

Incident Response

Prepare, mitigate, appropriately remediate

With 68% of UK medium businesses and 75% of UK enterprises suffering cyber attacks, according to research published in 2020, preparedness to detect, defend against and remove cyber attacks is critical – yet recent research also shows that only 16% of UK businesses have a formal cyber incident management process in place!

This 'it might never happen' mindset is no longer tenable. Without an effective response process in place, the danger is not only that you will be targeted by a cyber attack, but – worse - that you won't even know you've been hit, thus allowing an attacker long-term, undetected access to your networks.

Reliance acsn's Incident Response combines proactive and reactive services to help you prepare for a breach, detect the incident swiftly, and deal with it appropriately and decisively. We ready your people and processes for anticipated scenarios, understand your environment to better manage incidents when they happen, and come to your aid to mitigate breaches and remove attackers from your environment.

In a world where a cyber attack is launched every 39 seconds, but the average time taken for an organisation to identify a breach is 206 days, our Incident Response service is the difference between repelling an attack and unwittingly facilitating it.

What Incident Response delivers

Reliance acsn's Incident Response delivers a thorough review of your playbooks and procedures, to help ensure your internal processes cover all identified high-risk scenarios.

We then run live crisis management exercises to replicate real-world cyber incidents, validate the internal process reviews we have produced, and ensure your operational and Executive teams are ready for such situations when – not if - they occur.

Expertise and tools produce superior results

We use advanced Threat Modelling technology to establish where attacks could strike - but the findings are also manually analysed by our team of highly qualified and experienced security experts.

Rapid reaction, no bureaucracy

Our pre-deployed, proven tooling and specialist forensic support are available as retained services. No rushed proposals or panicked purchase orders!

Build operational resilience

Cyber threats evolve daily, but we ensure preparedness and reactivity become part of the operational fabric of your organisation.

How our approach benefits you

Our approach to Incident Response is tailored to your organisation, its assets, and the specific business risks that attack outcomes could cause.

Using advanced Threat Modelling, we identify and categorise the severity of potential attack types, monitor your systems and networks for them, and ensure your teams adopt secure behaviours to support the Incident Response service both proactively and reactively.

1 We help you stay compliant

Incident response planning is mandatory for regulatory and certification compliance, e.g. GDPR, ISO 27001, ISO 22301, PCI DSS, and others.

2 We tailor our delivery to your organisation

Based on initial scoping and ongoing consultation with key stakeholders. No 'one size fits all' approach!

3 We continually update our threat knowledge

Through our own threat researchers, and through membership of industry bodies and forums.

4 We help your IT team do more with less

Enabling them to deliver business-critical infrastructure projects, rather than spending limited resources trying to manage security.

5 We can cover you 24 x 7 x 365

When you speak to our teams you speak directly to security experts, not call centre operatives.

6 We deliver clear reporting & next steps

We help you through them, in jargon-free language from humans with security expertise and an understanding of your business priorities.

About Reliance acsn

Across five continents, enterprise and government clients depend on Reliance acsn to defend them against cyber threats like nobody else can.

Our managed security and consultancy services support organisations throughout the challenges of assurance, awareness, detection, response and prevention, 24 x 7, and focus on business risk – securing not just assets and data, but revenues, too.

- Reliance acsn's history goes back to 2003, with the founding of global cyber security specialist ACSN.
- In 2016, a merger created Reliance acsn in London, UK, to deliver real-time Managed Detection and Response (MDR)
- We've helped scores of the world's top brands plan, deploy and manage robust security solutions, in banking, telecoms, retail, government and insurance.
- Our people are accredited across all the major standards in IT security – including PCI, ISO27001, G-Cloud, CISSP, CREST, and many more – and accredited to support virtually any technology you have in place or are planning to procure.