CSCI E-117A SPRING 2025

Lecture 2
Feb 3, 2025

SECURE APPLICATIONS: MANAGING THE DEPLOYMENT INFRASTRUCTURE

LECTURE 2 AGENDA

- Housekeeping
  - Pre-Course Survey “Results”
  - Participation Grade
  - Assignment 1
- Lecture Material
  - Vulnerabilities
  - CVSS v EPSS
  - Zero Trust Maturity Model
  - Generative AI Impact (Gartner)
- Course Use Case Introduction

PRE COURSE SURVEY

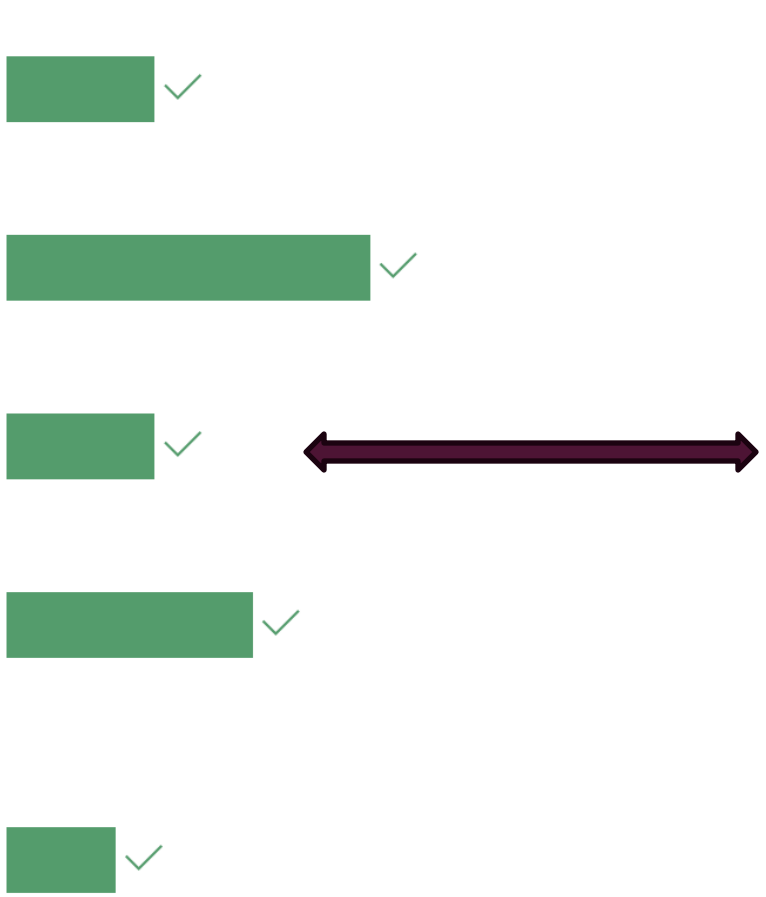
PRE COURSE SURVEY FEEDBACK

Goals:

- Learn more about deployment infrastructural security as this space will continue growing and be vital to organizations of all sizes.
- Comprehensive understanding end to end approach in securing apps during building and deployment.
- Learning how to validate and verify enterprise platforms, applications, tools, etc. are adequately secured.
- To gain more exposure for better decision and strategy, improve security compliance skills
- Broaden and deepen understanding of the threat landscape and how the threat attackers look at them to prevent threats from happening

4. How extensive is your development programming experience? (Check the box(es) that apply)

walked past the programming section at the bookstore	7 respondents	18 %
I can do “Hello world” in Python and that’s about it	18 respondents	47 %
I can do “Hello world” in 7 languages (including Kling	7 respondents	18 %
I have been a programmer/developer for my employer	12 respondents	32 %
I have >5 years development experience working for a Fortune 500 company	5 respondents	13 %



18% of you can do Hello World in Klingon!!!!!

Are you currently employed in a security / cybersecurity role?

Yes	11 respondents	**29 %**	✓
No	12 respondents	**32 %**	✓
Something Else	15 respondents	39 %	

Most of you do NOT have cyber role or background

“WHAT ARE YOU WORRIED ABOUT” COMMON THEMES

- Work/Life Balance ; Time
- Specific comments:
  - Balancing workloads with my daytime job
  - Getting the most value out of the courses during discussion via Zoom and YellowDig.
  - Impact of work and travel, how will asynch work

ASYNCH STUDENTS & PARTICIPATION

Class Participation: DUE: Throughout the Term

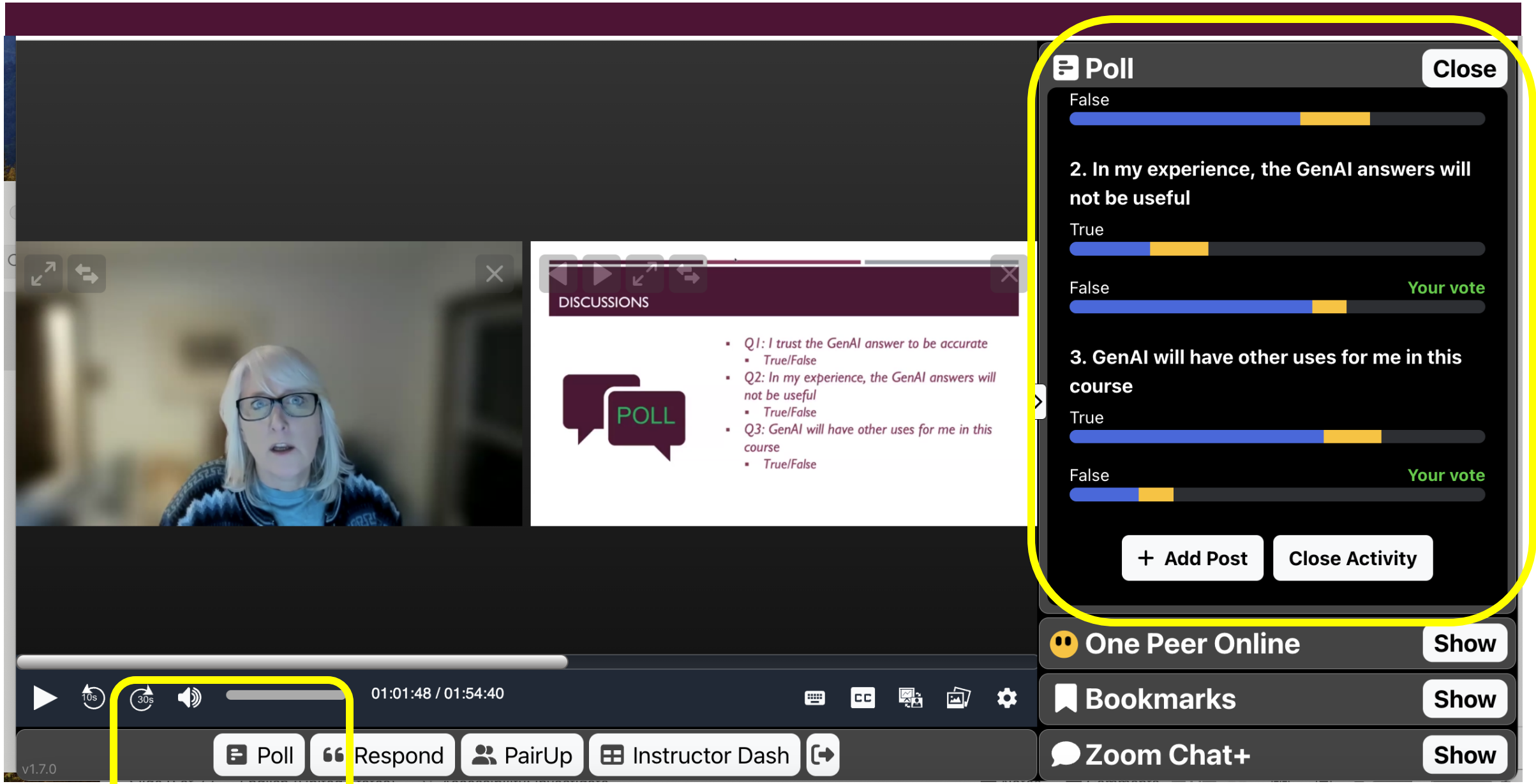
- 30% of your overall grade will be based on your active and engaged participation in the online lectures and offline discussions each week. Students are expected to contribute thoughtfully to conversations, demonstrating a clear understanding of the course material and its broader implications. In general, participation points are either earned, or not earned (i.e., a discussion happens over a specific period of time, and then it is over – it doesn't make sense to retroactively "participate" in a discussion that you missed, all by yourself).
- YellowDig participation credit will be assigned by the YellowDig tool based on creating posts and responding to posts created by classmates. Posts will be required to have a minimum word count ("Great idea!" will not earn posts). YellowDig points will be assigned weekly and will allow for a "credit" to be built up (you can earn more than 100% marks weekly to allow for a week of downtime if needed).

PARTICIPATION: YELLOWDIG

- There was some discussion of this on Yellow Dig, so let's address it here so we are all on same page
- → active and engaged participation in the online lectures and offline discussions each week.
- Participation includes Class participation through Polls and Breakouts in addition to YellowDig
- YellowDig points are easily tracked (and will be worth 15% out of the 30% participation grade)
  - But sadly they are also easily gamed (its really easy to post the same thing week over week and it's a PITA for the instructors to go and pull out repeat posts to properly set participation)
- So we also rely on in-class participation

PARTICIPATION: POLLS, BREAKOUTS

- Polls are available to everyone (Live and Asynch)
  - In class we will share the results during the lecture
  - Asynch students can see the Poll results in the recording and see how they voted


DISCUSSIONS
POLL
Q1: I trust the GenAI answer to be accurate
True/False
Q2: In my experience, the GenAI answers will not be useful
True/False
Q3: GenAI will have other uses for me in this course
True/False
01:01:48 / 01:54:40
Poll
Respond
PairUp
Instructor Dash
v1.7.0
Poll
Close
False
2. In my experience, the GenAI answers will not be useful
True
False
Your vote
3. GenAI will have other uses for me in this course
True
False
Your vote
+ Add Post
Close Activity
One Peer Online
Show
Bookmarks
Show
Zoom Chat+
Show

PARTICIPATION: BREAKOUTS, DISCUSSIONS

- Breakouts are discussions based on key points in the lecture and/or Poll results
  - Asynch students cannot actively participate in Breakouts
- Introducing Canvas Discussions (in support of Breakouts) (15%)
  - ALL students (synch/asynch) be required to participate in Canvas discussions
- Canvas discussion
  - Will be based on an identified in-lecture breakout discussion
  - Are to be completed BEFORE the next lecture
  - Will contribute to your participation grade
  - Prompt for the Canvas discussion will be provided in class
  - Discussion grades will be “participation” based – you participated in the Discussion, addressing the Discussion prompt

CANVAS DISCUSSION: THOUGHTS ON THE BREAKOUT DISCUSSION

- If there is more than one Breakout, the prompt in Canvas will specify which Breakout discussion to consider
- This should take you 5 minutes and no more than 15 minutes to answer.
- In general, this is what the Canvas discussion will entail:
- *If you participated in a Breakout in the live lecture, what surprised you the most from your team's discussion? What did you learn / what will you take away from that discussion?*
- *If you watched the Breakout discussion as part of the asynch lecture, what did you agree with / what made sense to you in the discussion? What surprised you in the discussion or provided a new way to look at the topic of discussion?*

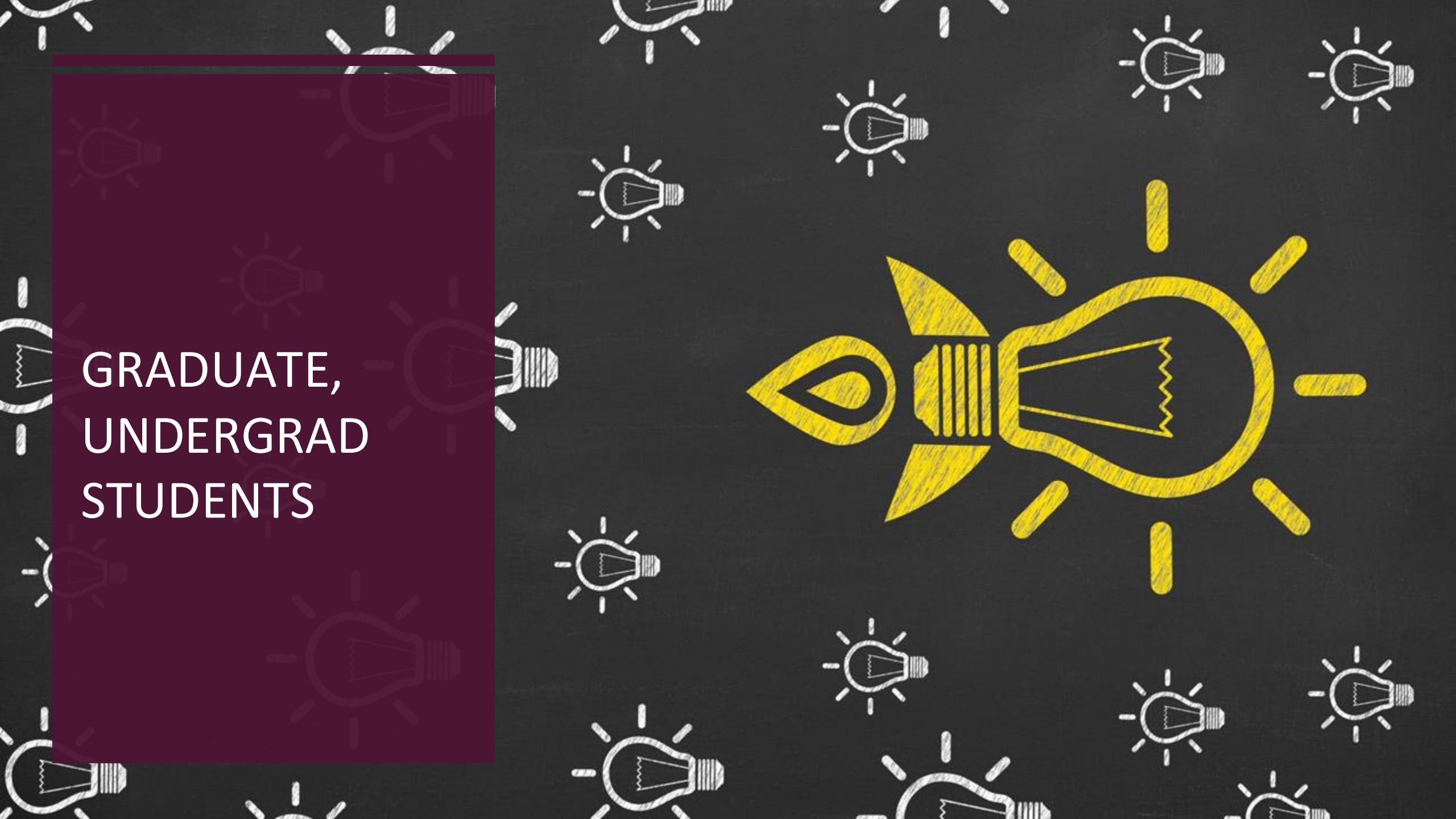
ROLL OF YELLOWDIG GIVEN CANVAS DISCUSSIONS

- I have added a new, high point item to YellowDig
  - If you make a post that references something in the news, be it an attack, an analysis, or an interesting viewpoint on cybersecurity, you will get an annotation that will be worth up to 150 points
  - This will help you get your YellowDig points and recognize that some of the YD discussions are now moved to Canvas
- YellowDig is still an important part of this course
  - The Canvas Discussion is to explicitly reflect on each lecture and its content
  - YellowDig provides a free-form place for you to discuss, comment on things in the class, and share experiences including additional reflections on the course discussions and prompts that are added to YD based on the course.

“YELLOW DIG LAST WEEK”

- The instructors do read/monitor YellowDig
- Each week we will identify the comments / posts that we think are interesting and impactful
- These posts will be marked with an “Accolade”
  - Post of the week : for especially interesting posts / observations
  - Interesting / Conversation Starter : for things that we think are worthy of further discussion in YD
  - Used in Class : for posts / observations / points that will be used in the “pre class” discussion
- Each class will start at approx10 minutes early
  - YOU DO NOT NEED TO JOIN EARLY but you are welcome to join and discuss
  - We will go through the posts that are “Used in Class” and talk about why there are interesting
  - This will allow this to be recorded so that all students can get a form of feedback on the YD discussions
- TO BE INCLUDED IN THE “USED IN CLASS” A POST MUST BE MADE ON/BEFORE MIDNIGHT SUNDAY BEFORE CLASS
  - Not matter HOW interesting, we will not include posts made 15 minutes before the lecture starts

GRADUATE, UNDERGRAD STUDENTS



GRAD V UNDERGRAD STUDENTS

- Graduate students are given extra work
  - This will show up in additional questions – primarily rhetoric/argument based – in the assignments and Capstone assignment

ASSIGNMENTS

ASSIGNMENT 1

Due Date: Feb 16

Purpose: Start to think about threats to the network, device and application asset classes, and as a bonus, the impact of GenAI in the attack and defense of the asset classes.

Assignment 1 Details

Sample answer for "MyFuBar" Asset class

Question 1A (10 points)			
Asset Class	Priority #1	Priority #2	Priority #4
MyFuBar Asset Class	*Integrity*	*Availability*	*Confidentiality*
Network	Pick One: Confidentiality, Integrity, Availability	Pick One: Confidentiality, Integrity, Availability	Pick One: Confidentiality, Integrity, Availability
Device	Pick One: Confidentiality, Integrity, Availability	Pick One: Confidentiality, Integrity, Availability	Pick One: Confidentiality, Integrity, Availability
Application	Pick One: Confidentiality, Integrity, Availability	Pick One: Confidentiality, Integrity, Availability	Pick One: Confidentiality, Integrity, Availability
Ordering, meet rules of assignment			

3 marks, 1 per cell

3 marks, 1 per cell

3 marks, 1 per cell

(Additional) 1 mark

Assignment 1 Details

Question 1B (15 points, 5 per asset class)	Your Answer
Networks: Control Order Justification:	*Answer here*
Devices: Control Order Justification:	*Answer here*
Applications: Control Order Justification: Your ar	*Answer here*
If you used Generative AI to help with your answers, you MUST include the prompt that you used.	*Prompt used:*

ASSIGNMENT 2

Due Date: Mar 2

Purpose: To look at the network asset class in more detail, from a zero-trust point of view, a threat point of view and a protection point of view.

ASSIGNMENT 3

Due Date: Mar 9

Purpose: To look at the device asset class in more detail, from a zero-trust point of view, a threat point of view and a protection point of view.

ASSIGNMENT 4

Due Date: Mar 30

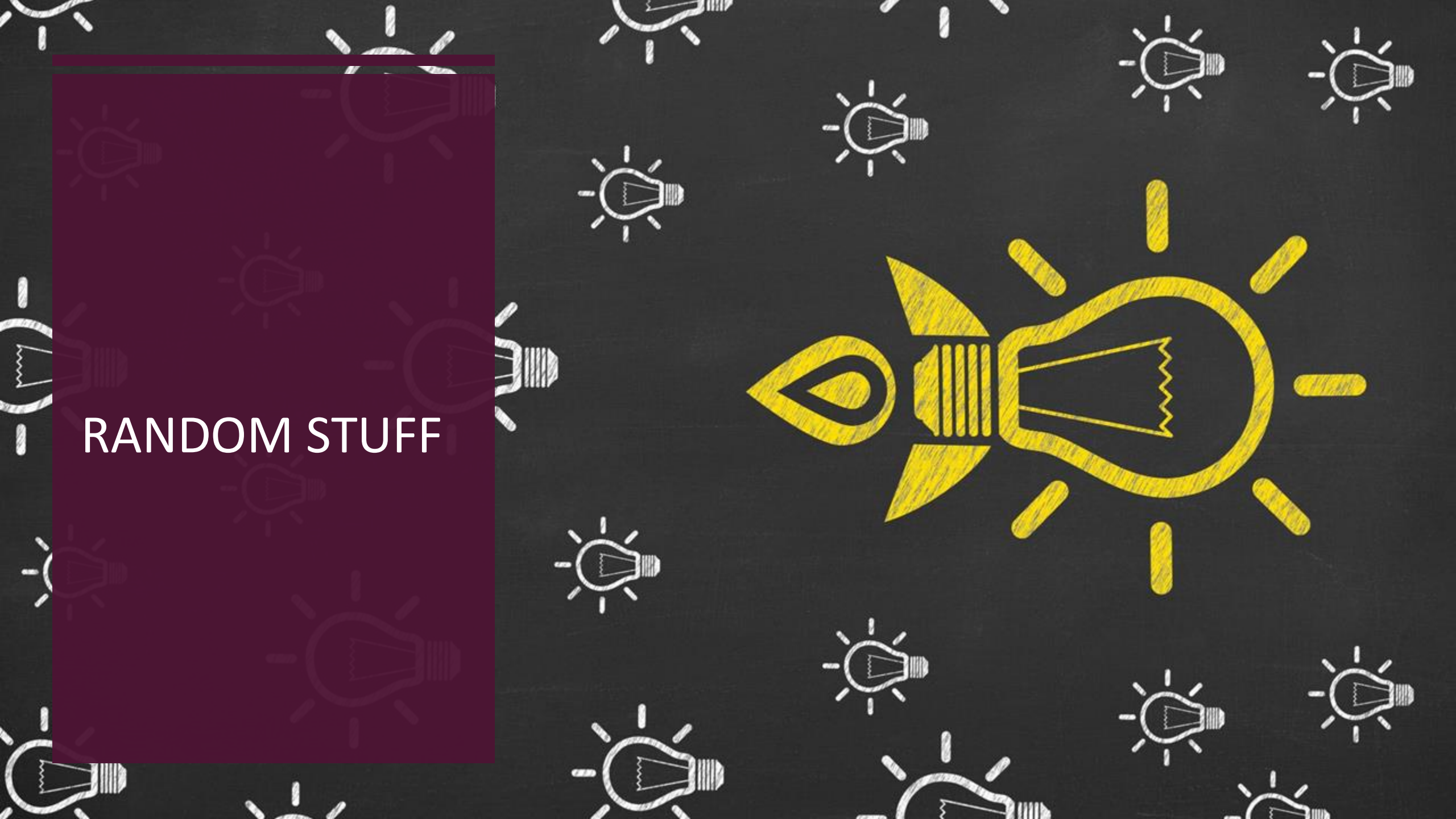
Purpose: To look at the (TBD applications, data, identity) asset class in more detail, from a zero trust point of view, a threat point of view and a protection point of view.

CAPSTONE ASSIGNMENT

Due Date: SATURDAY MAY 3

Purpose: To reflect on the intersection and benefits of a zero trust versus a secure be design versus a threat and risk point of view, given that ”you can’t have it all, but still have to protect an environment”.

RANDOM STUFF



REFERENCE

“MDR AS RIGHT OF BOOM TECHNOLOGY”

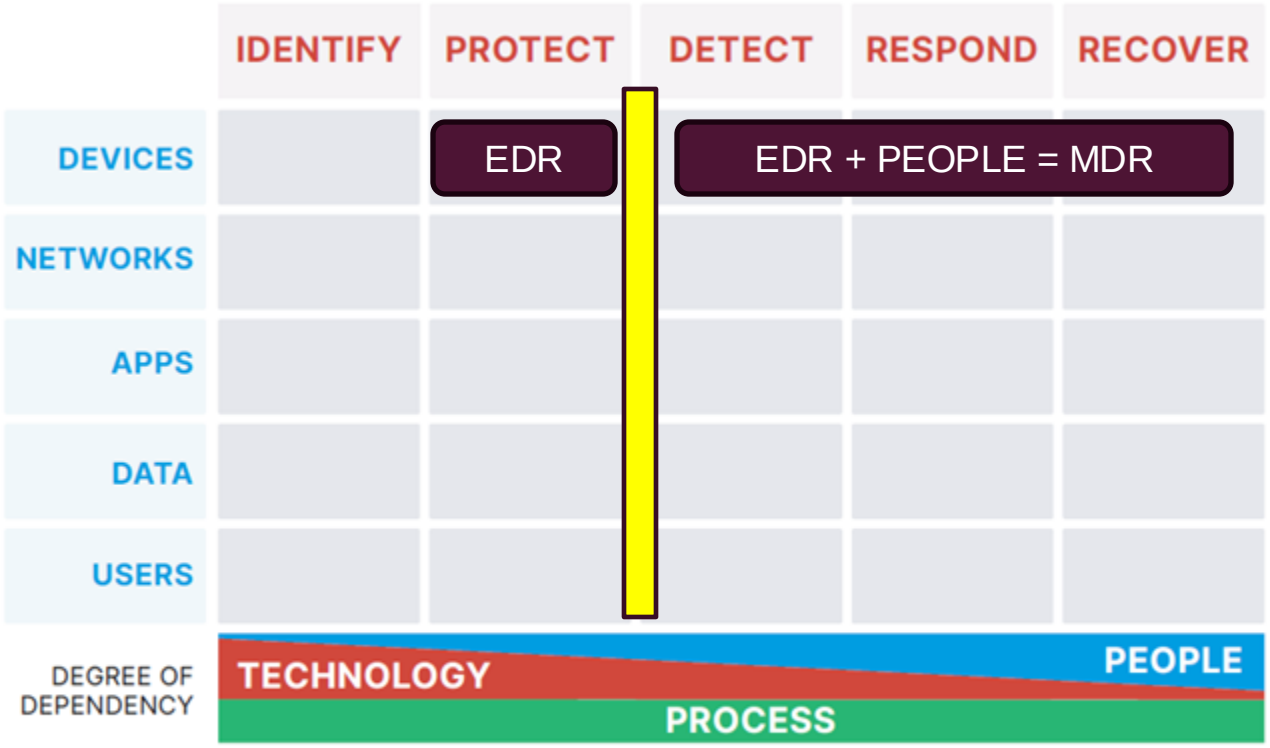


Figure 1: Cyber Defense Matrix

REFERENCE

Function	Action	Function Relationship
IDENTIFY	Create an inventory of things that are in scope for each of the asset classes and identify vulnerabilities and threats to those things → Define the defensive posture and mechanisms that prevents bad things happening (compromise of Confidentiality. Integrity, Availability) to the asset	*Activities in **IDENTIFY** let us decide what (and how) to **PROTECT***
PROTECT	Implement the defensive posture and mechanisms that prevent bad things → Define the events that indicate a failure of, or attempt to circumvent, protection mechanisms / capitalize on weaknesses / vulnerabilities.	*The mechanisms used to* **PROTECT** *must be monitored to **DETECT** attempts to compromised/bypass*
BOOM!		
DETECT	Monitor for events that indicate failure/compromise of protection → Raise alerts and notifications when events of interest are observed	*Activities in **DETECT** let us know what to **RESPOND** to*
RESPOND	On detection of (potentially) harmful events, take action to minimize / mitigate / neutralize the event	***RESPOND** activities determine what **RECOVERY** activities are required*
RECOVER	Restore environment and assets to intended state AND Review/update all functions for improvement to prevent a re-occurrence of Boom!	***RECOVERY** activities will include update of and improvements **to IDENTIFY, PROTECT, DETECT** and **RESPOND** functions*

THREATS, VULNERABILITIES, RISKS AND CVSS

COMMON VULNERABILITY SCORING SYSTEM

REFERENCE

CYBER THREATS

- *A Threat* is a process that magnifies the likelihood of a negative event, such as the exploitation of a vulnerability, leading to loss, damage, or destruction of assets
- Threats depend on vulnerabilities (with people, process, or technology)
- A cyber threat is an activity intended to compromise the security of an information system by altering the availability , integrity , or confidentiality of a system or the information it contains, or to disrupt digital life in general (https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment)

REFERENCE

CYBER RISKS

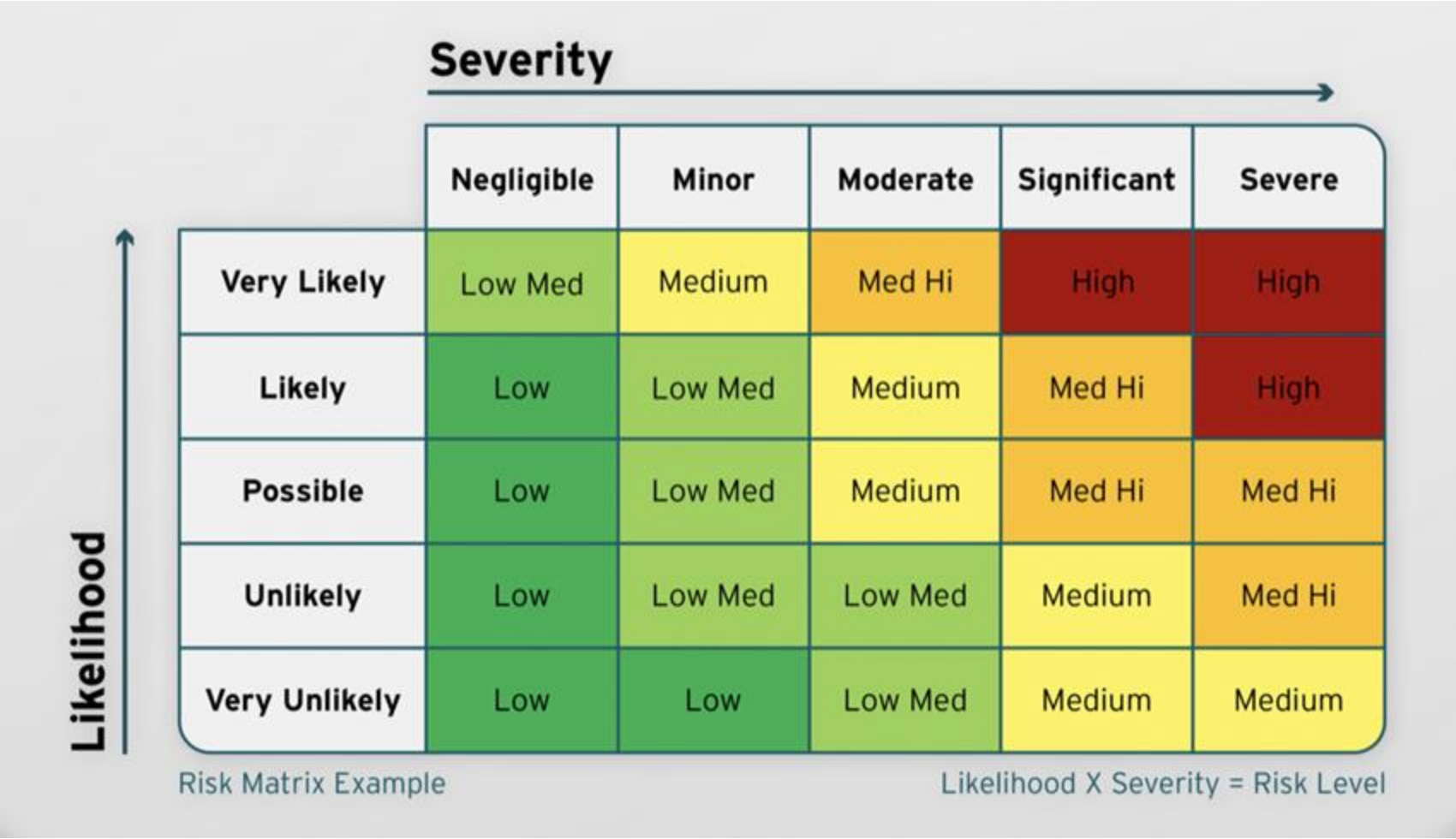
- What is a risk?
  - The likelihood of a negative (harmful) event occurring AND the potential of scale of that harm.
  - Organizational risk fluctuates over time, sometimes even on a daily basis, due to both internal and external factors.
  - Organizations focus on / care about risks that impact their business, namely their revenue
    - Cyber risks should be considered in the context of all of the business risks
    - This is where cyber struggles : financial risks are better understood and managed

ASSESSING THE RISK OF THREATS, VULNERABILITIES

- Assessing the risk of (the successful exploitation of) vulnerabilities means we need to be able to measure
  - The likelihood of its being exploited
    - Will it be exploited? Really????? → What is the probability or likelihood of something happening
  - The consequences or impact of its being exploited
    - What's the worst that could happen? Is it really that bad? → What is the financial impact?
- Because we always have competing priorities, we need to have a way to compare and evaluate the need to remediate a vulnerability (make it go away, or otherwise make it extremely unlikely to be exploited)

RISK ASSESSMENT MATRIX

- A risk assessment matrix identified IMPACT or CONSEQUENCES based on
  - the *likelihood* the risk event will occur, and,
  - the potential *severity* of the risk event



VULNERABILITIES

- What is a vulnerability?
  - A weakness, flaw or other shortcoming in infrastructure, networks or applications that exposes you to threats.
- Weaknesses can include:
  - Design vulnerabilities such as weakness built in due to design choices
  - Technical vulnerabilities, like bugs in code or an error in some hardware or software.
  - Human vulnerabilities, such as employees falling for phishing, smishing or other common attacks.
- Vulnerability exploitation involves taking advantage of weaknesses or flaws in the design, implementation, operation, or management of an IT system, device, or service, collectively referred to as vulnerabilities.

VULNERABILITY SCORING FOR SOFTWARE

- When dealing with technical vulnerabilities we can be a bit more rigorous because we have lots of experience and data to build a discipline
- The Common Vulnerability Scoring System (CVSS) allows us to classify vulnerabilities, assign a score, and use the classification and score determine which the vulnerabilities must be fixed within which timelines
- CVSS represents scoring based on
  - Exploitability & Impact Metrics
  - Threat metrics
  - Environmental Metrics
  - (Not included in score) Supplemental Metrics

REFERENCE

CVSS 4.0
https://www.first.org/cvss/v4.0/specification-document

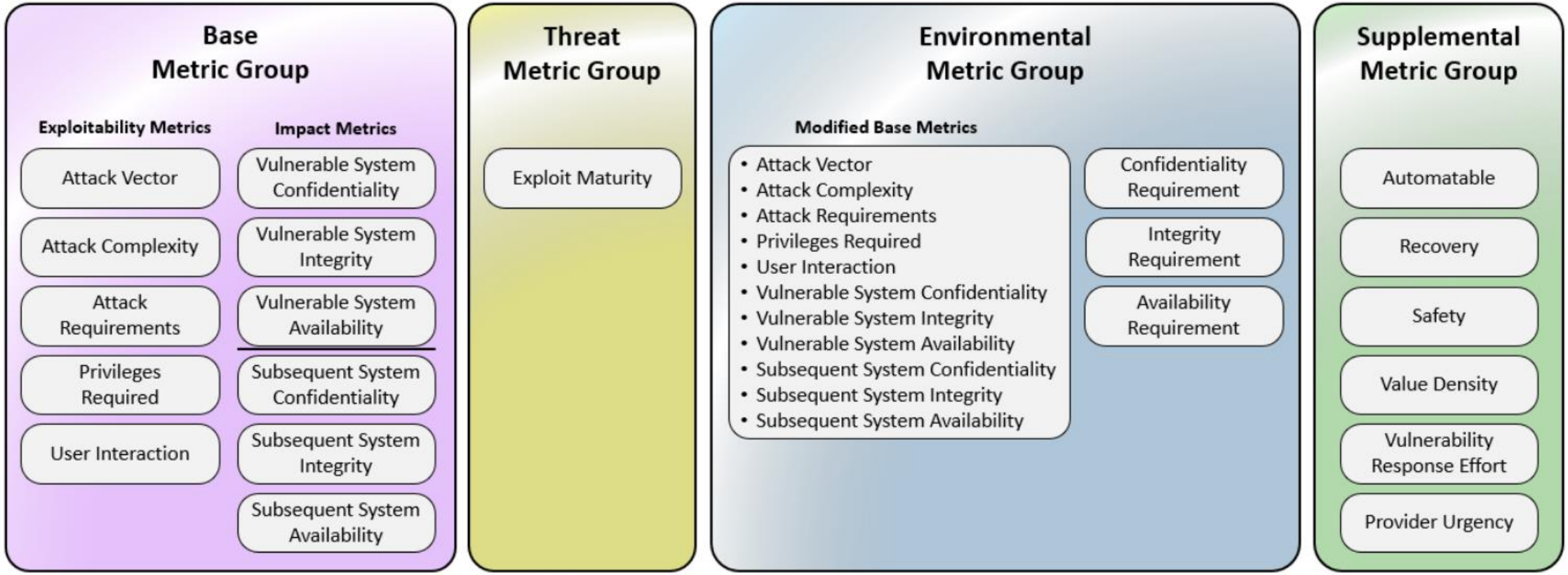


Figure 1: CVSS Metric Groups

CVSS
HTTPS://NVD.NIST.GOV/VULN-METRICS/CVSS

- The Common Vulnerability Scoring System (CVSS) is a method used to supply a qualitative measure of severity.
  - CVSS is not a measure of risk.

Severity	CVSS Base Score Range	Typical Time to Remediate
None	0.0	N/A
Low	0.1 - 3.9	180 Days
Medium	4.0 - 6.9	90 Days
High	7.0 - 8.9	30 Days
Critical	9.0 - 10.0	30 Days **

REFERENCE

REFERENCE NOTES
BREAKDOWN OF CVSS SCORING COMPONENTS

- The **Base** metric group represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments.
  - The **Exploitability** metrics reflect the ease and technical means by which the vulnerability can be exploited. That is, they represent characteristics of the "*thing that is vulnerable*", which we refer to formally as the "*vulnerable system*".
  - The **Impact** metrics reflect the direct consequence of a successful exploit and represent the consequence to the "*things that suffer the impact*", which may include impact on the vulnerable system and/or the downstream impact on what is formally called the "*subsequent system(s)*".
- The **Threat** metric group reflects the characteristics of a vulnerability related to threat that may change over time but not necessarily across user environments.
- The **Environmental** metric group represents the characteristics of a vulnerability that are relevant and unique to a particular consumers' environment. Considerations include the presence of security controls which may mitigate some or all consequences of a successful attack, and the relative importance of a vulnerable system within a technology infrastructure.
- The **Supplemental** metric group includes metrics that provide context as well as describe and measure additional extrinsic attributes of a vulnerability.
  - The response to each metric within the Supplemental metric group is to be determined by the CVSS consumer, allowing the usage of an end-user risk analysis system to apply locally significant severity to the metrics and values.
  - DOES NOT IMPACT CVSS SCORE

REFERENCE

REFERENCE NOTES
CISA’s KNOWN EXPLOITABLE VULNERABILITIES CATALOG
https://www.cisa.gov/known-exploited-vulnerabilities

- Cybersecurity and Infrastructure Security Agency: CISA (www.cisa.gov)
- CISA's Known Exploited Vulnerabilities (KEV) Catalog is a compilation of
  - Documented security vulnerabilities that have been successfully exploited
  - Vulnerabilities associated with ransomware campaigns
- The main criteria for KEV catalog inclusion, is whether the vulnerability has been *exploited* or is under *active exploitation*. These two terms refer to the use of malicious code by an individual to take advantage of a vulnerability.

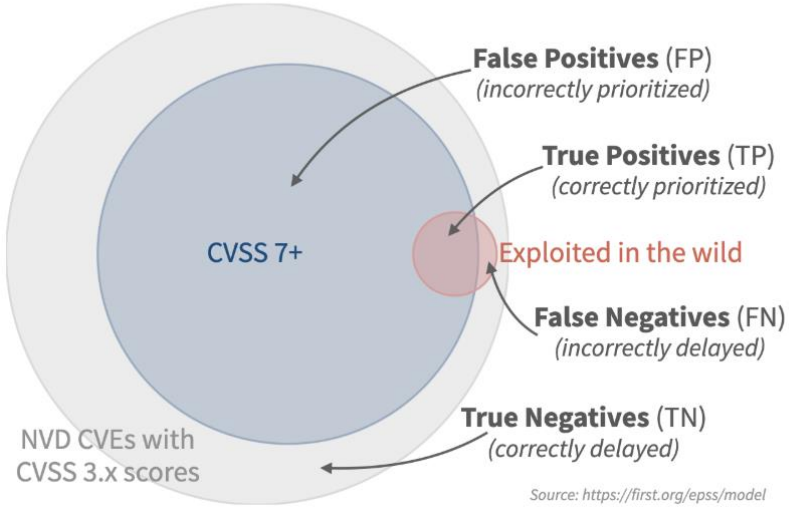
SOME OBSERVATIONS ABOUT CVSS SCORING

- Who you are MATTERS
- Kenna security, and now "FIRST.org" are looking at Exploit Prediction Scoring
  - The same vulnerability in a MSFT system is more likely to be exploited than if it occurred in "NobodyHasHeardOfUS Systems"

Performance: Remediating CVSS 7 and above

Looking at the performance of CVSS scores produced October 1st, 2023, comparing against the observed exploitation activity recorded from Oct 1st to Oct 30th, 2023. CVSS threshold is (arbitrarily) set at 7.

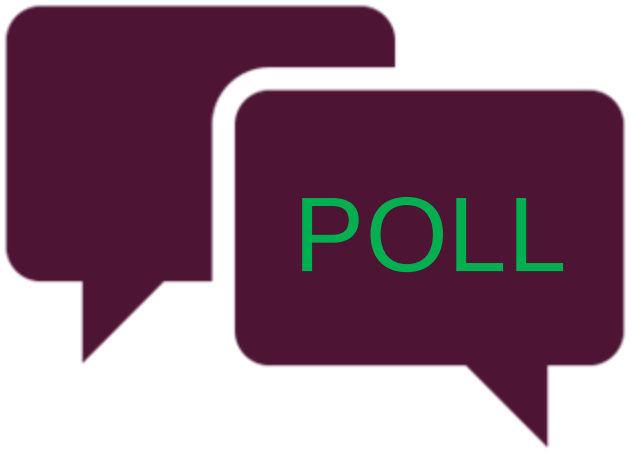
Our Decision…	Exploitation Activity… Observed	Not Observed
Remediate (CVSS 7+)	3,166 (2.3%) *True Positives (TP)*	76,858 (55.1%) *False Positives (FP)*
Delay (< CVSS 7)	686 (0.5%) *False Negatives (FN)*	58,763 (42.1%) *True Negatives (TN)*



CVSS IN YOUR ENVIRONMENT
https://www.first.org/cvss/v4.0/specification-document

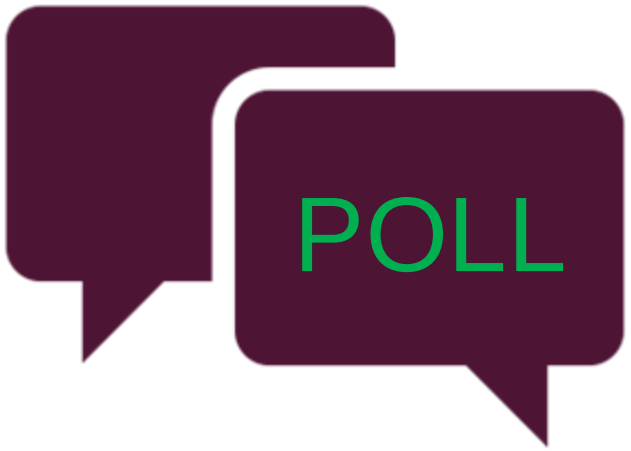
- Example 1 (Upgrading):
  - The default configuration of a component may require high privileges to access a particular function.
  - In a given environment, administrative privileges might be granted by default without authentication.
  - Setting Privileges Required to High and Modified Privileges Required to None to reflect this more serious condition in this environment.
  - TAKE AWAY: Authentication & Authorization matter
- Example 2 (Downgrading):
  - Systems and appliances located in an isolated network with no access to or from the Internet are not able to be attacked through the Wide Area Network (WAN).
  - All vulnerabilities found on those systems may have the Attack Vector (AV) values of “Network” reduced to “Adjacent”.
  - TAKE AWAY: Internet access / exposure matters

DISCUSSION PROMPT



- *Poll: Suppose I have two systems, one that is "mission critical" and one that is "yeah, meh, we can live without it". If I can only remediate one vulnerability, which should I prioritize*
  - *A mission critical system with a CVSS=6.9 vulnerability*
  - *A development system with a CVSS=9.8 vulnerability*
- *Which do I prioritize for remediation first?*

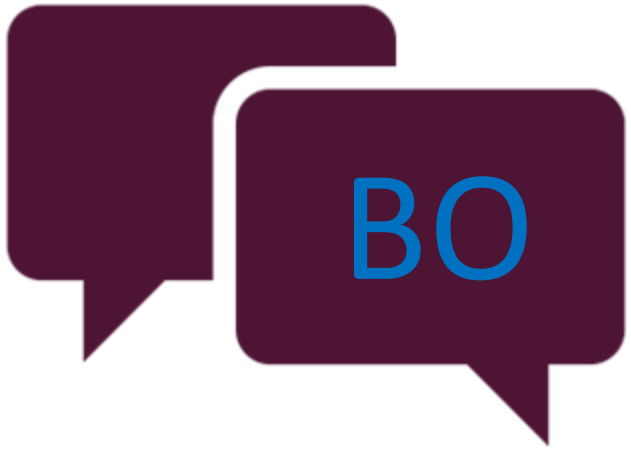
DISCUSSION PROMPT



- *Poll: Instead of two systems, one that is "mission critical" and one that is "yeah, meh, we can live without it" how do you prioritize if you are looking at two environments, "production" (where all my customer data / sensitive applications are located) and development/test ("yeah, meh, we can live without it because it is used to test and can be blown away at any point)*

- *What if*
  - *Production environment has system(s) with a critical vulnerability (CVSS 9.1) that is NOT in the KEV*
  - *Dev/Test environment has system(s) with moderate vulnerability (CVSS 6.7) that IS in the KEV*
  - *Which do you prioritize?*

BREAKOUT DISCUSSION: PRIORITIZIATION



- *How do the poll results and your experience support the observation of a "non-permanence mindset" when considering the overall protection of your environment from cybersecurity threats.*
- *would you have changed your answers if you had been told*
  - *The systems were (or were not) Internet facing*
  - *The systems were servers hosting customer data*
  - *The systems were network devices controlling access to environment*
  - *The systems hosted critical applications needed by business*
  - *The systems were used by privileged admins only*
- *Is this type of information more or less meaningful to you than information about the environment (production v dev/test)?*

CANVAS DISCUSSION: THOUGHTS ON THE BREAKOUT DISCUSSION

- *NOTE: Canvas Discussion, not YellowDig*
- *If you participated in a Breakout in the live lecture, what surprised you the most from your team's discussion? What did you learn / what will you take away from that discussion?*
- *If you watched the Breakout discussion as part of the asynch lecture, what did you agree with / what made sense to you in the discussion? What surprised you in the discussion or provided a new way to look at the topic of discussion.*
- *This should take you 5 minutes and no more than 15 minutes to answer.*

10 min
BREAK
BACK 6:XX
PM ET

SECURE BY DESIGN,
ZERO TRUST
ARCHITECTURE,
EO 14028,
CYBER DEFENSE MATRIX,

EXECUTIVE ORDER 14028

https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity#h-1

- 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 Fed
- Sec. 8. Improving the Federal Government's Investigative and Remediation Capabilities.

Zero Trust Architectures

Secure by Design

CVSS / Vuln Mgmt

SECURE BY DESIGN PLEDGE, PRINCIPLES

https://www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles

- The Secure by Design Pledge from CISA
  - Improve the discipline, maturity and security quality of products and services that are used as part of a company's operations
- The Pledge is structured with seven goals
  - Multi-factor Authentication
  - Default passwords
  - Reducing entire classes of vulnerabilities
  - Security Patches
  - Vulnerability Disclosure Policy
  - CVEs (Timely & accurate reporting of vulnerabilities)
  - Evidence of intrusions (access to logs)

Secure by Design Principles from NCSC

- Five principles for the design of cyber secure systems
- 1. Establish the context before designing a system
  - Have a good understanding of the fundamentals
- 2. Make compromise difficult
  - Make it hard(er) to compromise your data or systems.
- 3. Make disruption difficult
  - Design for acceptable 'down time' (including zero).
- 4. Make compromise detection easier
- 5. Reduce the impact of compromise
  - Design to naturally minimise the severity of any compromise.

SECURE BY DESIGN --> ZERO TRUST

Looking at the NCSC requirements for Secure by Design, three of these are represent controls / responsibilities that are joint for development and operations:

1. Make compromise difficult
2. Make disruption difficult
3. Reduce the impact of compromise

Zero Trust

- Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned)

Zero Trust is actually quite complicated to do comprehensively across all asset classes

- The Zero Trust Maturity Model will help us protect our enviroments

ZERO TRUST ARCHITECTURE

https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

- EO 14028 marked a renewed commitment to and prioritization of federal cybersecurity modernization. Among other policy mandates, EO 14028 embraced zero trust as the desired security model for the federal government and called for FCEB agencies to develop plans to implement ZTAs.
- The Federal Government, as with most large enterprises, faces several challenges in implementing ZTA. Legacy systems often rely on “implicit trust,” in which access and authorization are infrequently assessed based on fixed attributes; this conflicts with the core principle of adaptive evaluation of trust within a ZTA. Existing infrastructures built on implicit trust will require investment to change systems to better align with zero trust principles. Furthermore, as the technology landscape continues to evolve, new solutions and continued discussions on how to best achieve zero trust objectives are paramount.
- The ZTMM represents a gradient of implementation across five distinct pillars, in which minor advancements can be made over time toward optimization.
- The Zero Trust Architecture (ZTA) covers the pillars of Identity, Devices, Networks, Applications and Workloads, and Data.

NIST CSF / ASSET CLASSES / ITIL / ZERO TRUST MATURITY MODEL

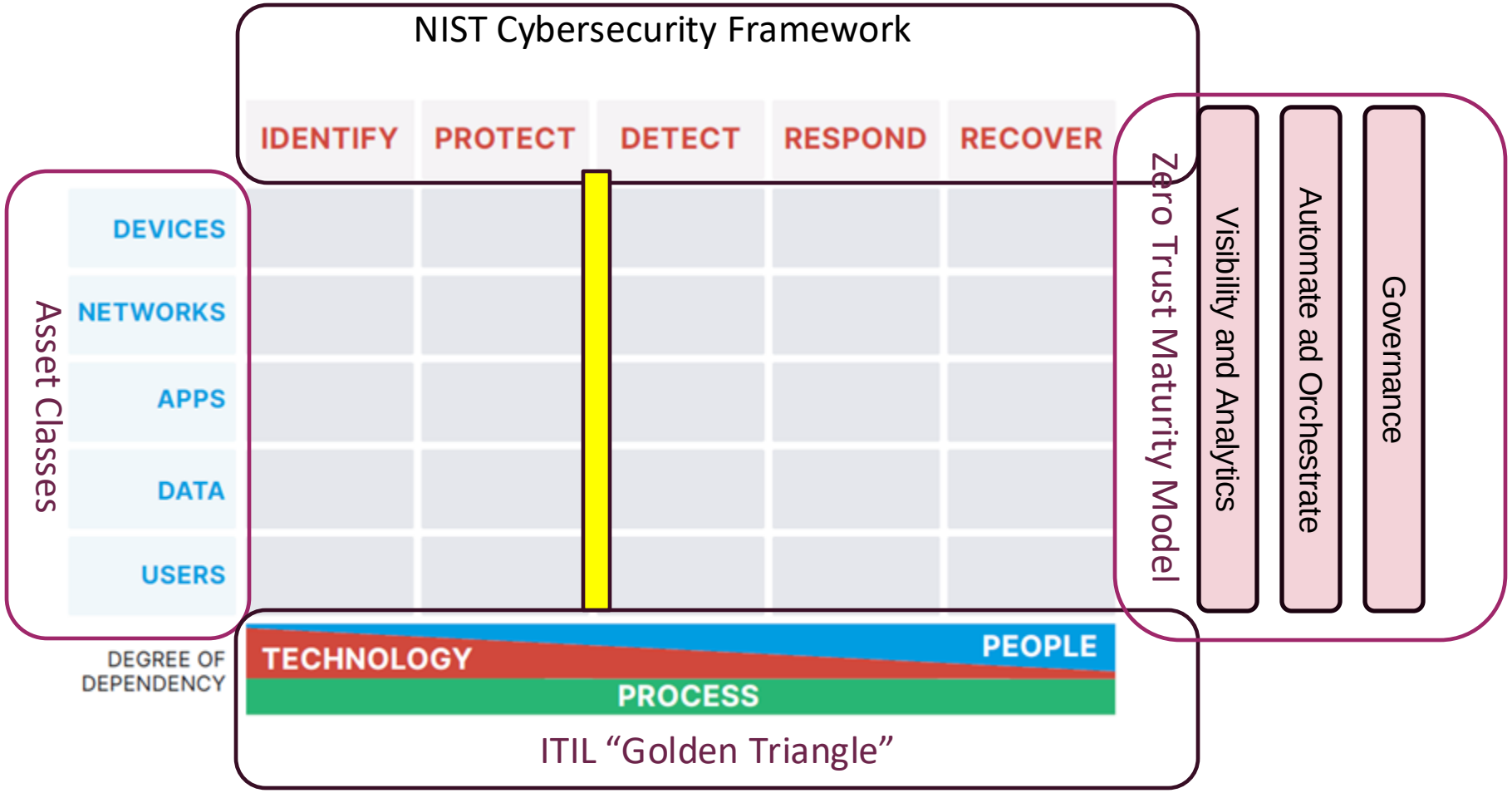


Figure 1: Cyber Defense Matrix

CYBER DEFENSE MATRIX (CDM)

Asset Class	Examples
Network	Communication channels, connections and protocols that enable traffic to flow among devices and applications. Note that this does NOT refer to the actual infrastructure (routers, switches) but rather to the paths themselves and the protocols used in those paths. This class includes VPC, VPN, CDN as well as DNS, BGP, email and web filtering
Devices	Workstations, servers, phones, tablets, IoT, containers, hosts, compute, peripherals storage devices, network devices, web cameras, infrastructure, etc. This asset class includes the operating systems and firms of these devices as well as other software that is native to or inherent to the device. Networking devices like switches and routers are included here because the devices themselves need to be considered separately from the communication path they create.
Applications	Software code and applications on the devices, separate from the operating system/firmware. This class includes serverless functions, APIs and microservices. This also includes the business applications that support a company - from HR Systems (eg Workday), to Customer Relationship Management (eg Salesforce), to payroll, billing, and the applications that are “used” to do work (email,G Suite/Box, web conferencing, telephone systems)
Data	The information residing on (data-at-rest), traveling through (data-in-motion), or processed (data-in-use) the resources listed above. This class includes databases, S3 buckets, storage blobs, and files
Users	The people using the resources listed above and their associated identities. This includes customers (using the applications/services your company provides) and the employees of your company

ZERO TRUST ARCHITECTURE (ZTA)

Asset Class	Examples
Network	A network refers to an open communications medium including typical channels such as agency internal networks, wireless networks, and the Internet as well as other potential channels such as cellular and application-level channels used to transport messages.
Devices	A device refers to any asset (including its hardware, software, firmware, etc.) that can connect to a network, including servers, desktop and laptop machines, printers, mobile phones, IoT devices, networking equipment, and more.
Applications	Applications and workloads include agency systems, computer programs, and services that execute on-premises, on mobile devices, and in cloud environments.
Data	Data includes all structured and unstructured files and fragments that reside or have resided in federal systems, devices, networks, applications, databases, infrastructure, and backups (including on-premises and virtual environments) as well as the associated metadata.
Users / Identity	An identity refers to an attribute or set of attributes that uniquely describes an agency user or entity, including non-person entities.

ZERO TRUST MATURITY MODEL

https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

TLP:CLEAR

- Visibility and Analytics: Visibility refers to the observable artifacts that result from the characteristics of and events within enterprise-wide environments. The focus on cyber-related data analysis can help … build a risk profile to develop proactive security measures before an incident occurs.
- Automation and Orchestration: Zero trust makes full use of automated tools and workflows that support security response functions across products and services while maintaining oversight, security, and interaction of the development process for such functions, products, and services.
- Governance: Governance refers to the definition and associated enforcement of agency cybersecurity policies, procedures, and processes, within and across pillars, to manage an agency's enterprise and mitigate security risks in support of zero trust principles and fulfillment of federal requirements.

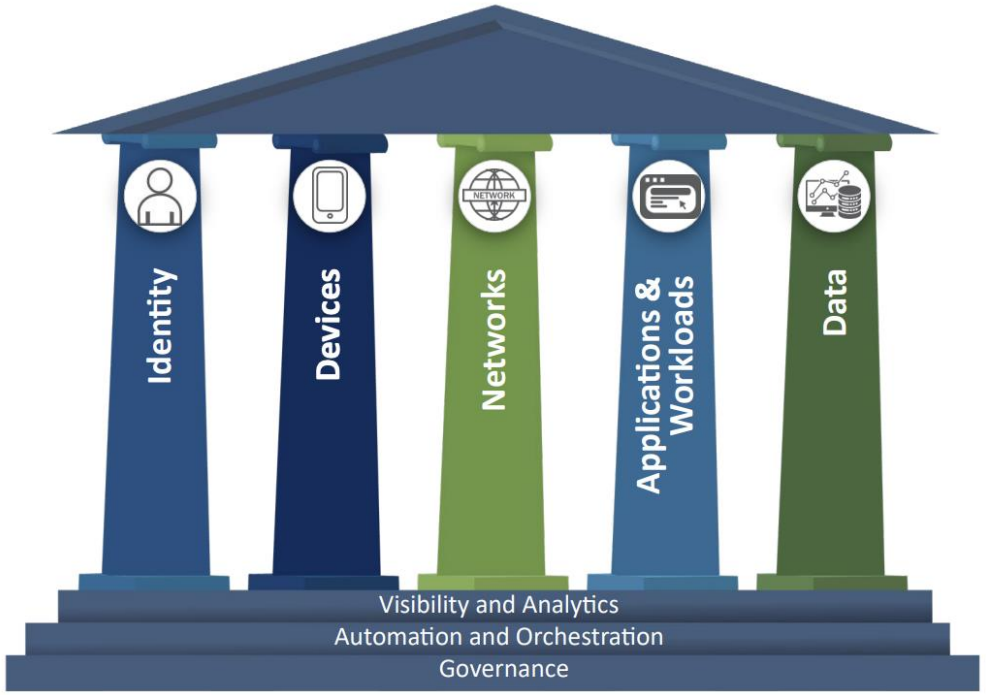


Figure 1: Zero Trust Maturity Model Pillars[8]

GENERATIVE AI IMPACT: GARTNER REPRINT

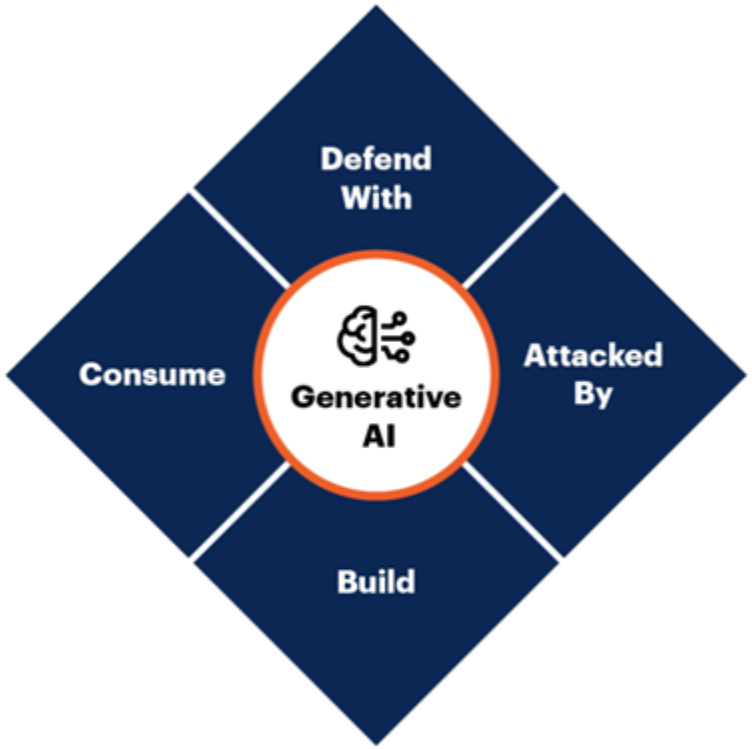
Gartner: 4 Ways Generative AI Will Impact CISOs and Their Teams

29 June 2023- ID G00793265

1. “Defend with” generative cybersecurity AI:
   a. Receive the mandate to exploit GenAI opportunities to improve security and risk management, optimize resources, defend against emerging attack techniques or even reduce costs.
2. “Attacked by” GenAI:
   a. Adapt to malicious actors evolving their techniques or even exploiting new attack vectors thanks to the development of GenAI tools and techniques.
3. Secure enterprise initiatives to “build” GenAI applications:
   a. AI applications have an expanded attack surface and pose new potential risks that require adjustments to existing application security practices.
4. Manage and monitor how the organization “consumes” GenAI:
   a. ChatGPT was the first example; embedded GenAI assistants in existing applications will be the next. These applications all have unique security requirements that are not fulfilled by legacy security controls.

Key Impacts of Generative AI for CISOs

- Lack of maturity
- Risks due to vendor rush
- Privacy and efficacy challenges



- Multiple consumption options
- Shadow AI
- Data privacy and copyright

- Skill augmentation
- Attack automation
- Content generation

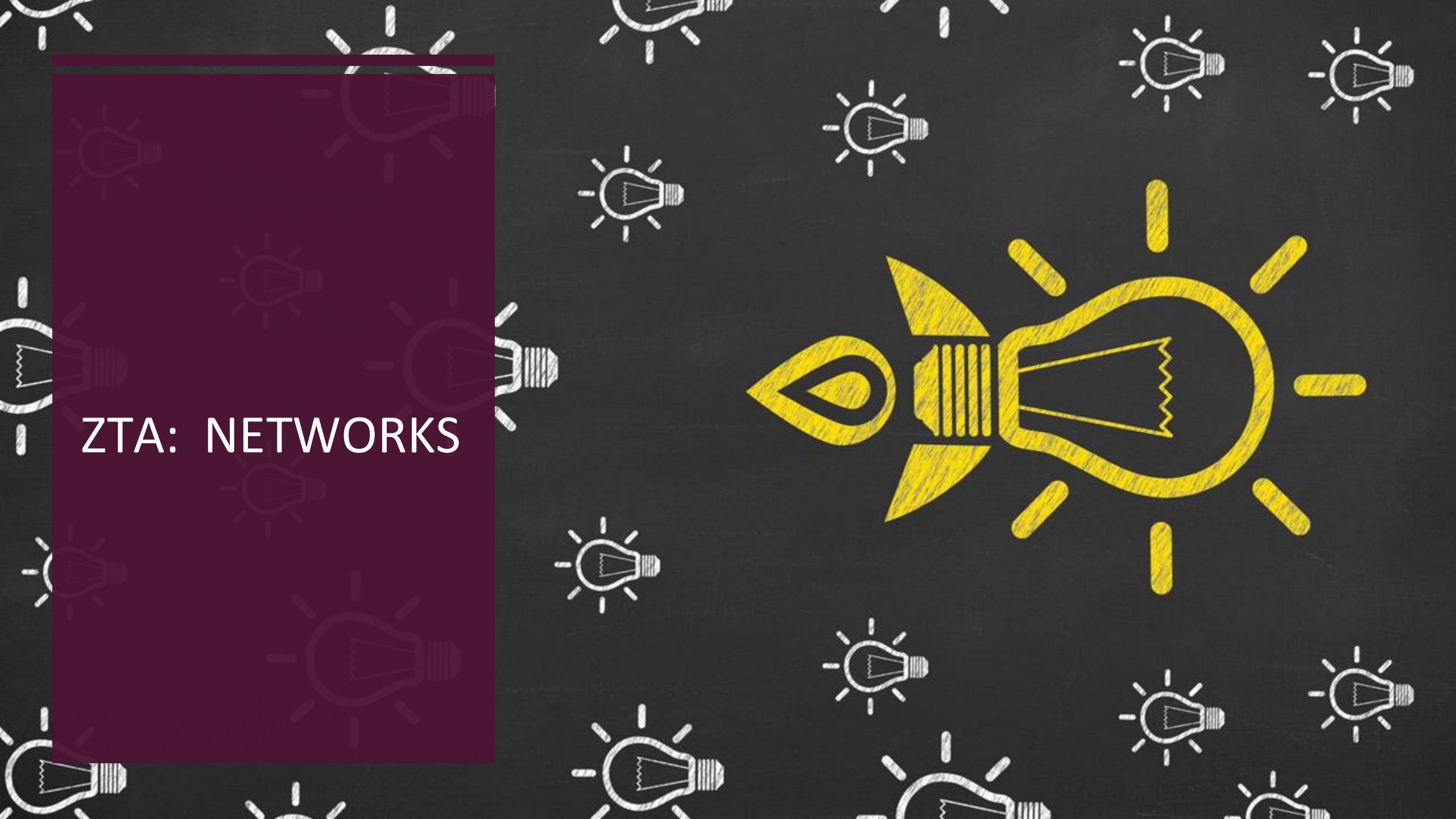
- Data theft/poisoning
- No best practice
- Upcoming regulation

Source: Gartner

793265_C

Gartner

ZTA: NETWORKS



NETWORKS: ZTA v CDM

ZTA

A network refers to an open communications medium including typical channels such as agency internal networks, wireless networks, and the Internet as well as other potential channels such as cellular and application-level channels used to transport messages.

CDM

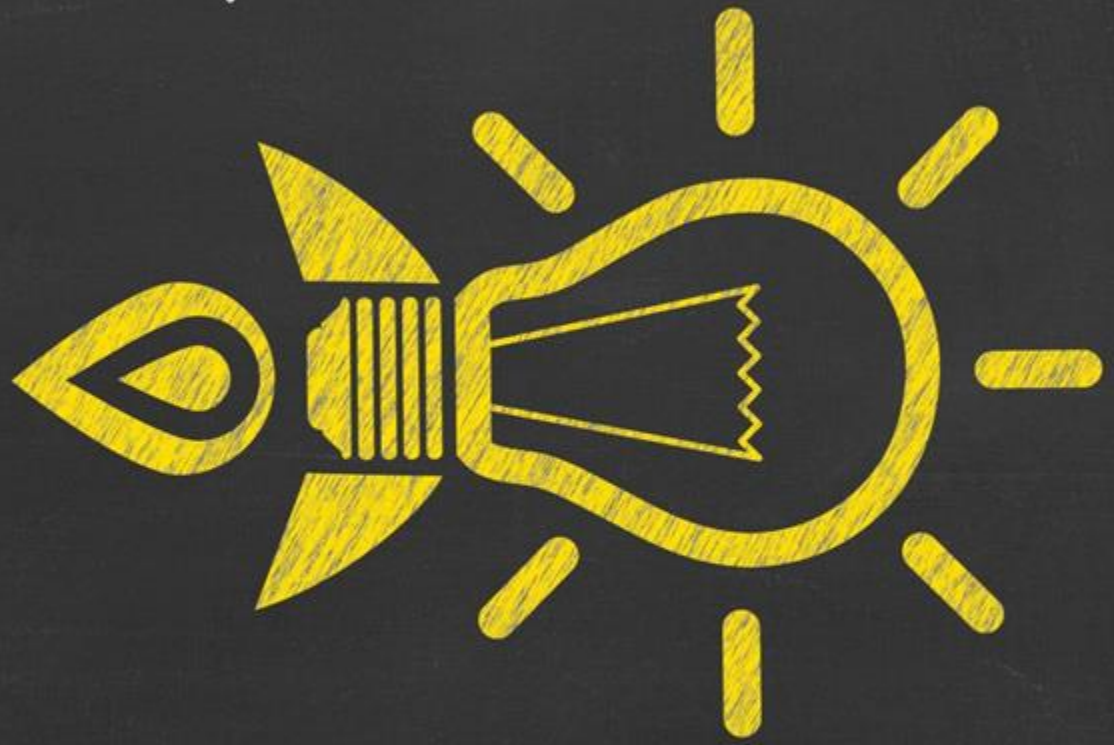
Communication channels, connections and protocols that enable traffic to flow among devices and applications.

Note that this does NOT refer to the actual infrastructure (routers, switches) but rather to the paths themselves and the protocols used in those paths. This class includes VPC, VPN, CDN as well as DNS, BGP, email and web filtering

REFERENCES
ANTICIPATED END OF LECTURE 2

REFERENCE

ENVIRONMENT FOR CLASS DISCUSSION, ASSIGNMENTS



REFERENCE

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

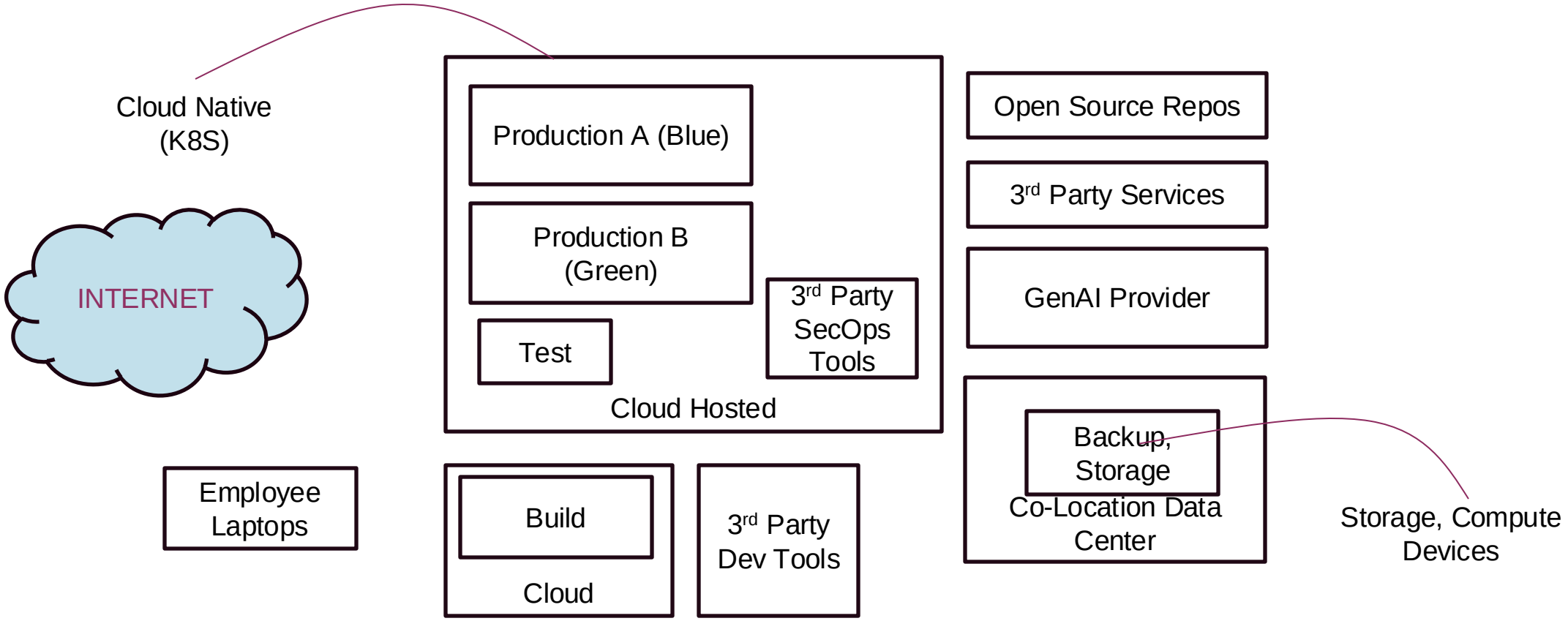
REFERENCE

VARY / COURSE DISCUSSION ENVIRONMENT (CDE)

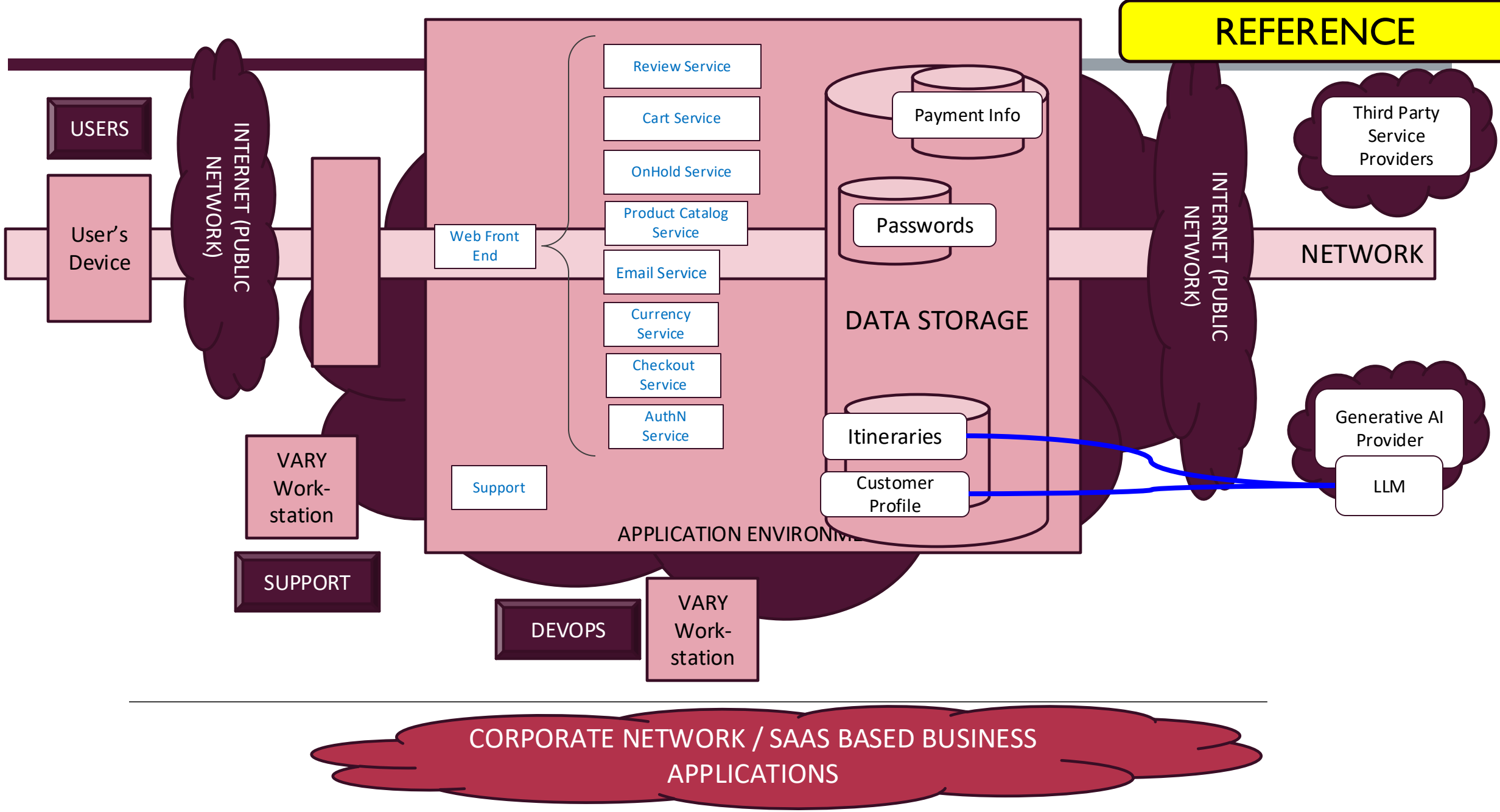
- VARY is hosted on the Cloud with a backup of data (including the configuration, customer and product data) in a co-located data center
- The cloud hosted environment/architecture includes container-based resources, cloud service provider resources and services (including a cloud hosted development environment and build pipeline)
- The co-lo data center is where VARY hosts its network termination gear (in a locked network closet) and servers (in a locked cage hosted in the server rooms/raised floor area of the date center).
- In the locked cage you have network, compute and, storage devices that you manage remotely
- VARY application provides a very important (software) service to its users/customers;
  - Your customers will suffer financial, emotional and reputational damage if it is not performing as expected
- Customers are located in and residents of the USA, Canada and the EU
- Service requires payment options from customers (processed by a third party)
- Service may host sensitive or confidential information about a customer and will host Personally Identifiable Information
- VARY has both in-house developed code as well as open-source software and third-party developed applications to provide your service
- VARY has recently added a GenAI angle to allow it to analyse its data and provide better services to customers

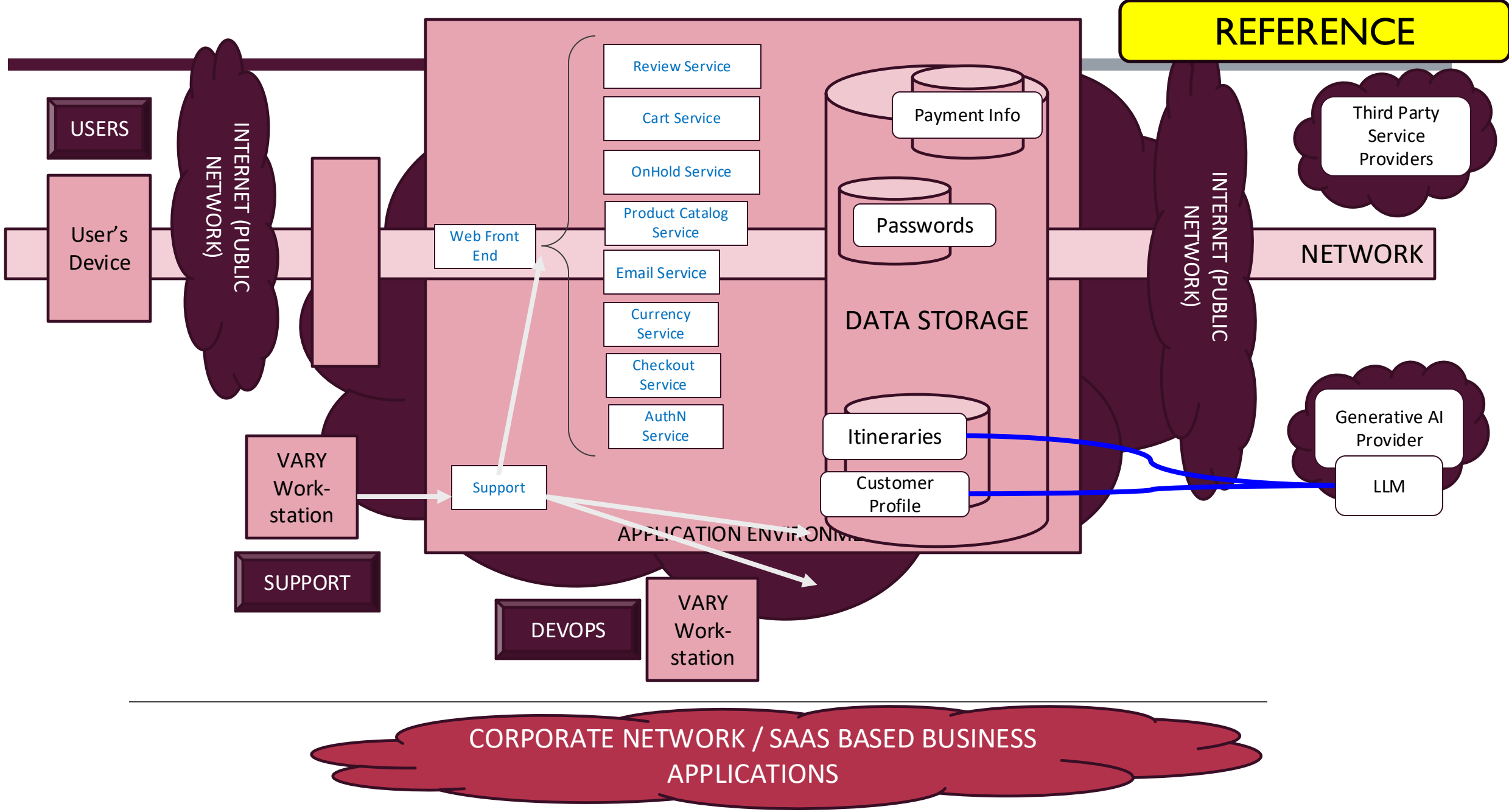
REFERENCE

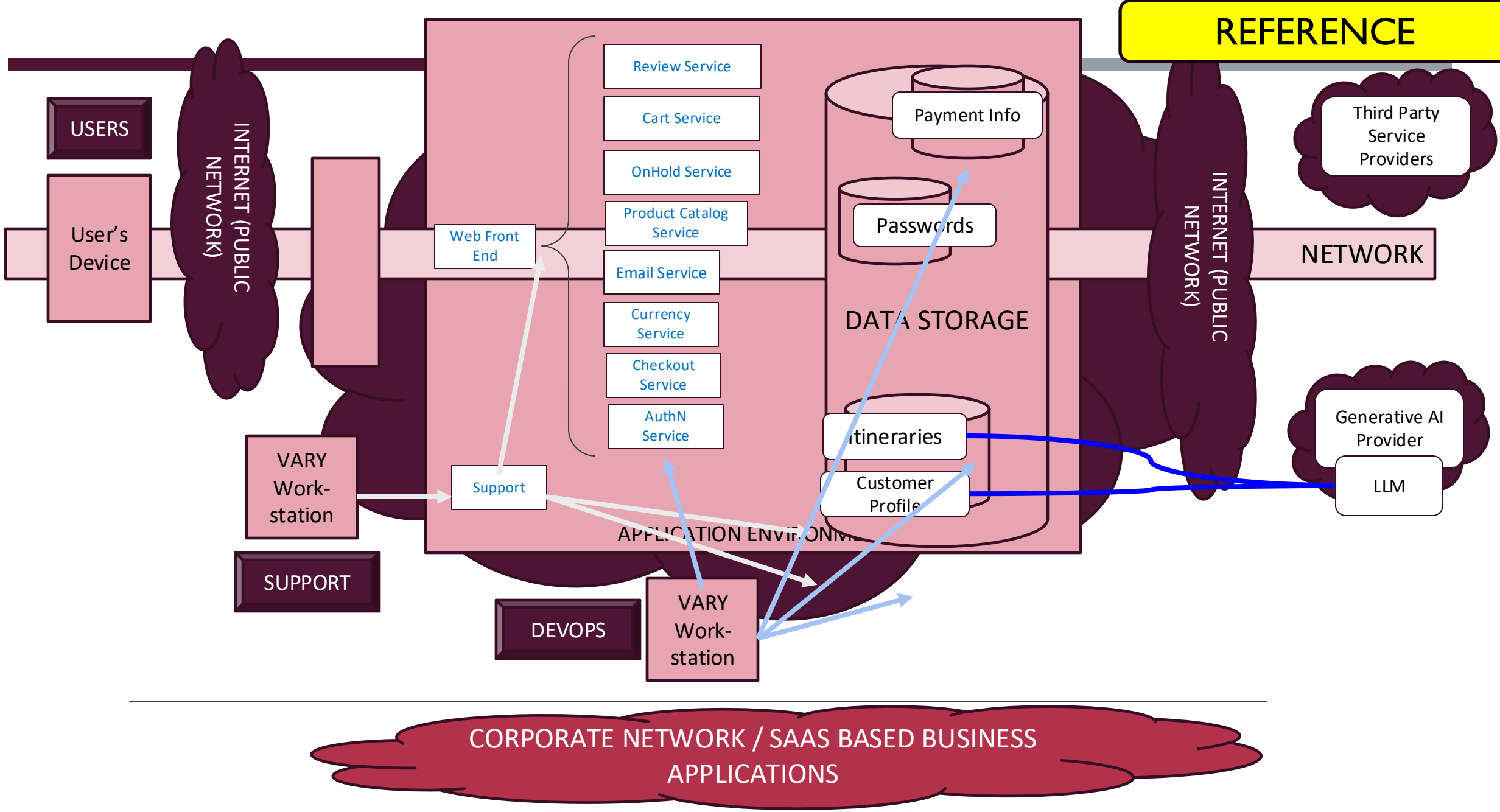
VARY HIGH LEVEL COMPONENTS

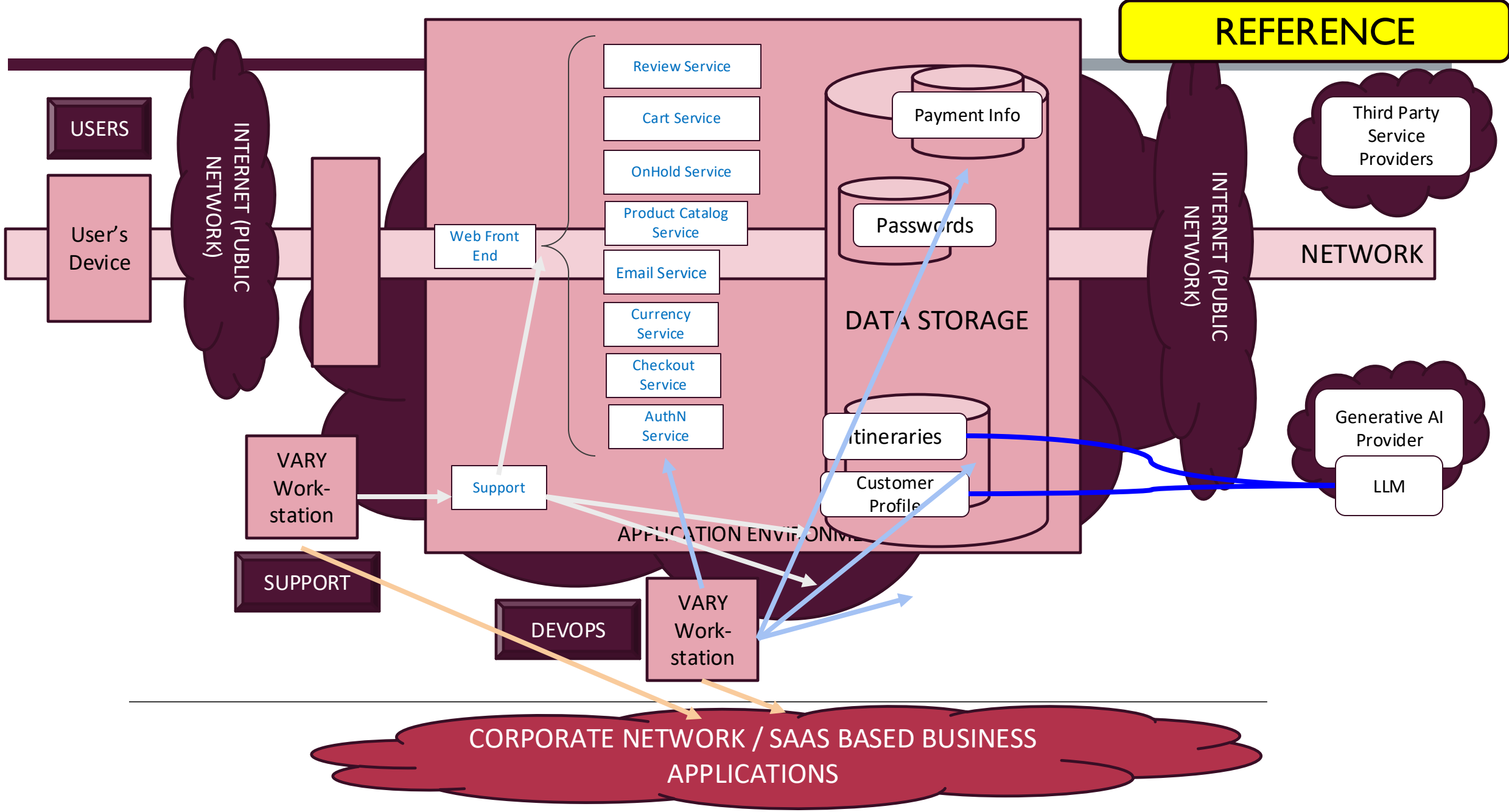


MORE DIAGRAMS AT THE BACK OF THE DECK


REFERENCE
USERS
User's Device
INTERNET (PUBLIC NETWORK)
Review Service
Cart Service
OnHold Service
Product Catalog Service
Email Service
Currency Service
Checkout Service
AuthN Service
Web Front End
Support
Payment Info
Passwords
DATA STORAGE
Itineraries
Customer Profile
INTERNET (PUBLIC NETWORK)
NETWORK
Third Party Service Providers
Generative AI Provider
LLM
VARY Work-station
SUPPORT
DEVOPS
VARY Work-station
CORPORATE NETWORK / SAAS BASED BUSINESS APPLICATIONS

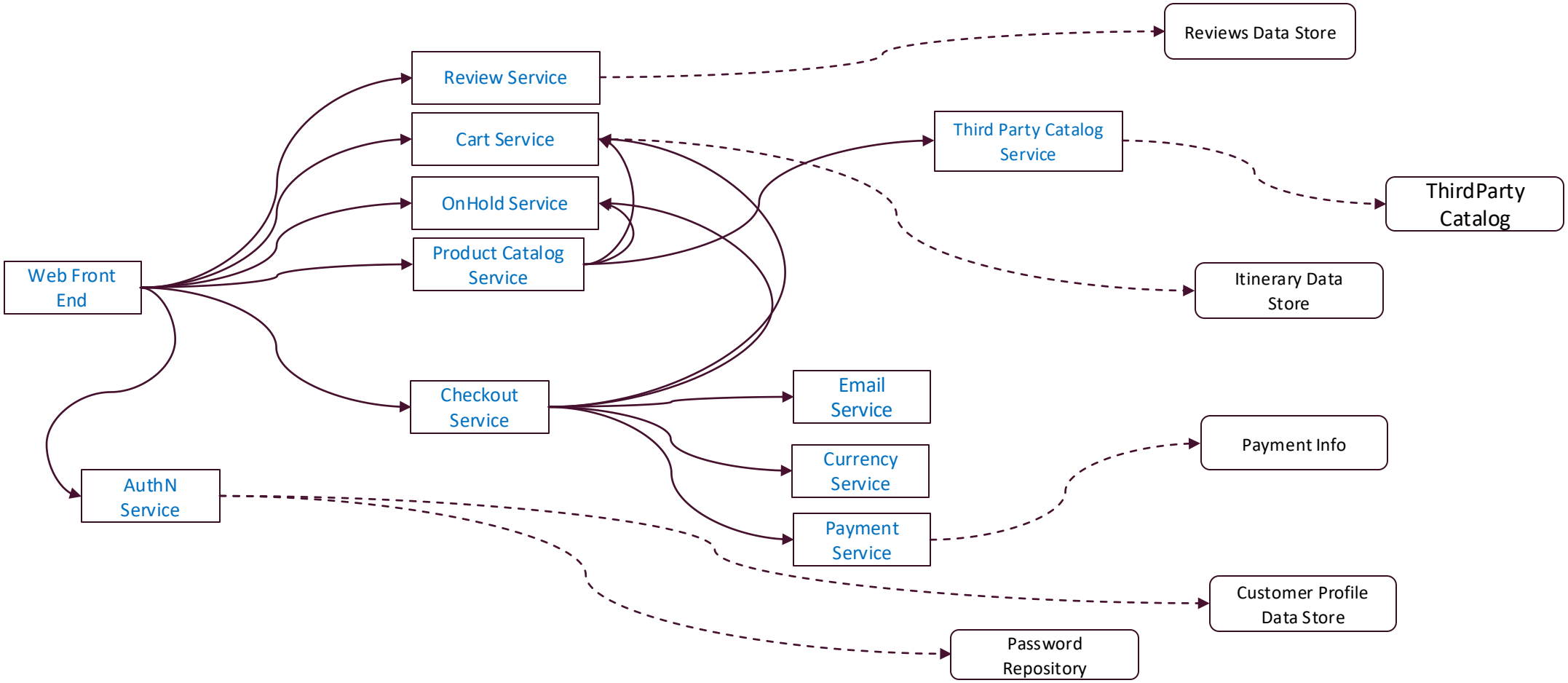

REFERENCE
USERS
User's Device
INTERNET (PUBLIC NETWORK)
Web Front End
Review Service
Cart Service
OnHold Service
Product Catalog Service
Email Service
Currency Service
Checkout Service
AuthN Service
Payment Info
Passwords
DATA STORAGE
Itineraries
Customer Profile
INTERNET (PUBLIC NETWORK)
NETWORK
Third Party Service Providers
Generative AI Provider
LLM
VARY Work-station
Support
SUPPORT
DEVOPS
VARY Work-station
CORPORATE NETWORK / SAAS BASED BUSINESS APPLICATIONS


REFERENCE
USERS
User's Device
INTERNET (PUBLIC NETWORK)
Web Front End
Review Service
Cart Service
OnHold Service
Product Catalog Service
Email Service
Currency Service
Checkout Service
AuthN Service
Payment Info
Passwords
DATA STORAGE
Itineraries
Customer Profile
INTERNET (PUBLIC NETWORK)
NETWORK
Third Party Service Providers
Generative AI Provider
LLM
VARY Work-station
Support
SUPPORT
DEVOPS
VARY Work-station
CORPORATE NETWORK / SAAS BASED BUSINESS APPLICATIONS


REFERENCE
USERS
User's Device
INTERNET (PUBLIC NETWORK)
Web Front End
Review Service
Cart Service
OnHold Service
Product Catalog Service
Email Service
Currency Service
Checkout Service
AuthN Service
Payment Info
Passwords
DATA STORAGE
Itineraries
Customer Profile
INTERNET (PUBLIC NETWORK)
NETWORK
Third Party Service Providers
Generative AI Provider
LLM
VARY Work-station
Support
SUPPORT
DEVOPS
VARY Work-station
CORPORATE NETWORK / SAAS BASED BUSINESS APPLICATIONS

REFERENCE

VARY SERVICE ARCHITECTURE



REFERENCE

VARY APPLICATION: RESERVATION/CHECKOUT