What I Learned

This week I studied the NIST Incident Response Lifecycle. It includes four phases: preparation, detection and analysis, containment/eradication/recovery, and post-incident activity. Preparation means having policies, tools, and trained staff in place before an incident happens. Detection and analysis involve collecting logs, alerts, and reports to confirm and scope the issue. Containment, eradication, and recovery focus on isolating affected systems, removing malicious code, and restoring normal operations. Post-incident activity documents lessons learned, updates procedures, and strengthens prevention.

The principle of “minimum necessary” is important in incident response. Investigators should only gather information that directly relates to the incident, not everything available. This limits unnecessary exposure of personal data and reduces legal or ethical risks. In *Ethics in Technology* (Weber, 2025), harm prevention is described as a central responsibility of technology professionals. By applying the minimum necessary rule, responders protect privacy while still preserving useful evidence. This shows how the NIST framework aligns with ethical decision-making that avoids causing extra harm.

How I’ll Apply It

If I were responding to a suspected malware infection on a professor’s computer at a small college, I would begin by collecting only what is needed. First, I would capture system event logs to determine when unusual activity started and what processes were affected. Second, I would preserve a memory snapshot to detect any malicious programs running in real time. What I would avoid is collecting all the professors' personal files or email content. That would exceed the incident's scope and violate the principle of minimum necessary without clear consent or policy approval. Following this approach keeps the investigation effective while protecting privacy and staying aligned with both NIST guidance and ethical obligations.

Muddiest Point

I am still unsure about the chain of custody requirements in different contexts. For example, what is the minimum level of logging needed for evidence to hold up in a campus or small-business case versus a federal case? I am also unclear about whether redacting sensitive data from logs later breaks the chain of custody, since the file would no longer match its original hash. Finally, I wonder how much containment should prioritize keeping

services online versus immediately isolating systems when both privacy and availability are at risk.

Portfolio Note

- Incident response reflection- Shows I can connect NIST guidance with ethical reasoning
- Evidence handling question- Highlights my awareness of open issues in chain of custody and redaction.
- Privacy and policy example – demonstrates ability to apply “minimum necessary” in a realistic workplace case.

AI Use Note

I used ChatGPT to help clarify definitions of the NIST incident response lifecycle phases and to refine how I explained the “minimum necessary” principle in relation to ethics and policy.

References

National Institute of Standards and Technology. (2023). *Computer security incident handling guide*. https://csrc.nist.gov/pubs/sp/800/61/r3/final

Weber, E. (2025). *Ethics in technology* (OER ed.).