THIRTEEN DELTA

FREE EDITION

Cyber crisis & incident response playbook: essentials.

The core of an incident response plan, ready to fill in: the team, the first hours and the legal deadlines. A free extract of the Thirteen Delta playbook, written with NIS2 in mind.

ORGANISATION
[Organisation name]

PLAN OWNER
[Name, role]

PREPARED BY
Thirteen Delta

DATE
[Date]

VERSION
Essentials 1.1

Contents

01 — About this edition 3

02 — Response organisation and mandates 7

03 — Classification and escalation 10

04 — The first hours 12

05 — Investigation and containment today 15

06 — Legal, regulatory and the deadlines 18

07 — The full playbook and how we can help 21

Annex A — Contact tree and escalation directory 24

Annex B — Triage intake form 26

Annex C — Decision log 27

Next step 28

> **If an incident is happening now:** go straight to section 04, The first hours. Call your incident response partner with the triage form in Annex B to hand, and start the decision log in Annex C. If your policy names the response firm, call your insurer's hotline first. If you have no incident response partner under contract, section 02 explains how to find one.

01 — About this edition

This free edition gives you the core of an incident response (IR) plan: who decides, who acts, what happens in the first hour, and which legal deadlines start to run under the NIS2 Directive and the General Data Protection Regulation (GDPR). Most of what goes wrong in an incident goes wrong because nobody agreed beforehand who does what. This edition helps you settle that before the day.

It is an extract of the full Thirteen Delta cyber crisis and incident response playbook. The approach is based on public guidance from ENISA, the EU agency for cybersecurity, and from national authorities: the NCSC in the Netherlands and the UK, Germany's BSI, France's ANSSI, and NIST (SP 800-61r3) and CISA in the United States. It also draws on the published practice of hands-on response firms and on almost two decades of incident response and investigations by Thirteen Delta's founder.

READ THIS FIRST

A starting point. This edition contains the core of a plan: the team, the severity levels, the first hours, the legal deadlines and three annexes to fill in. A complete plan needs more, such as investigation and containment in detail, communication, recovery, scenario playbooks and sector guidance. Section 07 lists what the full playbook adds. Use this edition to start your plan and build on it.

Where we come in. We adapt the full playbook with you and agree it with your management, and our workshops test the result with your team. Section 07 explains what each option gives you, and the last page how to start.

It will date. No document can foresee every incident, and adversary methods, technology and regulation change quickly. This edition reflects public sources and regulation as of November 2026. We update the template when the law, public guidance or what we see in incidents gives reason to. The latest version is always on thirteen-delta.com. Check current guidance from your national authorities and your IR partner and review your plan at least once a year.

Not legal advice. Regulatory duties differ per Member State and sector, and national implementations of NIS2 are still changing. Check your obligations with counsel and your national authority when you adapt your plan.

Your responsibility. The decisions in an incident, and the plan that prepares for them, stay with your organisation and its management. This edition supports that work. It doesn't replace professional incident response, legal advice or the conditions of your insurance policy.

Provided as is. Thirteen Delta provides this free edition as is. We can't promise that it is complete or suitable for your situation, and we accept no liability for decisions based on it.

HOW TO USE THIS DOCUMENT

Word version. This edition is also available as a Word document, so you can fill in and adapt the template directly. It is free; ask for it at info@thirteen-delta.com.

Fill it in. Everything between [brackets] is for you to complete, such as names, phone numbers, thresholds, regulators and retainer numbers. Without names and numbers, the plan won't help you on the day.

Print it. Keep copies outside your own IT: on paper, and in a separate cloud location you can reach from private devices. In a ransomware incident, a plan stored on the encrypted file server is of no use.

Exercise it. Run a tabletop exercise at least once a year, with the executive team in the room as well as IT. That is where you find the gaps. The full playbook explains how to run one.

Keep it current. Review it after every incident and exercise, after changes to the organisation or infrastructure, and at least once a year. Record each version in the document control table below.

WHO IT IS FOR

This edition is written for two groups. Leaders own the decisions and what is said: severity, business priorities, contact with the adversary, notifications and communication. IT and security own the triage and the evidence: containment, collection, investigation and recovery. During an incident both groups work from this document.

BEFORE THE DAY: THE MINIMUM

If you do nothing else, arrange the following.

☐ Crisis team named: owners and deputies, reachable out of hours

☐ One role mandated in writing to declare a crisis, with thresholds agreed

☐ Severity levels agreed, and anyone may raise the alarm

☐ IR partner (including threat hunting and compromise assessment) and insurer arranged, numbers in the offline contact tree

☐ Crisis communication specialist contracted and reachable out of hours

☐ Out-of-band crisis channel set up and tested

☐ Reporting map (NIS2 24 h / 72 h / 1 month, GDPR 72 h, plus sector rules where they apply) with an owner per filing

☐ Endpoint detection and response (EDR) on servers and endpoints, with coverage measured

☐ Logs centralised, retention known, one clock (UTC) across time zones

☐ Backups offline or immutable, and restored as a test every quarter

☐ Two emergency (break-glass) admin accounts outside single sign-on, with credentials stored offline and tested

☐ An emergency stop for supplier apps, application secrets and admin roles, prepared and tested (section 05)

☐ Tabletop exercise at least once a year, with executives

> **Where to start.** Unticked boxes are normal; that is what this edition is for. Start with the first four. They cost little and settle much of what goes wrong on the day. If you'd like a second opinion on where to start, section 07 explains how we work with you.

THE PRINCIPLES BEHIND EVERY PAGE

> **Assume breach.** You can't prevent every incident, but you can limit what one costs you.
> **Prepare before the day.** Organisations that handle an incident well have agreed beforehand how they will respond.
> **Contain first.** The time it takes to contain an incident decides most of its impact. Stabilise first, investigate in parallel, and don't let the response wait for a disk image to finish.

DEFINITIONS

TERM	WORKING DEFINITION
Event	Something observable in a system or network, such as an alert, an anomaly or a report. Most events are noise, but every incident starts as one.
Incident	An event that compromises, or credibly threatens to compromise, the confidentiality, integrity or availability of systems, data or services.
Significant incident (NIS2)	An incident that has caused or can cause severe operational disruption or financial loss, or that has affected or can affect others by causing considerable material or non-material damage (Art. 23(3), Directive (EU) 2022/2555). For digital-infrastructure and digital-service providers (cloud, data centres, managed services, DNS and others), Implementing Regulation (EU) 2024/2690 sets concrete thresholds. This is the trigger for the regulatory clock in section 06.
Crisis	An incident whose impact goes beyond what normal management can handle: damage that threatens the business, safety concerns, major legal exposure or public attention. A crisis activates the strategic crisis team and the mandates in section 02. Germany's BSI describes the same steps as Störung → Notfall → Krise.

DOCUMENT CONTROL

FIELD	VALUE
Owner	[Name, role; accountable for keeping this playbook current]
Approved by	[Name, role; management body approval, see NIS2 Art. 20]
Adopted by	[Organisation · date]
Version / date	[version · date]
Edition	Essentials 1.1 · November 2026
Last exercised	[Date and exercise form]
Next review	[Date; at least annually]
Storage locations	[Intranet location · printed copies location · out-of-band copy]

PERMITTED USE

Free to use in your organisation. You may copy, adapt and print this edition, and share it within your organisation and with the IR partner, insurer and advisers who act on your behalf.

Sharing outside your organisation. Please don't publish or sell it, and don't reuse it in work for other clients if you are a consultancy or service provider. To share it, point people to thirteen-delta.com, where it can be downloaded free of charge. Questions are welcome at info@thirteen-delta.com.

02 — Response organisation and mandates

THE FIRST RESPONDER

Whoever notices the incident first, whether a system administrator, a helpdesk agent or any other employee, has a large influence on how it goes. The first responder does three things: **observe** (note what you saw, when and where, before anything changes), **inform** (escalate to the contacts in Annex A; a false alarm costs far less than keeping quiet about a real one), and **act** (contain where you safely can, without destroying the evidence that explains what happened).

TWO CRISIS TEAMS

Most well-run responses split the crisis organisation into two teams. ANSSI's crisis-management guidance and BSI-Standard 200-4 use the same split, and so do professional IR firms. Both teams work on the same incident, but with different people and different questions. Keep their meetings separate.

	OPERATIONAL CRISIS TEAM	STRATEGIC CRISIS TEAM
Role	Handles the technical response.	Takes the business decisions.
Who	IT manager or team lead with system and network administrators, working directly with the (external) responders' analysts.	The management team, informed by the operational lead and advised by the IR partner's case manager, plus legal counsel and the communication owner.
Does	Implements containment and mitigation, gathers evidence, runs recovery, facilitates the investigation.	Sets business-continuity priorities; decides on adversary contact, notifications to authorities, internal and external communication, and legal steps.
Cadence	Technical updates at agreed, regular times, with priorities agreed by both teams.	Management updates at agreed, regular times, so decisions are taken on time and based on facts.

CORE ROLES

ROLE	OWNS	NAME AND DEPUTY
Crisis chair	Declares and closes the crisis, chairs the strategic team and makes sure the decision log is kept.	[Name · deputy]
Operational lead	Runs the operational team and is the single technical contact for the IR partner.	[Name · deputy]

ROLE	OWNS	NAME AND DEPUTY
Communication owner	Owns all communication with stakeholders, so the organisation speaks with one voice.	[Name · deputy]
Legal & privacy	Notifications to regulators, contracts, legal privilege and contact with the police.	[Name / data protection officer (DPO) · deputy]
Scribe / log keeper	Keeps the decision log and timeline from the start.	[Name · deputy]
HR & people	Staff welfare, insider cases and contact with the works council.	[Name · deputy]

Around this core are the external parties. Contract them now and list them in Annex A: the incident response partner, the cyber insurer, external counsel, the communication agency, a ransom negotiator (normally through the IR partner), your main managed service providers, the national computer security incident response team (CSIRT) and the police cybercrime unit.

> **Bring in response support straight away.** How early professional responders are involved makes the biggest difference to how an incident ends. Your own team can triage and stabilise, but scoping, eradication and negotiation are specialist work done under time pressure. If you have no IR partner under contract, make engaging one the first call of the incident and skip the usual procurement process. Ask your insurer for its panel, or use your national authority's list of qualified providers where one exists (such as BSI's list of advanced persistent threat (APT) response providers in Germany or ANSSI's PRIS qualification in France). Thirteen Delta can also introduce you to vetted IR firms and negotiators.

MANDATES, AGREED IN ADVANCE AND IN WRITING

The mandates below take little effort to agree now and a lot of time to sort out during an incident. They are based on the NCSC, CISA and BSI playbooks, and on seeing organisations lose hours over questions a signature could have settled in advance.

PRE-AUTHORISED DECISION	MANDATE HOLDER	LIMIT / NOTE
Declare a crisis and convene both teams	[Role]	Thresholds in section 03
Emergency spend (IR support, hardware, licences, hotel and catering)	[Role]	Up to € [amount]
Disconnect systems, sites or internet egress	[Role]	With operational lead
Engage the IR partner and (if needed) a negotiator	[Role]	Retainer ref. [number]
Notify regulators, insurer and police	[Role]	Deadlines in section 06
Approve external statements	[Role]	One voice

OUT-OF-BAND, FROM THE FIRST MINUTE

Assume the adversary can read your email and chat. In intrusions that run through identities, they often can. Move crisis coordination to a separate (out-of-band) channel set up in advance: [e.g. a Signal or equivalent group on private devices, plus a standing conference bridge]. Keep the offline contact tree (Annex A) in print and on private devices, with two ways to reach each person and two people per role. NCSC-UK guidance explains why. During an incident your usual channels may be unavailable or compromised. Verify every member of the crisis group with a call back on a number you already have, or in person. State-linked groups have used Signal and WhatsApp to approach targets and take over their accounts, and a crisis group is an obvious target.

Meeting rhythm. Every crisis team meeting follows the same steps, taken from the Dutch emergency services (BOB, for beeldvorming, oordeelsvorming, besluitvorming). First build the picture (facts, kept strictly apart from assumptions), then form a *judgement* (what it means, what the options and risks are), and then take a *decision* (owners, actions and the time of the next meeting). The scribe records every meeting: what was known, what was decided and why. The decision log shows regulators and insurers that you acted with due care, and it is the basis for the NIS2 final report.

Plan for a long response. Serious incidents last days or weeks, and people tire within 48 hours. Organise for that from the first day. Work in shifts of at most twelve hours with a proper handover, let deputies take over, arrange food, rest and transport, and make one person responsible for watching workload and welfare. A team that stops sleeping makes avoidable mistakes.

> **In the full playbook (see section 07):** eleven sector overlays, from healthcare to education, that show who joins the crisis team in your sector, plus a target operating model for the response.

03 — Classification and escalation

The severity level decides who gets called in, day or night. Agree the levels in advance. Three are enough. The response should match the impact, which is why CISA's federal playbook gives every incident a severity rating.

LEVEL	LOOKS LIKE	RESPONSE	REGULATORY CLOCK
SEV-3	Contained and minor, such as a phishing email caught in time, one endpoint quarantined or a scan blocked at the perimeter.	IT handles and logs it, with a weekly report to management.	Not started; record the assessment.
SEV-2	Confirmed intrusion with limited spread, such as a compromised account, an affected server or malware on more than one endpoint.	IR engaged, operational team activated, IT leadership informed.	Check whether this could be a significant incident under NIS2, and whether it is a personal-data breach (GDPR, 72 hours). Record both answers.
SEV-1	Threatens the business, such as ransomware encrypting systems, compromise of the domain, data being stolen, or impact on safety or operational technology (OT).	Crisis declared. Both teams meet, the strategic crisis team decides, and external IR and legal counsel are brought in at once.	Running. Treat this as the moment of awareness; early warning within 24 hours (section 06).

Set your own thresholds. [e.g. SEV-1 when more than __ users, or a process the business can't do without for more than __ hours, or more than __ personal records are affected]

> **In the full playbook (see section 07):** the baseline questionnaire that gives management the facts to set these thresholds, and readiness checklists for people, decisions and systems. Setting the thresholds is usually the hardest step, and it is the first thing we agree with you when we adapt the plan.

> **Rule 1: whoever sees it can declare it.** A helpdesk agent must be able to call SEV-1 without worrying about being wrong, and needs no permission to raise the alarm. The crisis chair or a deputy then confirms or downgrades it within [30] minutes.
> **Rule 2: declare high, downgrade later.** Over-escalating for an hour costs little, while under-escalating can let an adversary stay unnoticed for months.

FROM INCIDENT TO CRISIS

Declare a crisis when the impact goes beyond what normal management can handle. Any one of the following is enough: processes the business can't do without that are down or at risk, suspected large-scale data theft, impact on safety or OT, likely regulatory or legal exposure, outside attention (media, a leak site, customers), or an adversary you judge to be targeted or state-backed. The mandate to declare rests with [role], who can be reached 24/7 through the contact tree. Declaring a crisis brings both teams together, starts the decision log, moves coordination to the out-of-band channel and starts the notification checks in section 06.

Ending the crisis. The crisis ends with a decision, recorded in the decision log, once the criteria are met: the adversary is removed or the threat contained, the business is stable and the obligations are met. A post-incident review follows. Severity can be lowered at any crisis team meeting; record why.

Severity and NIS2. Severity and the legal test are related but separate. SEV-1 incidents almost always meet the significance test in Art. 23(3) NIS2, and SEV-2 incidents sometimes do (a single compromised mailbox can be a significant incident if the damage to others is considerable). At every escalation, legal & privacy answer one question in writing: has a reporting deadline started under NIS2, the GDPR or sector rules? The NIS2 deadline starts when you become aware of a significant incident, even if you don't yet understand it fully.

04 — The first hours

What you do in the first hours has a large effect on the outcome, and the first hour most of all. This section is the page to open when the call comes in at night. It lists the steps in order, the reflexes to hold back and what to tell your responders.

THE FIRST 60 MINUTES

0-10 · RECOGNISE & RAISE	10-30 · CONTAIN & CONVENE	30-60 · INSTRUMENT & INFORM
Trust the first observer (section 03, rule 1). Declare a severity. Set it high and downgrade later. Start the decision log: timestamps (UTC), observations, actions. If changes appear faster than people can make them, use the emergency stop (section 05).	Call your IR partner with Annex B to hand. If the policy names the firm, call the insurer's hotline first. Contain machines and identities together. Isolate machines through EDR or at network level, and keep them on. Disable the accounts used, reset credentials and revoke sessions. Do this at once and broadly if something is being destroyed or money or data is leaving. If it is quiet or may be an insider, scope first with your IR partner. Move the crisis team out of band. Assume email is read.	Start rolling out EDR or a triage collector, so you can see what is happening. Check whether a 24-hour reporting deadline applies. Notify the insurer. Send a first internal holding statement with facts only.

> **Leave for later:** root cause, blame and press releases. The first hour is for limiting the impact and keeping your options open.

A FIRST MESSAGE TO STAFF

> We are investigating a cybersecurity incident affecting [systems / services]. As a precaution we have [isolated the affected systems / limited access to …]. Please: do not switch off, "clean up" or investigate systems yourself; do not communicate about this outside the organisation, including on social media; report anything unusual to [contact]. Use [channel] for updates. Next update: [time]. [Crisis chair]

Bring in crisis communication specialists. In many incidents, vague statements, long silences or claims that later had to be withdrawn did more damage to the organisation's reputation than the attack itself. Norsk Hydro and Maastricht University, both hit by ransomware in 2019, are often cited for open and regular updates. TalkTalk in 2015 and Travelex in 2020 are often cited for the opposite: information that was unclear or late and drew sharp criticism from customers and the media. A

specialist crisis communication adviser or agency can make a real difference here, and we recommend one for every serious incident. Put them in Annex A now and let them work alongside legal counsel and the IR partner, so that every audience hears the right message at the right time.

THE DO'S

DO	WHY
Call your IR partner first, or the insurer's hotline if your policy names the response firm	The earlier they are involved, the smaller the damage. If you have no retained partner yet, ask for an introduction now (section 02).
Limit interactions	Every login and opened file changes the evidence. Touch impacted systems as little as possible.
Gather evidence under guidance	Preserve memory, triage data and logs before they roll over or are wiped, in the order your responders ask.
Provide access and facilities	Give them information, accounts, network diagrams and a room to work in, so they can start straight away.

THE DON'TS

NEVER	WHY IT HURTS
Turn systems off	Powering down wipes memory, which is where live malware and encryption keys often live. Isolate instead; power off only if there is no other way to stop active destruction (CISA's ransomware guide treats it strictly as a last resort).
Reinstall or wipe systems	Rebuilding overwrites the forensic record of how the attack happened, and with it the evidence that tells you whether it can happen again.
Delete or discard virtual machines (VMs) and snapshots	Virtual machines and snapshots are often the cleanest evidence you have. Keep all of them during an incident.
Announce the response in email or chat	If the adversary has access to a mailbox, they can read your containment plan as you write it. Coordinate out-of-band.
Fix problems one at a time	Resetting one password or blocking one IP address tells the adversary they have been seen, and they move to backdoors you haven't found yet. Contain broadly, then remove the adversary in one coordinated step.

Stabilise before you investigate. Investigating first gives the adversary time to keep moving. First limit the damage: isolate machines, end sessions and protect the backups. Then investigate alongside the recovery.

THE FIRST CALL TO YOUR RESPONDERS

What you tell your IR partner in the first ten minutes, and how quickly, sets the pace for the rest of the engagement. Share what you know straight away, even if it is incomplete. Have two things ready: who you are and what is happening. The full intake form is in Annex B.

WHO YOU ARE	WHAT IS HAPPENING
Name, organisation and role: who is speaking, and what they can authorise. Direct contact details: a direct phone number and a personal inbox. Two single points of contact: one operational, one management.	1. What is happening? What symptoms do you observe? 2. What is impacted: systems, data, people? 3. Is it still active right now? 4. Where is it: site, segment, cloud tenant? 5. What is the biggest risk if it spreads? 6. What has been done so far? (Every action changes the evidence.) 7. What do you need: contain, investigate, recover, report? 8. Is regulated or personal data involved? (Legal deadlines.)

> **In the full playbook (see section 07):** a checklist for hours 2 to 72, and what follows scenario by scenario: ransomware and extortion (with a pay-or-rebuild decision tree and negotiation principles), business email compromise and payment fraud, state-sponsored intrusion, data-theft extortion, and 17 further incident types, from compromised phones and fake remote IT workers to distributed denial-of-service (DDoS) attacks and supply-chain compromise.

05 — Investigation and containment today

Preserving evidence still matters, but it is no longer the first step. Responders used to image every disk and verify every hash before doing much else, which cost hours while the adversary was still active on the network. Today the response first gets visibility and control across the environment, limits the impact, and preserves evidence selectively where it matters.

THEN: IMAGE EVERYTHING FIRST	NOW: VISIBILITY AND CONTROL FIRST
Full bit-for-bit images of every affected disk, with verified hashes, before anything else happens. Analysis starts when the copies finish, hours or days later. Meanwhile the adversary keeps moving.	EDR sensors and rapid-triage collectors rolled out across all systems in the first hours. Isolate, hunt and contain using live telemetry; triage data collected in minutes per system. Full images only where legal exposure or disputed facts justify the time.

CONTAIN IDENTITIES AS WELL AS MACHINES

Most intrusions today run on a valid login, so unplugging a machine doesn't stop an adversary who holds a working account or session. Work on machines and identities at the same time. Isolate systems instead of switching them off. Disable accounts, revoke sessions and tokens, and remove the multi-factor authentication (MFA) methods and devices the adversary added. The full playbook sets out both tracks step by step.

WHEN THE ADVERSARY WORKS AT MACHINE SPEED

AI agents now carry out large parts of some intrusions. In October and November 2026 Microsoft described ARTEX, an open-source framework in which AI agents run an intrusion from reconnaissance to data theft with little human input. A China-linked group used it after a supply-chain compromise to try to sign in to more than 2,250 Microsoft 365 tenants, through apps the customers had already approved. In some cases the agents had privileged cloud access within three hours, and added their own credentials and admin roles, which can outlast the clean-up. In another case an agent went from searching GitHub for leaked secrets to taking data from a cloud key vault in about five minutes. Similar tools such as HexStrike-AI and Villager are freely available. In 2025 Anthropic reported a state-sponsored campaign in which its AI tool did most of the hands-on work.

Prepare an emergency stop. At this pace, changes happen before the crisis team can meet, and removing them one by one while the agent is still active is unlikely to work. The emergency stop is a short set of containment actions, agreed and tested in advance, that the person on call may use without waiting for the crisis team. Typical actions are:

- disable supplier and other third-party apps that have high privileges, and keep their registrations as evidence;
- remove the secrets, certificates and keys of the application identities the adversary used, and rotate everything they could read;
- revoke sessions for admin accounts, and remove standing admin rights except those of the break-glass accounts;
- cut VPN and supplier remote access, and block deletion of backups.

Test it, and automate the clearest cases. Rehearse the emergency stop twice a year and measure the time from decision to effect. Where a detection leaves no doubt, let your security tools disable the account or app on their own, and have a person review it afterwards. Use AI on your side too, for triage and threat hunting, and scan your own code for exposed secrets before an adversary's agent finds them.

WHERE THE EVIDENCE IS: CLOUD, EMAIL AND BUSINESS SYSTEMS

In intrusions that run through identities, most of the evidence is in cloud and software-as-a-service (SaaS) platforms, and much of it is deleted after a period that depends on your licence.

SOURCE	WHAT IT TELLS YOU	KEPT BY DEFAULT
Identity platform (Microsoft Entra ID, Okta, Google)	Who signed in, from where and with which token; changes to MFA methods and devices.	Entra ID: 30 days with P1/P2, 7 days on the free tier. Okta: 90 days.
Email and collaboration (Microsoft 365, Google Workspace)	Mailbox access and inbox rules, file access and sharing, admin actions.	Microsoft 365 audit log: 180 days as standard, longer with premium licences.
Business applications in the cloud: customer relationship management (CRM) such as Salesforce or HubSpot, enterprise resource planning (ERP), data platforms such as Snowflake	Data exports, reports and API use, admin and permission changes.	Varies per platform; detailed event logs often need an add-on licence.
Cloud infrastructure (Azure, AWS, Google Cloud)	Admin actions, new resources, keys and access policies.	AWS and Azure keep management activity for 90 days by default. Access to data is only logged if you set that up. Export the logs to storage you control.
Network edge (firewall, VPN, proxy)	Traffic in and out, connections to adversary infrastructure, volumes of data leaving.	Days to weeks; check per device.
Endpoints and servers (operating system logs, EDR)	What ran, lateral movement, credential access.	Event logs roll over fast; EDR history depends on your licence.

Two warnings. Logs roll over, so export and preserve them early, before retention deletes them. And put everything on one clock (UTC), or the timeline will be wrong.

Bring in the specialists. Searching cloud, identity and SaaS platforms for traces of the adversary is specialist work. Agree in advance that your IR partner covers these platforms, and how they get access during an incident.

> **In the full playbook (see section 07):** the tools for a faster investigation, threat hunting with your IR partner, evidence handling, and containment and eradication step by step, including how to prepare the shutdown and the emergency stop before you need them.

06 — Legal, regulatory and the deadlines

Reporting deadlines start before you have the full picture. **They run from the moment you become aware of the incident.** Under NIS2, essential and important entities must send a series of notifications for every significant incident (the test in section 01). Under the GDPR, a personal-data breach has its own 72-hour deadline. Agree in advance who notifies, who drafts and who signs off, and name an owner for each filing. If that is left until hour 70, deadlines get missed. Where appropriate, NIS2 also requires you to inform the recipients of your services without undue delay about significant incidents that are likely to affect those services (Art. 23(1)).

THE DEADLINES

DEADLINE	FILING	WHAT IT CONTAINS
Immediately	Cyber insurer	Notification under policy [number]. Late notice can put your cover at risk, and many policies limit which IR firms and negotiators you may use.
≤ 24 hours	NIS2 early warning, to [national CSIRT / authority]	Brief details, enough for a phone call: the incident, whether an unlawful or malicious act is suspected, and possible cross-border impact. The CSIRT responds without undue delay, where possible within 24 hours, with initial feedback and, on request, guidance.
≤ 72 hours	NIS2 incident notification	An update of the early warning with an initial assessment: severity, impact and indicators of compromise where available. Say what you know and mark what you don’t know yet.
≤ 72 hours	GDPR Art. 33, to [data protection authority]	Unless the breach is unlikely to put people at risk: nature of the breach, categories and approximate numbers, DPO contact details, likely consequences, measures taken. You may notify in phases, so don’t wait until you are certain. Inform the people affected without undue delay when the risk to them is high (Art. 34). Record every personal-data breach internally, including those you don’t notify (Art. 33(5)).
On request	NIS2 intermediate report	Status updates while the incident runs.

DEADLINE	FILING	WHAT IT CONTAINS
≤ 1 month after the 72-hour notification	NIS2 final report	Detailed description, severity and impact, type of threat and likely root cause, mitigation applied and ongoing, and cross-border impact. If the incident is still ongoing at that point, send a progress report, followed by the final report within one month of the end of incident handling. The decision log you kept from the start is the basis for it.

When you are aware under the GDPR. The European Data Protection Board says a controller becomes aware once it is reasonably certain that a security incident has compromised personal data. A short initial investigation to establish that is allowed, as long as it starts promptly. Record when you became aware and why, because the 72 hours run from that moment.

Processors and groups. If you process personal data on behalf of another organisation, tell that organisation without undue delay (GDPR Art. 33(2)). Processing agreements often set a shorter deadline, such as 24 or 48 hours, so check yours. If you process personal data in several EU countries, GDPR notification usually goes to your lead supervisory authority. Under NIS2 you generally report in the Member State where you are established, but some digital providers report where their main EU establishment is (Art. 26). Groups with entities in several countries may have to notify more than one authority; list them in Annex A.

Notifying doesn't increase liability. NIS2 says that the act of notification does not by itself expose you to increased liability (Art. 23(1)). Organisations outside the scope of NIS2 can also notify their CSIRT voluntarily (Art. 30).

Name an owner per filing. Insurer [name · deputy] · national CSIRT or authority [name · deputy] · data protection authority [name · deputy] · police [name · deputy]

Customers and suppliers. Contracts often add notification duties in both directions. List yours in Annex A.

Sector rules can change the deadlines. For financial entities within the scope of DORA, the EU Digital Operational Resilience Act, major ICT-related incidents are reported under DORA instead of NIS2. Manufacturers of hardware and software also report under the Cyber Resilience Act, and designated critical entities under their national law implementing the Critical Entities Resilience (CER) Directive. The full playbook covers each of these.

Does NIS2 apply to you? NIS2 generally applies to medium-sized and larger organisations (50 or more staff, or an annual turnover and balance sheet both above €10 million) in the sectors listed in its Annexes I and II, and to some entities regardless of size. Your national law sets the details, including

registration. If NIS2 doesn't apply, the GDPR deadline still applies whenever personal data is involved, and customers and insurers increasingly expect the same care. Working out your position per country and sector is part of adapting the plan (section 07).

WHERE TO FILE

Fill in your Member State's channels in Annex A: national CSIRT / competent authority [name and portal], data protection authority [name and portal], sector regulator [if any], police cybercrime unit [contact]. As of October 2026, NIS2 transposition still varies across the EU. Belgium has applied it since October 2024 (Centre for Cybersecurity Belgium, CCB), Germany's implementation act took effect in December 2025 (BSI), and the Dutch Cyberbeveiligingswet has applied since 15 August 2026, with mandatory registration and incident notification through the MijnNCSC portal. In some Member States the national law was still pending at the time of writing. Check current national rules, registration duties and portals with counsel when you adapt your plan. Two EU proposals are under discussion but not yet law: the Digital Omnibus (November 2025), which would change GDPR breach notification to a 96-hour deadline for high-risk breaches only, through a single EU reporting point, and targeted NIS2 amendments (January 2026). Until they are adopted, work with the deadlines in the table above. For incidents that affect several Member States at once, the EU Cyber Blueprint (Council Recommendation of 6 June 2025) sets out how national CSIRTs, the CSIRTs network and EU-CyCLONe (the network of national cyber crisis agencies) coordinate. In a large-scale incident, ask your national CSIRT whether support from the EU Cybersecurity Reserve is available.

DUTIES BEYOND NOTIFICATION

NIS2 makes the management body accountable. It must approve and oversee the cybersecurity risk-management measures of Art. 21, which explicitly include incident handling, business continuity, backup and crisis management, and supply-chain security, and its members can be held liable for infringements under national law. Members of the management body must also follow cybersecurity training (Art. 20). In the Netherlands the Cyberbeveiligingswet gives directors two years to meet the training duty, so until 15 August 2028 at the latest; new directors have two years from their appointment. Approving and exercising this playbook is one way for the management body to show it oversees incident handling. Keep the evidence: the decision log, the notifications and the reports.

> **In the full playbook (see section 07):** the DORA, Cyber Resilience Act and CER reporting duties, a notification checklist for every filing, what to settle before any payment (strategy with the board, insurer, sanctions check), working with your insurer and law enforcement, and legal hold.

07 — The full playbook and how we can help

This edition covers the team, the first hours and the deadlines. The full playbook, about 90 pages, takes you through the whole incident, from the first alert to the final report, with scenarios, sector guidance and annexes to fill in. It comes free with our workshops and with an advisory retainer, and in our advisory work we adapt it to your organisation and agree it with your management. The tables below show what it adds and how we can help.

WHAT THE FULL PLAYBOOK ADDS

CHAPTER	WHAT IT GIVES YOU
Chapter 2 · What you are up against	How adversaries get in today (through exposed systems, bought access, stolen identities, your own tools, phone calls and AI), the two main types of adversary compared, and the European picture.
Chapter 5 · Hours 2 to 72	A checklist for the days after the first hour: the NIS2 significance assessment, the GDPR decision, log exports, the insurer, the police, staff and the board.
Chapter 6 · Investigation	The tools for a faster investigation, the intelligence loop, threat hunting with your IR partner, which cloud and identity logs to export early, when full forensic images are still needed, and evidence handling.
Chapter 7 · Containment and eradication	Both containment tracks step by step, preparing the shutdown in advance, a tested emergency stop for adversaries that work at machine speed, dealing with the adversary, and removing the adversary in one coordinated eviction.
Chapter 8 · Communication	Four principles, a stakeholder matrix for staff, board, customers, regulators, insurer, police and media, one spokesperson, and working with crisis communication specialists.
Chapter 9 · Legal and regulatory	The DORA, Cyber Resilience Act and CER reporting duties, payments and sanctions screening, law enforcement, working with your insurer, and legal hold.
Chapter 10 · Ransomware and extortion	The first hour, measures to slow the spread across the network, scoping before you decide, a pay-or-rebuild decision tree drawn up in advance, negotiation principles, and recovery.
Chapter 11 · Business email compromise	Containing the identity in the right order, the investigation, and the payment dispute with banks and other parties.
Chapter 12 · State-sponsored intrusion	The main state programmes, hunting without malware, operational security during the response, involving the authorities early, and the eviction.

CHAPTER	WHAT IT GIVES YOU
Chapter 13 · Data-theft extortion and 17 more	Extortion without encryption, plus edge devices and mass exploitation, SaaS data theft by phone, extortion that reaches your customers, abuse of admin consoles, AI assistants and agents, AI-driven intrusions, pressure on staff, compromised phones, ransomware in the cloud, fake remote IT workers, developer machines and build pipelines, wipers, identity platform compromise, insiders, DDoS, supply-chain compromise, and incidents at your cloud provider.
Chapter 14 · Recovery and closure	Recovery in order of business impact, restoring onto clean infrastructure, closing the case and the post-incident review.
Chapter 15 · Staying ready	The building blocks, readiness checklists for people, decisions and systems, and how to run a tabletop exercise.
Chapter 16 · Sector overlays	Overlays for eleven sectors, from healthcare and energy to digital providers, professional services, retail and education, plus a target operating model.
Chapter 17 · Isolating vital systems	Knowing what is vital, preparing to isolate it, operating while isolated, and reconnecting safely.
Annexes	The full contact directory, ten holding statements (staff, a warning about calls and messages, customers, customers contacted by criminals, people whose data was affected, media, service desk, suppliers, social media and a closing statement), a notification checklist and filing log, an evidence register, an incident report template, a baseline assessment questionnaire, sources and a glossary. For the Netherlands, an annex with the authorities, sector CSIRTs and contact points.

WHAT EACH OPTION GIVES YOU

TOPIC	THIS EDITION	FULL PLAYBOOK	ADAPTED WITH YOU
Team, roles and mandates	Core roles and mandates to fill in	In full, including the external parties	Worked out with you and agreed with your management
Escalation and the first hours	Severity levels and the first 60 minutes	Also hours 2 to 72, and what follows scenario by scenario	Thresholds set for your organisation, and practised
Scenarios	The first hour, for any scenario	Four scenario chapters and 17 further incident types	Prioritised for your risks and sector
Investigation and containment	An overview	Step by step	Mapped to your systems, logs and suppliers
Communication	One sample message to staff	Stakeholder matrix and ten holding statements	Statements prepared for your audiences

TOPIC	THIS EDITION	FULL PLAYBOOK	ADAPTED WITH YOU
Legal and regulatory	The main deadlines	In full, including DORA, the Cyber Resilience Act, CER, sanctions and legal hold	A notification map for your sector and country
Sector guidance	General guidance for all sectors	Eleven sector overlays and a target operating model	Applied to your organisation
Isolating vital systems	Containing machines and identities (section 05)	Preparing, operating while isolated, and reconnecting	Planned for your vital systems
Testing	Exercise it once a year (section 01)	How to run a tabletop exercise	A tabletop exercise on your own plans, with a debrief

HOW WE CAN HELP

SERVICE	WHAT IT MEANS FOR YOUR INCIDENT READINESS
Adapting your plan	We work through the full playbook with you, map it to your organisation, systems and suppliers, set thresholds and mandates, and agree them with your management.
Capability building	Validating, structuring or scaling your incident response, threat intelligence and security monitoring, with your own people and suppliers.
Executive and CISO support	A vendor-independent sounding board for your chief information security officer (CISO) and security leadership, from tooling and architecture to strategy, board reporting and incident readiness.
Workshops	The First Responder Workshop, a full day of group exercises with a tabletop on your own plans, and the two-hour Board & Executive Workshop for executives and board members. Both come with the full playbook.
Keynotes	Talks on cyber crises and incident response for boards, management teams and events, in English or Dutch.
During an incident	We can introduce you to vetted IR firms and negotiators straight away, and we work alongside your contracted IR provider. We don’t run a 24/7 emergency service ourselves.

> **Next step.** A free first conversation of 30 to 60 minutes, without obligation. Email info@thirteen-delta.com, or read more at www.thirteen-delta.com.

Annex A — Contact tree and escalation directory

Two contact methods and two people per role. Keep this annex printed and stored off the network, and check it regularly, because an outdated contact tree is usually discovered during an incident.

INTERNAL

ROLE	NAME / DEPUTY	PHONE / ALT. CHANNEL	AVAILABILITY
Crisis chair	[Name · deputy]	[Mobile · alt]	[24/7?]
Operational lead	[Name · deputy]	[Mobile · alt]	[ ]
CISO / security	[Name · deputy]	[Mobile · alt]	[ ]
IT infrastructure lead	[Name · deputy]	[Mobile · alt]	[ ]
Communication owner	[Name · deputy]	[Mobile · alt]	[ ]
Legal & privacy / DPO	[Name · deputy]	[Mobile · alt]	[ ]
HR	[Name · deputy]	[Mobile · alt]	[ ]
Scribe / log keeper	[Name · deputy]	[Mobile · alt]	[ ]
OT / facilities (if applicable)	[Name · deputy]	[Mobile · alt]	[ ]
Service desk lead	[Name · deputy]	[Mobile · alt]	[ ]
Product security owner (if we make hardware or software; Cyber Resilience Act)	[Name · deputy]	[Mobile · alt]	[ ]

EXTERNAL

PARTY	CONTACT & REFERENCE	NOTES
Incident response partner	[Firm · 24/7 number · contract ref.]	[Service levels and retainer terms]
Cyber insurer	[Insurer · emergency line · policy no.]	Notify immediately; panel requirements
External counsel	[Firm · name · number]	Legal privilege; review of notifications
National CSIRT / authority	[e.g. NCSC-NL, NCSC-IE, CCB, BSI, CERT-FR · portal]	NIS2 filings; section 06
Data protection authority	[Authority · portal]	GDPR Art. 33
Police cybercrime unit	[Unit · number]	Report number for bank / insurer

PARTY	CONTACT & REFERENCE	NOTES
Crisis communication agency	[Agency · name · number]	Media and stakeholder communication; reachable 24/7
Bank fraud desk	[Bank · emergency line]	Payment recalls
Main managed service providers (MSPs) and suppliers	[Vendor · 24/7 line · account]	Access cut-off procedure
Sector CSIRT or information-sharing and analysis centre (ISAC)	[If applicable]	Sector warnings
Customer messaging platforms (app push, email, SMS, marketing)	[Vendor · admin · emergency stop contact]	Stop sending within the hour
ENISA Single Reporting Platform (Cyber Resilience Act)	[Single Reporting Platform account]	Product vulnerability and incident reports; section 06

Finding your authorities. Your national CSIRT is listed on the CSIRTs Network website (csirtsnetwork.eu), and your data protection authority on the website of the European Data Protection Board (edpb.europa.eu). Some Member States require notice to both the CSIRT and a sector supervisor. If you process personal data across several EU countries, GDPR notifications usually go to your lead supervisory authority.

In the Netherlands. Register and report under the Cyberbeveiligingswet on MijnNCSC (mijn.ncsc.nl); one report also reaches your sector CSIRT and supervisor. Report personal-data breaches with the Meldformulier datalekken of the Autoriteit Persoonsgegevens (datalekken.autoriteitpersoonsgegevens.nl). For an aangifte, call the police on 0900-8844. For business fraud, call your bank first and then the Fraudehelpdesk Zakelijk (088 786 7372). Organisations outside the Cyberbeveiligingswet can report to NCSC voluntarily through the form on ncsc.nl.

Annex B — Triage intake form

The first call to your responders, on one page. Share what you know quickly, even if it is incomplete.

WHO YOU ARE	FILL IN
Caller: name, organisation, role	[ ]
Authorised to decide?	[What can you approve?]
Direct phone and e-mail	[Personal, monitored; no shared mailbox]
Operational point of contact	[Name · number]
Management point of contact	[Name · number]

WHAT IS HAPPENING	ANSWER
1. What do you observe?	[Symptoms, messages, alerts, and since when]
2. What is impacted?	[Systems, data, people, locations]
3. Is it still active?	[Happening now / contained / unknown]
4. Where is it?	[Site, network segment, cloud tenant]
5. Biggest risk if it spreads?	[ ]
6. Actions already taken	[Everything; each action changes the evidence]
7. What do you need?	[Contain / investigate / recover / report]
8. Regulated or personal data?	[Starts legal deadlines; section 06]
9. When did we become aware?	[Date and time (UTC); starts the 24 h and 72 h deadlines]
First severity level	[SEV-1 / SEV-2 / SEV-3; declare high]

Annex C — Decision log

Start it from the first minute, with timestamps in UTC.

DECISION LOG

TIME (UTC)	WHAT WE KNEW	DECISION & RATIONALE	OWNER	REVIEW
[ ]	[Facts vs assumptions]	[What was decided, and why]	[ ]	[Next round]

Next step

With the brackets filled in and the first hour run through once with your team, you have a plan for the first day. The full playbook takes the response further, and we adapt it to your organisation.

The usual way to start is a free conversation of 30 to 60 minutes, without obligation. You tell us how your organisation is set up and what concerns you, and we tell you which gaps we would close first and how we can help.

If you want to work in this template yourself, ask for the Word version of this edition. It is free.

What we do. We give vendor-independent advice to executives and CISOs, and help you build your incident response capability and adapt this plan to your organisation. For response teams and boards we run workshops, and we also give keynotes. We work in English or Dutch.

Email info@thirteen-delta.com, or read more about our services at www.thirteen-delta.com.