

Datasheet

# WithSecure™ Incident Readiness

Prevent an incident from becoming a crisis

**W / T H**™  
secure



# Why being ready matters

A 2020 study from insurance company, Hiscox found that firms rated as novices at cyber readiness were three times more likely to suffer breaches than those who were rated as experts<sup>1</sup>.

Organizations typically struggle to adequately respond to a cyber incident, for two reasons:

1. They lack an understanding of who their relevant threat actors are, what are their tactics, techniques, and practices (TTP's), and how these TTPs evolve.
2. They have insufficient clarity around risks, strategy and responsibilities to act effectively during an incident.

WithSecure's Incident Readiness service solves these issues by enabling organizations to be well-prepared to deal with relevant incident scenarios.

<sup>1</sup>[https://www.hiscox.co.uk/sites/uk/files/documents/2020-06/Hiscox\\_Cyber\\_Readiness\\_Report\\_2020\\_UK.PDF](https://www.hiscox.co.uk/sites/uk/files/documents/2020-06/Hiscox_Cyber_Readiness_Report_2020_UK.PDF)



# The outcomes that we deliver

Our services enable you to:

1. **Increase Resilience:** maintain operations while under attack and minimize disruption.
2. **Reduce Risk:** enable and support your response teams, minimizing response and recovery cost.
3. **Achieve compliance:** comply with regulations (e.g. NIS2) and standards (e.g. ISO 27001, ISO 27035, CIS20, NIST CSF).



# Our approach

Our co-security approach goes beyond helping clients respond when they suffer an incident. We focus just as much on readiness, enabling clients to build confident teams that are trained to respond under pressure, specifically:

1. **Focusing resources:** through threat profiling and emergency containment modelling, we help organizations make risk-based prioritization decisions that enhance their cyber defense.
2. **Uplifting governance:** we review and create playbooks. We collaborate to develop clear organizational structures and operating procedures, and enable those involved to communicate with each other and with third-party incident response teams.
3. **Exercising response teams:** first responder training and tabletop exercises that enable them to evaluate and improve their technical and strategic response to realistic threat events.

Each focus area is composed of discrete activities designed to mature your incident response capability:

Focusing resources	Uplifting governance	Exercising response teams
<p><b>Threat profiling:</b> profile likely attackers and their tools and methods.</p>	<p><b>Incident response planning:</b> create, review, and improve the flow of actions that need to be taken at each stage of a security incident.</p>	<p><b>First responder training:</b> practical skills to enable decisive and appropriate response to suspected incidents.</p>
<p><b>Emergency containment modelling:</b> determine the most effective containment controls and identify how to minimize their potential business impact.</p>	<p><b>Incident response playbooks development:</b> create, review, and improve the flowcharts and guidelines that cover the most likely and impactful incident scenarios.</p>	<p><b>Incident response tabletop exercises:</b> how to triage, investigate and contain a relevant incident, preventing it from becoming a crisis.</p>
	<p><b>Major incident playbook development:</b> create, review, and improve the flowcharts and guidelines that cover all the key decisions and events an organization is likely to face during a major incident.</p>	<p><b>Incident management tabletop exercises:</b> how to manage a complex cross-organizational response through sound containment and recovery plan execution.</p>
	<p><b>Crisis management planning:</b> create, review, and improve the flow of actions necessary at each stage of a critical incident that requires an organization-wide response.</p>	<p><b>Crisis management tabletop exercises:</b> how strategically to steer a company-wide response to an existential cyber crisis.</p>

# Our offerings

WithSecure™ Incident Readiness service is offered in three pre-defined packages, that can be delivered as a project, or an ongoing program, as shown in the adjacent table:

- **Standard Package:** aimed at organizations that need to create basic incident response planning and exercise their first responders.
- **Advanced Package:** aimed at organizations with established basic incident response planning that wish to expand and improve them to include operational and tactical teams.
- **Premium Package:** aimed at organizations with a high-risk profile, with existing incident response planning, that want to exercise their organization-wide ability to security crises, at operational and executive levels.

Modules marked with an “+” within a package can be acquired separately on top of the already included modules.

If you want to improve your organization’s resilience to cyber-attacks, being ready is the most worthwhile investment you can make.

**Call us for an initial free-of-charge consultation.**

Focusing resources	Standard	Advanced	Premium
Threat profiling	+	Yes	Yes
Emergency containment modelling	+	Yes	Yes
Uplifting governance			
Incident response plan	Create	Review and improve	Review and improve
Incident response playbooks	Create up to 3 playbooks	Create up to 6 playbooks	Review and improve
Major incident management playbook	+	Create	Review and improve
Crisis management plan	+	+	Create
Exercising response teams			
First responder training	Yes (max. 5 participants)	Yes (max. 10 participants)	Yes (max. 10 participants)
Incident response exercise	Yes	Yes	Yes
Incident management exercise	+	Yes	Yes
Crisis management exercise	+	+	Yes
Engagement model			
Onboarding	Included	Included	Included
Program governance	+	Bi-Annual	Quarterly

# 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.

