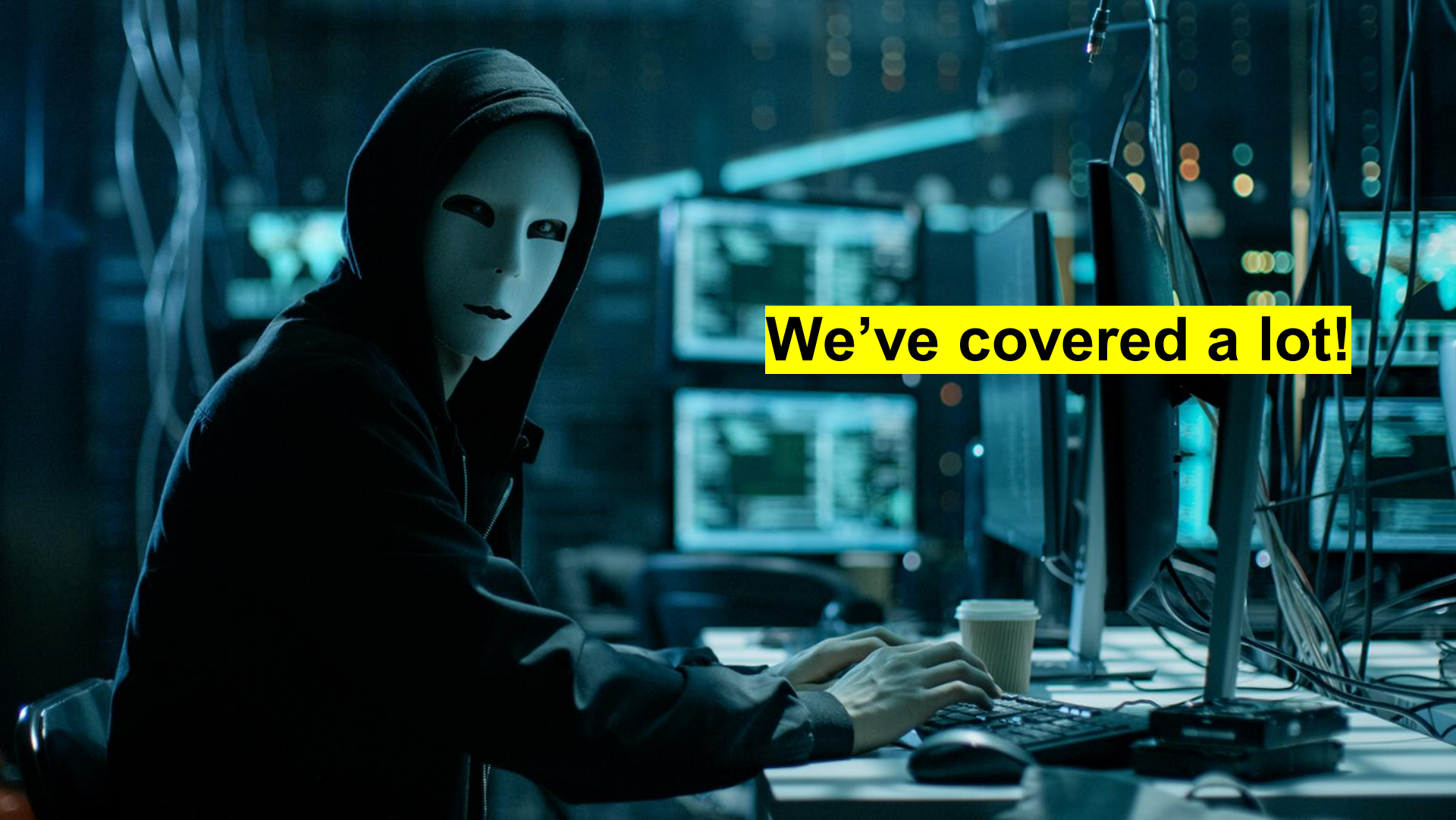
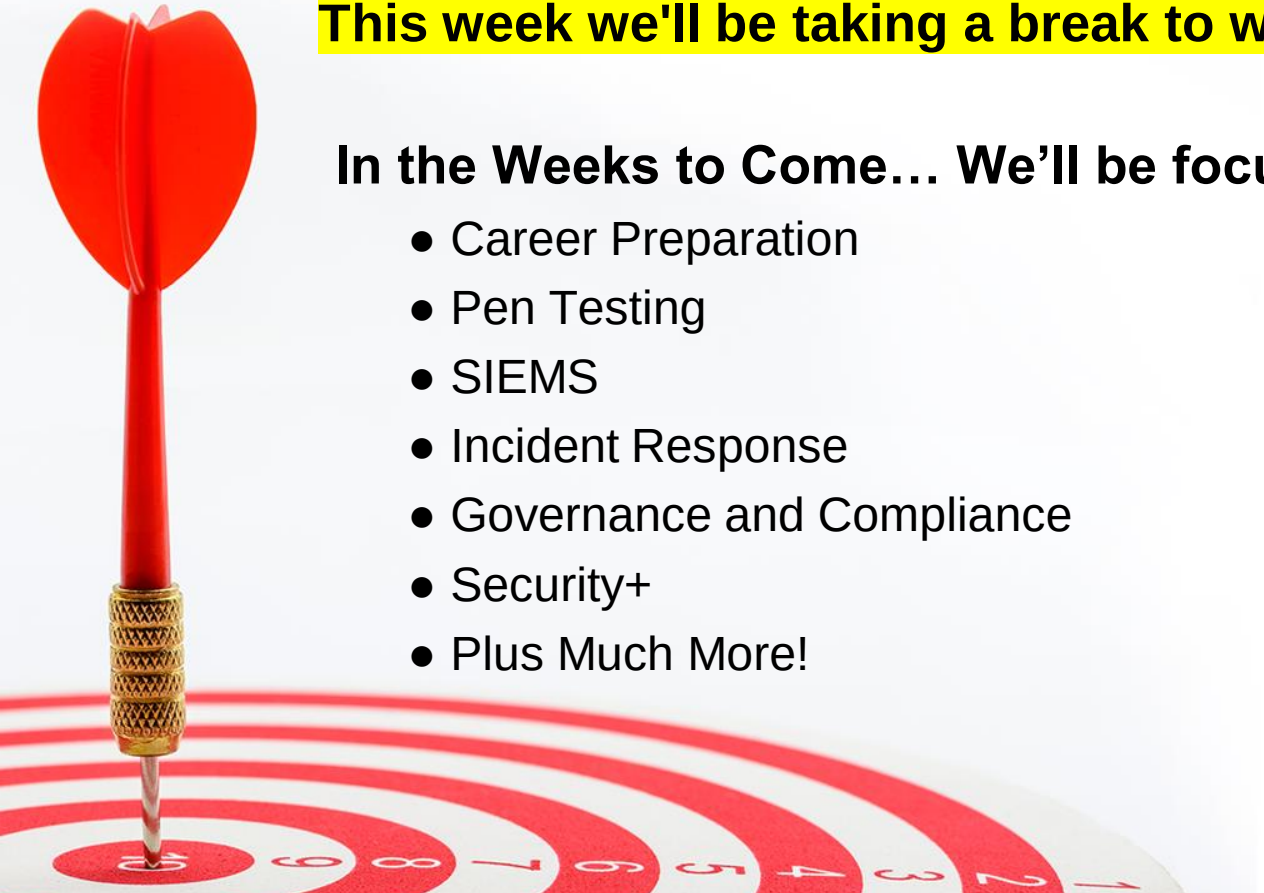
Cybersecurity

Project Week

Malware Research and Analysis


We’ve covered a lot!

Agenda for the Weeks Ahead!



This week we'll be taking a break to work on projects.

In the Weeks to Come… We'll be focused on:

- Career Preparation
- Pen Testing
- SIEMS
- Incident Response
- Governance and Compliance
- Security+
- Plus Much More!

This Week: Projects!

For your Project, you will:

- Select a Malware instance or class
- Document how it works, its scope, and extent of impact
- Document technical findings from existing analyses and industry reports
- Discuss containment and training strategies

SUGGESTED TIME:
All Week!

Your Project Deliverables:

Over the course of this week, you will be working in teams of four to prepare a:

- 10-12 minute presentation
- 4-5 page report

SUGGESTED TIME:
All Week!

Your Presentation and Report should include the following:

- Overview of the Malware
- Technical Expose
- Containment Strategy
- Awareness Training

SUGGESTED TIME:
All Week!

Example Malware:

Adylkuzz
GandCrab
Cryptominer
NotPetya
Satan

Note: Links are to the malware analyses run on Any.run

Overview of the Malware

Answer the following questions:

Definition of the malware and what it does
- Include at least one conceptual diagram
- Who made it
- When was it first discovered

Case study
- Discuss at least once case of the malware and problems causes

Severity scope of the impact
- How many devices/users/ orgs were affected
- Financial cost at the level of all people affected
- How the community responded
- How much of a risk it remains and future outlook

Definition of Key Terms that are new (3–5 key technical terms)

Technical Expose (Malware Analysis):

Set-up:

- Navigate to: https://any.run/
- Register for an account. Be sure to check your email and activate your account before proceeding.

- Use the **Student Instruction Handout** for more details on how to read the malware reports on Any.run

Instructions:

Analyze your assigned malware using the links provided.

Use the Technical Expose Template for the Analysis to guide you with your report

Technical Expose:

Answer the following questions:

Is this a remote or local exploit (does it attack a protocol or does it have to be on the target machine to be dangerous)?

How is it delivered (uploaded as a raw executable? Embedded in a Word, PDF, or PPT document, and delivered via phishing?)

What were the notable malware campaigns in which this malware was used?
How big were they (how many people affected)?
Who launched them (was it a bunch of script kiddies? Russian hackers, as in the case of the NotPetya campaign against Ukraine? etc.).

Behavior

- **Does the malware connect to the network? If so, why, and what does it do?**
- **Does the malware modify the target's filesystem? Why, and how?**
- **Is the malware known to "hide" itself somehow? If so, how? How does this technique work?**

Containment Strategy and Awareness Training

Select one of the following organizational structures

Government Agency/ Organization

Small to Mid-Size Private Organization

Containment Strategy

Scope of Impact:

- Summarize the scope of the attack surface vulnerable to this sample. Include information on:

Severity:

- Explain how severe this malware is. Based on this information, recommend a timeline for patching.

Solution:

- Explain the steps to fix a computer that has been affected; which patches to use, if any; and strategies for preventing future attacks.

What to Patch:

- Which services/software/etc. need to be upgraded, with a link to the patch to install. These can be easily found on most vulnerability databases.

Severity and Timelines: Suggest a "criticality level"/timeline for implementing the patches based on the organization you chose. How big is the threat and how quickly should patches be implemented

NOTE: Use the Containment Strategy and Awareness Training Template to guide you with your report.

Awareness Training

Write up a "how-to" with the following sections.

Identification: *Explain the steps to identify an infection with your sample. Refer to your Behavioral Analysis results from before, and list the prominent pieces of suspicious activity.*

Quarantine: *Based on your Behavioral Analysis results from before, explain the steps users should take to minimize damage to their computer and the rest of the network if they find their device to be infected.*

Escalation: Suggest a simple escalation protocol in the event an end user finds a compromised device. Who and which other teams should be notified?

NOTE: Use the Containment Strategy and Awareness Training Template to guide you with your report.

Every group must present a proposal that is approved by the instructor.

(Proposal should include topic + list of articles and other resources you will use to complete the report and presentation).

Be creative and make your topic **interesting** and a bit off the beaten path.

Due Dates:

Presentations will be on Day 3 of class

Reports will be due the following week

Requirements

For your presentation:

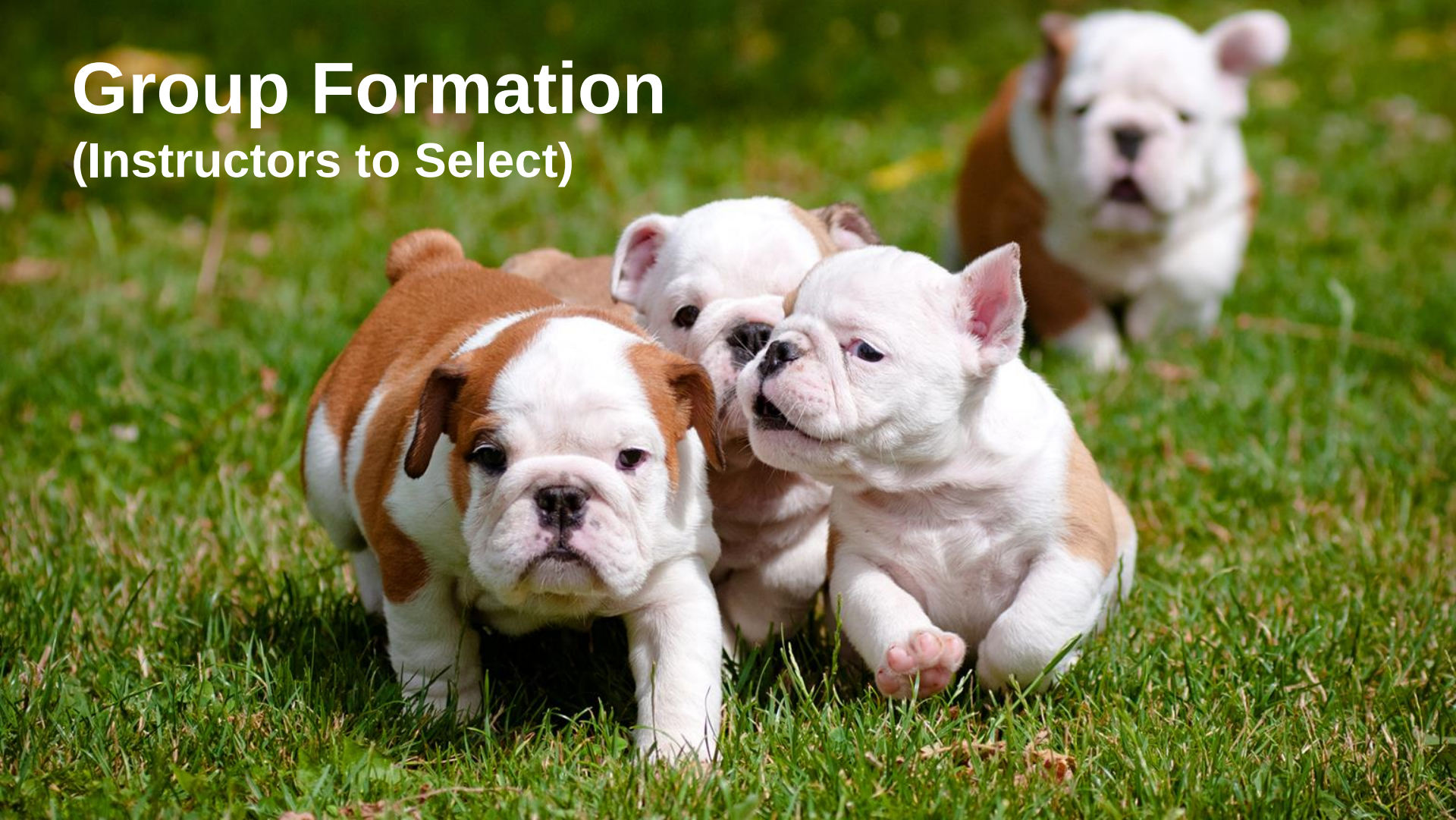
- Focus on both developing clean slides with technical accuracy and depth
- Try to make the presentations engaging
  (use this as an opportunity to practice your oral communication)
- Consider what in your 4-5 page report is relevant to include in your 10-12 minute presentation
- Each person must speak for at least 2 minutes
- You must be prepared to answer questions

For your report:

- At least 4–5 pages (double spaced)
- Include at least one diagram
- Report should cover the same themes as your presentation
- Include works cited at the end

You should consider this to be a **key part** of your job application materials.

Group Formation
(Instructors to Select)



Questions