Lecture 5
Feb 25, 2025

CSCI E-117A SPRING 2025

SECURE APPLICATIONS: MANAGING THE DEPLOYMENT INFRASTRUCTURE

LECTURE 5/6 AGENDA

- *Assignment 1*
  - *Marks*
  - *Statistics*
- *DEVICES*
  - *Workstations*
  - *Servers*
  - *IoT*
- *Devices & Zero Trust*

QUICK ANNOUNCEMENTS

Lecture 5 – March 4 POSTPONED – DISCUSS

Polls in Interactive Classroom

- If you have instances of Polls not being available, please email hhinton@g.Harvard.edu with information including:
  - Lecture #
  - Time marker during the lecture
  - Browser you are using
- I am working with the developer for the IC integrations and will let you know more as we learn more

YELLOW DIG LAST WEEK

YELLOW DIG LAST WEEK
MEMORY SAFE LANGUAGES

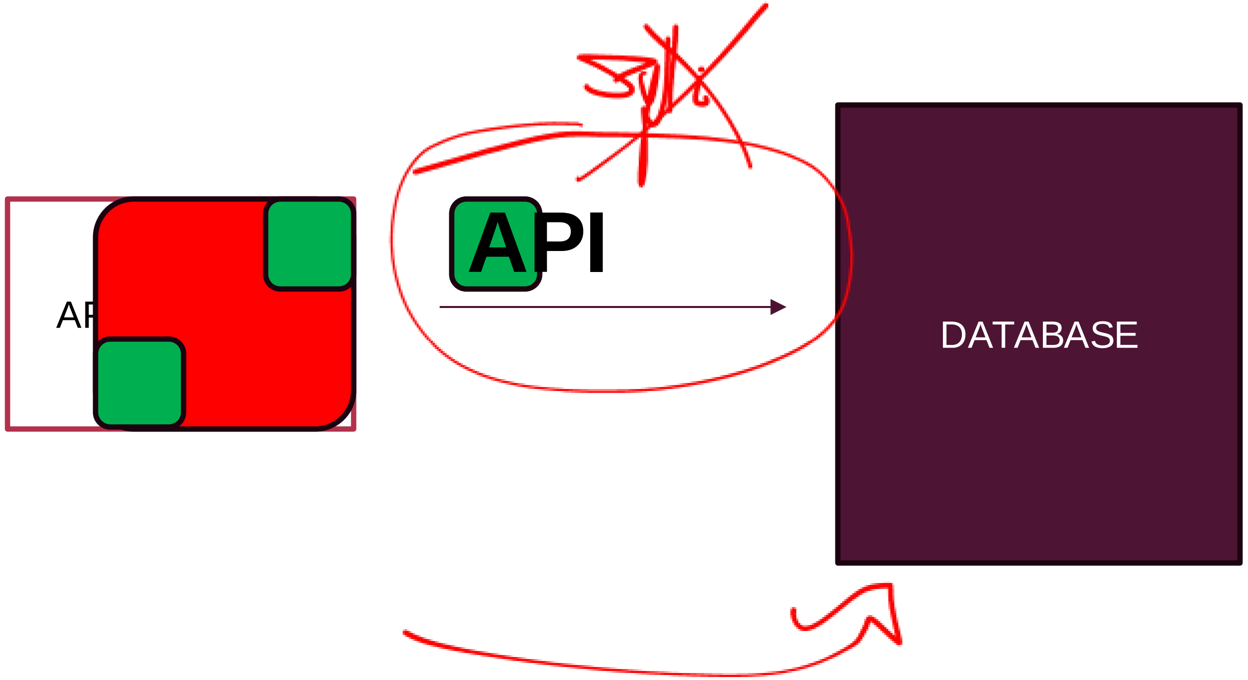
- The argument that older code has fewer bugs might be true, but the effects of those bugs are magnified a lot more - For example, the Linux kernel IP bug was not found for 8 years. Who knows what was exploited During that time? In fact, APT's (Advanced Persistent Threats) actually look for such bugs.
- To me a bug is a bug. Period. Old or new
- Having newer memory safe code while not tackling older code base is not a cure. Take for example rust - Rust is memory safe sure, but rust runtime runs atop multiple system libraries written in c and c++, and many rust code bases interface with these libraries. So a memory safe language by itself is no good, unless it's foundation is good - so we need to tackle the problem of hardening the base and running memory safe languages on top them to assure memory safety composition.

MEMORY SAFE LANGUAGES

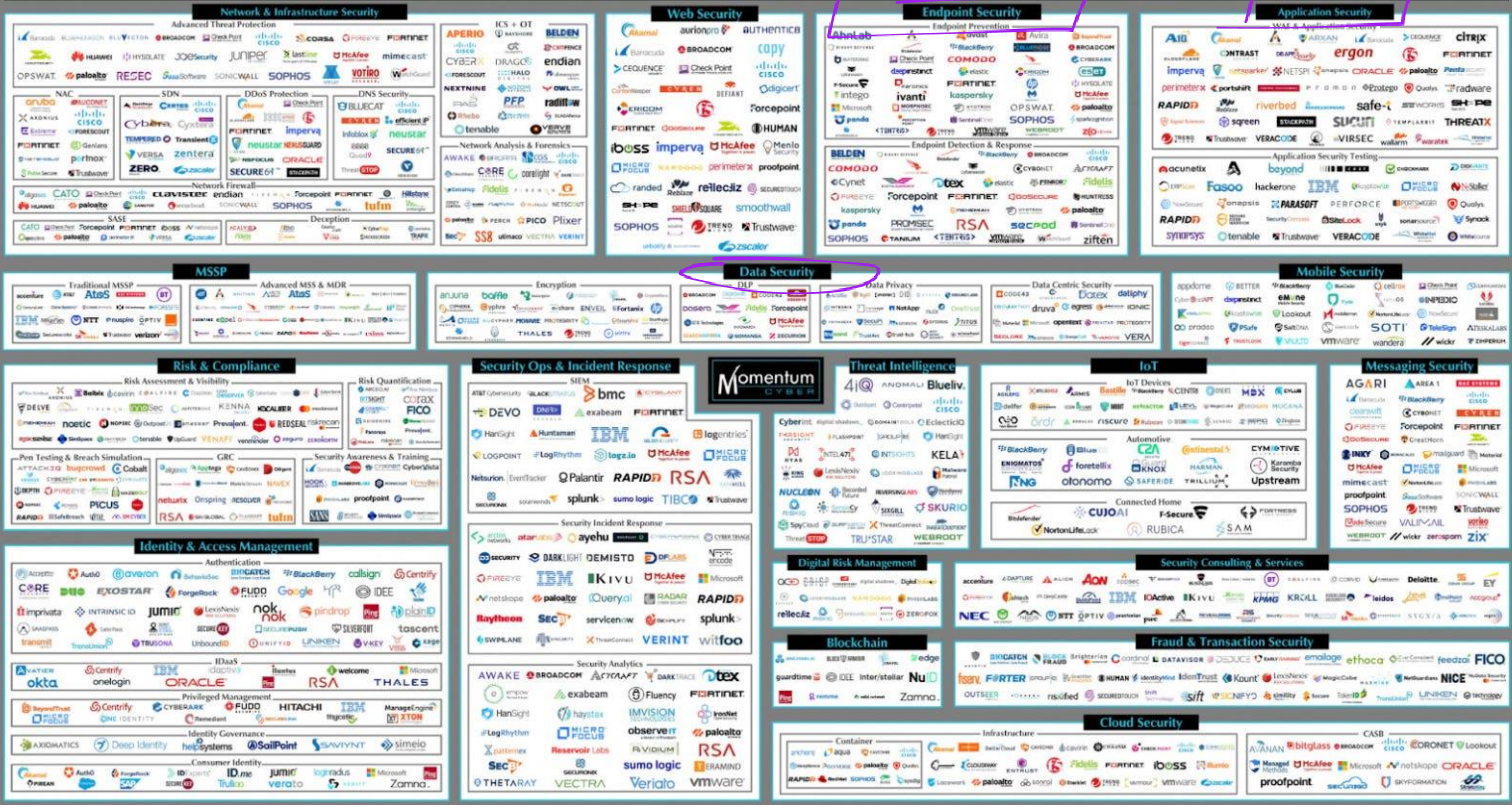
https://www.linkedin.com/events/resilientcyberw-christophkern-d7205984963228286977/theater/

🟥 Pre memory Safe

🟩 Memory Safe



CYBER SCAPE 2022



Network & Infrastructure Security

Advanced Threat Protection
Barracuda, Bluehexagon, BluVector, Broadcom, Check Point, Cisco, Corsa, FireEye, Fortinet, Huawei, Hysolate, Joe Security, Juniper, Lastline, McAfee, Mimecast, OPSWAT, Paloalto, Resec, SasaSoftware, SonicWall, Sophos, Votiro, WatchGuard

NAC
Aruba, Auconet, Cisco, Forescout, Extreme, Fortinet, Genians, Portnox, Trustwave

SDN
Cyberark, Certes, Cisco, Cybera, Cyxtera, Tempered, Transient, Versa, Zentera, Zero, Zscaler

DDoS Protection
Akamai, Check Point, F5, Fortinet, Imperva, Neustar, Netscout, Oracle, Secure64, Quad9, Threat Stop

DNS Security
BlueCat, Cisco, Infoblox, efficient iP, Neustar, Secure64

ICS + OT
Aperio, Bayshore, Belden, Cisco, CyberX, Dragos, Endian, Forescout, Halo, Nextnine, Nozomi, PAS, PFP, Radiflow, Rhebo, Tenable, Verve

Network Firewall
Algosec, Cato, Check Point, Cisco, Clavister, Endian, Forcepoint, Fortinet, Hillstone, Huawei, Paloalto, SonicWall, Sophos, Tufin

SASE
Cato, Check Point, Forcepoint, Fortinet, iboss, Netskope, Paloalto, Versa, Zscaler

Deception
Acalvio, Attivo, CyberTrap, Illusive, TrapX

Network Analysis & Forensics
Awake, Corelight, Core, ExtraHop, Fidelis, Gigamon, Netscout, Plixer, Pico, Perch, SS8, Vectra, Verint

Web Security
Akamai, Aurionpro, Authentic8, Barracuda, Broadcom, Cequence, Check Point, Cisco, Copy, ContentKeeper, Cyren, Defiant, Digicert, Ericom, F5, Forcepoint, Fortinet, GoSecure, HUMAN, iboss, Imperva, McAfee, Menlo Security, Micro Focus, Perimeterx, Proofpoint, Randed, Rebiaze, ReliaQuest, SecureTouch, Shape, ShieldSquare, Smoothwall, Sophos, Trend Micro, Trustwave, Zscaler

Endpoint Security

Endpoint Prevention
AhnLab, Avast, Avira, BeyondTrust, BlackBerry, Broadcom, Bitdefender, Check Point, Comodo, Cybereason, Deep Instinct, Elastic, ESET, F-Secure, Fortinet, Intego, Ivanti, Kaspersky, McAfee, Microsoft, Morphisec, OPSWAT, Paloalto, Panda, Sophos, Tehtris, VMware, Webroot, Zero

Endpoint Detection & Response
Belden, BlackBerry, Broadcom, Cisco, Comodo, Cybereason, Cynet, Cytract, Elastic, Fidelis, FireEye, Forcepoint, Fortinet, GoSecure, Huntress, Kaspersky, Microsoft, Paloalto, Panda, Promisec, RSA, SecPod, Sophos, Tanium, Tehtris, Tanium, VMware, Ziften

Application Security

WAF & Application Security
A10, Akamai, Arxan, Barracuda, Cequence, Citrix, Cloudflare, Contrast, Ergon, F5, Fortinet, Imperva, Netsparker, Netspi, Oracle, Paloalto, Perimeterx, Portshift, Protego, Qualys, Radware, Rapid7, Riverbed, Safe-T, Shape, Sqreen, Stackpath, Sucuri, ThreatX, Trustwave, Veracode, Virsec, Wallarm, Waratek

Application Security Testing
Acunetix, Beyond, Checkmarx, Fasoo, Hackerone, IBM, Micro Focus, Onapsis, Parasoft, Perforce, Qualys, Rapid7, Sitelock, Snyk, Sonarsource, Synopsys, Synack, Tenable, Trustwave, Veracode, WhiteHat

MSSP

Traditional MSSP
Accenture, AT&T, Atos, BT, CenturyLink, Deloitte, Fujitsu, IBM, NTT, Optiv, Orange, Verizon

Advanced MSS & MDR
Arctic Wolf, Atos, eSentire, Expel, Red Canary, Secureworks, Trustwave, Unisys

Data Security

Encryption
Aruna, Baffle, Cipher, Entrust, Envieil, Fortanix, HP, Protegrity, Thales, Trend Micro, Virtru

DLP
Broadcom, Code42, Digital Guardian, Fidelis, Forcepoint, GTB Technologies, McAfee, Somansa, Zecurion

Data Privacy
BigID, NetApp, OneTrust, Securiti, Privitar, Trustarc

Data Centric Security
Code42, Datex, Dataphy, Druva, Egress, Ionic, Opentext, Protegrity, Varonis, Vera

Mobile Security
Appdome, Better, BlackBerry, Check Point, Cellrox, Deepinstinct, eMome, Lookout, Pradeo, PSafe, Sophos, Soti, SaltDNA, TeleSign, Vmware, Wandera, Wickr, Zimperium

Risk & Compliance

Risk Assessment & Visibility
Axonius, Balbix, Bitsight, Covalence, Delve, Kenna, NoSec, Noetic, Prevalent, RedSeal, RiskRecon, RiskSense, Tenable, UpGuard, Venafi, Zeguro, ZeroNorth

Risk Quantification
Arceo AI, Corax, FICO, Prevalent

Pen Testing & Breach Simulation
AttackIQ, Bugcrowd, Cobalt, Cymulate, FireEye, Picus, Rapid7, SafeBreach, XM Cyber

GRC
Algosec, Apptega, Netwrix, Onspring, Resolver, RSA, Tufin

Security Awareness & Training
Barracuda, Cyber Vista, KnowBe4, Proofpoint, SANS

Security Ops & Incident Response

SIEM
AT&T Cybersecurity, Blackstratus, BMC, Cyberlant, Devo, DNIF, Exabeam, Fortinet, HanSight, Huntsman, IBM, LogPoint, LogRhythm, Logz.io, Logentries, McAfee, Micro Focus, Netsurion, Palantir, Rapid7, RSA, Securonix, Splunk, Sumo Logic, TIBCO, Trustwave

Security Incident Response
Arctos Networks, Atar Labs, Ayehu, Cyber Triage, D3 Security, DarkLight, Demisto, DFLabs, FireEye, IBM, Kivu, McAfee, Microsoft, Netskope, Paloalto, Query.ai, Radar, Rapid7, Raytheon, SecBI, ServiceNow, Splunk, Swimlane, ThreatConnect, Verint, Witfoo

Security Analytics
Awake, Broadcom, Cytract, Darktrace, Exabeam, Fluency, Fortinet, HanSight, Haystax, Imvision, LogRhythm, Micro Focus, ObserveIT, Paloalto, Patternex, Reservoir Labs, RSA, Securonix, SecBI, Sumo Logic, ThetaRay, Vectra, Veriato, VMware

Momentum CYBER

Threat Intelligence
4iQ, Anomali, Blueliv, Cisco, Cyberint, Digital Shadows, DomainTools, EclecticIQ, Flashpoint, Group-IB, HanSight, Intel471, Intsights, Kela, LookingGlass, Nucleon, Recorded Future, SixGill, Skurio, SpyCloud, Threat Stop, ThreatConnect, TruStar, Webroot

IoT

IoT Devices
Armis, Bastille, BlackBerry, Centri, Cylus, Dellfer, Ordr, Miscure, Rubicon

Automotive
BlackBerry, Blue, C2A, Continental, CymOTive, Enigmatos, Forelellix, GuardKnox, Harman, Karamba Security, NNG, Otonomo, SafeRide, Trillium, Upstream

Connected Home
Bitdefender, CujoAI, F-Secure, Fortress, NortonLifeLock, Rubica, SAM

Messaging Security
Agari, Area 1, Barracuda, BlackBerry, Cisco, Cybonet, Cyren, FireEye, Forcepoint, Fortinet, GoSecure, Inky, McAfee, Micro Focus, Mimecast, Microsoft, Proofpoint, Sophos, Trend Micro, Trustwave, Vali Mail, Votiro, Webroot, Wickr, Zerospam, Zix

Identity & Access Management

Authentication
Acceptto, Auth0, Averon, BehavioSec, BioCatch, BlackBerry, Callsign, Centrify, Core, Duo, Exostar, ForgeRock, Fudo, Google, IDEE, Imprivata, Intrinsic ID, Jumio, LexisNexis, Nok Nok, Pindrop, Ping, Plain ID, Secret Double Octopus, SecurEnvoy, Silverfort, Tascent, Transmit, TrustOnic, Trusona, UnboundID, Unifyid, Uniken, Vkey, Xage

IDaaS
Avatier, Centrify, IBM, Idaptive, Ilantus, Microsoft, Okta, OneLogin, Oracle, Ping, RSA, Thales, Welcome

Privileged Management
BeyondTrust, Centrify, CyberArk, Fudo, Hitachi, IBM, ManageEngine, Micro Focus, One Identity, Remediant, Thycotic, Xton

Identity Governance
Axiomatics, Deep Identity, Helpsystems, SailPoint, Saviynt, Simeio

Consumer Identity
Akamai, Auth0, ForgeRock, IDExperts, ID.me, Jumio, Loginradius, Microsoft, Ping, Pirean, Salesforce, SAP, SecureAuth, Trulioo, Verato, Zamna

Digital Risk Management
CIS, Digital Shadows, RiskIQ, ReliaQuest, ZeroFox

Blockchain
Edge, Guardtime, IDEE, Interstellar, NuID, Ping, Zamna

Security Consulting & Services
Accenture, Aon, BT, Deloitte, EY, IBM, IOActive, Kivu, KPMG, Kroll, Leidos, NEC, NTT, Optiv, Praetorian, Pure, Sygnia

Fraud & Transaction Security
BioCatch, Block Fraud, Brighterion, Cardinal, DataVisor, Emailage, Ethoca, Feedzai, FICO, Forter, Group-IB, HUMAN, IdentityMind, IdenTrust, Kount, LexisNexis, NICE, Outseer, Riskified, SecuredTouch, Sift, Signifyd, Socure, Uniken

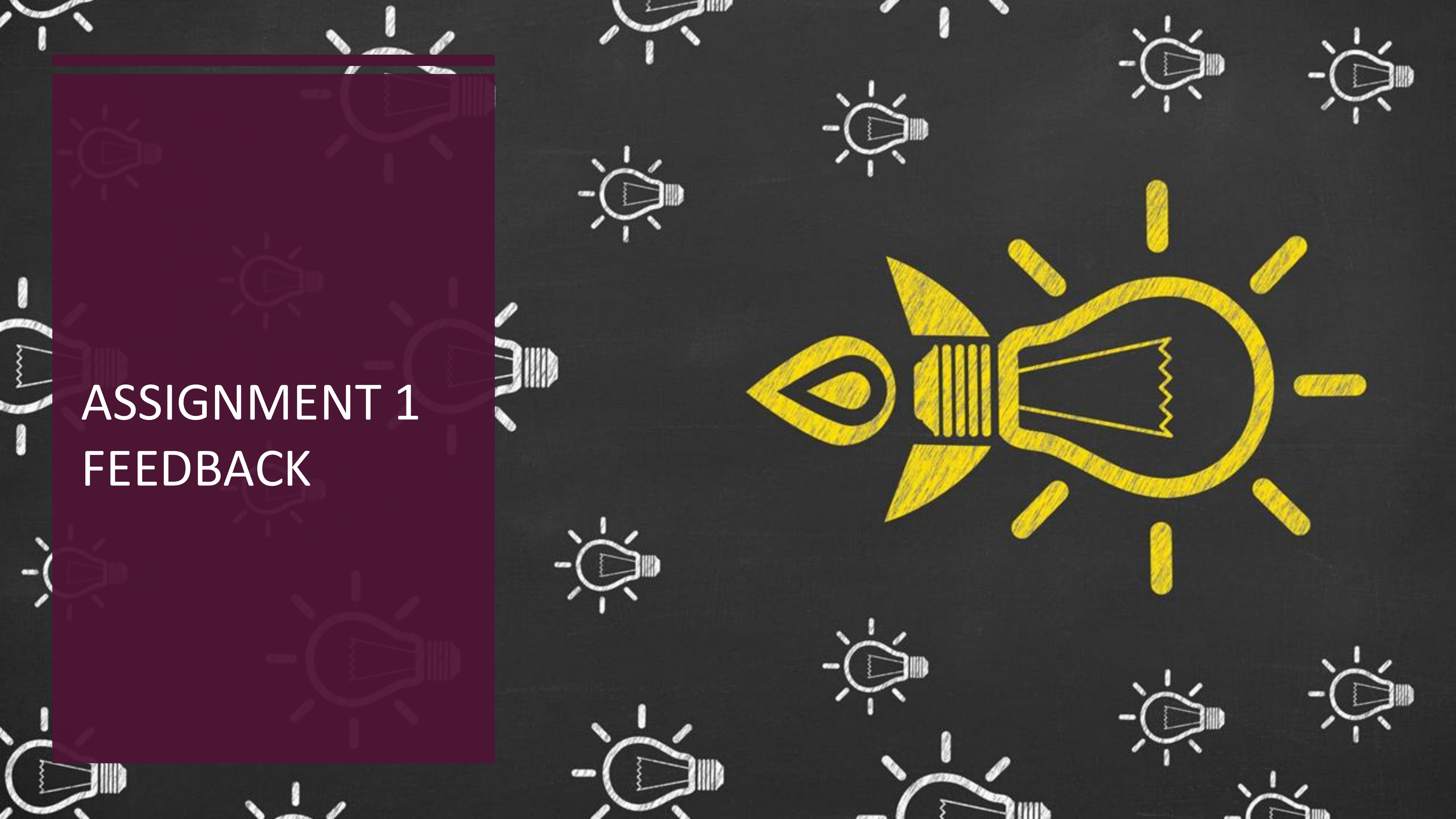
Cloud Security

Container
Aqua, Capsule8, Paloalto, Qualys, Rapid7, Sophos, Sysdig

Infrastructure
Akamai, CloudPassage, Cloudflare, Fidelis, Fortinet, iboss, Entrust, Paloalto, Trend Micro, VMware, Zscaler

CASB
Avanan, Bitglass, Broadcom, Cisco, Coronet, Lookout, Managed Methods, McAfee, Microsoft, Netskope, Oracle, Proofpoint, Skyformation

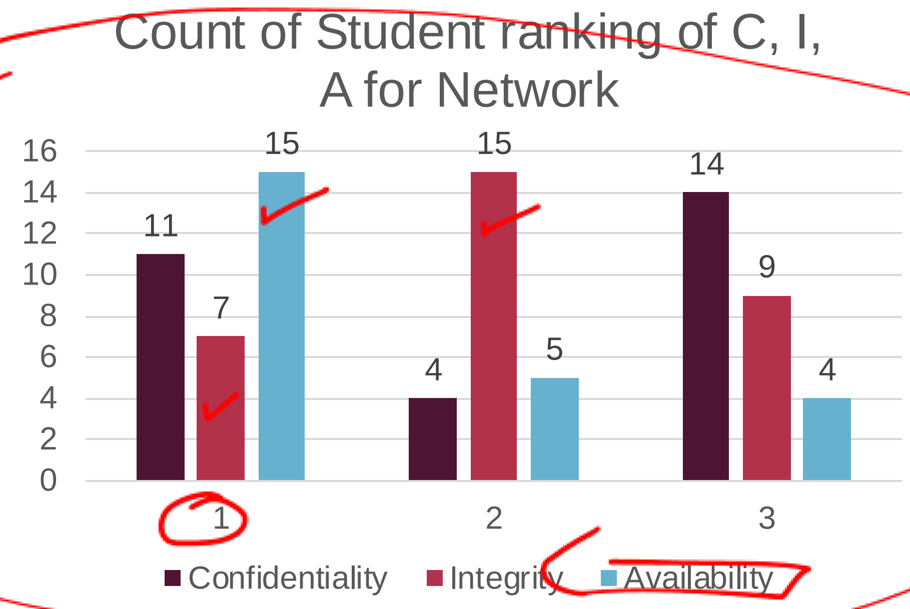
ASSIGNMENT 1 FEEDBACK

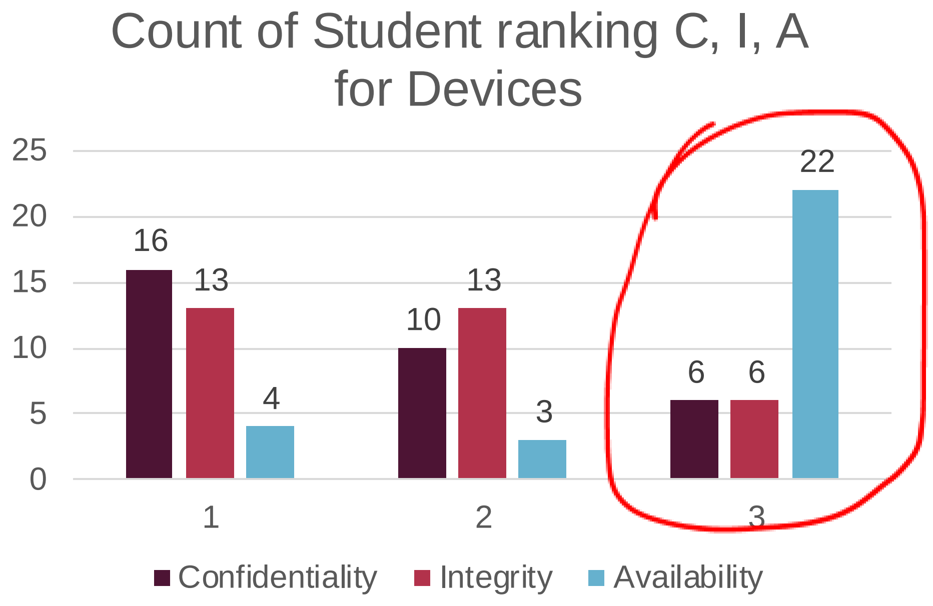


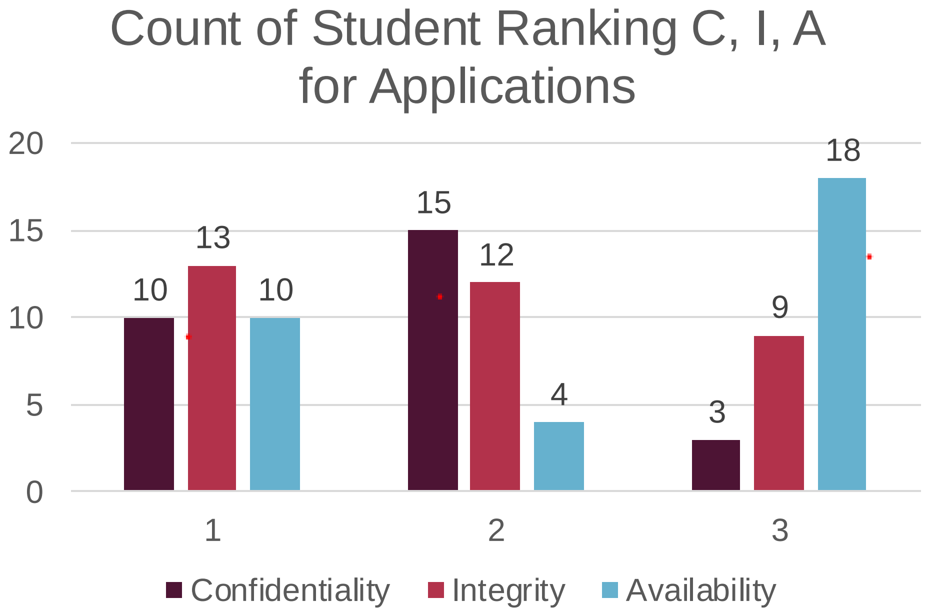
ASSIGNMENT 1 FEEDBACK

Due Date: Feb 16

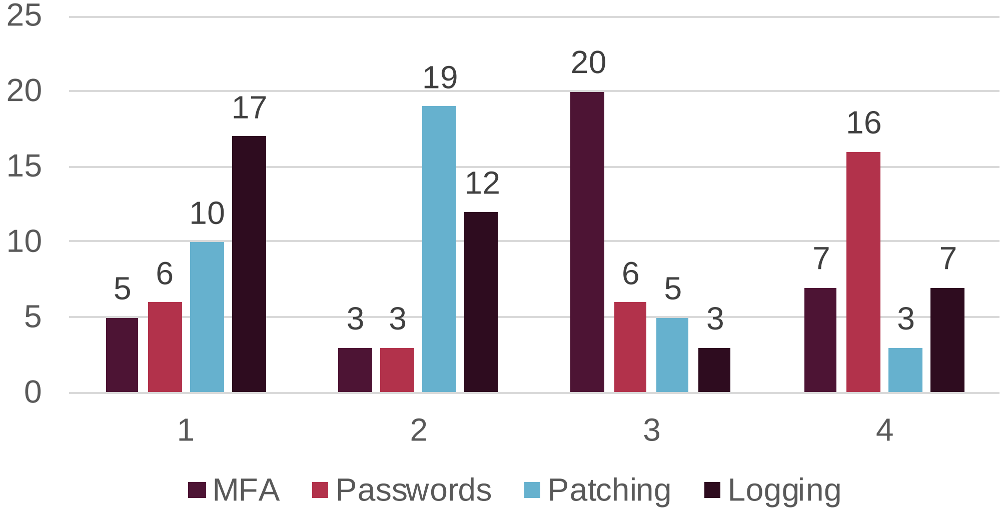
Purpose: Start to think about threats to the network, device and application asset classes, and as a bonus, the impact of GenAI in the attack and defense of the asset classes.


Count of Student ranking of C, I, A for Network

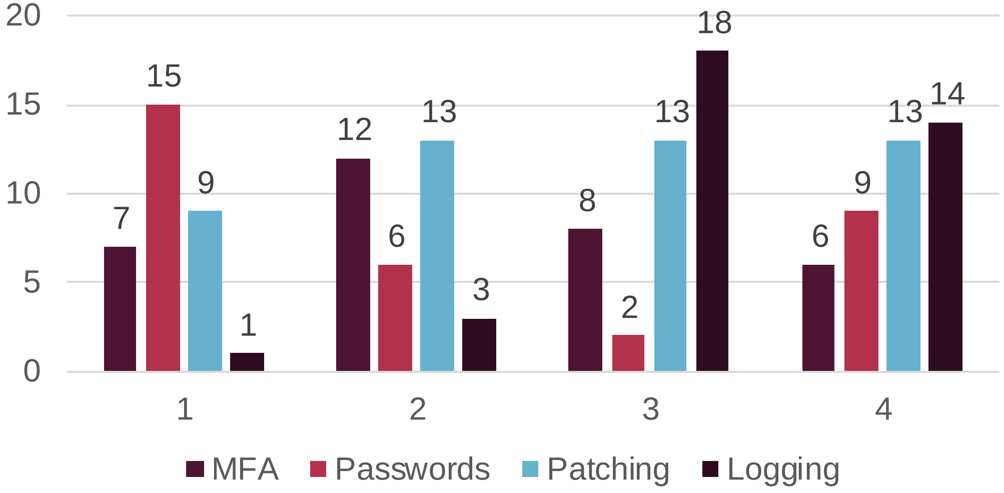

Count of Student ranking C, I, A for Devices


Count of Student Ranking C, I, A for Applications

Count of Student Rankings for Networks

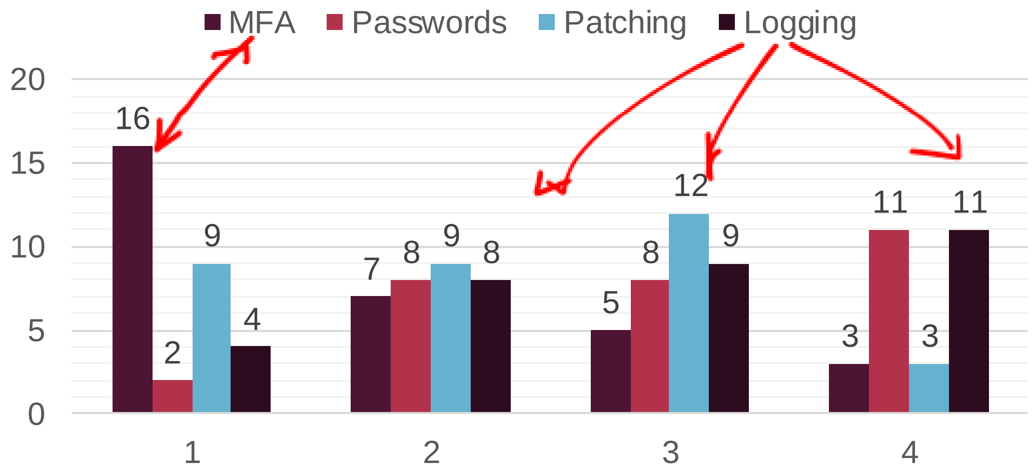


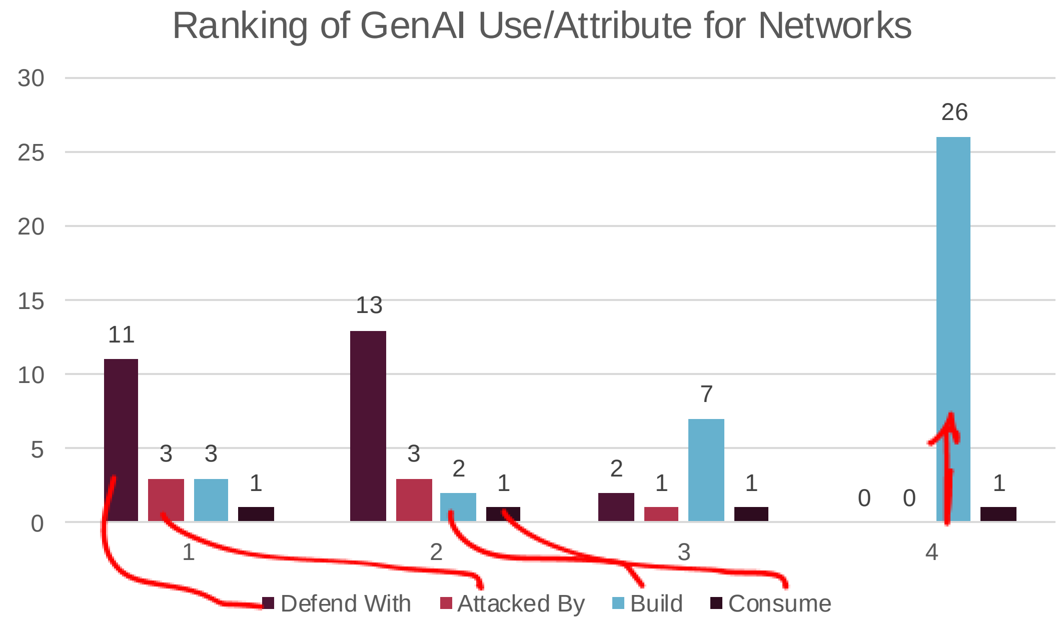
Count of Student Rankings for Devices

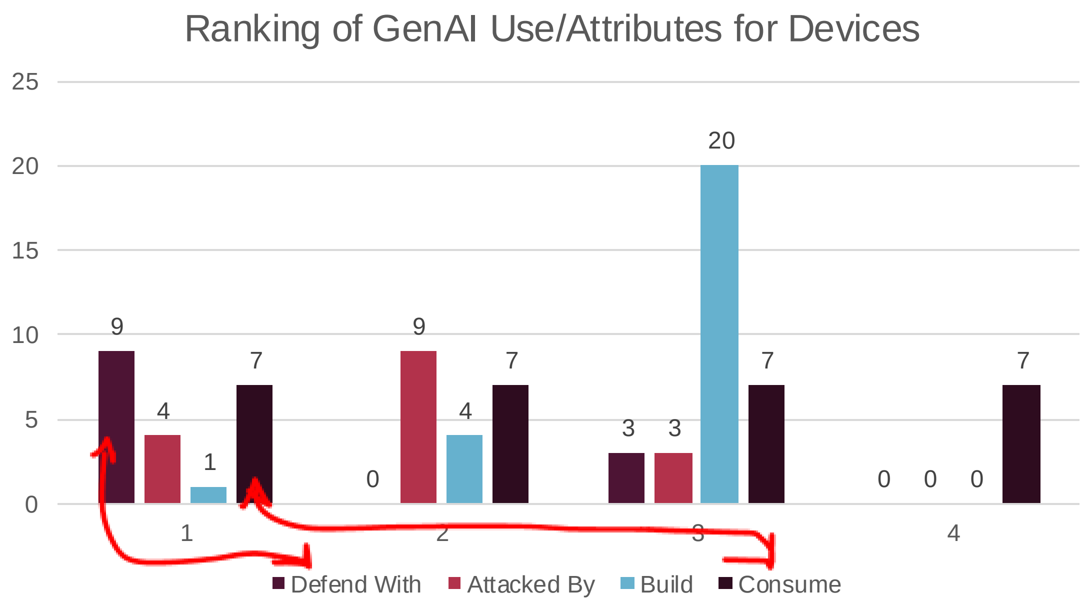


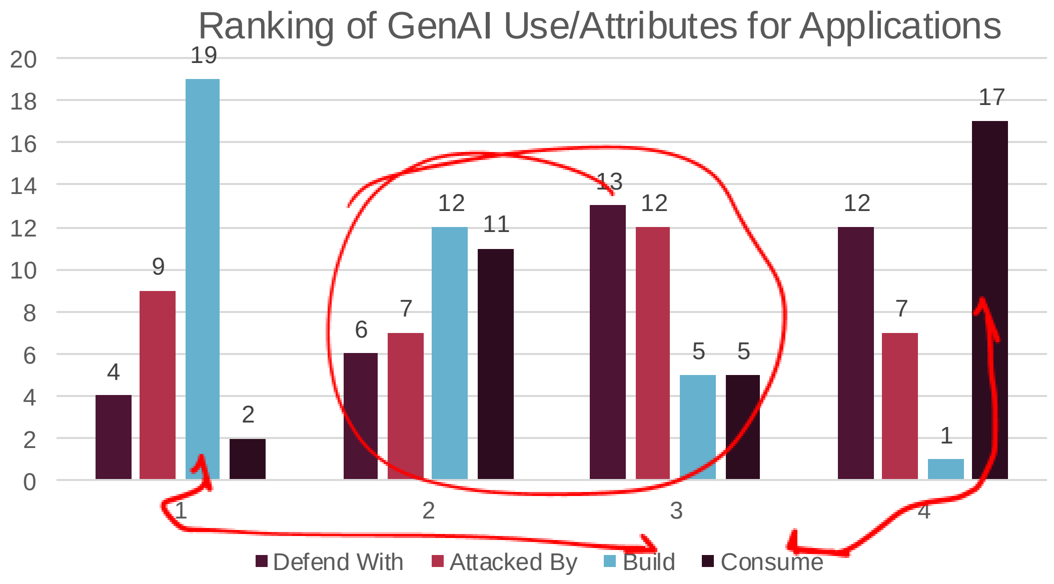
Count of Student Rankings for Applications

Ranking of
MFA, Passwords,
Patching, Logging




Ranking of GenAI Use/Attribute for Networks


Ranking of GenAI Use/Attributes for Devices


Ranking of GenAI Use/Attributes for Applications

COMMENTS ON WRITTEN ANSWERS

- Feedback: Executives and customers require different messaging—executives care about risk management budget constraints and ROI, while customers care about compliance (e.g., SOC 2, GDPR, PCI-DSS).

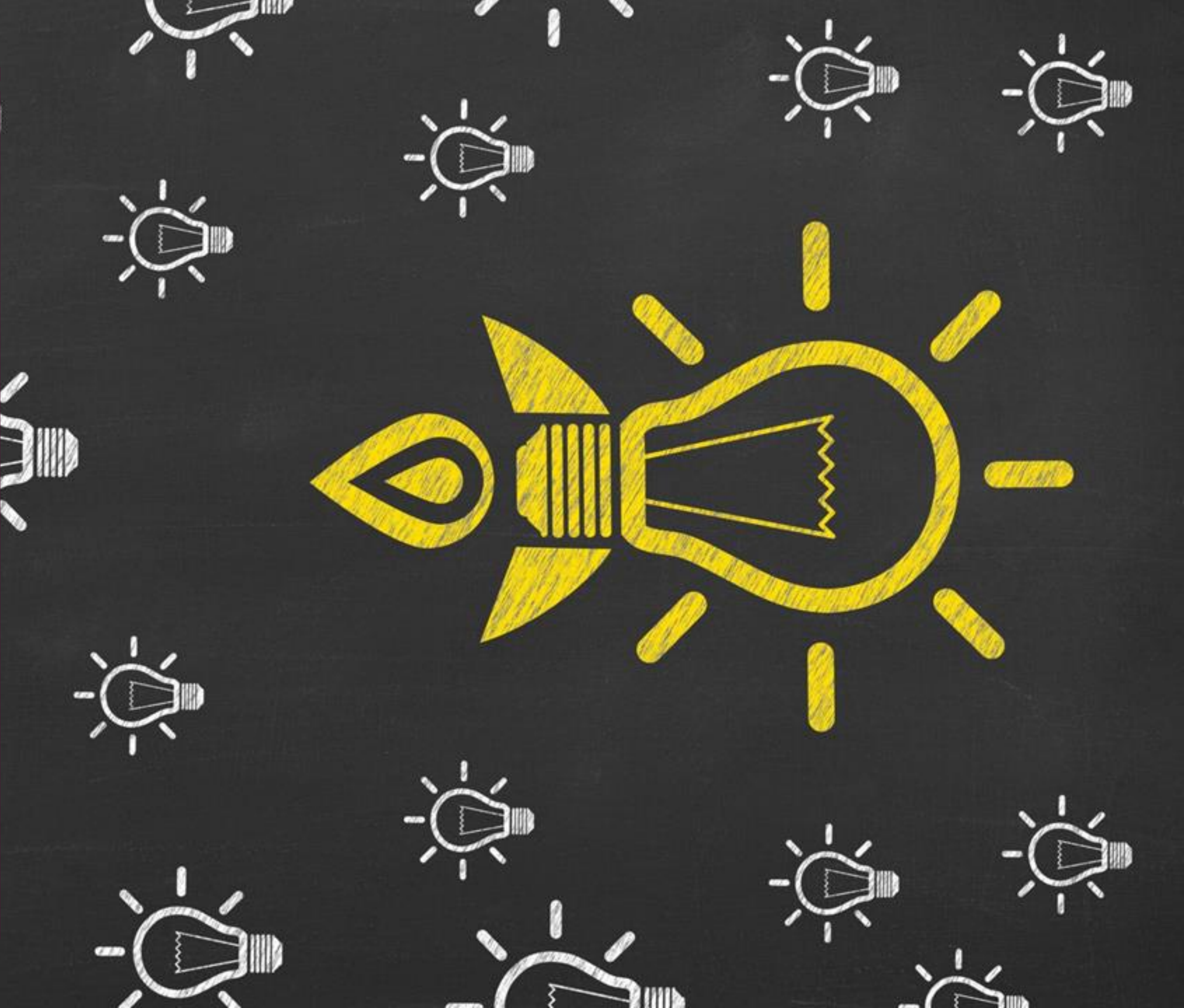
GOOD ANSWER (1B NETWORKS)

For the network, confidentiality is the highest priority because protecting data from interception and unauthorized access is essential for regulatory compliance and user trust. Since the system handles personally identifiable information (PII) and payment processing, a breach could expose sensitive data, leading to financial losses, legal penalties, and reputational damage. While availability is important to ensure the network remains operational, downtime can often be mitigated through redundancy and failover strategies, making it a secondary concern. Integrity is ranked lowest because although network configuration attacks, such as BGP hijacking or DNS poisoning, can disrupt traffic, they are often detectable and correctable faster than confidentiality breaches. Overall, while a network outage may cause temporary disruptions, a data breach could have long-lasting consequences, making confidentiality the top priority.

GEN AI PROMPTS

- Prompts used: "what is generative cybersecurity AI applications", "Please provide a Deep Dive into Generative Cybersecurity AI Applications", "Can you provide an example of "prompt injection" ?

REMINDERS



DEVICES AND ZERO TRUST

DEVICES: DEFINITION

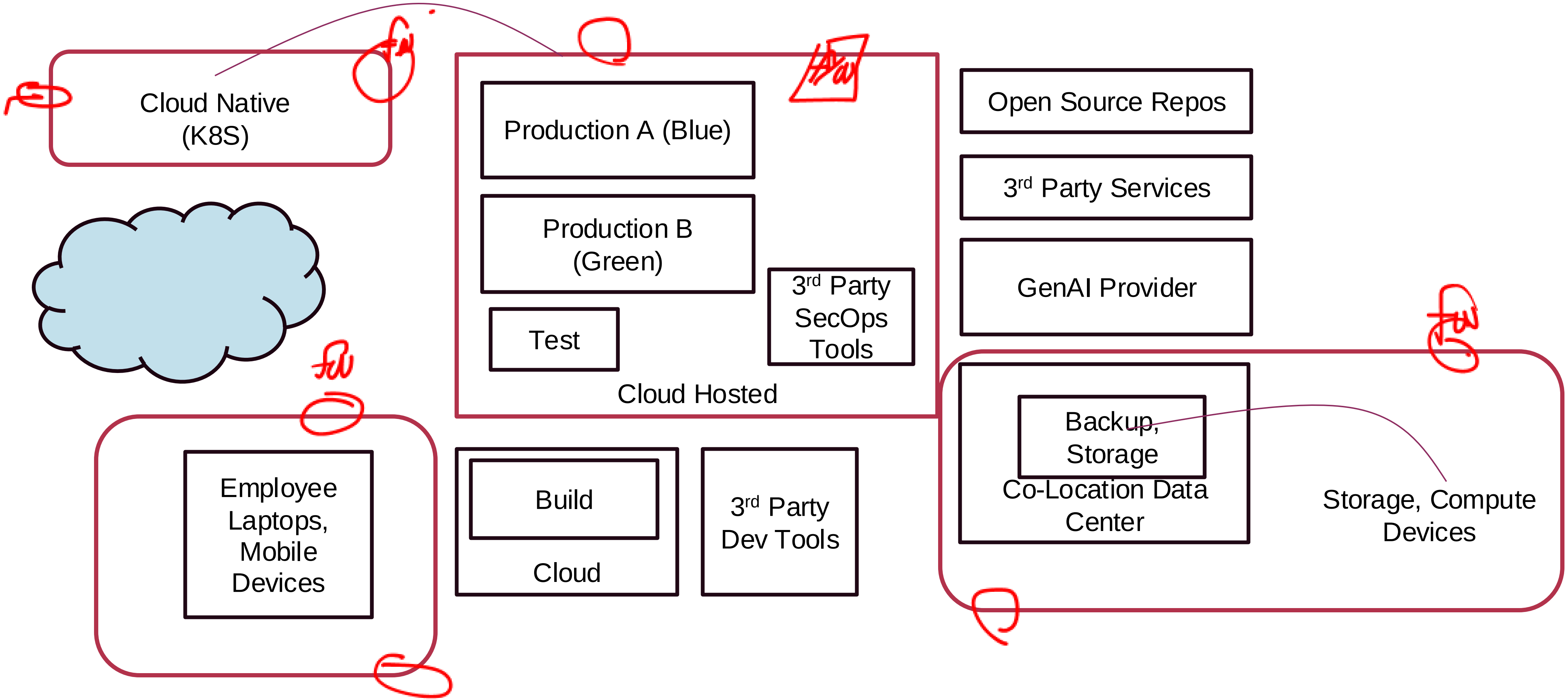
Devices

Workstations, phones, tablets, servers, containers, hosts, compute, peripherals storage devices, network devices, web cameras, IoT, infrastructure, etc.

This asset class includes the operating systems and firmware 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.

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.



DEVICES: High Level Zero Trust Maturity Model Categories and Goals

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.

ZTA Focus	Policy Enforcement & Compliance Monitoring	Asset & Supply Chain Risk Management	Resource Access	Device Threat Protection AV EDR
Desc	Focus is on management and enforcement of policies that establish the baselines and controls that are to be in place and enforced	Management of physical and virtual assets, internally and as found in the supply chain	Overall consideration of devices or virtual asset posture as part of access to resources.	Deploy, update, real time manage threat protection capabilities for devices and virtual assets and have robust third party / supply chain discipline
Maturity Goal	Move to automated compliance, vulnerability management of devices for continuous compliance	Move to automated inventory of assets including supply chain software and manages risk of supply chain failures	Move to dynamic, real time device posture & risk-based access	Centralized, automated device threat protection

DEVICES: Zero Trust Maturity Levels

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

Traditional	Initial	Advanced	Optimized
• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics
• *No configuration standards, manufacturer recommended*	• *Locally defined configuration*	• *Industry standards for configuration* CIS	• *Federal/Regulatory standards* DISA STIG

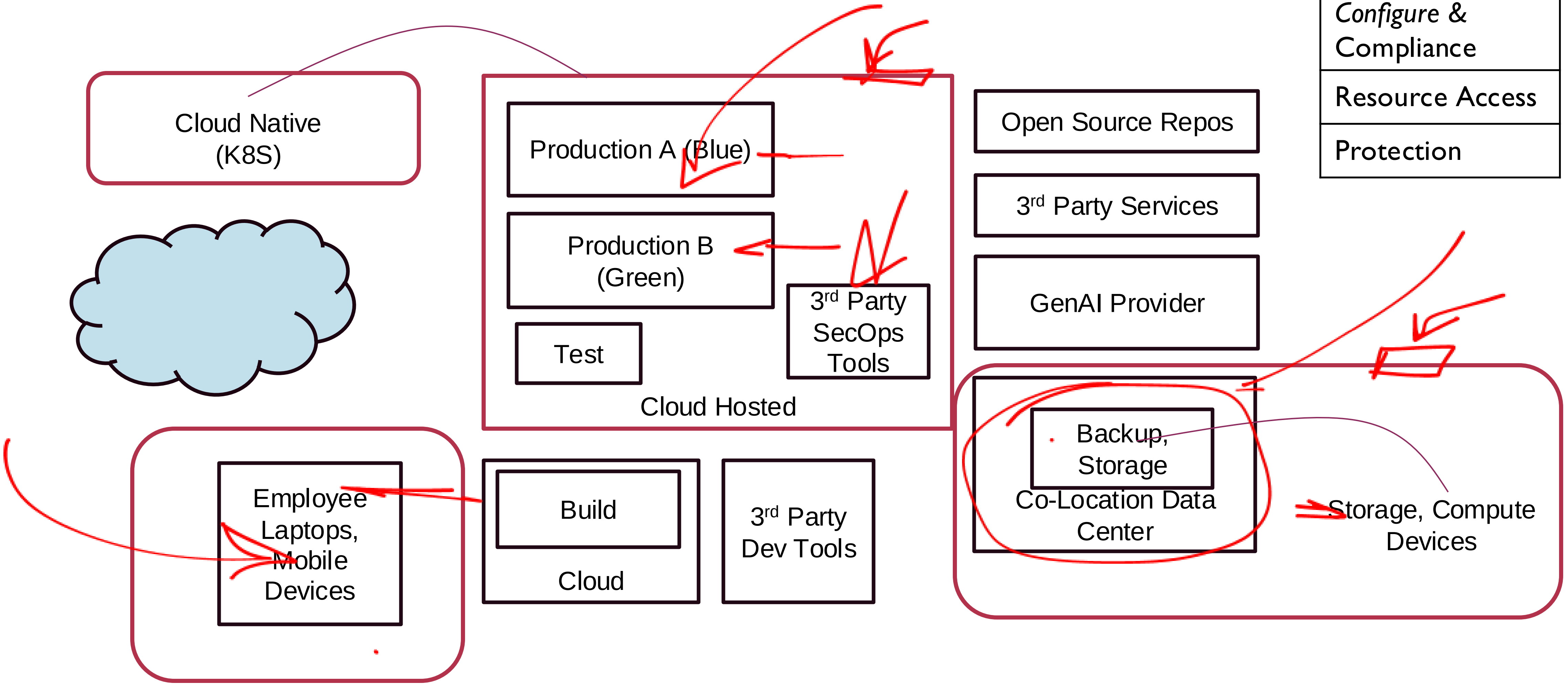
Figure 4: High Level Zero Trust Maturity Model Overview

DEVICES: Zero Trust Maturity Levels Broken down by function / goal

	Traditional	Initial	Advanced	Optimized
Inventory	Manually tracking of device inventory	All physical assets tracked	All physical, most virtual tracked (start to introduce automation to assist)	Continuous (automated) identification of physical, virtual asset inventory
Configure (*)	*Limited config stds*	*"Local" standards*	*CIS Benchmarks*	*DISA STIG Standards*
Compliance	Limited visibility into device compliance posture	Limited enforcement of device compliance	Enforced compliance + integrated threat protection	Continuous (automated) enforced compliance + integrated threat protection
Resource Access	No defined criteria enforced for access	Limited device-based access control	Initial resource access depends on device posture	Resource access depends on real-time device risk analytics
Protection	Manual deployment of protections to some devices	Some protections delivered via automation	Enforced compliance + integrated threat protection	Continuous (automated) enforced compliance + integrated threat protection

(*) Configure includes ensuring patched!!!

- Inventory
- *Configure* & Compliance
- Resource Access
- Protection



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, Mobile Devices

Build

Cloud

3rd Party Dev Tools

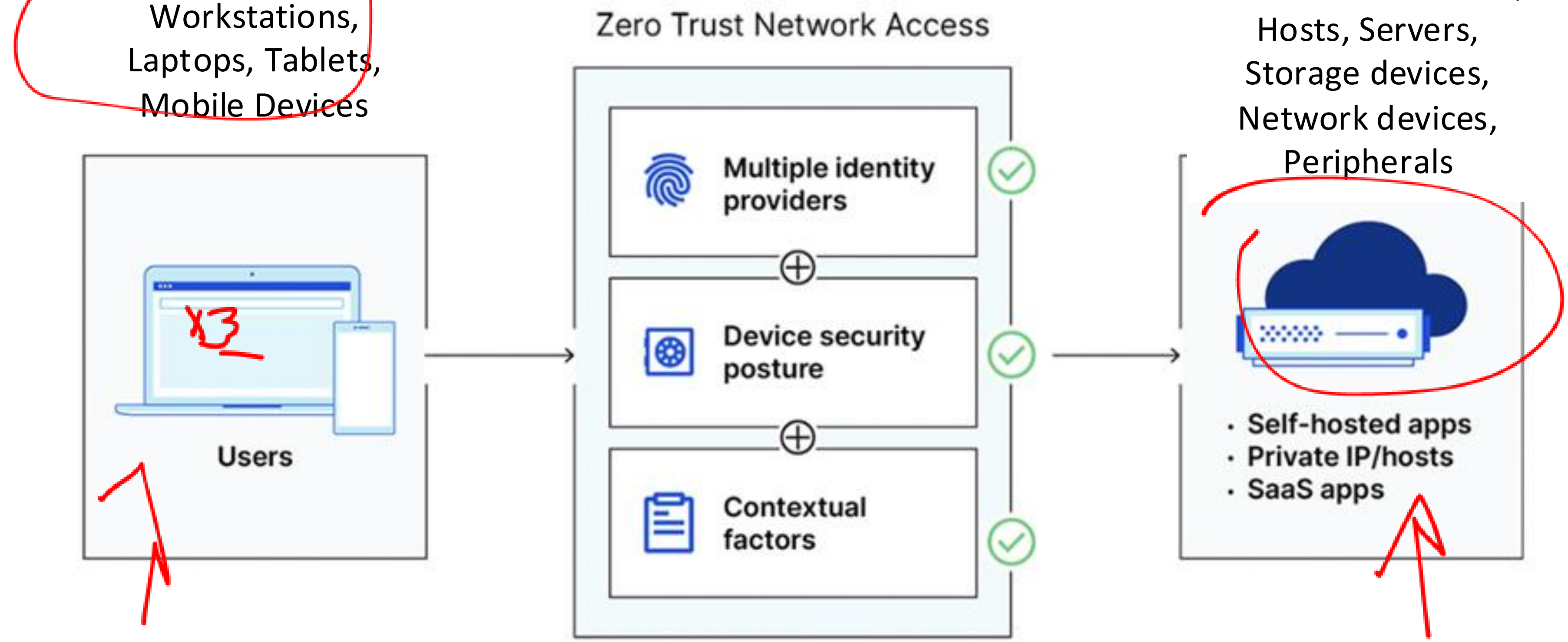
DEVICES

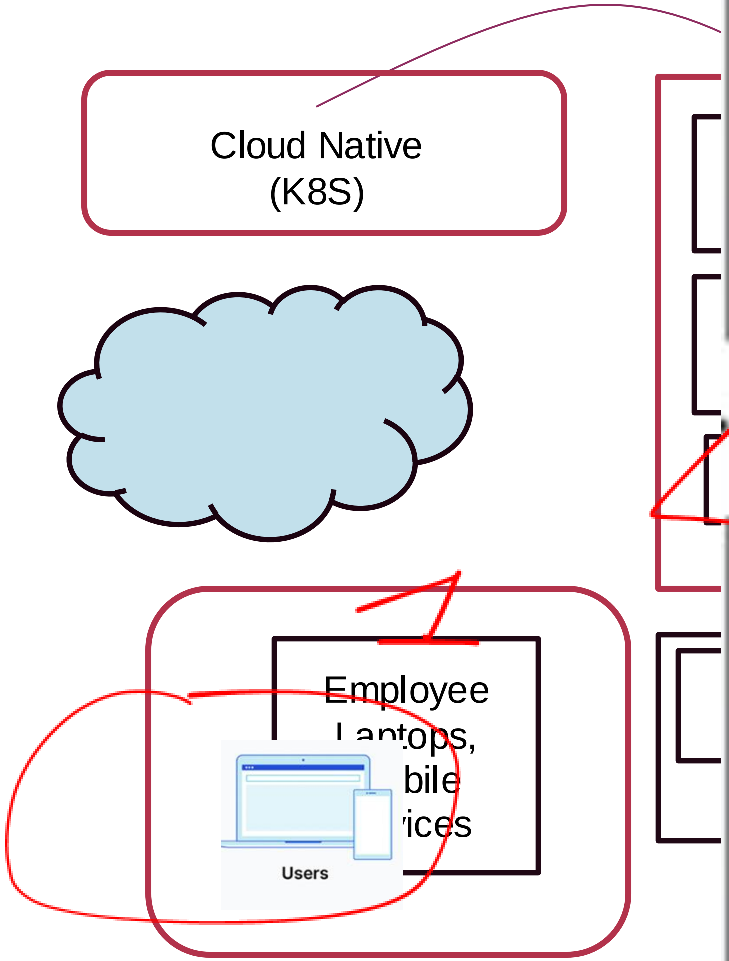
IOT: Badge Readers, CCTV, Video Conference

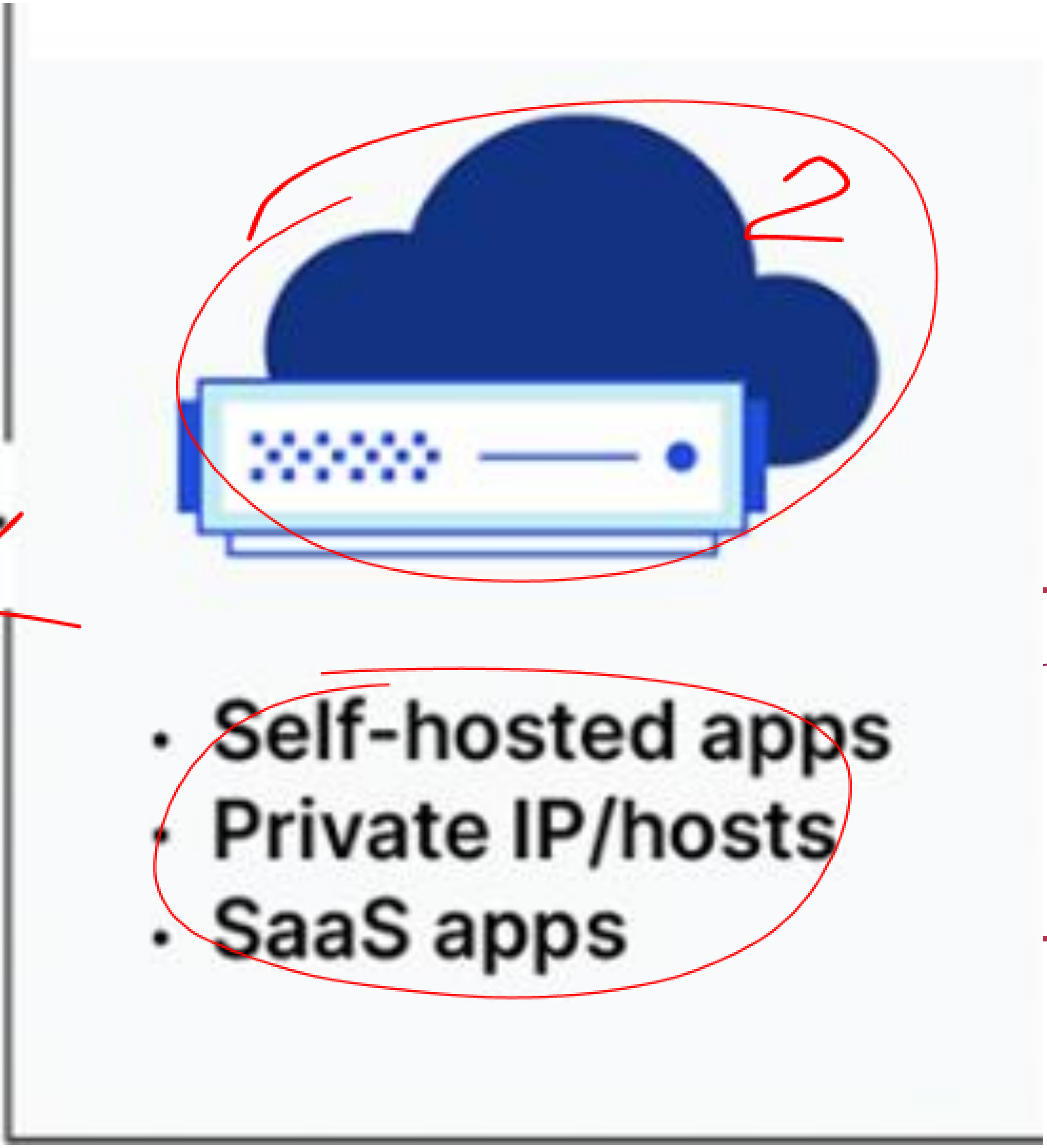
Zero Trust requires strict verification for (every user and) every device before authorizing them to access internal resources.

Devices : Workstations, Laptops, Tablets, Mobile Devices

Devices : Containers, Hosts, Servers, Storage devices, Network devices, Peripherals







- Self-hosted apps
- Private IP/hosts
- SaaS apps

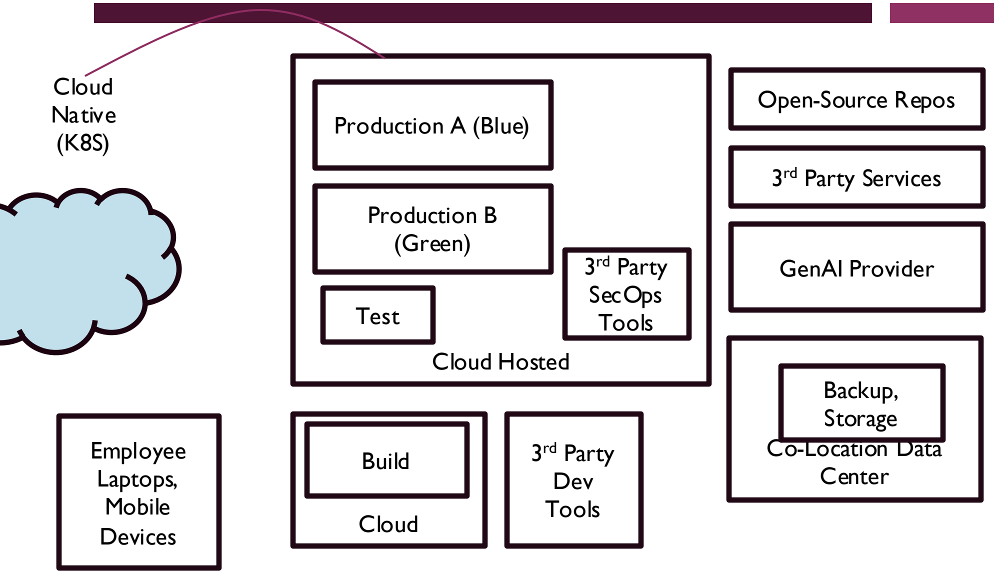
Inventory

Configure &
Compliance

Resource Access

Protection

Storage, Compute
Devices



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

Employee Laptops, Mobile Devices

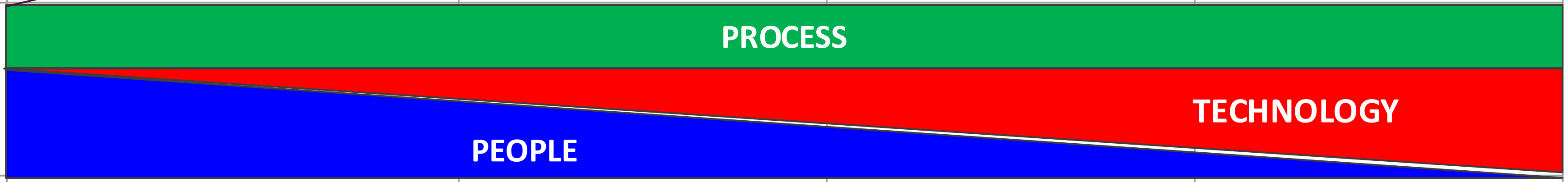
Build

Cloud

3rd Party Dev Tools

	Traditional	Initial	Advanced	Optimized
Inventory	Manually tracking of device inventory	All physical assets tracked	All physical, most virtual tracked (start to introduce automation to assist)	Continuous (automated) identification of physical, virtual asset inventory
Compliance	Limited visibility into device compliance posture	Limited enforcement of device compliance	Enforced compliance + integrated threat protection	Continuous (automated) enforced compliance + integrated threat protection
Resource Access	No defined criteria enforced for access	Limited device-based access control	Initial resource access depends on device posture	Resource access depends on real-time device risk analytics
Protection	Manual deployment of protections to some devices	Some protections delivered via automation	Enforced compliance + integrated threat protection	Continuous (automated) enforced compliance + integrated threat protection

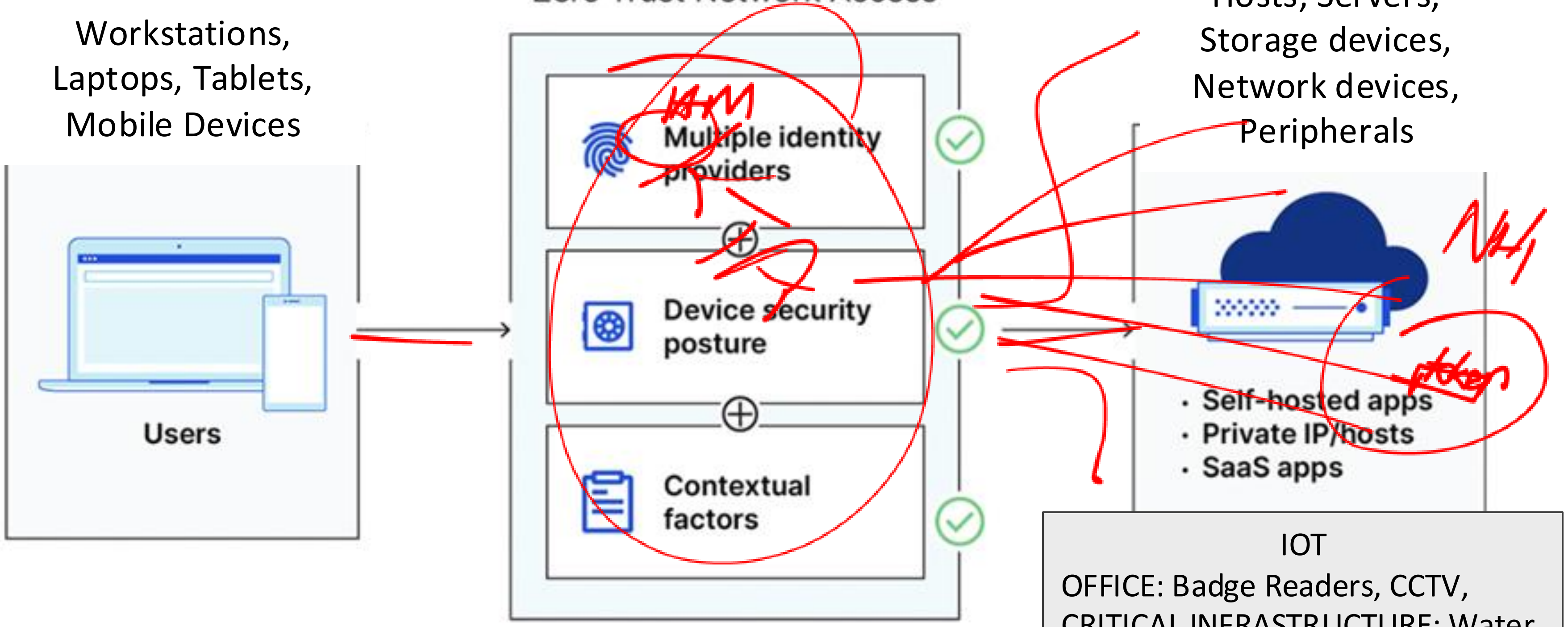
Traditional	Initial	Advanced	Optimized
END USER **Option 1**			
- Limited compliance visibility of end user devices - No (server) device criteria for resource access	- All physical assets ✓ tracked - End user device (excl mobile phone, tables) managed to company standards	- All end user device (excl mobile, table) are tracked - All server, container, network devices are tracked - End user ”ZTA” access depends on device posture	- Continuous analysis via EDR/MDR for end user device (excl mobile phone, tablet)
“PRODUCTION” **Option 2**			
- Manually tracking end user device inventory - Limited compliance visibility - No device criteria for end user resource access - Manual deployment of threat protections to some devices	- All physical assets tracked - Limited device-based access control and compliance enforcement - Some protections delivered via automation	- Most physical and virtual assets are tracked - Enforced compliance implemented with integrated threat protections - Initial resource access depends on device posture	- Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections - Resource access depends on real-time device risk analytics

CYBERSECURITY FRAMEWORK	**IDENTIFY**	**PROTECT**	**DETECT**	**RESPOND & RECOVER**
DEVICES	Inventory – API, Scanning Client-side tools (MDM) CMDB	EDR SIEM Device Hardening Next Gen AV	EDR SIEM	Incident Response
				
ZTMM	**TRADITIONAL**	**INITIAL**	**ADVANCED**	**OPTIMIZED**

DEVICES

Zero Trust requires strict verification for (every user and) every device before authorizing them to access internal resources.

Devices : Workstations, Laptops, Tablets, Mobile Devices

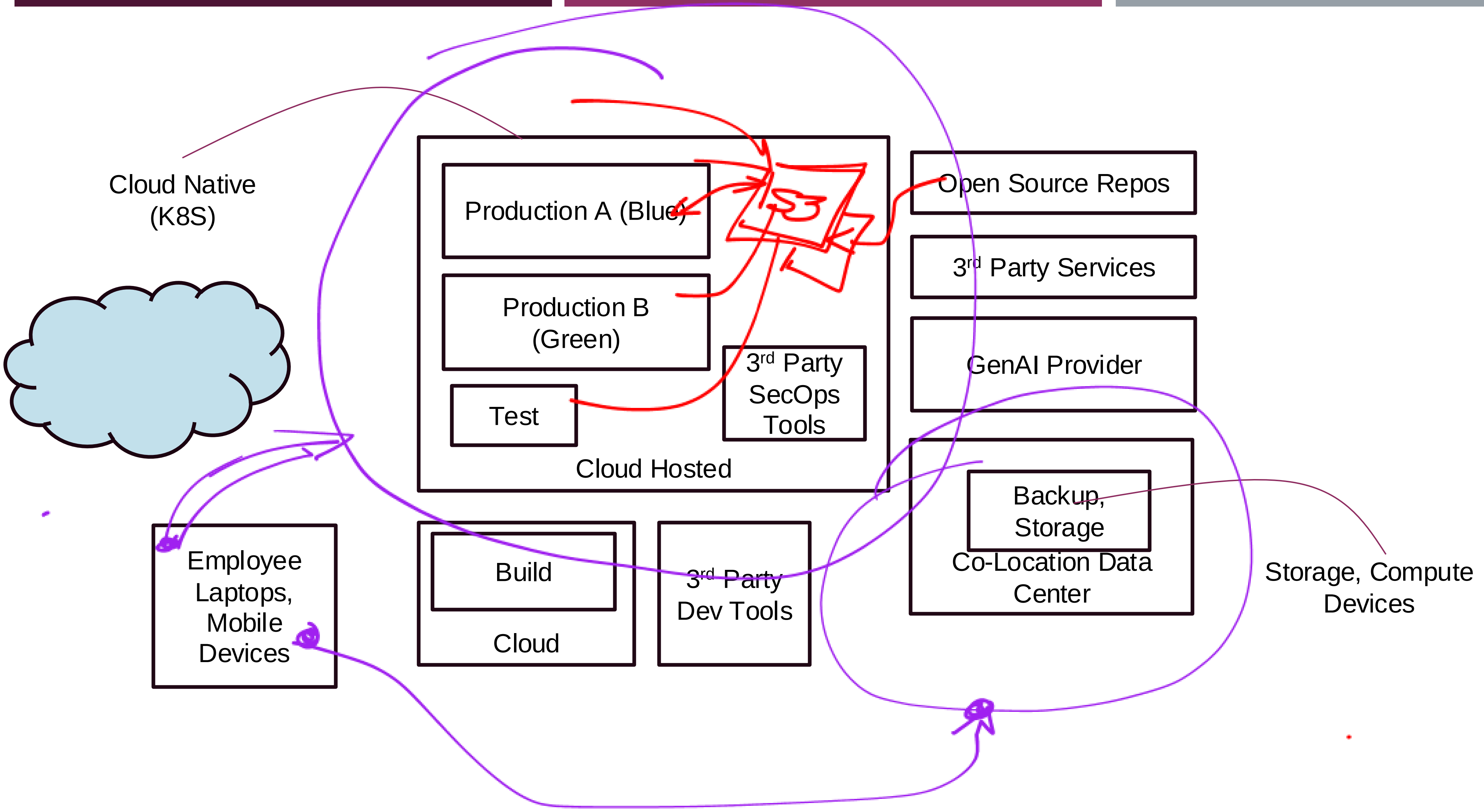


Devices : Containers, Hosts, Servers, Storage devices, Network devices, Peripherals

IOT
OFFICE: Badge Readers, CCTV, Video Conference

IOT
OFFICE: Badge Readers, CCTV,
CRITICAL INFRASTRUCTURE: Water Treatment, Power Grid
HOME: Routers, Washer/Dryer/Fridge, Airtags, etc

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, Mobile Devices

Build

Cloud

3rd Party Dev Tools

QUICK POLL

- *Is Zero Trust Maturity Model / Devices more easily and naturally applied to User devices (laptops, tables, mobile devices) or to Servers (Physical & Virtual)?*
- *Rank in order of priority the overall coverage of device protection by device "type"*
  - *End user devices (laptops, mobile devices)*
  - *Servers (physical/virtual compute, storage)*
  - *Specialty (physical network, storage)*
  - ~~*IoT*~~

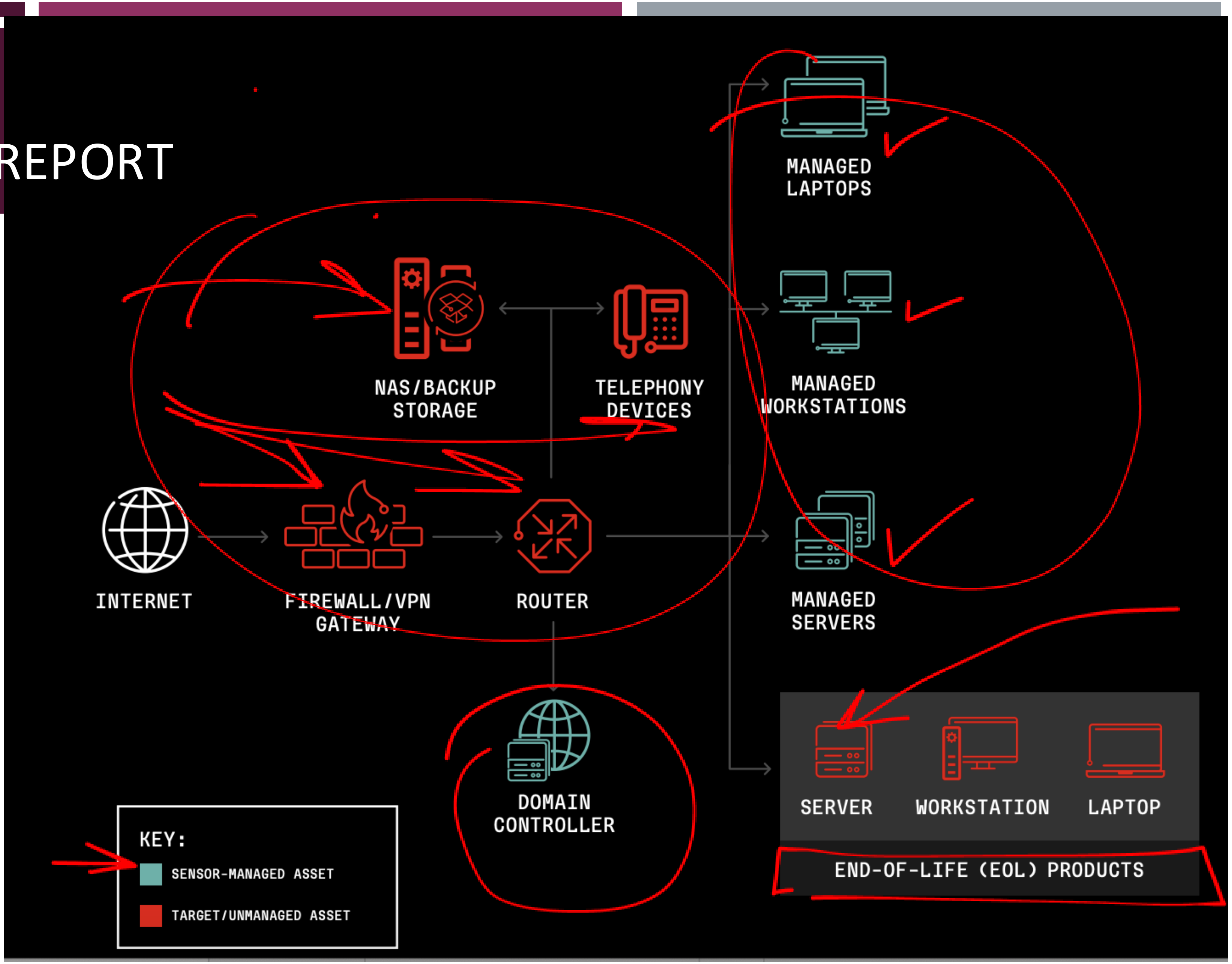
10 min

BREAK

BACK 6:23 ET

CROWDSTRIKE
GLOBAL 2024 THREAT REPORT

Threat actors have adapted to the enhanced visibility of traditional endpoint detection and response (EDR) sensors by altering their exploitation tactics for initial access and lateral movement. They are now targeting the network periphery, where defender visibility is reduced by the possibility that endpoints may lack EDR sensors or cannot support sensor deployment (Figure 3).



DEVICES – DON’T FORGET NETWORK DEVICES https://cyberscoop.com/edge-device-vulnerabilities-fuel-attack-sprees/

- Edge device vulnerabilities fueled attack sprees in 2024
  - The most consequential cyberattacks observed by Darktrace last year were linked to software defects in firewalls and perimeter network technologies.
- Vendors that supply security hardware and services were responsible for four of the six mostly commonly exploited vulnerabilities observed by Darktrace: a pair of vulnerabilities affecting Ivanti products (CVE-2023-46805 and CVE-2024-21887); a trio impacting Palo Alto Networks firewalls running PAN-OS (CVE-2024-3400, CVE-2024-0012 and CVE-2024-9474); and a vulnerability affecting Fortinet’s network management tool FortiManager (CVE-2024-47575).
- Forty percent of the malicious activity observed by Darktrace researchers in the first half of last year involved the exploitation of internet-facing devices.

60% →

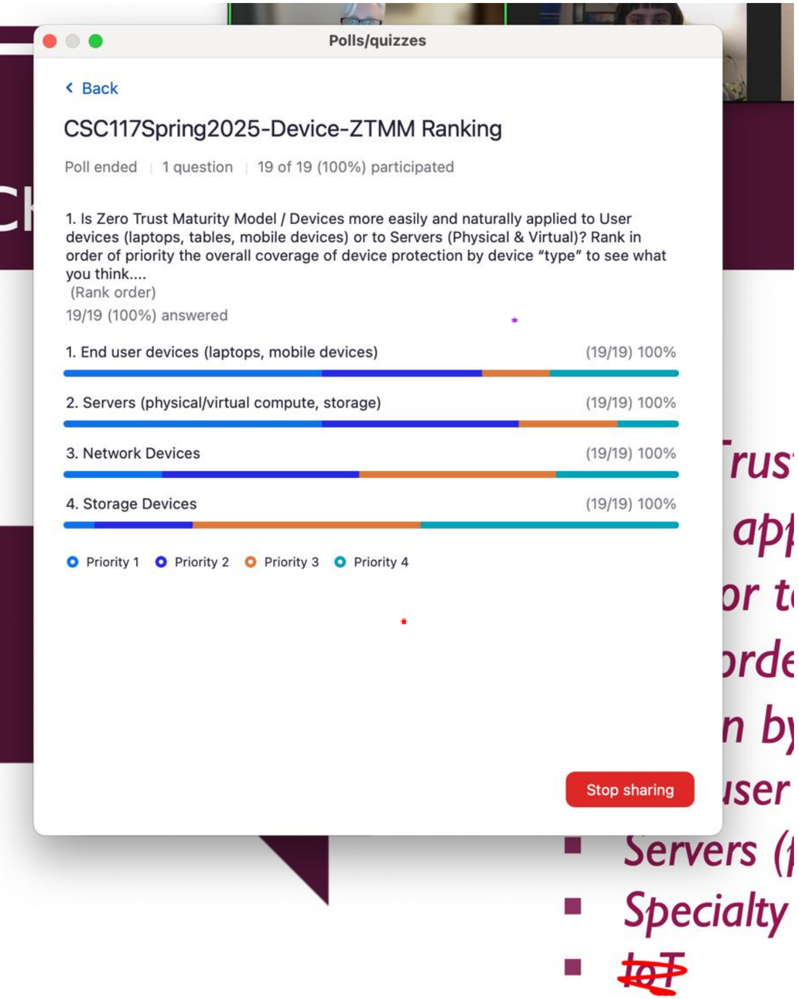
CROWDSTRIKE GLOBAL 2024 THREAT REPORT
https://go.crowdstrike.com/global-threat-report-2024-thank-you.html

- 2024 Report, 2023 Observation:
  - Unmanaged network appliances — particularly edge gateway devices — remained the most routinely observed initial access vector for exploitation during 2023. These devices are commonly based on obsolete architecture, leading to broadly exploited vulnerabilities in firewall and VPN platforms from Cisco (CVE2023-20198), Citrix (CVE-2023-3519, CVE-2023-4966) and F5 (CVE-2023-46747).

EOL

- 2024 Observations
  - 30 Known Exploitability Vulnerabilities in 2024 against
    - Cisco, Fortinet, Ivanti, Palo Alto
  - Aside from “its stinks to be one of those vendors what does this tell you?”

QUICK DISCUSSION POLL



CSC117Spring2025-Device-ZTMM Ranking

Poll ended | 1 question | 19 of 19 (100%) participated

1. Is Zero Trust Maturity Model / Devices more easily and naturally applied to User devices (laptops, tables, mobile devices) or to Servers (Physical & Virtual)? Rank in order of priority the overall coverage of device protection by device "type" to see what you think....
(Rank order)
19/19 (100%) answered

1. End user devices (laptops, mobile devices) (19/19) 100%
2. Servers (physical/virtual compute, storage) (19/19) 100%
3. Network Devices (19/19) 100%
4. Storage Devices (19/19) 100%

○ Priority 1 ○ Priority 2 ○ Priority 3 ○ Priority 4

Trus
app
or t
orde
n by
user
- Servers (
- Specialty
- ~~IoT~~

- *Do you agree with the poll after seeing the Crowdstrike & 2024 KEV results?*
- *What does this tell you about Networks v Devices in ZTMM?*

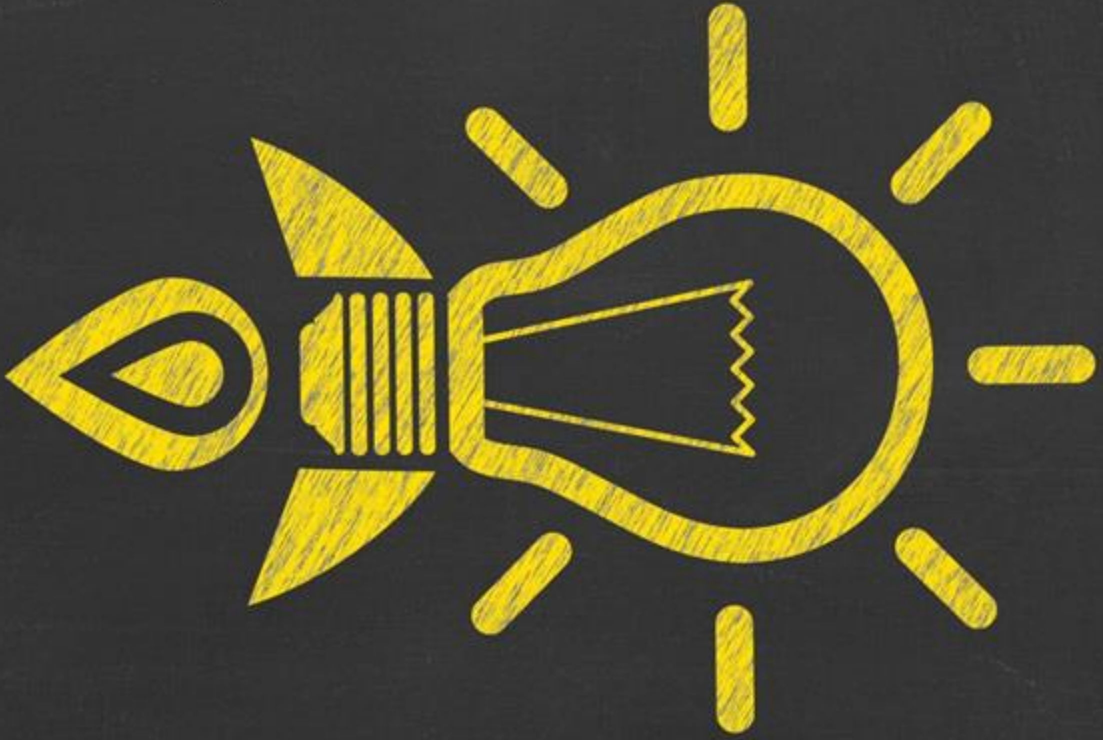
DEVICE ZERO TRUST

Option	Policy Enforcement & Compliance Monitoring	Asset & Supply Chain Risk Management	Resource Access	Device Threat Protection
1	(Traditional) You have limited ability to inspect device compliance for devices connecting to your network configuration patching	(Initial) You maintain a list of known computers/phones on your network but you do not block unknown ones	(Initial) Your network is configured network so that all devices must be at latest firmware level and O/S level to be allowed on the network You do not check configuration / baselines of computers joining your network	(Traditional) You have manually installed anti-virus to all of your executive-used devices
2	(Initial) You receive self-reported device characteristics (e.g., keys, tokens, users, etc., on the device) from devices on joining the network. You have a manual process to approve software use and push updates and configuration changes to devices.	(Traditional) You do not track (laptop/mobile) devices that join your network. You have a list of servers on your production network that is updated monthly	(Traditional) You allow any devices to join your network BYOD → avoid	(Initial) You require that all new computers joining your network have an approved A/V (and will block them from joining if they don't)

ANTICIPATED END OF LECTURE 5

REFERENCE

REMINDERS



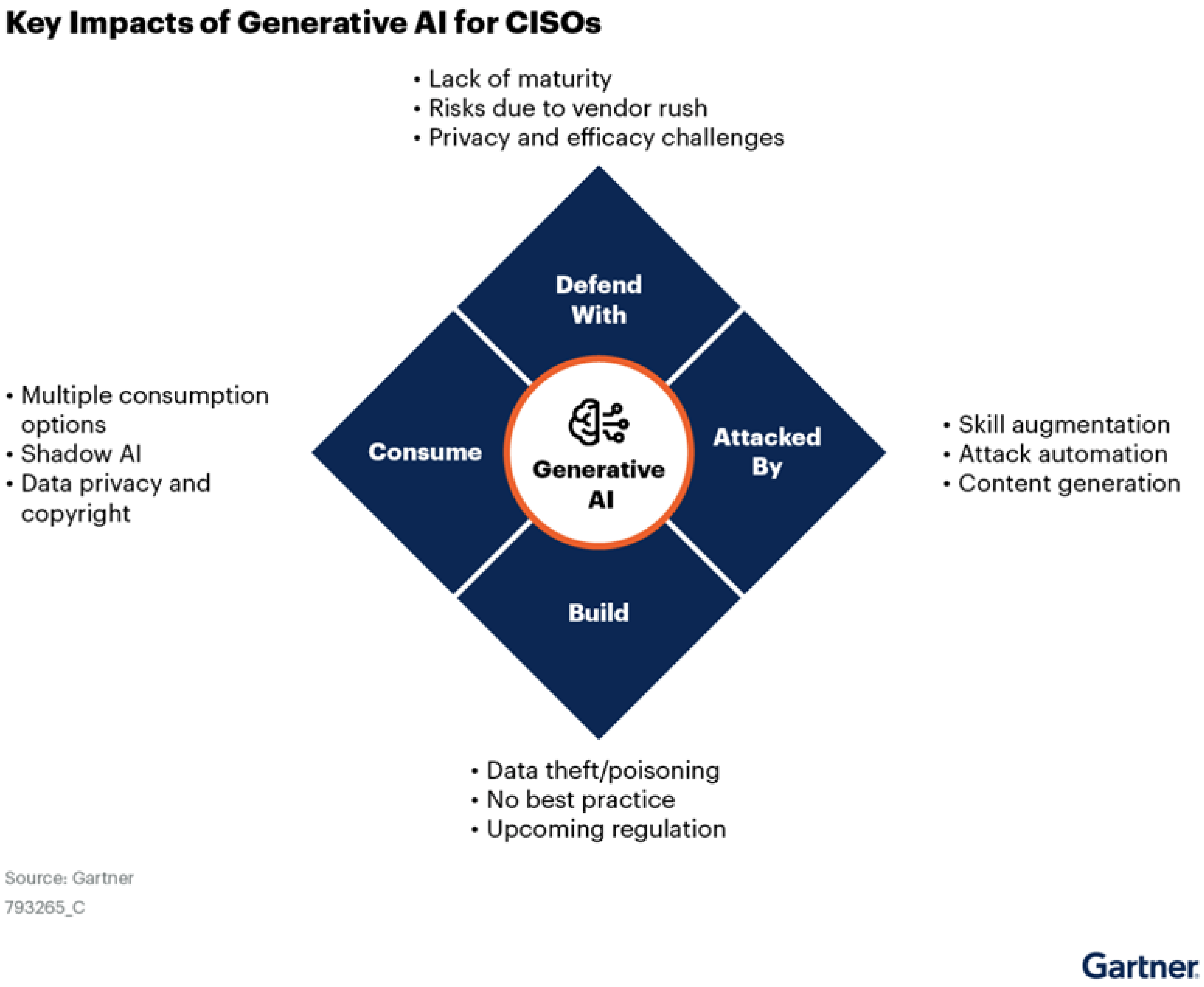
REFERENCE

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

- 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

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 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.

ZTA Focus	Policy Enforcement & Compliance Monitoring	Asset & Supply Chain Risk Management	Resource Access	Device Threat Protection
Description	Focus is on management and enforcement of policies that establish the baselines and controls that are to be in place and enforced	Management of physical and virtual assets, internally and as found in the supply chain (implicitly includes third party applications as assets)	Overall management of devices or virtual assets used to access resources.	Deploy, update, real time manage threat protection capabilities for devices and virtual assets
Maturity Goal	Move to automated compliance, vulnerability management of devices for continuous compliance	Move to automated inventory of assets including supply chain software and manages risk of supply chain failures	Move to dynamic, real time device posture & risk-based access	Centralized, automated device threat protection
Tools	CIS/STIG Benchmarks			EDR, A/V
In the News				

REFERENCE

Policy Enforcement & Compliance Monitoring

Traditional	Initial	Advanced	Optimal
Agency has limited, if any, visibility (i.e., ability to inspect device behavior) into device compliance with few methods of enforcing policies or managing software, configurations, or vulnerabilities.	Agency receives self-reported device characteristics (e.g., keys, tokens, users, etc., on the device) but has limited enforcement mechanisms. Agency has a preliminary, basic process in place to approve software use and push updates and configuration changes to devices.	Agency has verified insights (i.e., an administrator can inspect and verify the data on device) on initial access to device and enforces compliance for most devices and virtual assets. Agency uses automated methods to manage devices and virtual assets, approve software, and identify vulnerabilities and install patches.	Agency continuously verifies insights and enforces compliance throughout the lifetime of devices and virtual assets. Agency integrates device, software, configuration, and vulnerability management across all agency environments, including for virtual assets.

REFERENCE

Asset & Supply Chain Risk Management

Traditional	Initial	Advanced	Optimal
Agency does not track physical or virtual assets in an enterprise-wide or cross-vendor manner and manages its own supply chain acquisition of devices and services in ad hoc fashion with a limited view of enterprise risks.	Agency tracks all physical and some virtual assets and manages supply chain risks by establishing policies and control baselines according to federal recommendations using a robust framework, (e.g., NIST SCRM.)	Agency begins to develop a comprehensive enterprise view of physical and virtual assets via automated processes that can function across multiple vendors to verify acquisitions, track development cycles, and provide third-party assessments.	Agency has a comprehensive, at- or near- real-time view of all assets across vendors and service providers, automates its supply chain risk management as applicable, builds operations that tolerate supply chain failures, and incorporates best practices.

REFERENCE

Resource Access

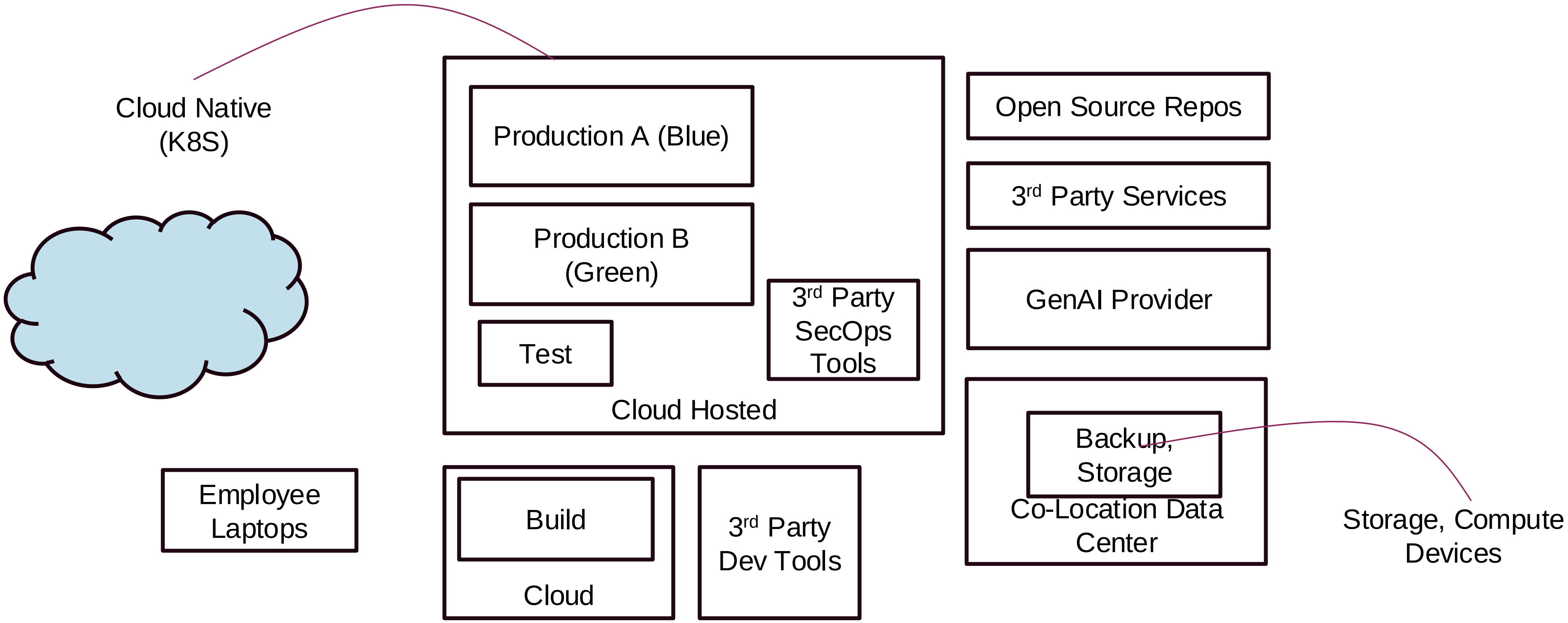
Traditional	Initial	Advanced	Optimal
Agency does not require visibility into devices or virtual assets used to access resources.	Agency requires some devices or virtual assets to report characteristics then use this information to approve resource access.	Agency’s initial resource access considers verified device or virtual asset insights.	Agency’s resource access considers real-time risk analytics within devices and virtual assets.

REFERENCE

Device Threat Protection

Traditional	Initial	Advanced	Optimal
Agency manually deploys threat protection capabilities to some devices.	Agency has some automated processes for deploying and updating threat protection capabilities to devices and to virtual assets with limited policy enforcement and compliance monitoring integration.	Agency begins to consolidate threat protection capabilities to centralized solutions for devices and virtual assets and integrates most of these capabilities with policy enforcement and compliance monitoring.	Agency has a centralized threat protection security solution(s) deployed with advanced capabilities for all devices and virtual assets and a unified approach for device threat protection, policy enforcement, and compliance monitoring.

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

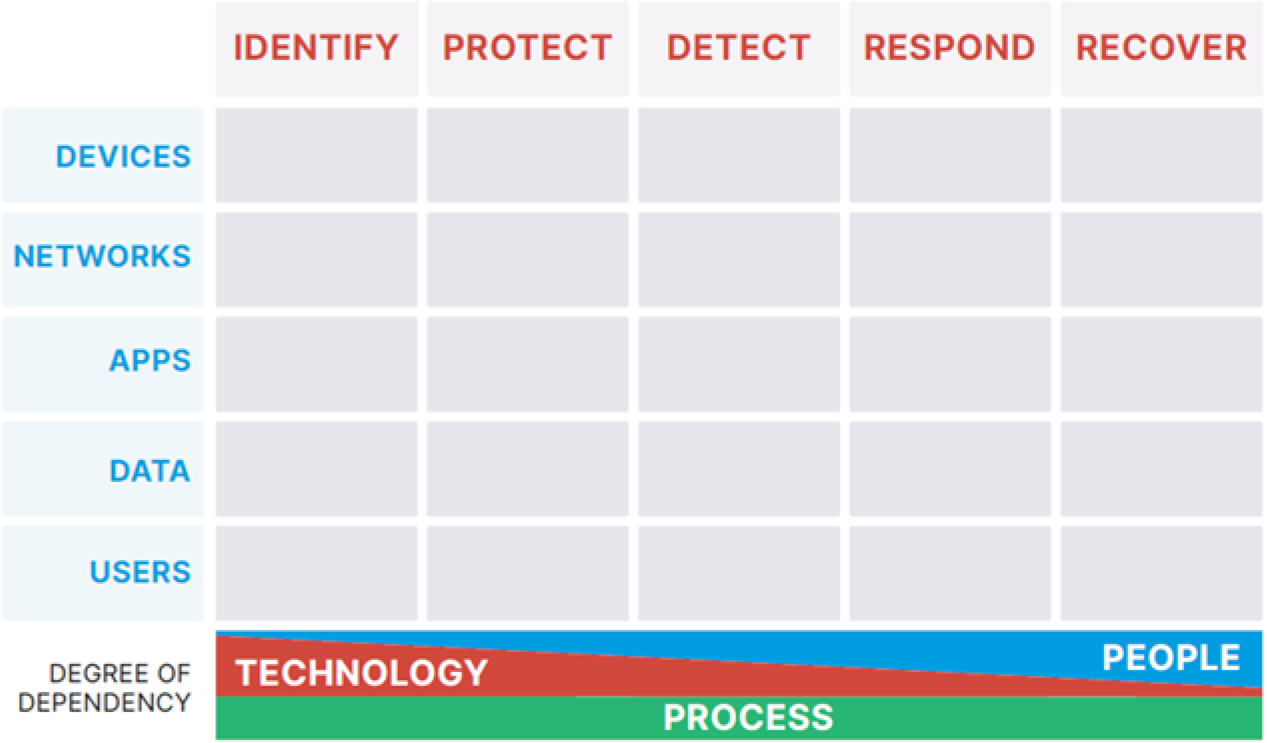
Build

Cloud

3rd Party Dev Tools

REFERENCE

CYBER DEFENSE MATRIX



	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
DEVICES					
NETWORKS					
APPS					
DATA					
USERS					

DEGREE OF DEPENDENCY

TECHNOLOGY

PEOPLE

PROCESS

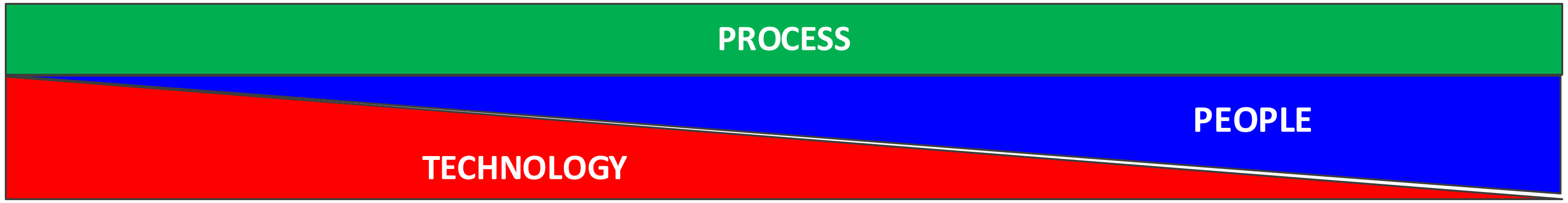
Figure 1: Cyber Defense Matrix

REFERENCE

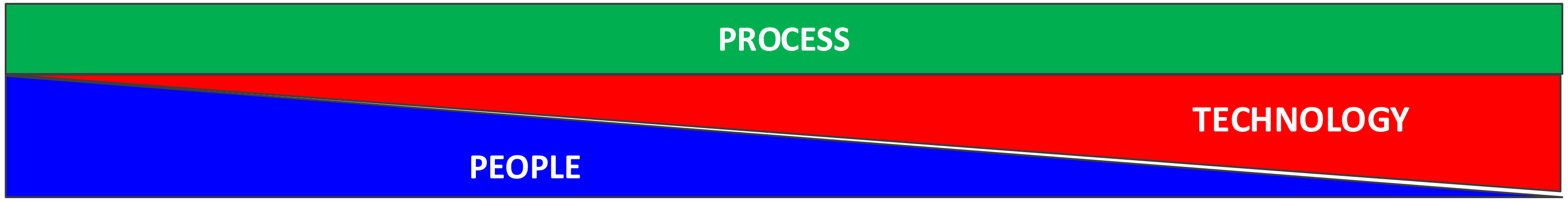
CISA ZERO TRUST MATURITY

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
USERS					USERS
ZTMM	TRADITIONAL	INITIAL	ADVANCED	OPTIMIZED	

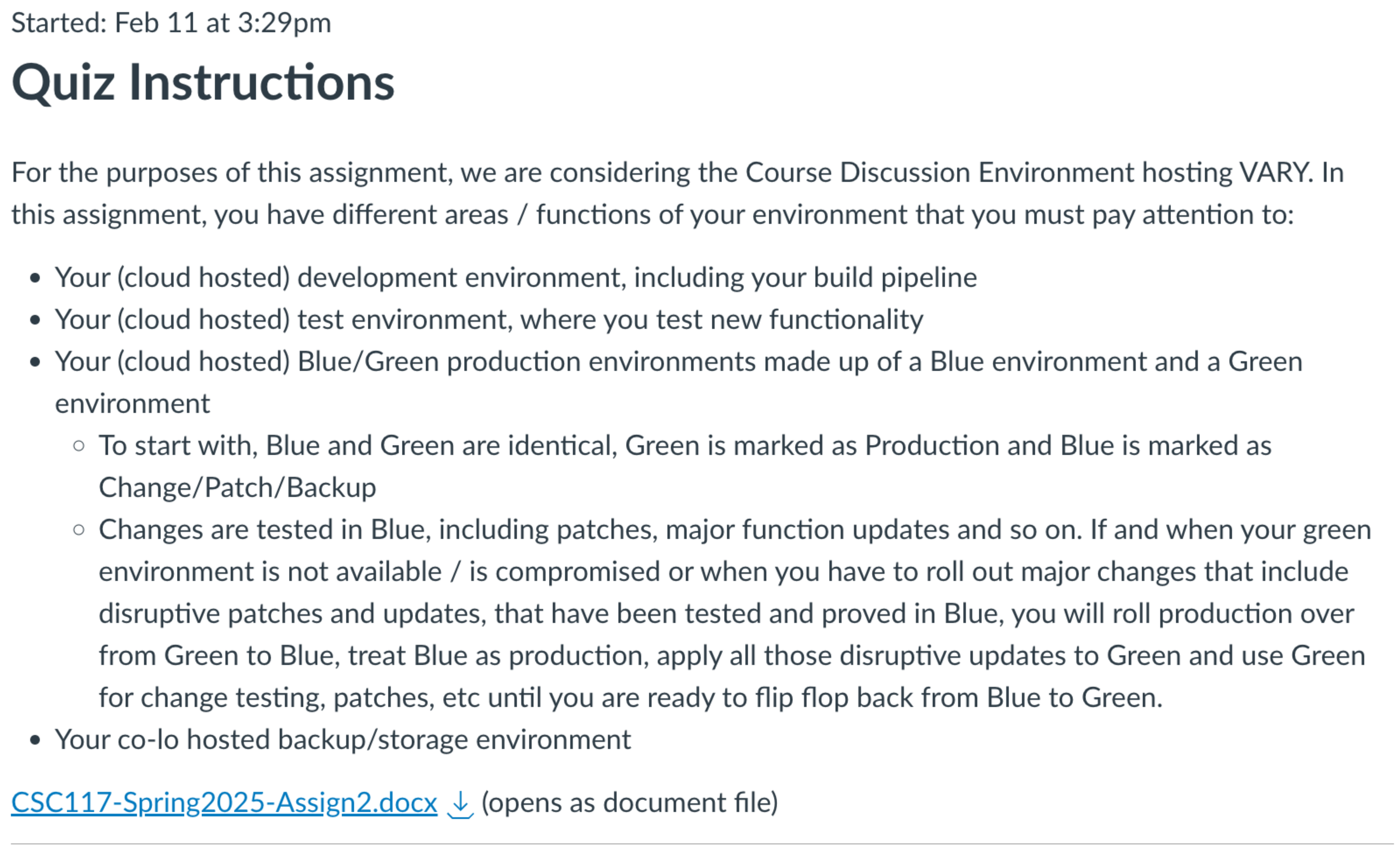


ASSIGNMENTS

ASSIGNMENT 2

Due Date: Mar 9

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)

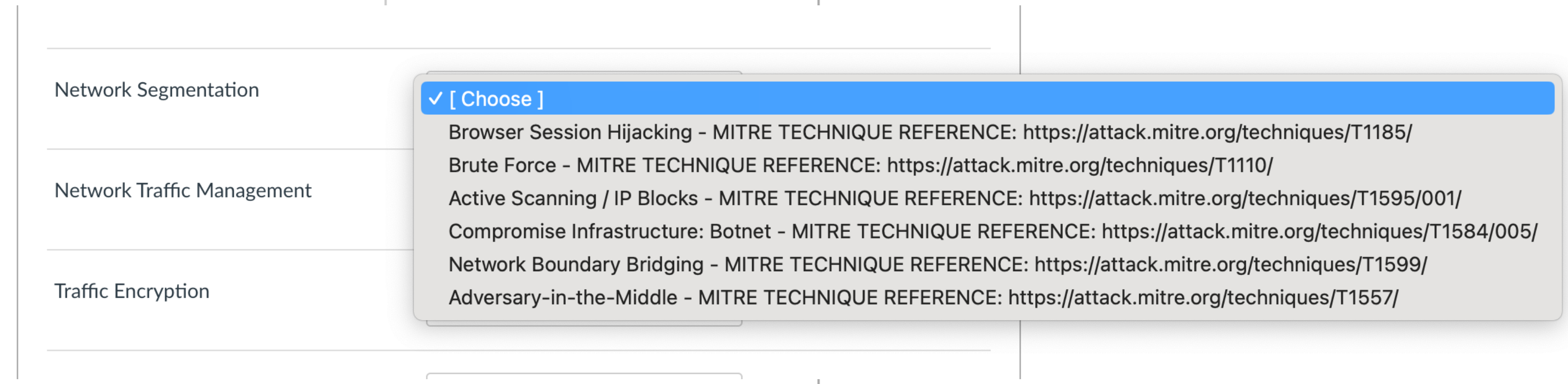
Question 1: Given the environment description above, map the best "fitting" MITRE ATT&CK technique to the Zero Trust Architecture network class. By "fit" we mean the MITRE ATT&CK technique that is the most effectively addressed / remediated / mitigated by the ZTA network class.

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]

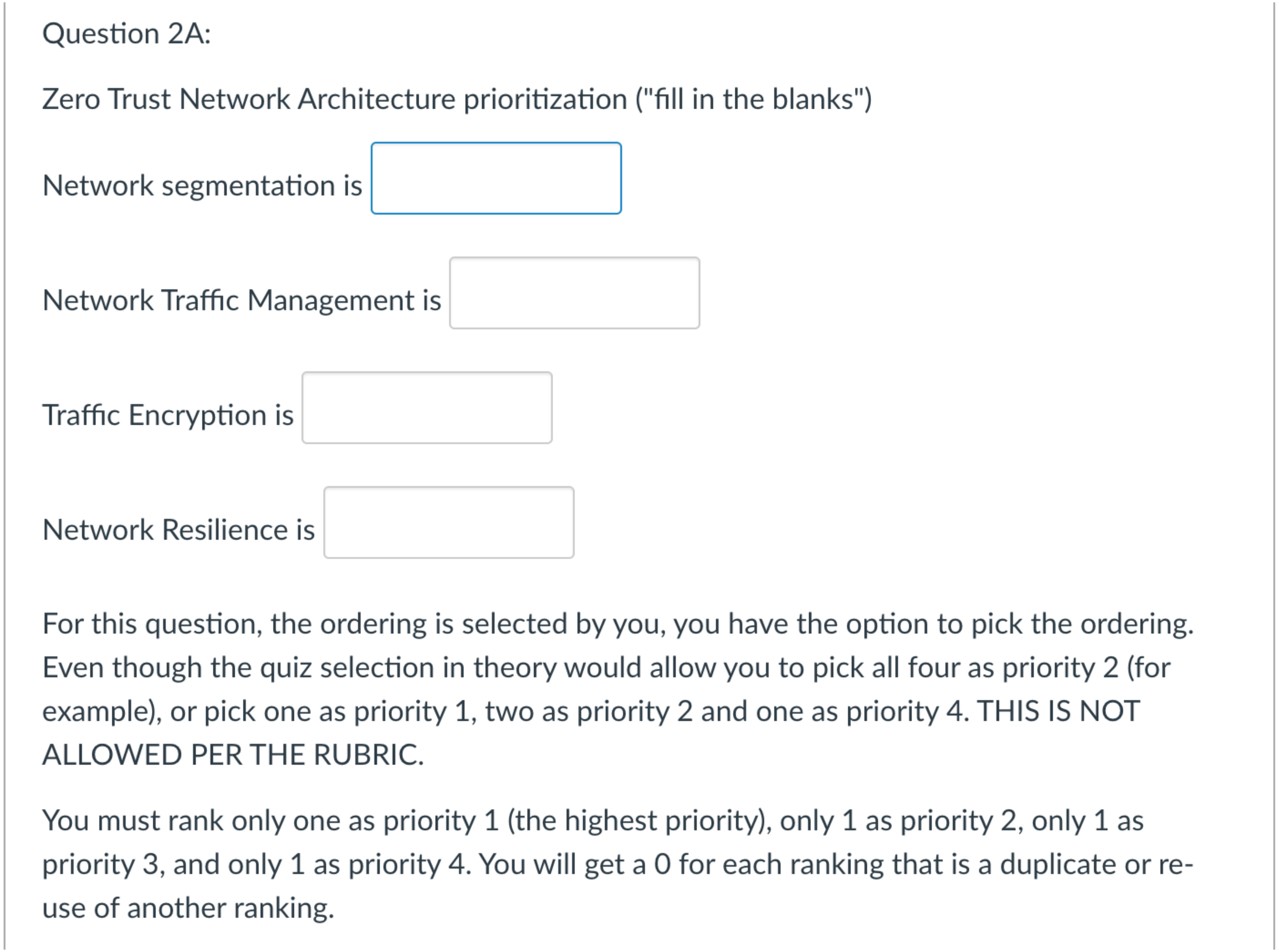


Network Segmentation

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 □

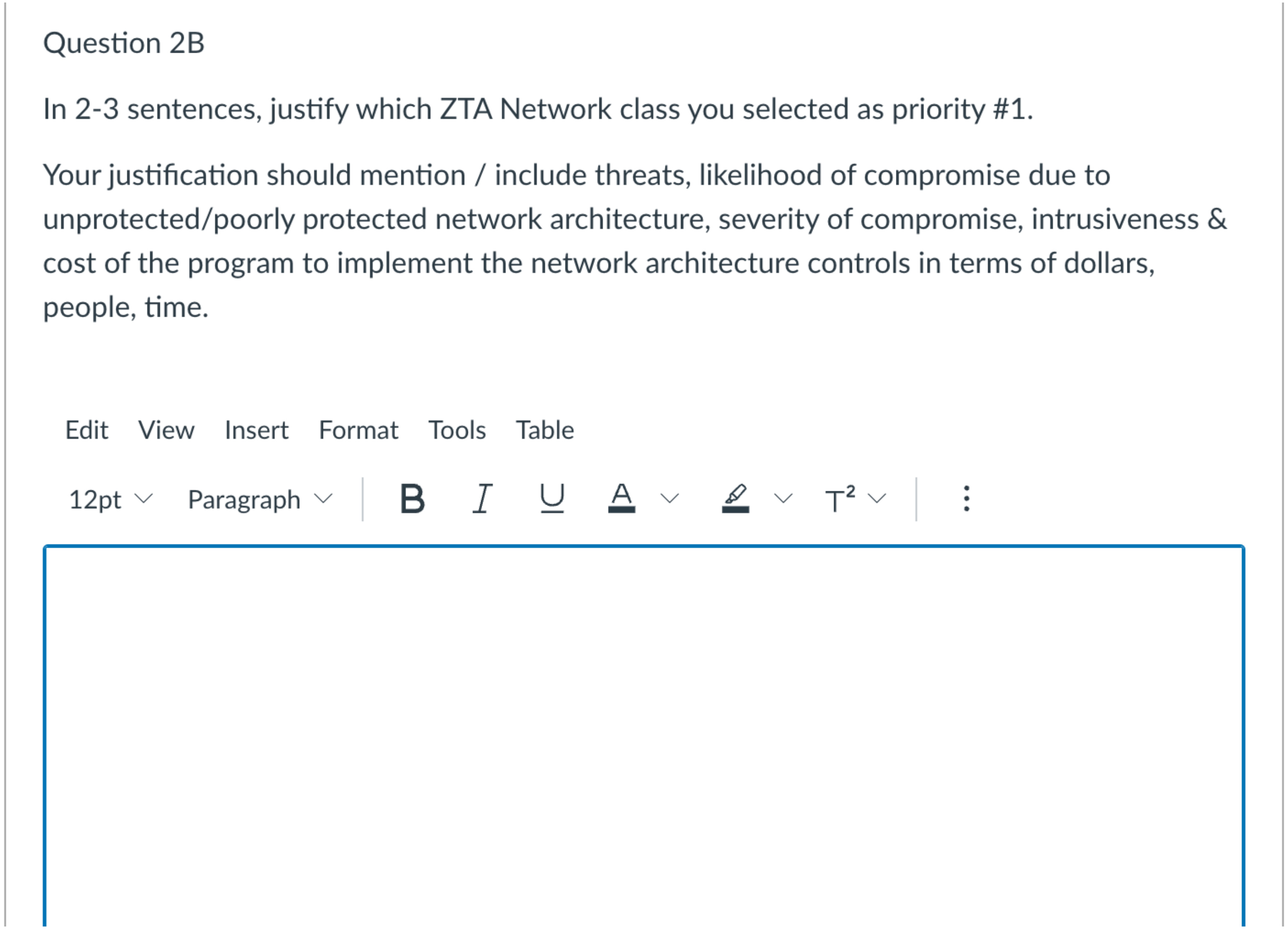
Network Traffic Management is □

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.

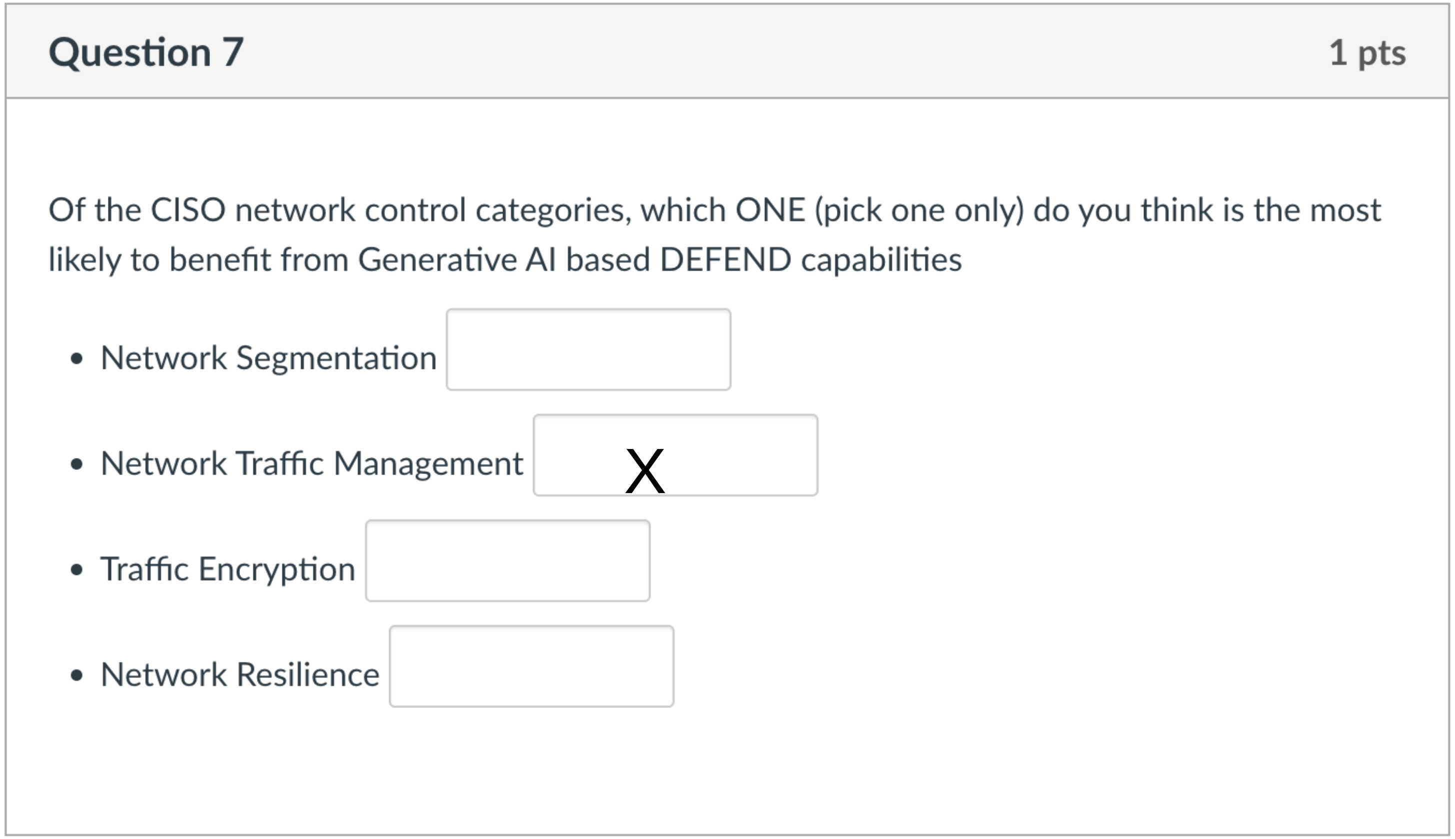
You must rank only one as priority 1 (the highest priority), only 1 as priority 2, only 1 as priority 3, and only 1 as priority 4. You will get a 0 for each ranking that is a duplicate or re-use of another ranking.



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”.

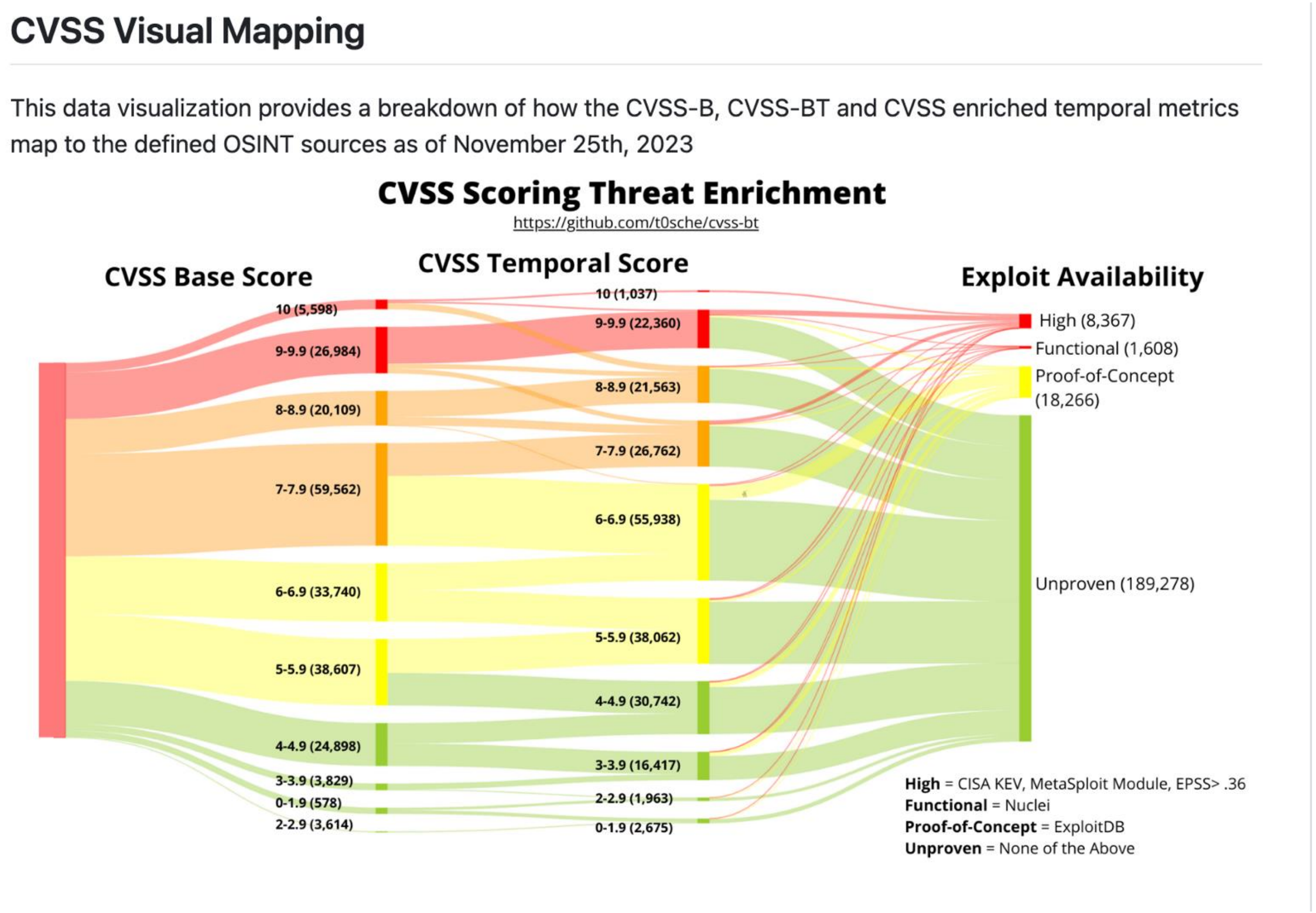
YELLOW DIG LAST WEEK

DISCUSSION LAST WEEK

- I participated asynch. What stood out to me in the breakout discussion regarding the poll results was the fact that each participant had slightly different reasoning, and each position was justifiable. This illustrated just how challenging it can be to prioritize one area over another, and that it will largely be determined by the environment you are operating in. Each of the participants in the break out came in with some preconceptions around the survey based on their personal work environments that informed which area they found to be most important. For example, in banking encryption might be the most important, while in a medical field availability and network resilience could potentially be the highest. The quote from the CISA ZTMM resonates with me, because it highlights the fact that each of these pillars stand on their own up to a certain point of maturity where further coordination is required. This class is really showing me how to frame conversations around these topics and help business partners make critical decisions around where to allocate resources based on the unique challenges of our environment.
- Our conversation stressed the importance of cross-pillar coordination. The discussion reinforced the CISA ZTMM quote that while each pillar (network segmentation, traffic management, traffic encryption, and network resilience) can progress at its own pace, maximum effectiveness occurs only when their capabilities are enterprise-wide.
- It does seem, sadly, that most of the conversations about software security are in fact conversations about budgets. I wish CISA would talk more about this.

YELLOW DIG – FAVORITE / TOPICAL / IN THE NEWS https://github.com/t0sche/cvss-bt

- If you are responsible for Patching and you look at this there are probably less than 3k CVE's that are 9.0 or higher with Exploits that are Functional or Highly available. Now if you marry those CVE's up to what's in your environment and you map that to risk of those assets. I am guessing you could automate this process and work yourself out of a job.



CVSS Visual Mapping

This data visualization provides a breakdown of how the CVSS-B, CVSS-BT and CVSS enriched temporal metrics map to the defined OSINT sources as of November 25th, 2023

High = CISA KEV, MetaSploit Module, EPSS> .36
Functional = Nuclei
Proof-of-Concept = ExploitDB
Unproven = None of the Above

A device refers to any asset (including its hardware, software, firmware, etc.) that can connect to a network, including serv ers, desktop and laptop machines, printers, mobile phones, IoT devices, networking equipment, and more.

ZTA Focus	Policy Enforcement & Compliance Monitoring	Asset & Supply Chain Risk Management	Resource Access	Device Threat Protection
Description	Focus is on management and enforcement of policies that establish the baselines and controls that are to be in place and enforced	Management of physical and virtual assets, internally and as found in the supply chain	Overall consideration of devices or virtual asset posture as part of access to resources.	Deploy, update, real time manage threat protection capabilities for devices and virtual assets and have robust third party / supply chain discipline
Maturity Goal	Move to automated compliance, vulnerability management of devices for continuous compliance	Move to automated inventory of assets including supply chain software and manages risk of supply chain failures	Move to dynamic, real time device posture & risk-based access	Centralized, automated device threat protection
Tools	CIS/STIG Benchmarks	CMDB, Asset Inventory, TPRM, “NIST SCRM/NIST 800-53r5”	CASB, SASE, alphabet soup	EDR, A/V

Cyber Defense Matrix Index

	Identify	Protect	Detect	Respond	Recover
Endpoint Devices (Workstations and Servers)	Remote Monitoring & Mgmt Continuous Vulnerability Scanning Mobile Device Mgmt	Next-Gen AV Web\DNS Protection Device Hardening Policies	Endpoint or Managed Detection and Response (EDR or MDR) Security Information and Event Management (SIEM)	Incident Response Team System Orchestration, Automation and Response (SOAR)	Cyber Insurance
Applications	Privileged Access Management	Email Protection Password Mgmt System Application Single Sign On	Cloud Detection and Response (CDR)	Incident Response Team	O365 Backup
Network	Network Mgmt Solution	Next-Gen Firewall w/ Intrusion Protection System Domain DNS Protection Radius Wireless	Next-Gen Firewall w/ Intrusion Detection System Extended Detection and Response (XDR)	Incident Response Team	
Data	Data Loss Protection Automated Data Identification and Classification	Email Encryption Framework Compliance	Data Detection and Response (DDR)	Incident Response Team	Backup Solution
Users/Identity	Identity Mgmt	Single Sign On Security Awareness Training	Darkweb Compromised User or Password Monitoring	Incident Response Team System Orchestration, Automation and Response (SOAR)	