

Datasheet

WithSecure™ Incident Response Retainer Services

Guaranteed IR-expert support,
when you need it

W / T H®
secure



Maintaining business continuity and minimizing incident response costs requires experience and regular practice. 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.

Acquiring and maintaining an in-house incident response (IR) capability is expensive. Organizations may have their own 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.

Incident Response Retainer Service

We offer an IR Retainer service in three predefined packages: Standard, Advanced, and Premium, as presented in the table below.

Additional IR capability can be purchased on-demand.

You can purchase an IR Retainer package, as a monthly or yearly subscription. Each service package guarantees access to WithSecure™ IR experts within a pre-agreed Initial Triage Service Level Agreement (SLA).

The IR Retainer package includes:

- At least one First Response Package that provides immediate support by a team of IR specialists during the critical first 72 hours of an incident
- Prepaid IR Support
- An onboarding workshop to establish points of contact and demonstrate how to invoke the service
- Monthly Threat Highlights Reports by WithSecure™ that summarize threat intelligence from across the cyber security industry and provide security advice on new developments
- Periodic Service Reviews to discuss how your business can be more resilient.

Benefits of WithSecure™ IR retainer

- **Availability** - On-call global support 24/7/365
- **Speed** - guaranteed quick assistance
- **Expertise** - guaranteed assistance from certified IR experts with daily experience
- **Flexibility** - we adapt to your tools and capabilities
- **Regulatory satisfaction** - we enable you to comply with industry regulation and standards.



Service Elements	Standard	Advanced	Premium
Initial Triage SLA	Within 6 hours	Within 3 hours	Within 3 hours
First Response packages	1	1	2
Included Prepaid IR Support (days of effort)	1 day	3 days	5 days
Service reviews	Annually	Bi-annually	Quarterly

For complex incidents that require support beyond the Retainer’s First Response Package and Prepaid Response Days, we offer the following on-demand services:

- WithSecure™ Endpoint Detection and Response sensor deployment to assist in containing and eradicating threats
- Incident Response Project to conduct tasks associated with the incident such as forensic analysis, IT recovery and detection and response services.

On-demand services are scoped to meet your specific needs. They give you flexible access to the specialist capabilities needed to resolve any security incident.



Our incident response framework

Our methodology is depicted below. It is based on NIST’s industry-standard incident response lifecycle and has been honed over a decade of dealing with cyber-attacks.

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.

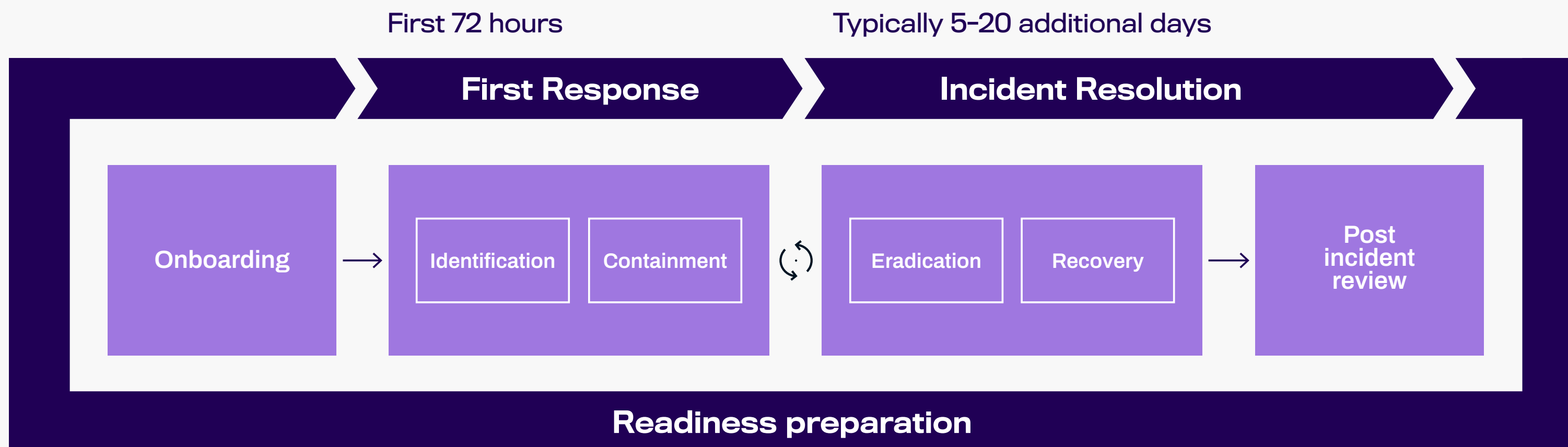
We conduct an onboarding session with new customers so that relevant stakeholders within their business can meet our IR team, and establish lines of communication and a common understanding of how the service will operate during an incident.

When you call us, we deliver incident response in two phases:

- **First Response** - immediate support provided by IR specialists during the critical first 72 hours. We contain the attack and seek to understand as much as we can without alerting the attacker. We provide you with an initial scope of the incident, guidance on preserving evidence and an estimated effort required to resolve the incident.
- **Incident Resolution** - once the attacker is contained and we understand sufficiently the attacker’s behavior, we coordinate with your IT team to expel the attacker, recover your business to your desired target state, and apply the lessons learned to protecting your business from future incidents.

Often, attackers attempt to regain entry to the environment. We cycle between containment and recovery until we are sure that the threat has been removed. When requested, we can extend the period of active monitoring and support clients in rebuilding their business and brand.

Customers use a range of tools. We are technology agnostic. We use available resources to deliver value as efficiently as possible. For customers that lack sufficient tooling, we use our endpoint detection and response sensors, which are the foundation for our products and MDR services.



The outcomes we deliver

Our service enables you to:

Achieve business continuity

Maintain operations while under attack, minimize disruption.

Minimize loss

Minimise incident response and recovery cost.

Be competitive

Earn customer trust. Comply with regulations.

WithSecure's IR team specializes in responding to cyber security incidents in complex on-premises and cloud environments. Additionally, the IR team can engage a wider team of WithSecure™ security specialists that covers all aspects of computer technology, such as Operational Technologies (OT) and Mainframe Systems to support complex engagements.

Our IR capabilities are accredited by government agencies: in the UK, by the National Cyber Security Centre's Certified IR scheme (CIR L1 & L2); and in Germany by the German Federal Office for Information Security (BSI) (APT-Responder Provider). We have over 20 years of incident response experience.



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.

