



HARVARD EXTENSION SCHOOL

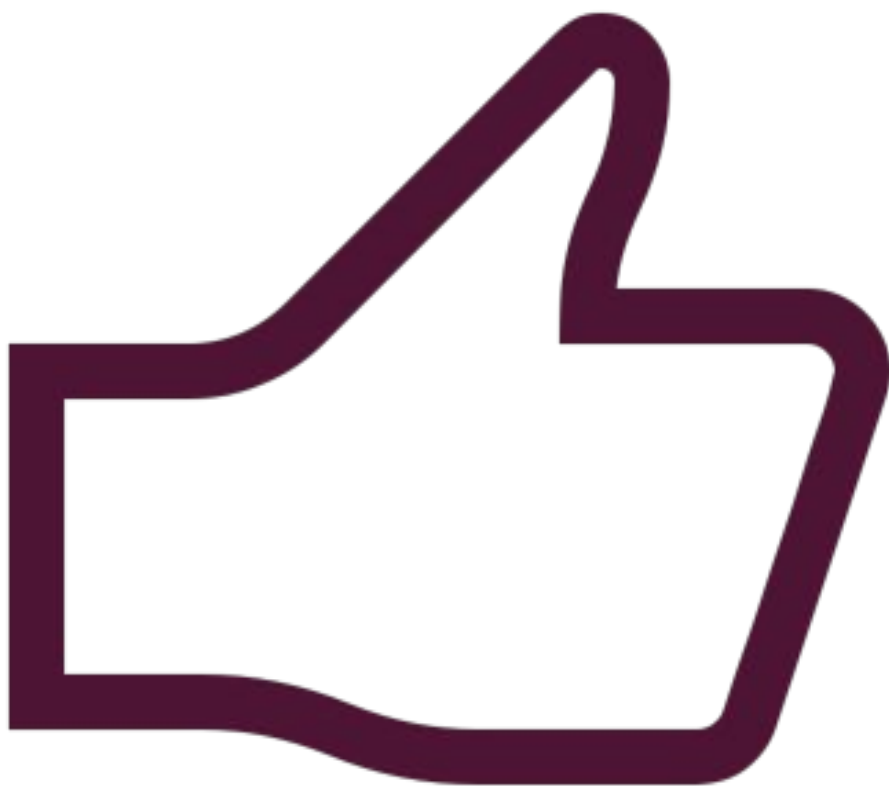
CSC E-117 SPRING 2025

**SECURE APPLICATIONS: MANAGING THE DEPLOYMENT
INFRASTRUCTURE**

Lecture 1
Jan 28, 2025

WEEK 1 AGENDA

- Introduction
 - Instructor Introduction
 - Coarse Goals
 - Grading Structure
 - Course Use Case / Sample App
- Key Concepts/Background
 - Threat Modeling and Architecture Implications
 - Data Protection Requirements and Practices
 - Executive Order 14028
 - CSIA Known Exploitable Vulnerabilities
 - CISA/NCSC Secure Development of AI



INTRODUCTION

INSTRUCTOR INTRODUCTION



- My email : hhinton@g.harvard.edu
 - I will answer email typically twice daily, early morning (8am-ish CT) and evening (7pm-ish CT)
- My Day Job:
 - CISO In Residence, Professional Association of CISOs
- My LinkedIn :
 - <https://www.linkedin.com/in/heather-hinton-9731911/>

Course Office Hours



Carlos Enamorado-Lopez

- Email: carlos_lopez@g.harvard.edu or in Canvas

Office Hours:

- Thursdays 9 am ET & Sundays @ 6pm ET - 30 min or as needed!
- Respond within 24 hours

Work:

- Technical Curriculum Developer @ Information Security Media Group (iSMG)

LinkedIn:

- <https://www.linkedin.com/in/carlos-analyst/>

WHY DID I CREATE THIS COURSE?

- As we move more and more applications to Cloud hosting, we are finding that “traditional, we manage our own data center” approaches to security do not always translate to Cloud hosted environments
 - And as we move more to Cloud, we are forgetting how to protect “On Prem”
- As we move more and more data to online sites (typically Cloud), that data is now concentrated in locations where it acts as a very attractive target for bad actors
- There are vendors who will claim to solve all your problems but
 - Nothing is a silver bullet
 - It's not even clear which bullets go into which barrels, let alone when you should be using which type of bullet (vampires or werewolves?)
- Generative AI is upending everything, or so the news tells us

MY GOALS FOR YOU

- Security vendors are all trying to sell you their silver bullet
 - But if you aren't trying to kill their version of a vampire, it likely won't work
- With limited budgets (in terms of both dollars and time that people can spend on something), focusing on the projects that are needed to remediate business risk is critical
 - Problem first, solution/tool second!
- In this course, we will look at the
 - Operational viewpoint of Internet facing environments (including software products) and
 - How to protect the networks, devices, applications, data and people (users) that use and maintain them
- My goal for you is for you to have a (better) understanding of the mess that is underneath the theory, and the ability to understand and articulate the trade-offs that are made for
 1. Maintaining the security your networks, devices, applications, data and users
 2. Understanding threats to applications and data
 3. How to protect the networks, devices that host the applications and data
 4. Dealing with users that access and use the applications and data
 5. AND... Be able to understand and explain the pros and cons of different solutions and options in the context of a business's risk tolerance

HOW IS THE COURSE STRUCTURED

- We will focus primarily on material that is introduced / discussed in class
 - We will bring in “You Can’t Make This Stuff Up” (YCMTSU) – stuff in the news that reads on this material
- AND
- We will supplement with offline discussions
 - In YellowDig (as part of course grade)
 - In Zoom Study Lounges (how you can meet, on your schedule, to discuss and work together - including group work)

2023-2024 Spring

[Home](#)

[Announcements](#)

[Syllabus](#)

[Zoom](#)

[Class Recordings](#)

Lecture 2

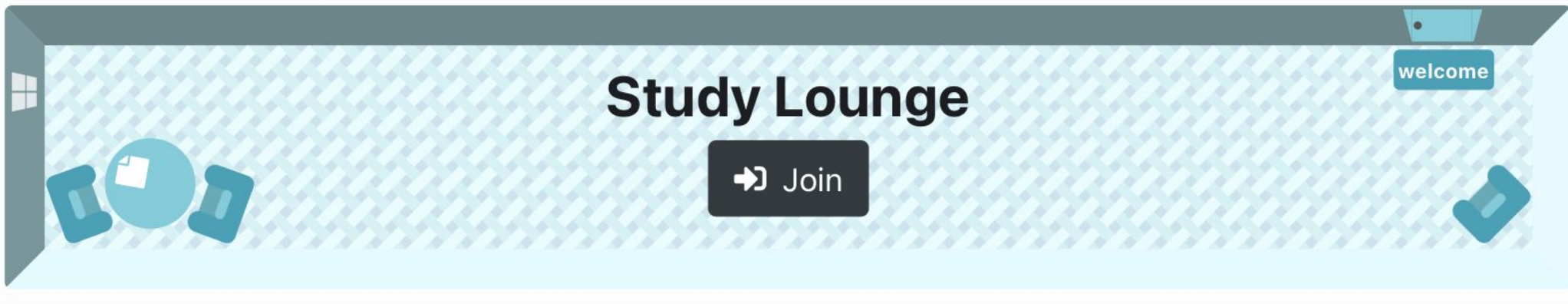


Gather

Test, hope you're doing well!

Current course: CSCI E-117 Section 1 (26436)

Study Lounges (open 24/7)

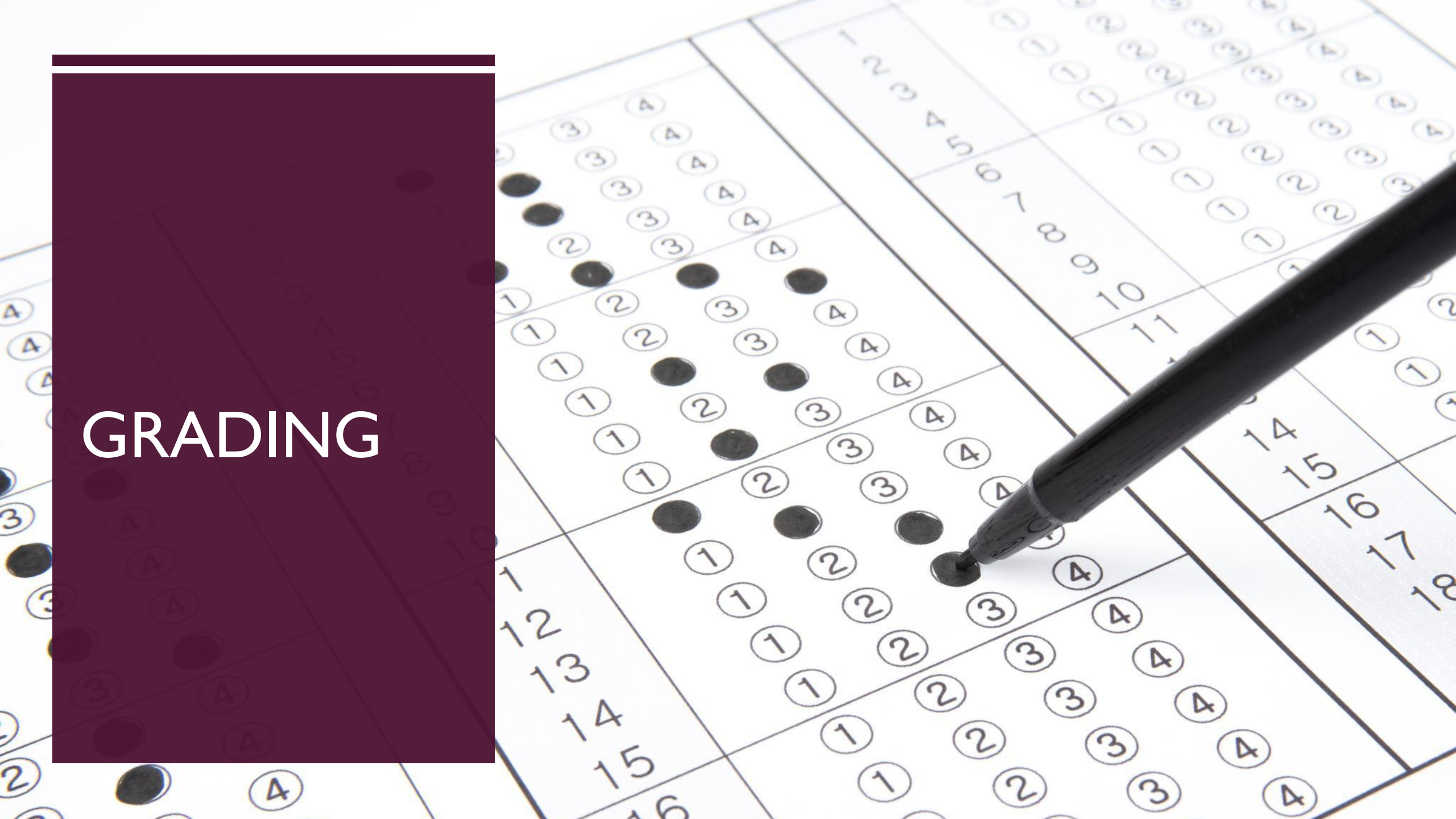


Study Lounge

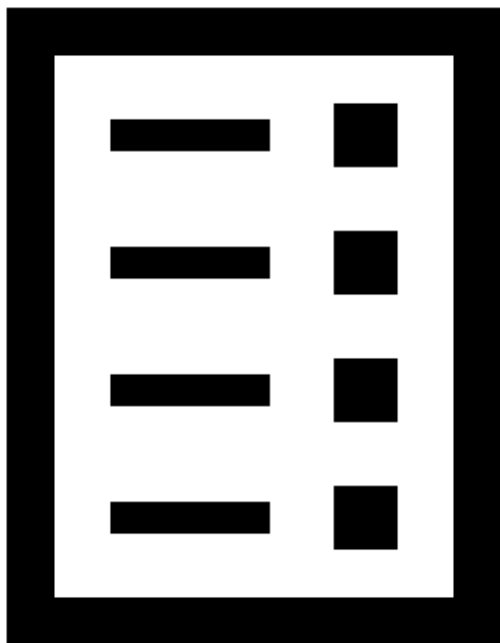
welcome

➞ Join

GRADING

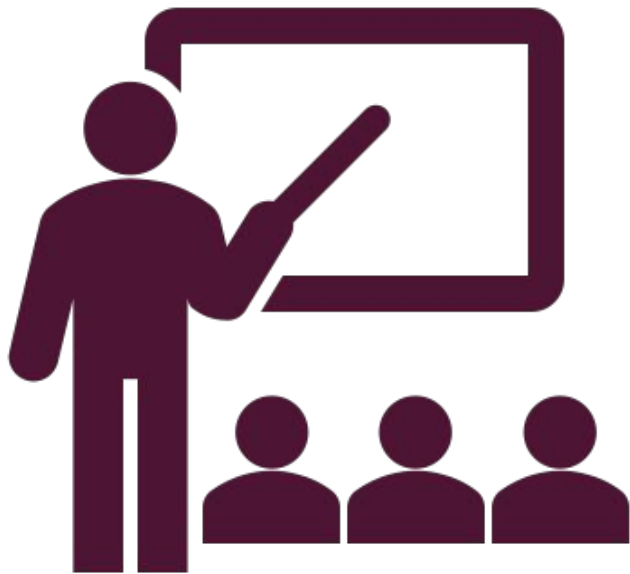


COURSE OUTLINE AND SCHEDULE




- Course Outline / Schedule in Canvas on course home page


GRADING: PARTICIPATION DISCUSSIONS



- 30% of your course total
- Evaluated based on class participation AND contributions in YellowDig
- YellowDig points are earned weekly
 - Up to 1,350 points available each week
 - Each week is scored out of 1,000 points
 - Extra points carry over week to week allowing you to skip a week or two but your total mark tops out at 100% (or 30/30)
- YellowDig Scoring Information here:
 - <https://help.yellowdig.co/kb/en/article/getting-points-and-passing-your-yellowdig-grade-to-the-lms-canvas-blackboard-d2l-etc>

CHECK YOUR POINTS HERE

 Points earned
940 / 14000

 Your pace
You have 940 of the 1000 point target for this period.

Your target this period is only 60 points away! Get there by Mon 09/05/2022 @10:59 pm EDT.

[Show details](#)

Point details


Current Period: 1 / 14

940
Cumulative Total


/


1000
Cumulative Target


=


94%
Grade 

Period Ends: April 27, 2025 11:59 EDT

Participation Log 
View all events that changed my points.

Earning Points 
Learn how to earn points in this community.

My Participation 
See a quick overview of my progress so far.

Point Earning Periods 
View a breakdown of the periods for this community.

PARTICIPATION / DISCUSSION GUIDELINES

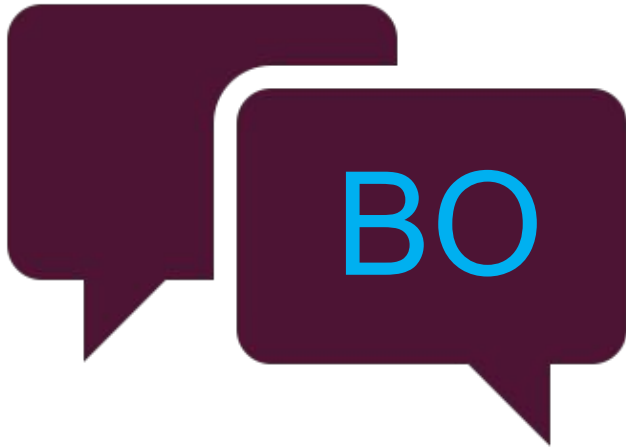
- Prompts will be added by the Instructor or Teaching Fellow following the lecture
 - Instructor or TA will try to post at least one “Conversation Starters” to start discussion
 - If we don’t get anything posted, use your initiative and create a thread yourself
- Regardless of what/when we post, you are encouraged to add your own conversation starters
 - Based on articles, LinkedIn posts, cybersecurity news, or things that peaked your interest during class
 - We will try to pick out the “interesting” comments from YellowDig and highlight them each week in class
- Don’t forget
 - This is NOT A MONOLOGUE: participate – comment on other posts in a thoughtful manner
 - Check in at least twice every period to make sure you can truly interact and discuss
 - Do not leave this until Sunday dinnertime to complete....

DISCUSSIONS



- *YellowDig Conversation Starter: This is how I will call out things from the lecture that may be of interest for further discussion*

DISCUSSIONS



- My goal is to spend at least 25% of our time on discussions during class
- Typically a 5-10 minute discuss and report
- *This is how we will identify pre-defined breakout discussion topics*

LOGISTICS OF CLASS BREAKOUT DISCUSSIONS

- Because not all students are able to participate live, students who participate by recording will miss out on the breakout discussions
- For this reason, each class one assigned group will NOT go into a separate breakout room but will stay in the “main” class and will have their discussion in the main section
 - This discussion will be recorded so that asynch students can hear the discussion and participate through comments in the Interactive Classroom
- In general, the instructors will NOT participate in the mainline conversation

GRADING: ASSIGNMENTS



- 30% of your course total
- Evaluated approximately bi-weekly
 - Total of 4 assignments; top 3 count to your final grade
 - This means that if you can score 100% on first 3, you can skip last assignment
- All assignments are equally weighted
 - Regardless of the number of “points” they may have
- Grading “rubric” will be published with assignments
 - Grading standards will get harder throughout the course

ASSIGNMENT GUIDELINES

- Assignments may be done in individual or group format
- Each assignment will build on the previous lectures and may also be built on discussion topics and threads
- Each assignment will include questions where you must justify your answers
 - This can be done with full sentences or bullet points but must be clear and understandable
- Don't forget: while it is tempting to say there is "No right or wrong" there may be a "more right"
- The Extension School's [Academic Integrity Policy](#) prohibits students from representing work as their own that they did not write, code, or create. It is never permissible to submit work generated by machine learning and AI technologies (such as ChatGPT) without proper attribution.

ANSWERING ASSIGNMENT QUESTIONS

- Sample question: Referring back to Question 1, you are told that you can only implement programs to address priorities #1 and #2, meaning that priorities #3 and #4 will not be addressed. This implies that you do not have the ability to put in place programs that protect you against the threats that you identified for the bottom two categories. In 2-3 sentences and no more than 2 paragraphs, make the case that the remaining risks are acceptable for your environment
- You do NOT get to simply say “I disagree, the risks are not acceptable”, you must make the case they are/not
 - You have some leeway in how to answer but you do not get to invoke magic wands, wishful thinking, a magical “the company accepted these risks” or unsubstantiated claims.
- A good answer will include
 - Notes on why priorities #1 and #2 are more important than #3 and #4 (it is important for you to remember that 3,4 may still be very important, but that 1,2 are more important)
 - This argument will likely focus on likelihood of compromise, impact of compromise, importance of the protected resources, and the ranking of the priorities.

GRADING: FINAL CAPSTONE ASSIGNMENT



- 40% of your course total
 - Will be cumulation of discussions and assignments
- Due Saturday May, 2025 3, 11:59pm ET
 - Capstone will be published mid March, and at the latest by 31 March 2023
- **STRONGLY RECOMMEND** completing as a group
 - Individual is allowed for your work/life schedule
 - Working as a group allows discussion ...

CLASS DISCUSSION

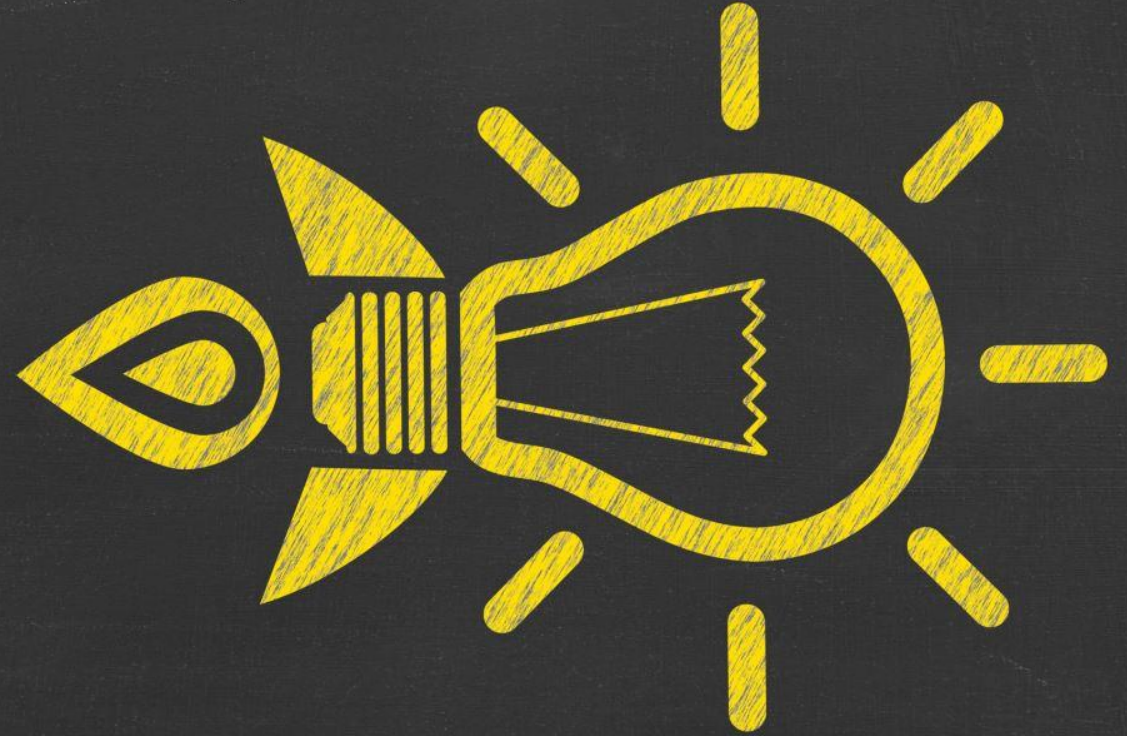


- *Any questions, concerns about the course structure? Things that you would like to see as part of learning goals or grading?*
- *You can also answer this in the Background Survey Quiz*



**BREAK
BACK
8:30PM ET**

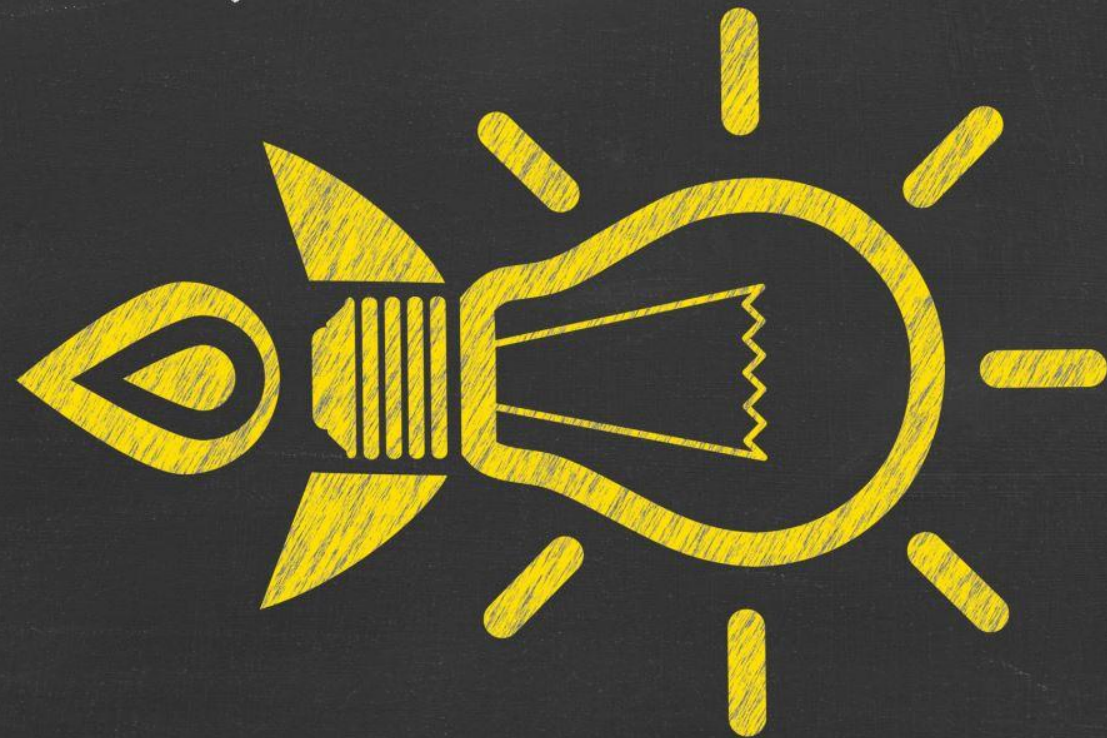
CIA TRIAD



CONFIDENTIALITY, INTEGRITY, AVAILABILITY

- Confidentiality: only authorized users may read data
 - Data is kept “secret”
- Integrity: only authorized users may modify data
 - Data is not corrupted
- Availability: data must be accessible when required
 - Data is not deleted / inaccessible

SOUNIL YU'S
CYBER
DEFENSE
MATRIX



CYBER DEFENSE MATRIX

- Created by Sounil Yu as a means of classifying products / solutions designed to address cybersecurity needs (or the needs that a start-up is trying to market)
- Provides a means of mapping and evaluating CSF Functions to Asset Classes and the role of People, Process and Technology in protecting each category

	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
DEVICES					
NETWORKS					
APPS					
DATA					
USERS					
DEGREE OF DEPENDENCY	TECHNOLOGY				
	PROCESS				PEOPLE

Figure 1: Cyber Defense Matrix

CYBER DEFENSE MATRIX

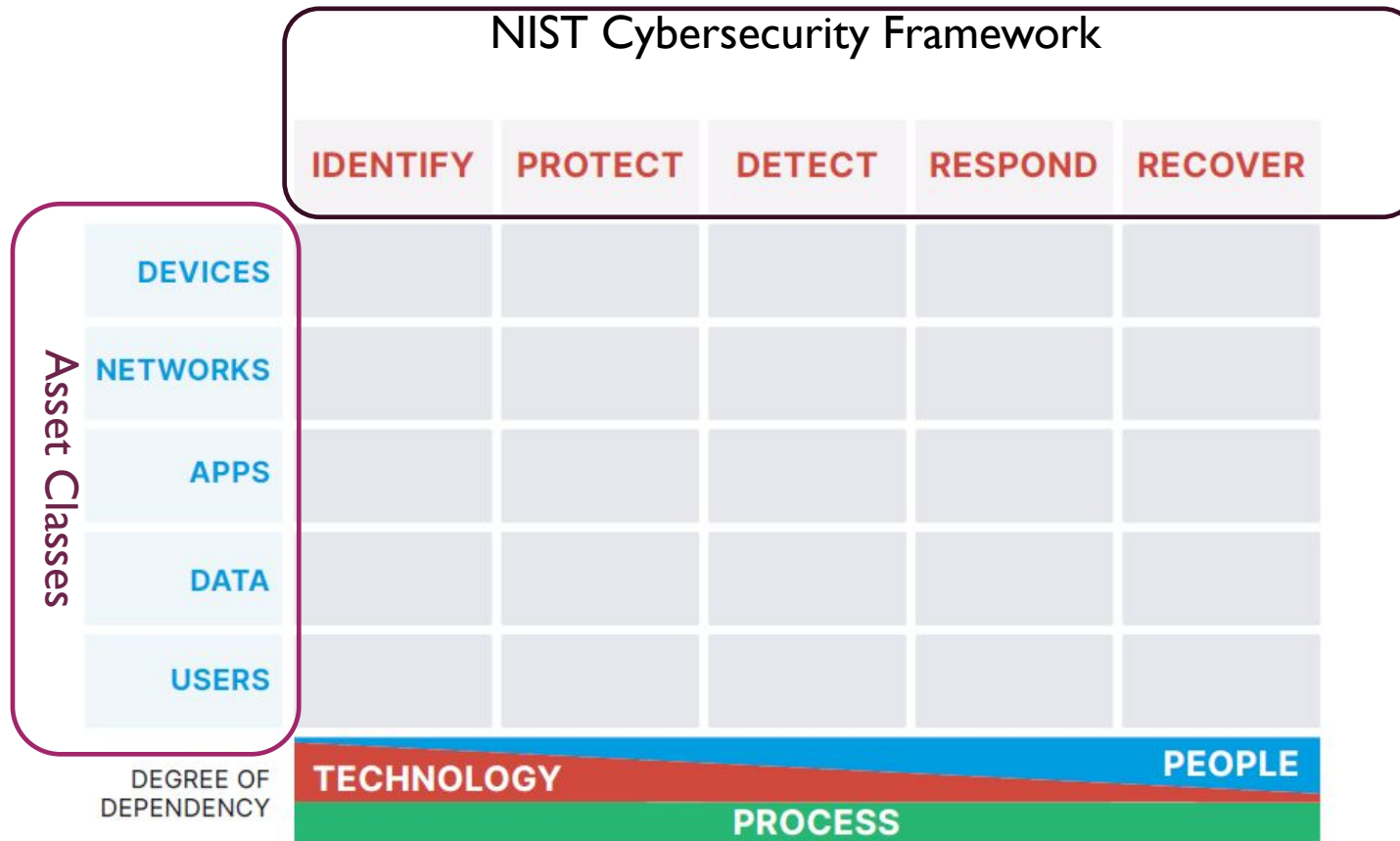


Figure 1: Cyber Defense Matrix

CYBER DEFENSE MATRIX

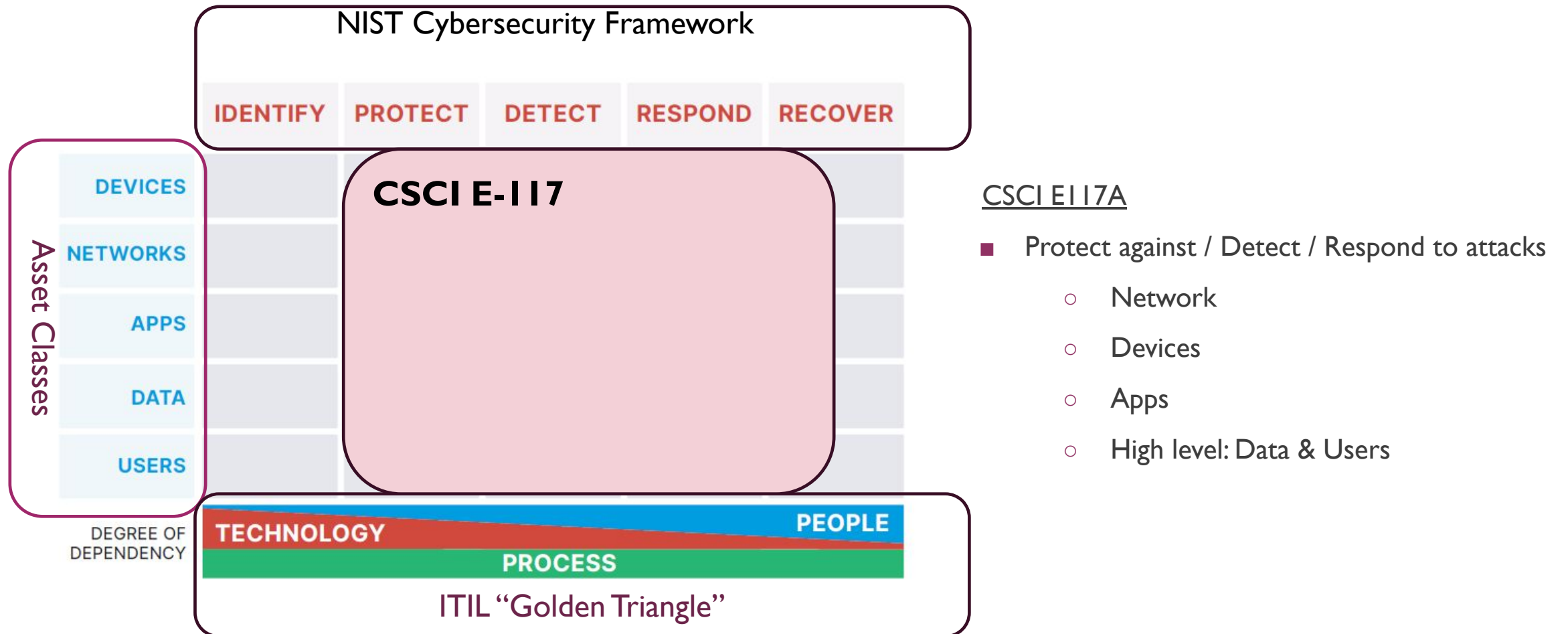


Figure 1: Cyber Defense Matrix

WHY IDENTIFY & PROTECT?

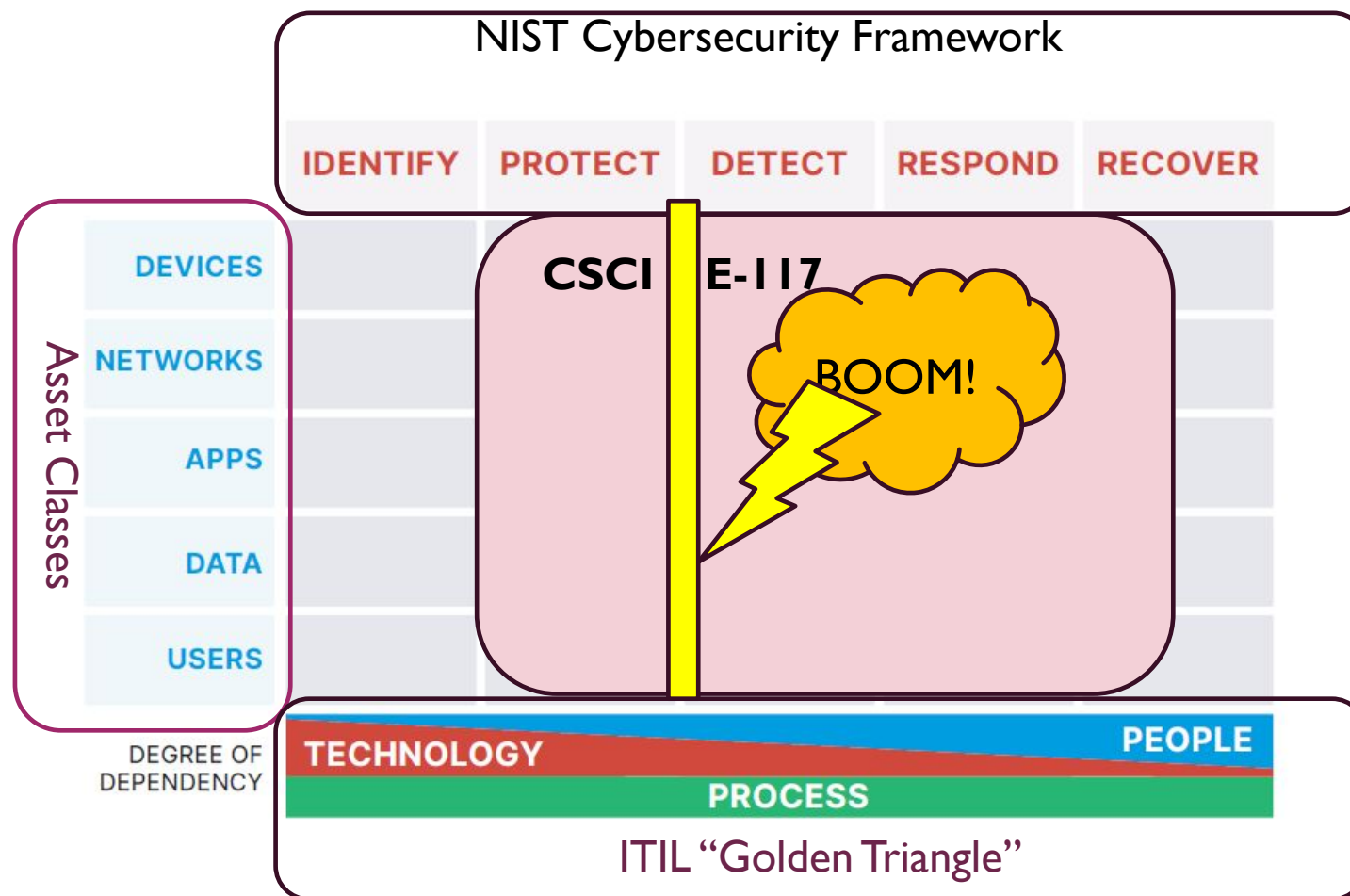
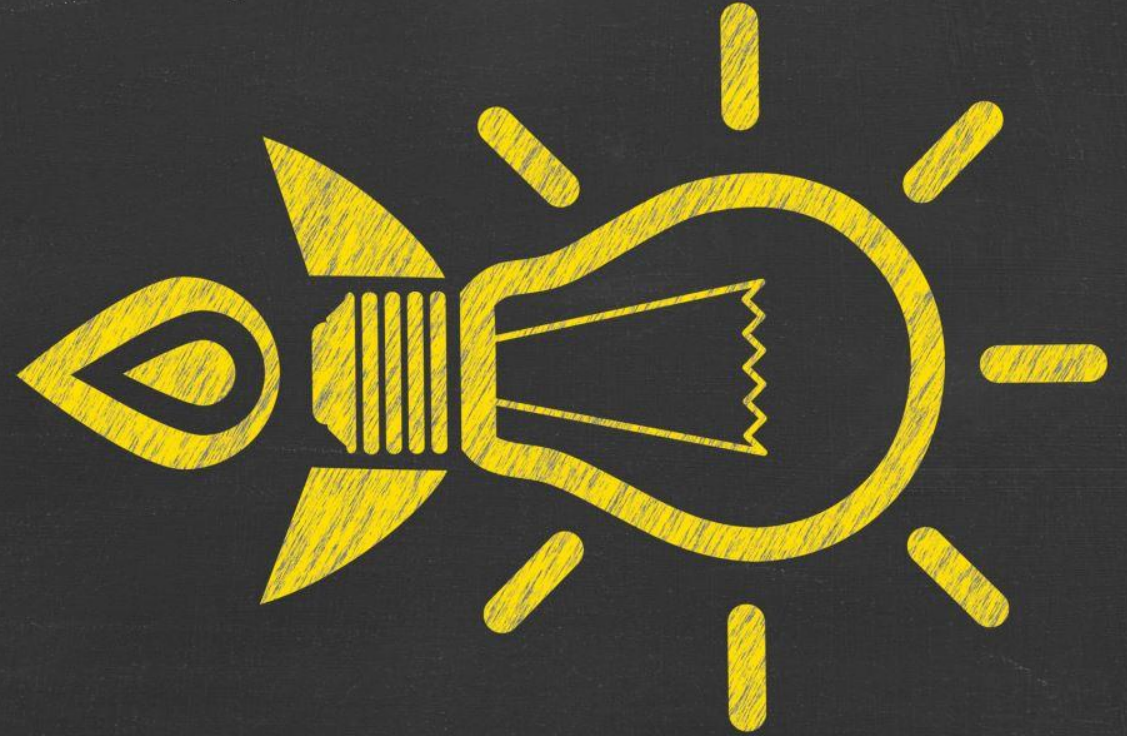


Figure 1: Cyber Defense Matrix

DEFINITION: BOOM!

- *Boom*, also known as a *Security Event*, is the successful exploitation of a weakness (vulnerability),
- **IDENTIFY** and **PROTECT** are on the “left of boom,” or before a security event.
 - “Left of boom” activities focused on efforts to disrupt the ability of the attacker to create a boom.
- **DETECT**, **RESPOND**, and **RECOVER** happen “right of boom,” or after the event.
 - “Right of boom” activities focused on assessing and addressing the damage after the boom has occurred.
- Security programs (and the tools that are part of them are intended to
 - PROTECT assets and
 - If we are lucky, help us DETECT when there are issues
 - Typically don’t do much for RESPOND OR RECOVER

THREAT MODELING



WHAT IS THREAT MODELLING?

Google Prompt

My question to Google Search: What is threat modeling

Google's answer →



OWASP

<https://owasp.org> › [www-community](#) › [Threat_Modeli...](#) ⋮

Threat Modeling

Threat modeling is **a family of activities for improving security by identifying threats, and then defining** countermeasures to prevent, or mitigate the effects ...

[Overview](#) · [Threat Modeling Across The...](#) · [Threat Modeling: Four...](#)

People also ask ⋮

What is the meaning of threat modeling? ▼

What are the 5 steps of threat modeling? ▼

What are the 4 stages of threat modeling? ▼

What is the difference between attack modeling and threat modeling? ▼

[Feedback](#)



Synopsys

<https://www.synopsys.com> › [glossary](#) › [what-is-threat-...](#) ⋮

What Is Threat Modeling and How Does It Work?

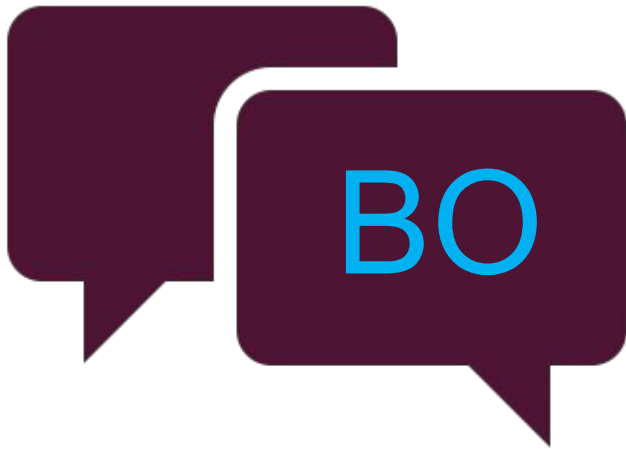
Threat modeling is a **process to identify security needs, locate threats and vulnerabilities, assess their severity, and prioritize solutions.**

WHAT IS THREAT MODELLING?

My prompt to ChatGPT: What is "threat modeling"

ChatGPT: Threat modeling is a structured approach used in the field of cybersecurity and software development to identify, assess, and prioritize potential threats and vulnerabilities in a system or application. The primary goal of threat modeling is to proactively enhance the security of a system by identifying potential risks and implementing appropriate countermeasures.

CLASS DISCUSSION



- *DISCUSSION PROMPT: On the surface, the ChatGPT answer looks “better” but ...*
- *Q1: How do you know that the ChatGPT answer is accurate?*
- *Q2: How does each “response” (ChatGPT, GoogleSearch) align with how you research & learn online?*
- *Q3: Which approach do you think will be most useful to you as you learn and why?*

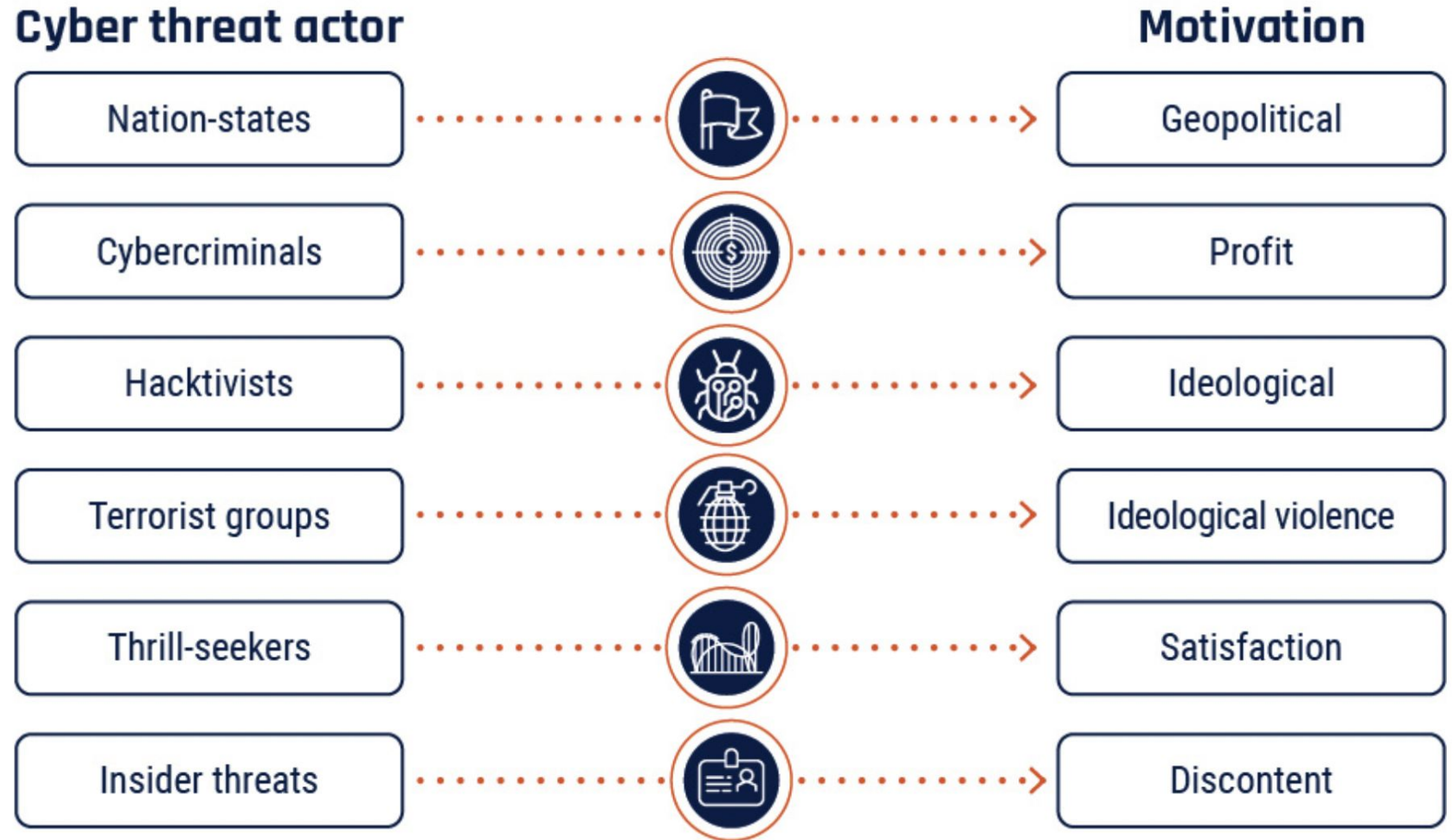
THREAT MODELING

- The discipline / exercise of identifying potential threats and vulnerabilities in a system / application / environment
- Good Threat Modeling requires that you understand what is valuable about your system / application / environment because this is what attackers will go after
 - This is often done with a Business Impact Analysis (more on this later)

The targets of cyber threat activity

Cyber threat actors conduct malicious activity against anything connected to or residing on the Internet, including devices, information, financial resources, opinions, and reputations

Figure 1: Cyber threat actors

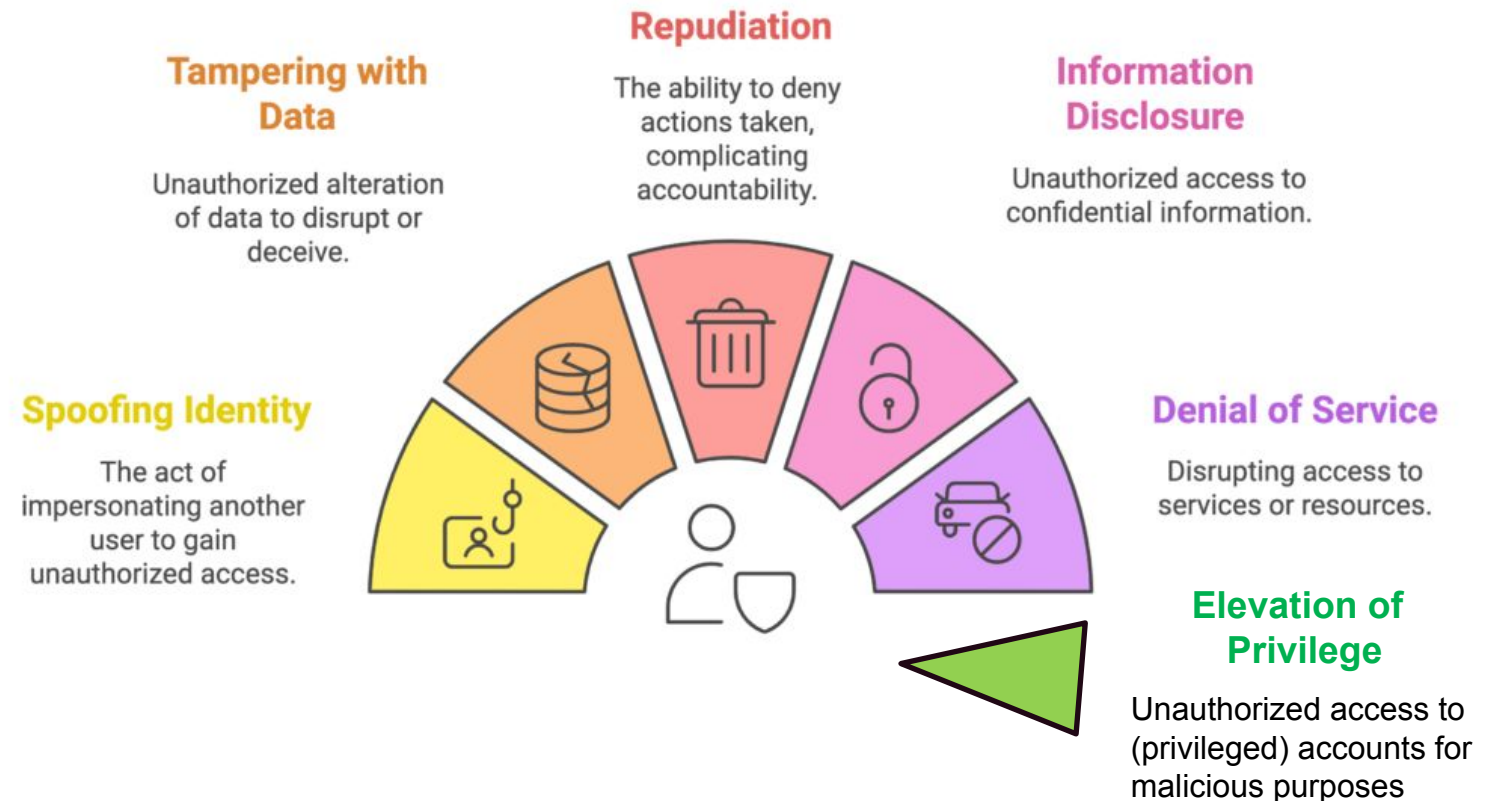


STRIDE THREAT MODELING

<https://www.practical-devsecops.com/what-is-stride-threat-model/>

- Spoofing identity
 - ☐ Authentication
- Tampering with data
 - ☐ Integrity
- Repudiation
 - ☐ Non Repudiation
- Information disclosure
 - ☐ Confidentiality
- Denial of service (DoS)
 - ☐ Availability
- Elevation of Privilege
 - ☐ Authorization

STRIDE Security Model



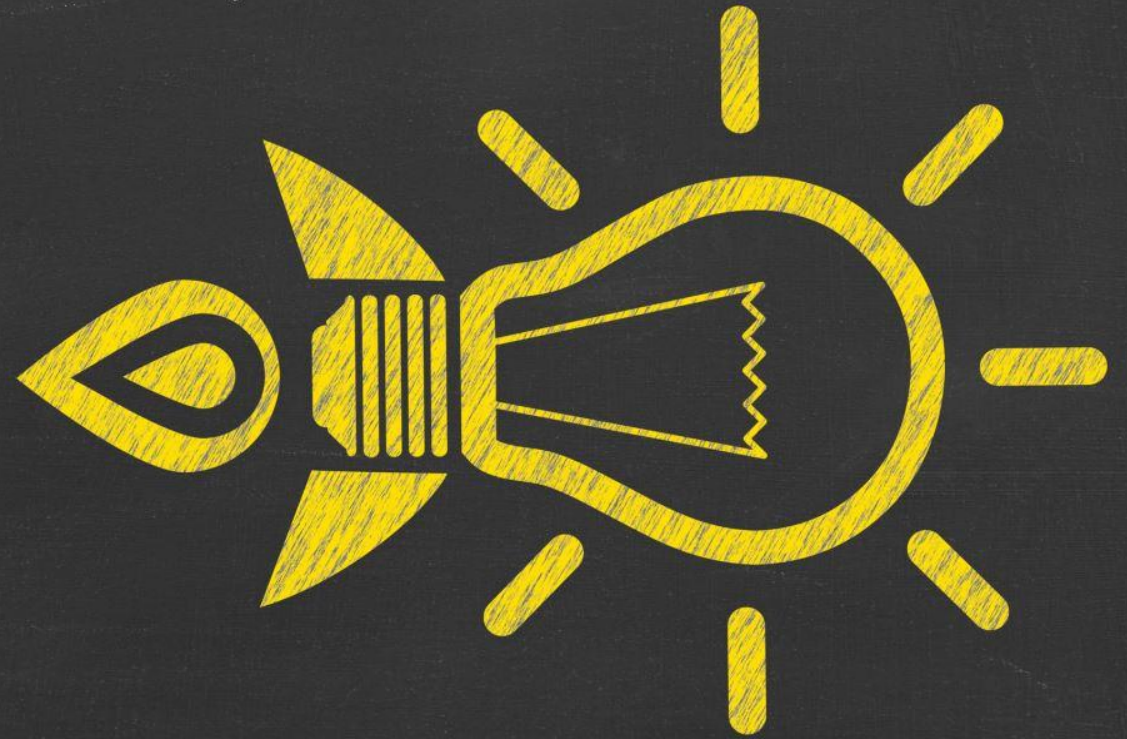
(ADAM) SHOSTACK'S "4 QUESTION FRAME FOR THREAT MODELING"

<https://github.com/adamshostack/4QuestionFrame>

Shostack's 4 Question Frame for Threat Modeling

- What are we working on (*what are we trying to do*)?
- What can go wrong (*what's the worst that can happen*)?
- What are we going to do about it (*how do we prevent the bad and worst things*)?
- Did we do a good job?

EXECUTIVE
ORDER 14028,
SECURE BY
DESIGN
PLEDGE



EXECUTIVE ORDER 14028

[HTTPS://WWW.WHITEHOUSE.GOV/BRIEFING-ROOM/PRESIDENTIAL-ACTIONS/2021/05/12/EXECUTIVE-ORDER-ON-IMPROVING-THE-NATIONS-CYBERSECURITY/](https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/)

- Section 1. Policy.
 - The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy... The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely,...
- Sec. 2. Removing Barriers to Sharing Threat Information.
- Sec. 3. Modernizing Federal Government Cybersecurity.
- Sec. 4. Enhancing Software Supply Chain Security.
- Sec. 5. Establishing a Cyber Safety Review Board.
- Sec. 6. Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents.
- Sec. 7. Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks.
- Sec. 8. Improving the Federal Government's Investigative and Remediation Capabilities.

SIDEBAR: WHAT IS SOFTWARE SUPPLY CHAIN SECURITY

ChatGPT: Supply chain security refers to the measures and practices implemented to safeguard the integrity, confidentiality, and availability of goods and information as they move through the various stages of a supply chain. It involves protecting the supply chain from various threats and risks, including disruptions, cyberattacks, theft, counterfeiting, and other forms of compromise.

- **Physical Security**
- **Information Security:** Safeguarding the integrity and confidentiality of information within the supply chain. This includes protecting against cyber threats, data breaches, and unauthorized access to sensitive information. Encryption, secure communication protocols, and regular cybersecurity assessments are common practices.
- **Risk Management**
- **Authentication and Verification**
- **Supplier Security:** Assessing and monitoring the security practices of suppliers and third-party partners in the supply chain. This includes conducting due diligence, implementing contractual agreements, and establishing standards for security compliance.
- **Resilience and Contingency Planning:**
- **Regulatory Compliance.**
- **Employee Training and Awareness**

SECURE BY DESIGN PLEDGE AND SUPPLY CHAIN SECURITY

- The Secure by Design Pledge is intended to improve the discipline, maturity and security quality of products and services that are used as part of a company's operations
 - a. Often referred to as supply chain security and/or third-party risk management
- This is a voluntary pledge focused on enterprise software products and services, including on-premises software, cloud services, and software as a service (SaaS).
- The pledge is structured with seven goals. Each goal has the core criteria which manufacturers are pledging to work towards, in addition to context and example approaches to achieve the goal and demonstrate measurable progress.
 - a. Multi-factor Authentication
 - b. Default passwords
 - c. Reducing entire classes of vulnerabilities
 - d. Security Patches
 - e. Vulnerability Disclosure Policy
 - f. CVEs (Timely & accurate reporting of vulnerabilities)
 - g. Evidence of intrusions (access to logs)



ANTICIPATED END OF LECTURE I

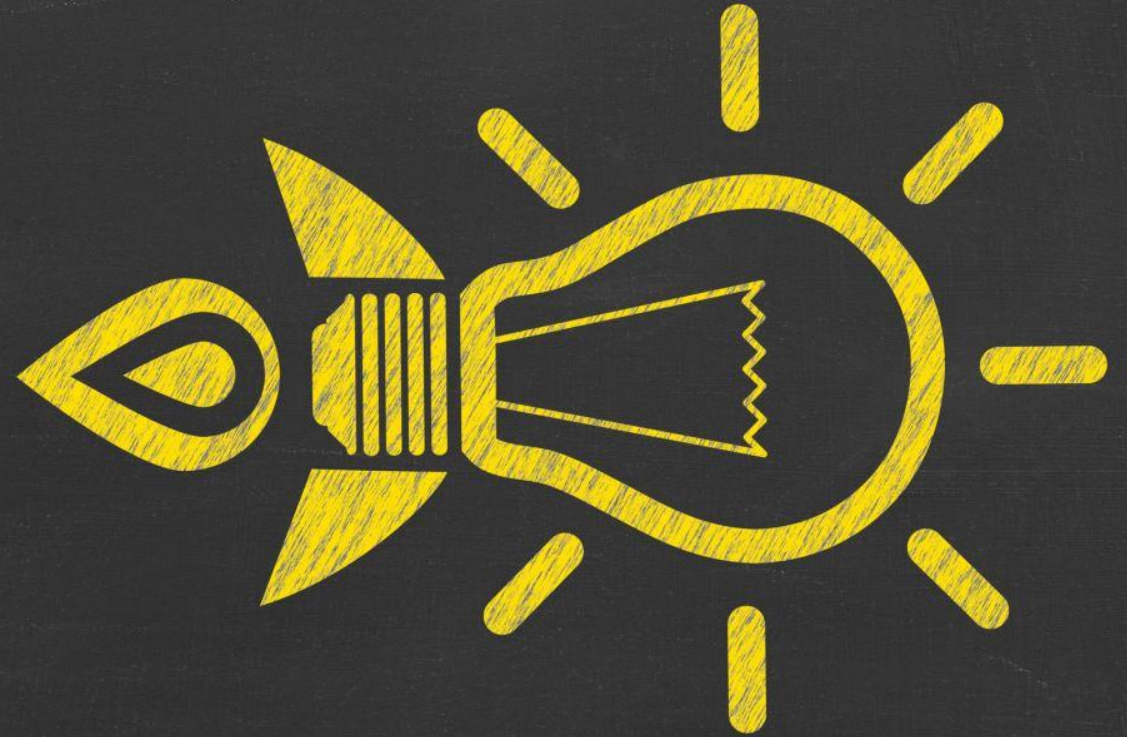




APPENDIX



COURSE USE CASE



COURSE “USE CASE / CASE STUDY”

- We are going to use a fictional company with a web-facing application throughout the course, to illustrate concepts and decision points
- OUR course use case : “Vacations and Rest for You” (VARY)

OUR COURSE USE CASE : “VACATIONS AND REST FOR YOU” (VARY)

- We provide
 - Online travel resource for all things vacation: hotels,/B&B, flights, car service, local site-seeing, etc
 - Concierge services for high end vacation including car service, fully arranged itinerary, personal tours, etc
- Users access us through our (mobile and browser formatted) Web page
 - Booked clients interact with us through a mobile application for viewing/managing their itinerary, chatting with agents
- We have phone, web chat, app chat, email support, including ability to turn a chat into a phone call
- We allow clients to view and download their itinerary
 - We are thinking about allowing them to upload files (esp photos) of good/bad things as part of reviews
- We want to improve our recommendations by adding GenAI functionality
 - Provide more targeted recommendations for things to do for customers



Customer/Users may access over

- Web Browser
- Mobile App

Most access requires authentication
but there are some public resources



VARY Support/Users may access
over

- Web Browser

All access requires authentication



Third Party tools access
EVERYTHING for management
purposes (eg scan/test tools)
All access requires authentication



Availability Zone 1

Availability Zone 2

Production Environment VPC contains

Production Environment VPC contains

- Web/API tier
- Application Tier
- Data Tier

Pre-Production Environment VPC

- Transient apps, functions, tiers

Development Pipeline

- Code Repo
- Commit, Build, Deploy tools



AWS
Management
Console



AI



ObjectStore



API Gateway



VARY SecOps/Users may access over

- Web Browser

All access requires authentication



VARY DevOps/Users may access dev
pipeline over

- Web Browser
- Client side development tools

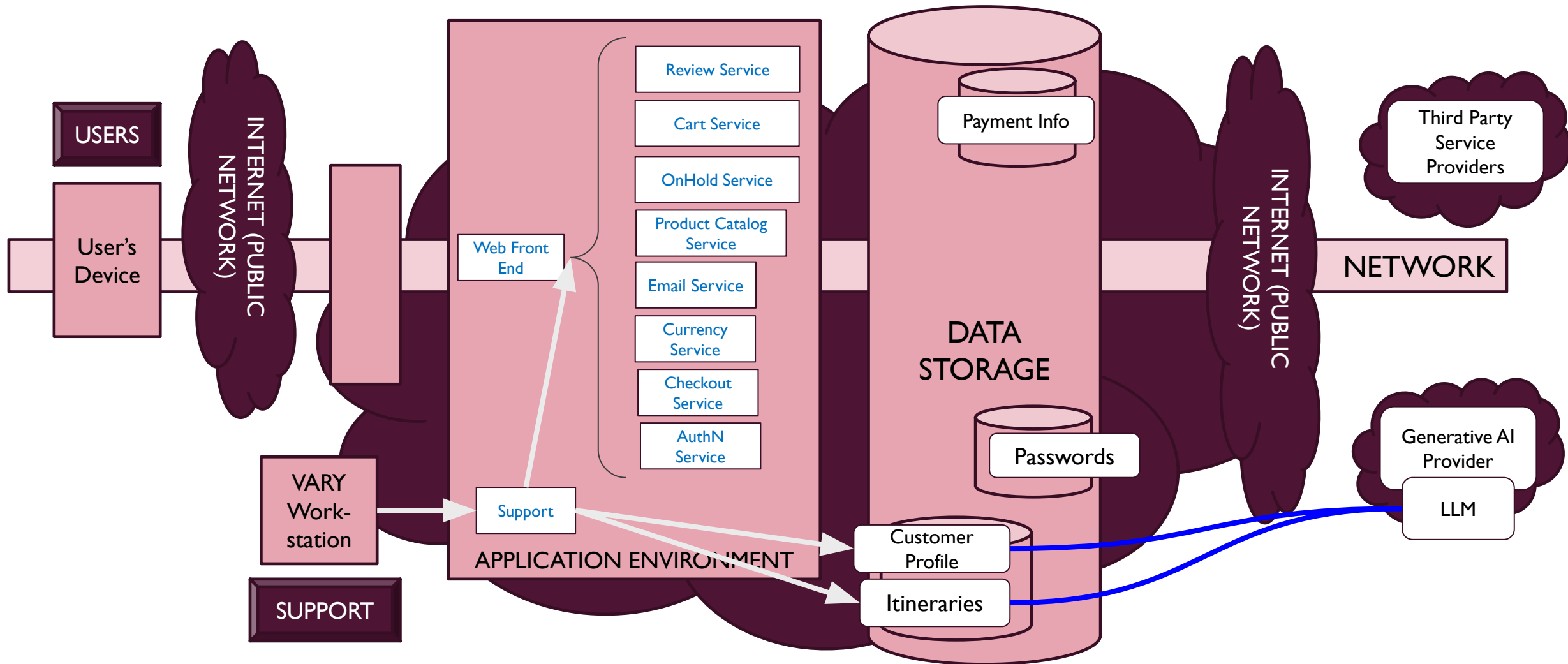
All access requires authentication



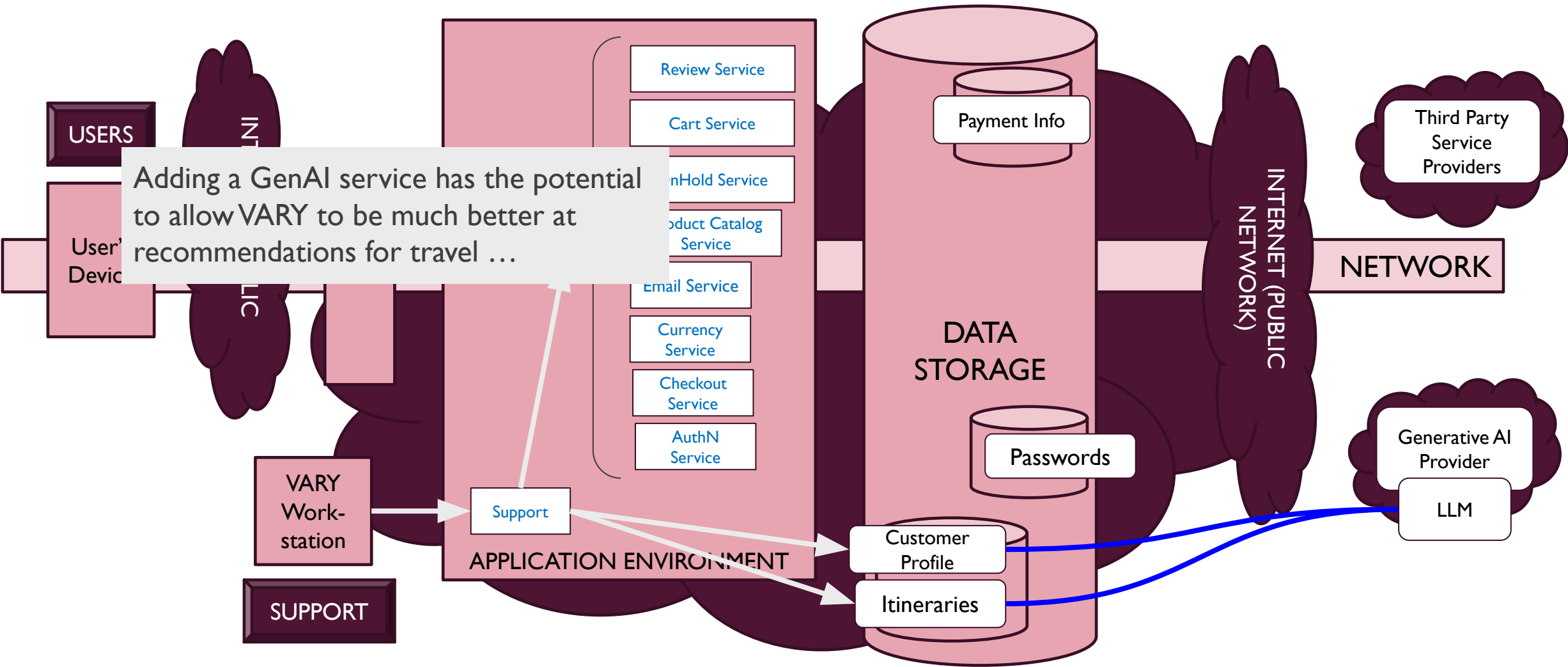
Third Party applications may access data
through API integration

All access requires authentication

VARY ARCHITECTURE



VARY ARCHITECTURE



SECURITY & PRIVACY

- While information security programs and privacy programs have different objectives, those objectives are overlapping and complementary.
- Information security programs are responsible for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction (i.e., unauthorized system activity or behavior) in order to provide confidentiality, integrity, and availability.
- Privacy programs are responsible for ensuring compliance with applicable privacy requirements and for managing the risks to individuals associated with the creation, collection, use, processing, dissemination, storage, maintenance, disclosure, or disposal (collectively referred to as “processing”) of PII.