Security response kit

A working brief for turning a concern into an owned, verifiable response.

Team _____

System / service _____

Accountable owner _____

Next review _____

Choose one concern. Establish the facts.

Complete this with the person responsible for your systems. Record what is known, what needs checking and where the evidence is held.

What is established?

Affected systems _____

Access _____

Business impact _____

Suspicious activity _____

Accountability _____

Progress _____

Change safety _____

Evidence _____

The action register

Use this as your meeting agenda. Agree actual owners and deadlines; suggested checkpoints below are not security SLAs.

01 Confirm which systems are affected

Match the official advisory to product names, versions and configurations. Include supplier-managed systems.

Suggested owner: IT owner / service provider

Checkpoint: Before deciding the response scope

Bring back: Advisory reference, affected inventory and reason for each conclusion

Owner: _____ Due: _____

Evidence / ticket: _____

02 Name one accountable owner

Agree who coordinates the response and who can approve the change. A supplier name alone is not an owner.

Suggested owner: Business sponsor

Checkpoint: At the next response discussion

Bring back: Named owner, approver and next review time

Owner: _____ Due: _____

Evidence / ticket: _____

The action register, continued

Keep the evidence with the work. Close the loop with the accountable owner.

03 Agree the urgency with your security team

Consider reachable systems, business impact and evidence of exploitation. Check the vendor advisory and CISA's known-exploited list; use these as inputs, not an automatic score.

Suggested owner: Security lead + business owner

Checkpoint: Before agreeing a change deadline

Bring back: Priority rationale, affected services and approved target date

Owner: _____ Due: _____

Evidence / ticket: _____

04 Choose the official fix or mitigation

Ask what the vendor recommends, whether your version is covered and what remains exposed while a permanent fix is pending.

Suggested owner: Technical owner

Checkpoint: At change approval; follow applicable deadlines

Bring back: Change reference, approved remedy and any temporary mitigation

Owner: _____ Due: _____

Evidence / ticket: _____

The action register, continued

Keep the evidence with the work. Close the loop with the accountable owner.

05 Agree a safe change and recovery plan

Define testing, downtime, restart requirements and a recovery route if the service fails. Confirm who will run the checks.

Suggested owner: Change owner / service provider

Checkpoint: Before deployment or the next change

Bring back: Test result, change window and service-recovery instructions

Owner: _____ Due: _____

Evidence / ticket: _____

06 Verify the running system, not just the ticket

Confirm the running version or configuration, repeat the relevant check and verify that the service works. Record unresolved items with an owner and review date.

Suggested owner: Technical verifier + accountable owner

Checkpoint: After deployment, before closure

Bring back: Running-state evidence, check result, service-health result and exception record

Owner: _____ Due: _____

Evidence / ticket: _____

Make the handoff count.

A 15-minute conversation that ends with a decision, a person and a next review.

First 5 minutes

Establish the facts

Which advisory applies? Which systems were checked? What is confirmed, and what is still an assumption?

Next 5 minutes

Agree the response

What is the next action, who owns it and what deadline is justified? What approval, access or supplier response is blocking it?

Final 5 minutes

Define “done”

What evidence will confirm the running system is fixed and the service still works? Who accepts any unresolved exception, and when is it reviewed?

Do not close on “the ticket is done”.

- ☐ Running product version or configuration recorded
- ☐ Relevant check repeated after the change
- ☐ Business service confirmed healthy
- ☐ Exceptions named, owned and given a review date

Decision / agreed next action

Owner / due date / evidence location