
# CSCI E-117A SPRING 2025

Lecture 6
Mar 4, 2025

## SECURE APPLICATIONS: MANAGING THE DEPLOYMENT INFRASTRUCTURE

# LECTURE 6 AGENDA

- *Assignment 1*
  - *Marks*
- *Assignment 2, 3*
  - *Office Hours*
- *DEVICES : In the News*

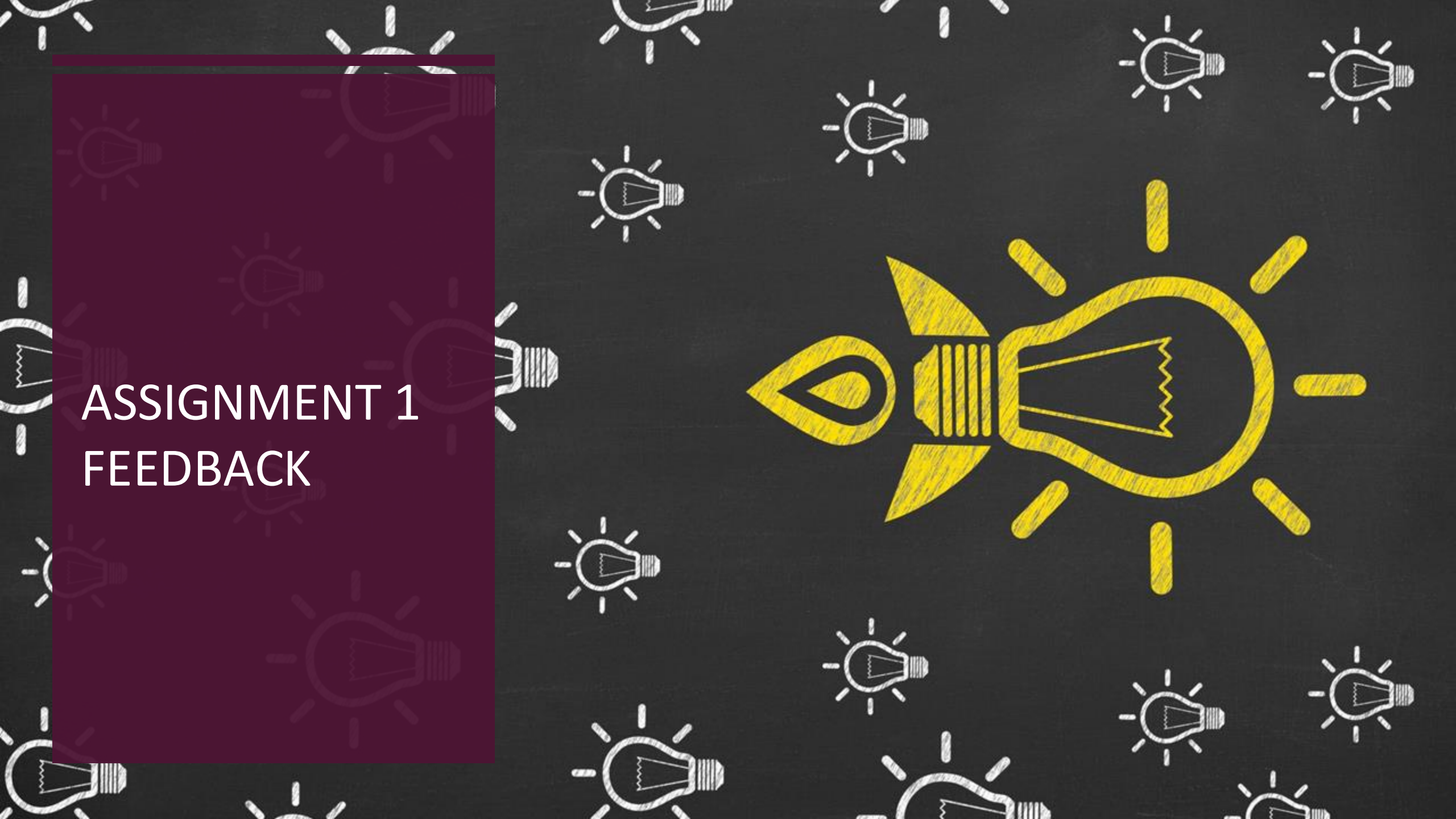
# QUICK ANNOUNCEMENTS

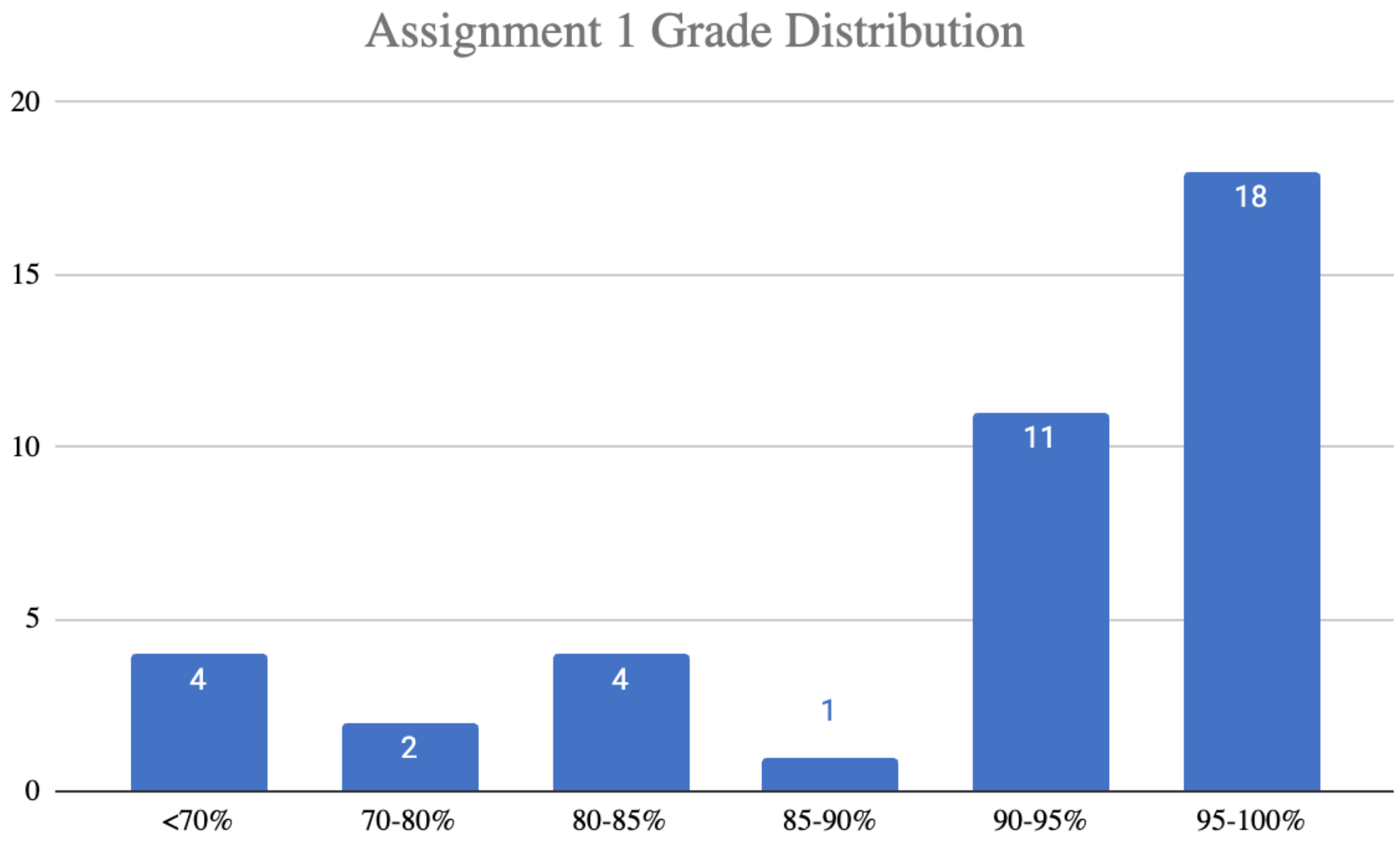
Assignment 3: March 16 (pushed back one week)

Assignment 4: April 6 (pushing back one week from March 30)

Capstone: (Still) Saturday May 3

# ASSIGNMENT 1 FEEDBACK




Assignment 1 Grade Distribution
20
15
10
5
0
4
2
4
1
11
18
<70%
70-80%
80-85%
85-90%
90-95%
95-100%

# 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.

# UPCOMING ASSIGNMENTS

# ASSIGNMENT 2

Due Date: March 2

Up to March 5 with no late penalties

# ASSIGNMENT 3

## Due Date: March 16 ~~March 9~~

**Purpose:** As we move to Devices, there are LOTS of vulnerabilities to consider. This is made worse as we consider the "variety" of devices we have to protect and how different Servers, Workstations and IoT are.

The protection and detection of vulnerabilities and compromises of devices includes people, process and technology; vendor solutions often cover both protect/detect and the CISA Zero Trust Maturity Model (ZTMM) assumes least maturity relies on people based solutions and most mature is full automated, technology based solutions.

The purpose of this assignment is to start to focus on the prioritization of Protection/Detection of devices, the ZTMM, and how Generative AI will impact our ability to move up (or down) the ZTMM.

# ASSIGNMENT 4

Due Date: ~~Mar 30~~ April 6

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

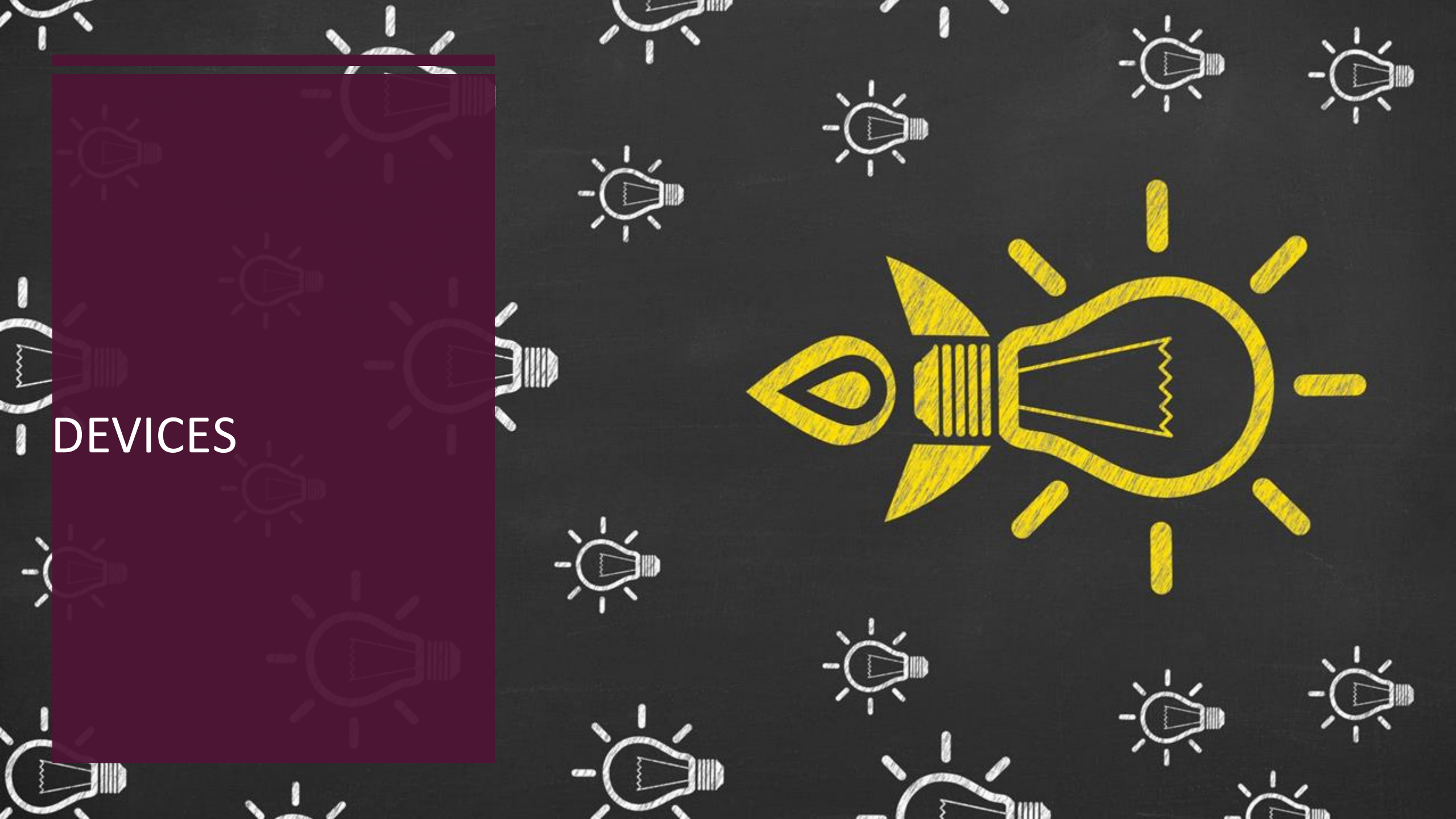
# CAPSTONE ASSIGNMENT

Due Date: SATURDAY MAY 3

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

# REMINDERS

# DEVICES

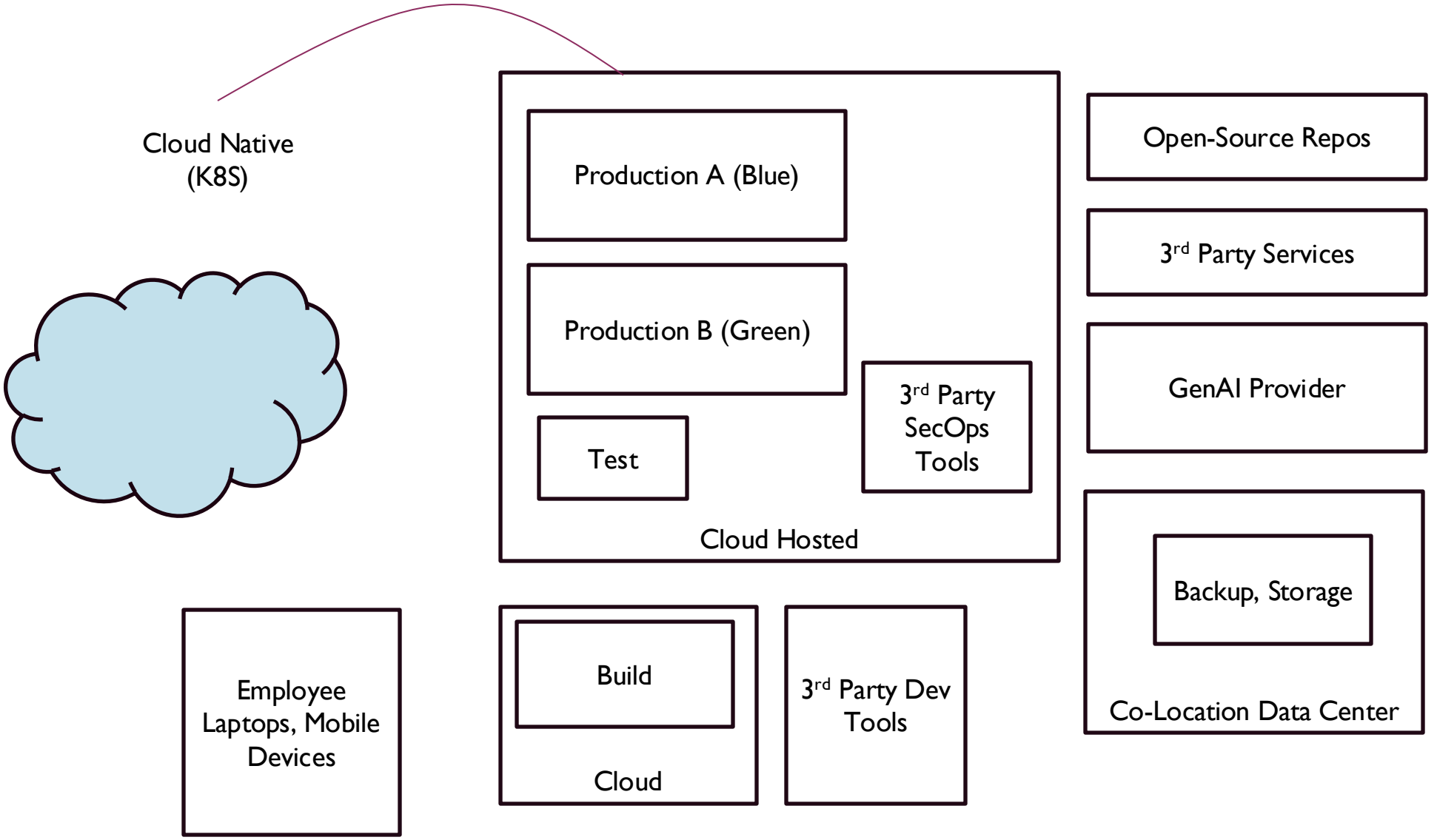


# DEVICES: DEFINITION

| | |
|---|---|
| **Devices** | Workstations, servers, phones, tablets, IoT, containers, hosts, compute, peripherals storage devices, network devices, web cameras, infrastructure, etc.<br><br>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. |

# NETWORKS: DEFINITION

| | |
|---|---|
| **Networks** | Communication channels, connections and protocols that enable traffic to flow among devices and applications.<br>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 |


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

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

Figure 4: High Level Zero Trust Maturity Model Overview

| DEVICES | 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 |
| (Config & Patch) 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 |

## NETWORKS: Zero Trust Maturity Levels

| 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. | | | |
|---|---|---|---|
| **Traditional** | **Initial** | **Advanced** | **Optimized** |
| • Large perimeter / macro-segmentation<br>• Limited resilience and manually managed rulesets and configurations<br>• Minimal traffic encryption with ad hoc key management | • Initial isolation of critical workloads<br>• Network capabilities manage availability demands for more applications<br>• Dynamic configurations for some portions of the network<br>• Encrypt more traffic and formalize key management policies | • Expanded isolation and resilience mechanisms<br>• Configurations adapt based on automated risk-aware applications profile assessments<br>• Encrypts applicable network traffic and manages issuance and rotation of keys | • Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience<br>• Configurations evolve to meet application profile needs<br>• Integrates best practices for cryptographic agility |

Figure 4: High Level Zero Trust Maturity Model Overview

| NETWORKS | Traditional | Initial | Advanced | Optimized |
|---|---|---|---|---|
| Network Segmentation | Flat network / limited segmentation, manually managed network architecture; minimal restrictions on reachability within network segments | Begin to deploy network architecture with the isolation of critical workloads, constrain connectivity to least function principles, and a transition toward service-specific management | Expand deployment of endpoint and application profile isolation mechanisms to more of their network architecture with ingress/egress micro- perimeters and service- specific interconnections. | 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 Distributed micro-perimeters, just-in-time and just-enough access control |
| Traffic Encryption | Minimal traffic encryption, ad hoc key management | Increased encryption, formalized key management | Encrypt application traffic, key management & rotation | Best practice crypto management including quantum aware |
| Network Traffic Management | Static network rules and configurations to manage traffic at service provisioning, with limited monitoring capabilities | Application profiles with distinct traffic management Features; begin to map all apps to profiles | Dynamic network rules and configurations for resource optimization | Dynamic network rules and configurations that continuously evolve to meet application profile needs |
| Network Resilience | Configures network capabilities on a case-by-case basis, manually managed | begins to configure network capabilities to manage availability demands for additional applications and expand resilience mechanisms | dynamically manage network capabilities for availability demands and resilience mechanisms for the majority of applications. | Holistic delivery and awareness in adapting to changes in availability demands for all workloads and provides proportionate resilience. |

## DEVICES

### End User Devices
(Fixed) Workstations
Laptops
Tablets
Mobile Devices
SOHO Routers

### Office I/F IT
Network
- ISP Termination
- WiFi Routers

Surveillance
- Cameras
- Recordings

Collab Equip
- Phones / Speaker
- TV / Display

### “Data Center” Devices
Physical Compute
Physical Storage Devices
Physical Network
- Firewalls
- Routers
- Switches

### PaaS/Cloud Hosted Devices
IaaS Compute, Networks
PaaS “Networks”
PaaS Network Devices
PaaS Compute
- Containers
- Microservices

## NETWORKS (Environments)

### Home (Office)
WiFi
Physical network devices)

### Office
WiFi
Physical network devices

### Cloud Hosted Environments
### Data Center Hosted
TCP/IP & Physical cable
Physical network devices

# NETWORK & DEVICE / READING

- https://www.bleepingcomputer.com/news/security/chinese-hackers-use-custom-malware-to-spy-on-us-telecom-networks/
- https://www.darkreading.com/cyberattacks-data-breaches/salt-typhoon-exploits-cisco-devices-telco-infrastructure
- https://www.darkreading.com/cyberattacks-data-breaches/salt-typhoons-impact-us-beyond
- https://thehackernews.com/2024/02/pegasus-spyware-targeted-iphones-of.html

# DARK READING : Salt Typhoon Exploits Cisco Devices in Telco Infrastructure

https://www.darkreading.com/cyberattacks-data-breaches/salt-typhoon-exploits-cisco-devices-telco-infrastructure

- Cisco spokesperson wrote that "We are aware of new reports that claim Salt Typhoon threat actors are exploiting two known vulnerabilities in Cisco devices relating to IOS XE. To date, we have not been able to validate these claims but continue to review available data." They added that "In 2023, we issued a security advisory disclosing these vulnerabilities along with guidance for customers to urgently apply the available software fix. We strongly advise customers to patch known vulnerabilities that have been disclosed and follow industry best practices for securing management protocols."
- Back in October 2023, Cisco urged all of its customers to immediately pull all their routers, switches, etc., off the Web — at least those running the IOS XE operating system.
- Just a few days later, Cisco revealed a second IOS XE web UI vulnerability that was being exploited in tandem with CVE-2023-20198. CVE-2023-20273 took the first vulnerability a step further, allowing attackers to run malicious commands on compromised devices using root privileges. It earned a "high" 7.2 CVSS score.
- Evidently, Cisco's warnings were not heard loudly and widely enough, as Salt Typhoon followed this exact path to just recently compromise large organizations on six continents. With the complete power afforded by CVE-2023-20198 and CVE-2023-20273, the threat actor would then configure Generic Routing Encapsulation (GRE) tunnels connecting compromised devices with its own infrastructure.

# BLEEPING COMPUTER: Salt Typhoon / Custom malware to spy on US telecom networks

https://www.bleepingcomputer.com/news/security/chinese-hackers-use-custom-malware-to-spy-on-us-telecom-networks/

- The Chinese state-sponsored Salt Typhoon hacking group uses a custom utility called JumbledPath to stealthily monitor network traffic and potentially capture sensitive data in cyberattacks on U.S. telecommunication providers.
- Cisco says Salt Typhoon hackers infiltrated core networking infrastructure primarily through stolen credentials. Apart from a single case involving exploitation of the Cisco CVE-2018-0171 flaw, the cybersecurity company has seen no other flaws, known or zero-days, being exploited in this campaign
  - While Salt Typhoon primarily gained access to targeted networks using stolen credentials, the exact method of obtaining the credentials remains unclear.
- Once inside, they expanded their access by extracting additional credentials from network device configurations and intercepting authentication traffic (SNMP, TACACS, and RADIUS).
- They also exfiltrated device configurations over TFTP and FTP to facilitate lateral movement, which contained sensitive authentication data, weakly encrypted passwords, and network mapping details.
- The attackers demonstrated advanced techniques for persistent access and evasion, including frequently pivoting between different networking devices to hide their traces and using compromised edge devices to pivot into partner telecom networks.

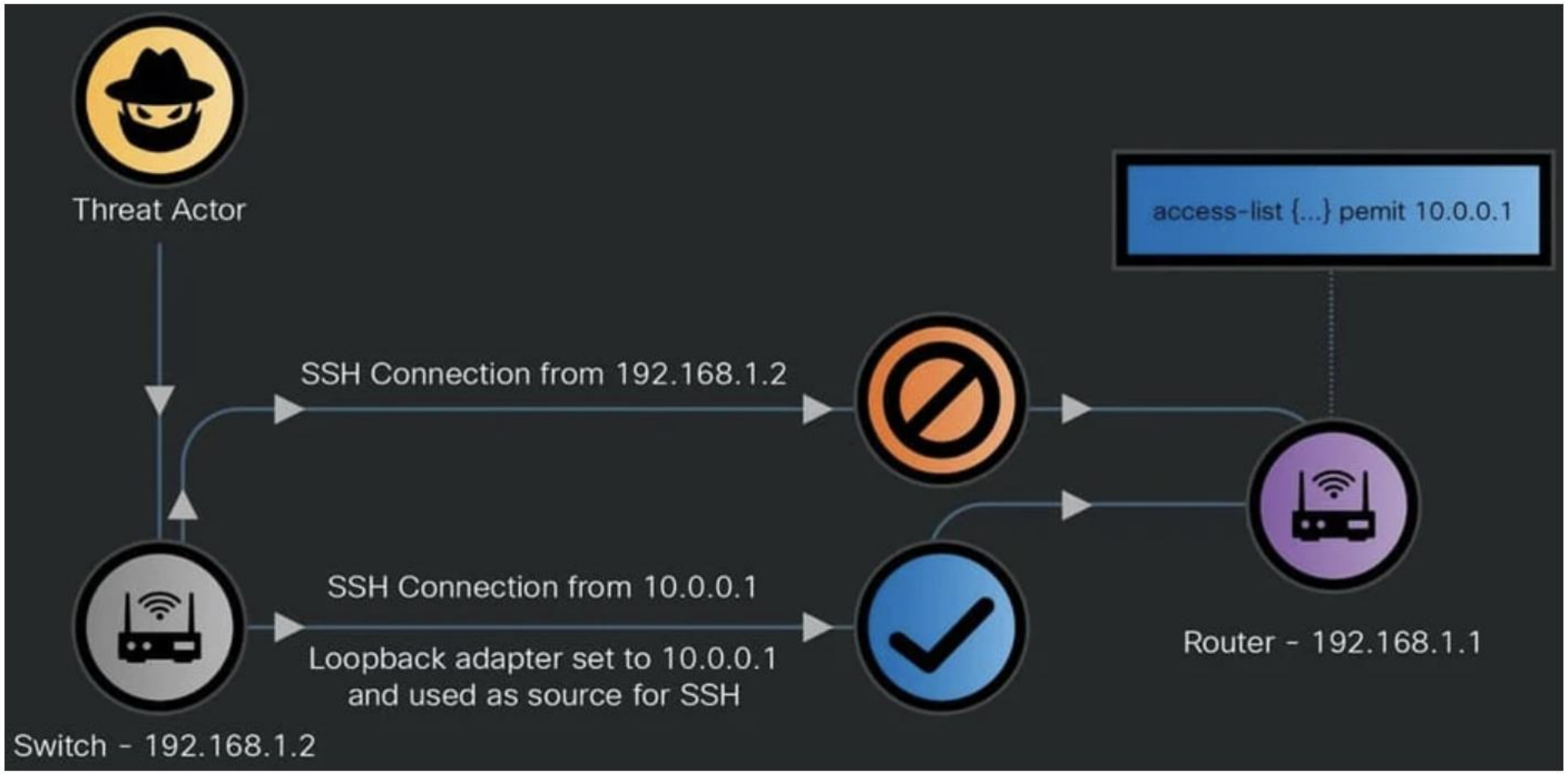
## BLEEPING COMPUTER: Salt Typhoon / Custom malware to spy on US telecom networks

https://www.bleepingcomputer.com/news/security/chinese-hackers-use-custom-malware-to-spy-on-us-telecom-networks/

- The threat actors were also observed modifying network configurations, enabling Guest Shell access to execute commands, altering access control lists (ACLs), and creating hidden accounts.
- A primary component of the Salt Typhoon attacks was monitoring network activity and stealing data using packet-capturing tools like Tcpdump, Tpacap, Embedded Packet Capture, and a custom tool called JumbledPath.
- JumbledPath allowed Salt Typhoon to initiate packet capture on a targeted Cisco device via a jump-host, an intermediary system that made the capture requests appear as if they originate from a trusted device inside the network while also obfuscating the attacker's true location.
- Cisco lists several recommendations to detect Salt Typhoon activity, such as monitoring for unauthorized SSH activity on non-standard ports, tracking log anomalies, including missing or unusually large '.bash_history' files, and inspecting for unexpected configuration changes.

## BLEEPING COMPUTER: Salt Typhoon / Custom malware to spy on US telecom networks

https://www.bleepingcomputer.com/news/security/chinese-hackers-use-custom-malware-to-spy-on-us-telecom-networks/

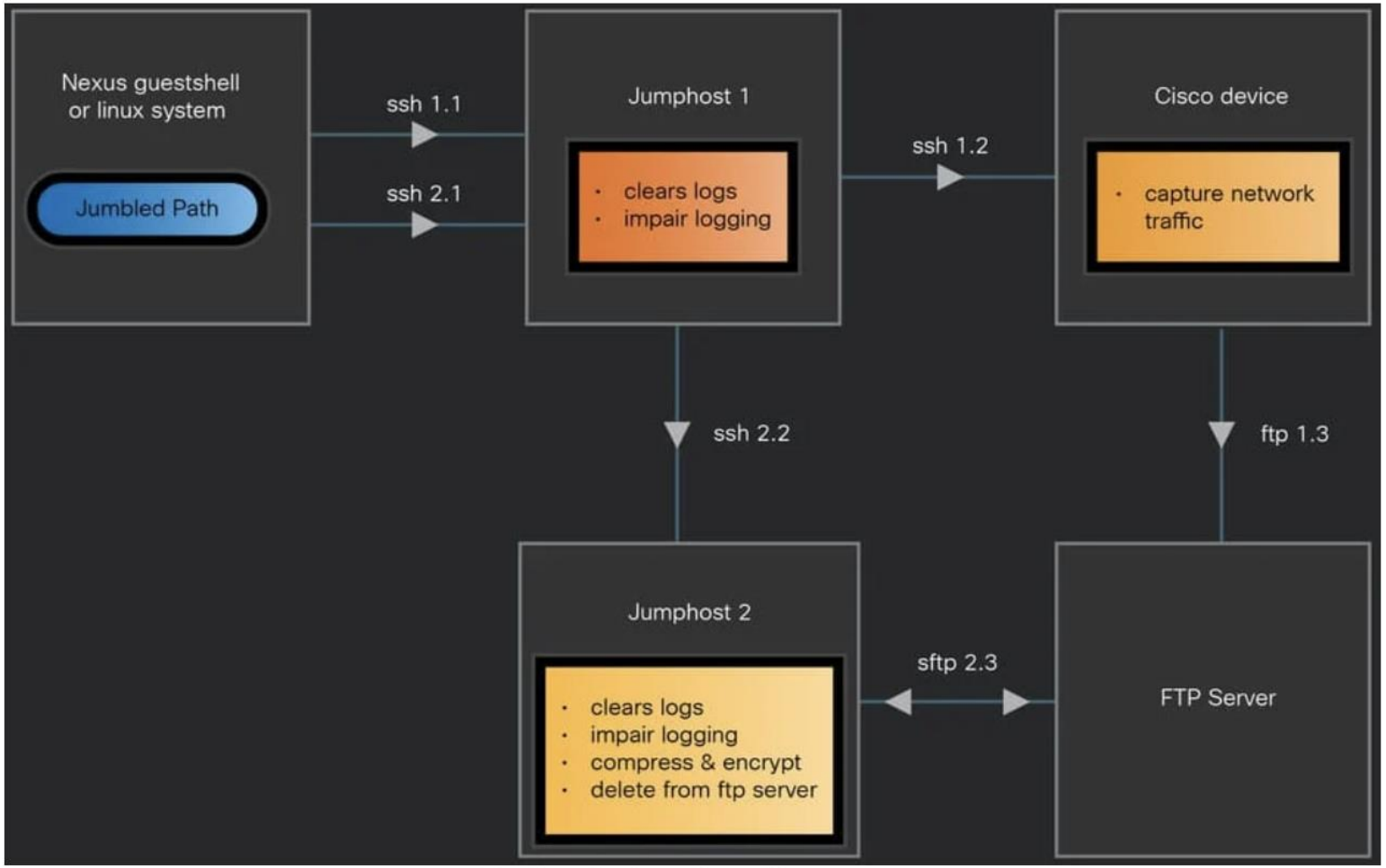



**Bypassing access control lists**

*Source: Cisco*

## BLEEPING COMPUTER: Salt Typhoon / Custom malware to spy on US telecom networks

https://www.bleepingcomputer.com/news/security/chinese-hackers-use-custom-malware-to-spy-on-us-telecom-networks/




JumbledPath data handling overview

# CLASS DISCUSSION PROMPT

- *This assumes you have done the reading in the deck and/or attended the office hours on Tuesday where this was discussed*
- *Before this class, if you were asked about a zero-trust network architecture, would you have gravitated to a description that required MFA to access to resources, with strong A/V-EDR on laptops (Yes/No)*
- *Once we broken down the categories to Network/Devices and (to be discussed) Identity/Applications/Data, would you have gravitated to Identity as the top priority (Yes/No)*
  - *How would you have priority ordered these categories before the start of this course?*
- *Given the reading on Salt Typhoon and the implications on networks and devices, how would you priority order these categories?*
  - *Why?*

10 min
BREAK
BACK
9:05PM ET

# BANNED TELECOMMUNICATION DEVICE MANUFACTURERS

https://www.npr.org/2022/11/26/1139258274/us-ban-tech-china-huawei-zte

- The U.S. is banning the sale of communications equipment made by Chinese companies Huawei and ZTE and restricting the use of some China-made video surveillance systems, citing an "unacceptable risk" to national security.
- QUOTES: Banning a company like Huawei, just because we started in China -- this does not solve cybersecurity challenges," Huawei's chief legal officer Dr Song Liuping said at the time…Song also claimed that both FCC chair Ajit Pai and other FCC commissioners failed to present any evidence to prove their claim that Huawei constitutes a security threat, and used words like "backdoors" to scare people.

# ANTICIPATED END OF LECTURE 5