Reporting levels and closing periods

Fictional case data and worked reasoning

The manufacturer of a networked control system becomes aware of a severe incident affecting product security on 7 February 2028 at 08:45 UTC. The incident notification following the early warning is confirmed on 8 February at 12:00 UTC. The manufacturer also becomes aware of an actively exploited product vulnerability on 7 February at 10:15 UTC. A documented mitigation measure is available on 15 February at 11:00 UTC. The manufacturer records the two reporting paths separately.

Test point Purpose or comparison Observation Decision		
Knowledge of the incident	7. February, 08:45 UTC Follow-up 8. February, 12:00 UTC	Monthly reference is the actual incident report
Knowledge of exploitation	7. February, 10:15 UTC Measure available on 15. February, 11:00 UTC	From that date, schedule 14 days
Derivatives Derivatives Own reference per reporting category	8 March and 29 February as plan marks	Confirm separate charges

Expected result

Computerised map marks and verifiable knowledge, distribution, measures and user tracks.

Record the reporting method, supported knowledge and time base per line.

Secure early warning, follow-up and actual action with receipts.

Follow the completion, user information and information that is in need of clarification.

Counter-test and next decision

Delete the confirmed incident report. The scheduled closing mark of the incident remains open while the closing reference for the actively exploited vulnerability is still available.

Reporting levels and closing periods

For your observation, specify a findable document.

Run the two CRA reporting branches on a consistent time basis with actual transmissions.

Verification identification, legal entity and date of processing and responsible body

Product, affected version and responsible role

Detection of the trigger and knowledge per mode of reporting with time

Early warning and follow-up with receipts

Correction or risk reduction and actual availability

Closing stamp, actual shipping and user information

Reporting levels and closing periods

Refer remedial and post-test to the original test order.

Findings and supporting evidence

Correction order with product effect and time reference

Tested follow-up test with date, observation and version documentation

Full file of transmission and decision

Release by and on the open order and date