Cyber Threat Intelligence (CTI) Maturity Assessment

Evaluate and evolve your capability to proactively defend against cyber threats

The Value of Threat Intelligence

In today's threat landscape, threat intelligence is vital to moving from reactive defence to proactive security operations. Yet many organisations struggle to turn data into actionable outcomes.

Threat intelligence transforms your security posture from reactive to proactive. It enables your organisation to:

- **Identify vulnerabilities early** – Gain advanced warning of exposures so you can mitigate before attackers exploit them.
- **Understand attacker methods** – Get insights into threat actor behaviours and tools, enabling faster, more informed response.

It's estimated that detecting and responding to threats costs three times more than preventing them. Investing in threat intelligence isn't just strategic – it's cost-effective defence.

Does This Sound Like You?

- You receive threat intelligence but don't know how to operationalise it.
- Your security strategy isn't clearly aligned to current threats or business risk.
- Threat intelligence reports are siloed and underused.
- Business leaders question the ROI of your threat intelligence investments.
- You're unsure how mature your threat intelligence function really is – or where to start improving.

Why Act Now?

Cyber threats are growing in volume, velocity, and sophistication—waiting to mature your threat intelligence capability means staying reactive, not resilient.

A well-structured threat intelligence function enables faster, more informed decisions, reduces risk exposure, and improves operational efficiency. Acting now positions your organisation to stay ahead of emerging threats, reduce unnecessary costs, and deliver measurable security outcomes aligned to your business goals.

The sooner you start, the sooner intelligence becomes your advantage.

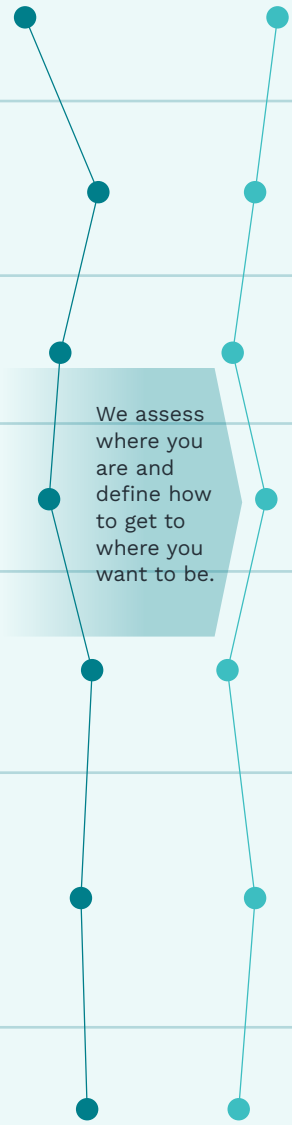
Adarma's Solution

Our Cyber Threat Intelligence Maturity Assessment follows a proven three-phase approach designed to deliver clear insights and actionable outcomes:

1. **Discovery** – We engage with your team to understand your threat intelligence objectives, evaluate current capabilities, and identify key strengths and areas for improvement.
2. **Analysis** – We assess the alignment of your threat intelligence efforts with broader business and security goals, benchmark maturity against industry frameworks, and pinpoint gaps that impact effectiveness.
3. **Report & Roadmap** – We deliver a comprehensive report including an executive summary, maturity benchmark, and a costed, prioritised roadmap to help you evolve from your current state to your desired level of maturity.

The result is a strategic plan to transform your threat intelligence function into a more integrated, proactive capability – ready to enable smarter security decisions and better defend your organisation.

Cyber Threat Intelligence (CTI) Capability Framework	Description	Minimal, Ad Hoc	CTI Maturity	Optimised
CTI Charter	Outlines the purpose of CTI team and how it interacts with the business, supports the long-term vision and enables growth.	CTI team objectives ill-defined or loosely coupled to business.		CTI objectives are clearly defined and consistently aligned with evolving business priorities.
Governance & CTI Management	Ensures structural support is in place for the CTI team to perform. Provides consistency across processes and performance management.	Ad hoc processes and business interaction. ROI not measured.		Processes documented. CTI drives security strategy, policies and assurance.
Direction	Team direction aligned to CTI Charter, prioritised business objectives and intelligence requirements.	Infrequent, inadequate assessment.		Defined, regular review of direction with all relevant stakeholders.
Collection & Processing	Ensures threat data coverage is sufficient to answer the intelligence requirements set by the business.	CTI limited to IOC feeds that supply preventative controls.		Threat data relevant to risk management objectives collected from necessary internal and external sources.
Analysis	Ensures that the processes and tools used to analyse the collected threat data are sufficient to create actionable insights that meet the intelligence requirement.	Reactive, slow to produce, unreliable, limited actionable CTI, lack of insight.		Proactive, analytics and AI used to create accurate, validated, actionable CTI.
Dissemination	Ensuring CTI is integrated into operational workflows (e.g., incident response or threat hunting) such that it is delivered on time to the relevant stakeholders, in the appropriate form.	CTI late, unintelligible and lacks clear insight or actions.		Consistent, real-time reporting customised to business and technical audiences delivering actionable intelligence, enabling organisations to stay one step ahead of the threat.
Feedback	Ensures the CTI team receives feedback of sufficient quality to improve performance and respond to new requirements.	Limited or no feedback or directional guidance.		Data-driven KPIs continuously monitored, CTI drives adaptive security



BENEFITS:

Improve your ability to detect, prevent and deter cyber-attacks by:

- Anticipating and responding to new threats and vulnerabilities deters a majority of cyber-attacks[1].
- Organisations can reduce their overall risk exposure by up to 25% through better threat intelligence and proactive measures to deter attacks[2].
- Mature threat intelligence programs can improve threat detection rates by up to 40%, leading to fewer false positives and more accurate identification of genuine threats[3].
- Organisations can achieve better compliance with cybersecurity regulations, reducing the risk of fines and penalties by up to 15%[4].
- Streamlining processes: enabling automated threat analysis and response can lead to a 20% increase in operational efficiency[5].
- Preventing successful attacks and minimising the impact of incidents. Organisations can save on average 30% in costs related to data breaches and recovery efforts[6].
- Organisations with mature threat intelligence capabilities can respond to threats more quickly, reducing the average incident response time by up to 50%[7].

Success Stories

Adarma has helped organisations across a range of regulated sectors to deter and prevent attacks with a more effective threat intelligence capability. Here are some examples:

Global Retailer

Adarma helped establish an intelligence-led security strategy that aligned threat intelligence with incident response, increasing detection fidelity and executive reporting visibility.

Read the case study

Global Insurer

Our team developed threat-driven detection and response rules to secure 300+ applications, improving threat visibility across a complex enterprise environment.

Read the case study

1 https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024
2 https://www.mdpi.com/2079-8954/13/1/52
3 https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-maturity-assessment/
4 https://www.nccgroup.com/us/should-your-organization-independently-assess-cyber-security-maturity/
5 https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-maturity-assessment/
6 https://www.mdpi.com/2079-8954/13/1/52
7 https://www.nccgroup.com/us/should-your-organization-independently-assess-cyber-security-maturity/

Why Customers Choose Adarma

In a cyber security market where quality is hard to measure, organisations trust Adarma for our consistency, credibility, and results.

Here's why:

Unmatched Expertise
We are accredited to deliver SOC-CMM assessments and have deep experience in intelligence-led operations.

Technology-Independent
We deliver outcomes, not licenses. You get independent advice tailored to your needs.

UK-Based Delivery
Our consultants work on-shore, ensuring close collaboration and compliance alignment.

Proven Track Record
Trusted by FTSE 350 organisations and regulated industries to deliver critical, high-impact results.

Meet the team

Leanne Salisbury

Principal Consultant – Threat Intelligence Maturity

Leanne brings over 20 years' experience in Threat Intelligence and Cyber Security, including roles in the Royal Air Force and in regulatory-driven red teaming (TIBER-EU & ICAST) across Europe and Asia. Her focus is enabling security teams to transition from reactive defence to proactive operations.

Connect with Leanne on LinkedIn

> **"Threat intelligence should empower security teams to make faster, smarter decisions. It should be actionable, aligned to business priorities, and embedded into operations."**

Who We Are

Adarma is a trusted partner in security consulting and co-managed security operations. We work as an extension of your team to help simplify operations, build resilience, and deliver measurable outcomes.

We specialise in 24/7 threat detection, investigation and response, security consulting, and engineering support for large, complex organisations in high-risk sectors. Our platform, Socket, enhances automation, insight, and orchestration – empowering teams to act faster and more decisively.

Technology-independent and customer-led, we integrate with platforms like Microsoft, Splunk, CrowdStrike and Google SecOps to maximise the return on your security investments. Together, we build stronger business resilience and deliver measurable security outcomes that matter.

Ready to Enhance Your Threat Intelligence Maturity?

Book a discovery session with one of our solution consultants and receive a complimentary Threat Landscape Report tailored to your industry.

Book a consultation