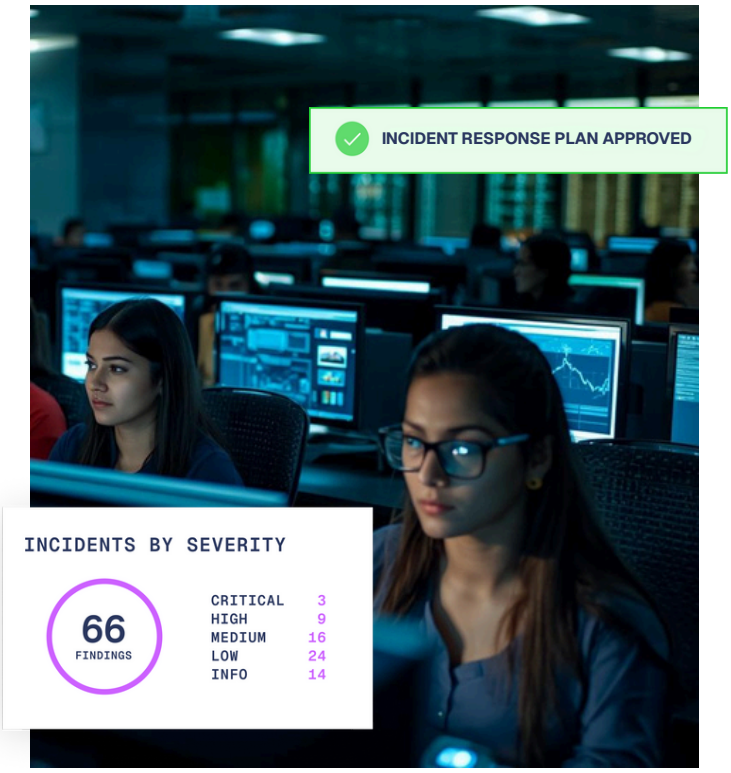
Cyber Incident Response | IR

- A full-service covering cyber incident planning, response, containment, and recovery
- Rely on a team with experience against every type of cyber-attack
- Our tailored plans and playbooks enable clear communication when it matters most

The Vambrace difference during a cyber-attack

The first few hours of a cyber-attack are critical. It should not be the trigger to start searching for an incident responder or creating response plans. Our elite and experienced cyber incident response team deliver a clear, calm, and trusted service when it really matters.



- A focus on rapid response and containment
- We leverage AI to quickly enrich data, drive intelligence, and identify patterns in attacker tactics
- Support from SIEM and SOAR operations, CISO level consultants, and Threat Intelligence analysts
- Forensic investigators remove hidden implants that are used to initiate follow-up attacks
- Return to normal as soon as possible with our incident remediation service

> It's refreshing to have real face-to-face conversations with the team instead of just emails or calls about contracts. Their openness and willingness to travel to meet us and discuss our needs in detail makes a huge difference. I have no concerns, only confidence.

Click here to start your journey

Preparation: The difference between a successfully contained incident and a major breach

The first time a cyber incident response plan is tried out should not be on the day of an attack. Our team thoroughly prepares organisations by testing the effectiveness of planning, the clarity of policies, and robustness of communication channels through:

Tabletop exercises

Discussion based sessions focusing on team roles, responsibilities, and communication in line with your IR plan for pre-agreed scenarios.

Ideal for organisations:

- Early in their incident response maturity, and need to validate plans on paper before progressing to technical drills.
- With leadership that need to experience decision-making under pressure.
- Operating in heavily regulated sectors where compliance and communication strategies are as important as technical actions
- With proactive teams with an appetite for identifying gaps in current plans without disrupting live systems.

Live play scenarios

Real-time sessions where participants execute their roles in response to controlled feeds of information representing a pre-agreed scenario.

Ideal for organisations:

- Who have existing security operations capabilities in house.
- Who maintain dedicated test environments where attacks can be safely simulated
- Who need real world validation of detection and response capabilities and containment workflows
- With proactive teams who understand the need to stress-test integrations between security tools, threat intel feeds, and automated response playbooks.

Proactive incident planning

We help you prepare by forming and testing, highly effective incident response plans and simulated scenarios based on the latest threat intelligence to reduce the impact of a future attack.

Rapid incident response

When an attack hits, our top priority is to stabilise the crisis fast by understanding what has happened as we move to protect and restore critical systems.

Post incident forensics and remediation

Our detailed sweeps show how attackers bypassed defences while surfacing hidden and dormant implants that could be used for follow-up attacks.