Datasheet

# 24/7 Emergency Incident Response Support

WITH secure

# Call us free-of-charge if you suspect that you have a security incident

| | |
|---|---|
| Finland | +358 9 4245 0223 |
| Denmark | +45 89 88 21 10 |
| United Kingdom | +44 (0) 333 311 0014 |
| United States | +1 (917) 341-2116 |
| Singapore | +65 3159 1795 |

# Why call us

20 years of incident response (IR) experience tells us that the cost of an incident is 70-90% lower if contained with 72 hours of detection.

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. But it takes a lot of experience to confirm you have a genuine incident and know what to do about it.

That is where we can help.

# Our promise

We will provide you with the expertise and leadership you need at every stage of an incident to minimize its impact and help you recover.

# How we defend you

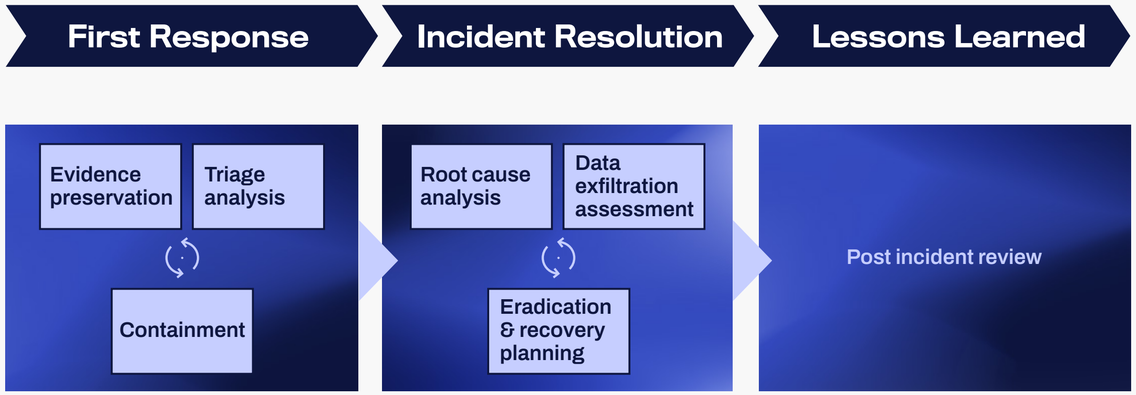
We start with an initial over-the-phone assessment to determine whether you need IR expertise.  In 25% of cases this is not necessary; the other 75% of the time is where our specialist threat intelligence, live attack management and digital forensics skills come into play.

Depending on the nature and scope of the incident, we respond using a two or three-phased approach :

1. **First Response:** we scope and start to contain the attack. We analyse collected data as quickly as we can without alerting the attacker and we provide initial containment advice. Additional tasks may include end point agent deployment, evidence preservation, stakeholder liaison and threat identification.

2. **Incident Resolution:** we provide advisory recommendations on attack eradication and recovery. By coordinating with your teams, we create a plan to expel the attacker and fully resolve the incident. Additional tasks may include: further root cause analysis, additional data and log retrieval and investigation, forensic analysis of artefacts to gather and preserve evidence.

3. **Lessons Learned:** post-incident support as required. Tasks may include: delivering an incident report, evidence presentation for legal and/or criminal proceedings, and follow-on consultancy services to address security concerns following the breach.




Our IR methodology is based on NIST's industry-standard incident response lifecycle and has been honed over two decades of dealing with cyber-attacks conducted by criminal syndicates and state-sponsored groups.

We are tool-agnostic, however we default to our own EDR technology which underpins our Countercept MDR service.

# 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 20 years of incident response experience. Our capability is assured by government agencies in Germany[1] and the UK[2].

# Pricing

The initial call is free-of-charge. During the call, we will establish whether you need our support and if so, the expertise you need.

Incident response expertise can be purchased on a per day basis across the following regions: Europe, UK, Singapore and North America. Day rates vary depending on the region and the required resources. An indicative day rate for emergency support is £2,200 GBP, per 8-hour day.

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

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

# The outcomes we deliver

- **Maintain operations** and minimize disruption while under attack.
- **Minimize response cost** by enabling and supporting your supporting your internal teams.
- **Maintain trust with customers** and comply with regulations by demonstrating a duty of care.

The enduring legacy we strive to create is to develop your incident response maturity so you can respond effectively to future incidents.

## Case study

**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.

# Next steps

**Concerned that you might have suffered a cyber security breach?**

**Call our 24/7 Emergency IR Support line free-of-charge**

**Conduct an initial assessment with an expert over the phone**

**Resolve incident with your resources**

25% of initial assessments identify that incident can be resolved without the need for IR experts

Resolution action

**Deploy IR experts to conduct time-critical containment tasks**

75% of calls result in IR experts being deployed

Within 30 minutes of calling our 24/7 Emergency IR Support line, we will typically complete an initial assessment, identify what if any IR expert resource is needed and confirm whether we have appropriate capacity to support you through to full resolution of the incident.

| | |
|---|---|
| **Finland** | **+358 9 4245 0223** |
| **Denmark** | **+45 89 88 21 10** |
| **United Kingdom** | **+44 (0) 333 311 0014** |
| **United States** | **+1 (917) 341-2116** |
| **Singapore** | **+65 3159 1795** |

Please choose the closest location to you.

# 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