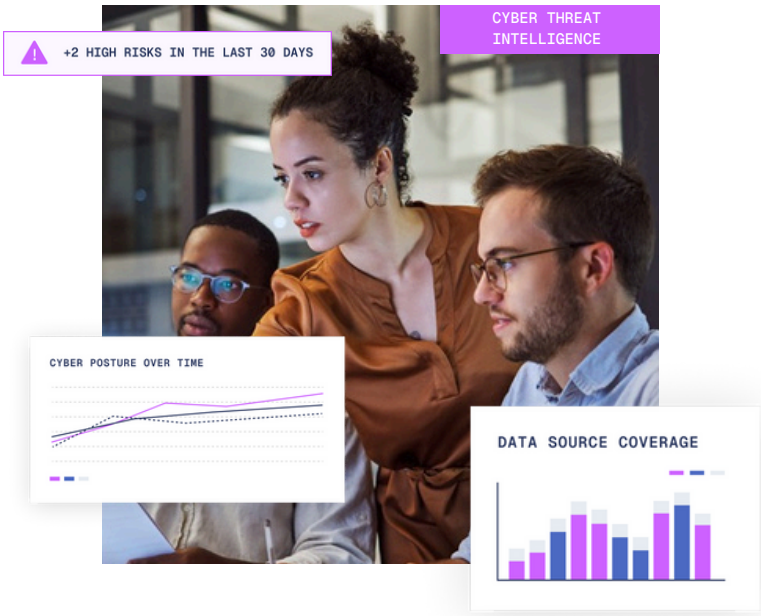
Cyber Threat Intelligence | CTI

- Clear and concise early warnings on threats relevant to your organisation
- CTI is essential for moving away from a reactive and towards proactive defences
- Enrich alerts and investigations regarding threat actors and likely attack patterns



What you can expect from Vambrace Cyber Threat Intelligence

Our CTI analysts work closely either with your own or our managed SOC to surface a real and complete picture of your threat landscape, trigger early warnings on emerging threats, present usable and actionable intelligence for threat-hunting, and create custom detection analytics.

The challenges for in-house teams: when it comes to CTI are substantial

Data that cannot be quickly contextualised is useless for in-house teams. Hours can be lost struggling to filter what is / not relevant from what is out of date or current.

- Keeping up with the latest TTPs requires around-the-clock monitoring.
- Raw data contains false positives and outdated indicators that eat up valuable time and resource.
- CTI analysts who understand adversary tactics and malware techniques are hard and expensive to acquire and retain.

Get early warnings on emerging threats, and cyber group activity.

Access people with the skills you need to achieve the coverage you require at a realistic price.

We filter and tailor intelligence to your industry, assets, tech stack, and threat profile.

CTI shapes big decisions on risk, compliance, and investment priorities, so we always go light on the jargon in our reports.

For a clearer view of cybersecurity

Click here to start your journey

vambrace

vambrace.co.uk

Why quality Cyber Threat Intelligence matters

CTI mapped to the MITRE ATT&CK framework

Providing teams with useful, usable intelligence when they need it via concise bulletins feeding directly into your SIEM, SOAR, and EDR solutions.

- Our intelligence is gathered from global feeds, dark web monitoring, malware analysis, and industry sources.
- We validate & enrich via our CTI analysts who remove false positives, contextualise findings, and ensure they are relevant to you before linking them to MITRE ATT&CK techniques.

It is a key driver for ROI on security spend

Instead of viewing it as an expense, CTI should be seen as adding value for security and business leaders, helping them get more from the tools they already have.

- Instead of investing in a new tool for every potential scenario, or trying to patch every vulnerability, CTI helps teams prioritise based on real attacker behaviour.
- CTI demonstrates proactive risk management and monitoring, which helps satisfy requirements for information security standards including PCI DSS, SOC 2, and ISO 27001

CTI helps deliver realistic and relevant training

Possessing up to-date knowledge of attacker tactics and techniques means you can up-skill teams faster using real and relevant threats.

- We feed indicators of compromise into your SIEM so your analysts can practice detecting, correlating, and responding to them in a safe environment.
- We highlight how recent attacks unfolded, so your teams can trial different response workflows against documented attack chains.

For a clearer view of cybersecurity

Click here to start your journey