run a tailored program for each customer without rebuilding it each time.

What a managed CTI service can deliver

Start with a focused offering and grow it, or deliver a complete intelligence program. With Morado, every service below runs from the same multi-tenant platform, so you choose what each customer receives.

INTEL OPERATIONS

Priority threat alerts

Timely warnings about the threats that can't wait, filtered to each customer's industry, technologies and threat profile.

DIGITAL RISK PROTECTION

Dark web and credential monitoring

Leaked credentials, infostealer logs, ransomware leak sites and marketplace listings tied to each customer, with credential validation workflows.

DIGITAL RISK PROTECTION

Brand and executive protection

Lookalike domains, impersonating social accounts, fake apps and executive exposure, with takedown support.

EXPOSURE MANAGEMENT

Exposure management and CTEM

Discovery, live validation of exploitability, drift tracking and threat context to prioritize remediation, then rescans to verify fixes.

DIGITAL RISK PROTECTION

Third-party intelligence

Breaches, ransomware listings and exploited vulnerabilities at each customer's suppliers and partners.

PHYSICAL SECURITY

Physical and travel risk

Conditions around facilities, events and executive travel, with camera integration, imagery and geopolitical intelligence.

INTEL OPERATIONS

Threat briefings and reporting

Recurring briefings, threat assessments and executive summaries, delivered under your brand.

INTEL OPERATIONS

RFIs and on-demand intelligence

Customer stakeholders ask questions and get analysis of what they are seeing, inside the platform.

INTEL OPERATIONS

Hunts and detection coverage

Retrospective hunts for new indicators in each customer's SIEM, and gaps between actor TTPs and their detections.

INTEL OPERATIONS

Program maturity

A CTI-CMM assessment for each customer that shows where their program stands and how it improves over time.

Labels show the Morado module behind each service. Alerts, News Stream, Agentic Workflows and Stakeholder Accounts work across all four.

Running the intelligence lifecycle for every customer

A managed CTI service follows the same lifecycle as an in-house program: plan, collect, process, analyze, deliver and learn from feedback. The difference is that you run it for many customers at once. Morado keeps each customer's lifecycle separate, in its own tenant, while your team works from a single login.

01 **Planning & direction** Define what each customer needs to know.	• A threat profile per customer: industry, technologies, locations, third parties and executives • Stakeholders who receive reporting and raise RFIs	• Priority Intelligence Requirements and supporting requirements • Assets, domains, IP ranges, brands and keywords to monitor
02 **Collection** Bring each customer's data and Morado's together.	• The customer's own tools: SIEM, EDR, vulnerability scanners and feeds • Threat feeds and news sources, collecting from day one	• Morado's scans: attack surface, validation, dark web, brand, executives • 30+ integrations with the tools customers already run
03 **Processing** Turn raw data into usable intelligence.	• Normalization across every source • Scoring and deduplication of indicators	• Enrichment with attacker context • STIX 2.1 ingestion and export
04 **Analysis & production** Connect threats with each customer's environment.	• Correlation of threats with the customer's exposures • Morado AI to assess relevance, with evidence visible	• Hunts, TTP coverage checks and vulnerability validation • Investigations that bring findings from every module together
05 **Dissemination & feedback** Get intelligence to the people who act on it.	• Reports and briefings under your brand • Customer tasks in your ticketing or ServiceNow	• Stakeholder accounts for feedback and RFIs • IOCs pushed to each customer's SIEM

> Feedback closes the loop. Stakeholder ratings, RFIs and each customer's CTI-CMM results update the threat profile and requirements, so the service gets more relevant the longer it runs.

Built for providers

Morado is fully multi-tenant across all four modules: Intel Operations, Digital Risk Protection, Exposure Management and Physical Security. Deliver individual capabilities or a complete intelligence program to each customer.

Separate customer tenants

Each customer has its own tenant for assets, intelligence, findings, investigations, reports and workflows. See every customer in one console and work one at a time.

Your brand, your customers

Deliver co-branded or powered by Morado, so customers see your name first. Full white-label is available on request.

Customers inside their tenant

Invite customer users, set access and export levels for each one, and tailor the modules and features each customer receives.

Analysts to extend your bench

Morado analysts work inside the platform: validated findings, RFI responses, dark web investigations and takedowns, without hiring.

Automation that scales

Agentic workflows run repeatable work for every customer, from credential validation to a full third-party breach investigation, with a human in the loop.

Connected to delivery

Send findings to your ticketing or ServiceNow, push IOCs to each customer's SIEM, and track each customer's CTI-CMM trend line.

Three ways to deliver

Choose the model that fits your team today, and change it as your service line grows.

MSSP delivers

Your analysts triage and respond for every customer from one console, with per-customer views, tasks and reporting.

MSSP with Morado analysts

Our analysts extend your bench on customer work: validated findings, reports, RFI responses and takedowns.

Consultancy

Add threat intelligence to your engagements, with customizable reports and Morado analysts supplementing your team.

Getting started

1. **Define your service catalogue**
   Choose the services you will offer, from a focused offering such as dark web and credential monitoring to a full intelligence program, and how each is packaged.
2. **Set up your platform and brand**
   Configure your provider console, branding and delivery model, and connect your ticketing and the tools your team uses.
3. **Onboard each customer**
   Create the customer's tenant and threat profile, add their assets, executives and third parties, and connect their SIEM, EDR and scanners.
4. **Deliver, report and improve**
   Run monitoring, investigations and briefings, collect stakeholder feedback, and show progress with each customer's CTI-CMM results. Bring in Morado analysts whenever you need more capacity.

What to measure

New revenue
A threat intelligence and exposure service line without building a platform.

Customers per analyst
Per-customer views from one login, so one team serves more customers.

Renewals
A CTI-CMM progress story for each customer that makes renewals easier to defend.

Time to launch
One platform with 30+ integrations, launched under your brand.

These are the measures MSSPs track. We scope your baseline with you.

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

Launch your threat intelligence service line.
Talk to us and see the multi-tenant platform your customers will use.

sales@morado.io
morado.io/platform/mssp