
Cybersecurity incident follow-up

Client information request | Any provider or system

Before we change anything, we need to see what was found. Please attach the report and fill in the gaps below.

If you do not know, write "Unknown". If it has not been checked, mark "Not checked".

Client / company / site

Date completed

Location / affected service

Completed by / role

Phone or email

1. What happened, and who raised the alarm?

Attach the report or email. Name the provider or person and include any ticket number.

2. When did it happen, and is it still happening?

First seen: date and time

Last seen: date and time

Time zone

Still happening?

☐ Yes

☐ No

☐ Unknown

3. Where was the activity seen?

Check all that apply, or choose "Not established".

☐ Internet / network edge

☐ Internal computers / devices

☐ Email / cloud accounts

☐ Not established

Traffic direction:

☐ Into site

☐ Out of site

☐ Both

☐ Unknown

4. Which accounts, systems or addresses were involved?

List accounts, devices, IPs or ports, if known. How were they linked to this client/site?

Impact, actions and supporting records

Please separate what was checked from what was only reported.

Client / company /
site

5. Did anything get through? What backs that up?

- ☐ Only blocked attempts found ☐ Traffic passed; access not confirmed
- ☐ Unauthorized access confirmed ☐ Not established

Who checked? Give the report page, log time or other record behind this answer.

6. Which systems are affected? Name them below.

- ☐ No issue found ☐ Issue found ☐ Not checked

- ☐ No issue found ☐ Issue found ☐ Not checked

What was checked? Note downtime, missing/changed files or exposed records, with evidence.

7. What has already been done?

Who did what, and when? Include blocks, resets, account or remote-access changes.

8. What records are attached, and what is still missing?

- ☐ Incident report / email / ticket ☐ Network / security logs or settings
- ☐ System / account logs or screenshots ☐ Other records / activity logs / captures

List missing records, who is getting them, and when we can expect them.

Save original logs before resets or clearing records. Leave out passwords and unrelated resident details.