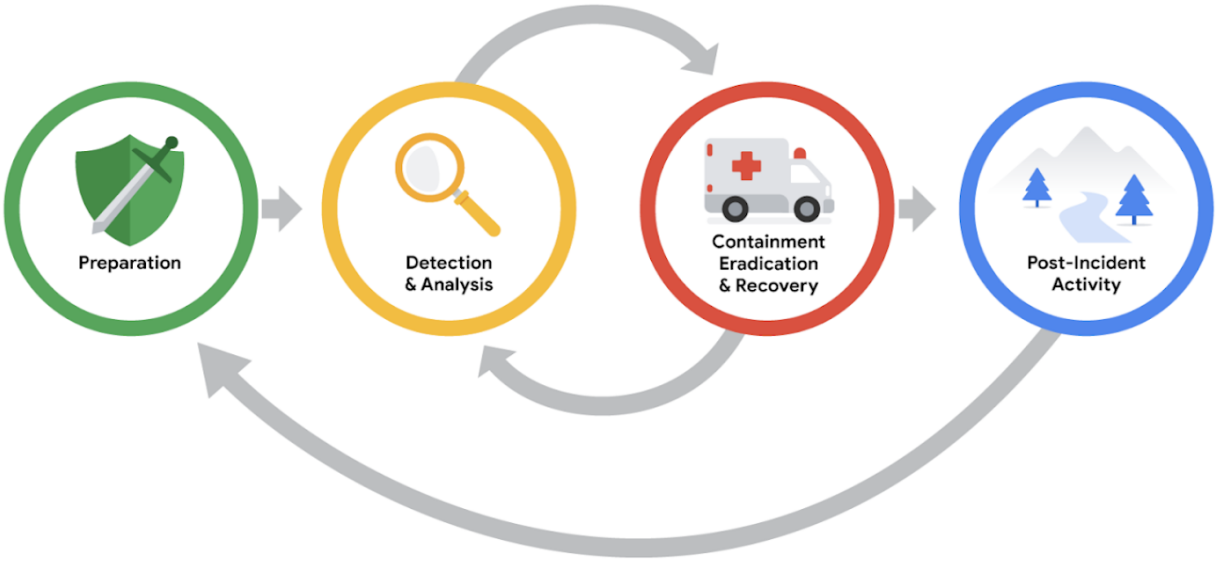
Post-incident review

Previously, you explored the Containment, Eradication and Recovery phase of the NIST Incident Response Lifecycle. This reading explores the activities involved in the final phase of the lifecycle: **Post-incident activity**. As a security analyst, it's important to familiarize yourself with the activities involved in this phase because each security incident will provide you with an opportunity to learn and improve your responses to future incidents.

Post-incident activity

The Post-incident activity phase of the NIST Incident Response Lifecycle is the process of reviewing an incident to identify areas for improvement during incident handling.



Lessons learned

After an organization has successfully contained, eradicated, and recovered from an incident, the incident comes to a close. However, this doesn’t mean that the work of security professionals is complete. Incidents provide organizations and their security teams with an opportunity to learn from what happened and prioritize ways to improve the incident handling process.

This is typically done through a **lessons learned meeting**, also known as a post-mortem. A lessons learned meeting includes all involved parties after a major incident. Depending on the scope of an incident, multiple meetings can be scheduled to gather sufficient data. The purpose of this meeting is to evaluate the incident in its entirety, assess the response actions, and identify any areas of improvement. It provides an opportunity for an organization and its people to learn and

improve, not to assign blame. This meeting should be scheduled no later than two weeks after an incident has been successfully remediated.

Not all incidents require their own lessons learned meeting; the size and severity of an incident will dictate whether the meeting is necessary. However, major incidents, such as ransomware attacks, should be reviewed in a dedicated lessons learned meeting. This meeting consists of all parties who participated in any aspect of the incident response process. Here are some examples of questions that are addressed in this meeting:

- What happened?
- What time did it happen?
- Who discovered it?
- How did it get contained?
- What were the actions taken for recovery?
- What could have been done differently?

Besides having the opportunity to learn from the incident, there are additional benefits to conducting a lessons learned meeting. For large organizations, lessons learned meetings offer a platform for team members across departments to share information and recommendations for future prevention.

Pro tip: Before a team hosts a lessons learned meeting, organizers should make sure all attendees come prepared. The meeting hosts typically develop and distribute a meeting agenda beforehand, which contains the topics of discussion and ensures that attendees are informed and prepared. Additionally, meeting roles should be assigned in advance, including a moderator to lead and facilitate discussion and a scribe to take meeting notes.

Recommendations

Lessons learned meetings provide opportunities for growth and improvement. For example, security teams can identify errors in response actions, gaps in processes and procedures, or ineffective security controls. A lessons learned meeting should result in a list of prioritized actions or actionable recommendations meant to improve an organization’s incident handling processes and overall security posture. This ensures that organizations are implementing the lessons they’ve learned after an incident so that they are not vulnerable to experiencing the same incident in the future. Examples of changes that can be implemented include updating and improving playbook instructions or implementing new security tools and technologies.

Final report

Throughout this course, you explored the importance that documentation has in recording details during the incident response lifecycle. At a minimum, incident response documentation should describe the incident by covering the 5 W's of incident investigation: *who*, *what*, *where*, *why*, and

when. The details that are captured during incident response are important for developing additional documents during the end of the lifecycle.

One of the most essential forms of documentation that gets created during the end of an incident is the **final report**. The final report provides a comprehensive review of an incident. Final reports are not standardized, and their formats can vary across organizations. Additionally, multiple final reports can be created depending on the audience it's written for. Here are some examples of common elements found in a final report:

- **Executive summary**: A high-level summary of the report including the key findings and essential facts related to the incident
- **Timeline**: A detailed chronological timeline of the incident that includes timestamps dating the sequence of events that led to the incident
- **Investigation**: A compilation of the actions taken during the detection and analysis of the incident. For example, analysis of a network artifact such as a packet capture reveals information about what activities happen on a network.
- **Recommendations**: A list of suggested actions for future prevention

Pro tip: When writing the final report, consider the audience that you're writing the report for. Oftentimes, business executives and other non-security professionals who don't have the expertise to understand technical details will read post-incident final reports. Considering the audience when writing a final report will help you effectively communicate the most important details.

Key takeaways

Post-incident actions represent the end of the incident response lifecycle. This phase provides the opportunity for security teams to meet, evaluate the response actions, make recommendations for improvement, and develop the final report.

Revision #2
Created 2023-10-25 20:58:51 UTC by naruzkurai
Updated 2023-11-01 01:10:46 UTC by naruzkurai