Datasheet

WithSecure™ Incident Response Retainer Services

Guaranteed support, when you need it most

Organizations may have their own incident response (IR) teams, but they 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.

WithSecure™ provides IR services to businesses and enterprises across the globe that want to be resilient to cyber attacks, minimize losses, comply with regulations, and earn the trust of their customers.

Our approach

Our co-security approach goes beyond just helping you respond when the worst happens - we focus just as much on readiness, enabling you to build confident teams that are trained to respond under pressure.
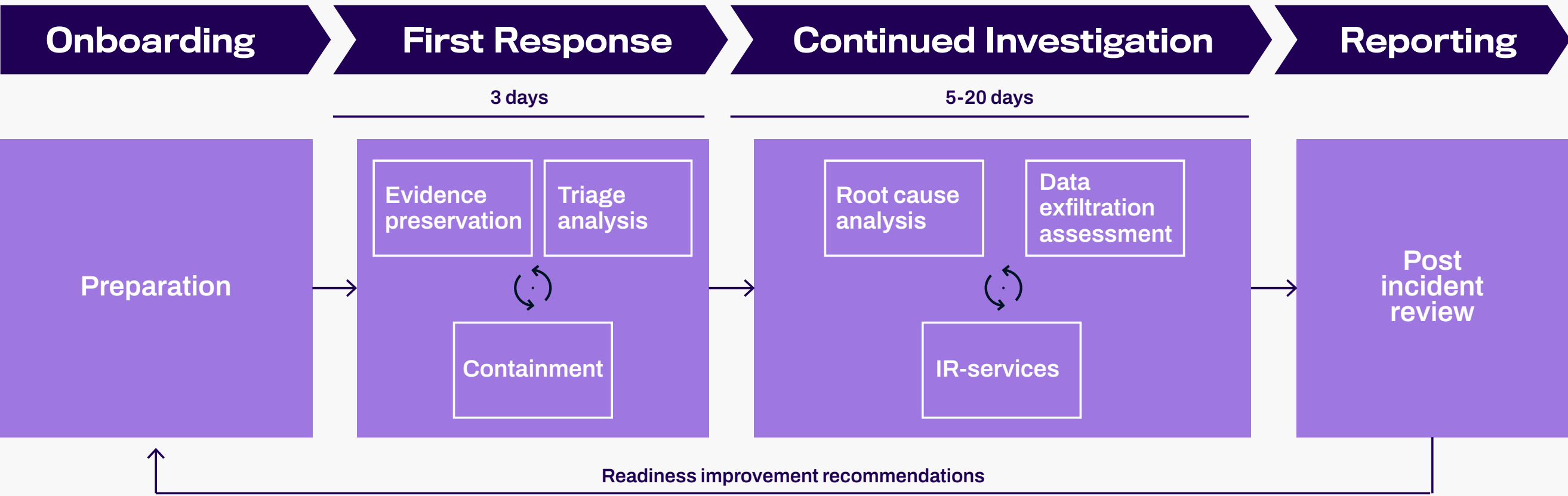
Our methodology is based on NIST's industry-standard incident response lifecycle and has been honed over a decade of dealing with cyber-attacks conducted by criminal syndicates operating for financial gain and state-sponsored groups conducting espionage or stealing intellectual property.

WithSecure's IR team specializes in threat intelligence, live attack management and digital forensics.

We are tool-agnostic, however we default to the Elements EDR platform that underpins our Countercept MDR service, and the services offered by hundreds of our Elements partners to their clients around the world.

Our incident response services

Onboarding	First Response	Continued Investigation	Reporting

| | 3 days | 5-20 days | |

Preparation	Evidence preservation / Triage analysis / Containment	Root cause analysis / Data exfiltration assessment / IR-services	Post incident review

Readiness improvement recommendations

During the Onboarding phase, we assess the level of readiness maturity and train clients on how to activate the retainer and engage WithSecure™ support.

Incident response is delivered in two phases:

- **First Response:** we contain the attack and seek to understand as much as we can without alerting the attacker.
- **Continued Investigation:** once the attacker is contained and we are armed with sufficient understanding of the attacker's behavior, we coordinate with your IT team to expel the attacker.

Often, attackers attempt to regain entry to the environment. We cycle between detection and eradication until we are sure that the threat has been removed. When requested, we can extend the period of active monitoring and support the client through our broader consultancy services.

Incident Response Retainer

We offer a continuous retainer service where clients pay a monthly or yearly fee based on the service package they have selected. Each service package contains guaranteed access to our experts within pre-agreed SLA. Detailed content of the service packages can be found in the table below.

Benefits of a retainer

- It guarantees our quick assistance when needed - even during industry-wide events when such talent is in high demand elsewhere

- It aids operational resilience: preparatory activities enable us to contain incidents sooner, minimizing their impact.

Incident Response Retainer

Prepaid response days provide priority access to expert resources. They can be used during the Continued Investigation phase for such tasks as: root cause, exfiltration, or log analysis; eradication planning and support and executive briefings.

Feature	Standard IR Retainer	Advanced IR Retainer	Premium IR Retainer
Onboarding workshop	✓	✓	✓
Emergency containment workshop	✗	✓	✓
Monthly threat highlight report	✓	✓	✓
Service reviews	Annually	Quarterly	Quarterly
First Response time SLA	Within 12 hours	Within 3 hours.	Within 3 hours.
First Response packages	1	1	2
Regular investigation updates and plans	✓	✓	✓
Priority access to consultants for executive level communications support	✗	✗	✓
Prepaid response days	0	5	10

The outcomes we deliver

In the UK, we are a founding member of the National Cyber Security Centre's Certified IR scheme[1]. At any point in time, our response team of over 50 experts collaborates with clients to resolve several incidents in complex on-premises and cloud environments.

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.

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

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/TH®
secure