What Can be Improved?

Identifying weaknesses in the response to an incident can help organizations to better prepare and respond in the future, potentially reducing the amount of damage that malicious actors can conduct, and minimizing the impact to the business. This lesson will cover how security teams and incident response stakeholders should identify where they lacked, and how it should be addressed.

During the post-incident meeting, all stakeholders should take the appropriate time to reflect on the issues they had during the process. Did someone mess up evidence collection? Were the team lacking resources such as laptops and blank hard drives? Once weaknesses have been identified, it is important to discuss how the organization can ensure that they don't happen in future incidents. Questions that could be asked include:

- What limitations were there regarding tooling?
- What limitations were there regarding procedures and guidelines?
- Did any individuals or departments hinder the incident response? How?
- Consider how each of the NIST Incident Response Lifecycle stages was weak, and how it can be improved in terms of resources, personnel, and documentation.

Now that the weaknesses have been uncovered, it is important to ensure that there is actually change. There's no point highlighting these issues if they won't be fixed. This is the perfect time to discuss with management the need for resources to strengthen the response to future incidents. This can include:

- More budget for security personnel such as Forensic Analysts, Incident Responders, Incident Commanders, etc.
- More budget for personnel in other departments, such as Legal, Public Relations, Communications, or Human Resources.
- More budget for tools that can assist with incident response activities.
- Review of documentation such as run-books, policies, and procedures.