

# Initial SOC triage: first 15 minutes | v7

Start: select C5, Ctrl+; then Space, then Ctrl+Shift+; then Enter. Workstation must use Eastern Time. Gold = selections.

Act on urgent harm now. Document throughout; preserve evidence and use authorized containment at any time. Bands start at analyst triage.

**Process tree → Parent process → Activity timeline → File creation events → Network activity**

|               |                                                                                                                                                                |                            |                   |                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|-------------------|--------------------------------------------|
| CASE          | Case / alert ID                                                                                                                                                |                            | Local priority    |                                            |
|               | Analyst name                                                                                                                                                   |                            | Eastern zone      |                                            |
|               | Alert generated UTC                                                                                                                                            |                            | Queue age (min)   |                                            |
| START         | START HERE<br>Eastern date & time                                                                                                                              |                            | Start time UTC    |                                            |
|               | Decision recorded UTC                                                                                                                                          |                            | Target (min)      | 15                                         |
|               | Primary host / account / tenant                                                                                                                                |                            | Triage time (min) |                                            |
|               | Original alert severity                                                                                                                                        |                            | Repeated hour     |                                            |
| Minutes       | Analyst action                                                                                                                                                 | Findings / decision / gaps | Step status       | Evidence IDs   v7<br>Case: [enter case ID] |
| 0-1<br>DETECT | READ THE ALERT                                                                                                                                                 |                            |                   |                                            |
|               | Read the full alert: rule, event, source, entities and event time. Record case, analyst and triage start above.<br>[NIST SP 800-53 Rev. 5: AU-3 / AU-8 / IR-5] |                            | Not started       |                                            |
|               | Finding recorded UTC                                                                                                                                           |                            |                   |                                            |
| 1-3<br>DETECT | CHECK WHAT IS NORMAL                                                                                                                                           |                            |                   |                                            |
|               | Is this normal? Check role, baseline and approved changes; corroborate the alert or explain the false positive.<br>[NIST SP 800-53 Rev. 5: AU-6 / SI-4]        |                            | Not started       |                                            |
|               | Finding recorded UTC                                                                                                                                           |                            |                   |                                            |

| Minutes          | Analyst action                                                                                                                                                                                                          | Findings / decision / gaps | Step status | Evidence IDs   v7<br>Case: [enter case ID] |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|-------------|--------------------------------------------|
| 3-7<br>DETECT    | <b>BUILD THE PICTURE</b>                                                                                                                                                                                                |                            |             |                                            |
|                  | Identify host/user/IP/app/owner. Start with 24-hour activity and alerts; compare peers and before/after events. Record window, peers, matches and gaps.<br>[NIST SP 800-53 Rev. 5: IR-4 / AU-6 / SI-4]                  |                            | Not started |                                            |
|                  | Finding recorded UTC                                                                                                                                                                                                    |                            |             |                                            |
| 7-10<br>DETECT   | <b>TRACE THE ACTIVITY</b>                                                                                                                                                                                               |                            |             |                                            |
|                  | Examine the process tree, parent, command line, children, files and connections, or the equivalent identity/cloud event chain.<br>[NIST SP 800-53 Rev. 5: AU-6 / SI-4]                                                  |                            | Not started |                                            |
|                  | Finding recorded UTC                                                                                                                                                                                                    |                            |             |                                            |
| 10-13<br>RESPOND | <b>MAKE THE INITIAL CALL</b>                                                                                                                                                                                            |                            |             |                                            |
|                  | Assess scope, impact, severity and uncertainty. Apply incident criteria; notify lead and use authorized containment. Preserve evidence; log approval, action and result.<br>[NIST SP 800-53 Rev. 5: IR-4 / IR-6 / AU-9] |                            | Not started |                                            |
|                  | Finding recorded UTC                                                                                                                                                                                                    |                            |             |                                            |
| 13-15<br>RESPOND | <b>SUMMARIZE AND HAND OFF</b>                                                                                                                                                                                           |                            |             |                                            |
|                  | Summarize trigger, checks, findings and assessment. Record next action/owner, due and handoff UTC, acknowledgment and open gaps.<br>[NIST SP 800-53 Rev. 5: IR-5 / IR-8]                                                |                            | Not started |                                            |
|                  | Finding recorded UTC                                                                                                                                                                                                    |                            |             |                                            |

N/A needs a reason. No matches applies only to checked coverage. Detect = orange; Respond = red. Detailed mappings: References.

| Minutes       | Analyst action                            | Findings / decision / gaps | Step status            | Evidence IDs   v7<br>Case: [enter case ID]                |
|---------------|-------------------------------------------|----------------------------|------------------------|-----------------------------------------------------------|
| <b>ASSESS</b> | Immediate harm / spread indicators?       |                            | Assessed severity      |                                                           |
|               | Preliminary assessment                    |                            | Assessment uncertainty |                                                           |
|               | Decision                                  |                            | Decision guidance      | Definitions: Team Setup                                   |
|               | Rationale, evidence, gaps and alternative |                            | Incident declaration   |                                                           |
| <b>ACTION</b> | <b>Action taken and result</b>            |                            | Declared by            |                                                           |
|               | <b>Action UTC</b>                         |                            | <b>Declared UTC</b>    |                                                           |
|               | Runbook / authority / approver            |                            | Authority unclear?     | Escalate to the lead. Record request and approval status. |

| Minutes | Analyst action                   | Findings / decision / gaps          | Step status       | Evidence IDs   v7<br>Case: [enter case ID] |
|---------|----------------------------------|-------------------------------------|-------------------|--------------------------------------------|
| HANDOFF | Handoff owner and channel        |                                     | Business impact   |                                            |
|         | Handoff sent UTC                 |                                     |                   |                                            |
|         | Next action and owner            |                                     | Observed scope    |                                            |
|         | Next action due UTC              |                                     |                   |                                            |
|         | Open gaps                        |                                     | Recovery referral |                                            |
|         | Next update UTC                  |                                     |                   |                                            |
|         | Ticket notes and evidence saved? |                                     |                   |                                            |
|         | Recipient acknowledged?          |                                     |                   |                                            |
|         | Handoff review                   | Complete case and assessment fields |                   |                                            |