Lecture 4
Feb 18, 2025

CSCI E-117A SPRING 2025

SECURE APPLICATIONS: MANAGING THE DEPLOYMENT INFRASTRUCTURE

LECTURE 4 AGENDA

- YellowDig
  - ”Most impactful” (One excerpt only)
- Assignment 1 Feedback
- Networks
  - Network Architectures
  - Network Stack Intro
  - Stack-level threats
- Network Protocol Vulnerabilities
- Network Zero Trust Architecture
- Industrial Control Systems (ICS) and ZTA
- Vulnerabilities
  - Known Exploitable
- End of “formal” material
  - YellowDig last week
  - Course Assignment reminders

QUICK ANNOUNCEMENTS

- From YellowDig
- Useful
  - https://consumer.ftc.gov/articles/how-secure-your-home-wi-fi-network
- Not so useful (and called out as such in the YD post)
  - https://internetmarketingsteps.com/best-ai-cybersecurity-tools-for-home-networks-in-2024
  - A list of vendors who claim to use AI to thwart home network/computing attacks. The reason I said "claim to" is because I think most of these solutions are probably more "machine learning" than AI. Nonetheless, it was interesting to scroll down the list to see which vendors are jumping on the AI-bandwagon in an effort to sell their product

How Phished Data Turns into Apple & Google Wallets

- https://krebsonsecurity.com/2025/02/how-phished-data-turns-into-apple-google-wallets/

- This is a GREAT basis for discussion of ZTA principles for devices and applications
- We will follow this in upcoming lectures (no “In the News” points for posting this in YellowDig)

YELLOW DIG LAST WEEK

YELLOW DIG – FAVORITE / TOPICAL / IN THE NEWS

- I have always heard that the average cybersecurity budget is 10-15% of total IT budget, but I know IT budget can vary greatly between companies.
  - Discussion of budget amounts …
- [Consider] the concept of "cost" on both sides. By utilizing encryption, secure passwords, MFA, and other types of security controls we increase the cost of an attacker to compromise or gain access.. When we implement these controls the cost of running, maintaining and building these controls requires cost in the resources to operate which we assign value to in mitigating risk
- Building secure workloads requires headcount, cutting headcount makes maintenance harder. It's a razors edge.

UK DEMANDS APP CREATE BACK DOORS

https://archive.is/20250210125416/https:/www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/#selection-655.0-655.177

- https://archive.is/20250210125416/https:/www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/#selection-655.0-655.177
- Per the Washington Post, Security officials in the United Kingdom have demanded that Apple create a back door allowing them to retrieve all the content any Apple user worldwide has uploaded to the cloud. The British government's undisclosed order, issued last month, requires blanket capability to view fully encrypted material, not merely assistance in cracking a specific account.
- The British government's undisclosed order, issued last month, requires blanket capability to view fully encrypted material, not merely assistance in cracking a specific account, and has no known precedent in major democracies

UK DEMANDS APP CREATE BACK DOORS

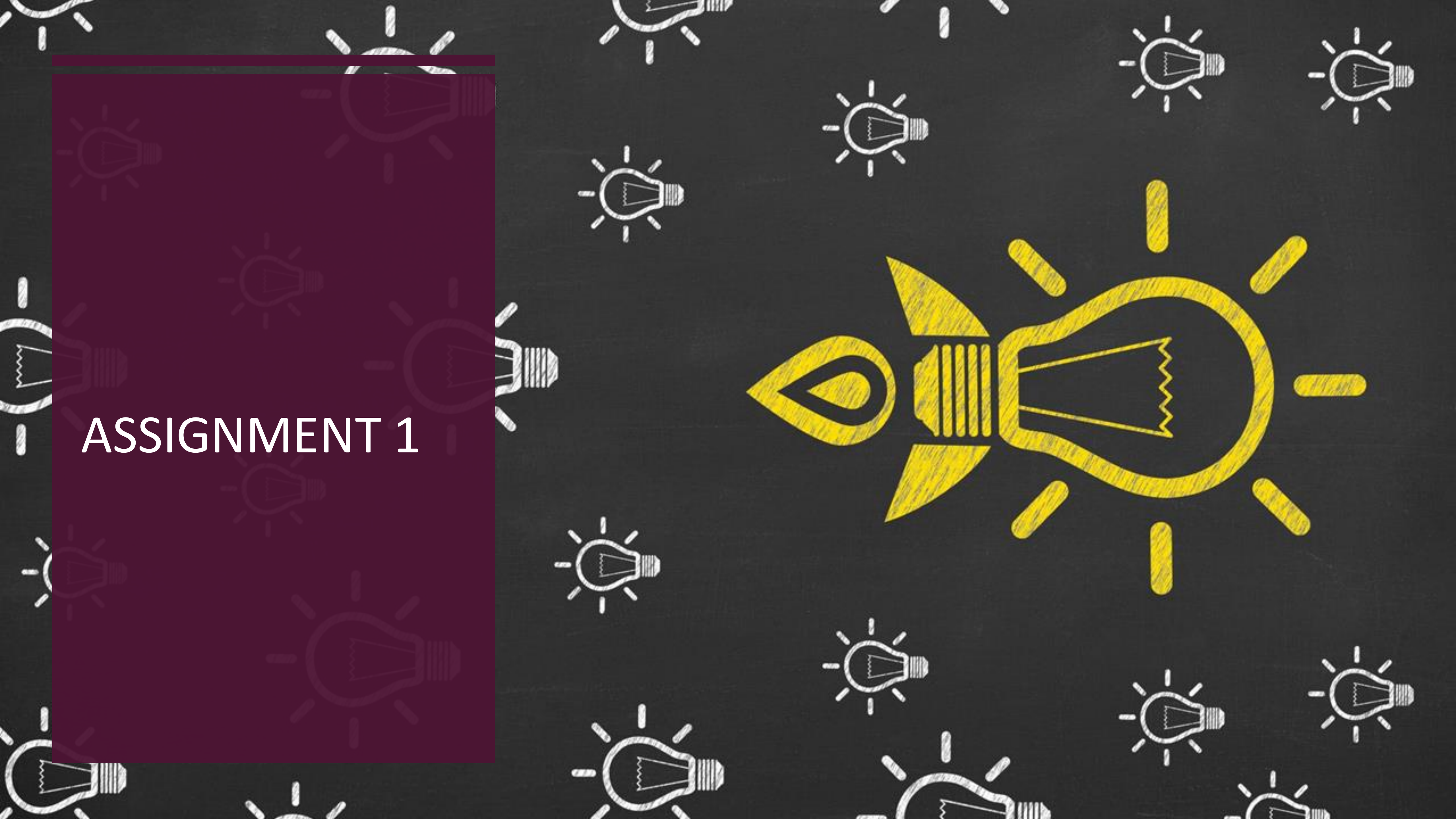
https://archive.is/20250210125416/https:/www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/#selection-655.0-655.177

- At issue is cloud storage that only the user, not Apple, can unlock. Apple started rolling out the option, which it calls Advanced Data Protection, in 2022. It had sought to offer it several years earlier but backed off after objections from the FBI during the first term of President Donald Trump, who pilloried the company for not aiding in the arrest of “killers, drug dealers and other violent criminal elements.” The service is an available security option for Apple users in the United States and elsewhere.
- iCloud storage and backups are favored targets for U.S. search warrants, which can be served on Apple without the user knowing.
- Law enforcement authorities around the world have complained about increased use of encryption in communication modes beyond simple phone traffic, which in the United States can be monitored with a court’s permission.
- The U.K. and FBI in particular have said that encryption lets terrorists and child abusers hide more easily. Tech companies have pushed back, stressing a right to privacy in personal communication and arguing that back doors for law enforcement are often exploited by criminals and can be abused by authoritarian regimes.

UK DEMANDS APP CREATE BACK DOORS

https://archive.is/20250210125416/https:/www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/#selection-655.0-655.177

- Apple argued then that wielding the act against strong encryption would conflict with a ruling by the European Court of Human Rights that any law requiring companies to produce end-to-end encrypted communications "risks amounting to a requirement that providers of such services weaken the encryption mechanism for all users" and violates the European right to privacy.
- In the United States, decades of complaints from law enforcement about encryption have recently been sidelined by massive hacks by suspected Chinese government agents, who breached the biggest communications companies and listened in on calls at will. In a joint December press briefing on the case with FBI leaders, a Department of Homeland Security official urged Americans not to rely on standard phone service for privacy and to use encrypted services when possible.
- Also that month, the FBI, National Security Agency and the Cybersecurity and Infrastructure Security Agency joined in recommending dozens of steps to counter the Chinese hacking spree, including "Ensure that traffic is end-to-end encrypted to the maximum extent possible."



ASSIGNMENT 1

ASSIGNMENT 1 FEEDBACK

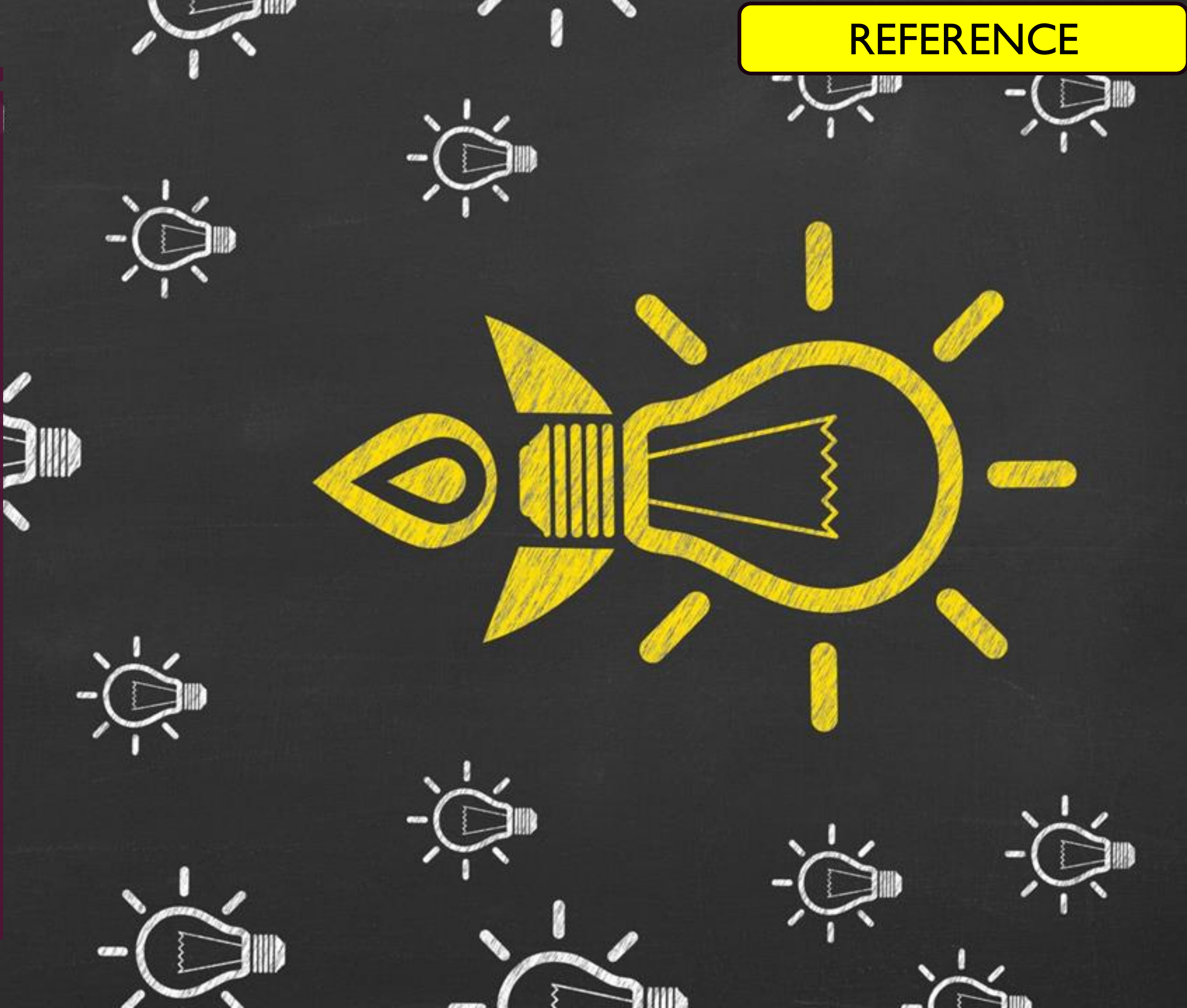
Due Date: Feb 16

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 Feedback, Statistics and other Details

REFERENCE

REMINDERS



REFERENCE

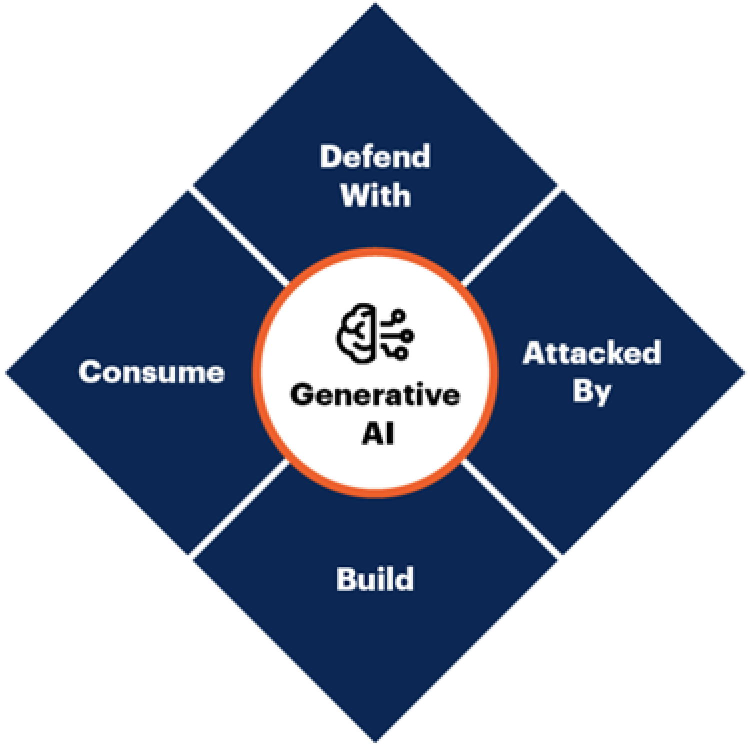
Gartner: 4 Ways Generative AI Will Impact CISOs and Their Teams

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.

REFERENCE

Key Impacts of Generative AI for CISOs



Defend With

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

Consume

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

Generative AI

Attacked By

- Skill augmentation
- Attack automation
- Content generation

Build

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

Source: Gartner

793265_C

REFERENCE

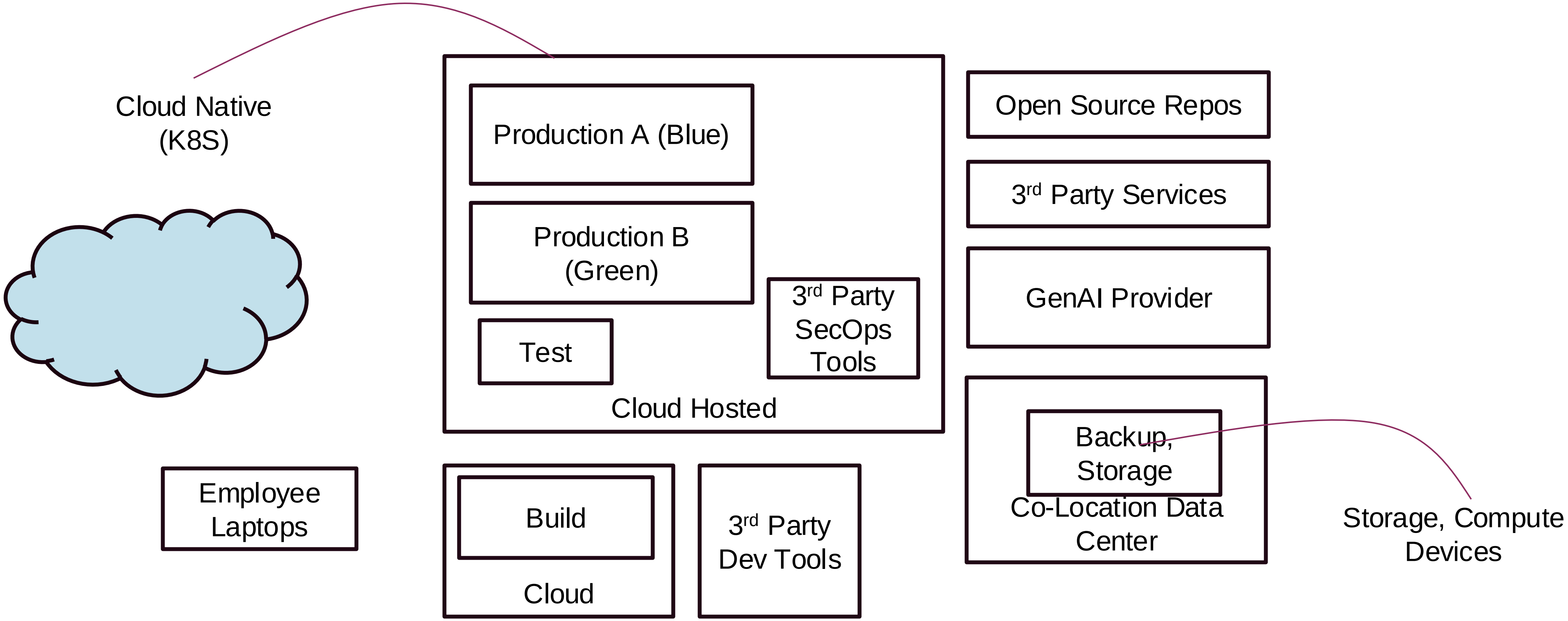
Asset Class	Examples
Network	Communication channels, connections and protocols that enable traffic to flow among devices and applications. Note that this does NOT refer to the actual infrastructure (routers, switches) but rather to the paths themselves and the protocols used in those paths. This class includes VPC, VPN, CDN as well as DNS, BGP, email and web filtering, SSL/TLS, HTML
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

REFERENCE

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.

ZTA Focus	Network Segmentation	Network Traffic Management	Traffic Encryption	Network Resilience
Description	Segments / subnets with controlled access to move from flat to segmented network	Monitor traffic to track and analyse data flowing across a network; identify potential issues, understand usage patterns, and optimize performance	Point to point, End to end with robust key management	System designed to withstand disruptions, recover quickly from failures, and maintain operational continuity even during unexpected events
Maturity Goal	Moving from perimeter-internal to “segments” that allow isolation of workloads in progressively more restrictive segments	Move from manual management of static rules and configurations to automation and dynamic rules and configurations including dynamically responding to new/emerging threats	Moving from minimal to comprehensive encryption of traffic including mutual authentication of parties as part of encryption	Move from limited resilience of networks to fully redundant and always available networks
Tools	Firewalls , VPNs, IPTables	Network monitoring tools	P2P with segmentation tools E2E with applications / ”endpoints”	CDN, Redundant network paths
In the News	Ivanti, Fortinet, Nobelium Stuxnet, Ukranian Utilities	SolarWinds	Mitre T1040	Volumetric DDOS Undersea networks

REFERENCE



Cloud Native (K8S)

Production A (Blue)

Production B (Green)

Test

3rd Party SecOps Tools

Cloud Hosted

Open Source Repos

3rd Party Services

GenAI Provider

Backup, Storage

Co-Location Data Center

Storage, Compute Devices

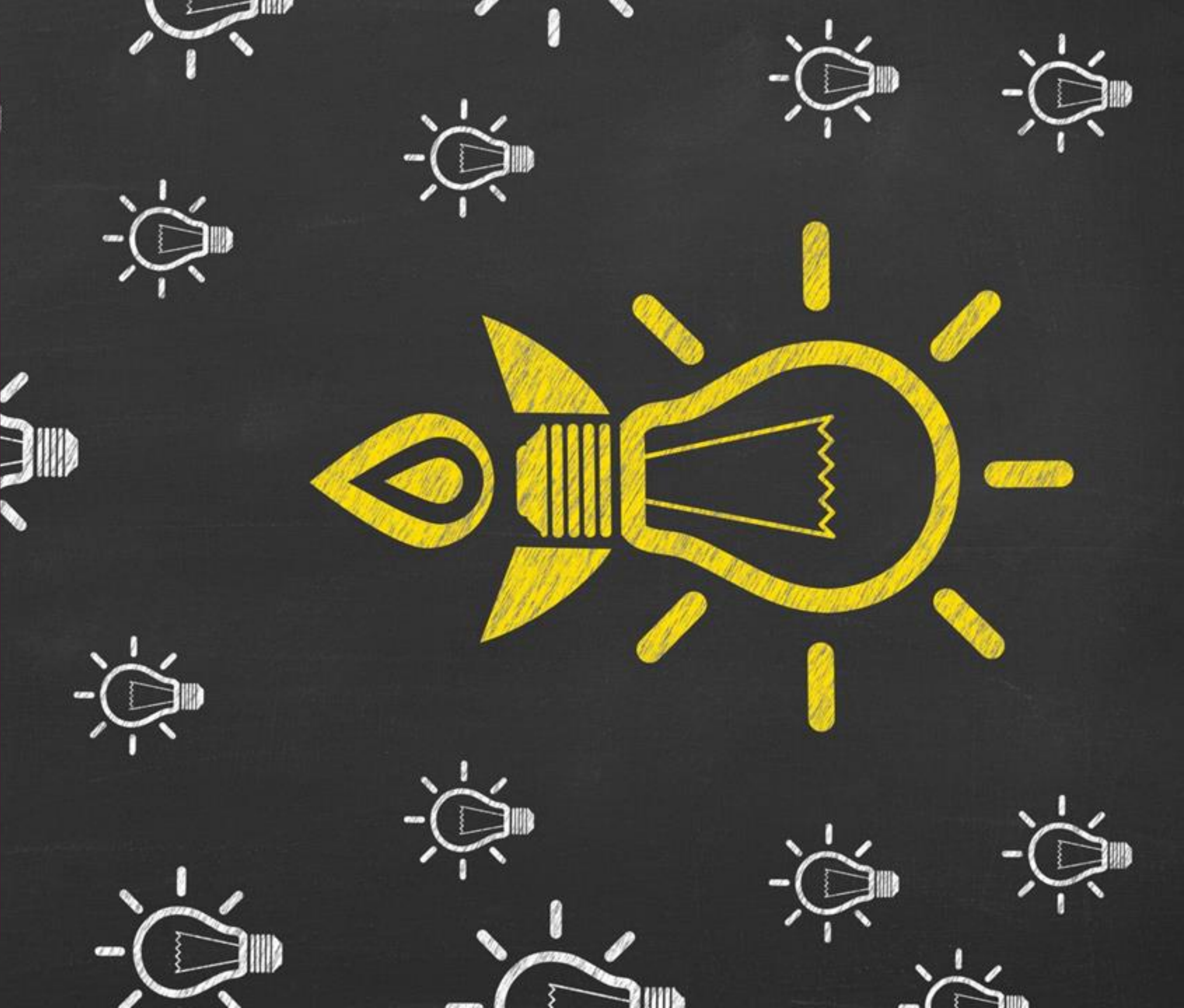
Employee Laptops

Build

Cloud

3rd Party Dev Tools

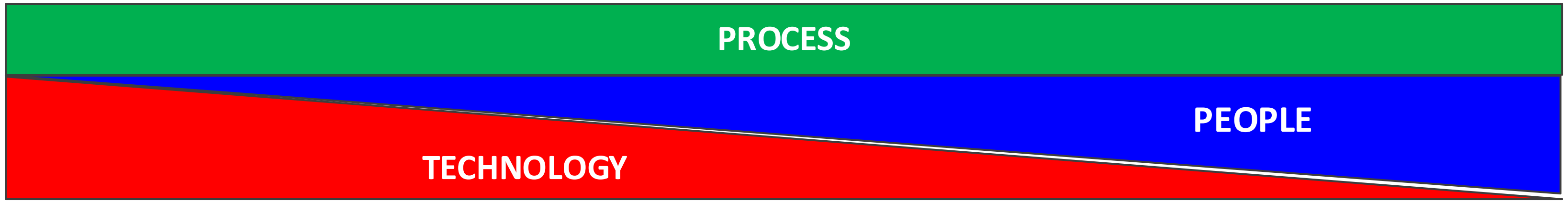
ZTMM,
800-207 &
CYBER DEFENSE MATRIX



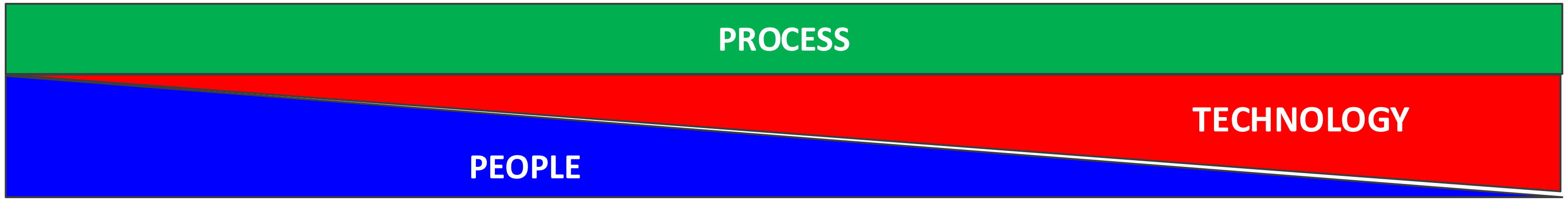
CISA ZERO TRUST MATURITY

Various ZTA publications informed the development of this maturity model (see Section 6 for additional details). This model reflects the seven tenets of zero trust as outlined in NIST SP 800-207:

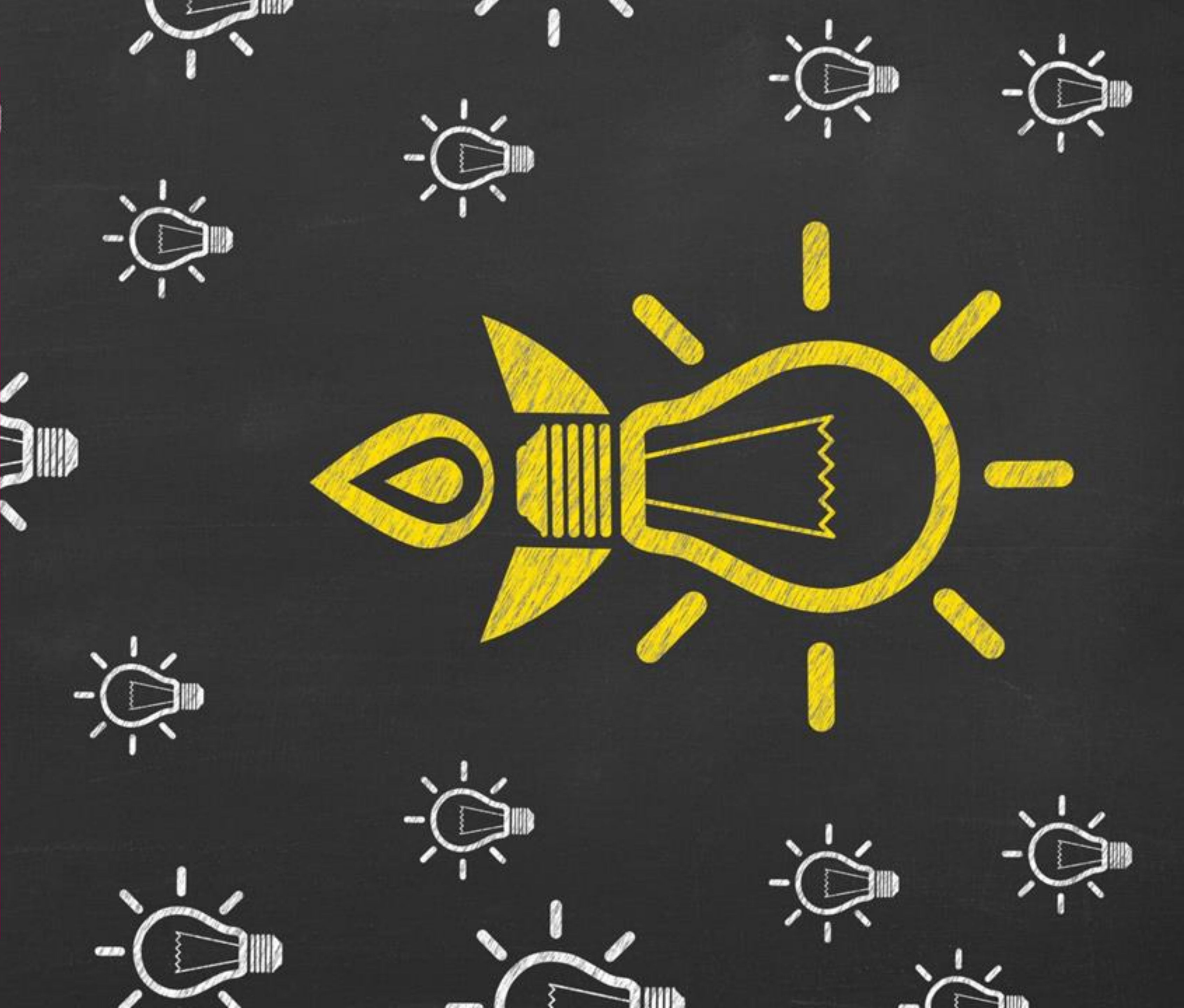
1. All data sources and computing services are considered resources. (DEVICES, APPLICATIONS, DATA)
2. All communication is secured regardless of network location. (NETWORKS)
3. Access to individual enterprise resources is granted on a per-session basis. (USERS, DEVICES, APPLICATIONS, DATA)
4. Access to resources is determined by dynamic policy. (USERS, DEVICES, APPLICATIONS, DATA)
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets. (ALL ASSET CLASSES)
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed. (ALL ASSET CLASSES)
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture. (ALL ASSET CLASSES)



CYBERSECURITY FRAMEWORK	**IDENTIFY**	**PROTECT**	**DETECT**	**RESPOND & RECOVER**	
DEVICES					**DEVICES**
NETWORKS					**NETWORKS**
APPLICATIONS & DATA					**APPLICATIONS & DATA**
IDENTITIES					**IDENTITIES**
ZTMM	**TRADITIONAL**	**INITIAL**	**ADVANCED**	**OPTIMIZED**	



NETWORKS, DATA CENTERS,
ZERO TRUST:
THEN AND NOW



REFERENCE

PHYSICAL LOCATION AND NETWORKS

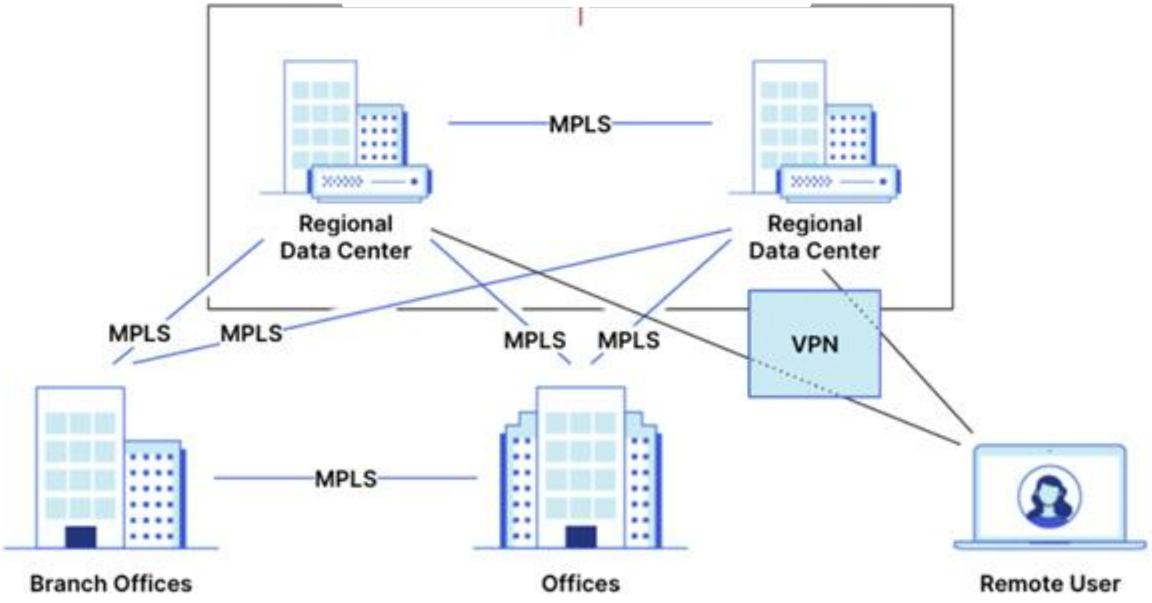
- Internet backbone - Core infrastructure that forms the foundation of the global Internet. It consists of the largest and fastest networks, linked by high-capacity fiber-optic connections and advanced routers and switches.
  - Internet Service Providers (ISPs), content delivery networks, and cloud service providers offer Internet access, applications, and services to businesses and end-users worldwide.
- Public Cloud Network - Networks are managed by cloud hosting provider even when used by CHP's customers
  - Cloud hosting provider is responsible for the entire network stack at the "entry" to the CHP's data center
- Private Network / OnPrem Environment - Networks that are run by an organization whether hosted in their or a 3rd party's data center or within the organization's buildings
  - Organization is responsible for the entire network stack at the "entry" to their data center / environment
- Hybrid (Cloud) Network - Mix of Public & Private
  - Will typically run connectivity between public/private over the Internet
  - "Advanced" organizations may run dedicated connectivity between public, cloud & private environments

NETWORK “EVOLUTION”: THAT WAS THEN

https://www.cloudflare.com/learning/network-layer/enterprise-networking/

THEN:

- Enterprise networks covered office buildings and “on-premise” self-hosted centralized data centers.
- Users/devices were connected via local area networks within the office
  - Pre WiFi, this was Ethernet, TokenRing, etc
- Office LANs were connected to each other with enterprise WAN, usually constructed via dedicated multiprotocol label switching (MPLS) routes.



This “THEN” model of Enterprise network security trusts anyone and anything inside the network

- ➢ Focus was on defending the network perimeter via firewalls, intrusion prevention systems (IPS), and other security products.
- ➢ This was known as CASTLE-AND-MOAT.

NETWORK SEGMENTATION VERSUS VPN

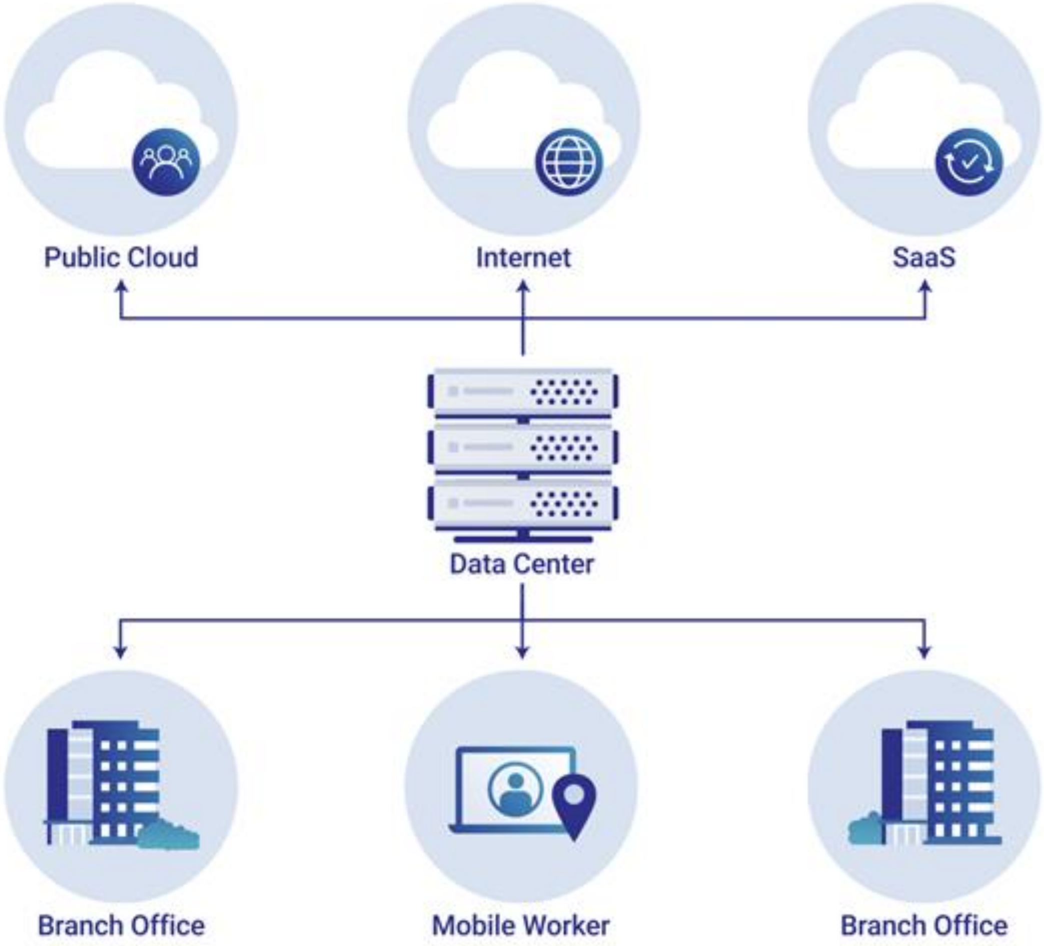
- Key points about network segmentation:
  - **Function:** Divides a network into smaller segments with defined access controls, limiting the spread of potential attacks within the network.
  - **Implementation:** Uses tools like firewalls, VLANs, and subnetting to isolate segments.
  - **Benefits:** Improved security by limiting lateral movement of attackers, better control over data access, and enhanced compliance with regulations.
- Key points about VPNs:
  - **Function:** Creates a secure, encrypted tunnel over a public network to protect data privacy and anonymity when connecting to a remote network.
  - **Implementation:** Uses encryption protocols to protect data transmitted between a user's device and a VPN server.
  - **Benefits:** Secure remote access to internal networks, protection from eavesdropping on public Wi-Fi, masking IP address for privacy.

NETWORK “EVOLUTION”: THIS IS NOW (2019 VERSION)

https://www.cloudflare.com/learning/network-layer/enterprise-networking/

2019 NOW:

- Employees are now likely to connect to the network from both inside and outside the office with WiFi.
  - Enterprise has both cloud and on-premise data centers (a hybrid cloud model)
  - New companies often cloud only / ”cloud native”
- The “2019 NOW” model of Enterprise network security trusts anyone and anything inside the network
  - VPNs used to a) authenticate user’s device (certificate associated with VPN client) b) encrypt traffic in transit
- Zero Trust Security was emerging as “Authenticate user and VPN from the workstation” variety

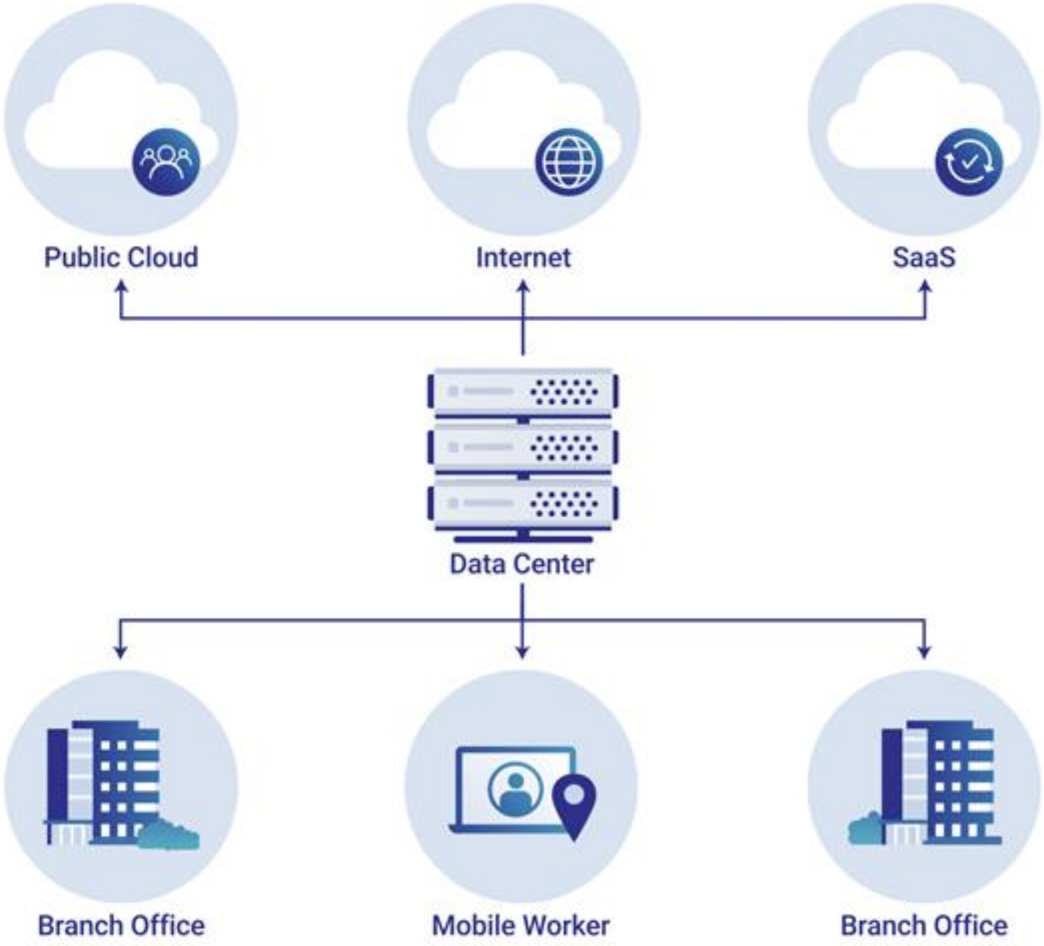


NETWORK “EVOLUTION”: THIS IS NOW (2019 VERSION + ZERO TRUST)

https://www.cloudflare.com/learning/network-layer/enterprise-networking/

2019 EMERGING ZERO TRUST NOW

- VPNs used as the basis of Zero Trust
- Trusted because of the VPN client and password (restricted budget approach) or certificate (flush budget approach)
- However
  - This was easily circumvented, especially password based
  - Did not drive the discipline of network segmentation
- Zero Trust: Early zero trust was all about trusting user + device before granting access to network
- ”Enhanced” VPN clients checked the device
  - Known – MAC address
  - Configured / managed – client on device to enforce
  - Authorized – certificate associated with user
- Still did not drive discipline of network segmentation

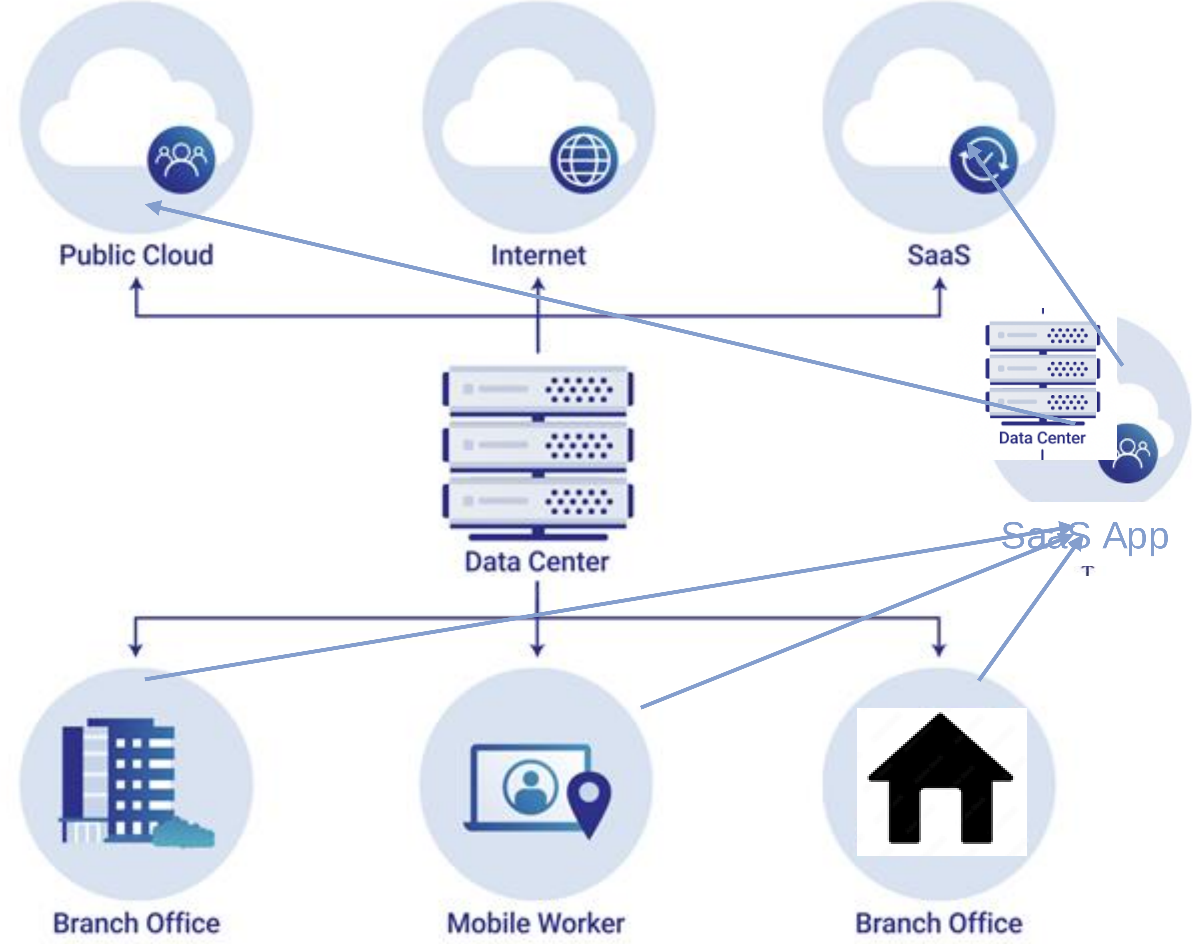


NETWORK “EVOLUTION”: THIS IS 2025

https://www.cloudflare.com/learning/network-layer/enterprise-networking/

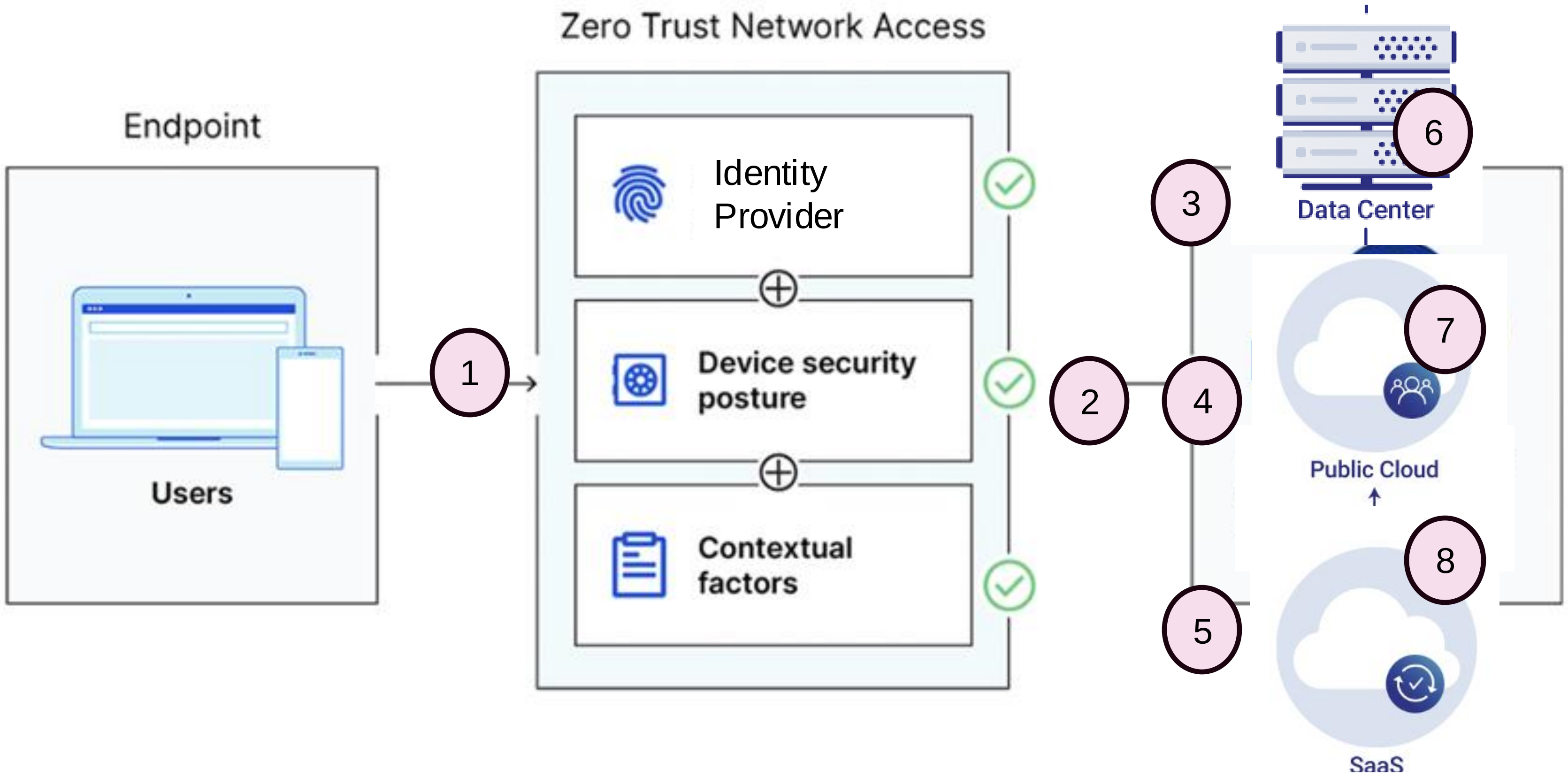
2025 NOW : ADD IN SAAS, CLOUD NATIVE

- SaaS applications do not coexist nicely with VPNs
- Home networks are likely not well protected – or at least not to a common meets-min standard
- “Zero Trust in SaaS Land”:
  - User: Add a proxy that brokers access for authenticated users to authorized (SaaS) applications
  - Devices: Add (other) solutions to check configuration of devices as part of user authentication
- Still did not drive discipline of network segmentation
  - “Segment by SaaS”
  - Network segmentation now relies on data center ownership & shared responsibility model



	Network Segmentation	Network Traffic Management	Traffic Encryption	Network Resilience
Traditional	Agency defines their network architecture using large perimeter/macro- segmentation with minimal restrictions on reachability within network segments. Agency may also rely on multi-service interconnections (e.g., bulk traffic VPN tunnels).	Agency manually implements static network rules and configurations to manage traffic at service provisioning, with limited monitoring capabilities (e.g. application performance monitoring or anomaly detection) and manual audits and reviews of profile changes for mission critical applications.	Agency encrypts minimal traffic and relies on manual or ad hoc processes to manage and secure encryption keys.	Agency configures network capabilities on a case-by- case basis to only match individual application availability demands with limited resilience mechanisms for workloads not deemed mission critical.
Initial	Agency begins to deploy network architecture with the isolation of critical workloads, constraining connectivity to least function principles, and a transition toward service-specific interconnections.	Agency establishes application profiles with distinct traffic management features and begins to map all applications to these profiles. Agency expands application of static rules to all applications and performs periodic manual audits of application profile assessments.	Agency begins to encrypt all traffic to internal applications, to prefer encryption for traffic to external applications, to formalize key management policies, and to secure server/service encryption keys.	Agency begins to configure network capabilities to manage availability demands for additional applications and expand resilience mechanisms for workloads not deemed mission critical.
Advanced	Agency expands deployment of endpoint and application profile isolation mechanisms to more of their network architecture with ingress/egress micro-perimeters and service- specific interconnections.	Agency implements dynamic network rules and configurations for resource optimization that are periodically adapted based upon automated risk-aware and risk-responsive application profile assessments and monitoring	Agency ensures encryption for all applicable internal and external traffic protocols, manages issuance and rotation of keys and certificates, and begins to incorporate best practices for cryptographic agility.	Agency has configured network capabilities to dynamically manage the availability demands and resilience mechanisms for the majority of their applications.
Optimal	Agency network architecture consists of fully distributed ingress/egress micro-perimeters and extensive micro-segmentation based around application profiles with dynamic just-in-time and just-enough connectivity for service-specific interconnections.	Agency implements dynamic network rules and configurations that continuously evolve to meet application profile needs and reprioritize applications based on mission criticality, risk, etc.	Agency continues to encrypt traffic as appropriate, enforces least privilege principles for secure key management enterprise-wide and incorporates best practices for cryptographic agility as widely as possible.	Agency integrates holistic delivery and awareness in adapting to changes in availability demands for all workloads and provides proportionate resilience.

"ZERO TRUST NETWORK"



Network

1. From User to "ZTNA" tool
    1. Note probably a SaaS tool
2. To Internet accessible stuff
    1. Includes 3-5 and cat photos+
3. To Org's Data Centers
4. To Org's Public Cloud Content
5. To Org's SaaS Providers
6. Within Org's Data Centers
7. Within Org's Public Cloud Env
8. Within Org's SaaS Provider's Environments

POLL PROMPT PART

POLL

1. *Using the previous slide, which are the most critical network segments for your org*
   1. *User to (SaaS) ZTNA tools*
   2. *ZTNA tools to Network/Internet*
   3. *Network to Data Centers/Public Cloud/SaaS providers*
   4. *Networks within (3's) environments*
2. *If you had a magic wand, and could ensure Advanced Maturity for one of the categories for ALL of the above, which would you choose (and in breakouts, why?)*
   1. *Network Segmentation*
   2. *Traffic Management*
   3. *Traffic Encryption*
   4. *Network Resilience*

BREAKOUT DISCUSSION: PRIORITIZIATION

BO

- *What did you pick, and why?*
- *What did you assume about your environment and your business priorities when making these decisions?*
- *Would your decision have changed if the magic wand moved you to OPTIMAL? What about Initial?*
- *Assume that the class majority choice (fill in the blank during class) is going to cost you 5x as much to implement than choice #2 (fill in the blank during class), does that change your point of view? Why or why not?*

CLASS REFLECTIONS ON BREAKOUT

- *What, if anything, surprised you during your breakout discussions?*
- *Did any of the discussions change your mind?*
- *How does your discussion support the following quote from the CISA ZTMM:*
  - *Each pillar can progress at its own pace and may progress more quickly than others until cross-pillar coordination is required.*
  - *However, this coordination can only be achieved with capabilities and dependencies compatible with one another and the enterprise-wide environment*

CANVAS DISCUSSION: PRIORITIZIATION

CANVAS

- *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 6:10
PM ET

INDUSTRIAL CONTROLS SYSTEMS AND NETWORKS

INDUSTRIAL CONTROL SYSTEMS (ICS) / OPERATIONS TECH (OT) https://gca.isa.org/blog/common-ics-cybersecurity-myth-1-the-air-gap

- ICS : Industrial Control Systems (also know as operations technology or OT).
  - Generic term used to describe various control systems and their instrumentation.
- ICS are used for controlling and monitoring industrial processes
  - Monitor remote sensors
  - Send commands to (OT) machinery / devices
- ICS systems integrate hardware, software, and network connectivity
- ICS systems run and support critical infrastructure (such as electricity, gas, water, and so on)
- ICS have been built with a primary focus on safety, reliability, and availability, with physical gates and locks used as primary protection mechanisms.
- Because ICS were not viewed as a cybersecurity target, many organizations believe that approaches such the air gap and proprietary ICS protocols provide sufficient defense against cybersecurity attack
- Operations technology (OT) has moved from ICS world to "your world"
  - OT includes your Wifi connected doorbell, camera, washing machine, thermostat, etc etc

NETWORK PROTOCOLS & ICS
https://gca.isa.org/blog/common-ics-cybersecurity-myth-4-serial-communication

- Serially connected industrial sites or substations have multiple networks for operations:
  - A serial network (eg RS232) to the control center (not routable, not Ethernet/TCP/IP)
  - A local IP/Ethernet network for plant/substation OT communications.
  - (Not uncommon) IP network for corporate purposes, such as email, web browsing, and so on.
- Not uncommon to have
  - “Bridging points” where one network device deals with both IP and serial (i.e. serial-to-IP converters) or
  - A firewall that segregates OT and corporate networks.
- Further, industrial sites may depend on remote management protocols (RDP, SSH)

RS 232

https://www.linkedin.com/pulse/deactivating-rs-232-rs-485-ports-industrial-cyber-security-augusto-rucfc/

- PROTOCOL/ENCRYPTION: RS-232 and RS-485 protocols do not have built-in encryption and authentication mechanisms.
  - → This makes them susceptible to eavesdropping and data tampering
- SEGMENTATION: Industrial devices installed in accessible locations within a controlled environment
  - The RS-232 / RS-485 ports available to anyone with physical access.

MYTH: ICS SYSTEMS ARE AIR GAPPED (AND THEREFORE SECURE)

- Air gaps between the ICS network and other networks—if implemented correctly and maintained—are very effective barriers against cyberattacks. However, a true air gap is **no longer practical in an interconnected world**.
- ICS: Even in an air-gapped ICS network, there are many business reasons for files and data to be moved between the ICS and outside networks. Some examples include configuration files, software patches, and files from vendors such as system integrators or contractors.
- OT: Every single device in your home that needs access to WiFi (from your doorbell, to your thermostat, washing machine, etc) is (almost certainly) accessible from the Internet

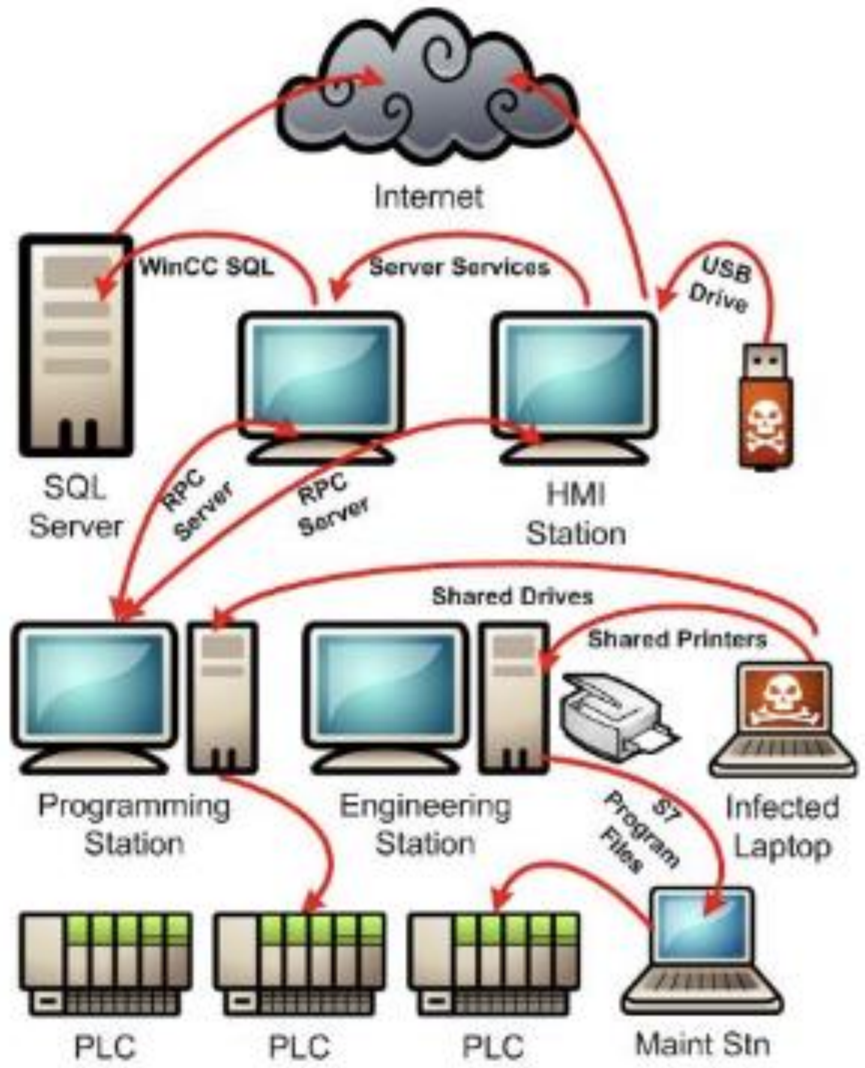
IN THE NEWS: BREAKING INDUSTRIAL CONTROL SYSTEMS

BREAKING THE AIRGAP: EXAMPLES
https://attack.mitre.org/campaigns/

- It all starts with access to the network:
  - The victim’s corporate network and then laterally move to the ICS network
  - The victim’s ICS control systems/network and then laterally move to the ICS / OT systems
  - A suppliers’ systems, introduce malware/backdoors included in updates to ICS systems
- Goal: Access the network to then upload malware to the ICS / OT systems

STUXNET

- Makes use of a previously unpatched Windows vulnerability and a digitally signed kernel-mode rootkit.
- There have been two digital certificates used to sign this rootkit.
  - The original and second variant certificate have been revoked.



OTHER PLC ATTACKS

- **Duqu (2011)**. Based on Stuxnet code, Duqu was designed to log keystrokes and mine data from industrial facilities, presumably to launch a later attack.
- **Flame (2012)**. Flame, like Stuxnet, traveled via USB stick. Flame was sophisticated spyware that recorded Skype conversations, logged keystrokes, and gathered screenshots, among other activities. It targeted government and educational organizations and some private individuals mostly in Iran and other Middle Eastern countries.
- **Havex (2013)**. The intention of Havex was to gather information from energy, aviation, defense, and pharmaceutical companies, among others. Havex malware targeted mainly U.S., European, and Canadian organizations.
- **Industroyer (2016)**. This targeted power facilities. It's credited with causing a power outage in the Ukraine in December 2016.
- **Triton (2017)**. This targeted the safety systems of a petrochemical plant in the Middle East, raising concerns about the malware maker's intent to cause physical injury to workers.
- **Most recent (2018)**. An unnamed virus with characteristics of Stuxnet reportedly struck unspecified network infrastructure in Iran in October 2018.

CISA ON STUXNET

https://www.cisa.gov/news-events/ics-advisories/icsa-10-238-01b

Last revised January 08, 2014

- According to reports and analysis, Stuxnet uses a total of five vulnerabilities;
  - One previously patched (MS08-067) and
  - Four (4) zero-days.
- Two of the four zero-day vulnerabilities have been patched since Stuxnet's discovery.
  - The first zero-day was addressed in MS10-046b on August 24th, 2010.
  - The second zero-day was addressed in MS10-061c: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290), released on Sept 14th, 2010.
  - According to Microsoft, "This vulnerability in the Print Spooler Service is rated Critical for Windows XP and Important on all other affected platforms and is used by Stuxnet to spread to systems inside the network where the Print Spooler service is exposed without authentication."
- The other two vulnerabilities are local escalation of privilege vulnerabilities that enable an attacker to gain full control of an affected system.
  - One the vulnerabilities affects Windows XP and
  - The other affects Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2.

STUXNET

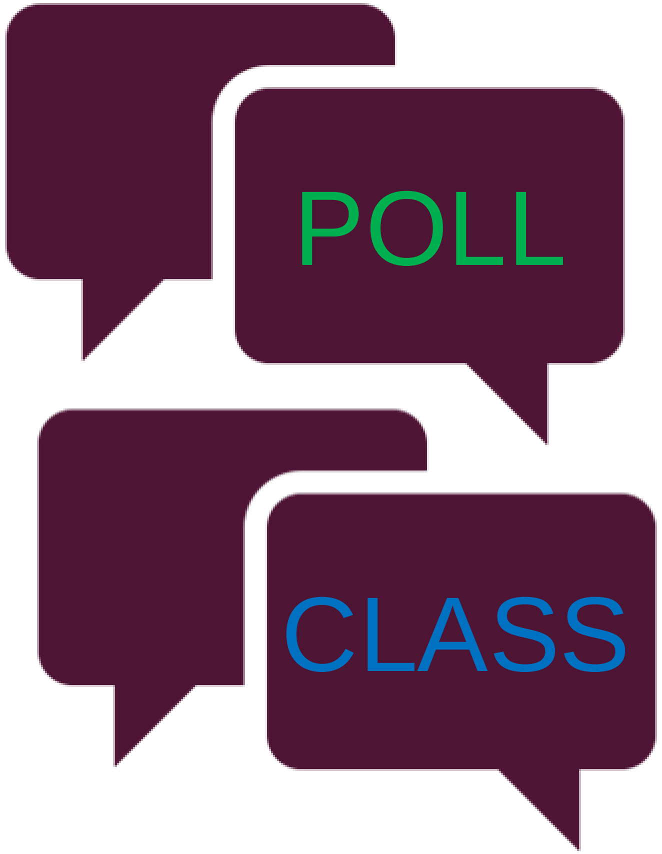
https://www.trellix.com/security-awareness/ransomware/what-is-stuxnet/

https://www.cyberark.com/resources/stream-embed-for-securing-iot-and-ot/the-three-phases-of-iot-and-

- Trellix Guidance
  - Separate the industrial networks from general business networks with firewalls and a demilitarized zone (DMZ)
  - Closely monitor machines that automate industrial processes
  - Use application whitelisting
  - Monitor and log all activities on the network
  - Implement strong physical security for access to industrial networks, including card readers and surveillance cameras

- CyberArk ICS Security Best Practices
  - #1. Secure Physical Access.
  - #2. Create an ICS Asset Inventory.
  - #3. Develop a Network Baseline.
  - #4. Segment ICS Networks.
  - #5. Implement Least Privilege.
  - #6. Use IPS To Identify Known Threats.
  - #7. Secure Remote Access to ICS Devices.

DISCUSSION



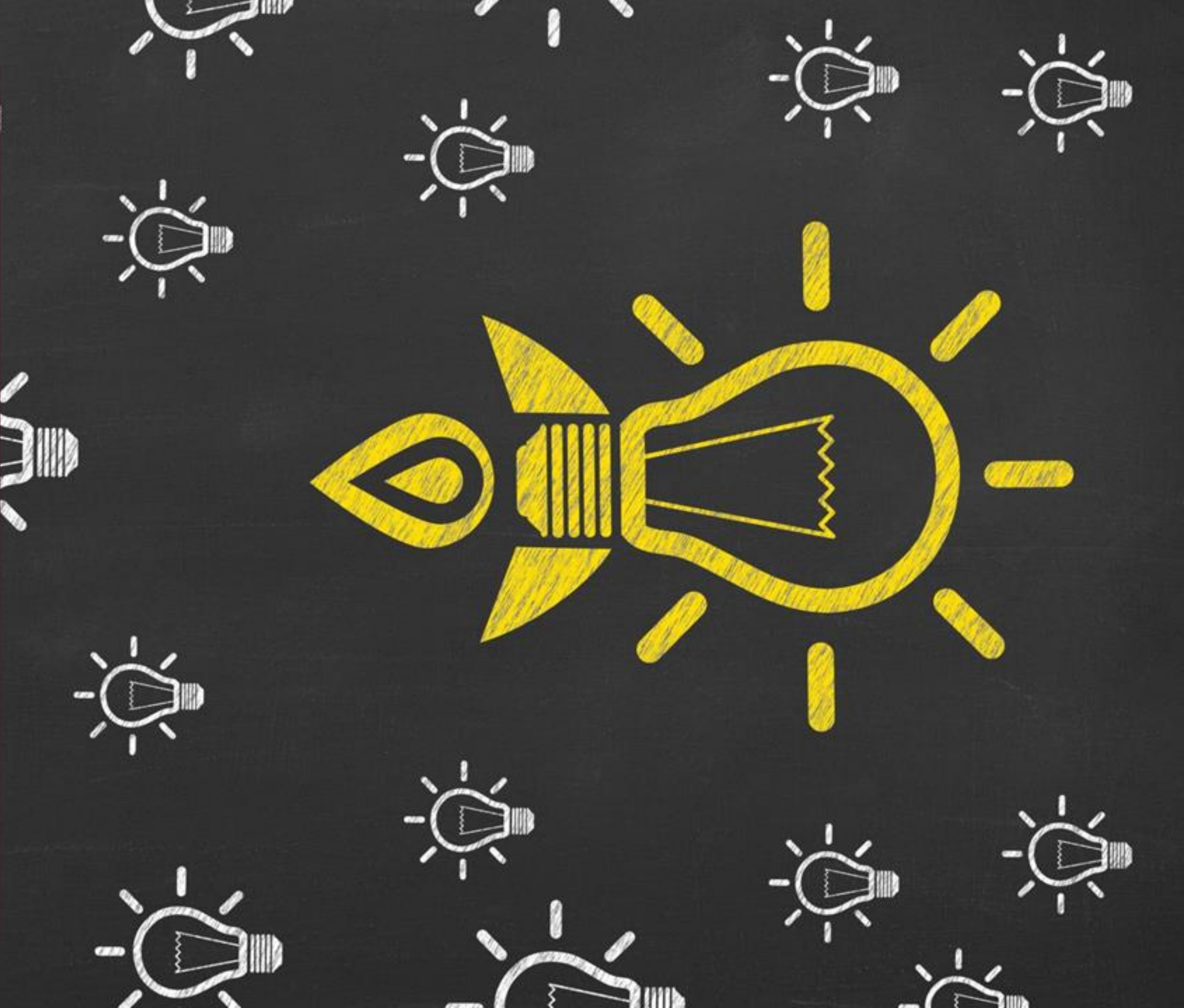
- *POLL*
- *Which "list" for protecting Industrial Control Systems do you think is more actionable and accurate:*
  - *Trellix*
  - *CyberArk*

- *CLASS DISCUSSION*
  - *Why?*

AIR GAPPED SYSTEMS ARE NOT REALLY AIRGAPPED
https://gca.isa.org/blog/common-ics-cybersecurity-myth-1-the-air-gap

- *In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network. On average, we see 11 direct connections between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network.*
  - *Sean McGurk, Former Director, NCCIC, the Department of Homeland Security*

ZERO TRUST NETWORK MATURITY MODEL



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.

ZTA Focus	Network Segmentation	Network Traffic Management	Traffic Encryption	Network Resilience
Desc	Segments / subnets with controlled access to move from flat to segmented network	Monitor traffic to track and analyse data flowing across a network; identify potential issues, understand usage patterns, and optimize performance	Point to point, End to end with robust key management	System designed to withstand disruptions, recover quickly from failures, and maintain operational continuity even during unexpected events
Maturity Goal	Moving from perimeter-internal to "segments" that allow isolation of workloads in progressively more restrictive segments	Move from manual management of static rules and configurations to automation and dynamic rules and configurations including dynamically responding to new/emerging threats	Moving from minimal to comprehensive encryption of traffic including mutual authentication of parties as part of encryption	Move from limited resilience of networks to fully redundant and always available networks
Tools	Firewalls , VPNs, IPTables	Segmentation tools, network monitoring tools	P2P with segmentation tools E2E with applications / "endpoints"	CDN, Redundance network paths
In the News	Ivanti, Fortinet, Nobelium Stuxnet, Ukranian Utilities	SolarWinds	Mitre T1040	Volumetric DDOS

Zero Trust Maturity Model: Cross Cutting Capabilities

	Traditional	Initial	Advanced	Optimal
Visibility and Analytics Capability	Agency manually collects limited logs across their enterprise with low fidelity and minimal analysis.	Agency begins to automate the collection and analysis of logs and events for mission critical functions and regularly assesses processes for gaps in visibility.	Agency expands the automated collection of logs and events enterprise-wide (including virtual environments) for centralized analysis that correlates across multiple sources.	Agency maintains comprehensive visibility enterprise-wide via centralized dynamic monitoring and advanced analysis of logs and events.
Automation and Orchestration Capability	Agency relies on static and manual processes to orchestrate operations and response activities with limited automation.	Agency begins automating orchestration and response activities in support of critical mission functions.	Agency automates orchestration and response activities enterprise-wide, leveraging contextual information from multiple sources to inform decisions.	Agency orchestration and response activities dynamically respond to enterprise-wide changing requirements and environmental changes.
Governance Capability	Agency implements policies in an ad hoc manner across the enterprise, with policies enforced via manual processes or static technical mechanisms.	Agency defines and begins implementing policies for enterprise-wide enforcement with minimal automation and manual updates.	Agency implements tiered, tailored policies enterprise- wide and leverages automation where possible to support enforcement. Access policy decisions incorporate contextual information from multiple sources.	Agency implements and fully automates enterprise-wide policies that enable tailored local controls with continuous enforcement and dynamic updates.

Network Segmentation Maturity Model

Traditional	Initial	Advanced	Optimal
Agency defines their network architecture using large perimeter/macro segmentation with minimal restrictions on reachability within network segments. Agency may also rely on multi-service interconnections (e.g., bulk traffic VPN tunnels).	Agency begins to deploy network architecture with the isolation of critical workloads, constraining connectivity to least function principles, and a transition toward service-specific interconnections.	Agency expands deployment of endpoint and application profile isolation mechanisms to more of their network architecture with ingress/egress micro-perimeters and service specific interconnections.	Agency network architecture consists of fully distributed ingress/egress micro-perimeters and extensive micro-segmentation based around application profiles with dynamic just-in-time and just-enough connectivity for service-specific interconnections

Traffic Management Maturity Model

Traditional	Initial	Advanced	Optimal
Agency manually implements static network rules and configurations to manage traffic at service provisioning, with limited monitoring capabilities (e.g., application performance monitoring or anomaly detection) and manual audits and reviews of profile changes for mission critical applications.	Agency establishes application profiles with distinct traffic management features and begins to map all applications to these profiles. Agency expands application of static rules to all applications and performs periodic manual audits of application profile assessments.	Agency implements dynamic network rules and configurations for resource optimization that are periodically adapted based upon automated risk-aware and risk-responsive application profile assessments and monitoring.	Agency implements dynamic network rules and configurations that continuously evolve to meet application profile needs and reprioritize applications based on mission criticality, risk, etc.

Traffic Encryption Maturity Model

Traditional	Initial	Advanced	Optimal
Agency encrypts minimal traffic and relies on manual or ad hoc processes to manage and secure encryption keys.	Agency begins to encrypt all traffic to internal applications, to prefer encryption for traffic to external applications, to formalize key management policies, and to secure server/service encryption keys.	Agency ensures encryption for all applicable internal and external traffic protocols, manages issuance and rotation of keys and certificates and begins to incorporate best practices for cryptographic agility.	Agency continues to encrypt traffic as appropriate, enforces least privilege principles for secure key management enterprise wide, and incorporates best practices for cryptographic agility as widely as possible.

Network Resilience Maturity Model

Traditional	Initial	Advanced	Optimal
Agency configures network capabilities on a case-by-case basis to only match individual application availability demands with limited resilience mechanisms for workloads not deemed mission critical.	Agency begins to configure network capabilities to manage availability demands for additional applications and expand resilience mechanisms for workloads not deemed mission critical.	Agency has configured network capabilities to dynamically manage the availability demands and resilience mechanisms for the majority of their applications.	Agency integrates holistic delivery and awareness in adapting to changes in availability demands for all workloads and provides proportionate resilience.

NETWORK SECURITY “STRATEGIES” - ”SASE”

- SASE: Secure Access Service Edge
  - Not to be confused with SSE, Secure Secure Edge…
- SASE can be broken down into six essential elements in terms of its capabilities and technologies:
  - Software-Defined Wide Area Network (SD-WAN)
  - Secure Web Gateway (SWG)
  - Cloud Access Security Broker (CASB)
  - Firewall as a Service (FWaaS)
  - Zero Trust Network Access (ZTNA)
  - Centralized Management
- AND: Where do strategies such as single sign-on, 2FA/MFA fit into this from a vendor pov?

ZTNA VERSUS VPN

- Virtual private networks (VPNs) are what many organizations use to control access instead of Zero Trust Network Architecture (ZTNA).
- Technical differences between ZTNA and VPNs include:
- OSI model layer:
  - Most VPNs run on the IPsec protocol at layer 3, the network layer; some VPNs do run on the application layer using TLS protocol
  - ZTNA typically operates on the application layer using TLS
- Endpoint software installation:
  - IPsec VPNs require the installation of software on all user devices.
  - ZTNA does not always require software installation on user devices
- Hardware:
  - VPNs often require the use of on-premise VPN servers, with user devices connectivity through their organization’s perimeter firewall to these servers.
  - ZTNA is typically delivered through the cloud, enabling users to connect from anywhere without impacting network performance.
- Level of connectivity:
  - ZTNA sets up one-to-one encrypted connections between a user's device and a given application or server.
  - VPNs give users encrypted access to an entire LAN all at once. If a user's IP address connects with the network, it can connect with all IP addresses on that network.

ADDITIONAL MATERIAL FOR GENERAL EDIFICATION

TO BE DISCUSSED TOWARDS END OF THE COURSE
RED TEAM AI (BY MICROSOFT)

https://airedteamwhitepapers.blob.core.windows.net/lessonswhitepaper/MS_AIRT_Lessons_eBook.pdf

1. Understand what the system can do and where it is applied.
2. You don’t have to compute gradients to break an AI system.
3. AI red teaming is not safety benchmarking.
4. Automation can help cover more of the risk landscape.
5. The human element of AI red teaming is crucial.
6. Responsible AI harms are pervasive but difficult to measure.
7. LLMs amplify existing security risks and introduce new ones.
8. The work of securing AI systems will never be complete.

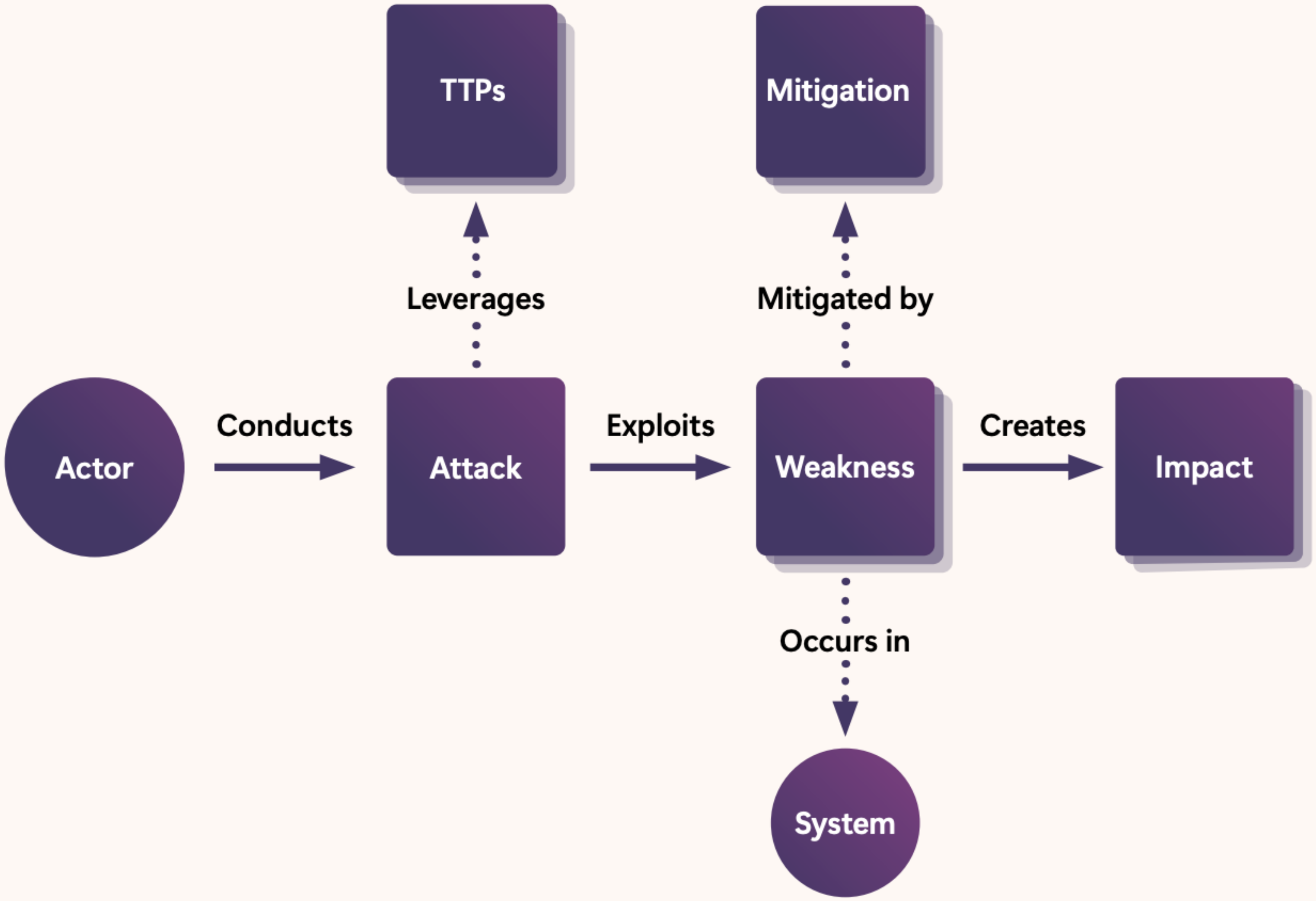


Figure 1: Microsoft AIRT ontology for modeling GenAI system vulnerabilities. AIRT often leverages multiple TTPs, which may exploit multiple Weaknesses and create multiple Impacts. In addition, more than one Mitigation may be necessary to address a Weakness. Note that AIRT is tasked only with identifying risks, while product teams are resourced to develop appropriate mitigations.

IN THE NEWS:
NOBELIUM (JAN 2024)

MICROSOFT’S EXPLOITATION BY NOBELIUM

https://www.cybersecuritydive.com/news/midnight-blizzard-hack-microsoft-security/705416/

https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/

This time last year, Microsoft disclosed a hack by Midnight Blizzard, the Russia-affiliated threat actor formerly known as Nobelium. The group stole email and other documents from key Microsoft executives through a password spray attack dating back to late November.

The hackers compromised a legacy, non-production test tenant account and the attack was not discovered until Jan. 12, according to Microsoft.

“If the same team were to deploy the legacy t]enant today, mandatory Microsoft policy and workflows would ensure [multifactor authention] and our active protections are enabled to comply with current policies and guidance]

NOBELIUM

https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/

- Initial access through password spray
  - Successfully compromised a legacy, non-production test tenant account that did not have multifactor authentication (MFA) enabled
- Malicious use of OAuth applications
  - Compromise user accounts to create, modify, and grant high permissions to OAuth applications that they can misuse to hide malicious activity.
- Collection via Exchange Web Services
  - leveraged these malicious OAuth applications to authenticate to Microsoft Exchange Online and target Microsoft corporate email accounts.
- Use of residential proxy infrastructure
  - Used residential proxy networks, routing their traffic through a vast number of IP addresses that are also used by legitimate users to obfuscate connections makes traditional indicators of compromise (IOC)-based detection infeasible due to the high changeover rate of IP addresses.

NOBELIUM: MSFT DEFENSE AND PROTECTION GUIDANCE

- Due to the heavy use of proxy infrastructure with a high changeover rate, searching for traditional IOCs, such as infrastructure IP addresses (NETWORK TRAFFIC MANAGEMENT), is not sufficient to detect this type of Midnight Blizzard activity. Instead, Microsoft recommends the following guidance to detect and help reduce the risk of this type of threat:
- Defend against malicious OAuth applications
  - Audit the current privilege level of all identities, users, service principals, and applications
  - Audit identities that hold *elevated* privileges in critical apps (eg Exchange Online)
  - Identify malicious OAuth apps using anomaly detection policies.
  - Implement conditional access app control for users connecting from unmanaged devices
- Protect against password spray attacks
  - Lots of deets…

LATERAL MOVEMENT: NCSC https://www.ncsc.gov.uk/guidance/preventing-lateral-movement

- Applying the following protections will buy time and make it easier to detect attempts at lateral movement.
  - 1. Protect credentials
  - 2. Deploy good authentication practices
  - 3. Protect high privilege accounts
  - 4. Apply the principle of least privilege
  - 5. Lock down devices
  - 6. Segregate networks as sets
  - 7. Monitor networks
  - 8. Consider using honeypots
- Also recommended: https://www.ncsc.gov.uk/collection/10-steps/architecture-and-configuration

POLL PROMPT PART

POLL

- *Given the high-level description of Nobelium attack by MSFT including*
- *"its use of proxy infrastructure with a high changeover rate, searching for traditional IOCs, such as infrastructure IP addresses (NETWORK TRAFFIC MANAGEMENT) is not sufficient to detect this type of activity"*
- *And fact that MFA doesn't "work" for non-interactive (Oauth) enabled environments (NETWORK SEGMENTATION),*
- *Is network segmentation just a breaking up of the crunchy exterior / squishy interior into smaller and smaller chunks? (Is it really worth it)?*

NETWORK TRAFFIC MANAGEMENT

https://blog.netwrix.com/2023/12/27/network-monitoring-tools/

- Network monitoring tools includes
- Performance monitoring
  - Analyze real-time and historical metrics, such as bandwidth utilization, packet loss, latency and response times, to ensure the network runs at its optimal level.
  - SNMP alerts, event logs, syslog triggers, flow-based monitoring, packet capture analysis and streaming telemetry.
- Availability monitoring
  - Ensure network resources, infrastructure up-and-running
  - ICMP pings to all critical network devices and servers
- Traffic monitoring
  - Network traffic monitor software analyzes the flow of data across the network
- Security monitoring
  - Monitor all the logs

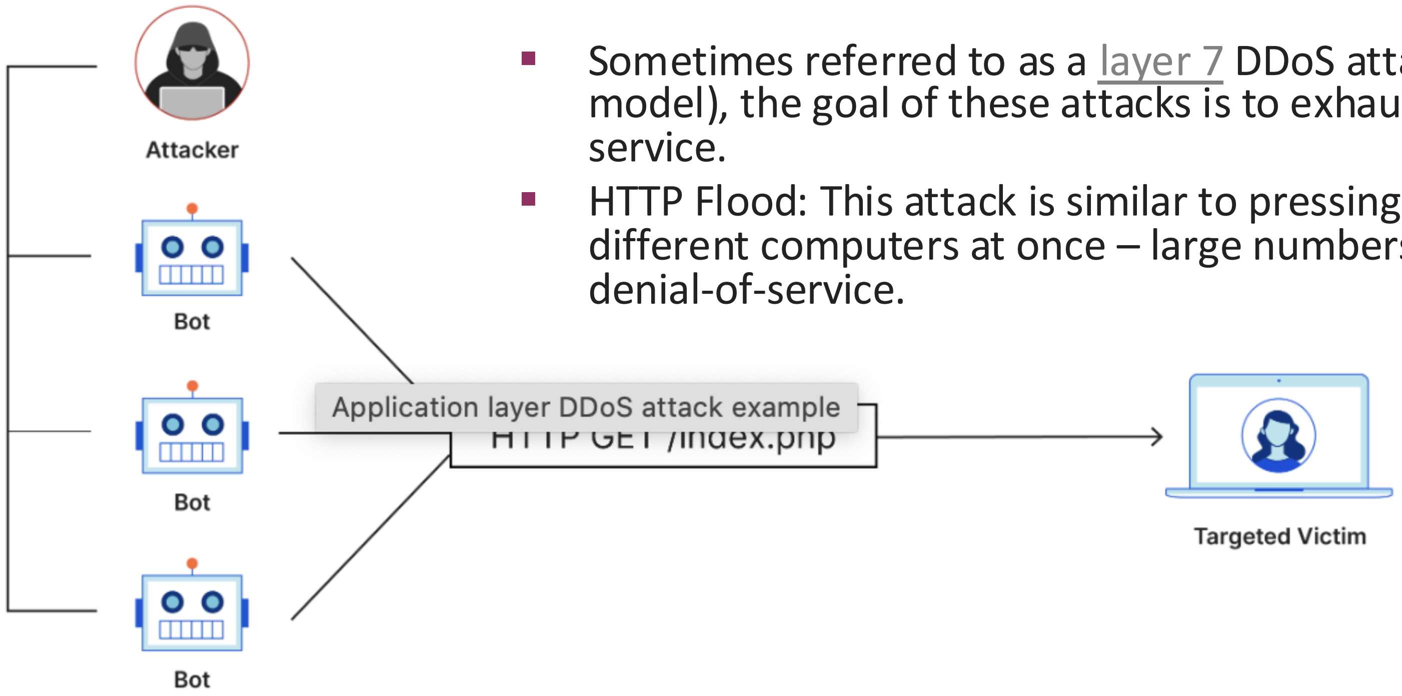
NETWORK / SERVICE MESH
https://aws.amazon.com/what-is/service-mesh/

- In server/virtual machine environments, encryption between servers is possible (annoying, complicated, but possible) by enabling SSL/TLS between all the devices
  - The biggest headache is managing the TLS certificates, including rollover prior to expiration or on demand
- This approach doesn't scale to K8S/micro services environments
- Enter the service mesh
  - To manage connections between services, a service mesh provides new features like monitoring, logging, tracing, and traffic control. It's independent of each service's code, which allows it to work across network boundaries and with multiple service management systems.
- Service mesh offer advanced traffic management features,
  - Comprehensive monitoring and observability features to gain insights into your services' health, performance, and behavior.
  - Traffic splitting (supports the Blue/Green production environment rollover)
  - Duplicate traffic to a test or monitoring service for analysis
  - Direct a small subset of users or traffic to a new service version to confirm behavior and performance
  - Secure communication features such as mutual TLS (mTLS) encryption, authentication, and authorization.

IN THE NEWS: NETWORK TRAFFIC MANAGEMENT, NETWORK RESILIENCE
DDOS WITH HTTP/2 RAPID RESET

APPLICATION LAYER DDOS ATTACKS
https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

- Sometimes referred to as a layer 7 DDoS attack (in reference to the 7th layer of the OSI model), the goal of these attacks is to exhaust the target's resources to create a denial-of-service.
- HTTP Flood: This attack is similar to pressing refresh in a web browser over and over on many different computers at once – large numbers of HTTP requests flood the server, resulting in denial-of-service.

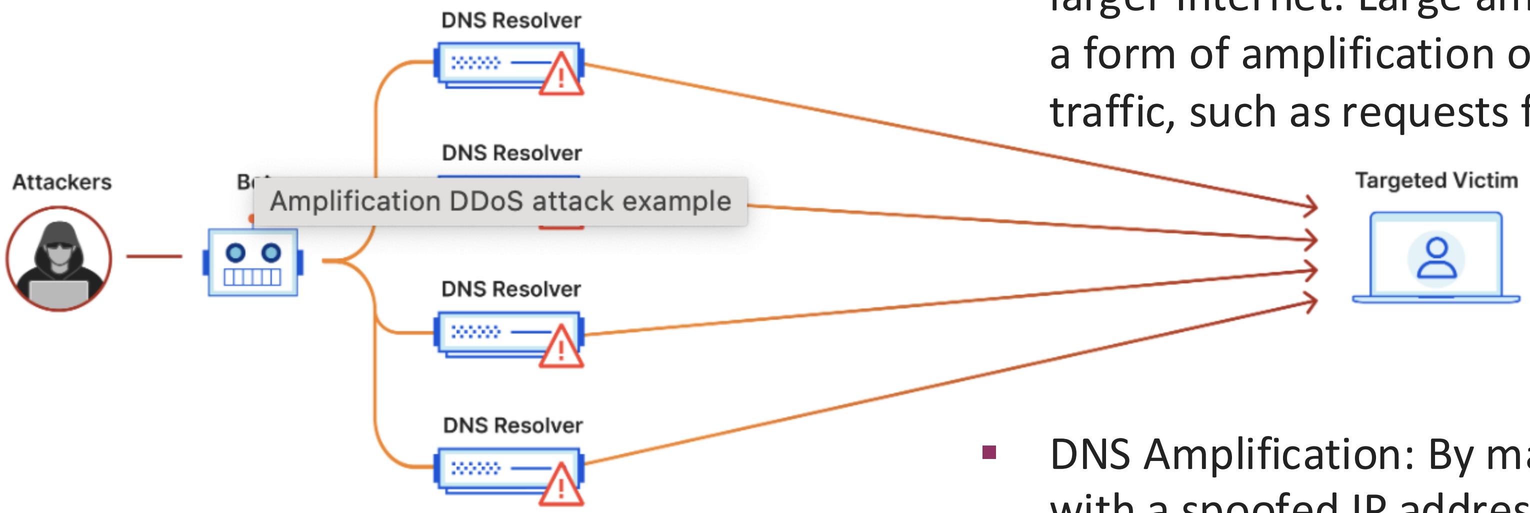


LAYER 3, 4 (PROTOCOL ATTACKS)

- Protocol attacks, also known as a state-exhaustion attacks, cause a service disruption by over-consuming server resources and/or the resources of network equipment like firewalls and load balancers.
- Protocol attacks utilize weaknesses in layer 3 and layer 4 of the protocol stack to render the target inaccessible.
- SYN Flood: This attack exploits the TCP handshake by sending a target a large number of TCP “Initial Connection Request” SYN packets with spoofed source IP addresses.
- The target machine responds to each connection request and then waits for the final step in the handshake, which never occurs, exhausting the target’s resources in the process.

VOLUMETRIC ATTACKS

- This category of attacks attempts to create congestion by consuming all available bandwidth between the target and the larger Internet. Large amounts of data are sent to a target by using a form of amplification or another means of creating massive traffic, such as requests from a botnet.



Amplification DDoS attack example

- DNS Amplification: By making a request to an open DNS server with a spoofed IP address (the IP address of the victim), the target IP address then receives a response from the server.

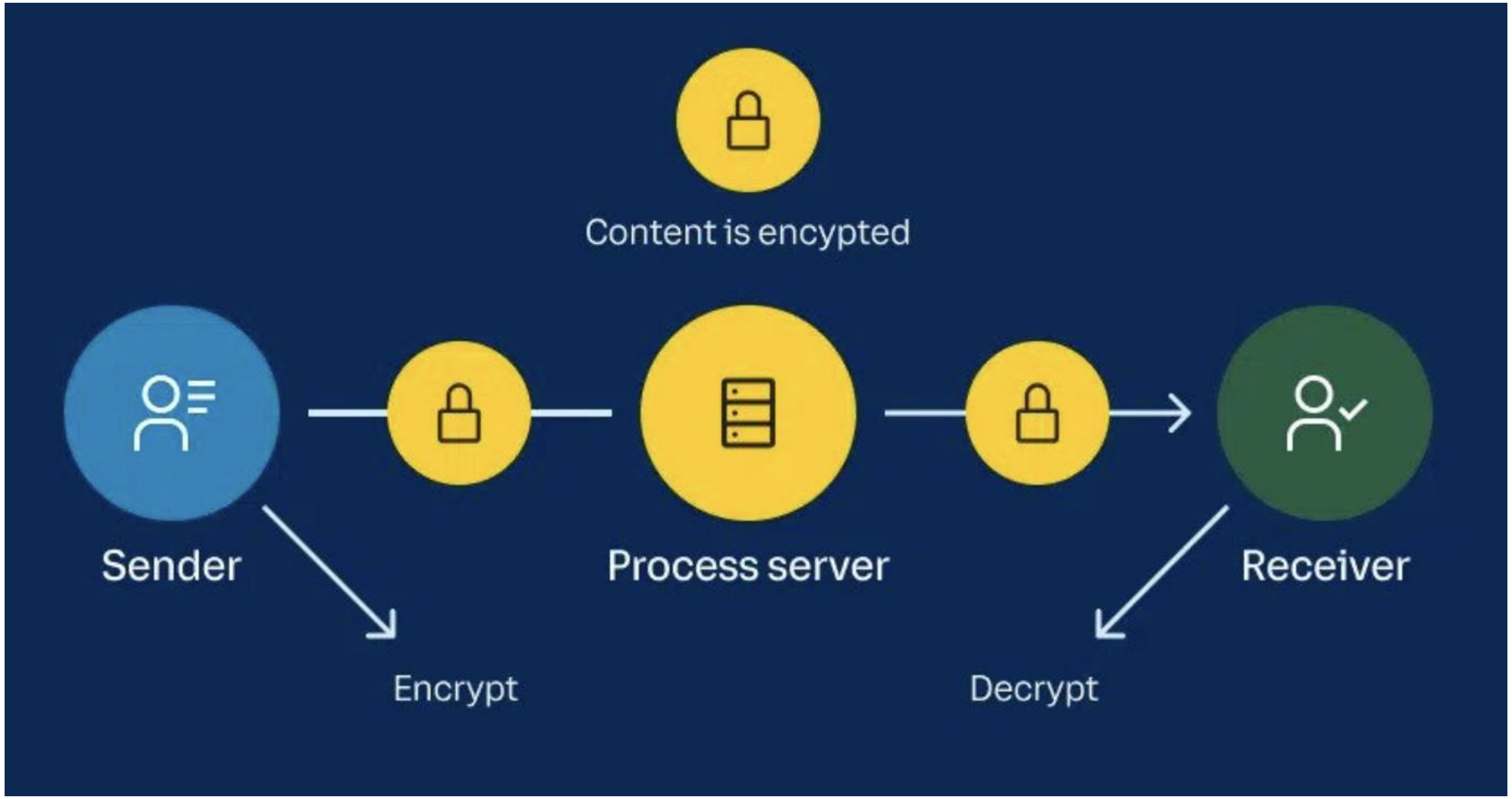
DDOS WITH NETWORK PROTOCOLS VULNERABILITY

https://cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack

- https://nvd.nist.gov/vuln/detail/CVE-2023-44487
- A novel HTTP/2-based DDoS attack peaked in August 2023.
  - These attacks were significantly larger than any previously-reported Layer 7 attacks, with the largest attack surpassing 398 million requests per second.
- One of the main constraints when mounting a Layer 7 DoS attack is the number of concurrent transport connections.
  - In HTTP/1.1, each request is processed serially. The server will read a request, process it, write a response, and only then read and process the next request.
  - With HTTP/2, the client can open multiple concurrent streams on a single TCP connection, each stream corresponding to one HTTP request.
- This attack is called Rapid Reset because it relies on the ability for an endpoint to send a RST_STREAM frame immediately after sending a request frame → this makes the other endpoint start working and then rapidly resets the request. The request is canceled, but the HTTP/2 connection is left open, leading to resource exhaustion

IN THE NEWS: TRAFFIC ENCRYPTION VIDEO MEETINGS, SMS

TRAFFIC ENCRYPTION



- Point to Point versus
- End to End

ZOOM E2E ENCRYPTION

- Zoom is the lack of true end-to-end encryption (E2EE).
- While Zoom does encrypt data during transmission,
  - Meeting content must be accessible by Zoom or third parties depending on features desired
  - Transcription, translation, notes, etc all require Zoom (or the appropriate third party) to have access to the content

ENCRYPTING TEXT MESSAGES

https://www.npr.org/2024/12/17/nx-s1-5223490/text-messaging-security-fbi-chinese-hackers-security-encryption

- In full end-to-end encryption, tech companies make a message decipherable only by its sender and receiver — not by anyone else, including the company. It has been the default on WhatsApp, for instance, since 2016. Along with a promise of greater security, it makes companies "warrant-proof" from surveillance efforts.
- The good news for people who use Apple phones is that iMessage and FaceTime are also already end-to-end encrypted, says Hong. For Android phones, encryption is available in Google Messages if the senders and recipients all have the feature turned on.
- SEE ALSO https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf

ANTICIPATED END OF LECTURE 2
MOVING TO YELLOWDIG, ASSIGNMENTS

YELLOW DIG LAST WEEK

YELLOW DIG LAST WEEK

- Would you say that the the IoT security environment struggles to keep up with the threat environment because of new vulnerabilities in software or because the existing frameworks we have not are not working? I believe the quote is in reference to the latter and while creative new security threats arrive every day, the frameworks made to respond to them are still effective.
-

CYBERSECURITY AS COST V STRATEGIC INVESTMENT

- I think simply viewing cybersecurity as a cost rather than a strategic investment misses the larger picture - and frankly, this is where a lot of issues stem from - lack of spending on security. We actually discussed this in our class on Tuesday in the breakout room around why a lot of IoT products don't have sufficient access controls. It's essential to shift the narrative and view cybersecurity as an ongoing, evolving necessity for business success and growth, rather than something that can eventually reach "maintenance mode." I think while the idea of a "maintenance mode" might make sense in certain contexts, it should never equate to becoming static or a reduced focus on security. Cybersecurity (and the spend) must evolve to meet emerging challenges and continuously protect the organization's most valuable assets - which is user data and it's own reputation. My question has always been - what's the problem in spending more than we need for cybersecurity?

YELLOW DIG LAST WEEK

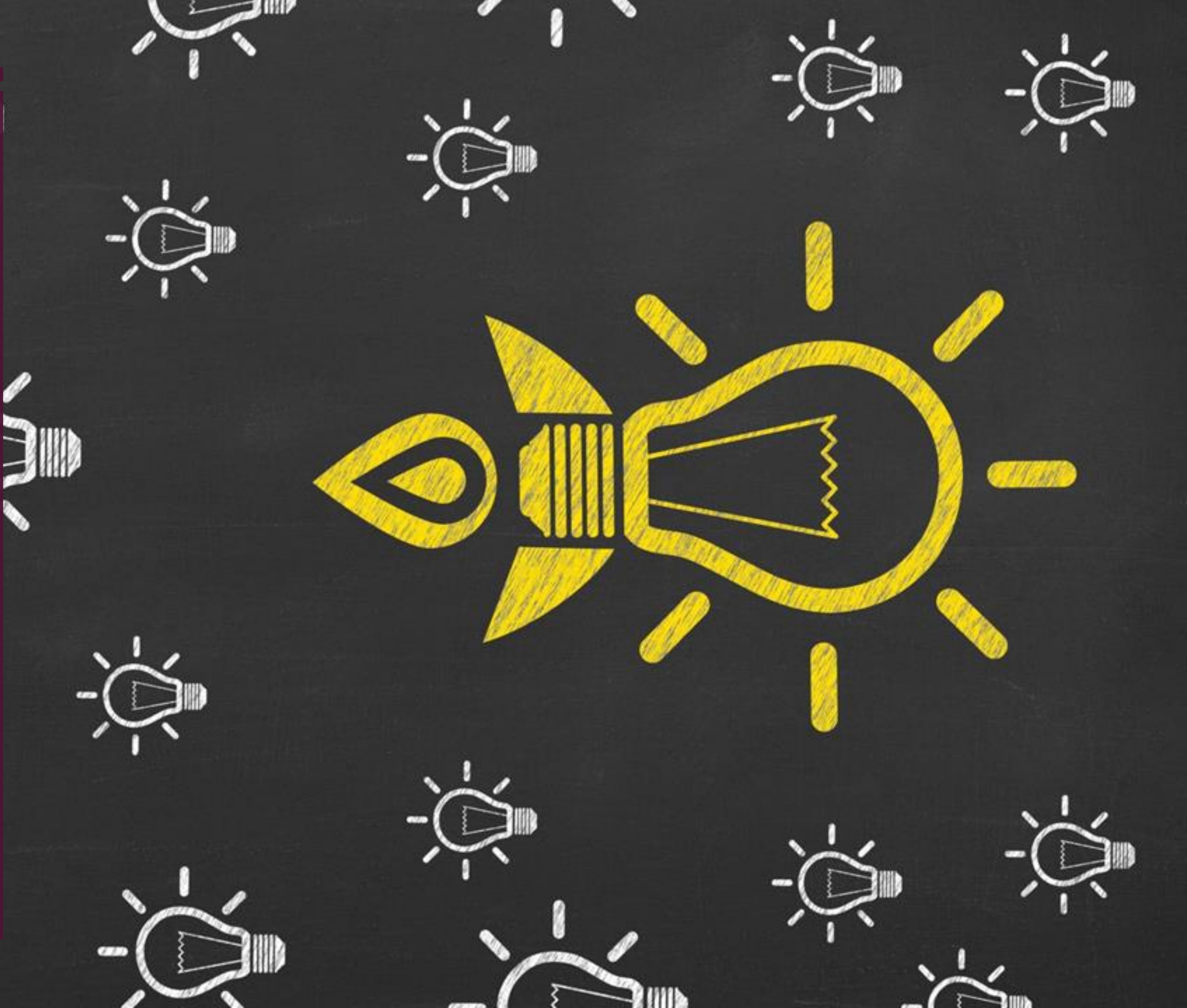
- I’m not a fan of the name Zero Trust. It is really a marketing buzzword and gives the connotation of “No Trust” and this just isn’t the case. I do love that it represents a significant shift from legacy security models like ”Trust but Verify”, which have repeatedly proven inadequate in preventing breaches. However, it does not mean no access to anyone or anything rather, Zero Trust focuses on verifying every request and enforcing the principle of least privilege, granting users only the minimum access necessary to perform their tasks. It’s about reducing implicit trust and continuously validating all access attempts.
- Trust still exists in Zero Trust, but it‘s dynamic and conditional. The goal isn’t to assume all users or devices are malicious but to ensure that access is contextually appropriate and constantly verified. This approach minimizes attack surfaces and limits the damage potential if an attacker does gain access, ultimately creating a more resilient security posture.

SHODAN IN THE NEWS https://cyberintel.substack.com/p/doge-exposes-once-secret-government

- QUOTE 1:
- Between January 14 and February 8, servers belonging to Lawrence Livermore National Laboratory, Los Alamos National Laboratory, Thomas Jefferson National Accelerator Facility, and Fermi Accelerator National Laboratory have been found with Remote Desktop Protocol (RDP) services exposed to the public internet. This grants malicious actors the opportunity to hack into servers hosting sensitive nuclear research data, a golden egg for spy agencies across the globe.
- Alarmingly, a Department of Energy server allowed anonymous login with **write access,** raising the risk of hackers uploading malicious code or installing backdoors for persistent network access.
- Shodan Search: Department of Energy nuclear laboratories [Internet]. Shodan.io. 2025 [cited 2025 Feb 9]. Available from: https://www.shodan.io/search?query=department+of+energy+country%3A%22US%22

- On February 6, the Washington Post reported that DOGE fed sensitive data into AI systems while auditing the Department of Education. The specific AI product used by DOGE was not known to the Post at the time.
- Proof: 8 IP addresses on Amazon’s GovCloud now point to Inventry.ai’s REST API, indicating a massive firehose of data being sent to the AI company’s servers. The IP addresses are: 18.253.166.131, 182.30.117.29, 18.253.153.187, 182.30.154.252, 18.254.229.158, 18.253.160.247, 18.254.175.18, 18.254.191.201

ASSIGNMENT 1



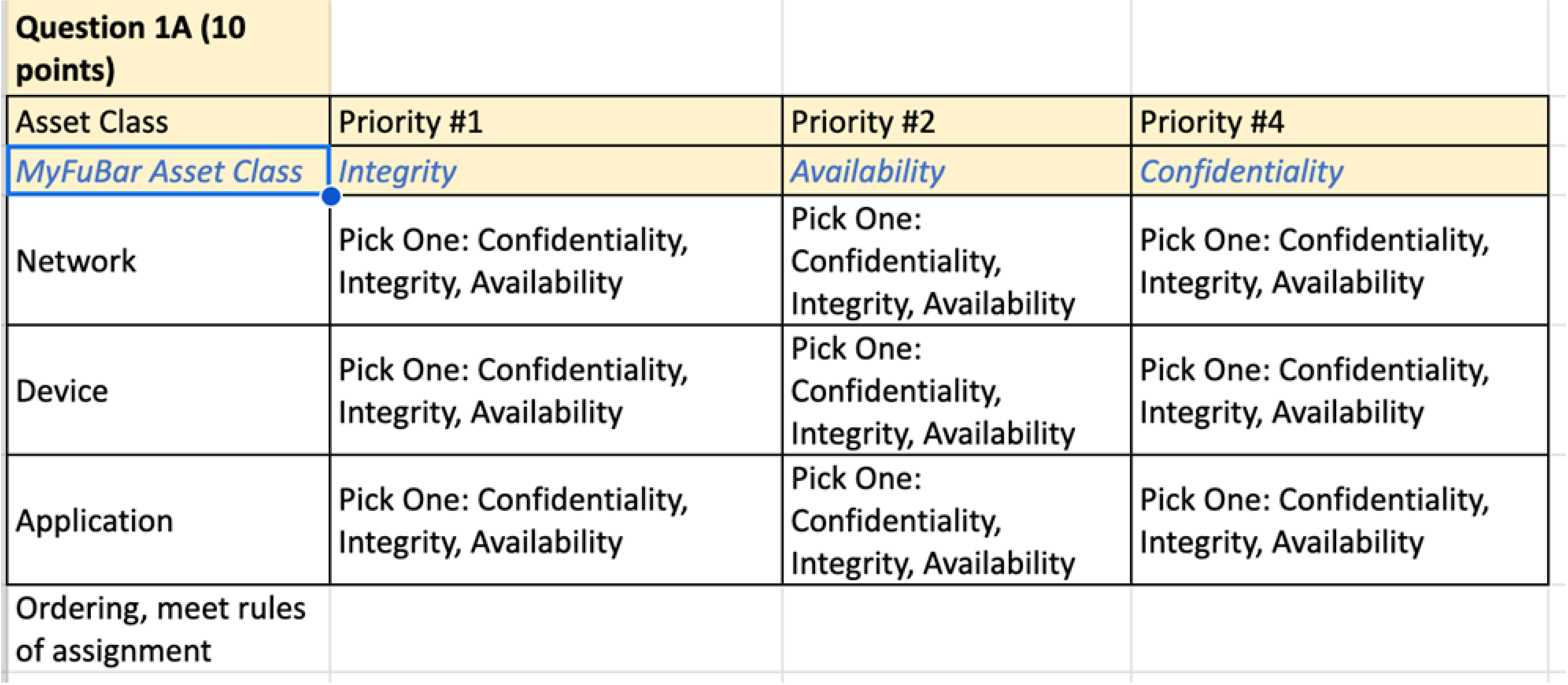
ASSIGNMENT 1

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			

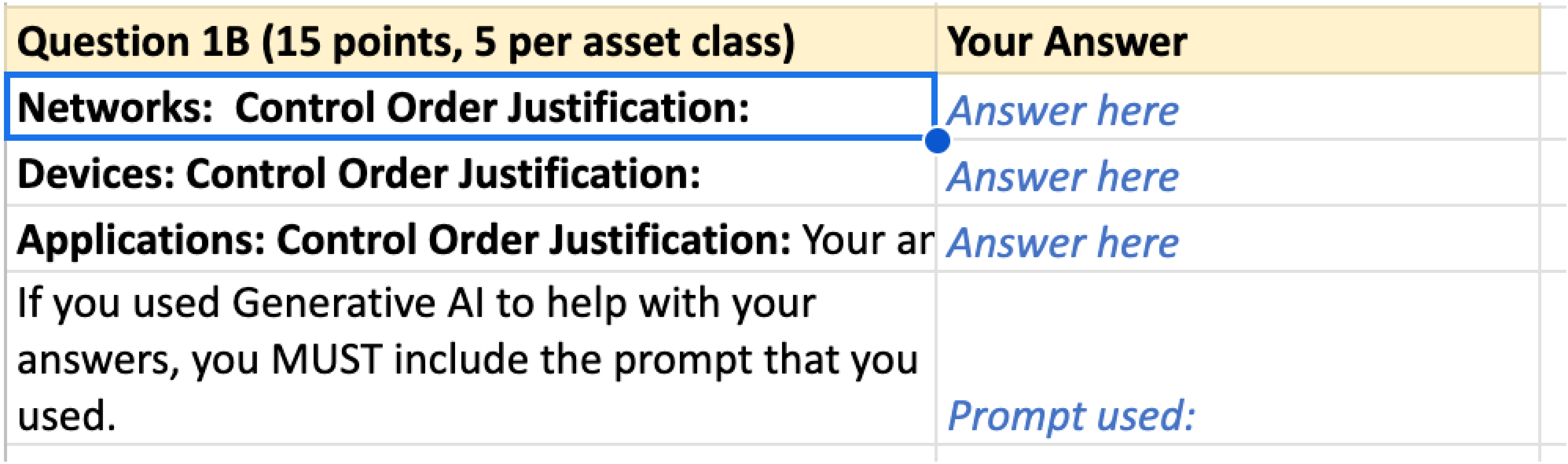
3 marks, 1 per cell

3 marks, 1 per cell

3 marks, 1 per cell

(Additional) 1 mark

Assignment 1 Details

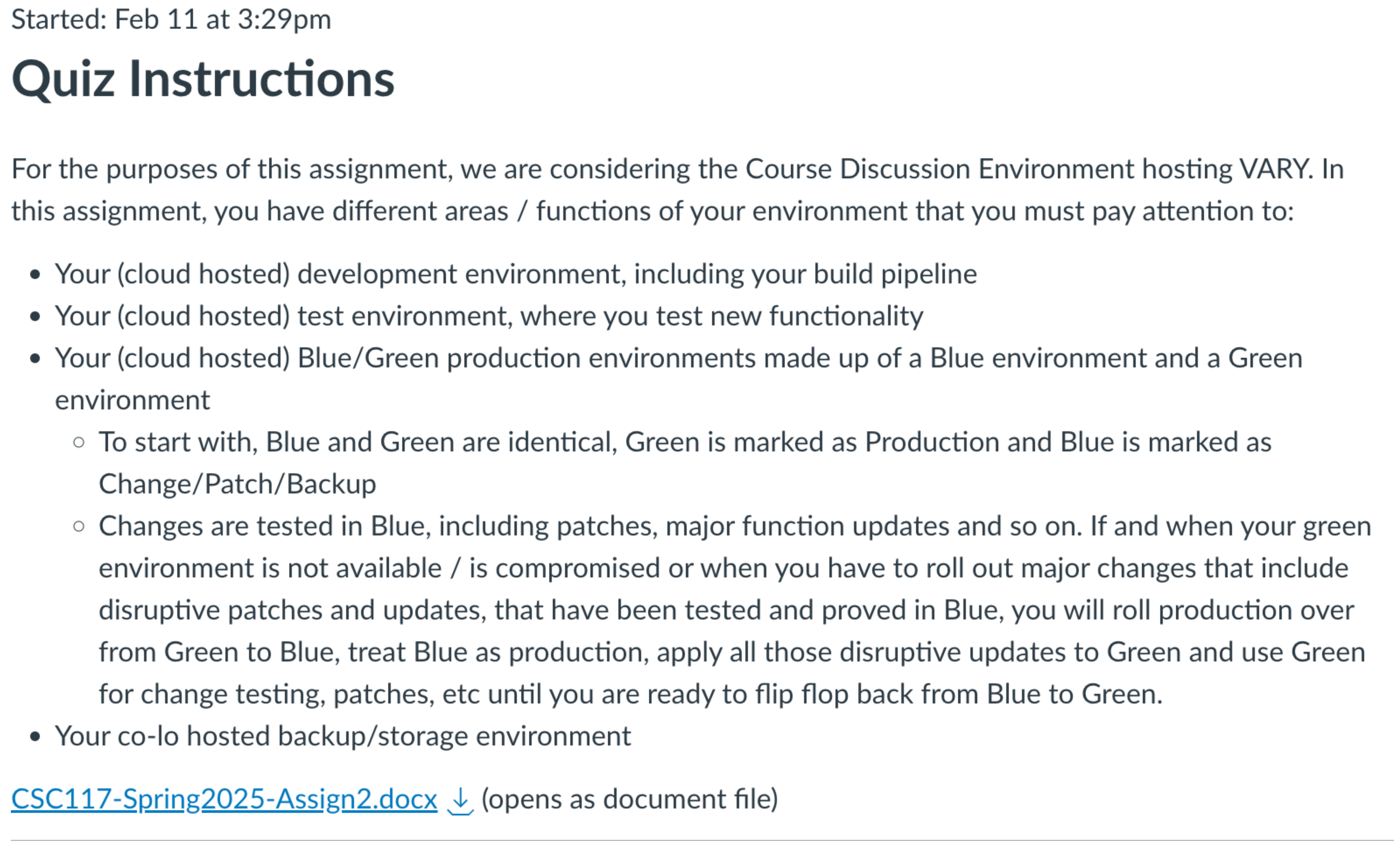


Question 1B (15 points, 5 per asset class)	**Your Answer**
Networks: Control Order Justification:	*Answer here*
Devices: Control Order Justification:	*Answer here*
Applications: Control Order Justification: Your ar	*Answer here*
If you used Generative AI to help with your answers, you MUST include the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



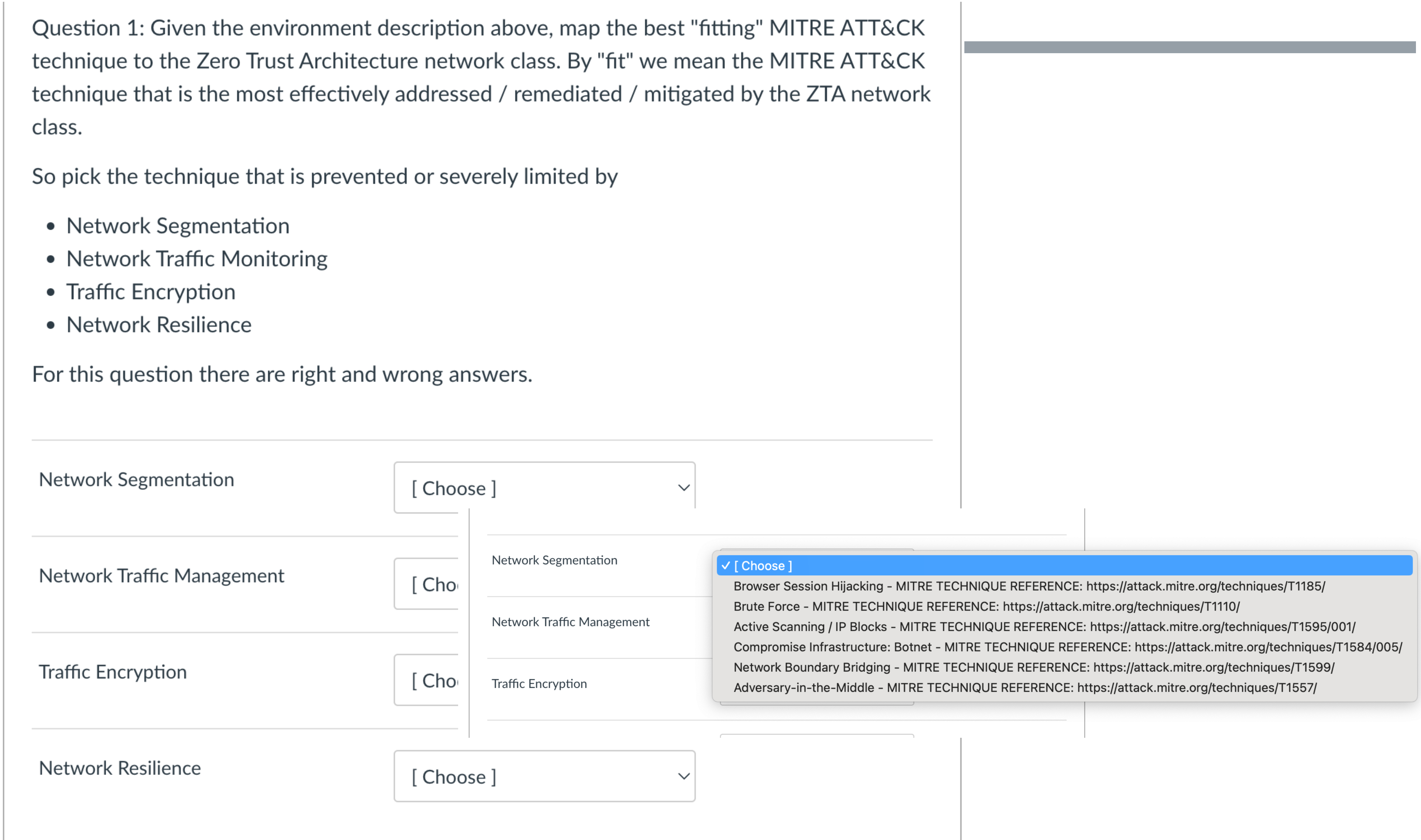
Started: Feb 11 at 3:29pm

Quiz Instructions

For the purposes of this assignment, we are considering the Course Discussion Environment hosting VARY. In this assignment, you have different areas / functions of your environment that you must pay attention to:

- Your (cloud hosted) development environment, including your build pipeline
- Your (cloud hosted) test environment, where you test new functionality
- Your (cloud hosted) Blue/Green production environments made up of a Blue environment and a Green environment
    - To start with, Blue and Green are identical, Green is marked as Production and Blue is marked as Change/Patch/Backup
    - Changes are tested in Blue, including patches, major function updates and so on. If and when your green environment is not available / is compromised or when you have to roll out major changes that include disruptive patches and updates, that have been tested and proved in Blue, you will roll production over from Green to Blue, treat Blue as production, apply all those disruptive updates to Green and use Green for change testing, patches, etc until you are ready to flip flop back from Blue to Green.
- Your co-lo hosted backup/storage environment

CSC117-Spring2025-Assign2.docx (opens as document file)



Question 1: Given the environment description above, map the best "fitting" MITRE ATT&CK technique to the Zero Trust Architecture network class. By "fit" we mean the MITRE ATT&CK technique that is the most effectively addressed / remediated / mitigated by the ZTA network class.

So pick the technique that is prevented or severely limited by

- Network Segmentation
- Network Traffic Monitoring
- Traffic Encryption
- Network Resilience

For this question there are right and wrong answers.

Network Segmentation	[Choose]
Network Traffic Management	[Cho
Traffic Encryption	[Cho
Network Resilience	[Choose]

Network Segmentation

Network Traffic Management

Traffic Encryption

✓ [Choose]

Browser Session Hijacking - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1185/

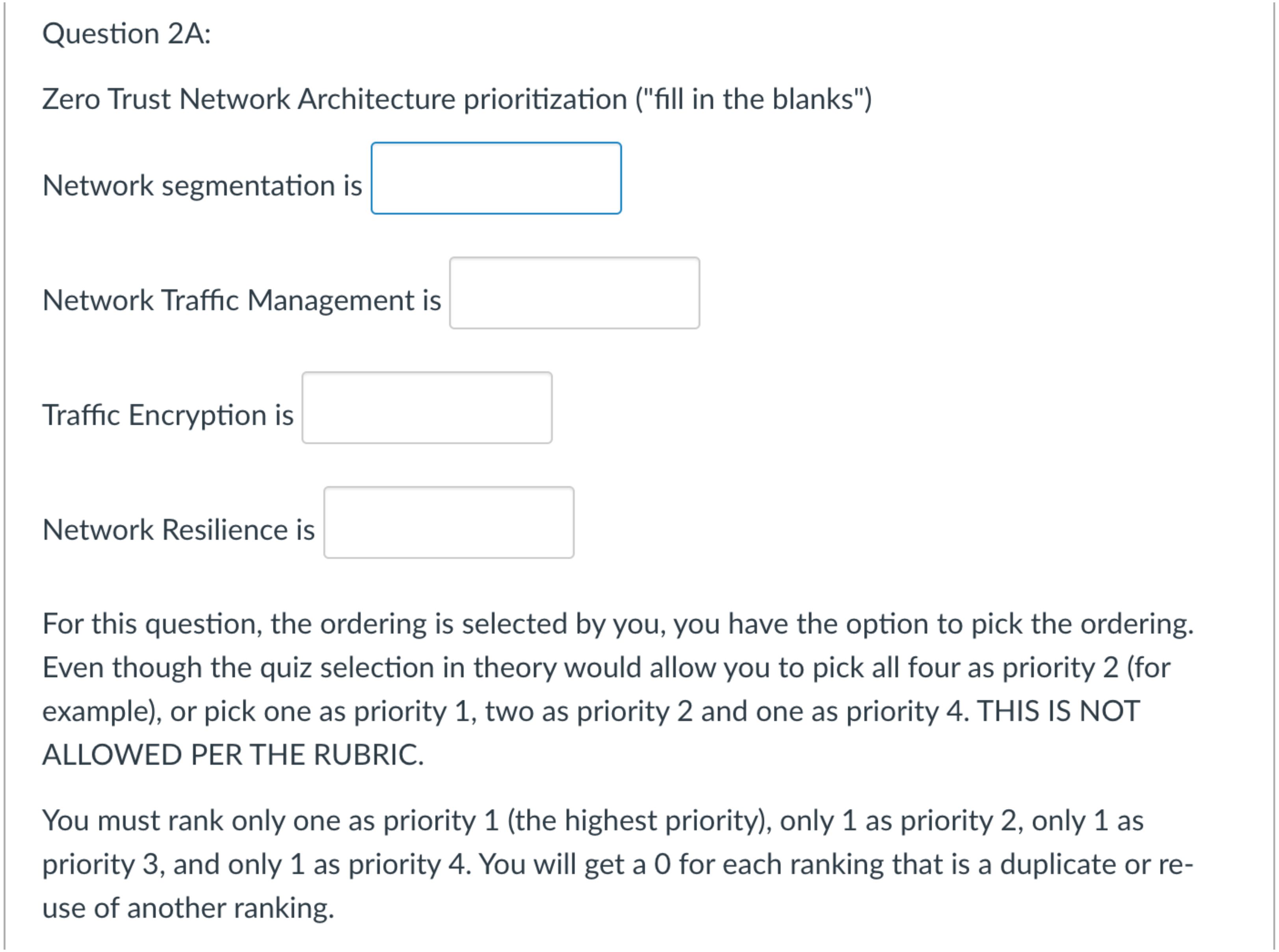
Brute Force - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1110/

Active Scanning / IP Blocks - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1595/001/

Compromise Infrastructure: Botnet - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1584/005/

Network Boundary Bridging - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1599/

Adversary-in-the-Middle - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1557/



Question 2A:

Zero Trust Network Architecture prioritization ("fill in the blanks")

Network segmentation is

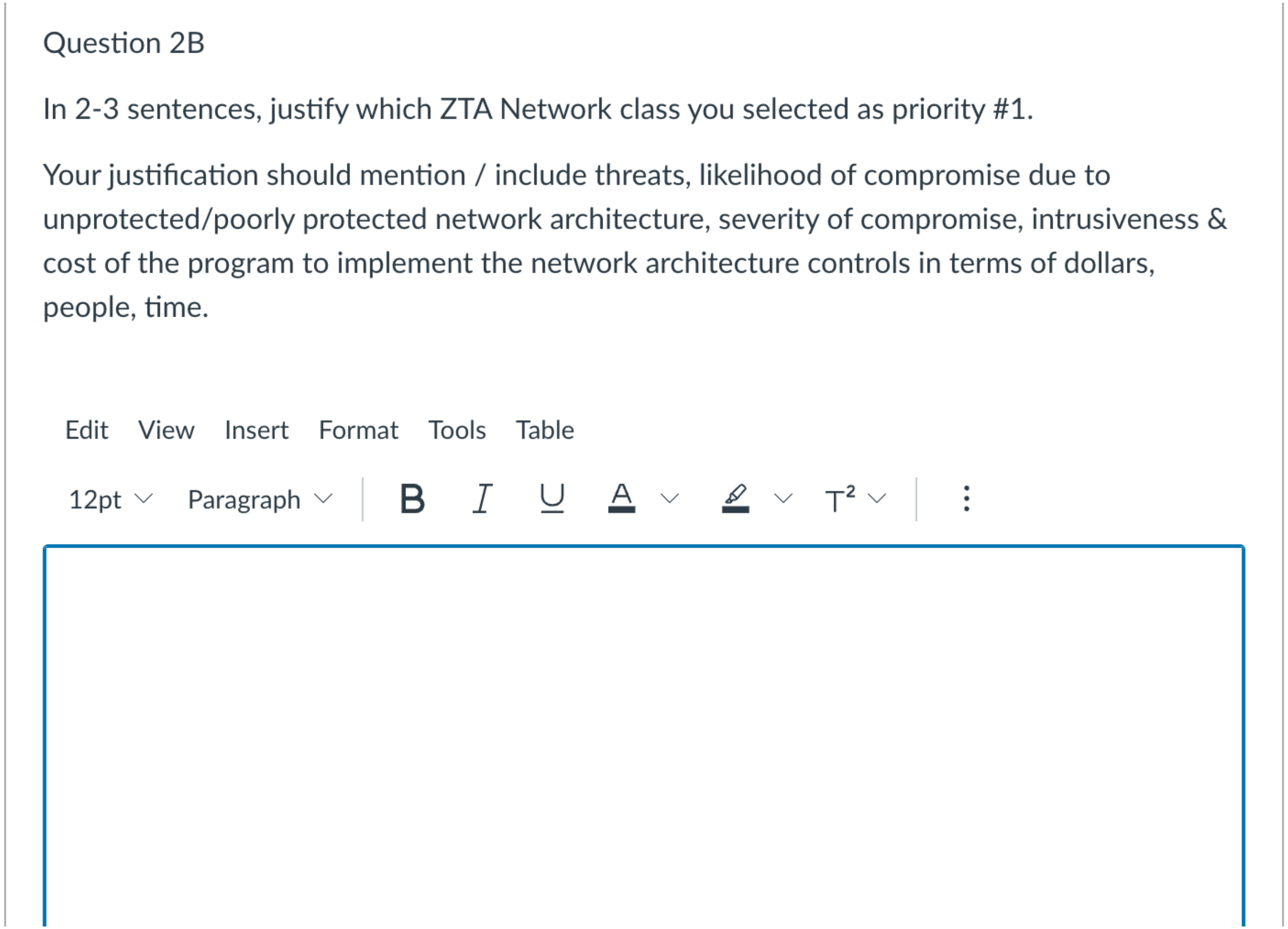
Network Traffic Management is

Traffic Encryption is

Network Resilience is

For this question, the ordering is selected by you, you have the option to pick the ordering. Even though the quiz selection in theory would allow you to pick all four as priority 2 (for example), or pick one as priority 1, two as priority 2 and one as priority 4. THIS IS NOT ALLOWED PER THE RUBRIC.

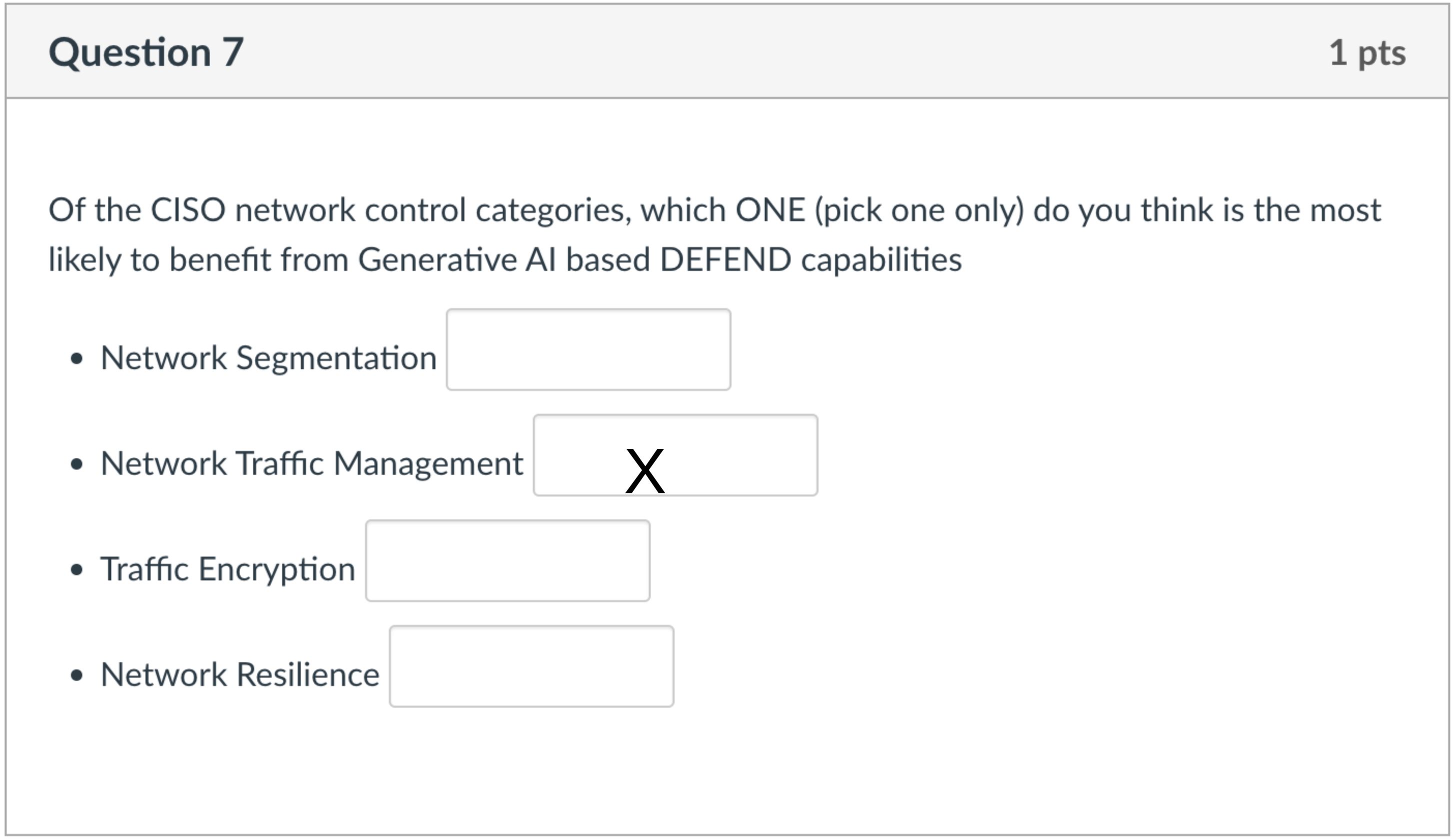
You must rank only one as priority 1 (the highest priority), only 1 as priority 2, only 1 as priority 3, and only 1 as priority 4. You will get a 0 for each ranking that is a duplicate or re-use of another ranking.



Question 2B

In 2-3 sentences, justify which ZTA Network class you selected as priority #1.

Your justification should mention / include threats, likelihood of compromise due to unprotected/poorly protected network architecture, severity of compromise, intrusiveness & cost of the program to implement the network architecture controls in terms of dollars, people, time.



Question 7 1 pts

Of the CISO network control categories, which ONE (pick one only) do you think is the most likely to benefit from Generative AI based DEFEND capabilities

- Network Segmentation
- Network Traffic Management X
- Traffic Encryption
- Network Resilience

Fill in the blanks with a "X" or " "
"X" means you think it is the one that is most likely to benefit

ASSIGNMENT 3

Due Date: Mar 9

To be released no later than Feb 23

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

To be released no later than Mar 2

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

To be released no later than March 31

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”.

ANTICIPATED END OF LECTURE 4