Reporting Considerations

There are a number of things we need to consider when writing a report or similar documentation post-incident. We will be looking at the following considerations in this lesson:

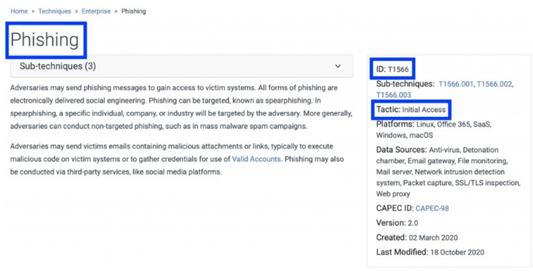
- Report Audience
- Incident Investigation
- Screenshots and Captions

As mentioned in the previous lesson, incident reports will typically have a number of different audiences, especially Executive Board members, IT staff, and the wider security team. We need to ensure that each section is tailored to the intended audience, making sure it has the appropriate level of detail and technical jargon.

- **Executive Summary –** This should be short, sweet, and talk about the whole incident at a high-level. This means technical terms and phrases should be avoided and the incident should be explained using business risks. For example, if an incident occurred where the company's website was defaced, the executive summary should talk about how the incident was discovered, how it was resolved, and how this could've affected the business if it wasn't addressed quickly (loss of sales, reputation damage, loss of customer trust, etc). It's also important to remember that Executives are extremely busy, and they will likely not read any more than the executive summary – we need to make this as impactful as possible.
- **Rest of the Report –** The remainder of the report will typically be aimed at technical staff so this should include a lot of detail, annotated screenshots, and should use technical language where appropriate.

This section needs to be detailed. Really detailed. Any points you make need to be backed up with evidence, otherwise it is just speculation (try not to do this – if there's no proof, you can't prove it actually happened). For example, let's pretend we're investigating a system that was compromised by a phishing email that contained a Microsoft Word document with a malicious macro which downloads malware to the system. We can state a phishing email was the initial access vector, but we need to provide evidence. This could include a screenshot of the email, a screenshot of the malicious macro contents, a screenshot of the SIEM logs showing the outbound beaconing and download of the malware, etc. Try to follow the below approach: **Make a Point > Provide Evidence.**

For security teams it's helpful to also include the MITRE ATT&CK tactics that were used. Continuing with the above example regarding phishing, the following would be applicable:



Therefore, when explaining these stages of the incident in our report, we would mention T1566 for phishing initial access, and T1204.002 for code execution using a malicious file (attached to the phishing email).

Screenshots are a great way to provide evidence, remember the saying "a picture speaks a thousands words"? Well it really does apply with security reports (not just incident handling, but also penetration testing!). Above we mentioned the 'Make a Point > Provide Evidence' process, and screenshots are a perfect way to do this. If you're talking about a port scan conducted from one internal system to another and you have PCAPs available, then screenshot Wireshark with a filter showing the scanning activity! If you're stating that an adversary moved between systems using password re-use then provide screenshots of login events from the SIEM, local access logs, or anything else that shows this activity.

All images should also be captioned with a short sentence or two, summarising what is being shown in the screenshot. The helps people to quickly digest the information in case they don't fully understand what they're looking at (such as output from a tool they've never used before).