Importance of Documentation

As mentioned previously in this domain, maintaining an incident response plan (IRP) and response run-books for different scenarios is key to quick and straightforward responses. By recording every incident in detail, if a similar one occurs, analysts can refer to the documentation of the old incident for guidance. The following documentation could be updated after an incident, if appropriate:

Incident Response Case Notes

Whatever tool the organization uses to record security investigation notes in (such as ServiceNow and IBM Resilient) should be completely updated to ensure that the case contains everything it should, such as information from all stages of the incident response lifecycle, artefacts should be included, such as file names, file hashes, IP addresses, domain names, etc. Attachments should be added to the case, including emails sent to stakeholders, copies of malicious files, log files, and anything else deemed important to the investigation.

Incident Response Plan

Maybe the overall response process could be improved, which should be discussed and any changes be implemented to the organization's incident response plan (IRP). This could include changes to stakeholders that are part of the incident response team, new methods for secure communication, changes to contact numbers or email addresses, and other details that are consistent across all potential incidents.

Incident Run-Books

Reviewing run-books for the type of incident that has occurred can help to improve future responses by providing guidance for analysts that respond to the incident in the future. The more detail in these run-books the better, as it'll encompass more potential scenarios, working to make future responses more structured and organized.

You can find lots of example run-books here to get a feel for what they look like and include.

Organization Policies

Maybe the incident occurred as a result of an action that wasn't properly restricted by organizational policies, such as a user downloading software from the internet because the Acceptable User Policy doesn't prohibiting them from doing so. Updating this policy stating that all software should be acquired from an internal repository, or employees can create a ticket with the IT Service Desk to have software downloaded for them from known safe sources will prevent future incidents, or at least provide solid accountability. Another example would be an internet-facing system that didn't have updates and security patches applied, because there is no vulnerability management or patching policy, requiring the system owners to keep it up-to-date and secure. Implementing this could again help prevent similar incidents in the future.