Lecture 8
Mar 25, 2025

CSCI E-117A SPRING 2025

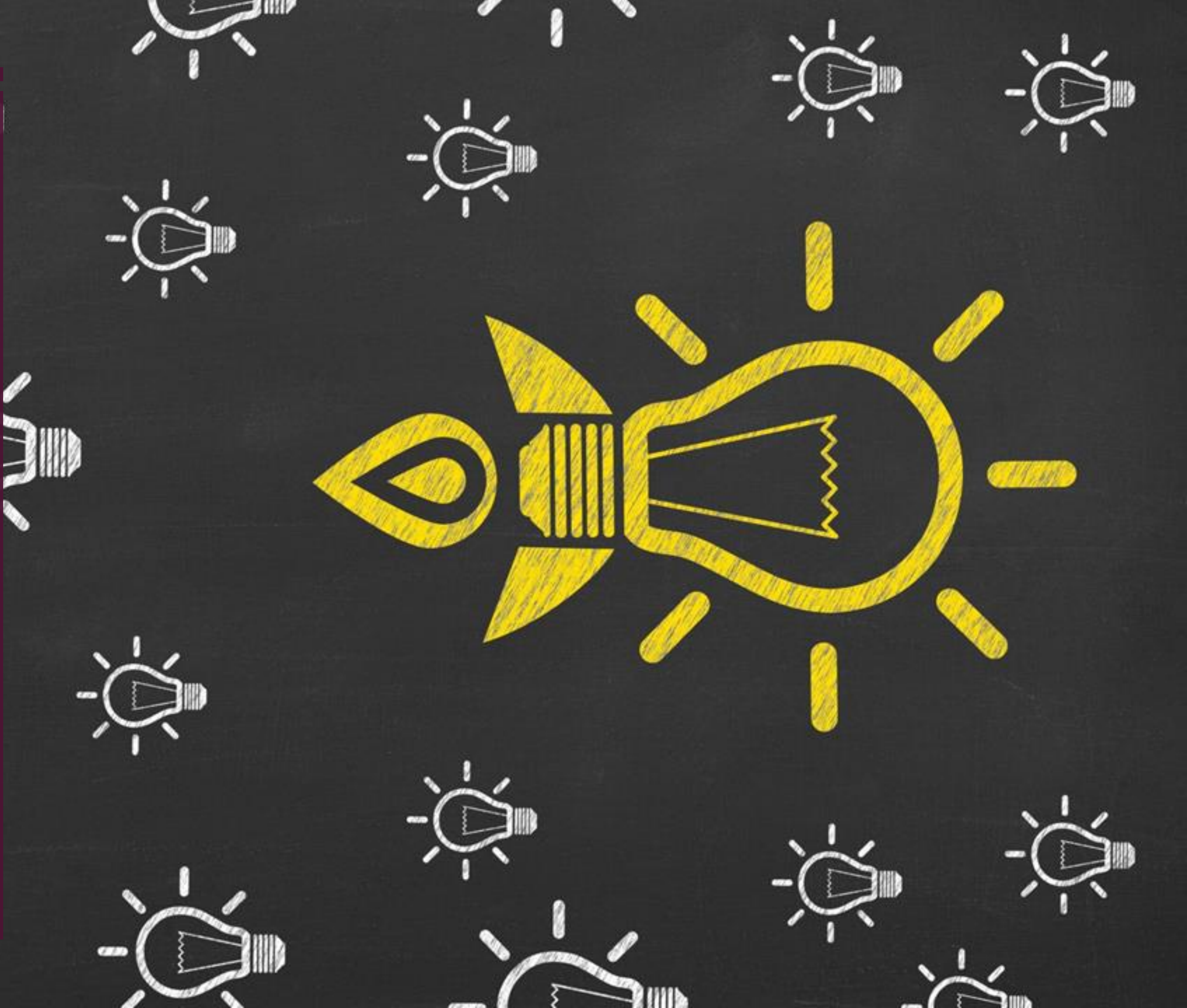
SECURE APPLICATIONS: MANAGING THE DEPLOYMENT INFRASTRUCTURE

LECTURE 8 AGENDA

- *Applications & Workloads*
  - *Zero Trust Maturity*
- *Case Study*
  - *Rippling v Deel*
  - *How Zero Trust Maturity concepts played a role*
- *Assignment III*
  - *Q&A , “Class Office Hours”*

SOME HIGHLIGHTS FROM LAST WEEK’S YELLOW DIG

ASSIGNMENT 3



ASSIGNMENT 3

Due Date: March 16

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.

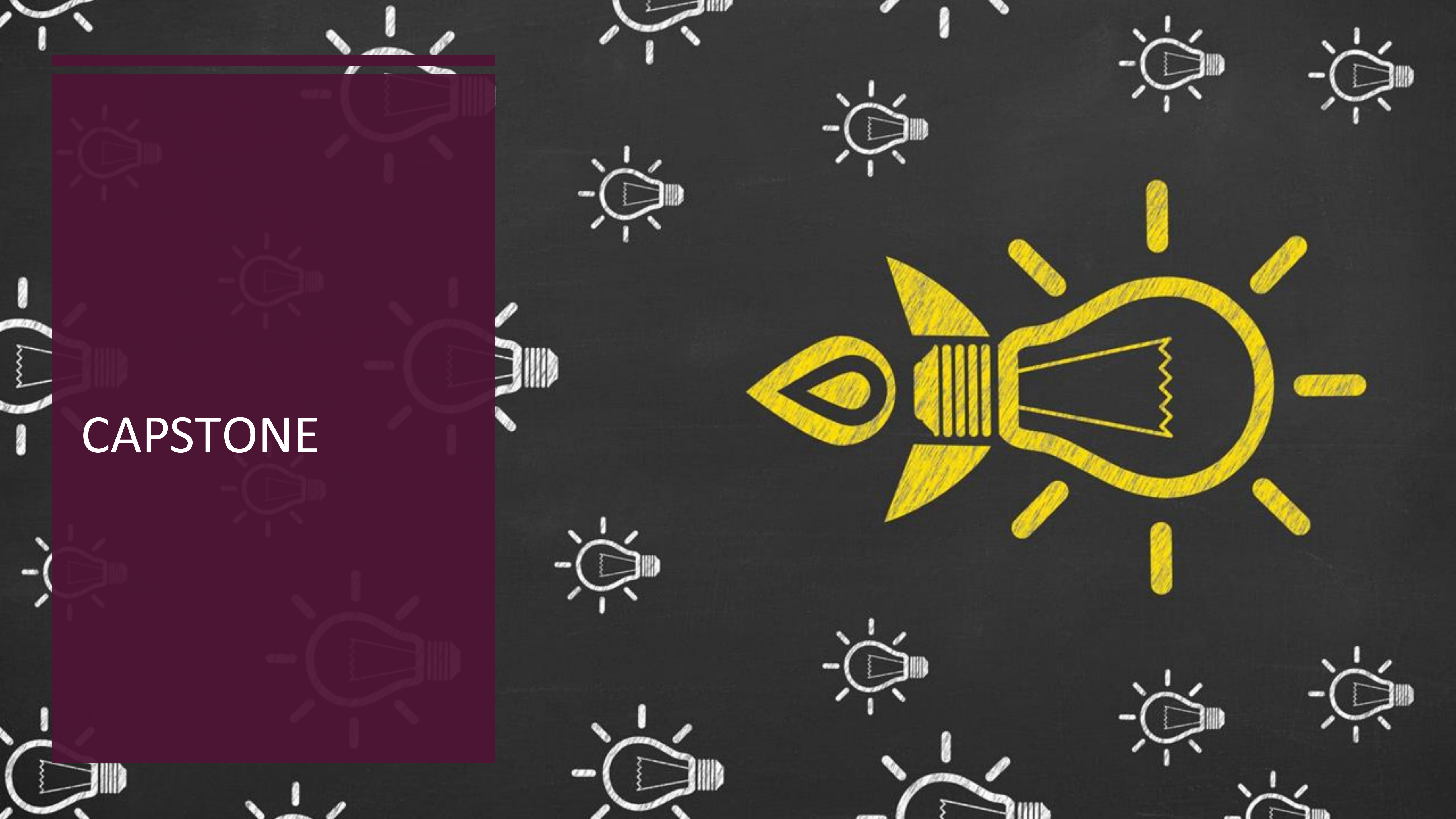
DATA

ASSIGNMENT 4

ASSIGNMENT 4

Due Date: April 6

Purpose: Understand Application category of Zero Trust Maturity

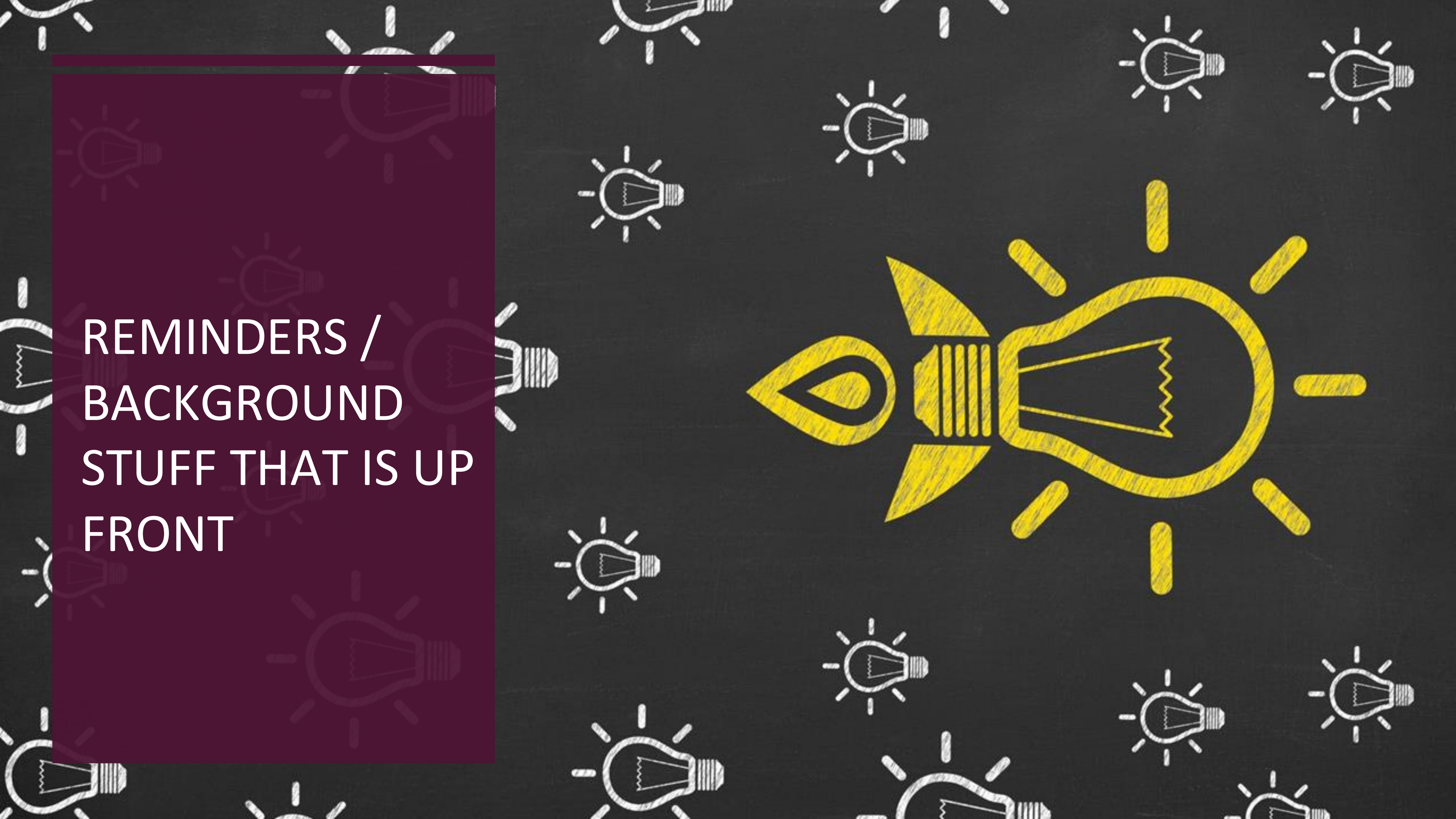


CAPSTONE

CAPSTONE

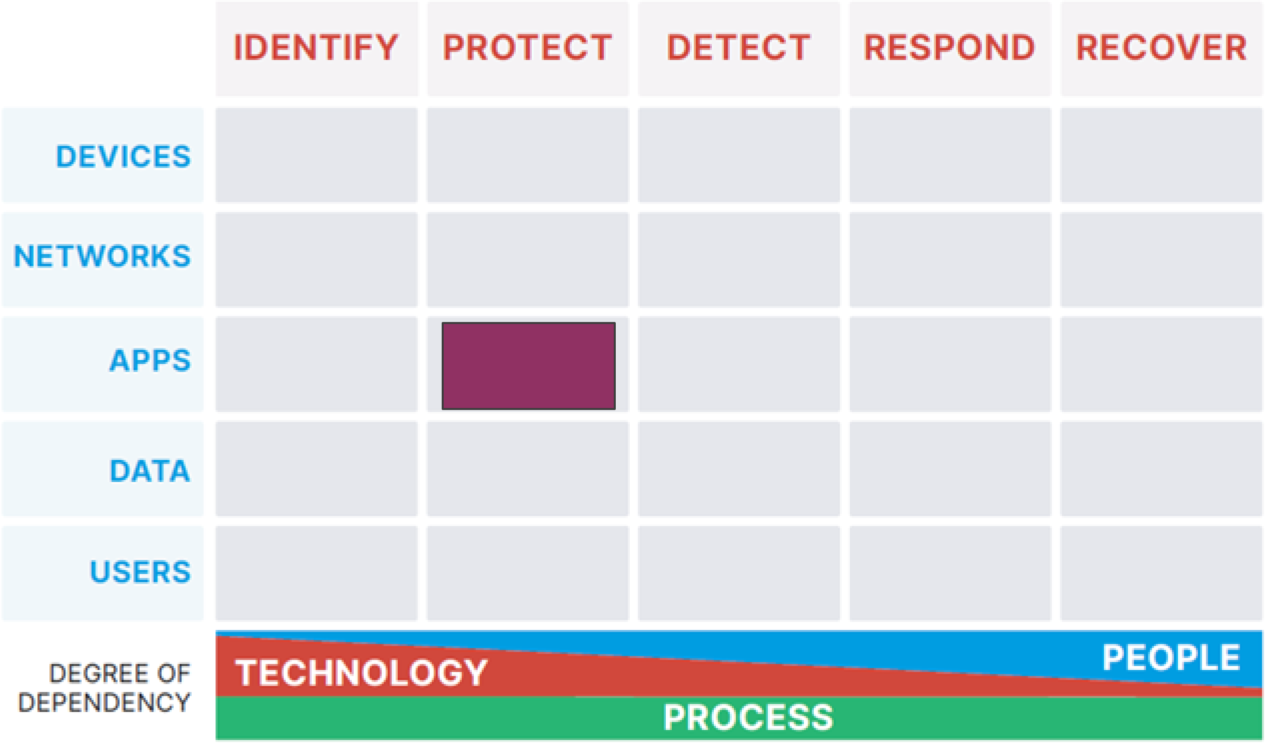
Background will be published by end of this week
It will be added to Canvas as a Quiz or Assignment (TBD) by March 31

REMINDERS / BACKGROUND STUFF THAT IS UP FRONT



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

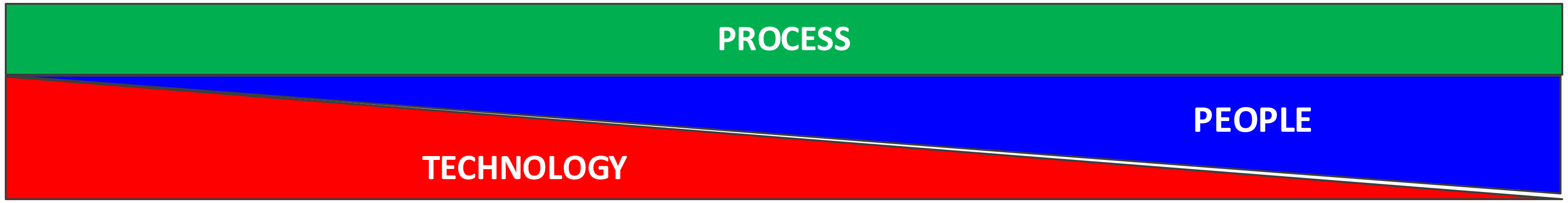
CYBER DEFENSE MATRIX



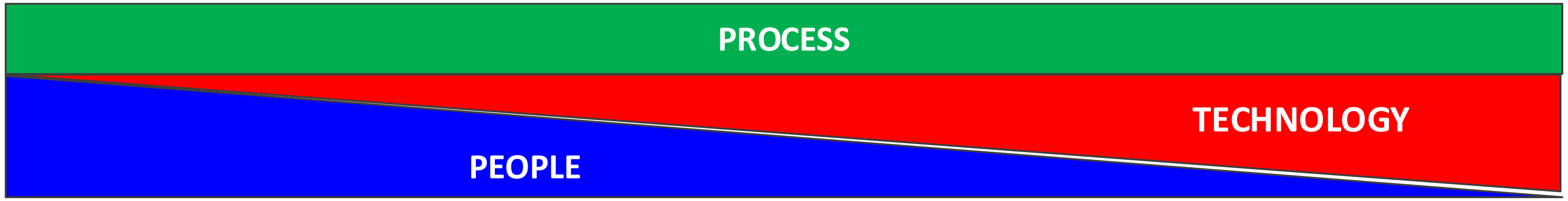
	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
DEVICES					
NETWORKS					
APPS		■			
DATA					
USERS					

Figure 1: Cyber Defense Matrix

Cyber Defense Matrix



	IDENTIFY	PROTECT	DETECT	RESPOND & RECOVER	
DEVICES					DEVICES
NETWORKS					NETWORKS
APPLICATIONS & DATA					APPLICATIONS & DATA
USERS					USERS
	TRADITIONAL	INITIAL	ADVANCED	OPTIMIZED	



Zero Trust Maturity

APPLICATION, IDENTITY BASICS

APPLICATIONS & WORKLOADS

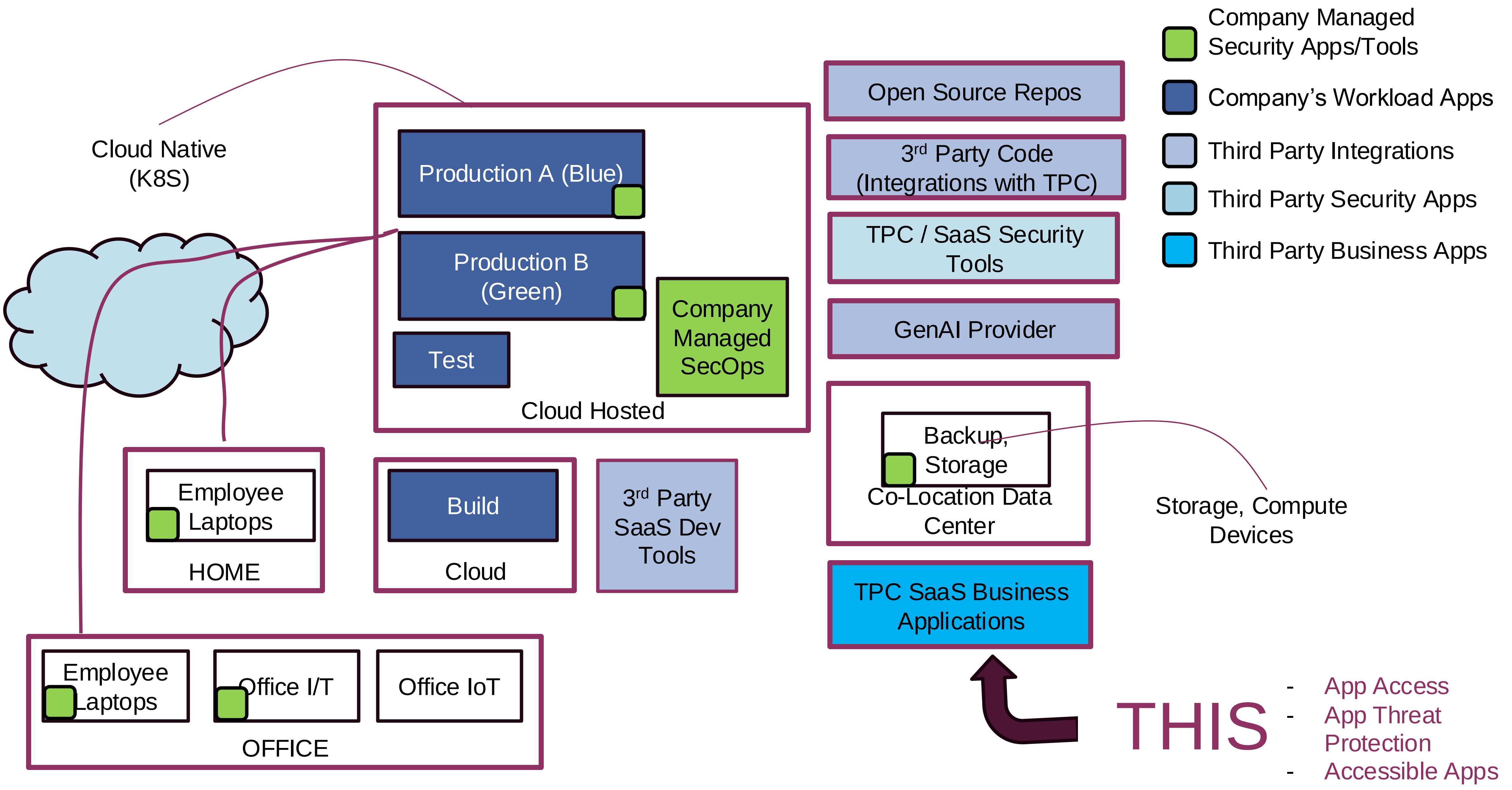
Software code and applications on the devices, separate from the operating system/firmware. This class includes serverless functions, APIs and microservices.

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)

- Application Access
  - Formerly Access Authorization
- Application Threat Protections
  - Formerly Threat Protection
- Accessible Applications
  - Formerly accessibility
- Secure Application Development and Deployment workflow
  - New function
- Application Security Testing
  - Formerly Application Security

APPLICATION & WORKLOAD ZERO TRUST FUNCTIONS

- Application Access (former Access Authorization)
  - Covers authorization for access to applications moving from local authorization and static attributes to real-time risk analytics and factors such as behavior or usage patterns
- Application Threat Protections (formerly Threat Protection)
  - Covers threat protections including general purpose protections for known threats moving to continuous dynamic monitoring across all applications for comprehensive visibility.
- Accessible Applications (formerly accessibility)
  - Moves from some mission critical applications available only over private networks and protected public network connections (e.g., VPN) with monitoring.
  - Moves towards all applicable applications available over open public networks to authorized users and devices, where appropriate, as needed
- Secure Application Development and Deployment workflow (new function)
  - Covers development, testing, and production environments and code deployment mechanisms.
- Application Security Testing (formerly Application Security)
  - Covers application security testing prior and post deployment moving from manual testing to automated continuous testing.



Cloud Native (K8S)

Production A (Blue)

Production B (Green)

Test

Company Managed SecOps

Cloud Hosted

Employee Laptops

HOME

Build

Cloud

3rd Party SaaS Dev Tools

Employee Laptops

Office I/T

Office IoT

OFFICE

Open Source Repos

3rd Party Code (Integrations with TPC)

TPC / SaaS Security Tools

GenAI Provider

Backup, Storage

Co-Location Data Center

Storage, Compute Devices

TPC SaaS Business Applications

- 🟩 Company Managed Security Apps/Tools
- 🟦 Company's Workload Apps
- ◻ Third Party Integrations
- ◻ Third Party Security Apps
- 🟦 Third Party Business Apps

THIS

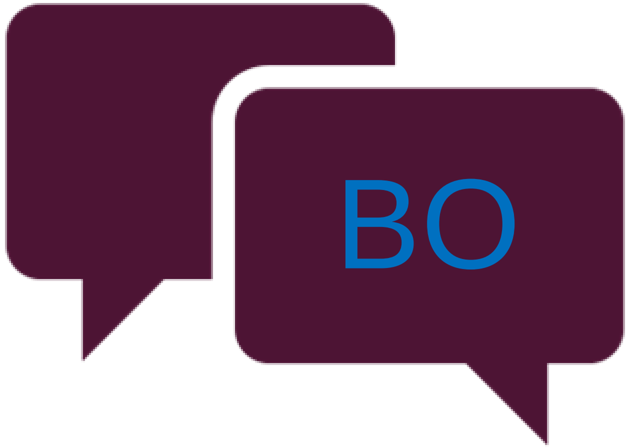
- App Access
- App Threat Protection
- Accessible Apps

CLASS DISCUSSION: POLL

- *Regardless of the Case Study (which you should have already read), which would you rather make the case for increased maturity within YOUR organization*

- ***Option 1:***
  - *Application Access*
  - *Application Threat Protections*
  - *Accessible Applications*
- ***Option 2**:*
  - *Secure Application Development and Deployment workflow*
  - *Application Security Testing*

CLASS DISCUSSION: BREAKOUT



- *Within your breakout group, explain why you picked the option you did*
  - *Its okay to ask questions about other student's environments and assertions so that it is not just a show-and-tell session*
- ***Option 1:***
  - *Application Access*
  - *Application Threat Protections*
  - *Accessible Applications*
- ***Option 2**:*
  - *Secure Application Development and Deployment workflow*
  - *Application Security Testing*

10 min

BREAK

BACK

9:05PM ET

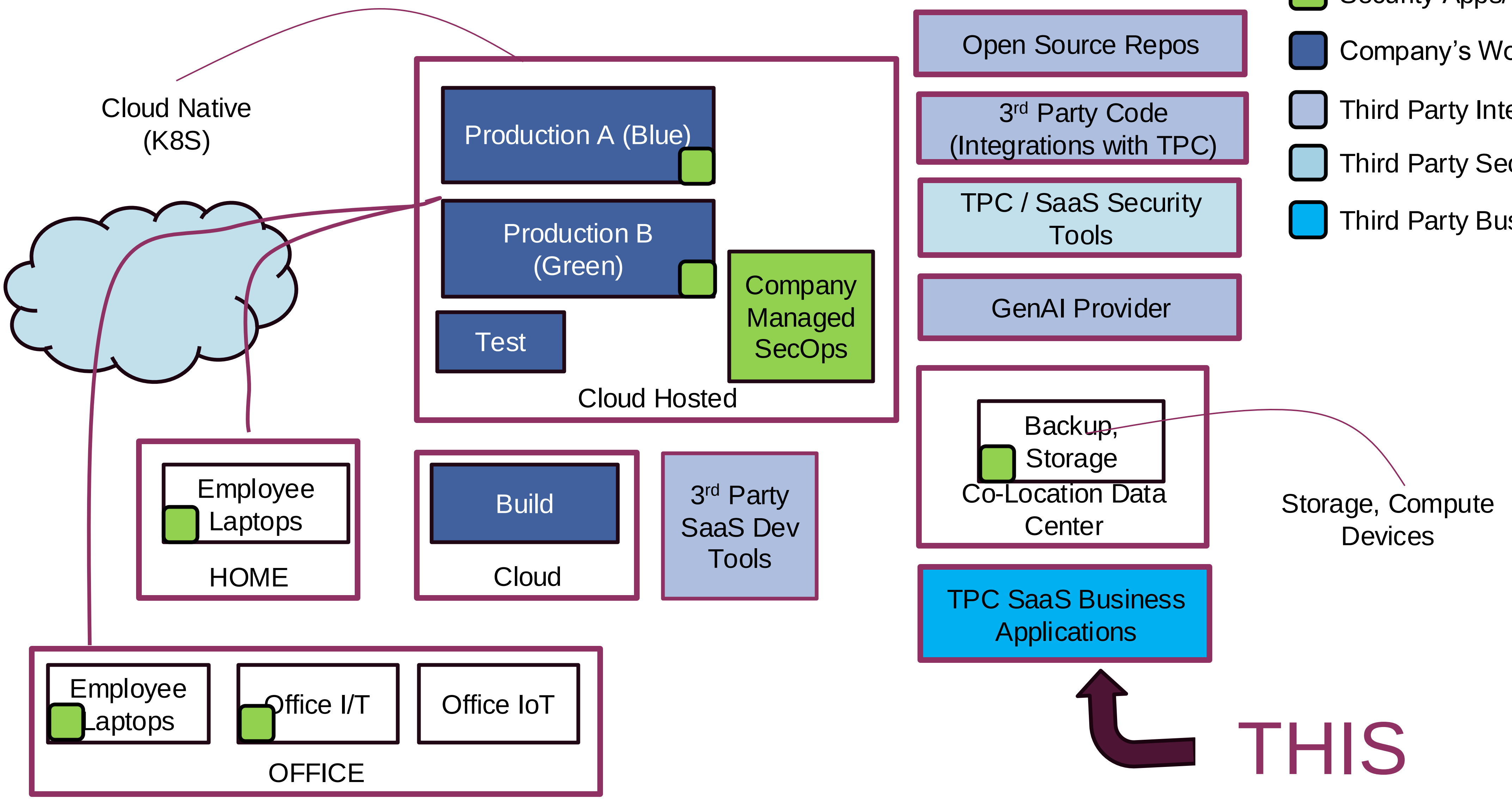
APPLICATIONS.& WORKLOADS V IDENTITES

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)

An identity refers to an attribute or set of attributes that uniquely describes an agency user or entity, including non-person entities.
This includes people using resources and assets and their associated identities, including customers (using the applications/services your company provides) and the employees of your company.
This also includes all of the "tokens" or "Non-Human Identities" that are used to authenticate between servers (eg mutually authenticated TLS) and to authenticate on behalf of a human (eg Oauth for SSO)

IDENTITY

- REFERENCE SO THAT WE CAN CONSIDER DURING CASE STUDY
- Identity Authentication
  - Covers username, passwords, moving to continually validated identity phishing resistant MFA
- Identity Stores
  - Covers identity stores, moving from self-managed and on-prem to identity stores integrated across all partners and environments as appropriate
- Identity Risk Assessment
  - Move from “trust” that identity not compromised identity to automated analysis and dynamic rules to inform access decisions to continuous analysis and dynamic rules to identity/prevent identity compromise
- Access Management
  - Permanent access with periodic review for both privileged an unprivileged account to automation to just-in-time authorization and just-enough access tailored to individual actions an individual resource needs.



Cloud Native (K8S)

Production A (Blue)

Production B (Green)

Test

Company Managed SecOps

Cloud Hosted

Employee Laptops

HOME

Build

Cloud

3rd Party SaaS Dev Tools

Employee Laptops

Office I/T

Office IoT

OFFICE

Open Source Repos

3rd Party Code (Integrations with TPC)

TPC / SaaS Security Tools

GenAI Provider

Backup, Storage

Co-Location Data Center

Storage, Compute Devices

TPC SaaS Business Applications

THIS

🟩 Company Managed Security Apps/Tools

🟦 Company's Workload Apps

⬜ Third Party Integrations

⬜ Third Party Security Apps

🟦 Third Party Business Apps

APPLICATION ACCESS ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency authorizes access to applications primarily based on local authorization and static attributes.	Agency begins to implement authorizing access capabilities to applications that incorporate contextual information (e.g., identity, device compliance, and/or other attributes) per request with expiration.	Agency automates application access decisions with expanded contextual information and enforced expiration conditions that adhere to least privilege principles.	Agency continuously authorizes application access, incorporating real-time risk analytics and factors such as behavior or usage patterns.

APPLICATION THREAT PROTECTION ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency threat protections have minimal integration with application workflows, applying general purpose protection for known threats	Agency integrates threat protections into mission critical application workflows, applying protections against known threats and some application- specific threats.	Agency integrates threat protections into all application workflows, protecting against some application-specific and targeted threats	Agency integrates advanced threat protections into all application workflows, offering real-time visibility and content-aware protections against sophisticated attacks tailored to applications.

ACCESSIBLE APPLICATION ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency makes some mission critical applications available only over private networks and protected public network connections (e.g., VPN) with monitoring.	Agency makes some of their applicable mission critical applications available over open public networks to authorized users with need via brokered connections.	Agency makes most of their applicable mission critical applications available over open public network connections to authorized users as needed.	Agency makes all applicable applications available over open public networks to authorized users and devices, where appropriate, as needed.

SECURE APPLICATION DEVELOPMENT ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency has ad hoc development, testing, and production environments with non-robust code deployment mechanisms.	Agency provides infrastructure for development, testing, and production environments (including automation) with formal code deployment mechanisms through CI/CD pipelines and requisite access controls in support of least privilege principles.	Agency uses distinct and coordinated teams for development, security, and operations while removing developer access to production environment for code deployment.	Agency leverages immutable workloads where feasible, only allowing changes to take effect through redeployment, and removes administrator access to deployment environments in favor of automated processes for code deployment.

APPLICATION SECURITY TESTING ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency performs application security testing prior to deployment, primarily via manual testing methods.	Agency begins to use static and dynamic (i.e., application is executing) testing methods to perform security testing, including manual expert analysis, prior to application deployment.	Agency integrates application security testing into the application development and deployment process, including the use of periodic dynamic testing methods.	Agency integrates application security testing throughout the software development lifecycle across the enterprise with routine automated testing of deployed applications.

OFFLINE THINKING (FOR YOU TO NOODLE ON….)

- *Consider the categories we have considered so far, Networks and Devices. It is hard to imaging moving up to an Optimal are for one function while staying at a Traditional level for another within a given category.*
- *This isn't as obvious for Applications:*
  - *I can move to Optimal for Application Security testing while still being Traditional for Application Access*
  - *I can even move to Optimal for AppSec testing while being Initial for Secure Application Development*
- *What does this tell us about the Application category?*
  - *Is it trying to cover too much (too many "types" of applications?)*
  - *Should Development of Applications be a separate category from Use of Applications?*

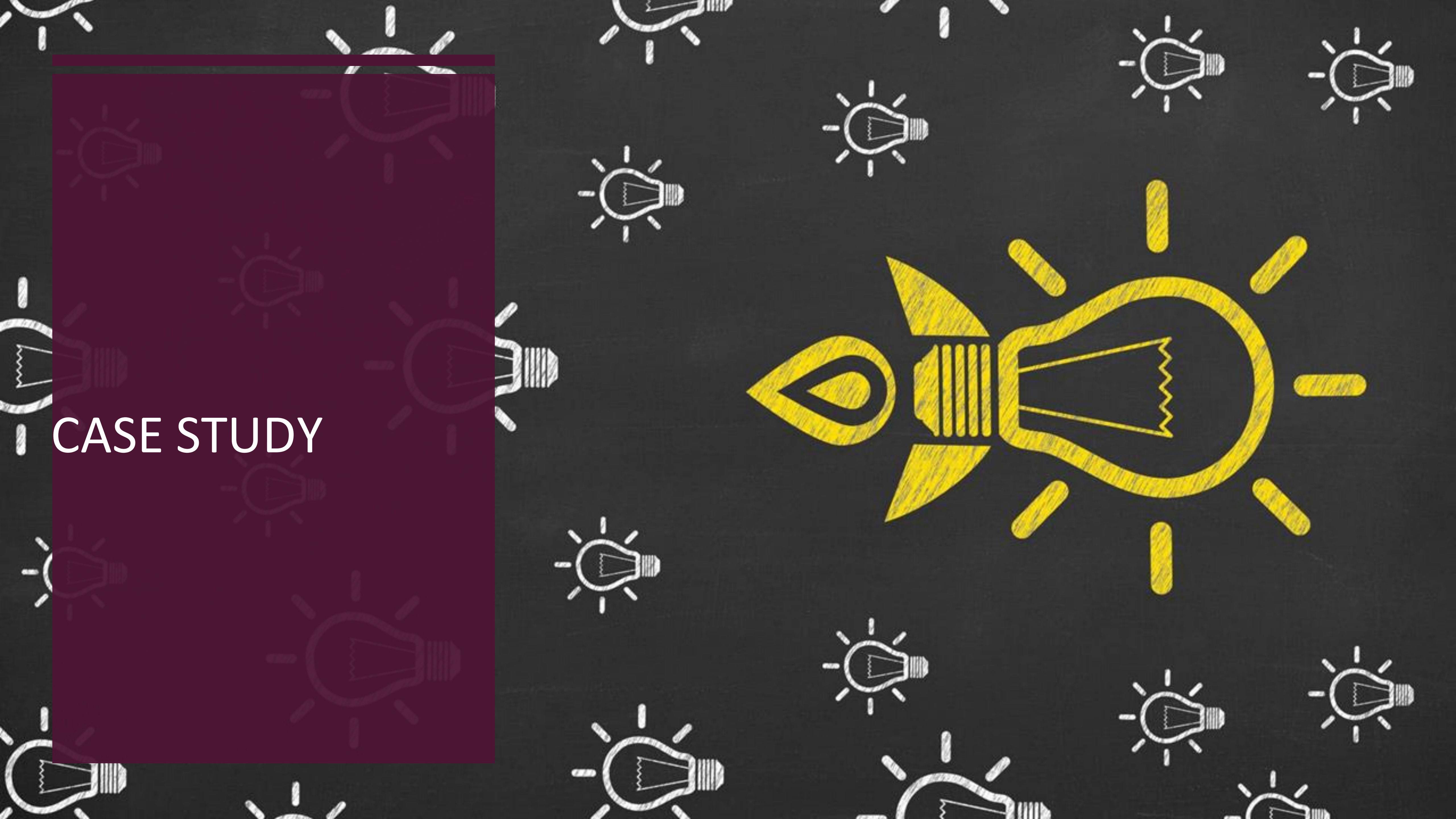
This is simply for your own reflection and is NOT required to be addressed in the weekly Canvas Discussion!

OFFLINE THINKING (FOR YOU TO NOODLE ON….)

- *Consider the explicit details about Application Security Development …*
- *Does this maturity model assume or require that you have a modern development methodology that is supported by CI/CD pipelines, configuration as code, infrastructure as code, and micro-services?*
- *How realistic is this given that there are many traditional development environments and applications still "in use"?*
    - *Is this something where the benefits of completely re-doing "how you work" to meet these new approaches will out weight the costs and the risks?*

This is simply for your own reflection and is NOT required to be addressed in the weekly Canvas Discussion!

CASE STUDY



APPLICATIONS: THIRD PARTY SAAS

- For the purposes of “case study” for this course, we are going to consider third-party SaaS business apps including
  - Slack (discuss sales, customers, churn, success stories, etc)
  - (Salesforce) Databases (CRM typically used to manage sales leads, pipeline, client sentiment/churn
  - Internal Web - eg Confluence (Battlecards, Customer Success Stories)
  - ”Gong” (Record and pull intelligence from customer meetings/recordings)
  - Workday (HR system)

RIPPLING TIMELINE (BUILT FROM COMPLAINT AND READING BETWEEN THE LINES – BTL)

- (Hopefully) You have read either the complaint or the summary of the complaint posted to this lecture's page
- June 2023: "D.S." Hired by Rippling
- Jan-Feb 2025: (Some) Rippling employees expressed concern because they did not know how Deel had access to their personal data (which not available through social media)
- February 18, 2025: Investigative reporter reaches out with info that is traced back to internal Slack messages
- Early Feb 2025: Rippling opens a security investigation into the matter (Access to HR/PII and/or Report, unclear)
  - BTL: Investigate Slack logs to see who is searching for ("Russia," "Belarus," "Iran," "Syria," and/or "Sanctions")
  - BTL: Identify "D.S." as source of these searches
  - BTL: Extend searches for other anomalous behavior by D.S. and find Deel/customer searches
  - BTL: Extend searches to other platforms for anomalous behavior by D.S. including HR, Email
- March 3, 2025: Rippling executes HoneyPot
- March 4, 2025: Honeypot executes
- Wednesday, March 12, 2025: Court order, attempt to seize D.S. Mobile device

CASE STUDY : ZERO TRUST CHARACTERISTICS

NETWORK

- Network Segmentation (through SaaS based applications)
- Network Encryption (presumed based on SaaS best practices)

DEVICES

- Resource Access (limited for BYOD Mobile Device, no info on Laptop)

APPLICATIONS

- Application Access (local authorization, static attributes)
- Application Threat Protections (logging good enough to support investigation)
- Accessible Application (SaaS apps open public networks to authorized users and devices,)

DATA

- Data Access (data access controls that incorporate elements of leas privilege across the enterprise
- Data Encryption (presumed in place based on SaaS characteristics)

IDENTITY

- Risk Assessments (has identity been compromised)
- Access Management ("permanent access" with period review of access)

RIPPLING'S CONTROLS (AS DOCUMENTED IN COMPLAINT)

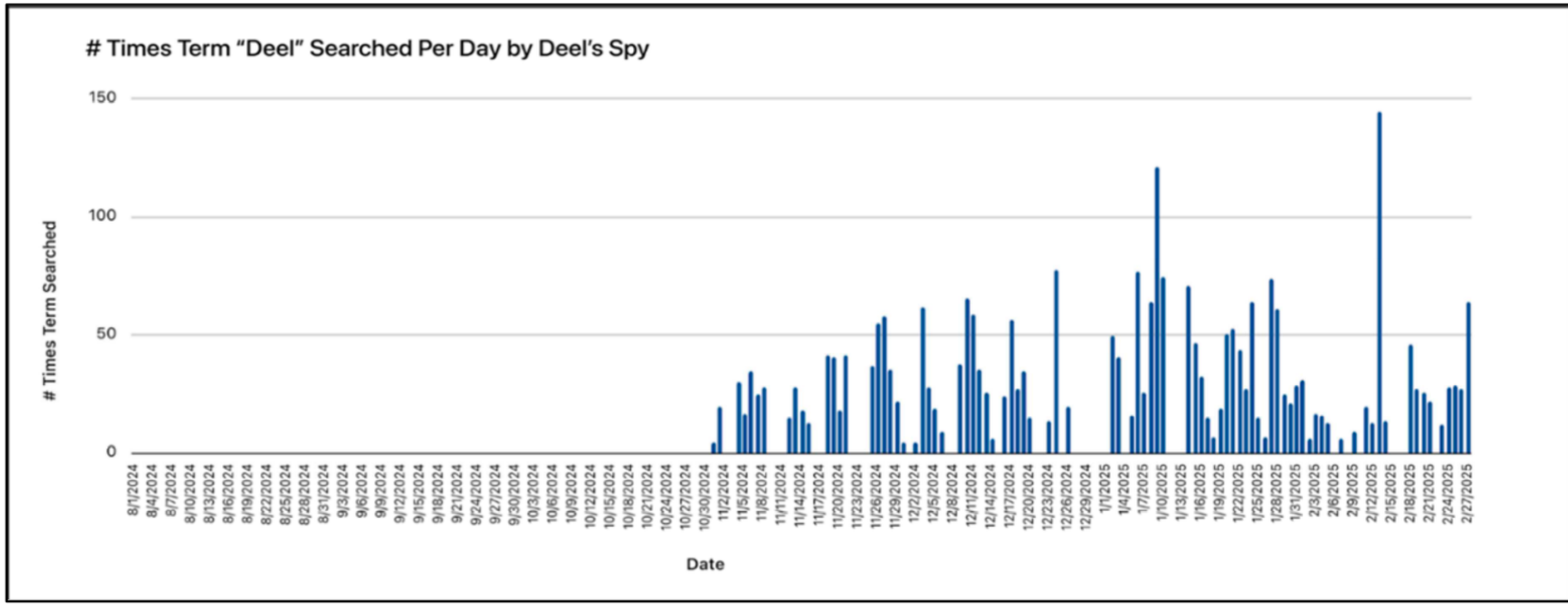
- Due to the fast-paced and global nature of Rippling's business and target market, it is imperative that Rippling employees can exchange information quickly and efficiently to expeditiously close deals with prospective customers or identify and resolve issues a current customer is facing and deploy a solution as fast as possible. To achieve this, Rippling stores its Sales and Marketing Trade Secrets in centralized databases accessible to all of its employees, including databases hosted by Salesforce, Slack, and Google. Rippling's use of these databases for storage is not uncommon for a modern technology company of its size.
- Rippling utilizes to facilitate its global work are also restricted to employee-only access and require various authentication methods. For example, for an individual to be able to access and utilize Rippling's Slack function, Rippling must add that person as an active Slack user. Rippling only provides such credentials to active employees and certain contractors that are providing services to Rippling for a particular purpose. Moreover, Rippling's practice is for employees to only access public Slack channels within the Rippling universe that pertain specifically to their job function
- Moreover, while Rippling permits its employees to remotely access Rippling's company systems, networks, or applications, in accordance with Rippling's Bring Your Own Device ("BYOD") Policy, that remote access is also heavily restricted. For example, in order to access an application such as Slack from their mobile device, the Rippling employee must use a device meeting certain security requirements (such as having a strong password, automatic locking of the device upon a number of failed login attempts, and the latest security patches and updates installed). The employee must use their Rippling login credentials and, where required by the system, is subject to a multi-factor authentication process or is required to use a token for access.
- In part to ensure that the confidential information in Rippling's Slack channels is used only for authorized purposes, Rippling employees' Slack activity is "logged," meaning every time a user views a document through Slack, accesses a Slack channel, sends a message, or conducts searches on Slack, that activity (and the associated user) is recorded in a log file.

RIPPLING: DEETS ON THE MALICIOUS INSIDER (BACKGROUND)

- On June 20, 2023, an affiliate of Rippling hired Deel's spy ("D.S."), because of his experience in global payroll, into a management role at Rippling as its Global Payroll Compliance Manager. D.S.'s responsibilities in that role included hiring payroll specialists, country launches, and setting up payroll processing and operations for approximately 15 countries in which Rippling offers global payroll services. D.S.'s daily responsibilities included managing a team of Global Payroll Operations Specialists to ensure timely and accurate performance of local payroll activities for customers, as well as resolving payroll-related customer escalations related to the countries within his job scope. As a result of his employment in this role—and pursuant to several contracts he signed in connection therewith, detailed below—D.S. was granted access to: Rippling's secure internal electronic messaging application, Slack (the "Slack Platform"); Rippling's Salesforce database (the "Salesforce Database"), which contained confidential information about current and prospective customers; Rippling's secure Google Drive repository ("Rippling's Google Drive"); and Rippling's internal human resources system, which contains information such as names, addresses, and personal cell phone numbers for Rippling employees (the "Rippling HR Platform"). The Slack Platform, the Salesforce Database, Rippling's Google Drive, and Rippling HR Platform are confidential. Moreover, not all Rippling employees have access to all files stored on these platforms; rather, they must be granted permissions to access specific file. As described above, that restriction is enforced through industry standard authentication protocols.

RIPPLING: MALICIOUS INSIDER ACTIVITIES AGAINST SLACK

- D.S. (malicious insider) hired in June 2023
- Rippling's Slack logs show that D.S. began searching and accessing Rippling's Slack channels at an unprecedented rate beginning in or around early November 2024. Notably, D.S. searched the term "deel" approximately 23 times per day

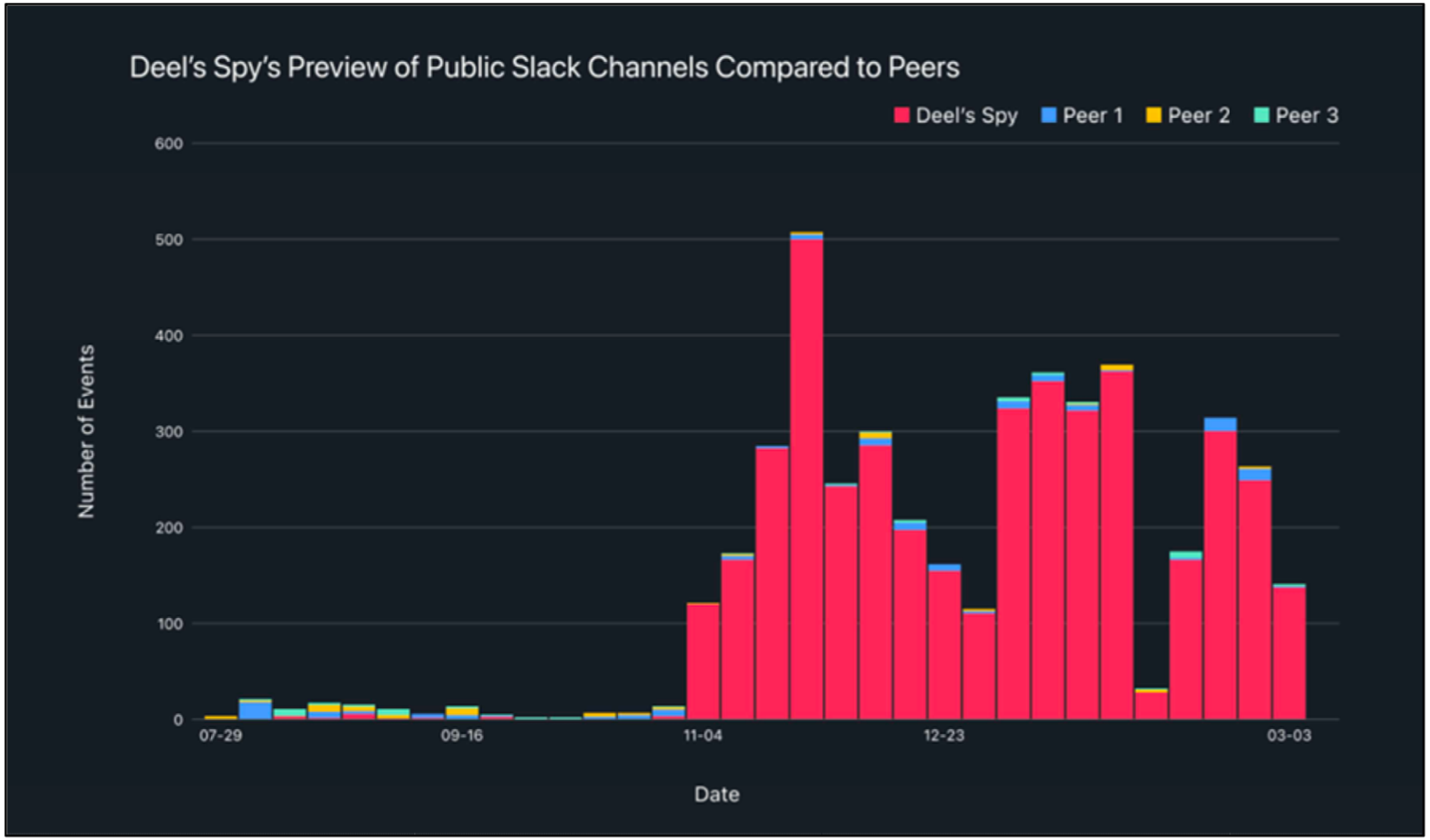


RIPPLING: D.S.’S ANAMOLOUS BEHAVIOUR AGAINST SLACK

- The log-generated chart below shows that, between August and October 2024, D.S. rarely previewed any Slack channels, consistent with typical employee behavior. Moreover, on the rare occasions in which he did so, D.S. previewed the channels no more than four times in any given month, and did so for channels like “#ppl-dogs,” a channel dedicated to Rippling employees sharing pictures of their dogs
- However, beginning in November 2024, D.S. beginning previewing channels at a rate orders of magnitude greater than he had before—both in terms of the number of channels previewed, and in the number of times he previewed each of those channels
- The channels D.S. previewed during this period have no connection to his payroll operations job responsibilities. What they do relate to, however, are all aspects of Rippling’s business development, sales, and customer retention strategies—the most sensitive of the Company’s Sales and Marketing Trade Secrets and confidential business information—with a particular emphasis on a single competitor, Deel. Leaving no doubt about the ultimate beneficiary of the brazen espionage scheme, D.S. viewed channels related specifically to Rippling’s competitive intelligence concerning Deel over 450 times during the course of the scheme.
- Indeed, D.S.’s top 10 channel previews since November 2024 are all sales-related channels, completely unrelated to D.S.’s role in payroll operations:

RIPPLING: INTELLIGENCE PULLED FROM SLACK

- D.S.’s Slack activity beginning in November 2024 was not merely a departure from his own prior activities. As shown below, D.S. previewed Slack at orders of magnitude more than his peer Rippling employees as well; in this chart, red bars indicate D.S.’s channel previews over time, while three of his peers are represented with other colors (barely noticeable by comparison)



RIPPLING: D.S. ATTEMPTS TO AVOID DETECTION RE SLACK

- D.S. frequently accessed various channels in "preview" mode— allowing him to see the contents of the channels without "joining" them. Although it is more common for Slack users to join a channel to review its contents, joining a channel generates an automated message to the members of the channel identifying the new user who has joined. On information and belief, D.S. chose to review the channels in question in preview mode to avoid alerting the channels' members that he had accessed them.
- Throughout the scheme, D.S.'s Slack searches frequently followed a distinctive and unusual pattern: he searched for a channel on his personal iPhone, then, moments later, searched for the same channel on his company-issued computer, and then (and only then) did he download a file from that channel. On information and belief, D.S. followed this pattern so that most of his searches would occur on his personal device, on which he was less susceptible to detection, and so that he could reserve the use of his work computer for downloading information that he had determined was worthy of misappropriating.

RIPPLING: D.S. ACTIVITIES AGAINST INTERNAL SYSTEM DIRECTORY

- Deel appears to have induced its spy to misappropriate contact information for Rippling employees of his own team, the Global Payroll Operations Team.
- Several of the team members reported that these offers were made without any substantive interview, and only after direct unsolicited contact from Deel's Chief Operating Officer, XXX. Some of these team members were contacted directly via WhatsApp, a messaging application that requires knowledge of a person's mobile phone number to send a message.
- In one telling case shown below, on January 23, 2025, XXX messaged a member of Rippling's Global Payroll Operations Team on LinkedIn... Four days later, on January 27, 2025, D.S. visited this individual's page in Rippling's internal personnel directory, which contains employees' personal phone numbers. Later that same day, Mr. Westgarth messaged the team member on WhatsApp

RIPPLING: INTERNAL SYSTEM DIRECTORY CONTROLS

- Rippling's internal personnel directory is viewable only by active Rippling employees, and only upon logging into their Rippling account using their unique username, password, and other authenticating credentials.
- The profile logs that capture when a Rippling employee is viewing a particular employee profile on the Rippling HR Platform line up with Deel's attempted poaching activities described above. Once again, Rippling investigated D.S.'s activity around the time Rippling employees were contacted by Deel representatives, and once again, Rippling learned that D.S. had accessed and viewed the profiles of several of the Rippling employees who were contacted by Deel.
- Some of the Rippling employees who received unsolicited contact from Deel expressed concern about this contact because they did not know how Deel had access to their personal data. Some of the contacted employees had not updated their public profiles on sites like LinkedIn, so Deel could not readily determine from public sources their current position in Rippling or even (for some of them) that they worked at Rippling at all. Some of the employees also noted that their phone numbers were de-listed. As a result of these employee concerns, Rippling opened a security investigation into the matter in early February 2025, but did not identify an internal source at that time. After conducting additional forensics in February and March 2025, Rippling believes that D.S. likely provided contact information on some or all of these individuals to Deel.

RIPPLING: TIP OFF LEADING TO INVESTIGATION

- On February 18, 2025, an investigative reporter at *The Information* contacted Rippling about a forthcoming article concerning Deel's Russia-related sanctions activity, noting he had "been working on a story on Deel for the past few weeks" that "started as an exercise to look into the veracity of that lawsuit I previously reported on." This reporter was referring to his January 9, 2025, article entitled "Deel Accused of Money Laundering, Sanctions Failures in Lawsuit," which reported on *Damian v. Deel Inc.*, No. 25-cv-20017 (S.D. Fla. Jan. 3, 2025).
- The reporter's email listed eleven assertions regarding supposed issues at Rippling relating to payments into Russia and other sanctioned jurisdictions. Each individual assertion was followed by internal Rippling Slack messages—thirteen messages in total—that supposedly supported or related to the assertion (the "Shared Slack Messages"). … the fact that internal Rippling Slack messages (which are only available to Rippling employees) were in the possession of someone other than a Rippling employee caused Rippling to immediately open a security investigation.

RIPPLING: SLACK INVESTIGATION (RELATED TO RUSSIA SANCTIONS)

- An analysis of the Shared Slack Messages revealed that these messages came from thirteen different channels in Rippling's Slack workspace, and that the messages all contained certain searchable keywords ("Russia," "Belarus," "Iran," "Syria," and/or "Sanctions"). Rippling's investigators proceeded to review Slack log files. Upon review, Rippling learned that a single account associated with a single Rippling employee—D.S.—had searched for specific, targeted, and highly unusual names and keywords that corresponded with the Shared Slack Messages. Rippling further learned from the various Slack logs that the searches were tied to specific internet protocol (IP) addresses associated with D.S.'s location in Ireland, strongly suggesting that it was D.S. himself (rather than someone with D.S.'s login credentials impersonating him) conducting these searches
- Rippling' forensic research revealed that D.S. had specifically conducted targeted keyword searches on each of the eleven points raised by *The Information*'s reporter in and around the time Rippling was contacted by that reporter,

RIPPLING: D.S. ENGAGED IN NON-WORK ACTIVITIES

- While D.S. was logged into his Rippling work browser on December 9, 2024, he reviewed an email to himself indicating that he had a scheduled meeting with Deel that afternoon—approximately one month after his pattern of suspicious activity began.
- D.S.'s browser history also reveals that, on that same day, he searched for an email thread with "alex@deel.com" (Deel's CEO)

RIPPLING: THE HONEYPOT

- Rippling conceived of a test (known in the security world as a "honeypot") that would leave no doubt.
- The evening of March 3, 2025, Rippling's General Counsel sent a letter to three individuals: (1) XXX1, Deel's Board Chair, Chief Financial Officer, General Counsel, and father of Deel's CEO, (2) XXX2, Deel's Head of US Legal, and (3) an employment attorney at Deel's outside law firm.
- Rippling's letter included a screenshot of a Slack message from its Chief Revenue Officer YYY, referencing a "#d-defectors" Slack channel along with three points, which were all believed to be true but redacted for dramatic effect. The screenshot and reference to #d-defectors was intended to indicate to Deel that Rippling had a Slack channel for ex-Deel employees now employed by Rippling where they shared embarrassing information about Deel and that the channel contained information which would cause negative press attention if revealed.
- In truth, the renamed #d-defectors channel did not exist until March 3, 2025 (or early morning March 4, 2025, Irish Time (UTC)). Rather than being a gathering place for ex-Deel employees, the channel was set up as part of a ruse designed to confirm that Deel was instructing D.S. to search for specific information in Rippling's Slack.
- Within hours of Rippling sending the letter referencing the #d-defectors channel—again, a channel that existed only as bait for Deel, and one which D.S. could not have known existed absent a connection between himself and Deel—D.S. ran the following searches in Slack:
  - YYY (the name of the CRO)
  - Defector
  - D-defector
- At the time the letter was sent to Deel, no one at Rippling (apart from the investigations team) had ever viewed the (new) #d-defectors channe

RIPPLING: D.S. - NOT HELPING THEMSELVES…

- Wednesday, March 12, 2025, Rippling obtained an order from the High Court in Ireland directing seizure and inspection of D.S.'s phone
- The court order required that D.S. surrender his cell phone to an independent solicitor for preservation, pending an adversarial hearing to determine whether Rippling would be entitled to access the data on the phone. The court order also included a penal endorsement, which typically all but assures compliance, as the penalty of non-compliance could lead to imprisonment.
- Served with the court order at Rippling's Dublin office, D.S. initially feigned compliance—before hiding in the bathroom and then fleeing the scene.
- After misdirecting the independent solicitor, D.S. then went into a bathroom, locking the door behind him and refusing to come out, despite the independent solicitor's repeated warnings hat these actions were in violation of the court order. Rather than comply, D.S. was heard "doing something" on his phone by the independent solicitor, who also heard D.S. flush the toilet— suggesting that D.S. may have attempted to flush his phone down the toilet rather than provide it for inspection. Later that day, Rippling had the plumbing of its Dublin offices inspected, but did not locate any mobile devices.
- While in the bathroom and continuing after leaving the bathroom, D.S. was again told repeatedly that he was required to provide the device or he would be in violation of a court order. After D.S. left the bathroom, he was informed that taking another step forward rather than handing over the phone immediately would be an additional breach of the order. D.S. then replied: "I'm willing to take that risk." D.S. then stormed out of the office and fled the scene.

APPLICATION

	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Visibility and Analytics Capability	Agency performs some performance and security monitoring of mission critical applications with limited aggregation and analytics.	Agency begins to automate application profile (e.g., state, health, and performance) and security monitoring for improved log collection, aggregation, and analytics.	Agency automates profile and security monitoring for most applications with heuristics to identify application-specific and enterprise-wide trends and refines processes over time to address gaps in visibility.	Agency performs continuous and dynamic monitoring across all applications to maintain enterprise-wide comprehensive visibility.
Automation and Orchestration Capability	Agency manually establishes static application hosting location and access at provisioning with limited maintenance and review.	Agency periodically modifies application configurations (including location and access) to meet relevant security and performance goals.	Agency automates application configurations to respond to operational and environmental changes.	Agency automates application configurations to continuously optimize for security and performance.
Governance Capability	Agency relies primarily on manual enforcement policies for application access, development, deployment, software asset management, security testing and evaluation (ST&E) at technology insertion, patching, and tracking software dependencies.	Agency begins to automate policy enforcement for application development (including access to development infrastructure), deployment, software asset management, ST&E at technology insertion, patching, and tracking software dependencies based upon mission needs (for example, with Software Bill of Materials).	Agency implements tiered, tailored policies enterprise- wide for applications and all aspects of the application development and deployment lifecycles and leverages automation, where possible, to support enforcement.	Agency fully automates policies governing applications development and deployment, including incorporating dynamic updates for applications through the CI/CD pipeline.

ANTICIPATED END OF LECTURE 8

DATA INVENTORY MANAGEMENT ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency manually **identifies and inventories some agency data** (e.g., mission critical data).	Agency begins to **automate data inventory processes for both on-premises and in cloud environments**, covering most agency data, and begins to incorporate protections against data loss.	Agency **automates data inventory and tracking enterprise-wide**, covering all applicable agency data, with **data loss preventio**n strategies based upon static attributes and/or labels.	Agency c**ontinuously inventories all applicable agency data and employs robust data loss prevention** strategies that dynamically block suspected data exfiltration.

BREAKOUT ROOM DISCUSSION PROMPT

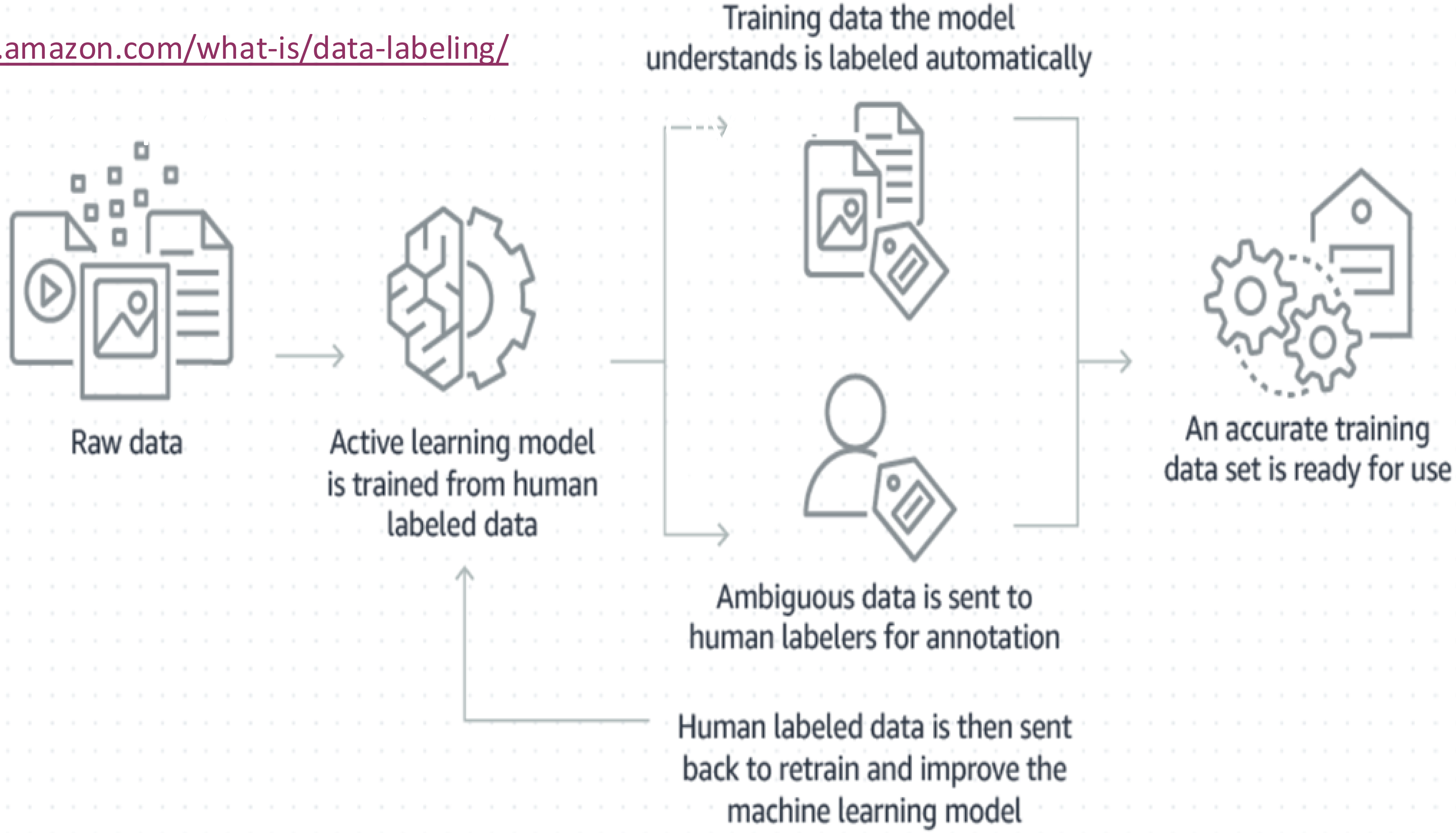
Data Inventory “for” Data Loss

- *Data Inventory allows us to know what we have, and how we have to protect it*
  - *It plays an important part of Privacy (a totally separate topic)*
- *Data Loss Prevention is “Just that”*
- *DISCUSSION*
  - *Do we really need a data inventory to have a DLP program?*
  - *What else is data inventory “required” for?*

DATA CATEGORIZATION ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency employs **limited and ad hoc data categorization** capabilities.	Agency begins to implement a **data categorization strategy with defined labels** and manual enforcement mechanisms.	Agency a**utomates some data categorization and labeling** processes in a consistent, tiered, targeted manner with simple, structured formats and regular review.	Agency automates **data categorization and labeling** enterprise-wide with robust techniques; granular, structured formats; and mechanisms to address all data types.

https://aws.amazon.com/what-is/data-labeling/



Raw data

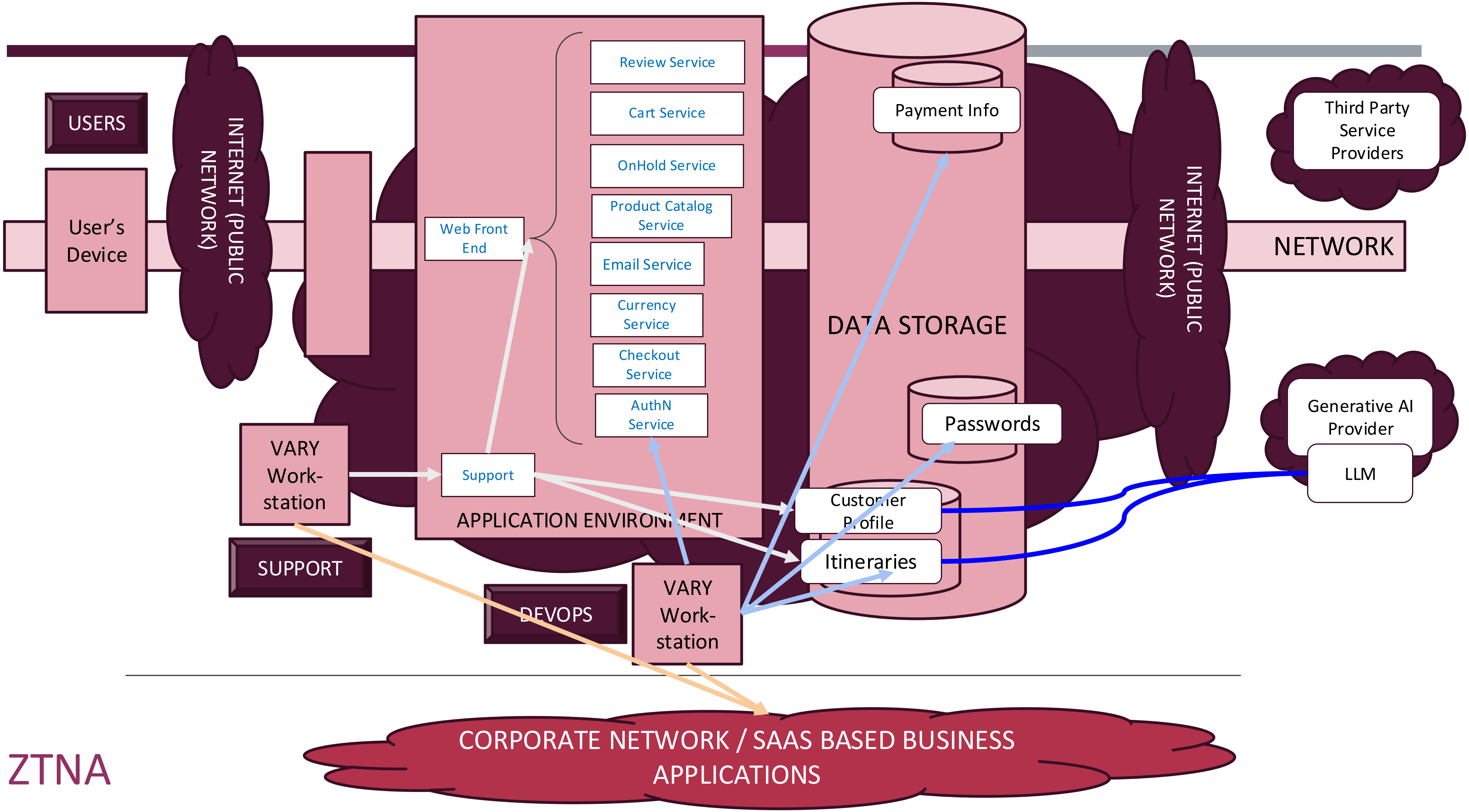
Active learning model is trained from human labeled data

Training data the model understands is labeled automatically

Ambiguous data is sent to human labelers for annotation

Human labeled data is then sent back to retrain and improve the machine learning model

An accurate training data set is ready for use


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

ZTNA

IN CLASS POLL DISCUSSION PROMPT

Data categorization implies that some data is “more important / valuable” than other data - that is, that we may need to protect some data differently from other data

- *What can go wrong with data categorization - how “many” categories should you have?*
  - *Public*
  - *Confidential*
  - *Sensitive/secret*
  - *Protected (PHI, PII)*
  - *Top Secret*

BREAKOUT DISCUSSION PROMPT

What can go right, what can go wrong, with the set of categories the (majority) of the class identified?

- *Public*
- *Confidential*
- *Sensitive/secret*
- *Protected (PHI, PII)*
- *Top Secret*

DATA AVAILABILITY ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency primarily makes data available from **on-premises data stores with some off-site backups.**	Agency makes some data available from r**edundant, highly available data stores (e.g., cloud) and maintains off-site backups for on- premises data.**	.Agency primarily makes **data available from redundant, highly available data stores and ensures access to historical data.**	Agency uses **dynamic methods to optimize data availability,** including historical data, according to user and entity need.

BREAKOUT DISCUSSION PROMPT

Data Availability is (usually) all about High Availability, Backup and Recovery

Observations

  - *Moving up the maturity scale implies moving to cloud for data availability*
  - *Backups for OnPrem data include Offsite*
    - *But Offsite is not called out as part of Cloud*

- *Questions*
  - *What has this got to do with Zero Trust?*
  - *What could go wrong following this maturity progression?*

DATA ACCESS ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency governs user and entity access (e.g., permissions to read, write, copy, grant others access, etc.) to data through **static access controls.**	Agency begins to deploy **automated data access** controls that incorporate **elements of least privilege across** the enterprise.	Agency **automates data access controls that consider various attributes** such as identity, device risk, application, data category, etc., and are time limited where applicable.	Agency a**utomates dynamic just-in-time and just-enough data access controls enterprise-wide** with continuous review of permissions.

BREAKOUT DISCUSSION PROMPT

Data Access

Observations

  - *Least privilege not called out across the board (goes from LP to “just enough” without progression)*
  - *Increasing maturity focuses on automation and “more rich” access control decisions*

- *Questions*
  - *Dynamic, just-in-time and just-enough sounds really hard : is it worth it? Where should this be part of discipline?*
  - *Would this help in cases of social engineering of user access?*

DATA ENCRYPTION ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency **encrypts minimal agency data at rest and in transit** and relies on manual or **ad hoc processes to manage and secure encryption keys.**	Agency **encrypts all data in transit and, where feasible, data at rest** (e.g., mission critical data and data stored in external environments) and **begins to formalize key management policies and secure encryption keys**	Agency e**ncrypts all data at rest and in transit across the enterprise** to the maximum extent possible, begins to **incorporate cryptographic agility**, and **protects encryption keys** (i.e., secrets are not hard coded and are rotated	Agency **encrypts data in use** where appropriate, **enforces least privilege principles for secure key management** enterprise-wide, and **applies encryption using up-to-date standards and cryptographic agility** to the extent possible

BREAKOUT DISCUSSION PROMPT

Data Encryption

Observations

    - *So either this maturity model is all over the board OR most environments that i know of a totally mixed bag of maturity*

- *Questions*
    - *Initial: EiT ALL, where possible EaR*
        - *Is this backwards?*
    - *Advanced: Protect encryption keys*
        - *Isn’t this a bit “late”?*
    - *From your experience, is this a sensible progression?*
    -

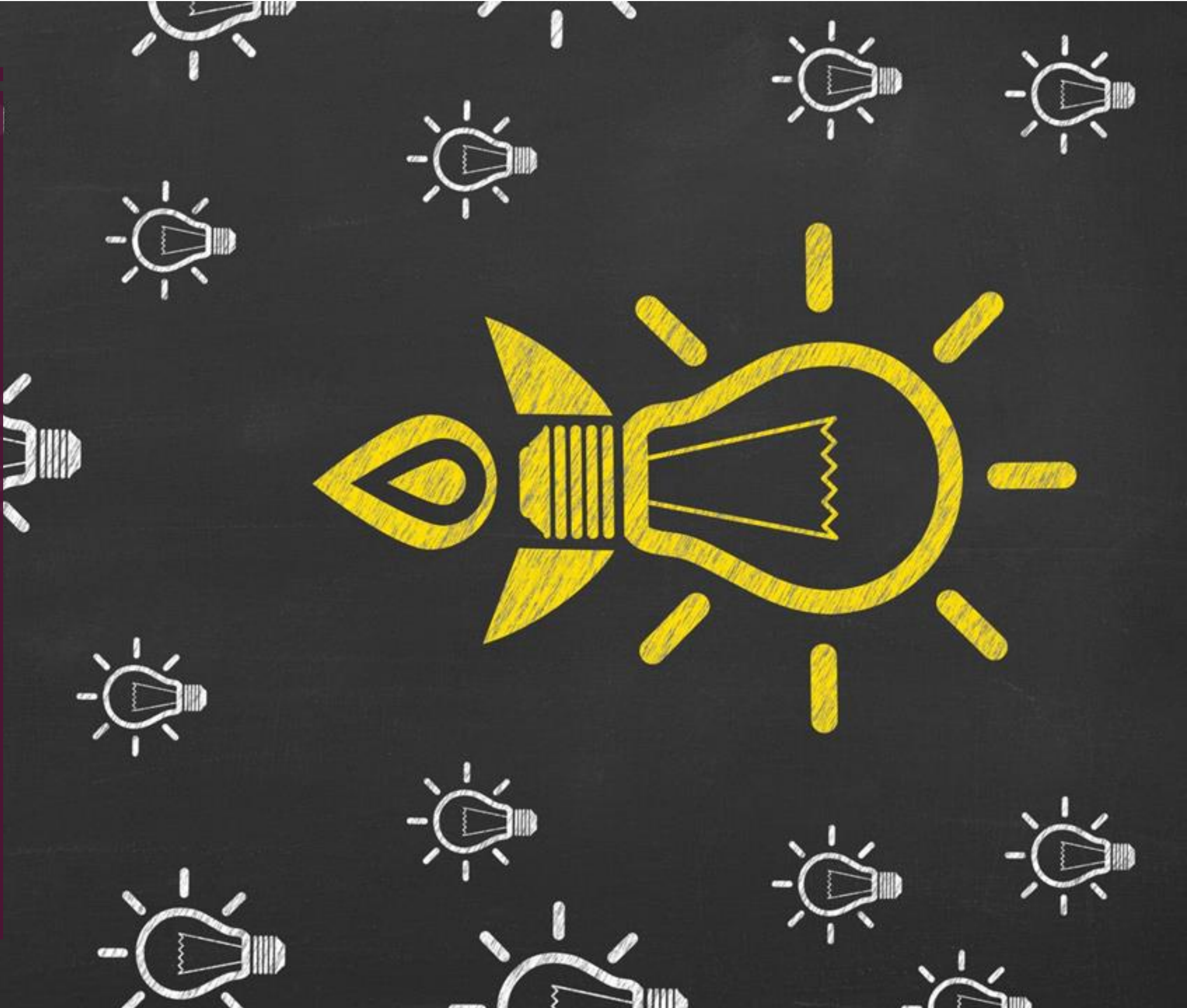
	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
DATA **Visibility and Analytics Capability**	Agency has limited visibility into **data** including location, access, and usage, with analysis consisting primarily of manual processes.	Agency obtains visibility based on data inventory management, categorization, encryption, and access attempts, with some automated analysis and correlation.	Agency maintains data visibility in a more comprehensive, enterprise-wide manner with automated analysis and correlation and begins to employ predictive analytics.	Agency has visibility across the full data lifecycle with robust analytics, including predictive analytics, that support comprehensive views of agency data and continuous security posture assessment.
Automation and Orchestration Capability	Agency implements data lifecycle and security policies (e.g., access, usage, storage, encryption, configurations, protections, backups, categorization, sanitization) through manual, and potentially ad hoc, processes.	Agency uses some automated processes to implement data lifecycle and security policies.	Agency implements data lifecycle and security policies primarily through automated methods for most agency data in a consistent, tiered, targeted manner across the enterprise.	Agency automates, to the maximum extent possible, data lifecycles and security policies for all agency data across the enterprise.
Governance Capability	Agency relies on ad hoc data governance policies (e.g., for protection, categorization, access, inventorying, storage, recovery, removal, etc.) with manual implementation.	Agency defines high-level data governance policies and relies primarily on manual, segmented implementation.	Agency begins integration of data lifecycle policy enforcement across the enterprise, enabling more unified definitions for data governance policies.	Agency data lifecycle policies are unified to the maximum extent possible and dynamically enforced across the enterprise.

BREAKOUT ROOM DISCUSSION PROMPT

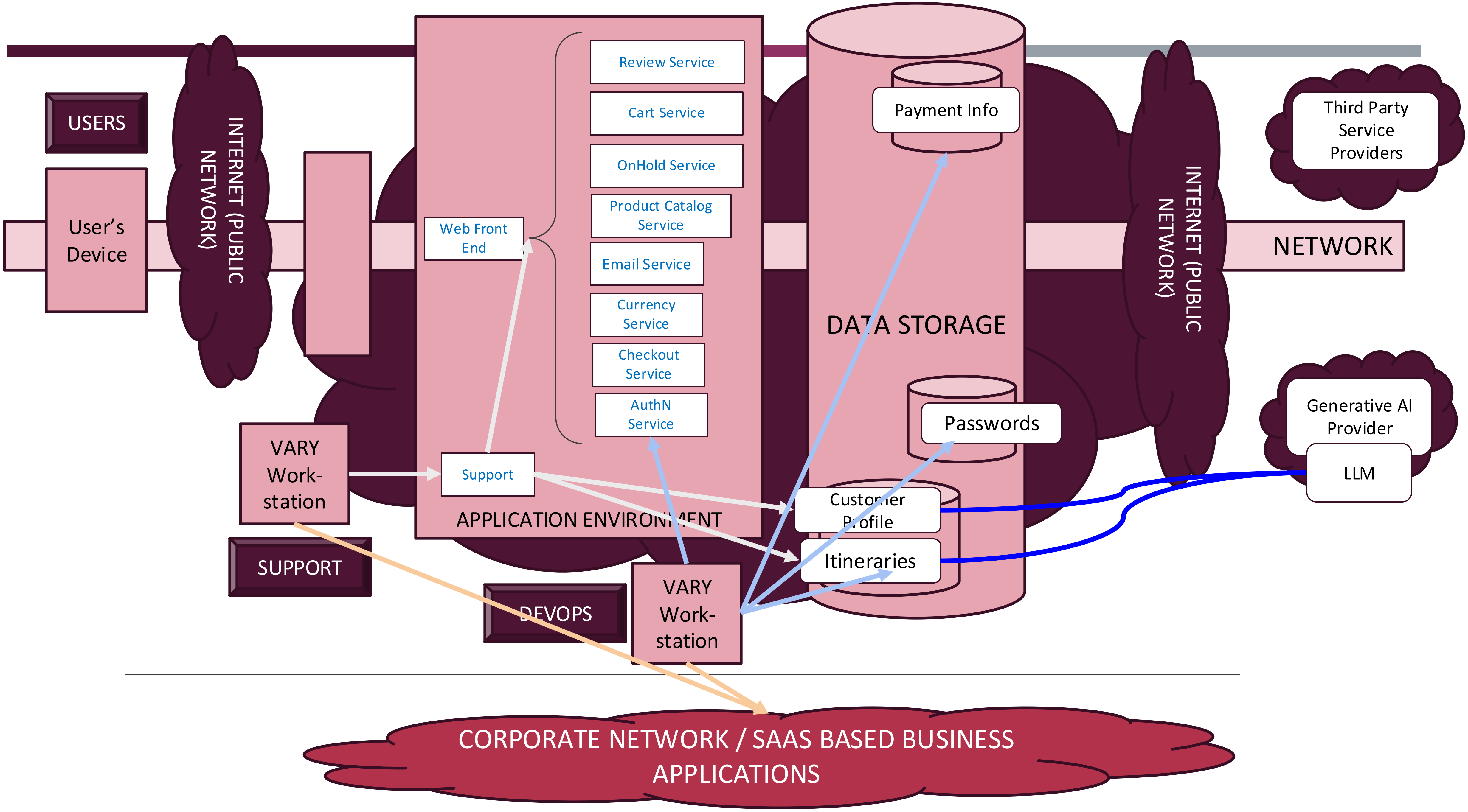
- *You are in charge of application security for your firm*
- *You have budget to do EITHER*
    - *Move each Functional area to INITIAL maturity*
- *OR*
    - *Move each Capability area to INITIAL maturity*
- *Do they have the same result?*
- *Which is going to be more impactful for overall posture?*
- *(Think ransomware!!!)*

ANTICIPATED END OF LECTURE 8

REFERENCE STUFF



10 min
BREAK
BACK
9:05PM ET



USERS

User's Device

INTERNET (PUBLIC NETWORK)

Web Front End

Review Service

Cart Service

OnHold Service

Product Catalog Service

Email Service

Currency Service

Checkout Service

AuthN Service

Support

APPLICATION ENVIRONMENT

DATA STORAGE

Payment Info

Passwords

Customer Profile

Itineraries

INTERNET (PUBLIC NETWORK)

Third Party Service Providers

NETWORK

Generative AI Provider

LLM

VARY Workstation

SUPPORT

DEVOPS

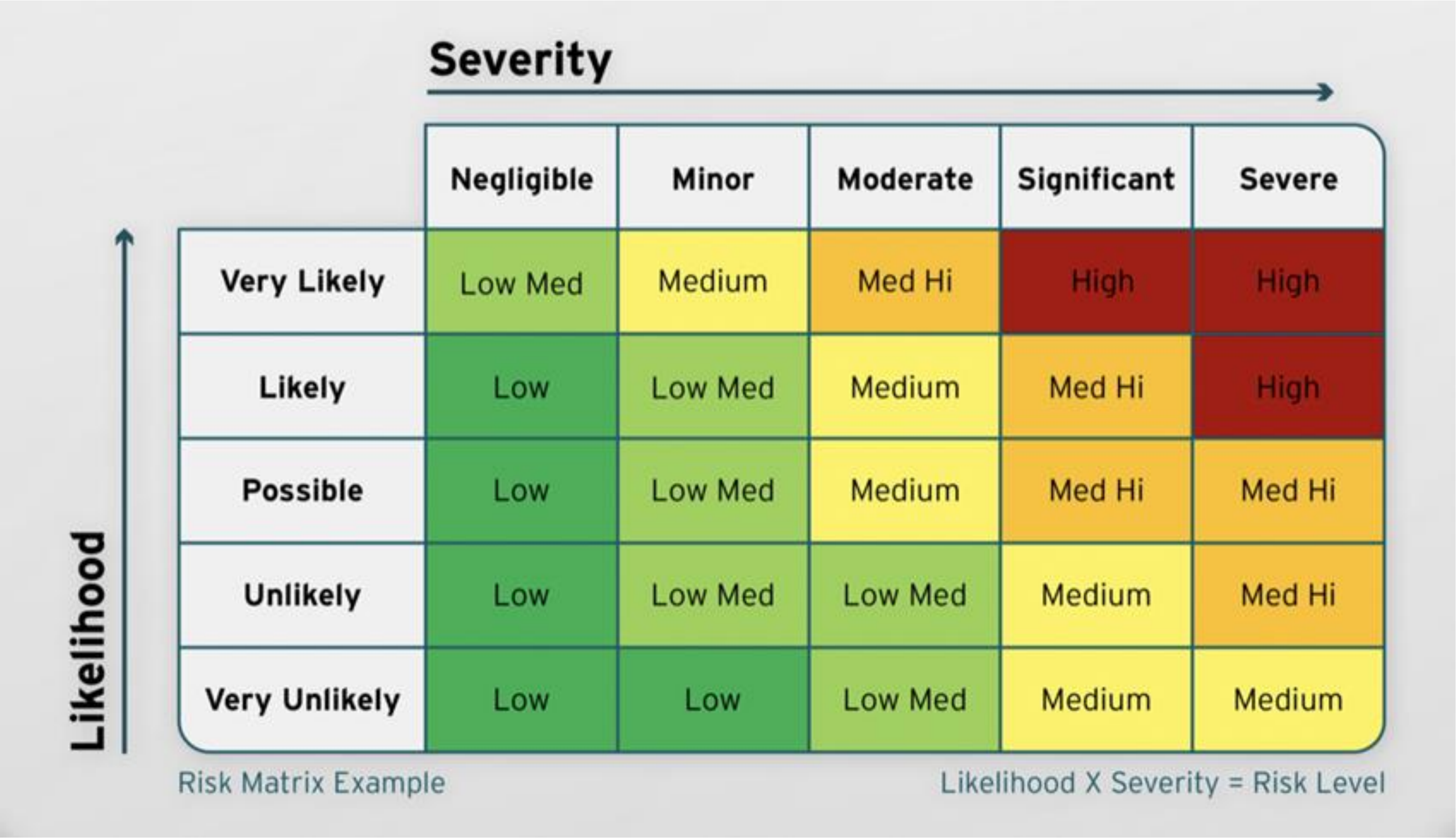
VARY Workstation

CORPORATE NETWORK / SAAS BASED BUSINESS APPLICATIONS

RISK ASSESSMENT MATRIX

A risk assessment matrix identified IMPACT or CONSEQUENCES based on

- the *likelihood* the risk event will occur, and,
- the potential *severity* of the risk event



Severity

Likelihood

	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Risk Matrix Example

Likelihood X Severity = Risk Level

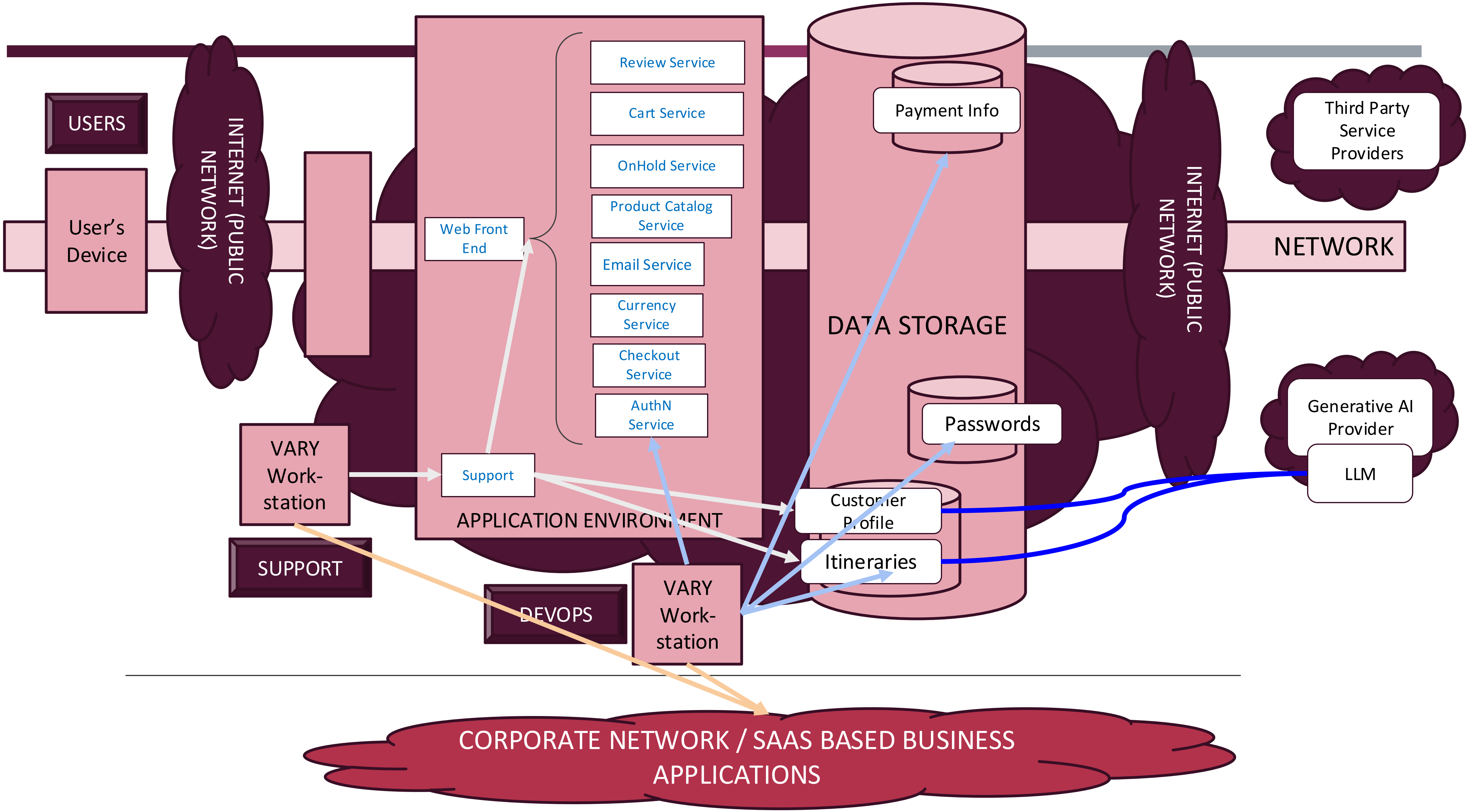
COURSE “USE CASE / CASE STUDY”

- We are going to use a fictional company with a web-facing application throughout the course, to illustrate concepts and decision points IF AND WHEN NEEDED

- OUR course use case : “Vacations and Rest for You” (VARY)

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

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



USERS

User's Device

INTERNET (PUBLIC NETWORK)

Web Front End

Review Service

Cart Service

OnHold Service

Product Catalog Service

Email Service

Currency Service

Checkout Service

AuthN Service

Support

APPLICATION ENVIRONMENT

Payment Info

DATA STORAGE

Passwords

Customer Profile

Itineraries

INTERNET (PUBLIC NETWORK)

Third Party Service Providers

NETWORK

Generative AI Provider

LLM

VARY Work-station

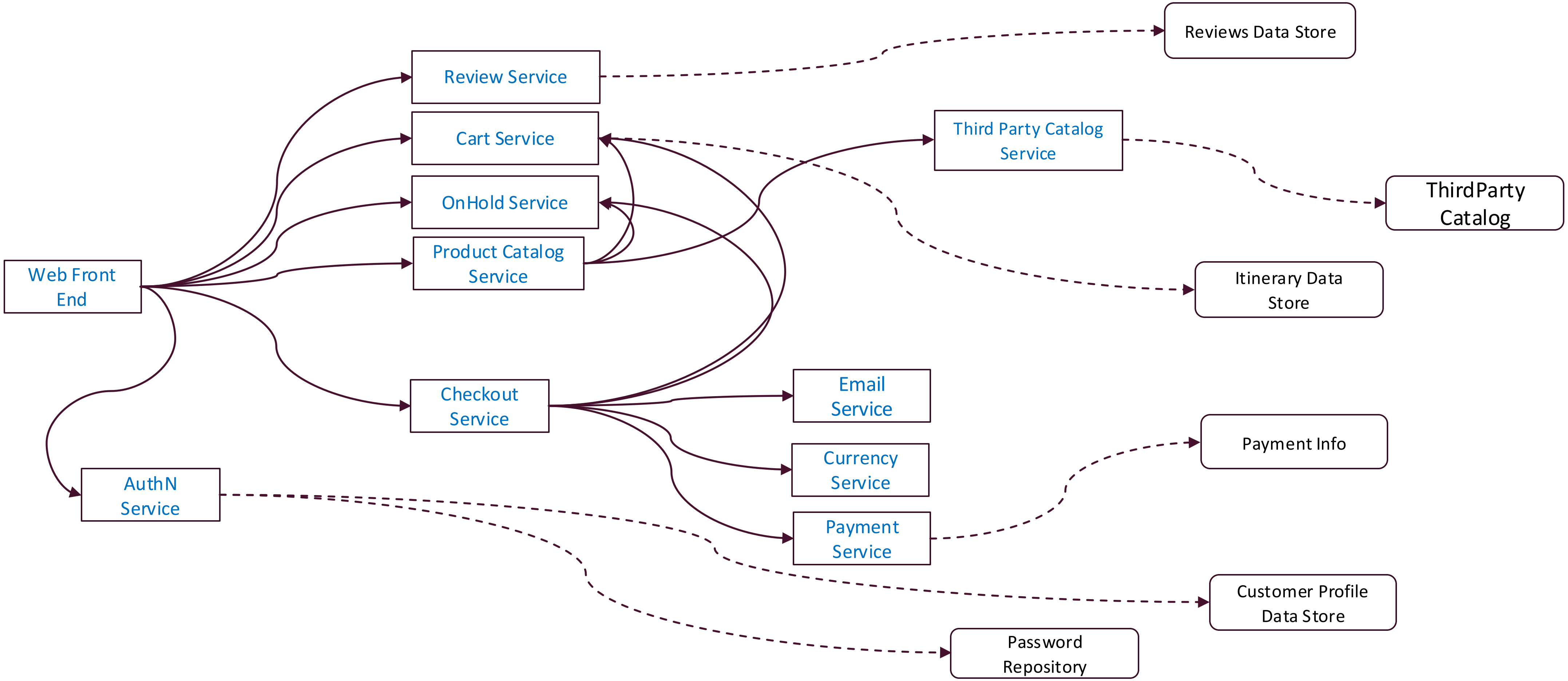
SUPPORT

DEVOPS

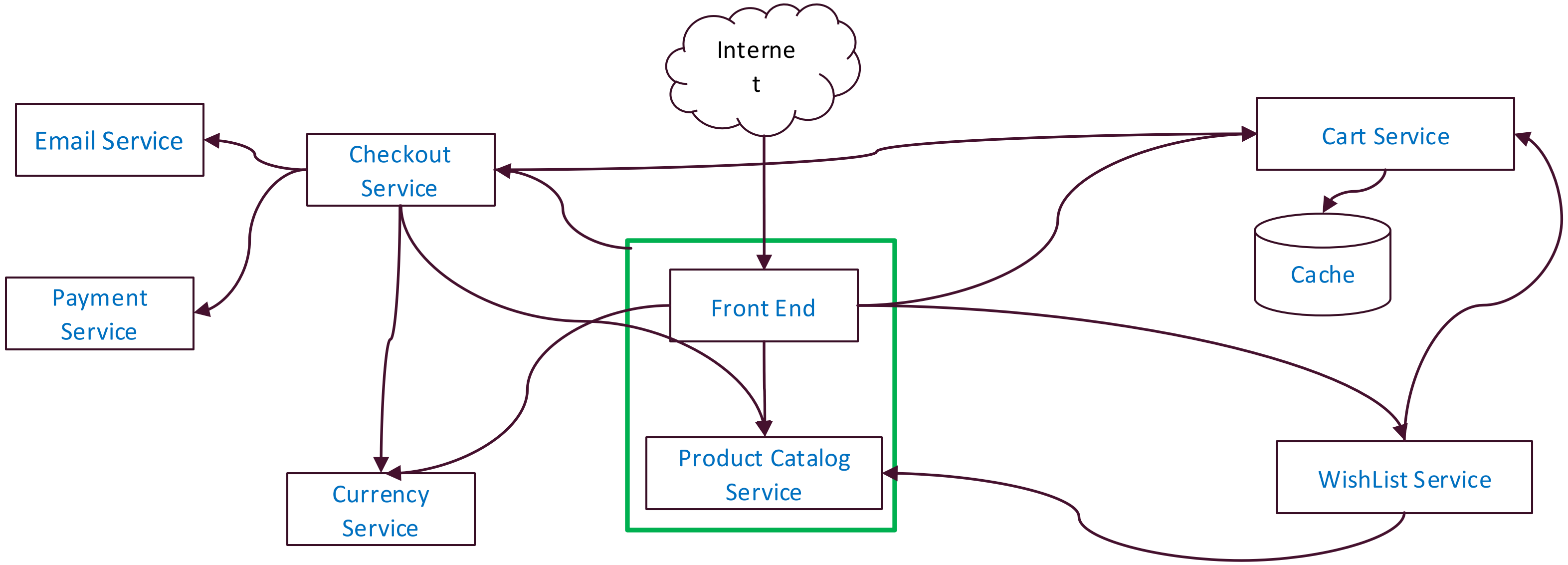
VARY Work-station

CORPORATE NETWORK / SAAS BASED BUSINESS APPLICATIONS

VARY SERVICE ARCHITECTURE



VARY APPLICATION: RESERVATION/CHECKOUT


Interne
t
Email Service
Checkout Service
Cart Service
Cache
Payment Service
Front End
Product Catalog Service
Currency Service
WishList Service