Cybersecurity Incident Readiness

What an organization needs to do the right things when an incident hits: contain fast, put resources where they matter, and avoid the costly missteps.

The question it answers

Readiness is not a document. It is whether the people who will be woken at three in the morning know what to do, have the authority to do it, and have practised it. A plan that satisfies an auditor and a plan that works under pressure are rarely the same plan.

Written, then pressure-tested

The service builds the response framework and then puts it under load. Plans and handling guides are developed against your actual threat landscape and existing documentation, not fitted to a template.

Exercises follow, because a procedure nobody has run is an assumption. Both are shaped by hundreds of real incidents rather than by a standard.

The three components

Incident response plan

Strategy, procedures and protocols for identifying, responding to and recovering from cyber threats, covering identification, containment, eradication and recovery, and mobilizing only the business resources the incident actually requires.

Incident handling guides

Step-by-step guides for specific incident types, so responders follow a known path under pressure rather than improvising the basics.

Table-top exercise

A facilitated discussion of realistic scenarios for technical or management audiences, focused on communication, coordination and decision-making rather than tooling.

DFIR functional exercise

A hands-on exercise that puts the response team against technical challenges from initial alert triage through complex evidence analysis, on scenarios built for your environment.

AT A GLANCE

PLAN AND GUIDES
5 weeks, kick-off to final

TABLE-TOP EXERCISE
3 weeks, kick-off to report

DFIR FUNCTIONAL EXERCISE
4 weeks, kick-off to report

AUDIENCES
Technical teams and executives, separately

DELIVERY
Principal-level operator, start to finish

WHO THIS IS FOR

- Organizations with a response plan nobody has tested, or none at all.
- Teams that have grown or reorganized since the plan was written.
- Boards that need to know the organization can respond, not just that a document exists.
- Security functions facing regulatory expectations on incident response capability.

How an engagement runs

01 **Kick-off and documentation request**

The current cybersecurity landscape, policies and specific needs are established, and the existing security documentation is requested.

02 **Review of existing documentation**

Everything already in place is analyzed so the new plan integrates what works instead of replacing it, and so gaps are identified against the real starting point.

03 **Plan and guides, draft stage**

The incident response plan and the tailored handling guides are developed and delivered in draft for review.

04 **Feedback integration, final stage**

The draft is presented and discussed, and feedback is incorporated so the plan matches your requirements and operational context rather than a generic model.

05 **Exercise and debrief**

Scenarios are developed for your profile and run with the relevant audience, followed by a debriefing on performance, decision-making and where to improve.

WHY ALEXSTA

- Senior hands only. The operator whose experience you are buying does the work, rather than reviewing it.
- Scenarios and plans are built from real incidents, so the pressure they apply is the pressure you will actually face.
- Every deliverable is walked through with your team, so the capability stays after the engagement ends.

WHAT WE NEED TO SCOPE IT

- Size of the organization: number of employees.
- Whether playbooks are in scope, and how many.
- Type of exercise required: technical, or for management.
- Number of participants and their roles.
- The three most important objectives for the exercise.

What you receive

Incident response plan

The overall strategy and procedures for responding to cybersecurity incidents, aligned to industry standards and your regulatory obligations.

Incident handling guides

Guides for specific incident types, detailing identification, containment, eradication and recovery step by step.

Exercise report and action plan

Objectives, scenario, participants, key observations and findings, with an actionable plan for the gaps the exercise exposed.

Performance analysis

An assessment of how the team responded, where its strengths are, and what skills and processes to develop next.

Request an engagement

Readiness is easiest to judge from the outside. Tell us what plan you have today and we will tell you where it would break.

contact@alexsta-cybersecurity.com
+41 76 76 44884
alexsta-cybersecurity.com