Cyber Threat Intelligence
as a Service

How security teams can benefit
from a managed service approach to Cyber Threat Intelligence

https://www.linkedin.com/company/morado-intelligence

www.morado.io

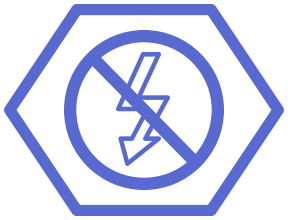
© Morado Intelligence, LLC / All rights reserved.

Benefits of Cyber Threat Intelligence

Cyber Threat Intelligence helps security teams defend against attacks that may target their environment. By analyzing what tactics attackers and threat groups are using, organizations can better prioritize their security goals. Security teams that understand the threats they are most likely to face in their environment are able to put the most efficient detection and deterrent capabilities in place, allowing them to effectively mitigate those threats ahead of time.

63%
Faster resolution of security threats [1]

32%
Overall more efficient cybersecurity teams [1]



86%
Reduction in unplanned downtime [1]

34%
Less staff time compiling security reports [1]

The Demand for Cyber Threat Intelligence is Increasing

Zero-day attacks are rare. 98% of attacks are conducted using known vulnerabilities, which means the data is available if you know what to look for. Knowing which vulnerabilities are being actively exploited allows security teams to target the threats that matter most to their organization. This has created an increased demand from companies that are looking to add full-time Cyber Threat Intelligence Analysts to their security teams to help find the most relevant data for their organization.

98%
Of attacks are conducted using known vulnerabilities [2]

25,000+
Active Cyber Threat Intelligence related job openings [4]

© Morado Intelligence, LLC / All rights reserved.

Costs of Building a Cyber Threat Intelligence Team

Overhead

In order to effectively produce Cyber Threat Intelligence (CTI), a security team needs manpower, tools and data. A CTI Analyst is a specialized role that requires a specific skillset, different from that of other security team members. The average compensation for a CTI Analyst is $121K per year. In addition, an analyst will need a Threat Intelligence Platform (TIP) to monitor and curate intelligence data. Licensing costs for most TIPs vary depending on the number of users and typically range between $100K & $500K per annum. Additionally, intelligence data is necessary for your TIP to produce effective, curated intelligence. High-end data feeds can cost up to millions of dollars per year. [2] [3]

Misaligned Expertise

Some organizations choose to get a TIP and utilize their existing security team to manage the platform. This can cause the analyst to feel overburdened and lead to burn out. Cyber Threat Intelligence operations include numerous tasks that require advanced skills, and should not be treated as a part-time or secondary job function.

Time

Recruiting, hiring and training a CTI analyst can take months before they're fully up to speed and producing actionable intelligence. If the CTI responsibilities are treated as an operational task, they dilute overall team effectiveness. Adding additional responsibilities can take time away from the other requirements a security team may have, and will require additional specialized training and experience to operate properly.

Advantages of Managed Cyber Threat Intelligence

Lower Cost Burden

Rolling out an in-house Cyber Threat Intelligence team can be cost prohibitive for some companies. Because of this, organizations will often cut corners in the name of the bottom line. Managed CTI as a service prevents an organization from having to purchase a Threat Intelligence tools, hire a team of CTI analysts, and figure out what data feeds to pay for. When enrolling in this type of program, clients can expect to get actionable CTI at a fraction of the cost.

Specialized Expertise

As the industry of cybersecurity continues to widen, tasks are increasing in difficulty and volume as more areas of expertise are introduced. Cybersecurity analysts are required to understand numerous technical concepts and are expected to be subject matter experts in various roles. Due to the depth of knowledge required to conduct full scale Cyber Threat Intelligence operations, having a trained Cyber Threat Intelligence specialist will increase the efficacy of the overall program.

Experts on Day One

Building out an internal team can take months. By implementing the Managed Service model, organizations have access to a team of trained CTI experts that will produce actionable intelligence specific to their organization immediately.

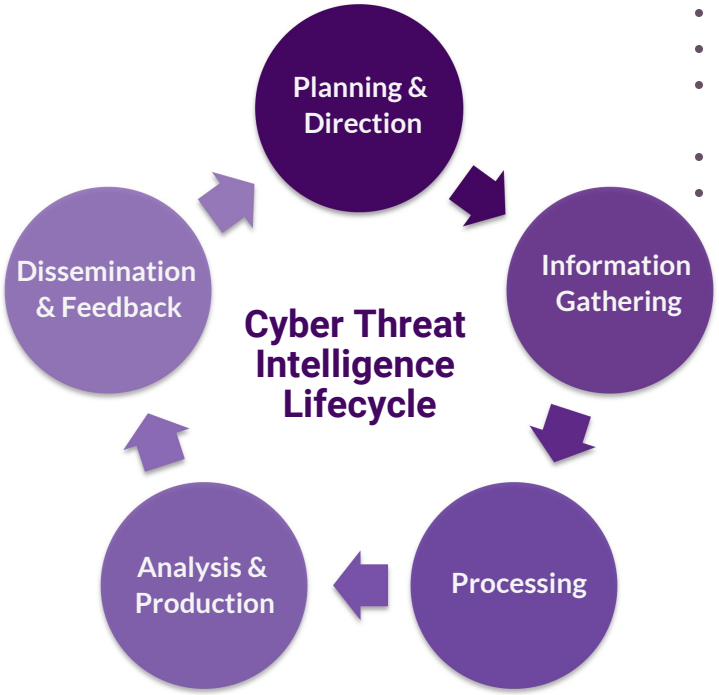
© Morado Intelligence, LLC / All rights reserved.

Our Process

Planning & Direction
Construct Threat Profile
- Organizational infrastructure
- Vertical market/industry
- Size
- Location
- Scope / reach
- Vendors/ partners
- International presence
- Employee risk
- Time to recovery
- Outage cost

Information Gathering
- Technical & human intelligence
- Data feeds
- Honeypot & dark-web intelligence gathering
- Curated OSINT sources
- Vulnerabilities based on infrastructure

Dissemination & Feedback
- Ongoing Threat Briefings
- Action items
- Recommendations
- Customer feedback
- Threat profile updated



Analysis & Production
- Sorting and prioritization
- Scored based on established risk
- Determine threat maturity & current level of exploitation
- Predictive efforts
- Forecasting

Processing
- Curation and contextualization
- Establish attack chain relationships
- MITRE ATT&CK Framework alignment
- Vulnerability analysis

© Morado Intelligence, LLC / All rights reserved.

CTI Technology Management - We utilize a suite of intelligence tools and technologies in order to provide our clients with customized intelligence relevant to their organization.

Priority Threat Alerts - Receive alerts for the threats that can't wait. We aggregate customized threat intelligence data for organizations to quickly provide clients with high-impact alerts warning them of the most dangerous threats that require immediate attention.

On-Demand Intelligence - Our analysts are available to provide CTI-informed contextual analysis of real-time observables a client may see in their environment.

Comprehensive Threat Briefings - Our analysts meet with clients on a regular basis to help walk them through the threats most relevant to their organization and provide personalized feedback on their security strategy.

Exploitable Vulnerability Prioritization - Over 98% of attacks are conducted using known vulnerabilities. Using a combination of novel threat intelligence tools, hybrid technology, and proven tradecraft methods, we provide our clients with comprehensive prioritization of the vulnerabilities that are most likely to cause damage to their organization. [2]

Dark Web Monitoring - The dark web serves as an anonymous place for threat actors to collaborate and exchange illicit information. Morado monitors the dark web for mentions and or relevant leaked client data. Our team analyzes the data and provides actionable insights and recommendations in real time.

© Morado Intelligence, LLC / All rights reserved.

Conclusion

Threat Actors are becoming more confident, bold, and technologically advanced. Finding and prioritizing the most critical security data is a difficult and expensive task. CTI helps organizations protect their critical infrastructure by providing security teams with more knowledge about the threats that matter most to their organization.

Security teams are awash with a constant flow of data. Streams of unfiltered indicators, IP blacklists, bad domains, malicious file hashes, are constantly blasted through a firehose. Contextualizing the stream of unfiltered data is hard. It requires a dedicated, knowledgeable team with the time and skill to make the threat data actionable within the context of an organization's security environment.

Many organizations find that doing Cyber Threat Intelligence correctly can also be prohibitively expensive. It requires expensive tools and knowledgeable experts to make the data actionable.

Morado solves these problems by providing the expertise and the tooling, while being a one-stop source for actionable Cyber Threat Intelligence. Morado does it all at a cost that fits the tight operational budget of a typical cybersecurity team.

About Morado

Morado Intelligence is a Veteran-owned Cyber Threat Intelligence agency headquartered in San Diego, CA, that helps streamline cyber defense efforts by effectively identifying and prioritizing cyber threats. Morado acts as a work-reducer for any cybersecurity team; providing customized Cyber Threat Intelligence, cybersecurity framework alignment, and ongoing cybersecurity enhancement recommendations.

Get in touch with our team of experts to discuss how Morado can help strengthen your security posture.

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

Contact Us: morado@morado.io

https://www.linkedin.com/company/morado-intelligence

www.morado.io

Sources
[1] Recorded Future
[2] Gartner Group
[3] Salary.com
[4] ZipRecruiter

© Morado Intelligence, LLC / All rights reserved.