

AUTOMATE **Advanced** 45 MIN · UPDATED 2026-09-30

Investigate a security incident and draft the response timeline.

Use Security Copilot to support an incident investigation and produce a structured, defensible response timeline as the investigation unfolds.

MICROSOFT 365

Word

Teams

WORKS WITH

Security Copilot

Business Outcome

Faster, more complete incident documentation during and after a security event, when accuracy and speed both matter.

Workflow Steps

Step 1: Start the timeline the moment the incident is confirmed

Security Copilot

Have Security Copilot begin correlating alerts and log entries around the incident's start time as soon as it's confirmed, rather than reconstructing the timeline from memory after the fact.

Step 2: Ask for a structured, evidence-linked timeline

Security Copilot

Request specific timestamped entries — first alert, actions taken, systems affected, containment steps — each linked back to the source log or alert, not a narrative summary that can't be individually verified.

PROMPT

Build an incident timeline for the suspicious login activity flagged on account `jdoue@company.com` starting at 2:14am. Pull the relevant sign-in logs and alert data, and list each event with its exact timestamp and source log reference.

Step 3: Update it live as the investigation progresses

Security Copilot

Keep feeding new findings and containment actions into the same timeline as the response continues, rather than building a separate summary at the end that has to be reconciled with real-time notes.

Step 4: Have the incident lead validate before it's finalized

Word

Export the timeline into Word and have the incident lead read it against the raw logs entry by entry, not just skim for overall plausibility.

This becomes the official record for the post-incident review and any external or regulatory reporting, so an unverified timestamp or misattributed action here carries real consequences later.



✓ Check the work

- Verify every timestamped entry against the actual source log – an incident timeline with an inaccurate detail undermines the whole investigation.
- Confirm no gap in the timeline was silently filled with an assumption instead of being marked as unknown.
- Cross-check the timeline against any parallel notes taken by responders during the live incident.

Expected Outcome

A structured, evidence-linked timeline of the incident – detection, actions taken, resolution – ready for the post-incident review.

Want help rolling this out across your team? **Go to Liminals.Tech** 📄