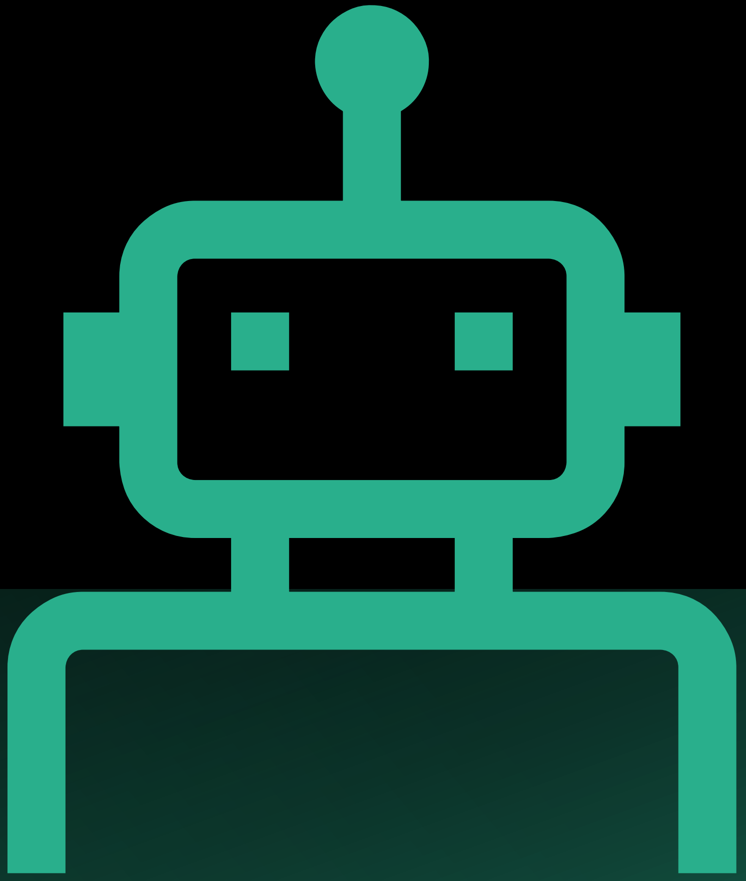
Effectively Integrating AI into Cybersecurity Practitioner’s Toolbox



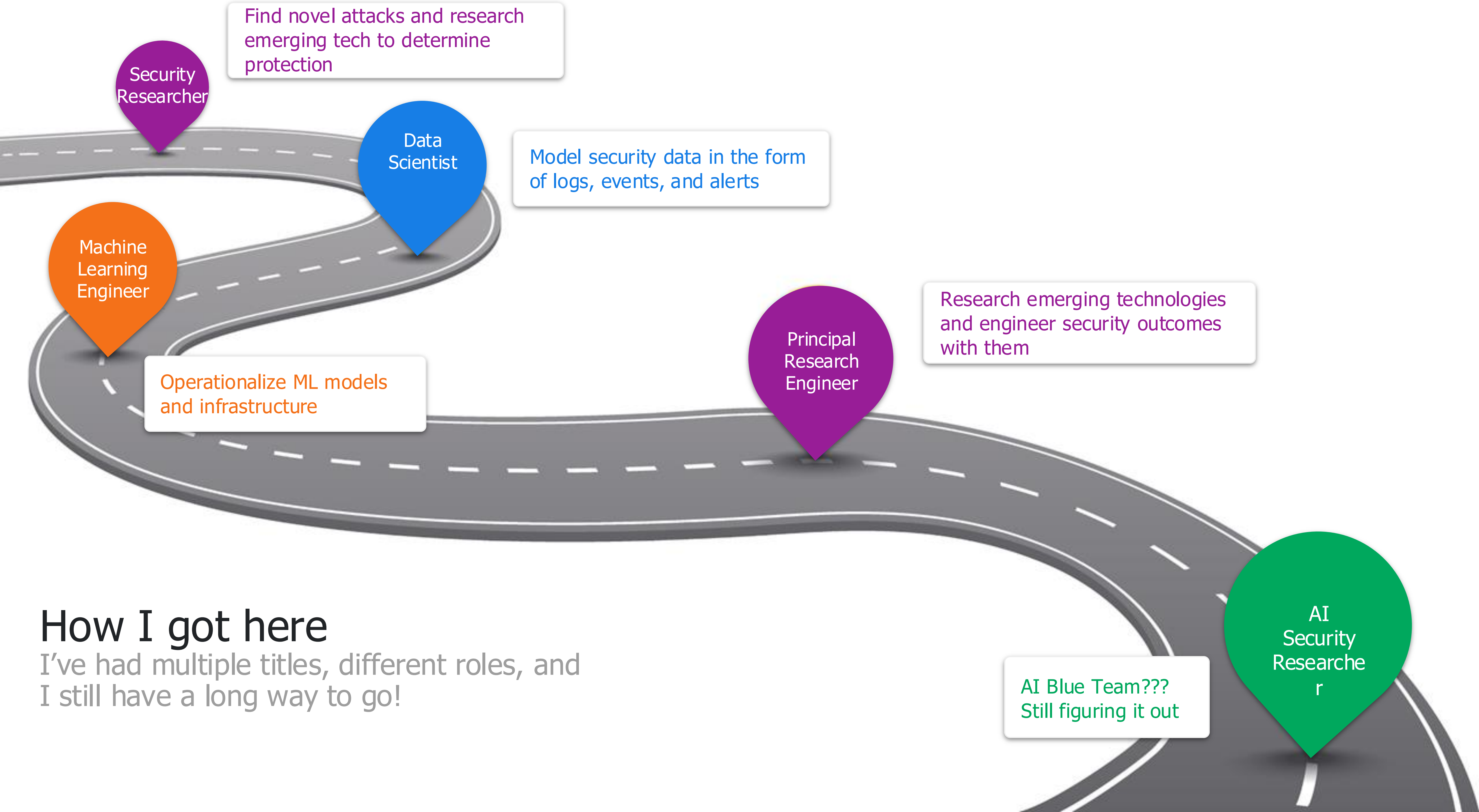
Preeti Ravindra & Sheryl Takahashi

Liaison: Prajna Bhandary

whoami - Preeti

- Security generalist, AI specialist
- Seen 'em all: Security vendors, enterprise security teams, services ranging from startups to Fortune 100 companies
- Speaker at security and AI conferences
- Claim to Fame: Inventor on 3 patents, industry first AI product for SIEM
- Outside of work: Boardgame lover, meme enthusiast, dark theme fanatic, enjoys being walked by dogs

Preeti Ravindra



How I got here

I've had multiple titles, different roles, and I still have a long way to go!

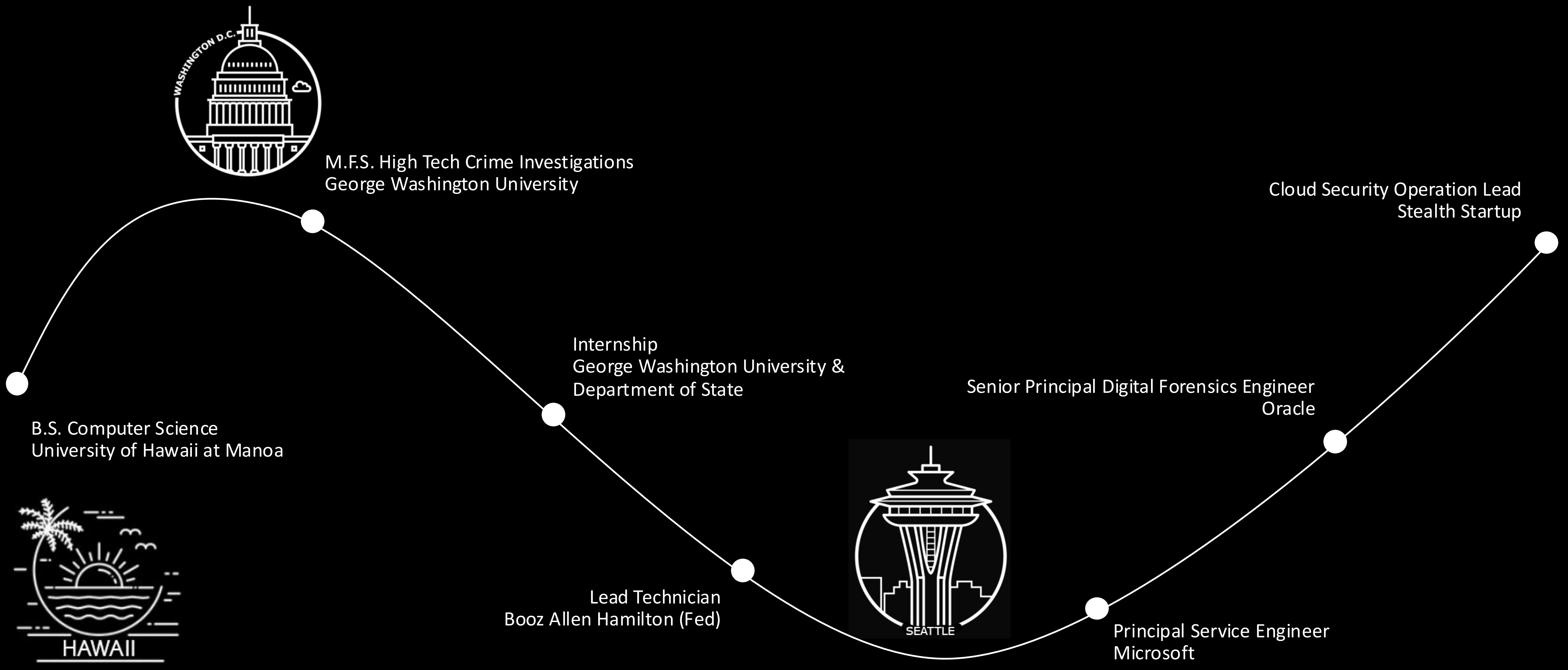
whoami – Sheryl

- Cloud Security Operations Lead, Stealth Startup
- Digital Forensics, Incident Response, SOC Analyst
- Federal Government, major corporations, start ups
- Claim to Fame: Lead for several incidents involving A.P.T. attacks (with whiteboard diagramming and art)
- Outside of work: Video games, arts & crafts, corgi-mama (by marriage)

Sheryl Takahashi
Linkedin.com/in/sheryltakahashi

How I Got Here

Sheryl Takahashi
Linkedin.com/in/sheryltakahashi



whoami – Prajna

- PhD Candidate, University of Maryland, Baltimore County(UMBC)
- Cybersecurity Specialist, Threat Intel, Software Engineer
- Research: Malware Analysis using Machine Learning, AI
- Claim to Fame: Teaching Assistant for "almost" all courses of Undergrad CS courses
- Outside of work: Video games, Board Games, Cooking, and diving into anything I hold no knowledge of yet.

Prajna Bhandary
Linkedin.com/in/pjbhandary

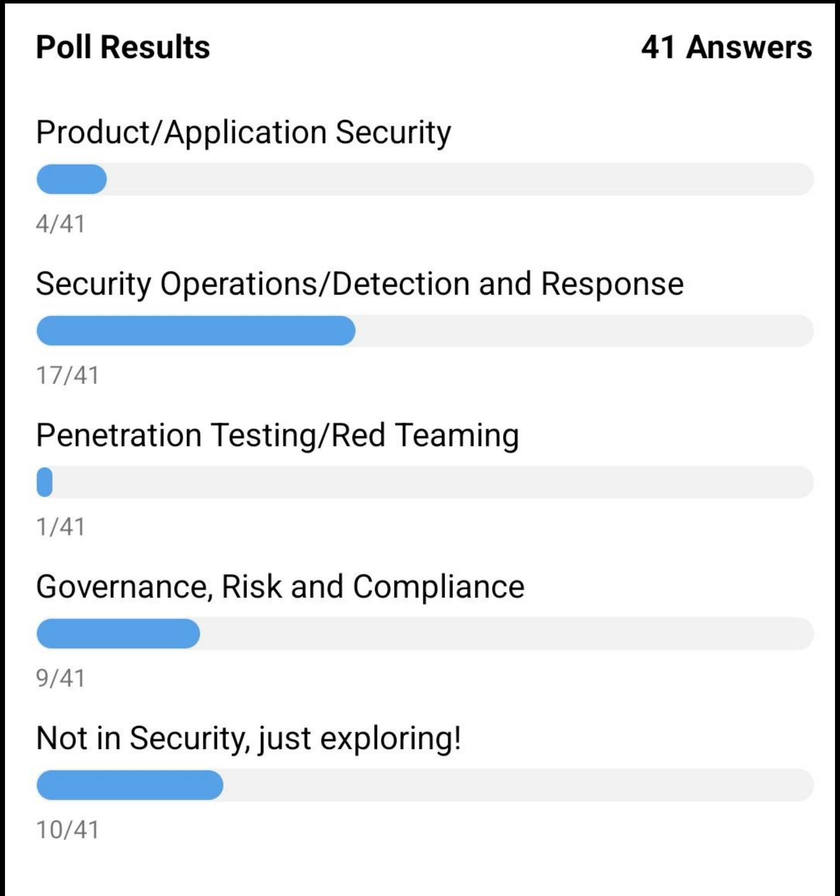
“We must find the time to stop and thank those people who make a difference in our lives”

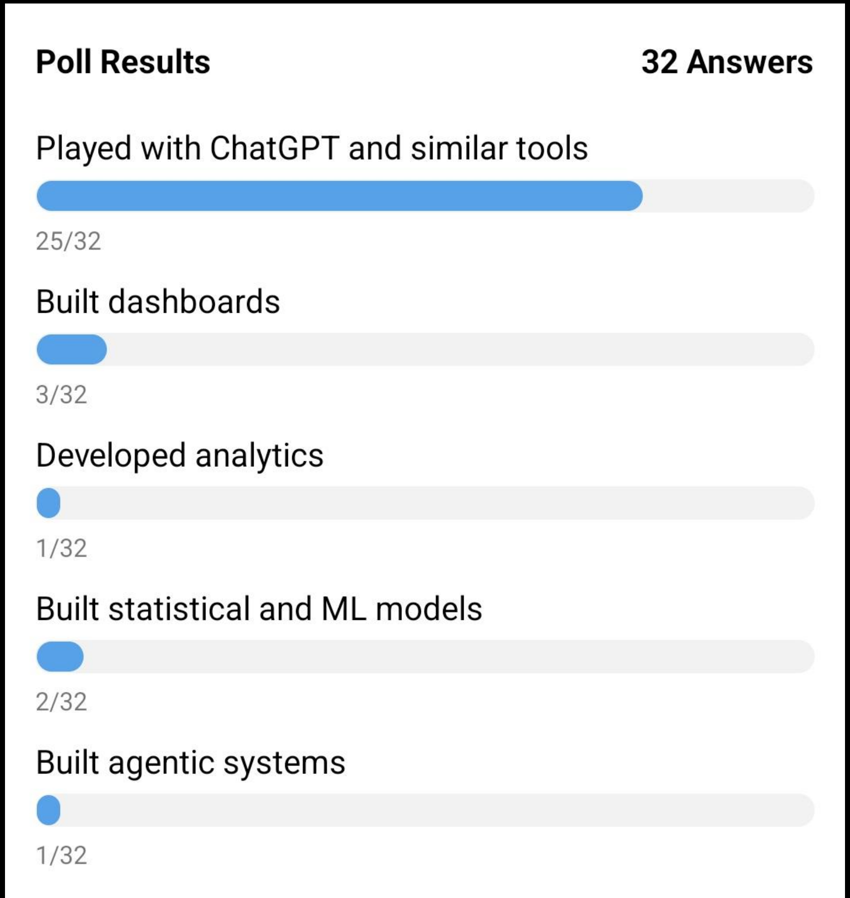
John F. Kennedy

Jessie Jamieson
Craig Chamberlain
Xenia
Robert Freeman
Santosh Kandala
Arun Kannawadi
Kristina Laidler
Troy Larson
Bret Arsenault
Andrew McHarg & Pontus

Show of Hands

Survey Results





Agenda

Setup

4 exercises

Concepts

Hands-on-keyboard

Discussion/Q&A

Goals

Make math less scary

Make AI tools more accessible

Non-Goals

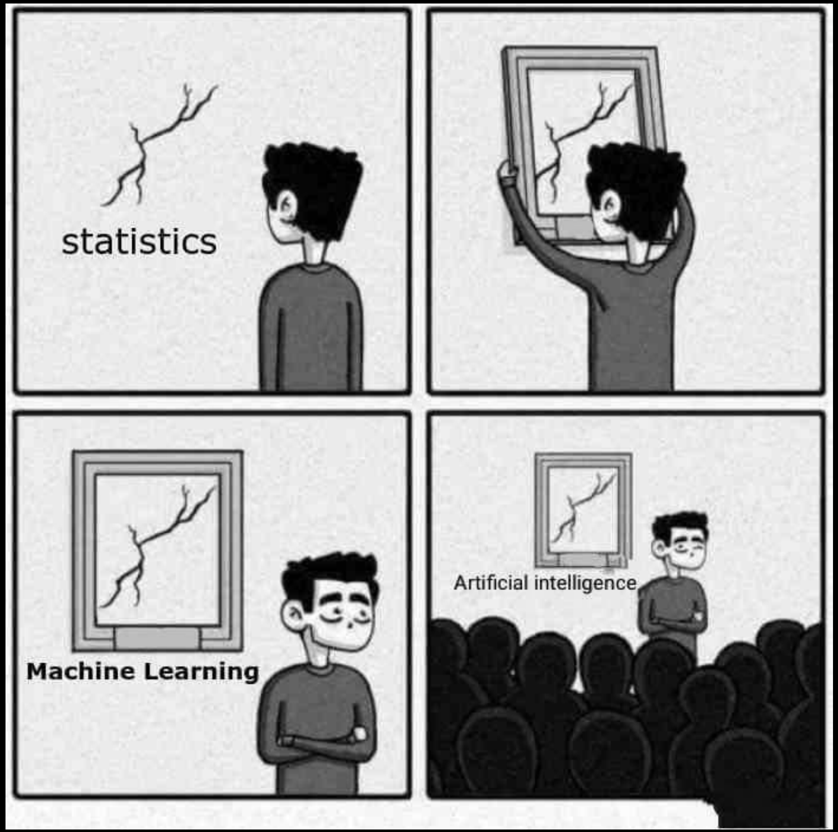
Coding AI algorithms

Focus on LLMs exclusively

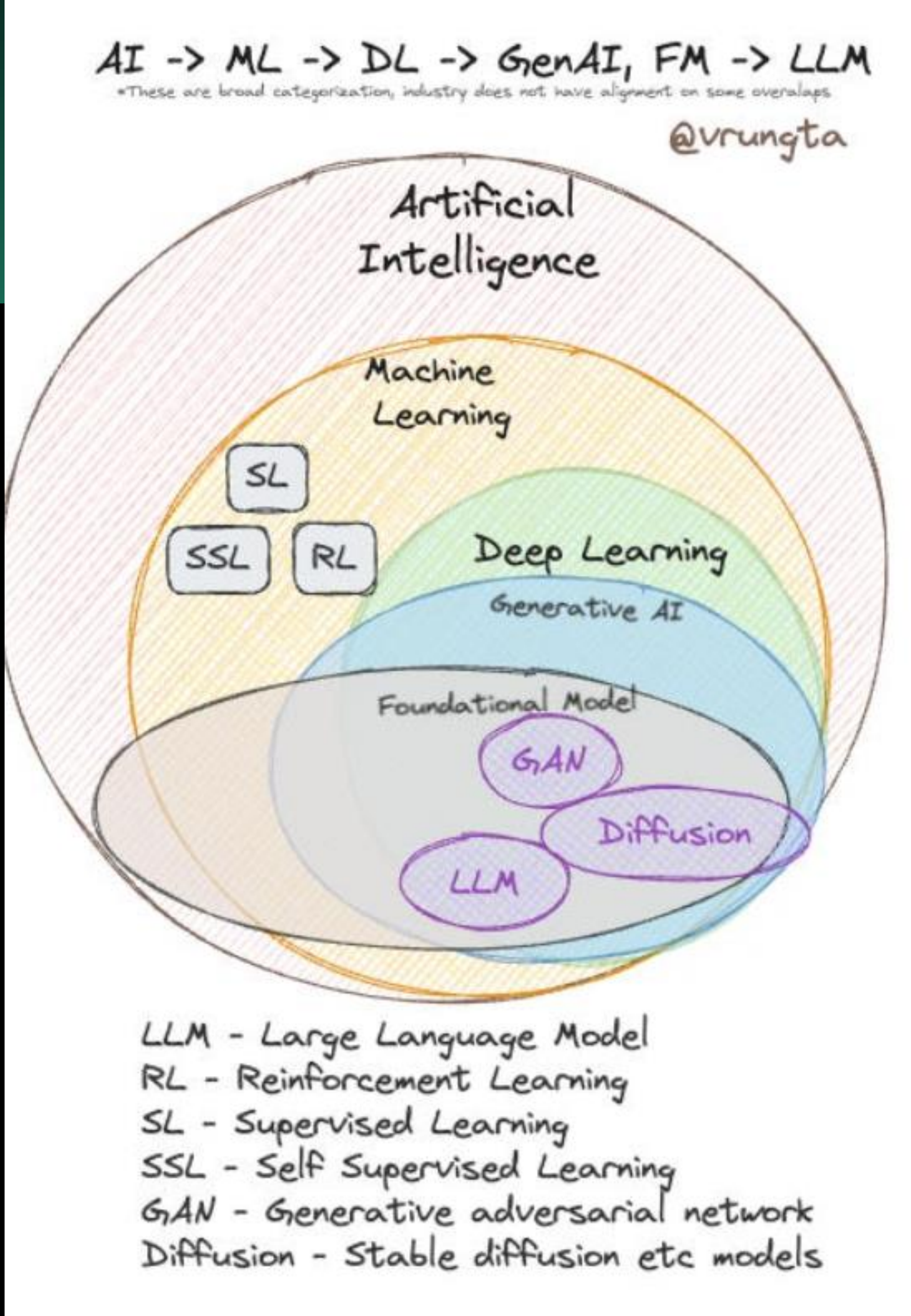
Setup

10:00

What is AI?



statistics
Machine Learning
Artificial intelligence



AI -> ML -> DL -> GenAI, FM -> LLM
*These are broad categorization, industry does not have alignment on some overalaps
@vrungta
Artificial Intelligence
Machine Learning
SL
SSL
RL
Deep Learning
Generative AI
Foundational Model
GAN
Diffusion
LLM
LLM - Large Language Model
RL - Reinforcement Learning
SL - Supervised Learning
SSL - Self Supervised Learning
GAN - Generative adversarial network
Diffusion - Stable diffusion etc models

Flavors of AI and Security

**AI for
offensive applications**

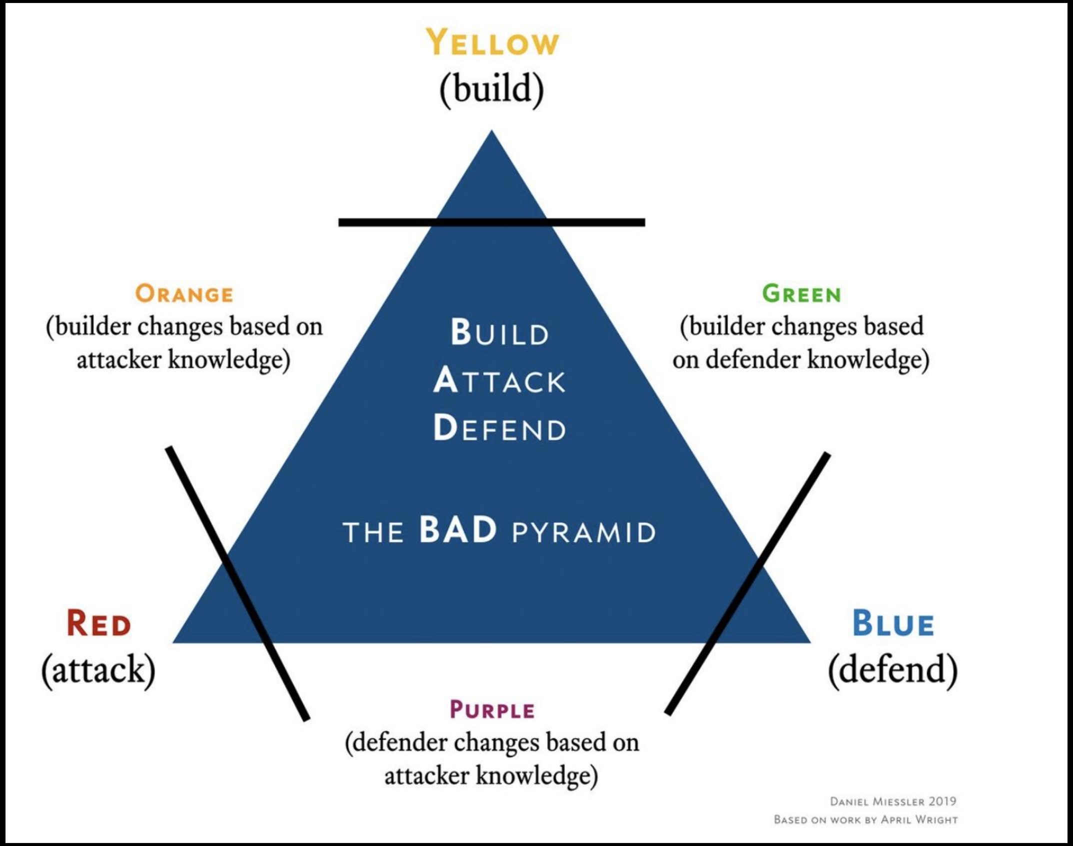
**AI for
defensive applications**

Adversarial AI

**Secure and
trustworthy ML**


ML and AI for security is snake oil
CHANGE MY MIND

Why data skills?



Skills evolution

SOC Analyst/ Incident Responder

Data Analyst

Security Engineer

Data Engineer/ AI Engineer

Threat Researcher

Data Scientist

STATE OF DETECTION ENGINEERING

Current		Need Development	
76%	**Understanding/ mapping attack frameworks** This reflects the organizations' strong adoption of frameworks like MITRE ATT&CK for threat detection and security program development.	53%	**Threat modeling** Teams are recognizing the importance of proactive security architecture and attack path mapping.
74%	**Triage & incident response** As the second most valuable skill set, it demonstrates that detection engineering teams maintain strong operational security skills essential for effective threat response.	52%	**Data engineering** This highlights the growing need for security professionals who can effectively manage and analyze large security datasets.
67%	Processing/ querying languages (e.g. SPL, SQL, KQL)	47%	**Reporting/ visualization** This indicates that teams struggle to communicate their findings and metrics to key stakeholders effectively.
61%	Regular expressions	47%	Software engineering
60%	Threat intelligence / research analysis	46%	Detection-as-code, CI/CD
54%	Documentation	45%	Log pipeline monitoring and health

80% of surveyed detection engineers said their organizations are putting real money behind DE

The majority of detection engineers reported that their organizations are actively funding detection engineering, with investment rising to 85% among large enterprises (5,000+ employees). The takeaway is clear: detection engineering isn't just being adopted—it's becoming a strategic priority.

Leadership support is strong, but understanding still lags

Most detection engineers (67%) reported strong leadership buy-in, with some even saying it's viewed as "the future" of security. For those without strong backing, the main reason is clear: detection engineering is still misunderstood in some organizations. The takeaway? Education and communicating the ROI to leaders will be key in closing the gap.

From tactical to strategic: custom behavioral detections take the lead

Organizations are shifting from tactical alerting relying mostly on vendor-provided rules to strategic, custom-built detections. The top detection type preferred is behavior-based (67%), and custom-derived detections were the most common source (42%). Only 2% relied solely on vendor-provided detections. As detection engineering matures, threat modeling (53%) has emerged as a key skill for teams looking to level up.

Data access and quality remain a key challenge

Detection engineering is only as strong as the data that fuels it. But for many teams, access and quality remain major obstacles. Our survey revealed a near-even split between those with adequate data access and those hitting roadblocks that limit their detection capabilities. Data engineering (52%) is now a top skill gap that detection teams are looking to close.

Automation is thriving, AI is arriving

Participants overwhelmingly believe AI will play a major role in detection engineering (88% in the next three years), and today, 45% of organizations have already integrated AI into their detection workflows. Automation adoption shows stronger momentum, with 93% of organizations using or planning to implement automation in their workflows.

Anvilogic State of Detection 2025 Report

Data to AI

Decision Support/Automation

Descriptive

Diagnostic

Predictive

Prescriptive

Our Philosophy

Lesson 1

Security Scenario

Vuln Management

- Scan Objectives
  - Identify vulnerabilities in environment
  - Assess risks of identified vulnerabilities
  - Plan mitigation or acceptance of risk
- Vendor Data
  - Pros: Constant and reliable scans to see trends and identify possible systemic issues
  - Cons: Vendor (default) tailors results for user and may not have details needed in data nor context to apply to user's environment

Descriptive Statistics

"Our comforting conviction that the world makes sense rests on a secure foundation: our almost unlimited ability to ignore our ignorance."

- Daniel Kahneman, Thinking, Fast and Slow

There is a difference between…

{ Asking Questions + Having Data } VS { Asking the ***Right*** Questions + Having the ***Right*** Data }

The most robust institutions don't just collect data – they produce ***actionable intelligence*** that *serves* a holistic, proactive, and adaptable security strategy

Descriptive Statistics

Type 1: Descriptive Data Science

Answers the question, “What happened?”

- Basic statistics and visualizations
- Often critical for **orienting** to a problem, decision, or event
- Typically conveyed in reports, slide decks, or dashboards
- May include some trend analysis

Examples:

Software Investment

The following software packages are present in our environment...

Incident Response

A compromise has occurred affecting the following environments...

Maturity

Descriptive

Descriptive Statistics

Descriptive Data Science: Adding Rigor

Statistical and scientific rigor can elevate your analysis

- Define clear objectives and research questions
- Formulate hypotheses and design experiments to test hypotheses
- Engage in exploratory data analyses often
- Verify assumptions, parameters, and methods used to analyze the data
- Conduct peer reviews of your analyses and methodologies

Exercise 1

05:00

Discussion

Lesson 2

Security Scenario

Mirai

Mirai Botnet

- First detected in 2016 as a self-propagating worm
  - Exploitation of Remote Services, Technique T0866 - ICS | MITRE ATT&CK®
- Infected IoT devices used to scan the internet to find additional vulnerable targets
  - Internet Accessible Device, Technique T0883 - ICS | MITRE ATT&CK®
- Attacker collects vulnerable targets to create a botnet
  - 1Tbps and is estimated to have used about 145,000 devices
  - Acquire Infrastructure: Botnet, Sub-technique T1583.005 - Enterprise | MITRE ATT&CK®

CISecurity - The Mirai Botnet – Threats and Mitigations

Security Scenario

Investigation - Hunting

- Indicators of compromise (IOCs)
- Tactics, Techniques, and Procedures (TTPs)
- Querying internal environment
- Referencing OSINT
- Identify vulnerabilities / gaps

Diagnostic Data Science

Type 2: Diagnostic Data Science

Answers the question, “Why did it happen?”

- Beginning stages of inference and narrative
- Correlations, variable analysis, and even regression analysis
- Descriptive analytics coupled with statistical rigor

Examples:

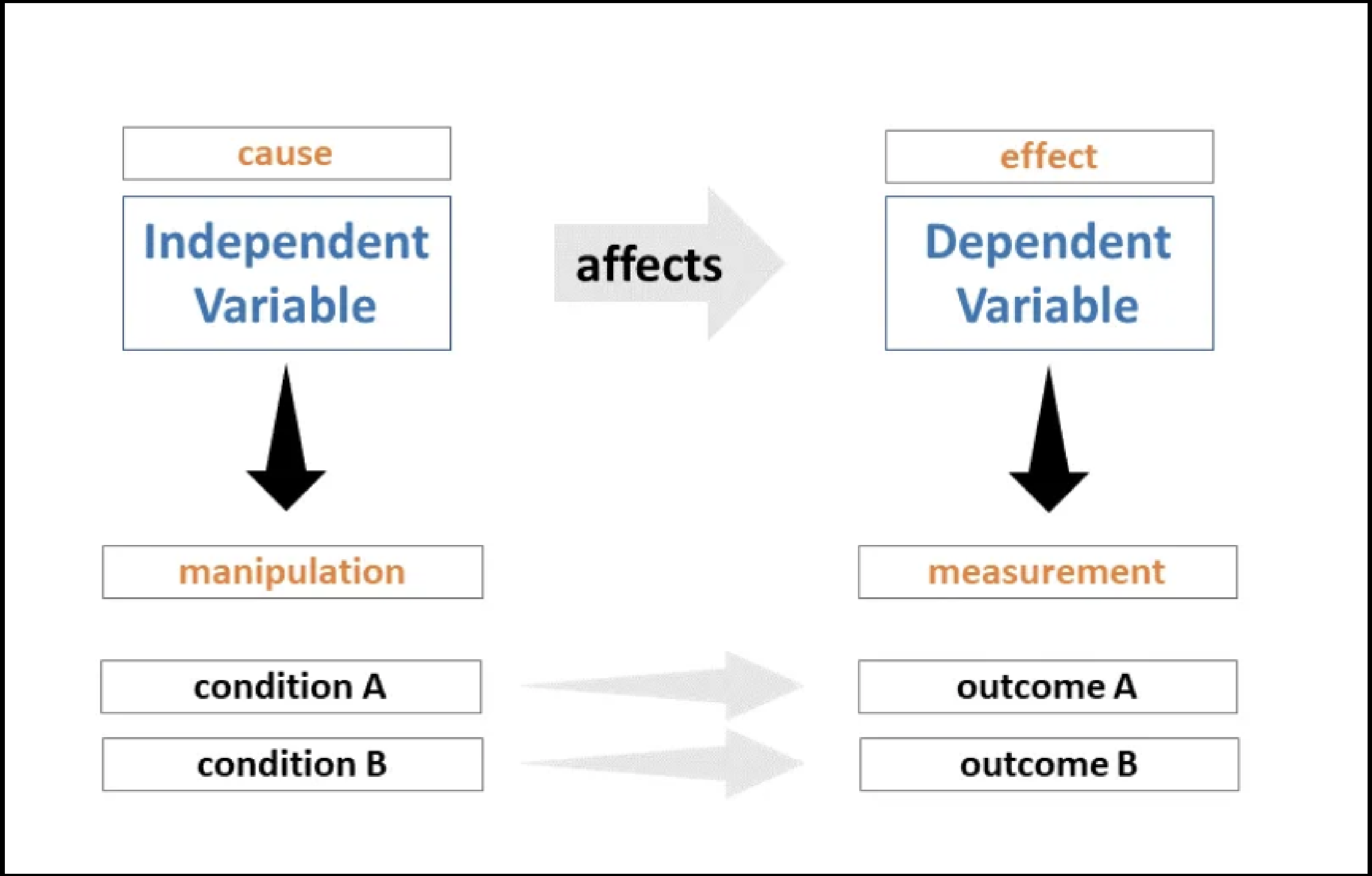
Software Investment

We use the software packages for these essential functions and job roles…

Incident Response

These software characteristics tend to correlate with patterns of compromise…

Lesson



cause
Independent Variable
affects
effect
Dependent Variable
manipulation
measurement
condition A
condition B
outcome A
outcome B

Exercise 2

10:00

Discussion

Break

Lesson 3

Security Scenario

Network Analyst

- Security Tools, When they are helpful vs when they are not
  - Network Data
- What to look for in this type of data
- Implications of botnet/DDoS attacks (Mirai data)

Exercise 3a

Predictive Data Science

Type 3: Predictive Data Science

Answers the question, “What is likely to happen?”
- Forecasts, models, and theorizations
- Advanced analytics, such as machine learning algorithms
- Learning from the past
- Diagnostic analytics looking forward

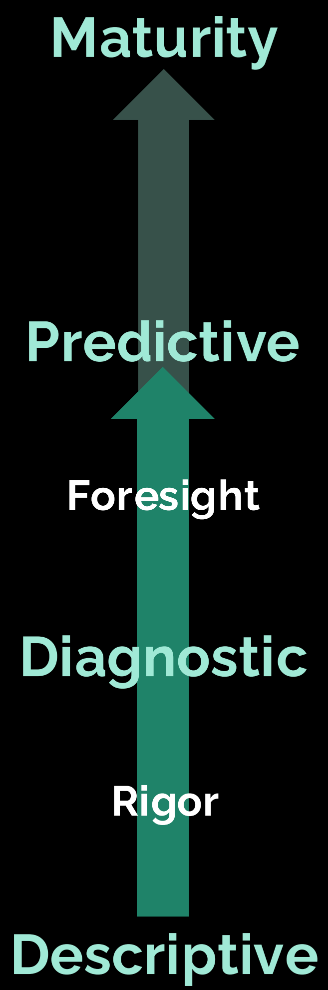
Examples:

Software Investment

These will be the effects of a software compromise:...

Post-Incident Response

We predict the following future attack attempts:...



Predictive Data Science

Predictive Data Science: Thinking Ahead

Data analyses coupled with elements of structured analytical techniques tend to be forward-looking

- Timeline analysis and retrospectives/prospectives– can you use the past to predict the future?
- Structured project planning and risk assessments
- Project/analysis pre-mortems
- Indication and warning (I&W) analysis
- Continuous feedback and improvement

Correlation and Feature Engineering

id	color
1	red
2	blue
3	green
4	blue

One Hot Encoding

id	color_red	color_blue	color_green
1	1	0	0
2	0	1	0
3	0	0	1
4	0	1	0

To GPT or To Not

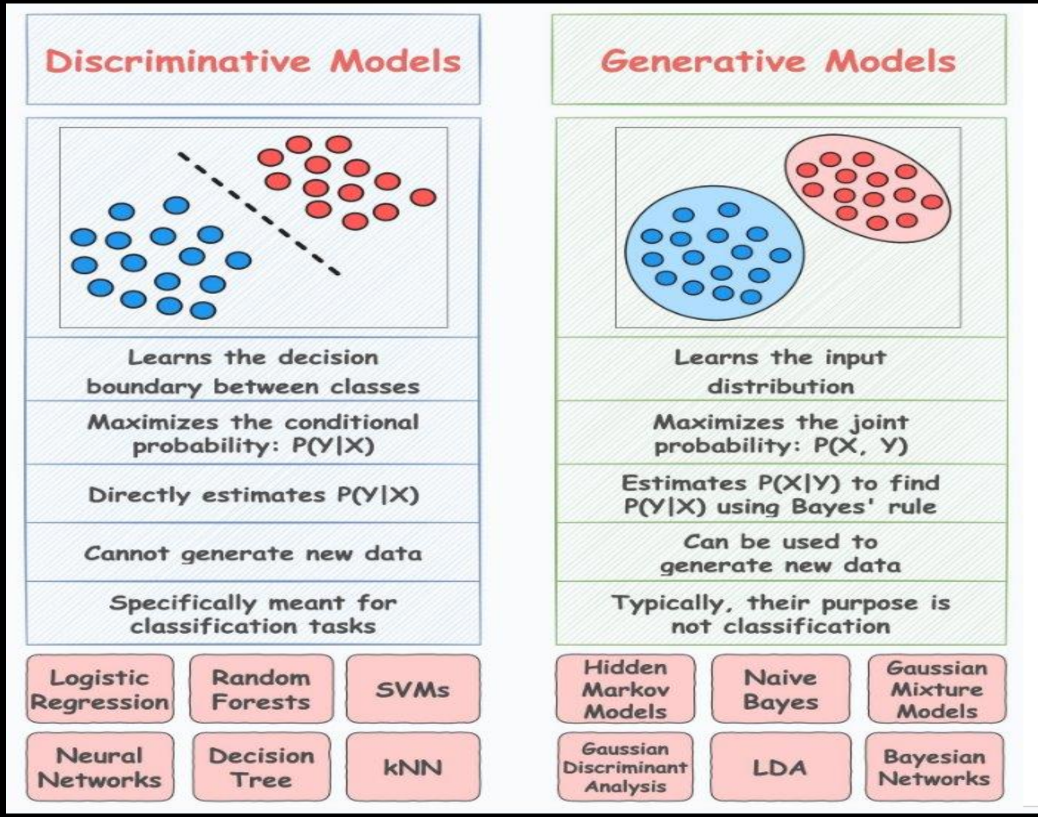
Answer in only one word, either YES or NO.

1. Can you detect false positive and true positive alerts in security?

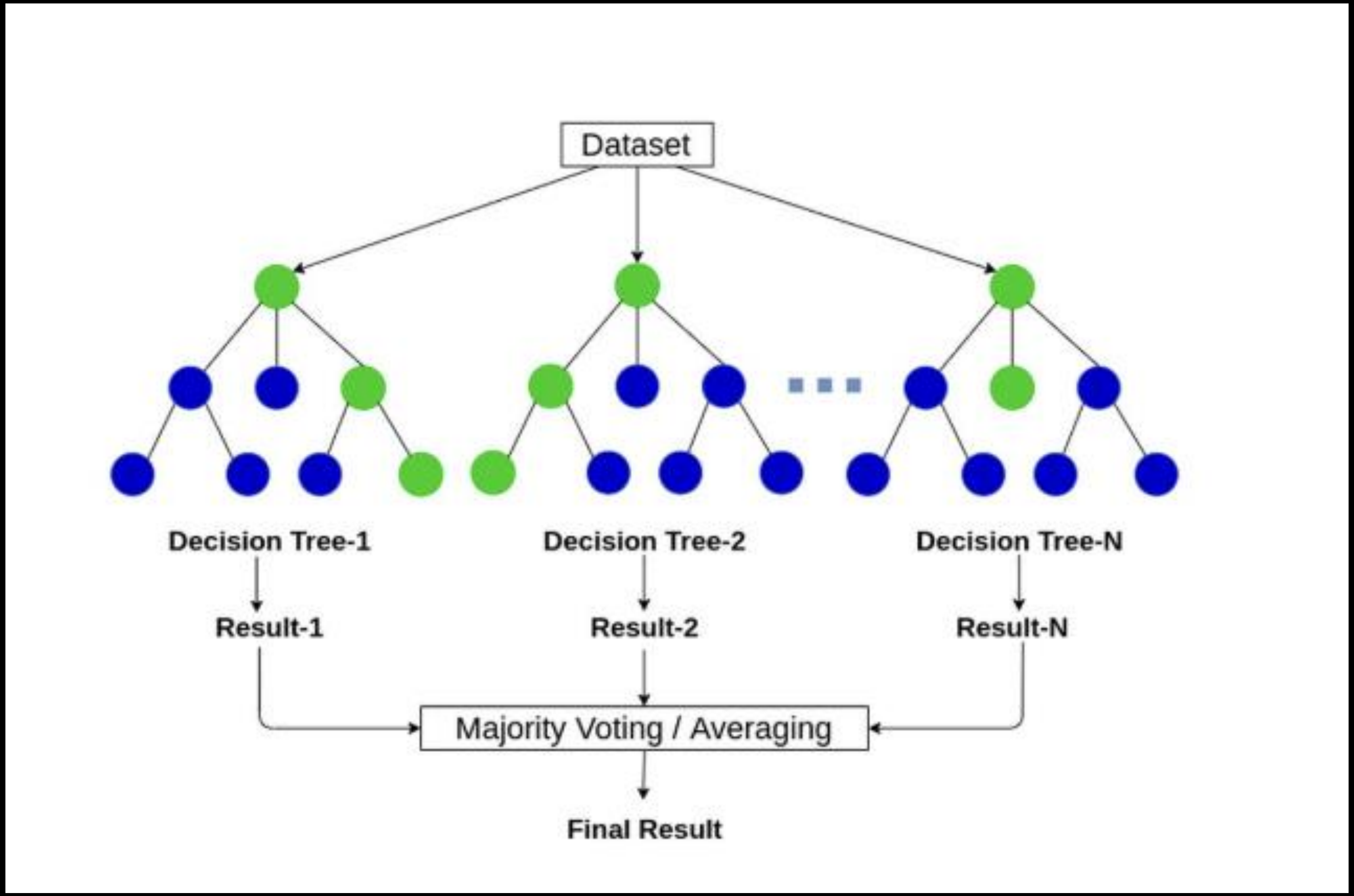
NO

What types of models can I use to do this? Answer in lesser than 3 sentences

You can use **logistic regression**, **decision trees**, or **random forests** for structured data analysis, and **neural networks** for complex patterns. For security alerts, **anomaly detection models** like Isolation Forest or Autoencoders are effective. Ensemble methods or XGBoost can also boost predictive accuracy.



Classification Algorithms



Exercise 3b

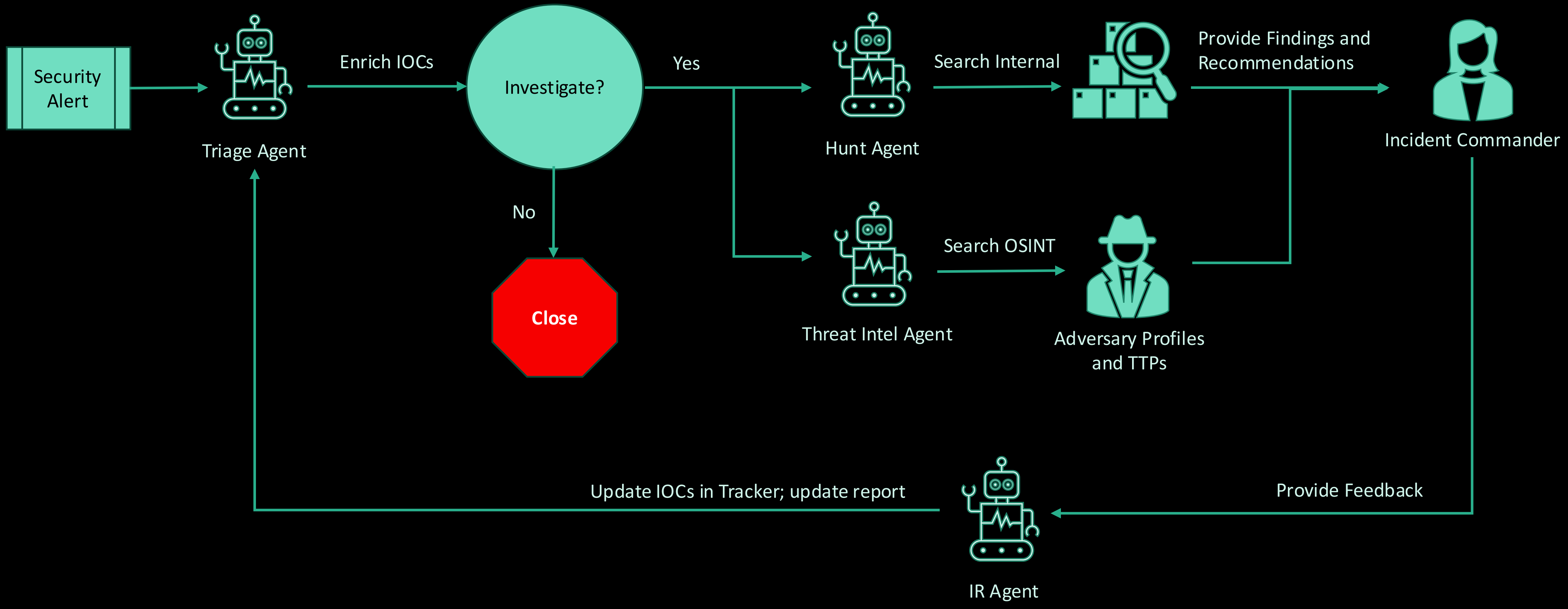
Exercise 3

10:00

Discussion

Lesson 4

Response Workflow



Prescriptive Data Science

Type 4: Prescriptive Data Science

Answers the question, “What should we do next?”

- Data-driven organizational strategy and outcome optimization
- Course of action development
- May require in-house algorithms unique to your use cases
- **Predictive analytics coupled to organisational goals**

Examples:

Software Investment

Our software procurement strategy should change, and here’s how.

Post-Incident Response

We can tolerate <these> risks, and should adapt accordingly.

Agency and Autonomy Levels

	AI agent	AI assistant	Bot
Purpose	Autonomously and proactively perform tasks	Assisting users with tasks	Automating simple tasks or conversations
Capabilities	Can perform complex, multi-step actions; learns and adapts; can make decisions independently	Responds to requests or prompts; provides information and completes simple tasks; can recommend actions but the user makes decisions	Follows pre-defined rules; limited learning; basic interactions
Interaction	Proactive; goal-oriented	Reactive; responds to user requests	Reactive; responds to triggers or commands

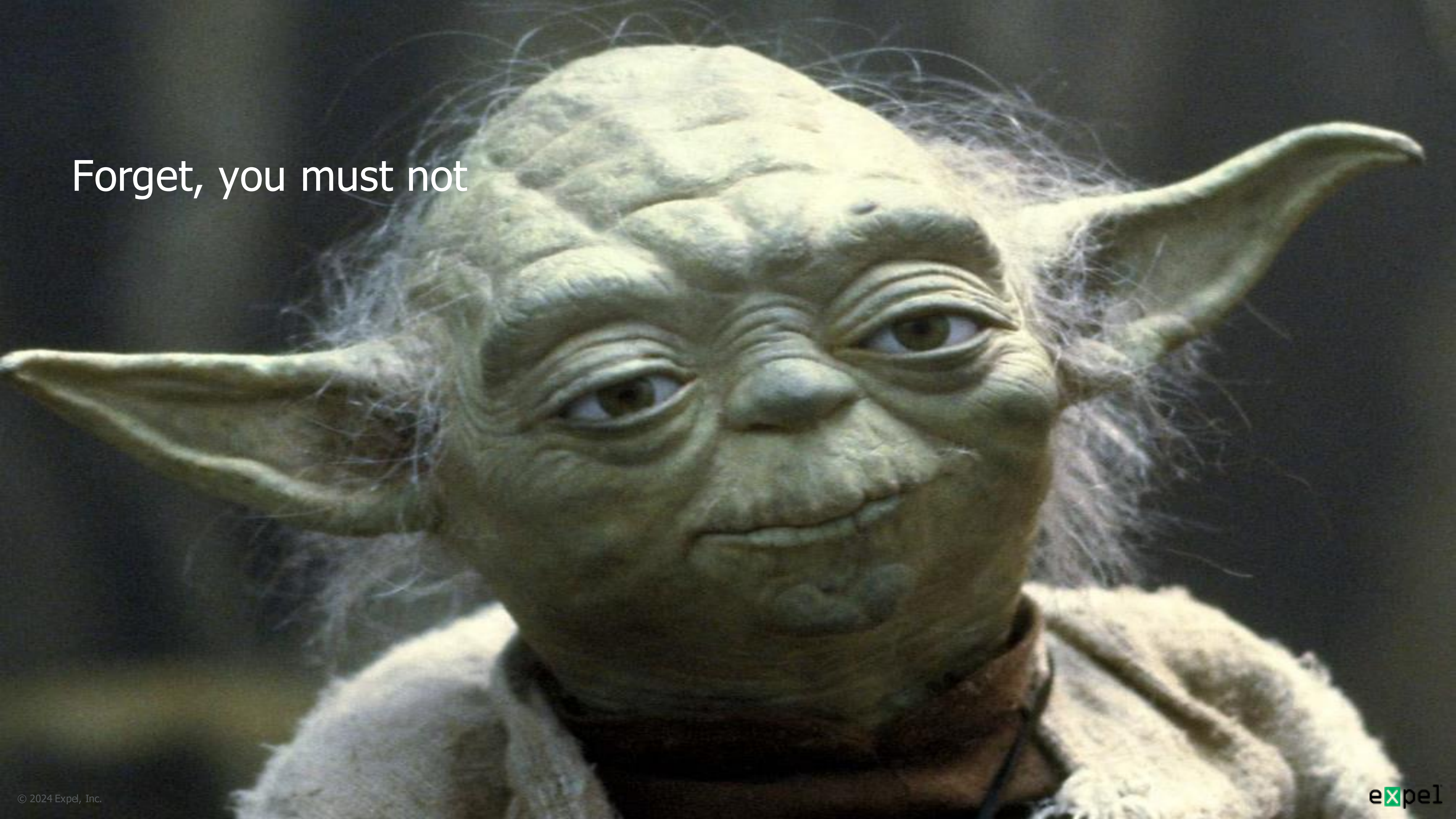
Google Cloud

Exercise 4

Discussion

Survey

Forget, you must not



Takeaways

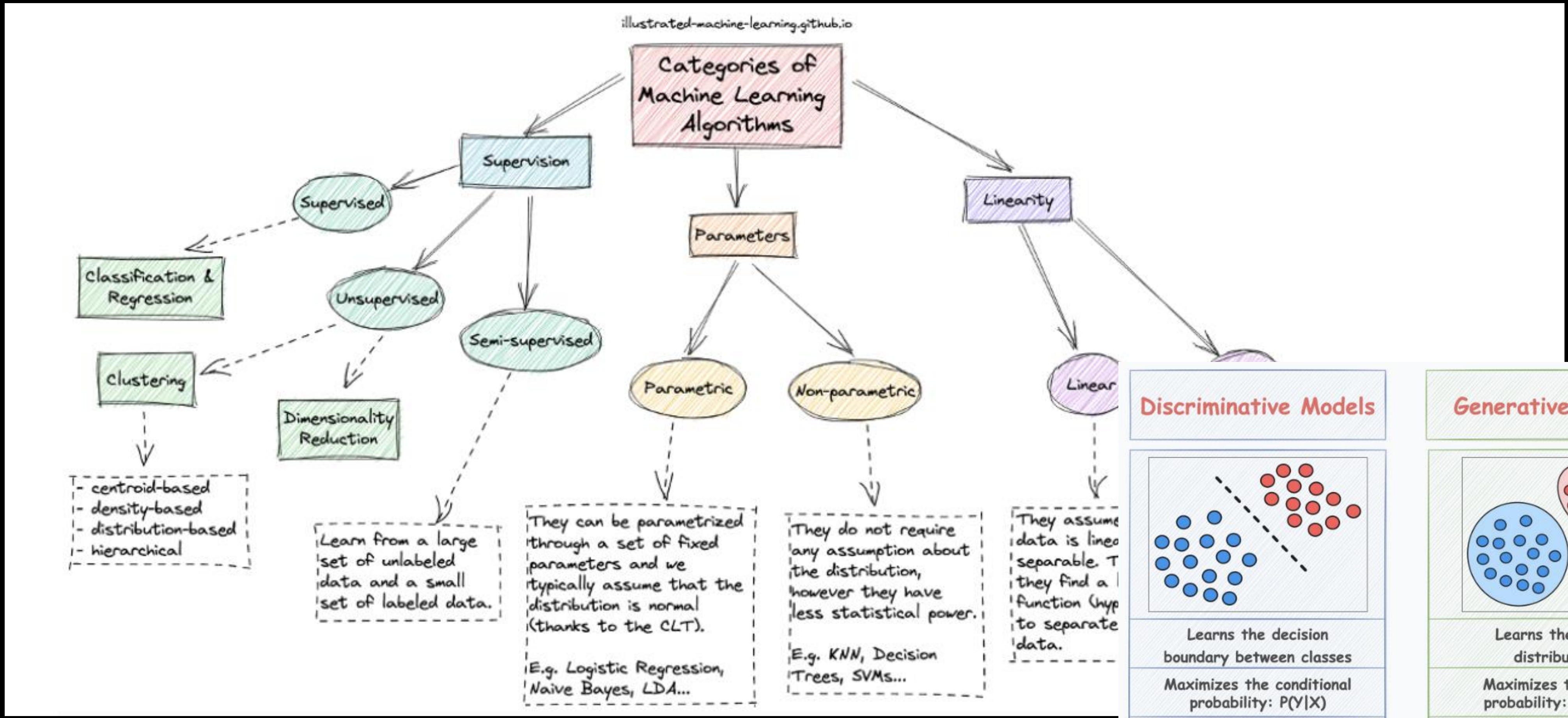
- Pilot vs Flight Engineer
- Lessons from Exercise 1: Deeply examine your data, be one with it!
- Lessons from Exercise 2: LLMs are great for explainability, For high impact diagnostics LLMs are not ready for prime time yet
- Lessons from Exercise 3: Build from basics, use the correct tool. If existing models yield high performance and you have automation systems for them, keep it simple
- Lessons from Exercise 4: Keep in mind that we're moving towards different autonomy levels

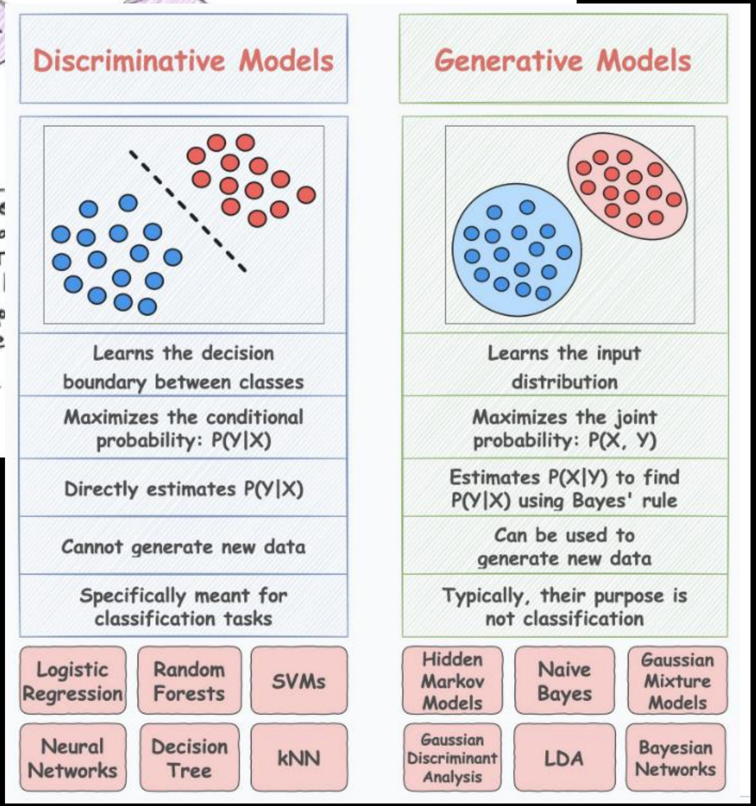
Resources For You

Security Jupyter Notebooks - https://infosecjupyterthon.com/introduction.html

More security datasets:https://github.com/OTRF/Security-Datasets/tree/master/datasets

Offensive AI resources: https://github.com/jiep/offensive-ai-compilation


illustrated-machine-learning.github.io
Categories of Machine Learning Algorithms
Supervision
Supervised
Classification & Regression
Unsupervised
Clustering
- centroid-based
- density-based
- distribution-based
- hierarchical
Dimensionality Reduction
Semi-supervised
Learn from a large set of unlabeled data and a small set of labeled data.
Parameters
Parametric
They can be parametrized through a set of fixed parameters and we typically assume that the distribution is normal (thanks to the CLT).
E.g. Logistic Regression, Naive Bayes, LDA...
Non-parametric
They do not require any assumption about the distribution, however they have less statistical power.
E.g. KNN, Decision Trees, SVMs...
Linearity
Linear


Discriminative Models
Learns the decision boundary between classes
Maximizes the conditional probability: P(Y|X)
Directly estimates P(Y|X)
Cannot generate new data
Specifically meant for classification tasks
Logistic Regression
Random Forests
SVMs
Neural Networks
Decision Tree
kNN
Generative Models
Learns the input distribution
Maximizes the joint probability: P(X, Y)
Estimates P(X|Y) to find P(Y|X) using Bayes' rule
Can be used to generate new data
Typically, their purpose is not classification
Hidden Markov Models
Naive Bayes
Gaussian Mixture Models
Gaussian Discriminant Analysis
LDA
Bayesian Networks

Motivation

"Our comforting conviction that the world makes sense rests on a secure foundation: our almost unlimited ability to ignore our ignorance."
- Daniel Kahneman, *Thinking, Fast and Slow*

There is a difference between…

Asking Questions + Having Data → Asking the *Right* Questions + Having the *Right* Data

The most robust institutions don't just collect data– they produce ***actionable intelligence*** that *serves* a holistic, proactive, and adaptable security strategy

Getting this right has never been more important!

Artificial intelligence / Machine learning

Hundreds of AI tools have been built to catch covid. None of them helped.

Some have been used in hospitals, despite not being properly tested. But the pandemic could help make medical AI better.

by **Will Douglas Heaven** July 30, 2021

Not fit for clinical use

This echoes the results of two major studies that assessed hundreds of predictive tools developed last year. Wynants is lead author of one of them, a review in the British Medical Journal that is still being updated as new tools are released and existing ones tested. She and her colleagues have looked at 232 algorithms for diagnosing patients or predicting how sick those with the disease might get. They found that none of them were fit for clinical use. Just two have been singled out as being promising enough for future testing.

What went wrong

Many of the problems that were uncovered are linked to the poor quality of the data that

Self-driving Uber car that hit and killed woman did not recognize that pedestrians jaywalk

The automated car lacked "the capability to classify an object as a pedestrian unless that object was near a crosswalk," an NTSB report said.

Security

Microsoft AI researchers accidentally exposed terabytes of internal sensitive data

Carly Page @carlypage_ / 9:05 AM EDT • September 18, 2023

James Webb Telescope question costs Google $100 billion — here's why

By Elizabeth Howell published 15 days ago

A promo ad for Google's unreleased artificial intelligence (AI) chatbot made an embarrassing mistake.

WILL KNIGHT BUSINESS FEB 23, 2023 12:00 PM

Should Algorithms Control Nuclear Launch Codes? The US Says No

A new State Department proposal asks other nations to agree to limits on the power of military AI.

Outline

Segment 1: Central Tenets of Data Science

The roles of trust, transparency, traceability, etc. within a robust data pipeline

Segment 2: The Different Flavors of Data Science

The road from descriptive to prescriptive data science and data strategy maturity

As we walk through this presentation, reflect on where you and your teams fall in terms of operational maturity, and how concepts we discuss apply to your particular use cases and applications.

Central Tenets of (Good) Data Science

Building ***confidence*** in your data and your analysis is the objective!

Requirements	**Documented functional or physical needs that a product/solution must satisfy**
Traceability	**The ability to track changes and updates to data, pipelines, and solutions**
Transparency	**Data is used with integrity, lawfully, fairly, and for valid purposes**
Documentation	**Fields, tables, schemas, and processes used to generate them are documented**
Verification and Validation	**<u>Independent</u> procedures used to check that products, services, and systems meet requirements and specifications**

**This is not an exhaustive list!*

Central Tenets of (Good) Data Science

In order to solve the *sexy* problems, we have to solve the *unsexy* problems first

Requirements	Do you know how to set good requirements?
Traceability	When was the last time you tried to track a change in your codebase or data architecture?
Transparency	Can you get answers to difficult questions within your organization?
Documentation	Do you know where documentation lives? What all your fields mean?
Verification and Validation	What is your V&V procedure? Have you revisited it lately?

**This is not an exhaustive list!*

The Different Flavors of Data Science

"When a measure becomes a target, it ceases to be a good measure."
- Charles Goodhart

It is important to remember that different kinds of data science exist, and serve different purposes. However, your ability to **confidently** execute proactive and prescriptive analytic initiatives is an indicator of **maturity**

At the end of the day, ***the analysis you do and the results you use should inform decisions and the objectives of your organization, and <u>they need not be sophisticated</u>***

- The right metrics should inform the right decisions
- Why develop an LLM when a linear regression will do the trick?

Maturity

Type 1: Descriptive Data Science

Answers the question, “What happened?”

- Basic statistics and visualizations
- Often critical for **orienting** to a problem, decision, or event
- Typically conveyed in reports, slide decks, or dashboards
- May include some trend analysis

Examples:

Software Investment

The following software packages are present in our environment...

Incident Response

A compromise has occurred affecting the following environments...

Descriptiv

Descriptive Data Science: Adding Rigor

Maturity

Statistical and scientific rigor can elevate your analysis

- Define clear objectives and research questions
- Formulate hypotheses and begin designing experiments to test these hypotheses
- Engage in exploratory data analyses often
- Verify assumptions, parameters, and methods used to analyze the data
- Conduct peer reviews of your analyses and methodologies

Rigor

Descriptiv

Type 2: Diagnostic Data Science

Maturity

Answers the question, "Why did it happen?"

- Beginning stages of inference and narrative
- Correlations, variable analysis, and even regression analysis
- **Descriptive analytics coupled with statistical rigor**

Examples:

Software Investment

We use the software packages for these essential functions and job roles:...

Post-Incident Response

These software characteristics tend to correlate with patterns of compromise:...

Diagnostic

Rigor

Descriptiv

Predictive Data Science: Thinking Ahead

Maturity

Data analyses coupled with elements of structured analytical techniques tend to be forward-looking

- Timeline analysis and retrospectives/prospectives– can you use the past to predict the future?
- Structured project planning and risk assessments
- Project/analysis pre-mortems
- Indication and warning (I&W) analysis
- Continuous feedback and improvement

Foresight

Diagnostic

Rigor

Descriptiv

Type 3: Predictive Data Science

Answers the question, “What is likely to happen?”

- Forecasts, models, and theorizations
- Advanced analytics, such as machine learning algorithms
- Learning from the past
- **Diagnostic analytics looking forward**

Examples:

Software Investment

These will be the effects of a software compromise:...

Post-Incident Response

We predict the following future attack attempts:...

Maturity

Predictive

Foresight

Diagnostic

Rigor

Descriptiv

Predictive Data Analysis: Course of Action Development

How are you planning for the future?

- What are your roadmaps?
- How will you measure success? Assessments should be planned ahead of time
- Have you identified critical decision points, and data requirements for making those decisions?
- Scenario analysis, tabletop exercises

Maturity

Action

Predictive

Foresight

Diagnostic

Rigor

Descriptiv

Type 4: Prescriptive Data Science

Answers the question, “What should we do next?”

- Data-driven organizational strategy and outcome optimization
- Course of action development
- May require in-house algorithms unique to your use cases
- **Predictive analytics coupled to organisational goals**

Examples:

Software Investment

Our software procurement strategy should change, and here’s how.

Post-Incident Response

We can tolerate <these> risks, and should adapt accordingly.

Maturity

Prescriptive

Action

Predictive

Foresight

Diagnostic

Rigor

Descriptiv

Brief Recap

Your organisation's ability to get the most out of its data relies on a **strong foundation of data science best practices** and the ability to **mature a data-driven cybersecurity strategy**