DEFCON-APP

War Room Checklist

Before the Incident:

- Have a written plan (team, playbook, contact list, critical assets, etc.)
- Train, rehearse and test the plan
- Prepare a physical and/or virtual space (video conferencing, whiteboard, etc.)
- Ensure access to necessary tools (incident response systems, dashboards, communication)
- Have backup gear ready (5G router, non-domain joint PCs, etc.)
- Ensure sufficient supplies for extended work sessions (coffee, snacks, etc.)

During the Incident:

- Gather all essential personnel (both internal and external if needed)
- Assess GDPR or NIS2 issues
- Set up real-time communication channels (messaging apps, email, phone lines)
- Display live data (status dashboards)
- Have a visual timeline on screen or whiteboard
- Collect evidence
- Log key decisions and actions taken (use the decision log template)
- Monitor escalation levels and update as needed
- Communicate with stakeholders regularly (internal team, leadership, external partners)

Post-Incident:

- Conduct a debrief and document the timeline of events
- Review the incident response process and log any improvements
- Prepare a post-incident report and lessons learned
- Conduct a lessons learned process with the team
- Update the war room setup for future incidents