**Material Development Template**

**1. Topic Information**

* **Title**: APT & Zero Day Exploits
* **Description**: This module will cover what an APT is, Aswell as how Zero day exploits can play a role in APT. It will also give a real-world example of an APT group that has done damage in the real world.

**2. Learning Objectives**

* **Primary Objectives**: Participants should gain knowledge on APT attacks and understand what it entails, including why they can be so dangerous. This will include what a zero day attack is as it is often used hand in hand.
* **Secondary Objectives**: In addition, participants should have an idea of how to prevent an APT group from getting into their system, and some common ways to combat an attack from one of these groups.

**3. Target Audience**

* **Age Group**: Adults
* **Skill Level**: Intermediate.
* **Specific Needs**: N/A.

**4. Material Types and Formats**

* **Main Format**: Slideshow.
* **Supplementary Materials**: Quiz/Kahoot.
* **Accessibility Features**: None

**5. Instructor Guide**

* **Synopsis**: Slideshow is for learning. Then the quiz/Kahoot are the same questions. Group discussion questions linked Aswell.
* **Key Points**: Emphasize the difference from APT and malware, but that malware can be used in an APT group.

**6. Activities and Engagement Strategies**

* **Interactive Activities**: Paper quiz along with a Kahoot that has the same questions.
* **Engagement Tips**: Engage users my emphasizing that this is a real issue for large or even medium sized companies. Our government is a huge target for these APT groups. Do the quiz or Kahoot before and after to show the change in knowledge/awareness and also use group discussion questions as it fits.

**7. Assessment**

* **Evaluation Method**: Quiz/Kahoot.
* **Success Criteria**: 7/10 correct on the quiz at the end of the session.

**8. Sources and References**

* **Primary Sources**: <https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/>
* <https://www.ibm.com/topics/advanced-persistent-threats>
* <https://www.fbi.gov/wanted/cyber/apt-41-group>
* <https://www.ibm.com/topics/zero-day>
* <https://www.imperva.com/learn/application-security/zero-day-exploit/>
* <https://www.crowdstrike.com/cybersecurity-101/zero-day-exploit/>

**9. Legal and Compliance Checks**

* **Copyright Compliance**: Ensuring all used materials are correctly licensed or credited.
* **Privacy Considerations**: Ensuring content complies with privacy laws, especially if the personal data of learners might be involved.

**10. Technology Requirements**

* **Needed Software or Hardware**: Instructor needs a computer with PowerPoint on It and access to the internet, Audience needs a device with internet access to run Kahoot.
* **Technical Support Resources**: N/A.

**11. Feedback Mechanism**

* **For Learners**: Google Form
* **For Instructors**: Google Form

**12. Review and Update Schedule**

* **Review Frequency**: Every few months with new updated tactics if any.
* **Update Protocols**: Research current phishing trends.

**13. Delivery Modalities**

* **Online**: Read through the slides and take the quiz
* **In-Person**: Present the slides and then do group discussion questions before taking a quiz
* **Hybrid**: Mix of presenting and reading slides, then group discussions together and possibly do the quiz online or if in person on a Kahoot.

Blooms taxonomy: <https://www.celt.iastate.edu/instructional-strategies/effective-teaching-practices/revised-blooms-taxonomy/>