

cyberwhy

SERVICE GUIDE

Incident Response and Forensics

What to do when something goes wrong: the first hours, the investigation and the road back to normal.

01 · OVERVIEW

Why it matters

An incident is any event that threatens the confidentiality, integrity or availability of your systems or data: ransomware, a hijacked account, leaked data or an intruder in the network. Incident response is the discipline of doing the right things in the right order, under pressure.

The first decisions matter most: what is switched off, what evidence is kept and who is informed. Working from a plan, with specialists alongside your own team, keeps damage small and keeps the business running.

Typical triggers

- Ransom notes, encrypted files or locked systems
- Unusual logins, new admin accounts or accounts you cannot access
- Unexpected data leaving the network or data found online
- Customers or partners report fraud, strange emails or messages from your domain
- A system behaves oddly after a change and the cause is unclear
- A third party, a provider or authorities tell you about a possible compromise

Who benefits

Management

A calm, clear picture of what is happening and what comes next.

IT and security team

Specialist capacity next to the people who know your systems.

Legal and compliance

Technical facts for decisions on notification duties.

Communications

Reliable information for staff, customers and partners.

In this guide

01 Overview 2
02 What it is, and what it is not 3
03 How it works, step by step 4
04 What you receive 5
05 In practice 6
06 How to prepare 7
07 Questions, references and terms 8
08 How the services fit together 9

02 · SCOPE

What it is, and what it is not

What it is

- + Fast, structured action: contain, investigate, recover, strengthen
- + Done alongside your internal team, which knows the business
- + Evidence based: findings are traced back to logs and artifacts
- + Focused on cause as well as symptoms, so it does not happen again

What it is not

- – Not legal advice: notification duties are decided with your legal counsel
- – Not a promise that every system or all data can be recovered
- – Not only technical: decisions, communication and business continuity are part of it
- – Not something to start only after the investigation: containment comes first

Typical kinds of incident

Ransomware and extortion

Files are encrypted or stolen and payment is demanded. First questions: how far did it spread, are backups intact, is the attacker still inside?

Account takeover and email compromise

Attackers use real accounts to read mail, send fraud or reach systems. First questions: which accounts, since when, what was accessed?

Data breach or exposure

Data is stolen, leaked or left open. First questions: what data, whose, and who may have seen it?

Malware and intrusion

Unknown software or an intruder in the network. First questions: how did they get in, where else are they, what did they do?

03 · PROCESS

How it works, step by step

A typical engagement, from the first conversation to clear next steps. Exact steps and timing are agreed with you when the work is scoped.

01 Contact

Get a first picture and agree how to work together.

- Describe the situation in general terms by phone
- Clarify what is affected, since when and what has been done so far
- Agree who does what and how you communicate safely

YOU PROVIDE

A general description of the situation
Your contact person and decision maker

YOU GET

A clear first picture of what is happening

02 Contain

Stop the damage from spreading and remove the active threat.

- Limit the spread: isolate systems, block accounts and connections
- Remove the active threat while preserving evidence
- Keep the business running where possible, working alongside your internal team

YOU PROVIDE

Access to affected systems and logs
Fast decisions on trade-offs, such as taking a system offline

YOU GET

The incident is contained and the threat removed

03 Investigate

Establish what happened.

- Analyze logs, systems and artifacts to find the origin of the attack
- Reconstruct the methods that were used and the timeline
- Determine impact: which systems and data were affected
- Identify the vulnerabilities the attackers used

YOU PROVIDE

System and log access
Knowledge about normal behavior of your systems

YOU GET

Origin, methods and impact of the attack

04 Recover

Get the business back on its feet.

- Support restoring systems and data from clean sources
- Check that restored systems are clean before reconnecting
- Watch closely after recovery for signs of the attacker returning

YOU PROVIDE

Backups and recovery capacity
Priorities: what must come back first

YOU GET

Support to restore normal operations

05 Strengthen

Make sure it does not happen again.

- Review what worked and what did not in prevention, detection and response
- Close the vulnerabilities the attackers used
- Turn lessons into concrete recommendations for people, process and technology

YOU PROVIDE

Time for a lessons-learned discussion

YOU GET

Actionable recommendations to strengthen security

04 · DELIVERABLES

What you receive

The result is not only a technical file. It answers the questions management, legal and your technical team will ask afterwards: what happened, what was affected and what must change.

01
Timeline
What happened, in which order, reconstructed from evidence.

02
Origin and methods
How the attackers got in and what they did.

03
Impact
Which systems and data were affected.

04
Actions taken
What was contained, removed and restored.

05
Vulnerabilities used
The weaknesses that made the attack possible.

06
Recommendations
Concrete steps to strengthen security, in priority order.

Four questions that drive every decision

1	**What is affected?**	Which systems, accounts and data are involved, and which are still safe?
2	**Is the attacker still active?**	If yes, containment comes first. If not, preserving evidence takes priority.
3	**What data is at risk?**	Personal, financial or confidential data changes who must be informed.
4	**What does it cost the business?**	Which processes stop, and what must come back first?

Whatever kind of incident it is, the first hours are steered by the same four questions. The answers change as the investigation advances.

05 · IN PRACTICE

Seeing it at work

While you wait for help

DO

- Write down what you see, who noticed it and when
- Disconnect affected devices from the network, but keep them powered on unless advised
- Preserve evidence: keep logs, emails, screenshots and the affected machines
- Limit who knows to the people who need to
- Reach colleagues and us by phone or a channel the attacker cannot read

DO NOT

- Do not wipe, reinstall or reset affected systems
- Do not delete logs, emails or files
- Do not log in to affected systems with administrator accounts
- Do not contact the attacker or pay anything before you have advice
- Do not send logs, evidence or credentials through the website form

How forensic work stays reliable

1 Preserve

Copy evidence before touching it, so the original stays intact.

2 Document

Record who did what and when, so findings can be explained and defended.

3 Order of volatility

Capture what disappears first, such as memory and running connections, before disks and logs.

4 Align the clocks

Compare logs from different systems on a common timeline to reconstruct events.

GOOD TO KNOW

Notification duties

Legal

GDPR	A personal data breach may have to be reported to the supervisory authority within 72 hours of becoming aware of it, where it is likely to result in a risk to people (Article 33).
OTHER RULES	Sector rules, contracts and insurance policies may add duties and deadlines.
WHAT TO DO	Involve your legal counsel early. We provide the technical facts you need for those decisions.

FOR AI PROJECTS

Incidents involving AI

AI projects add their own incident types: leaked API keys that run up costs or expose data, prompts that make a model reveal internal information, and agents that take actions they should not. Keep logs of model inputs, outputs and tool use, and know which keys and data sources each project can reach.

06 · PREPARATION

How to prepare

A little preparation makes the work faster, safer and more useful. Here is what helps most.

Before we start

- Keep an up-to-date list of who to call, day and night, with deputies
- Know where your backups are, and test that they can be restored
- Make sure logs are kept long enough and stored where attackers cannot erase them
- Know your critical systems and their order of recovery
- Know who decides on shutting systems down
- Have contacts for legal counsel, insurance and communications ready

Typical ground rules

- + Evidence is preserved and handled so its origin can be shown
- + Actions are agreed with you and written down
- + Information is shared on a need-to-know basis
- + Communication runs over channels the attacker cannot read

Common misconceptions

~~We will just restore from backup.~~	**In practice:** Restoring without finding the cause brings the attacker back. Backups also need to be checked for tampering.
~~Our antivirus would have told us.~~	**In practice:** Many intrusions use legitimate tools and stolen accounts that antivirus does not flag.
~~It is only IT's problem.~~	**In practice:** Incidents stop business processes and may trigger legal duties. Management, legal and communications are involved from the start.

07 · REFERENCE

Questions, references and terms

Frequently asked questions

What should we do first?
Write down what you see, isolate affected devices without switching them off, preserve evidence and call us. Do not wipe or reinstall anything.

Should we switch the machines off?
Usually not. Switching off can destroy evidence in memory. Disconnect them from the network instead, unless advised otherwise.

Do you take over from our IT team?
We work alongside your team. They know your systems and the business, we bring incident experience.

Why should we not use the website form?
Logs, evidence and credentials are sensitive. Describe the situation in general terms and we agree a safe way to share details.

Will you find who did it?
The investigation focuses on origin, methods and impact. Naming attackers is often not possible and not needed to recover and improve.

What happens after recovery?
You get a report with a timeline and recommendations, and the vulnerabilities used are closed.

Reference frameworks and sources

NIST SP 800-61 Rev. 3	Incident response recommendations, aligned with the NIST Cybersecurity Framework 2.0.
ISO/IEC 27035	International guidance on information security incident management.
NIST SP 800-86	Guidance on integrating forensic techniques into incident response.
MITRE ATT&CK	A catalog of attacker techniques that helps describe what happened.
GDPR Articles 33 and 34	Rules on reporting personal data breaches.

Terms in plain language

Containment. Stopping an incident from spreading further.

Eradication. Removing the attacker's access and tools.

Indicator of compromise. A trace, such as a file or address, that points to an attack.

Lateral movement. An attacker moving from one system to others.

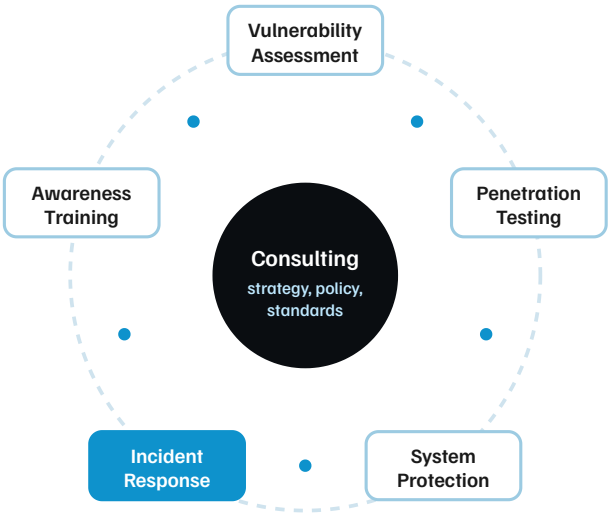
Root cause. The underlying weakness that made the incident possible.

Chain of custody. The record showing who handled evidence and when.

08 · NEXT STEPS

How the services fit together

Security works best as a cycle: find weaknesses, test them, protect, prepare to respond and keep people alert, all guided by a strategy. You can start with any one of them.



Vulnerability Assessment
Finds known weaknesses across your systems and ranks them.

Penetration Testing
Shows what an attacker can actually exploit.

System Protection
Closes gaps with layered, maintained defenses.

Incident Response and Forensics (this guide)
Acts when something gets through, and learns from it.

Security Awareness Training
Prepares the people who meet threats first.

Cyber Security Consulting
Sets strategy, policy and standards that tie it together.

Talk to a specialist about incident response and forensics.

Tell us what you are working on and what you need to protect. For an incident, describe the situation in general terms. Please do not send logs, evidence or credentials through the website form.

EMAIL
info@cyberwhy.com

WEB
cyberwhy.com/services/incident-response-and-forensics/

This guide describes how work of this kind typically runs. Scope, methods, timing and deliverables are agreed with you for your situation, and nothing in it is a guarantee. References to standards and frameworks are for orientation and do not mean certification. © CyberWhy. All rights reserved.