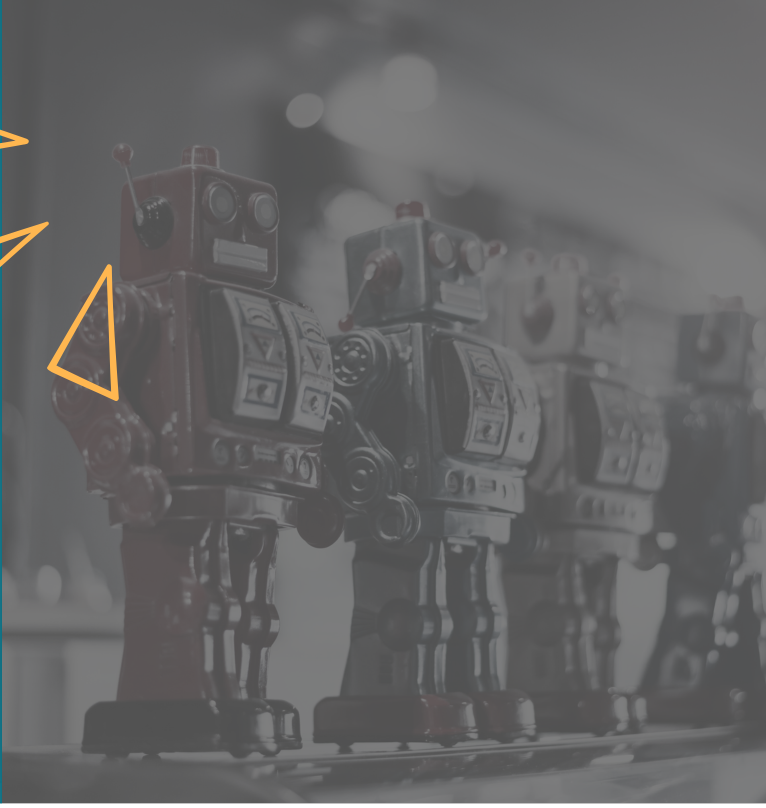
INCIDENT RESPONSE THAT WORKS UNDER PRESSURE

Frontline lessons for faster containment and safer recovery



Most organisations have an incident response (IR) plan.

Very few discover whether it actually works until they're already under attack.

When a real incident hits, we repeatedly see the same pattern:

Plans that looked solid on paper collapse under pressure.

Decision-making slows. Evidence disappears. Well-meaning teams accidentally help the attacker.

And valuable time is lost while people argue about what they're "allowed" to do.

BOARDS EXPECT CONTROL, NOT PERFECT INFORMATION

This paper draws on real-world incident response experience to highlight where IR plans most commonly fail, why those failures matter and what organisations can do now to close the gaps.

THE LESSONS NOBODY WANTS TO LEARN DURING A LIVE BREACH

There are some things you really don't want to figure out mid-incident:

- Who has authority to shut systems down
- Whether logs are still available
- Whether the help desk can safely reset credentials
- Whether security teams are allowed to act without business sign-off

Yet for many organisations, that's exactly when these questions surface.

We routinely see:

- Systems rebuilt before forensic evidence is preserved
- Credentials reset in ways that give attackers fresh access
- Cloud activity going completely unseen
- Teams working in silos while the attacker moves freely

None of these are technology problems. They are planning, ownership, and rehearsal problems, and with the right planning, can be avoided when it matters.

THIS IS NOT ABOUT FEAR.
IT'S ABOUT READINESS.

THE HIDDEN GAPS THAT BREAK IR PLANS

1.

EVIDENCE DISAPPEARS BEFORE THE INVESTIGATION EVEN STARTS

One of the most common and costly mistakes is losing forensic evidence in the rush to “fix” the problem.

Examples include:

- Logs overwritten due to short retention periods
- Servers rebuilt before evidence is collected
- Cloud audit data not retained or not enabled at all

Without evidence, teams are forced to guess. Guessing leads to incomplete remediation, repeat compromise, and uncomfortable conversations with regulators, insurers, and customers.

WHAT GOOD LOOKS LIKE

- Security and forensic teams are always consulted before systems are wiped or rebuilt
- Critical logs are retained for long enough to support investigation
- Evidence preservation is built into response playbooks, not treated as an afterthought

2.

SILOED TEAMS SLOW EVERYTHING DOWN

In many organisations, security detects incidents but does not control the systems needed to contain them.

During a breach, this leads to:

- Delays waiting for approvals
- Conflicting priorities between uptime and containment
- Fragmented investigations across business units

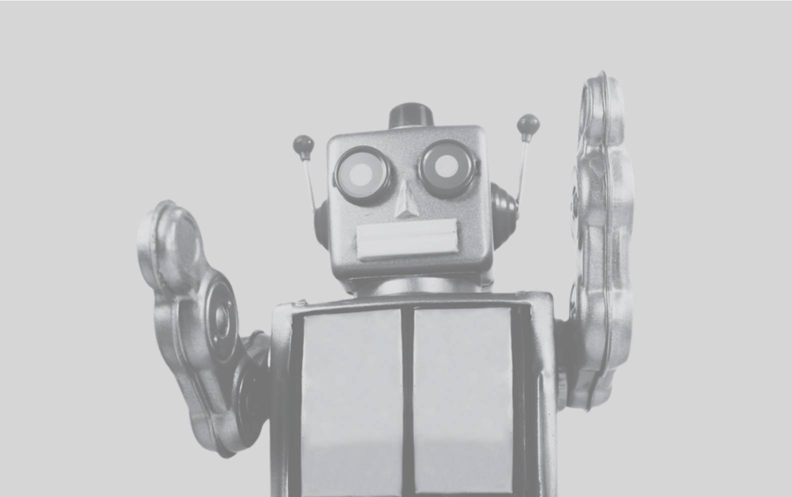
Attackers benefit from every minute of hesitation.

WHAT GOOD LOOKS LIKE

- Clear authority for security teams during incidents
- Pre-agreed escalation paths
- Shared understanding that short-term disruption may be necessary to prevent long-term damage

80% **of incident impact is driven by response decisions**

RESPONSE EXPERIENCE THAT STANDS UP UNDER PRESSURE



PLAN, OWN, TEST

3. THE HELP DESK BECOMES AN ACCIDENTAL ATTACKER ALLY

Help desks are trained to help. Attackers know this.

We commonly see incidents where:

- Credentials are reset without strong identity verification
- MFA protections are weakened "temporarily"
- Self-service password resets are abused

These actions often undo containment efforts and give attackers fresh access.

WHAT GOOD LOOKS LIKE

- Strong identity verification for credential and MFA resets
- Escalation requirements for high-risk requests
- Clear guidance on what not to do during an active incident

4. BLIND SPOTS ACROSS IDENTITY, CLOUD, AND SAAS

Many organisations still focus incident response almost entirely on endpoints. Attackers do not.

Common visibility gaps include:

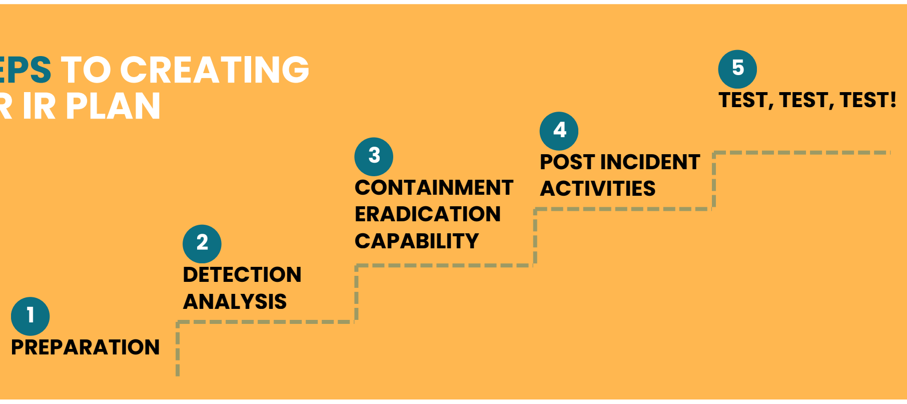
- Identity providers
- Cloud control planes
- Virtual infrastructure
- SaaS administrative activity

Without visibility across these areas, response teams are always reacting late.

WHAT GOOD LOOKS LIKE

- Centralised visibility across endpoints, identity, cloud, and SaaS
- Regular audits of logging, permissions, and conditional access
- No "trusted" areas that aren't monitored

5 STEPS TO CREATING YOUR IR PLAN



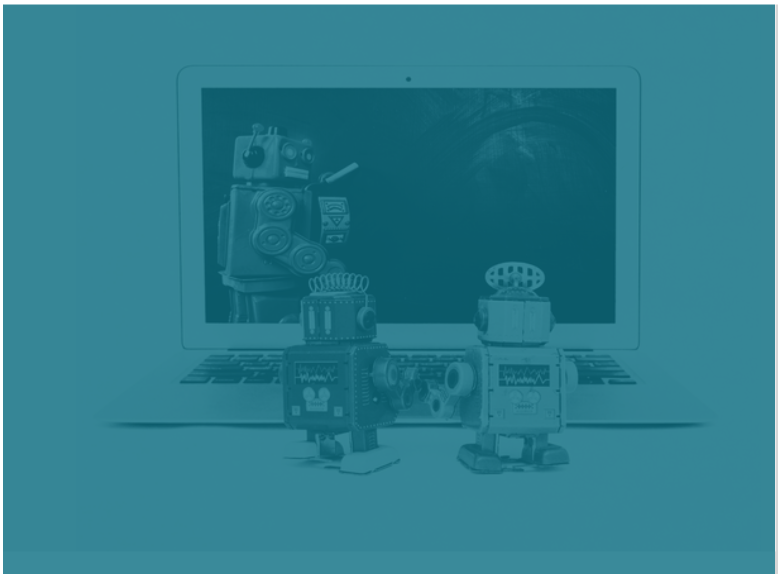
1 PREPARATION

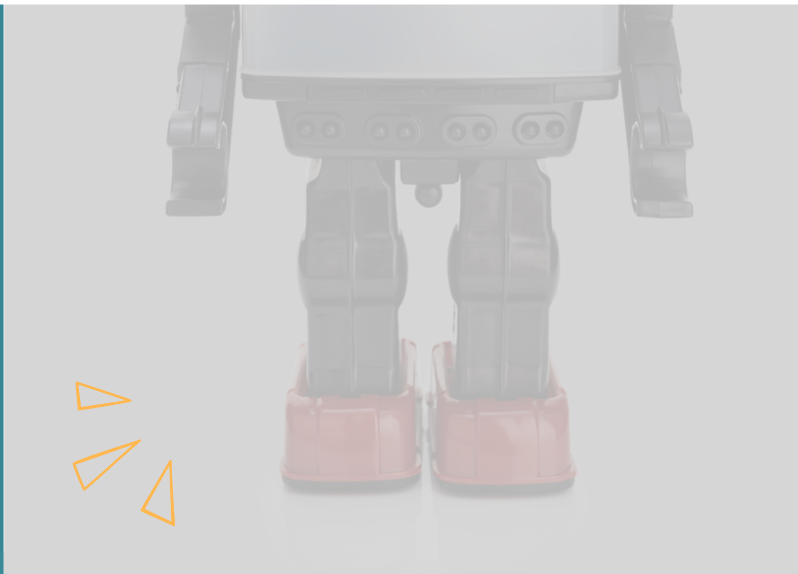
2 DETECTION ANALYSIS

3 CONTAINMENT ERADICATION CAPABILITY

4 POST INCIDENT ACTIVITIES

5 TEST, TEST, TEST!





5. CLOUD PRIVILEGE WITHOUT OVERSIGHT

Cloud environments often accumulate risk quietly:

- Over-permissive roles
- Exposed storage
- Hard-coded secrets
- Unused but valid access keys

Attackers don't need exploits if they can simply log in.

WHAT GOOD LOOKS LIKE

- Regular configuration and permission reviews
- Secure storage of credentials and secrets
- Active monitoring of privileged activity

6. THIRD-PARTY ACCESS IS RARELY TREATED AS FIRST-CLASS RISK

Suppliers, partners, and service providers often have deep access—and limited oversight.

We regularly see:

- Shared accounts without MFA
- No session monitoring
- No clear ownership of third-party risk during incidents

WHAT GOOD LOOKS LIKE

- Strong access controls for third parties
- Security requirements embedded into contracts
- Clear response expectations when a supplier is involved in an incident

7. INSIDER THREATS SIT OUTSIDE MOST IR PLANS

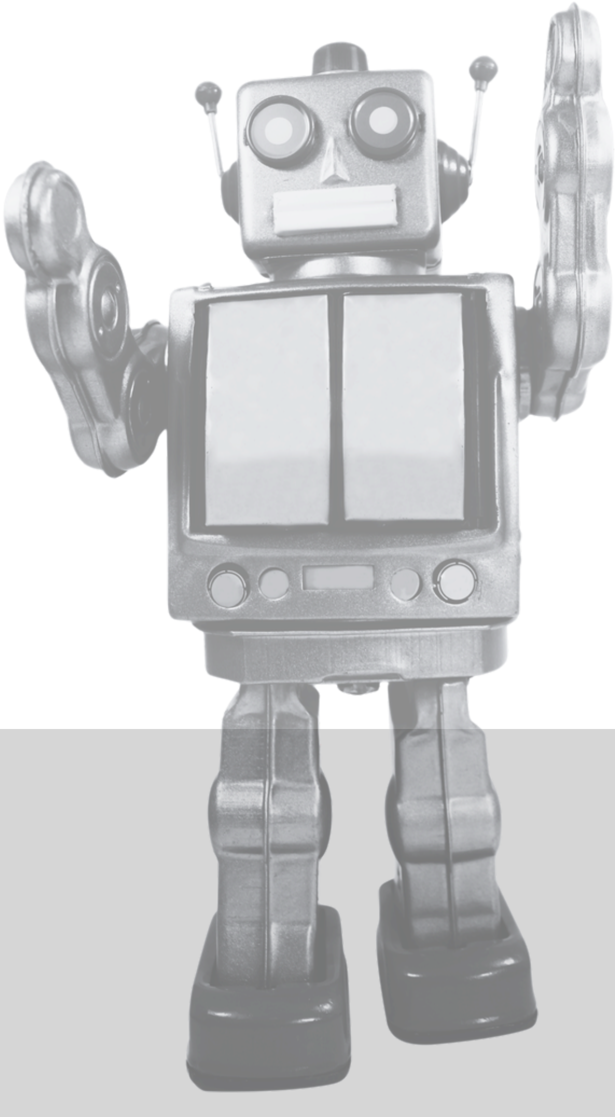
Whether malicious, coerced, or simply careless, insider threats are often missed entirely in response planning.

HR, IT, and security frequently operate in isolation, leaving gaps around:

- Vetting
- Monitoring
- Offboarding

WHAT GOOD LOOKS LIKE

- Coordination between HR and security
- Clear processes for rapid access revocation
- Monitoring for abnormal internal behaviour



CONFIDENCE THROUGH CLARITY,
PREPARATION AND EXPERIENCE

WHAT EFFECTIVE INCIDENT RESPONSE ACTUALLY LOOKS LIKE

START BROAD, THEN GO DEEP

Attempting to "image everything" slows response and increases cost.

Effective teams:

- Triage first
- Prioritise affected systems
- Focus forensic effort where it matters most

CONTAIN SURGICALLY, NOT DESTRUCTIVELY

The goal is not to rebuild everything—it's to cut off attacker access.

This means:

- Disabling compromised accounts
- Isolating affected systems
- Removing attacker persistence
- Hardening controls before restoring services

RESTORE DELIBERATELY, NOT HURRIEDLY

Recovery should reduce risk, not recreate it.

That includes:

- Coordinated credential resets
- Secure help desk processes
- Hardened rebuilds
- Implementing lessons learned immediately

Strengthening your readiness now (before you need it)

- You don't need an incident to improve.
- Practical steps include:
- Clearly defining decision-makers and authority during incidents
- Auditing visibility across endpoints, identity, cloud, and SaaS
- Rehearsing response actions under pressure
- Testing assumptions through realistic exercises
- Ensuring external response partners can access what they need quickly

FINAL THOUGHT

Plans only matter if they work under pressure.

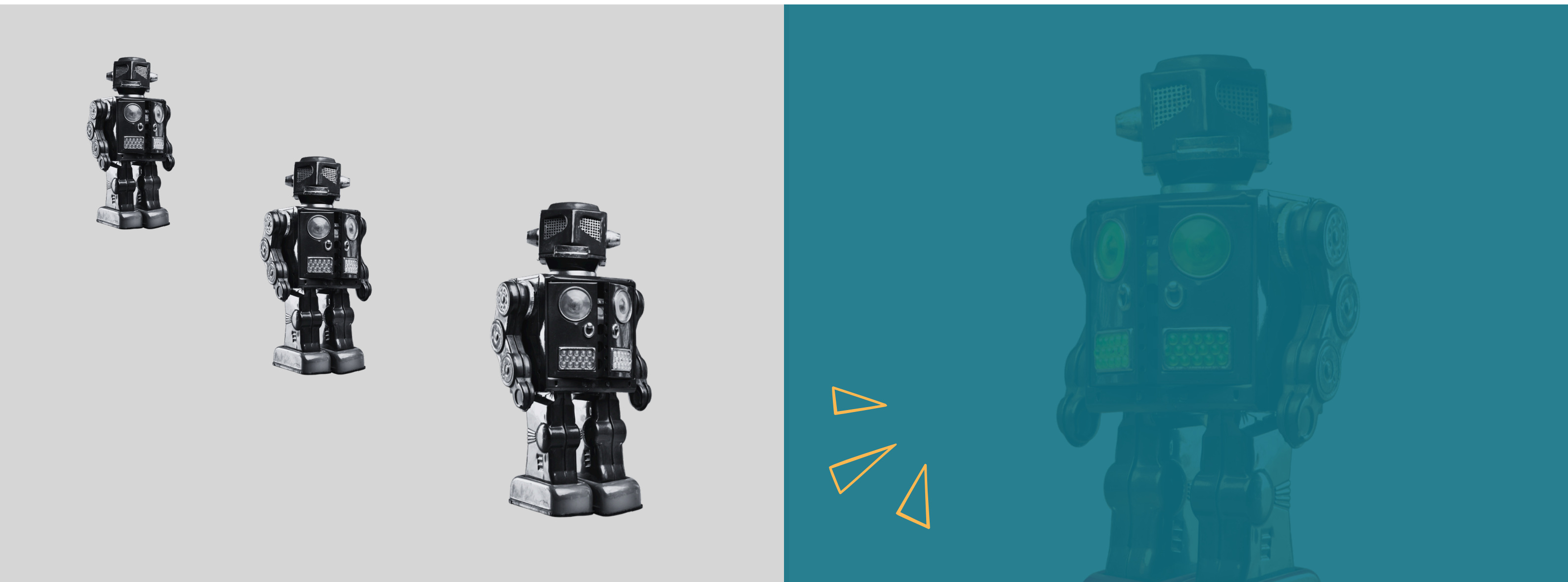
An incident response plan that hasn't been tested is an assumption, not a capability.

Prepared organisations:

- Expect the unexpected
- Practise difficult decisions in advance
- Accept that speed matters
- Empower teams to act

THE DIFFERENCE BETWEEN CHAOS AND CONTROL IS RARELY TECHNOLOGY.

IT'S PREPARATION.



INCIDENT RESPONSE READINESS CHECKLIST

USE THIS AS A SENSE-CHECK AGAINST YOUR CURRENT POSTURE:

PLANNING & AUTHORITY

□ Clear incident decision-makers defined
□ Security teams empowered to act without delay
□ Escalation paths agreed and documented
□ Business incident owner identified (not IT)
□ Authority to isolate systems agreed in advance

EVIDENCE & VISIBILITY

□ Logs retained long enough to support investigations
□ Visibility across endpoints, identity, cloud, and SaaS
□ Forensic preservation processes defined
□ Ability to reconstruct an incident timeline

PEOPLE & PROCESS

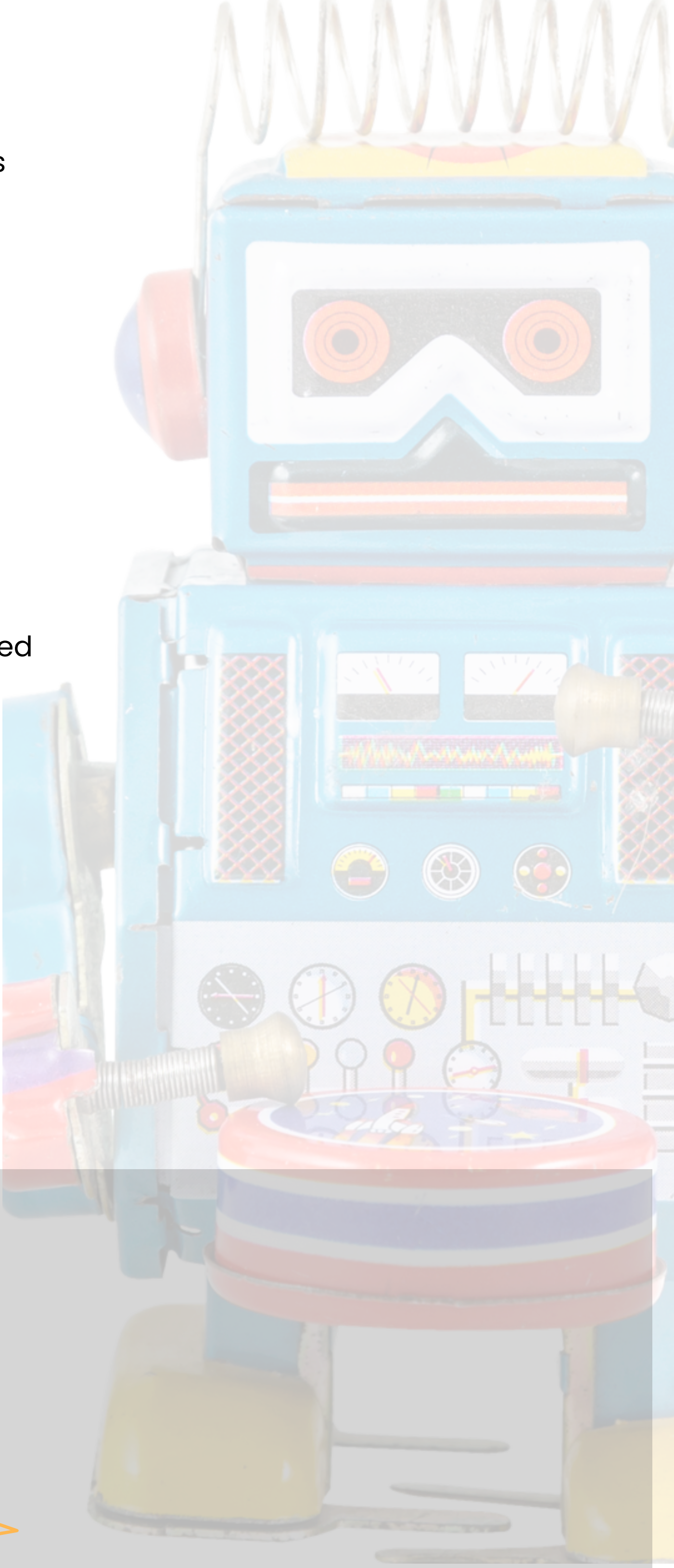
□ Help desk trained for incident scenarios
□ Strong identity verification for credential resets
□ Insider threat scenarios considered
□ HR, Legal and Comms roles defined for incidents

THIRD PARTIES

□ Supplier access reviewed and controlled
□ Contracts include security and incident obligations
□ Third-party incident notification requirements defined

TESTING

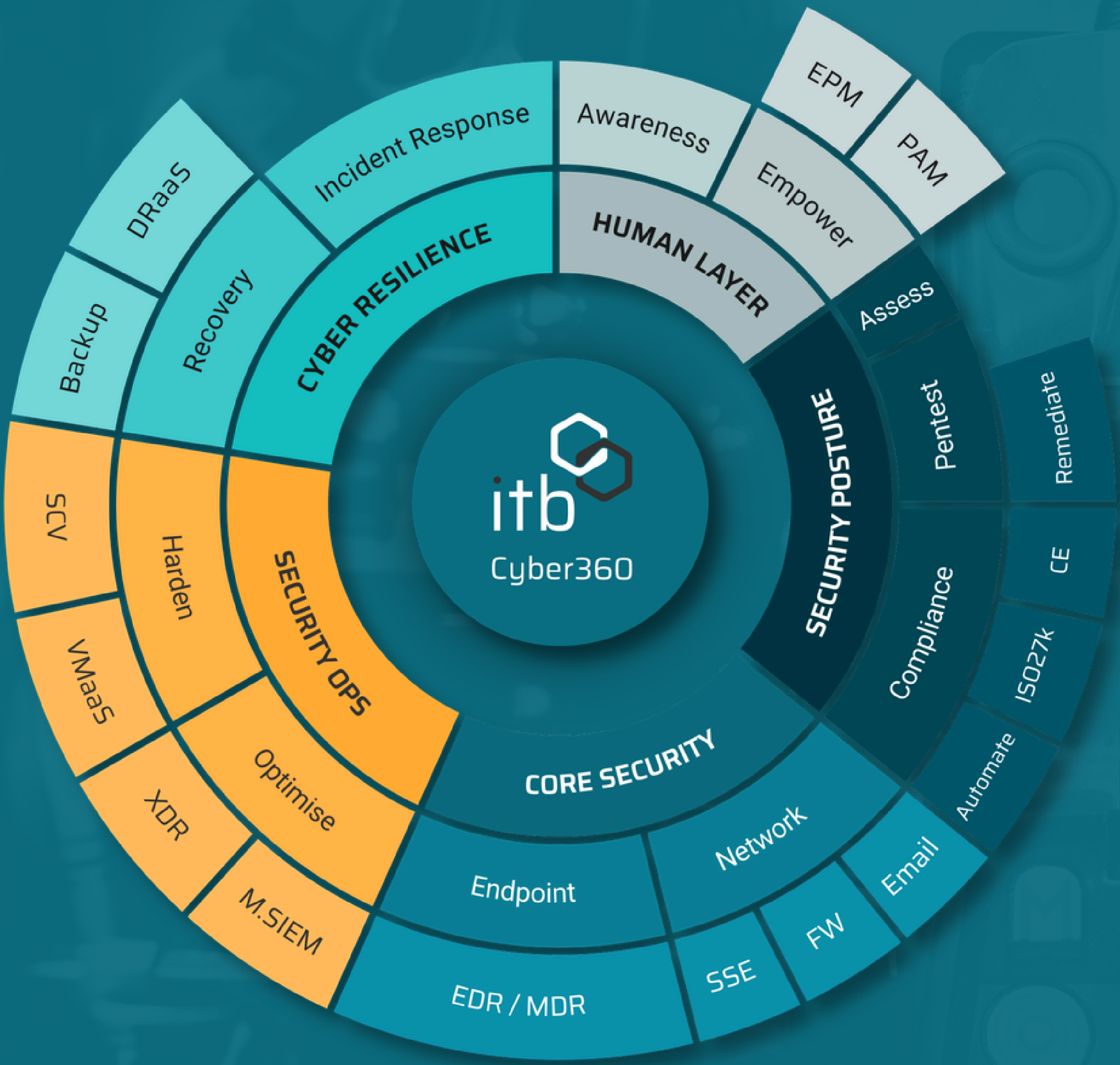
□ Tabletop or live exercises run regularly
□ Lessons learned applied, not just documented
□ Business and board roles exercised, not just IT



YOU DON'T HAVE TO SOLVE THIS ALONE.

If reviewing this checklist has raised questions, highlighted gaps, or simply feels overwhelming, we can help you make sense of it and focus on what matters most.

SECURITY MANAGED



WE JOURNEY TOGETHER
WE CONQUER TOGETHER

READY?

t: +44 (0)1856 595510
e: solutions@it-b.co.uk
w: https://it-b.co.uk

itb
cyber solutions