Brochure

WithSecure™ Incident Readiness and Response

Peace of mind

W / T H®
secure

Why incident response matters

27% of companies worldwide have suffered a data breach costing more than US $1M since Oct 2019[1].

Succeeding as a business means putting yourself in the firing line of cyber threats every single day. You can't eliminate these outside threats any more than you can control the rain. But you can be prepared.

The stakes are high: a well-handled security incident can be resolved in hours, rather than days or months, and at a fraction of the cost of a poorly handled incident.

1 https://www.pwc.com/gx/en/news-room/press-releases/2022/global-digital-trust-insights-survey.html

Doing the numbers

The insurance company Hiscox estimates the average cost of a cyber-attack is €180,000, with 60% of smaller companies going out of business within six months of an attack.

Many organizations don’t have their own IR teams, and the ones that do simply don’t encounter the volume and variety of incidents necessary to maintain battle fitness. If they could only outsource one security service, it would be IR.

How we help

Good security requires partnership. No one can solve every cyber security problem alone.

We take a ‘co-security’ approach, helping you to build a confident cyber security incident response team that is trained and equipped to respond to different conditions. We will help you to minimize the business impact of any cyber security crisis, understand why the incident happened and improve your security posture to reduce the likelihood of future breaches.

We offer 3 incident response services:

- **Incident Response Readiness** – exercise and improve your incident response capability without interruption to your business.
- **Incident Response Retainer** - guaranteed expert support in the event of a cyber-attack.
- **Emergency Incident Response Support** - for organizations that may call at any time, who we help with available resources.

The outcomes we deliver

In a crisis, we provide the support that you need. Our co-security approach and experience enables your incident response teams to:

Increase resilience

Maintain operations while under attack, minimize disruption.

Reduce risk

Enable and support your IR team, minimize response cost.

Maintain customer trust

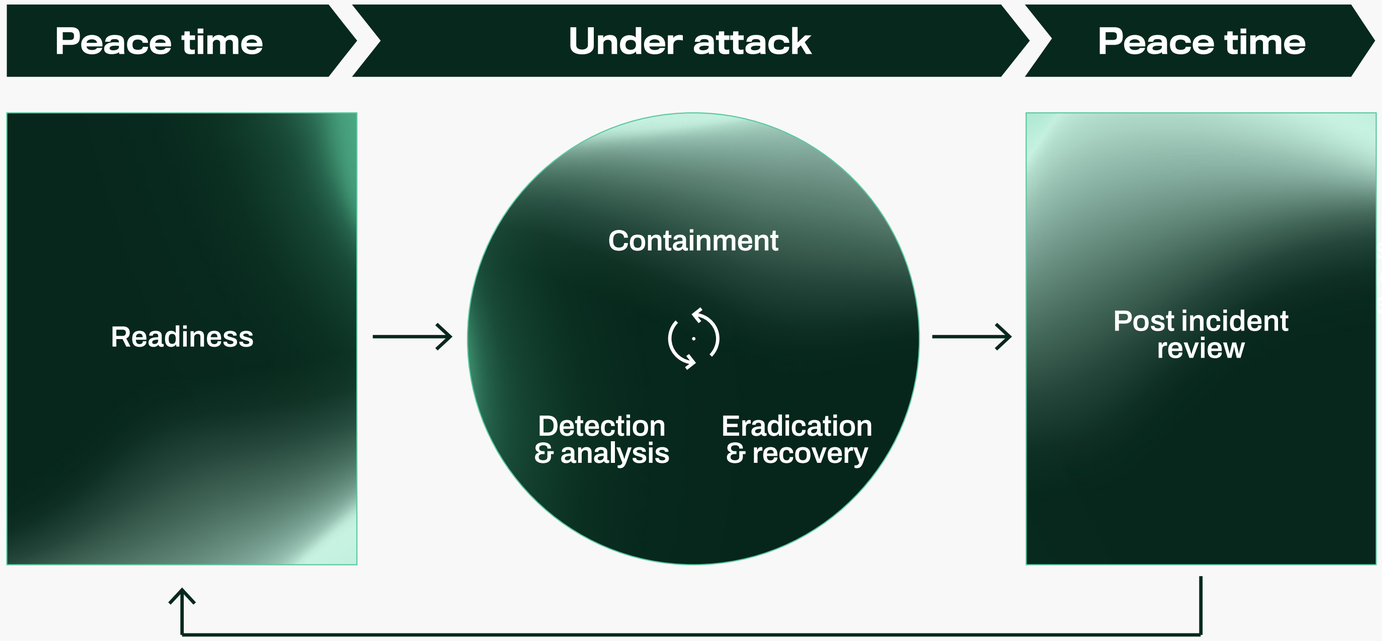
Comply with regulations, demonstrate a duty of care to your customers.

The way we work

Our methodology is based on NIST's industry standards[2] for incident response, business continuity management and other standards relevant to operational technology.

In addition to the services illustrated in the figure, we offer standardized incident response packages that deliver specific outcomes. They include:

- Root cause analysis to help mitigate or prevent recurrence of the incident
- Data exfiltration assessment to determine what data may have been exfiltrated.



2 National Institute of Standards and Technology (NIST): https://www.nist.gov/

Our record

We co-secure companies, and governments, worldwide. As a major Managed Detection and Response (MDR) service provider, we are regularly exposed to incidents. Every day, our incident response teams battle with organized, well-resourced criminal and state-sponsored groups that attack our clients' on-premises and cloud IT.

We have over 30 years of incident response experience. Our capability is assured by government agencies in Germany[3] and the UK[4].

It is by working in partnership that we are proud to say that many of our partnerships have lasted a decade or longer.

3 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.pdf?__blob=publicationFile&v=11

4 https://www.ncsc.gov.uk/section/products-services/verify-suppliers?scheme=Cyber+Incident+Response+%28CIR%29

Case study 1

IT estate – 15k~ Endpoints , ~700 web servers
Visibility – AV (No-EDR), SIEM with inconsistent log coverage

Timeline

- **Day 0** – collect data, preserve evidence, validate attack, plan response
- **Day 1** – find and analyze entry vector and payload
- **Day 2-7** – Hunt threat actor: identify infected hosts and command and control mechanism; investigate attacker identity
- **Day 8** – plan containment, muster resources, execute plan
- **Day 9-15** – battle the attacker's attempts to persist
- **Day 16-45** – deep forensic analysis to identify (and find) dormant attacker assets.

Statistics – 223 hosts compromised, 17 command and control IPs, 20 experts involved in 45-day engagement.
Outcome – accelerated security transformation, greater team cohesion.

Case study 2

IT estate – 200 servers, one 30 TB database
Visibility – AV (No-EDR), SIEM with inconsistent log coverage

Timeline

- **Day 0** – investigated suspicious activity, identified several encrypted hosts, cut internet access, supported getting DR environment running
- **Day 1** – Identified malware as BlackCat ransomware sold as a service on Russian dark web forums
- **Day 4** – attack surface mapping performed to minimise vulnerabilities that could be exploited in a DOS attack. 4 found plus a DOS protection workaround
- **Day 1-6** – verified that backups were not compromised before uploading them to DR environment
- **Day 10** – Countercept XDR deployed as IT environment brought back up.

Statistics – 250 hours of IR consultancy, forensic support and threat hunting.
Outcome – Ransom not paid. IT domain hardened, improved capability.Investigations indicated that no data exfiltration had taken place.

Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd

W / T H™
secure