



Mastering AI Security Boot Camp

TTAI2820: Hands-on AI Security: Essentials, Threat Detection,
Vulnerabilities, Forensics, Incident Response & Future Trends

Trivera Technologies www.triveratech.com

20240429

Jumping right In...

- **Welcome!**
 - Mastering AI Security Boot Camp (**TTAI2820**)
 - Geared for technical professionals eager to deepen their knowledge in machine learning and AI security. Roles include Data Scientists, Machine Learning Engineers, IT Security Professionals, and DataOps Engineers or similar.
 - Topics, labs and agenda may adjust during delivery based on your interests, roles and goals.
- **Hours:**
 - 10:00 to 6:00 PM Eastern; One Hour for Lunch; A few breaks as needed
- **A Bit About Me:** Dr. Ernesto Lee, Dr.Lee@triveratech.com
 - Chief Innovation Officer, Trivera Technologies www.triveratech.com
- **A Bit About You:**
 - What's your role / day to day?
 - Are you working with these skills already?
 - What kinds of related things are you working on?
 - What are you most excited to learn about in this class?

Teaming for Success

- Course Portal: Trivera's SkillJourneys LXP www.skilljourneys.com
 - Quick Look at the Learning Experience Platform / Course Portal
 - Where to find the Courseware: Course Guide, Deck & Resources
 - Feedback Surveys
 - Access is live for 60 days
- Sharing Feedback – We're Here to Provide Value!
 - Feedback is welcome & always encouraged
 - Real time is best
 - Other ways to connect
 - Course Check In & End of Course feedbacks – complete right in the LXP
- Course Recordings
 - Provided by separate link a few days after class; Live for 60 days
- Course Certificates
 - Will be sent out a few days after class after End of course survey is completed.

Agenda Review

1. Introduction to AI in Security:
 - Explore foundational AI security, threat identification, and protective strategies through practical examples.
2. Playing Detective:
 - Explores AI system vulnerabilities, different threat types, and data privacy concerns.
3. Building the AI Fortress: Defense Mechanisms 101
 - Teaches design and implementation of robust AI-driven defense systems..
4. CSI Cyber: Exploring AI Forensics
 - Focuses on applying forensic techniques and analyzing AI security incidents.

Agenda

5. AI Adversarial Attacks and Defenses:

- Covers strategies to tackle adversarial threats to AI systems.

6. Crisis Averted: Crafting Your AI Incident Response Plan:

- Develop and execute effective incident response plans for AI system breaches.

7. AI Privacy and Ethical Considerations:

- Addresses privacy risks and ethical considerations in AI applications.

8. What's Next? Preparing for Future AI Security Challenges:

- Explore future AI security trends and prepare for emerging threats like deepfakes.

Additional Resources

These Resources are in the back of your Course Guide

- Course Site References & Additional Information
- Glossary of Main Terms, Skills and Key Topics
- Next Steps, Follow on Courses & SkillJourneys

Getting Hands-On

- Demos & Activities
 - We'll focus activities on things that will be useful to you and provide value.
 - *ADD A few sentences about what the demos will show*



Any Questions?

Let's Dive In!

Experience is

Chapter 1:

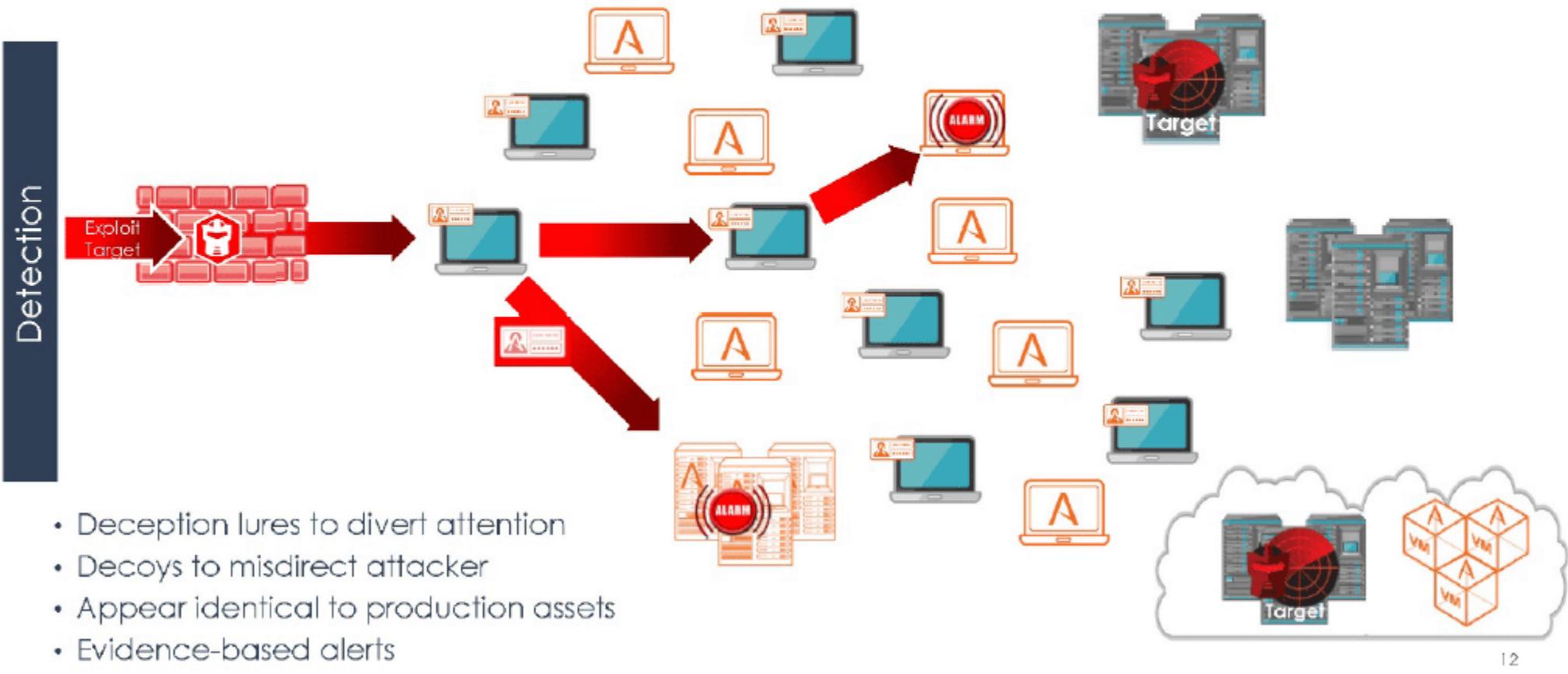
Introduction to AI & Security

Explore foundational AI security, threat identification, and protective strategies

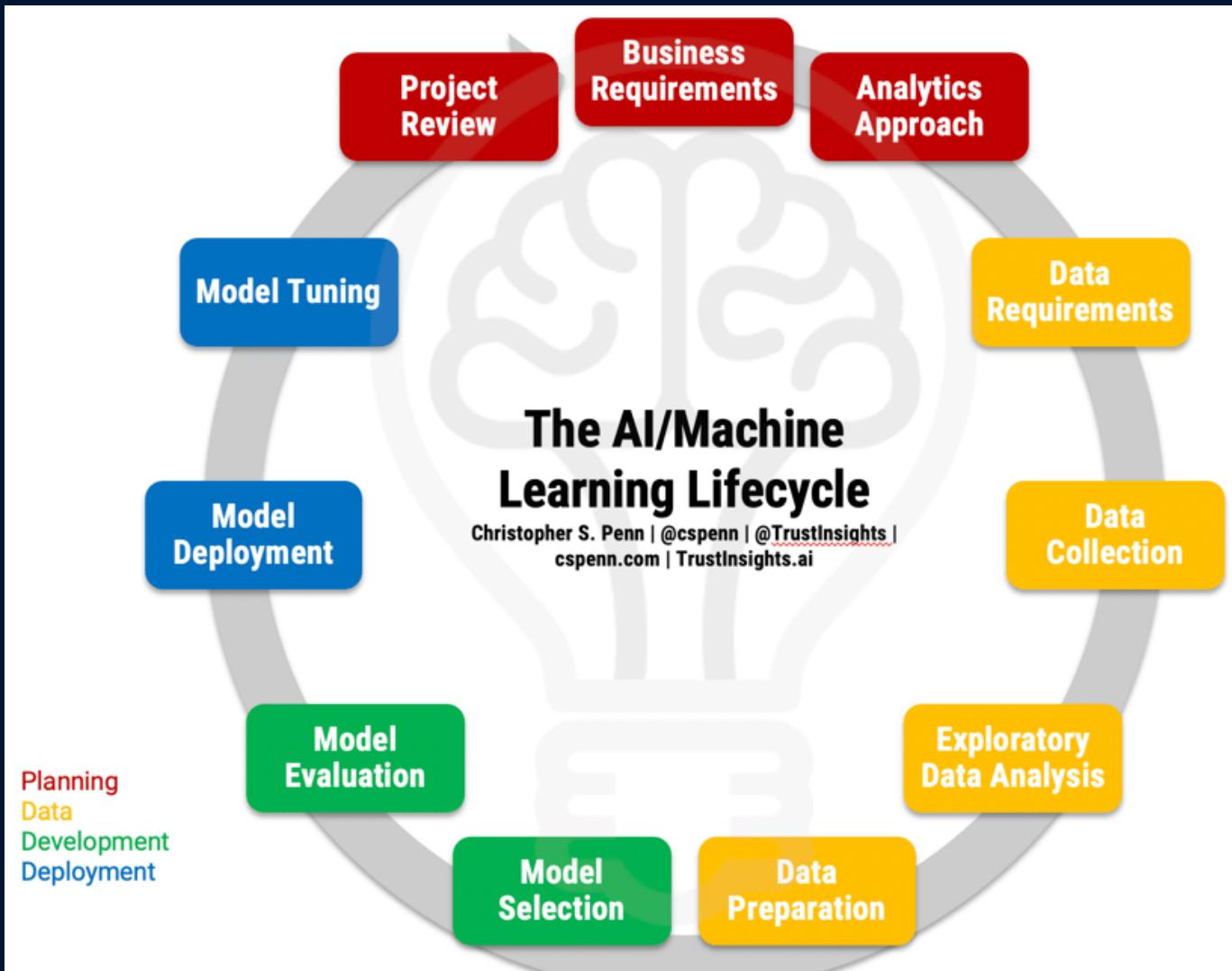
Defining Machine Learning Security

Changing the Game with Deception and Decoys

Deception Obscures the Attack Surface and Disrupts Attacks



A Picture of ML



This Photo by Unknown Author is licensed under [CC BY-NC-ND](#)

ML Only Works When...

- The source data is untainted
- The training and testing data are unbiased
- The correct algorithms are selected
- The model is created correctly
- Any goals are clearly defined and verified against the training and test data

Identifying the ML Security Domain

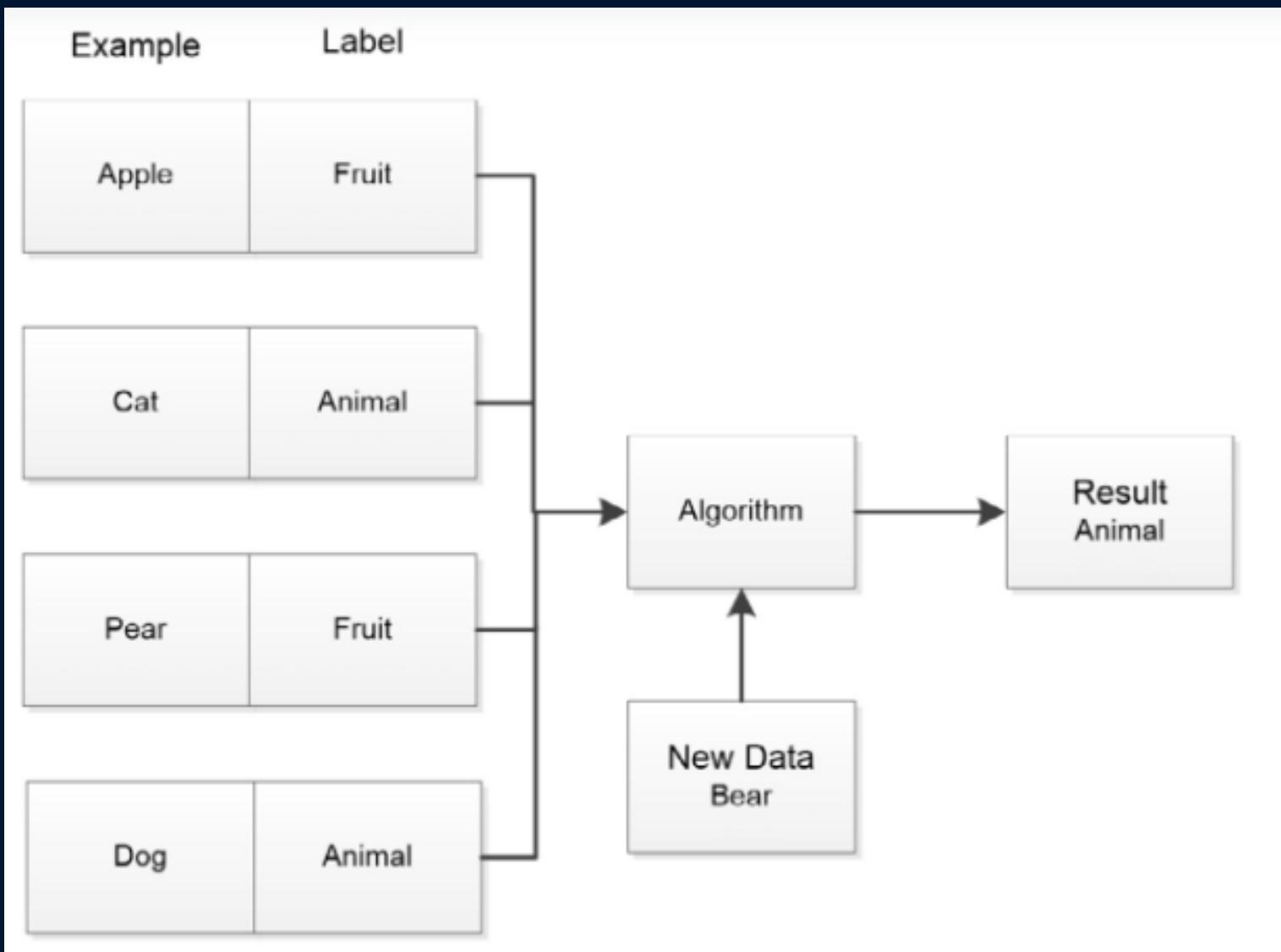
- Data Bias
- Data Corruption
- Missing critical data
- Errors in Data
- Algo correctness
- Algorithmic Bias
- Repeatable Results

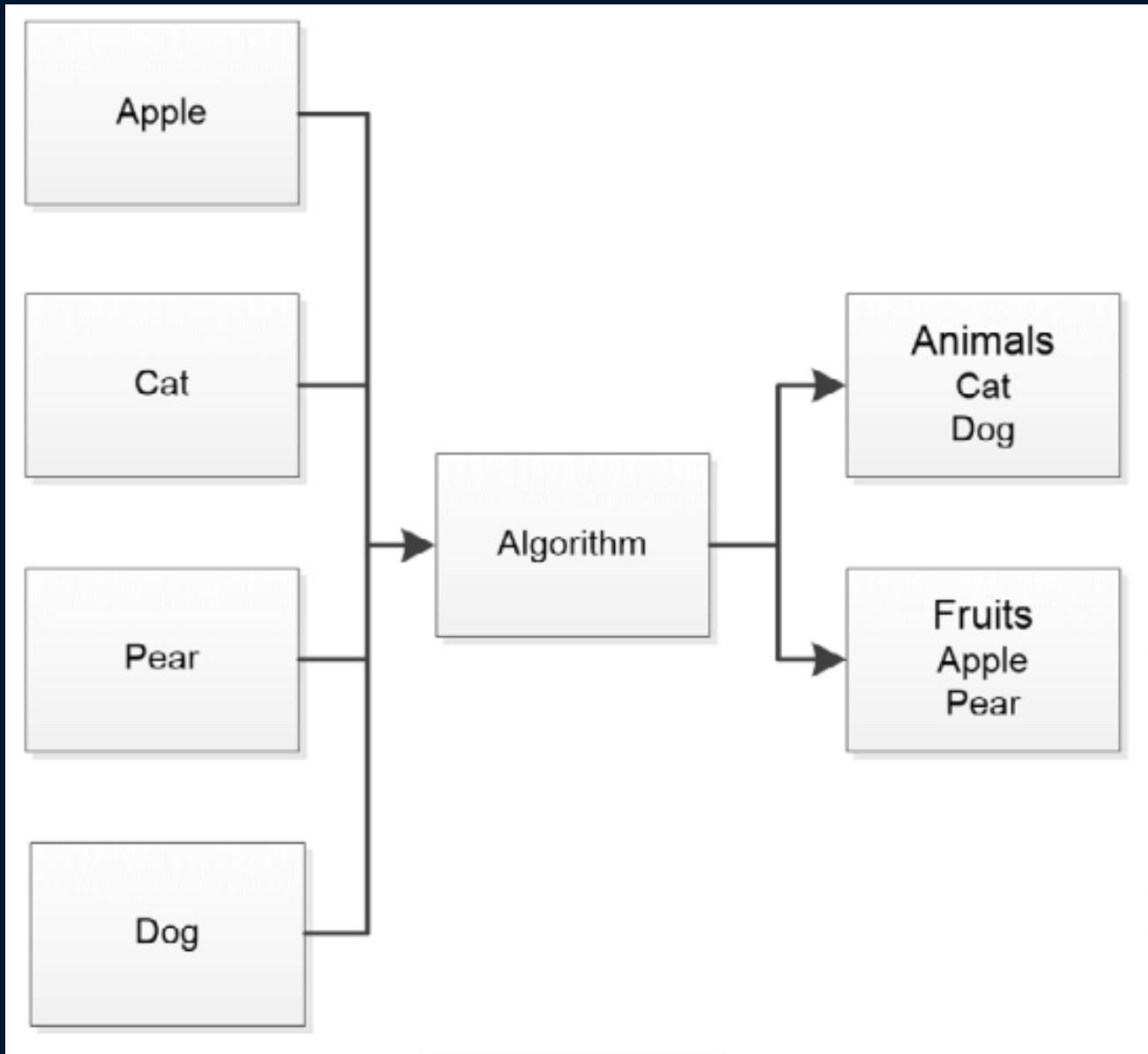
Vulnerabilities

- Evasion
- Poisoning
- Inference
- Trojans
- Backdoors
- Espionage
- Sabotage
- Fraud

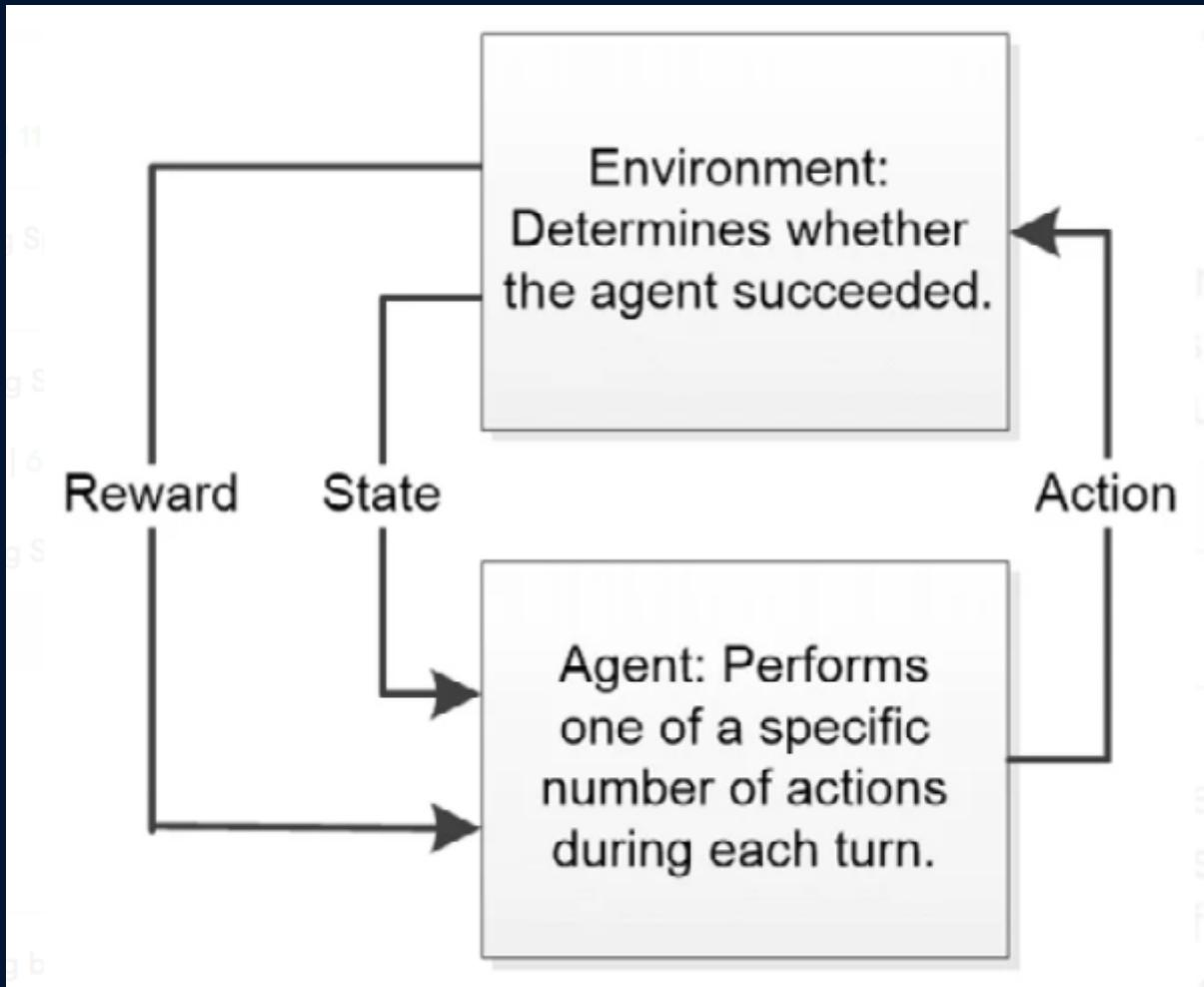
Types of ML

- Supervised
- Unsupervised
- Reinforcement





Reinforcement Learning



Add Security to ML

- Commission
- Omission
- Bias
- Perspective
- Frame of Reference



Compromising the integrity and availability of ML



Types of Attacks against ML

- <https://portswigger.net/daily-swig/vulnerabilities>
- Adversarial Attacks
- ML relies on Statistics!



This Photo by Unknown Author is licensed under CC BY-SA

The screenshot shows a web browser displaying the URL portswigger.net/daily-swig/vulnerabilities. The page features a hex dump of binary code at the top, followed by the title "The Daily Swig" and the subtitle "Cybersecurity news and views". Below this, there's a section titled "Latest cybersecurity vulnerability news" with a brief introduction and links to articles. A sidebar on the left is titled "Bug Bounty Radar" and lists "The latest bug bounty programs for March 2023". To the right, there are two small thumbnail images: one for an "Indian gov flaws" exploit and another for a "Chromium bug" related to SameSite cookies.

What Can be Achieved with ML Security

- Set understandable and achievable result goals that are verifiable, consistent, and answer specific needs
- Train personnel (which means everyone in the organization, along with consultants and third parties) to interact with the application and its data appropriately
- Ensure that data passes all of the requirements for proper format, lack of missing elements, absence of bias, and lack of various forms of corruption
- Choose algorithms that actually perform tasks in a manner that will match the goals set for the ML application
- Use training techniques that create a reliable model that won't overfit or underfit the data
- Perform testing that validates the data, algorithms, and models used for the ML application
- Verify the resulting application using real-world data that the ML application hasn't seen in the past

Setup for the class

- Google Colab
- To a lesser extent Microsoft Azure

What do you need to know?

- DEMO



Summary





Lab: Validate Colab

Hands-on Lab: Please refer to your Lab Guide
and follow the instructions provided by your Instructor

Experience is



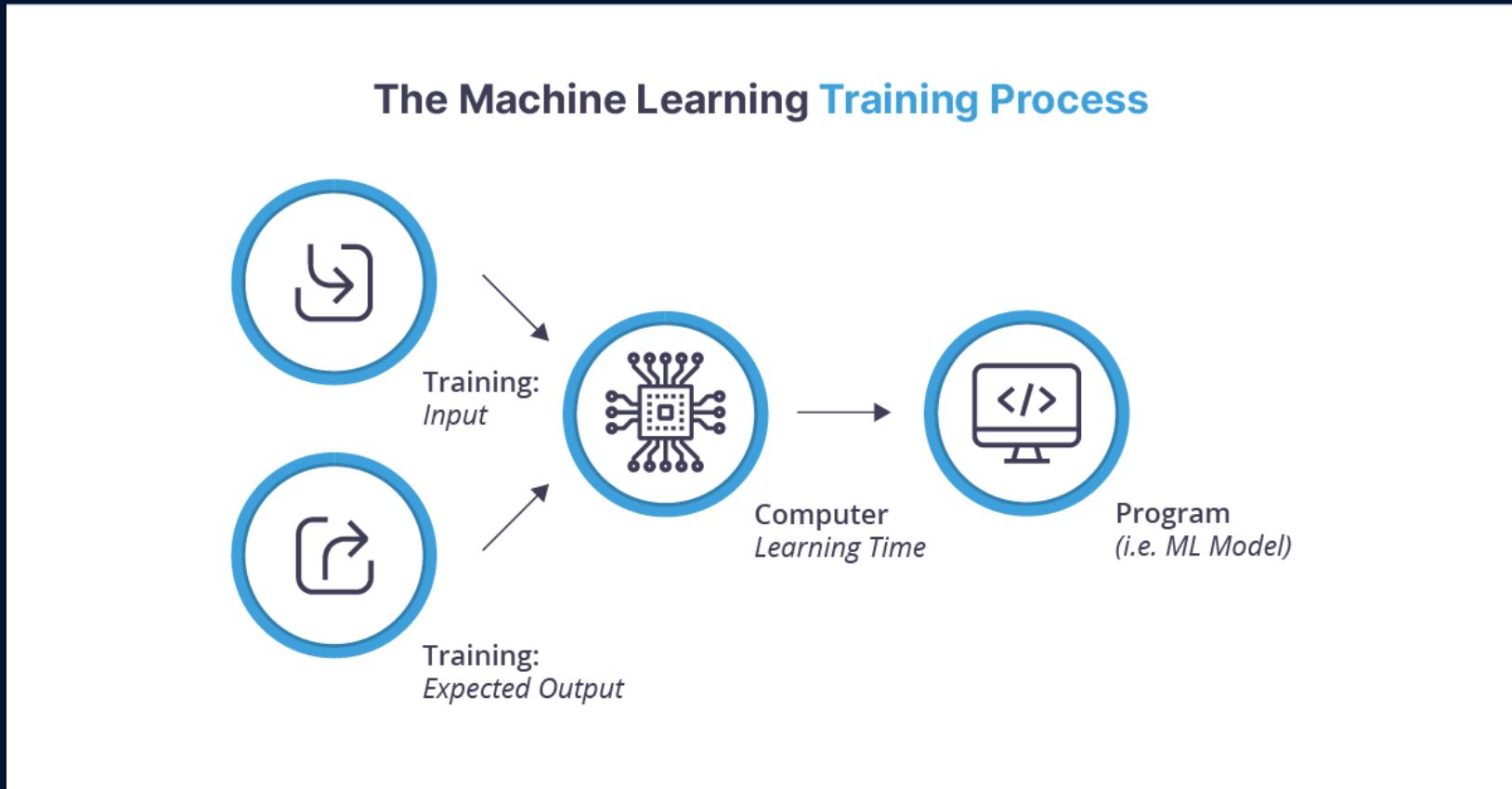
Chapter 2:

Playing Detective

Identify Threats and Vulnerabilities

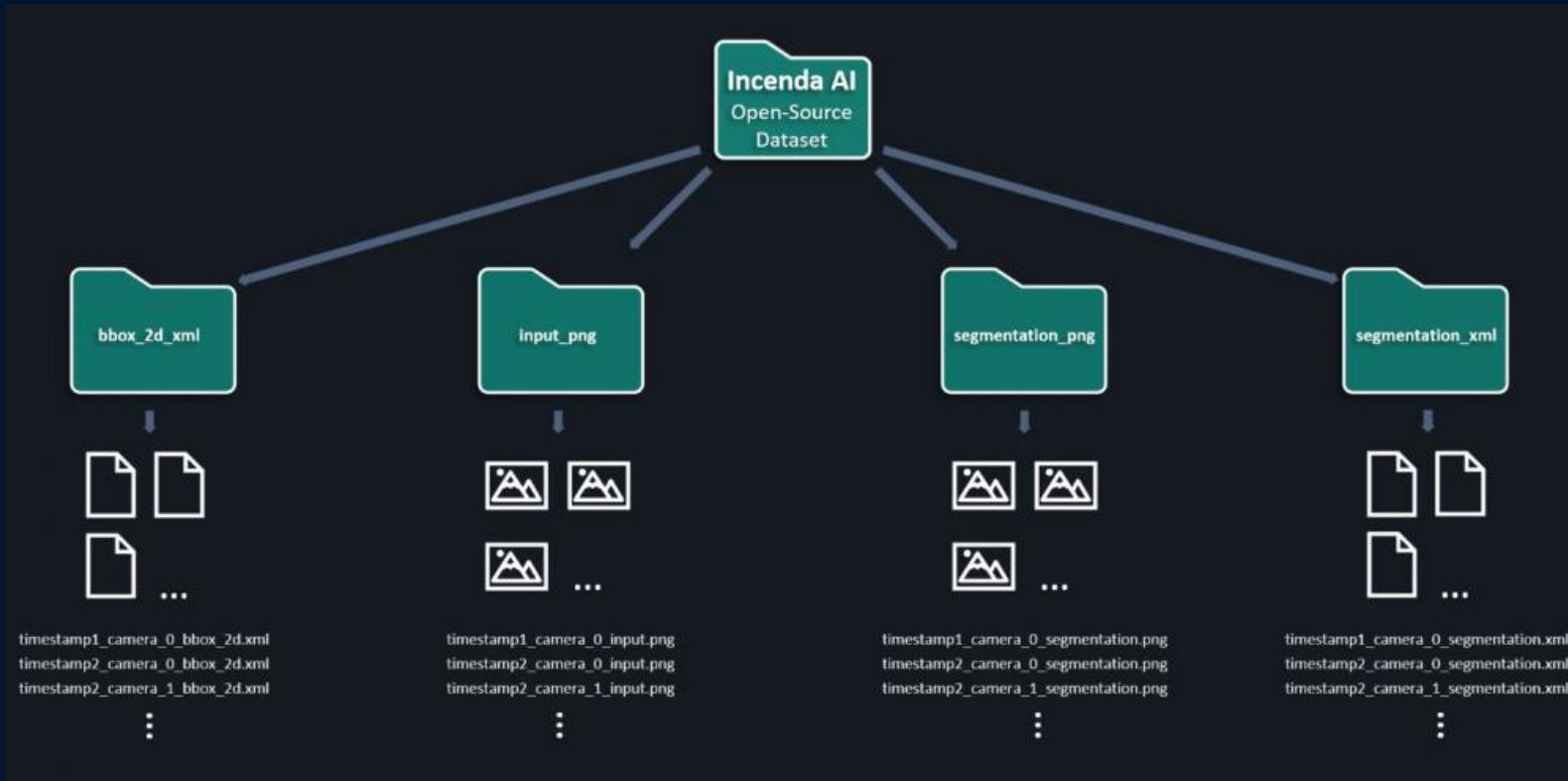
Threats at Training – Dataset vulnerabilities

- Defining dataset threats
- Detecting dataset modification
- Mitigating dataset corruption



Dataset Threats

- Dataset Modification
- Dataset Corruption



[This Photo](#) by Unknown Author is licensed under [CC BY](#)

Dataset Threat Sources

Task	Learning Type	ML Consideration	Task	Learning Type	ML Consideration	Task	Learning Type	ML Consideration
Automatic language translation	Supervised	Translates one language into another language using a sequence-to-sequence learning algorithm. The results are often less useful than expected due to variations between languages and the fact that languages generally contain words that don't have equivalents in other languages.	Medical diagnosis	Supervised and unsupervised	Predicts the progression and characteristics of diseases and other conditions, along with locating and identifying potential patient illnesses.	Self-driving cars	Supervised, unsupervised, and reinforcement	Allows a vehicle to drive itself by means of various cameras and detectors for the detection of obstacles, interpreting the content of signs, and so on.
		Susceptible to data errors, missing data, data corruption, algorithm bias, and an inability to repeat and verify results due to naturally occurring evolution in languages. This kind of application is also sensitive to speech patterns and misidentifying terms when words aren't enunciated clearly.			Susceptible to data bias, data corruption, data errors, incorrect algorithm selection, and algorithm bias. This particular application type can never operate alone; it always assists a physician with the required experience to make a diagnosis.			Susceptible to so many different kinds of attacks that it's truly amazing that self-driving cars work at all. In addition to ML, self-driving cars rely on other AI technologies such as sensor fusion systems (https://www.aitrends.com/ai-insider/expert-systems-for-self-driving-cars-cross-innovative-techniques/). It's possible that self-driving cars will eventually become completely successful, but don't hold your breath for this advance anytime soon.
Email spam and malware filtering	Supervised	Marks, moves, or deletes email that meets the criteria of spam or malware from an inbox as it's received from a server. There are usually several levels of filtering including Content, Header, Blacklist, Rule-based, and Permission.	Online fraud detection	Supervised	Reduces the risk of conducting transactions online by detecting conditions such as fake accounts, fake IDs, compromised sites, compromised security certificates, and so on.	Speech recognition	Supervised	Translation of spoken or written speech into text that the computer can recognize and process.
		Susceptible to a number of potential attacks including backdoors, Trojans, espionage, sabotage, fraud, evasion, inference, data errors, and data corruption. This is one of the more reliable forms of ML applications, but users still regularly find spam in their inboxes and useful messages in their spam folders.			Susceptible to a wide range of attacks, some of which have nothing to do with the application. For example, a compromised certificate authority could cause the application to fail by allowing the hacker access to the underlying infrastructure, even if the application itself isn't at fault. This kind of application is also known to display false positives and false negatives depending on the reliability of the code used to create it and the model training.			Susceptible to data errors and use of untrustworthy terms. This kind of application is also susceptible to speech patterns and misidentifying terms when words aren't enunciated clearly.
Image recognition	Supervised	Identification of objects, persons, places, patterns, and other elements within an image.	Product recommendation	Unsupervised	Outputs product recommendations based on previous buying habits, associated goods, and direct queries. It's one of the most widely used and common ML applications.	Stock market trading	Supervised	Predicts trends in the stock market based on past and current data. This is one of the most important applications that relies heavily on short-term memory and weighting processes to make predictions based on data count for more than past data.
		Susceptible to a variety of attack types, but also prone to misidentification when the image contains elements the application didn't expect or when those objects appear in positions that the application isn't trained to recognize.			Susceptible to data errors, data bias, missing data, algorithm bias, fraud, sabotage, and a wealth of other issues. This kind of application often provides irrelevant information along with useful product recommendations because the application has no method of judging user needs and wants.			Susceptible to data bias, data corruption, data errors, incorrect algorithm selection, and algorithm bias. Attackers will attempt to gain access by any means possible without emphasis on evasion, inference, Trojans, and backdoors. Reliability is a prime concern for this application type, but incredibly hard to achieve given the variability of the stock market.

Jump Into Data Exchange

- Automated software makes an unwanted update to a value
- Company policy or procedure changes so that the value that used to be correct is no longer correct
- Aging and archiving software automatically removes values that are deemed too old, even when they aren't
- New sensors report data using a different range, format, or method that creates a data misalignment
- Someone changes the wrong record

Jump into Data Corruption

Discover Feature Manipulation

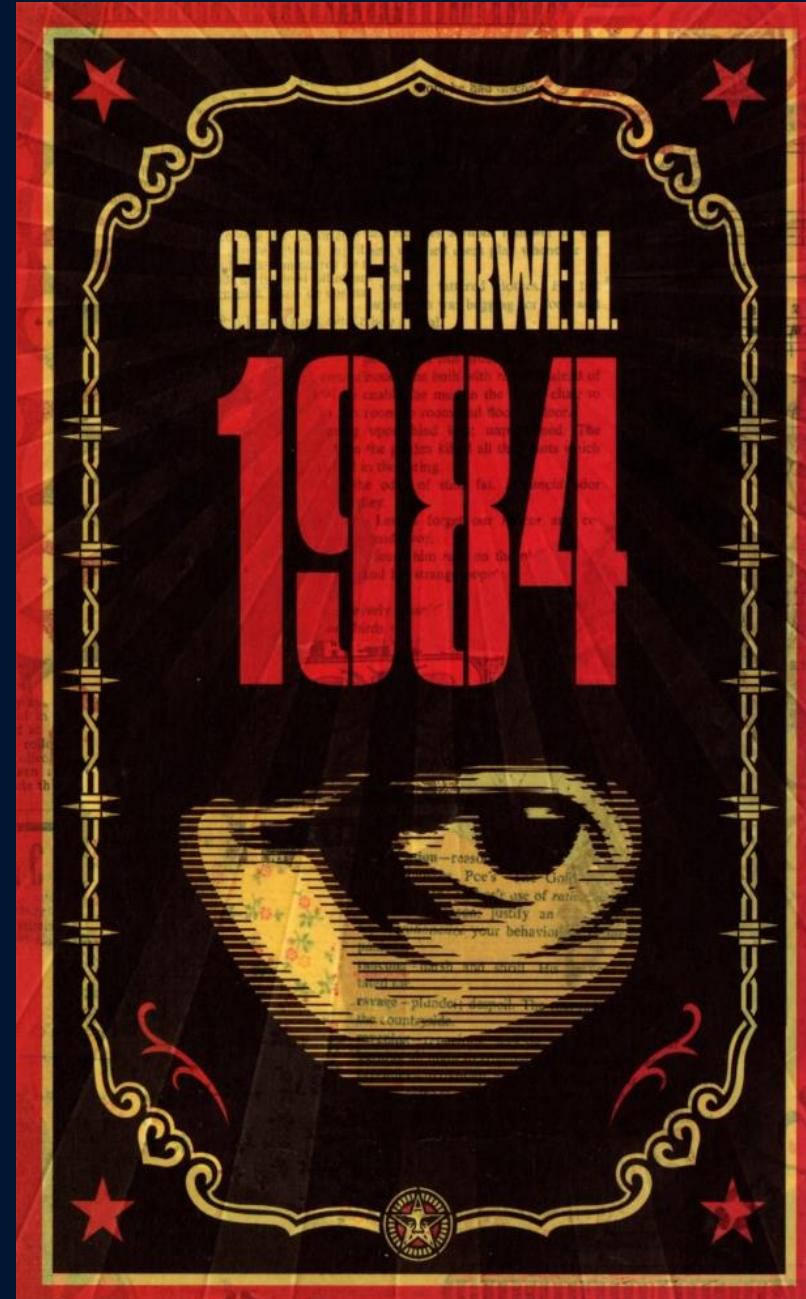
- Keep personal data out of the dataset when possible
- Use aggregate values where it's difficult to reconstruct the original value, but the aggregate still provides useful information
- Perform best practices feature reduction studies to determine whether a feature really is needed for a calculation

Source Modification

- Source modification attacks occur when a hacker successfully modifies a data source you rely on for input to your model.
- It doesn't matter how you use the data, but rather how the attacker modifies the site.

Thwarting Privacy Attacks

- Membership inference attack
- GAN
- Language Generation Models
- Federated ML System
- Aggregate location data
- Data extraction
- Genomic information
- Facial Recognition
- Unintended Memory
- Model Extraction



Detecting Dataset Modification

1. Hackers want to create an environment where products from Organization A, a competitor of Organization B, receive better placement on a sales site because the competitor is paying them to do so
2. The hackers discover that buyer product reviews and their product ratings are directly associated with the site's ranking mechanism
3. The hackers employ zombie systems (computers they have taken over) to upload copious reviews to the site giving Organization B's products a one-star review
4. The site's ML application begins to bring down the product rankings for Organization B and the competitor begins to make a ton of money

Rely on traditional methods... Hashes

- Data scientists, DBAs, and developers understand the underlying methodologies
- The cost of implementing this kind of solution is usually low
- Because people understand the methods so well, this kind of system is usually robust and reliable



Code Along...

Summary



Lab: Hash Your Dataset

Hands-on Lab: Please refer to your Lab Guide
and follow the instructions provided by your Instructor

Experience is

Chapter 2:

Building the AI Fortress

Design and implement robust AI-driven defense
and intrusion systems

Experience is

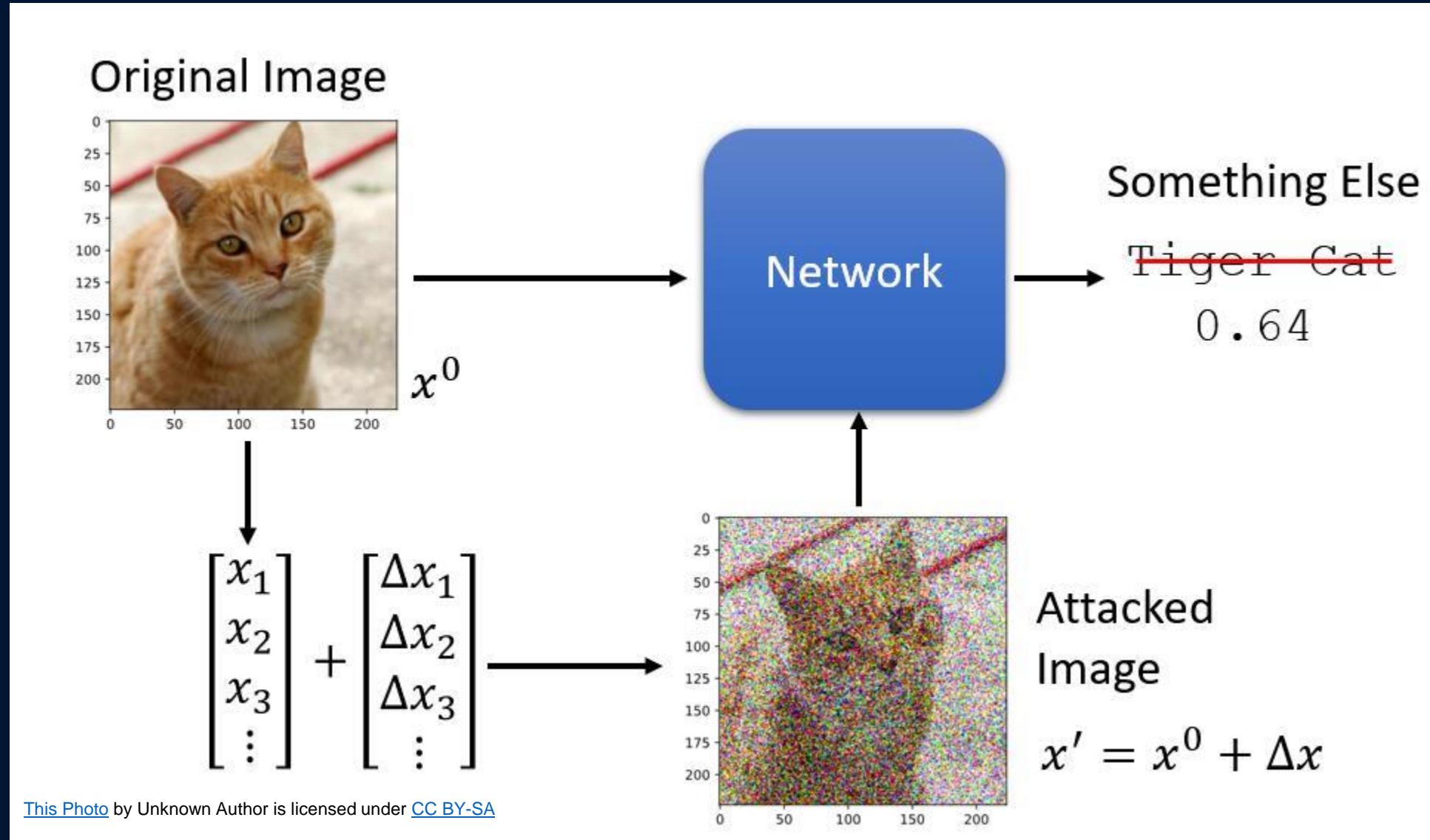
Avoid Adversarial Machine Learning Attacks

- Many adversarial attacks don't occur directly through data
- Attackers often rely on attacking the machine learning (ML) algorithms through the resulting models.
- Such an attack is termed adversarial ML because it relies on someone purposely attacking the software.

Let's do the following now:

1. Define adversarial attack
2. Consider security issues in ML
3. Describe the most common attack techniques
4. Mitigate threats to the algorithm

Define Adversarial ML



Categorize Attack Vectors

The Hackers Mindset

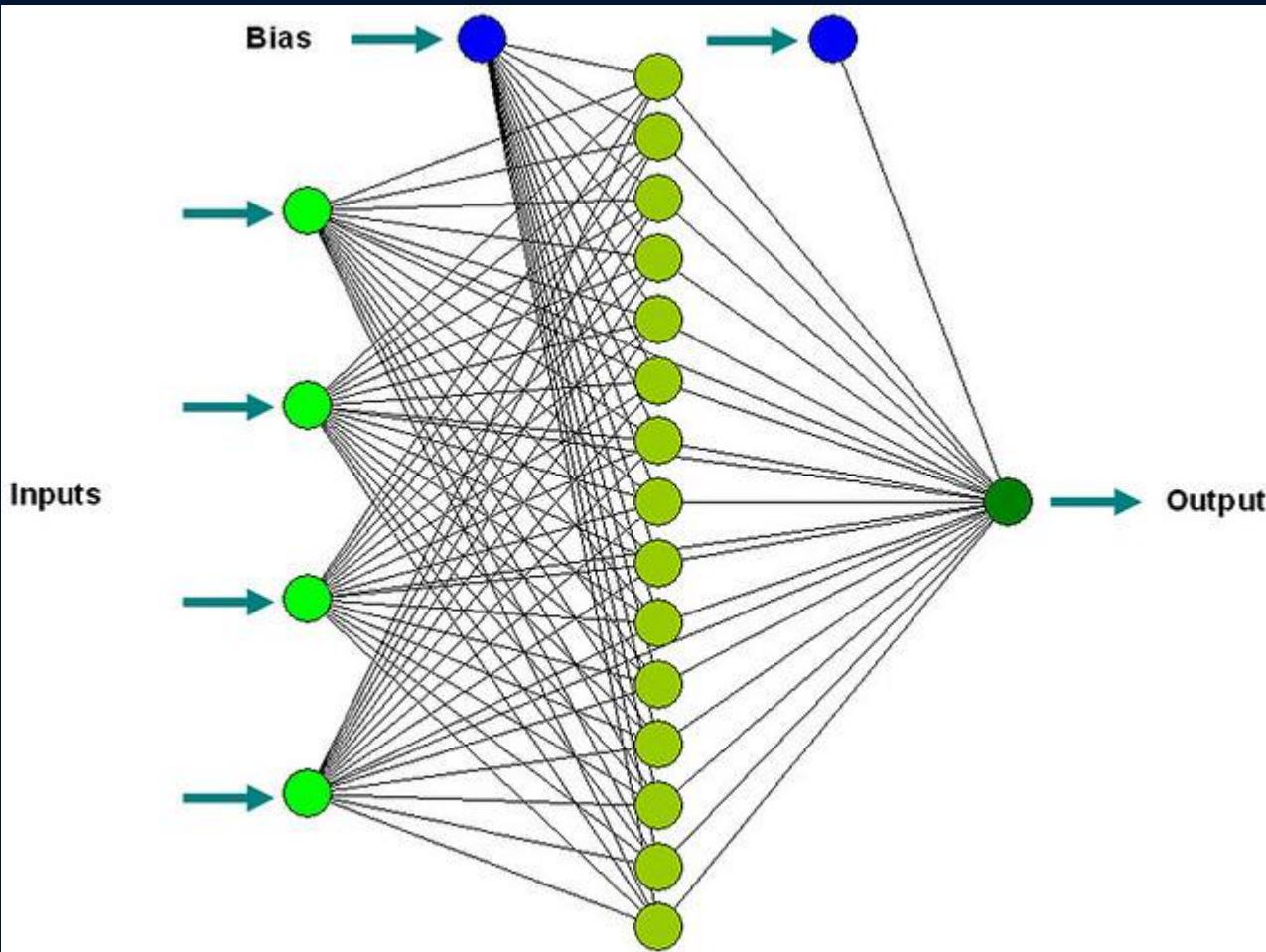
- To obtain money or power
- To take revenge on another party
- Because they need or want attention
- Because there is a misunderstanding as to the purpose of the application
- To make a political statement or create distrust
- Because there is a disagreement over how to accomplish a task

Hacker Goals

- Fly under the security radar
- Stay on the network as long as possible
- Perform specific tasks without being noticed
- Spend as little time as possible breaking into an individual site
- Reuse research performed before the break-in
- Employ previous datasets and statistical analysis to improve future efforts

Trial and Error and Humans as the Weakest Link

- Social Engineering
- Phishing Attacks
- Spoofing



[This Photo](#) by Unknown Author is licensed under CC BY-SA-NC

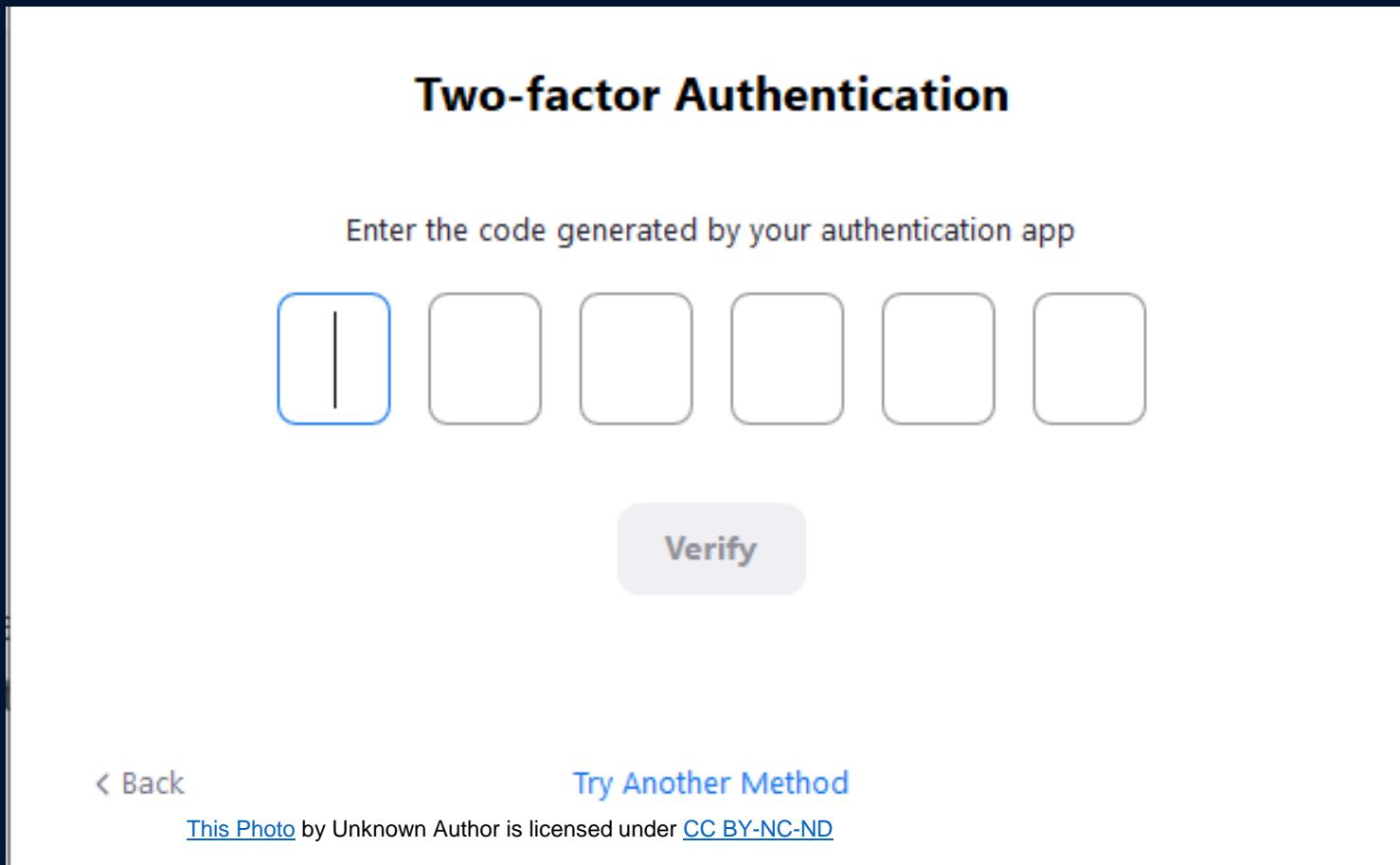
Don't Help the Attackers!

- Keep your secrets by not telling anyone (or keeping the list incredibly small)
- Eliminate clues
- Make the hacker jump through hoops
- Feed the hacker false information
- Learn from the hacker
- Create smarter models

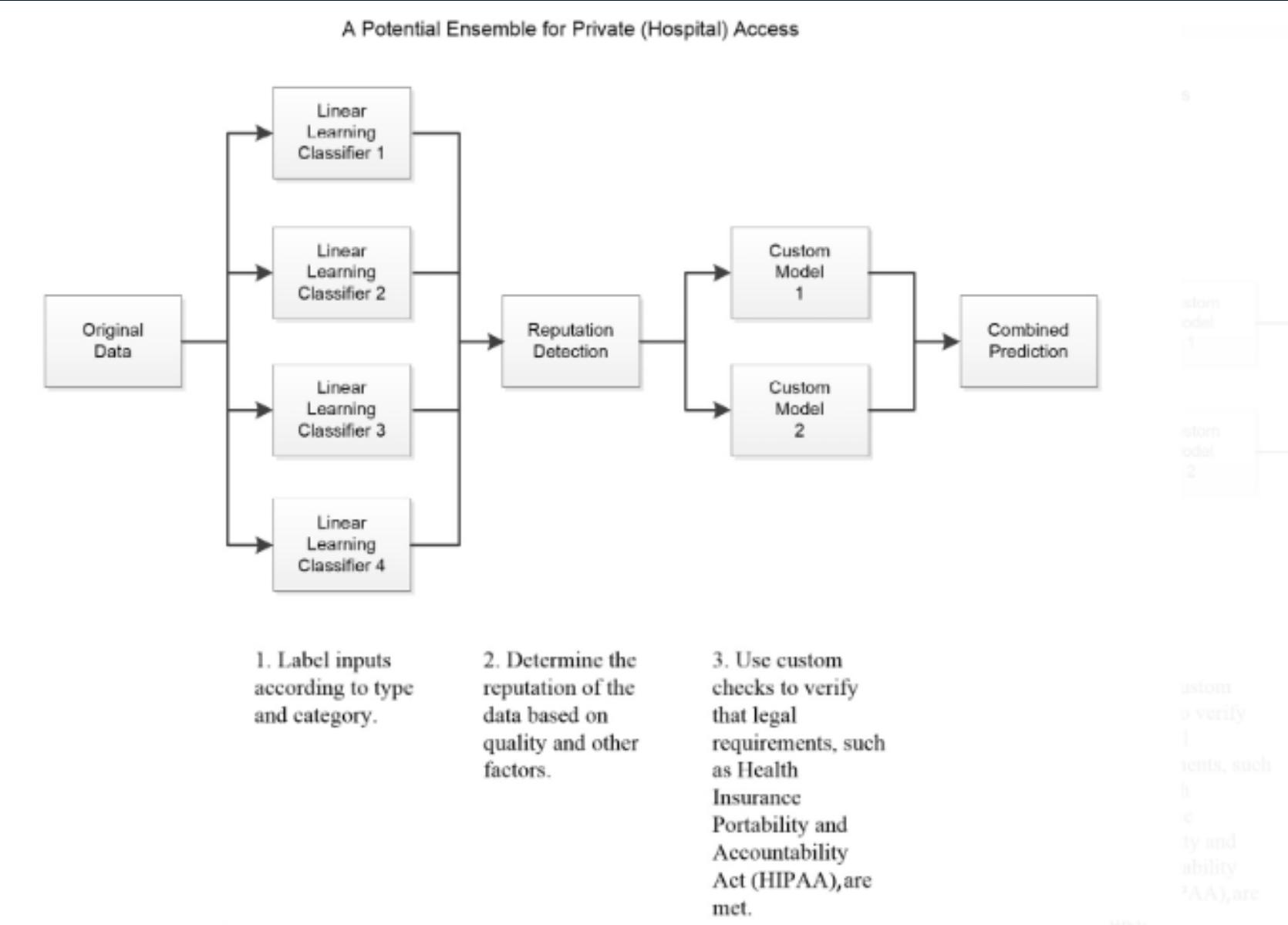
Limit Probing

- Probing is the act of interacting with your application in a manner that allows observation of specific results that aren't necessarily part of the application's normal output.
- A hacker could keep trying scripts, control characters, odd data values, control key combinations, or other kinds of inputs and actions to see if an error occurs.
- CONSIDER CAPTCHAS

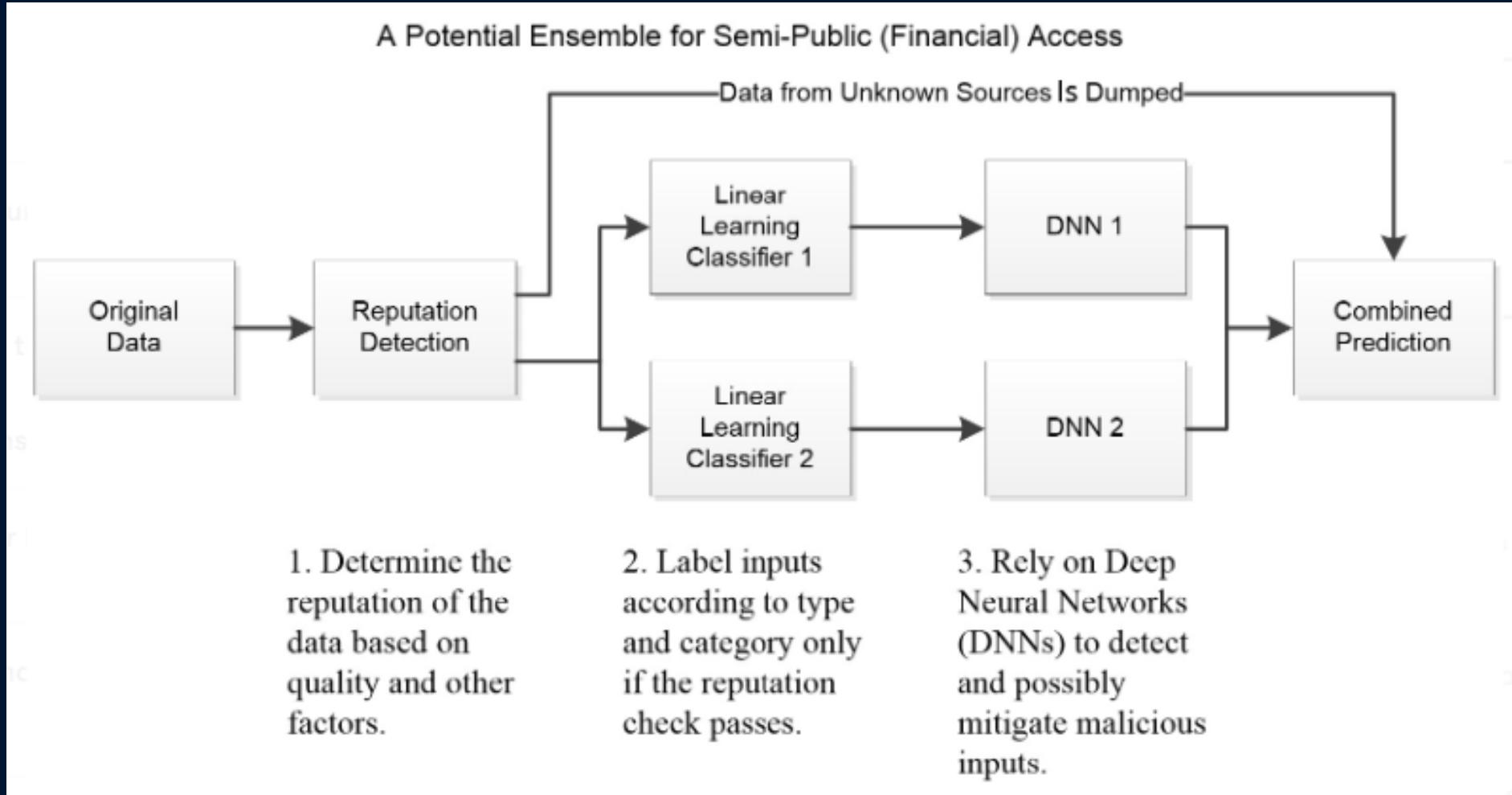
Use 2FA with your ML



Use Ensemble Learning



More Ensemble



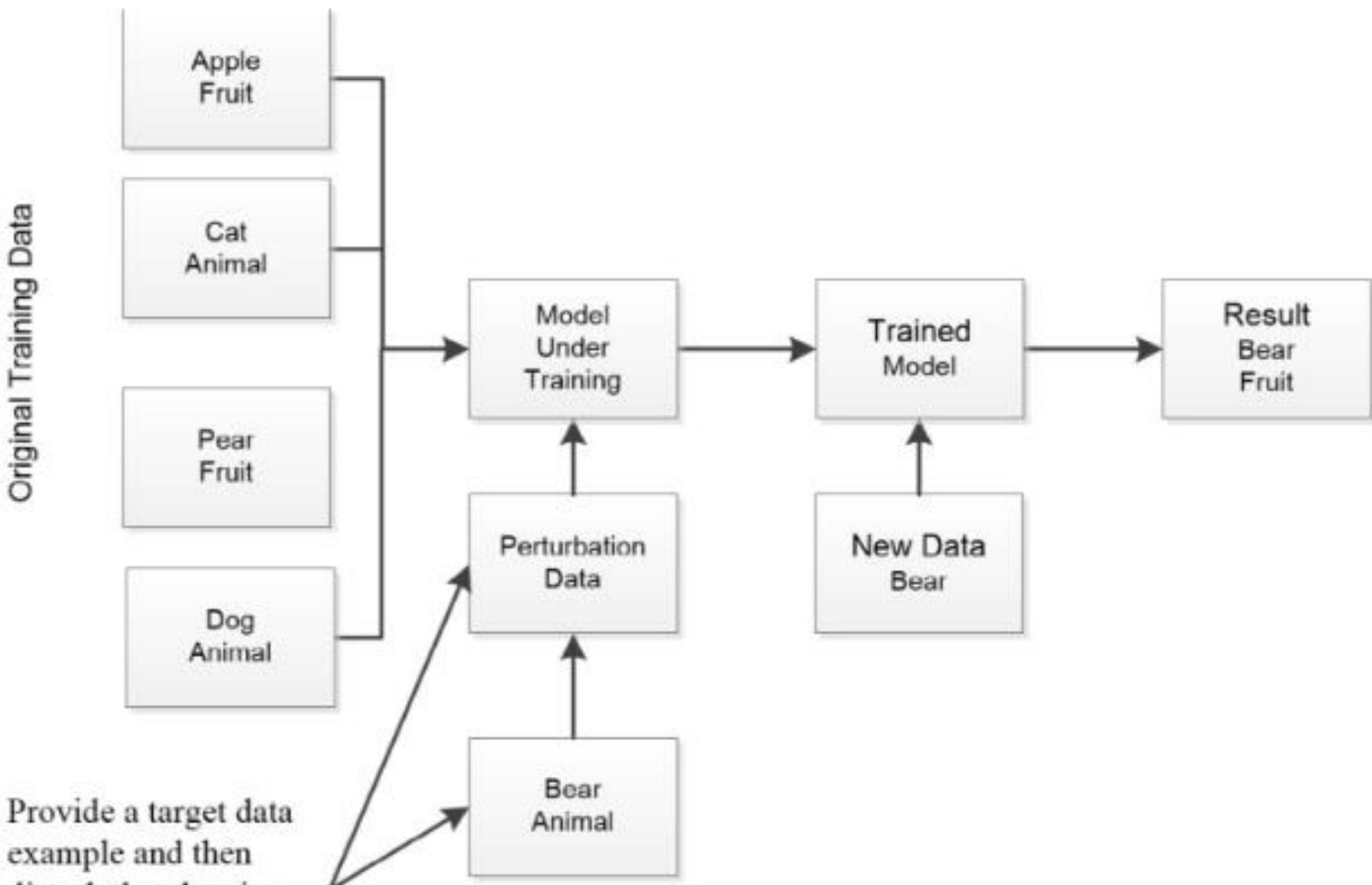
Understand Black Swan Theory

- High-profile, hard-to-predict, and rare events that history, science, finance, and technology can't explain
- Rare events that modern statistical methods can't calculate due to the small sample size
- Psychological biases that prevent people from seeing a rare event's massive effects on historical events

Antiknowledge

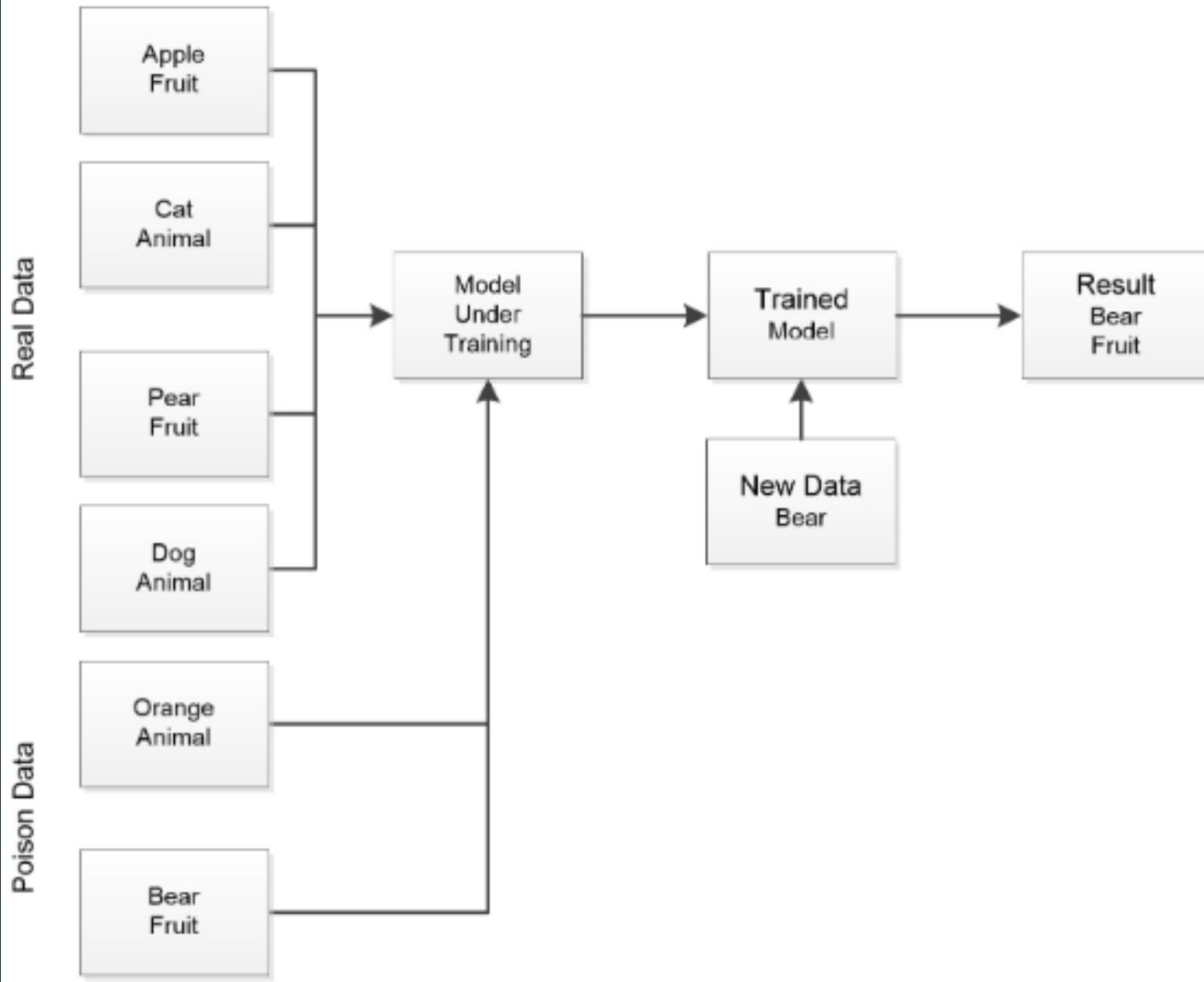
- Antiknowledge refers to any agent that reduces the level of knowledge available in a group or society.
- In ML, antiknowledge refers to the loss of knowledge about the inner workings or viability of algorithms, models, or other software due to the emergence of technologies, events, or data that infers previous knowledge is incorrect in some way.

Evasion Attack



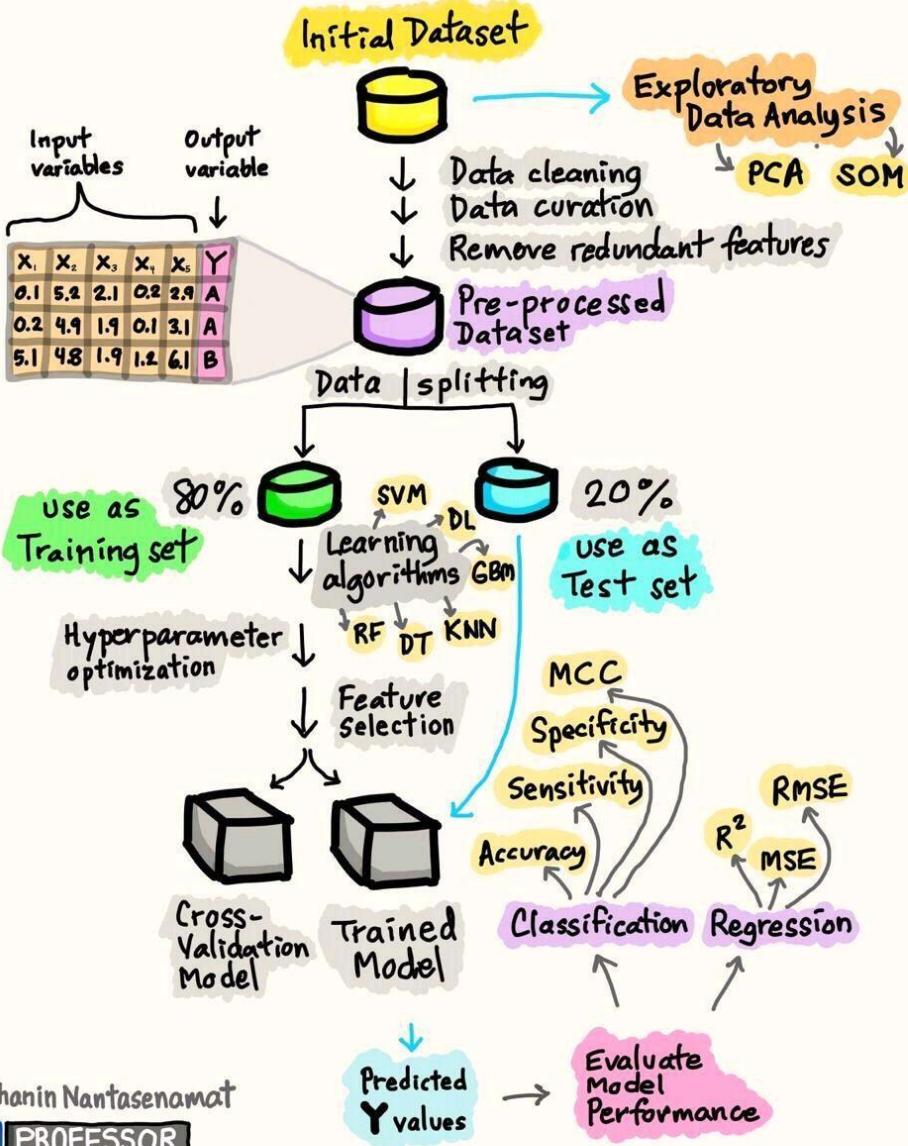
Provide a target data example and then disturb that data in a manner that causes misclassification.

Model Poisoning Attack



Model Skewing

BUILDING THE MACHINE LEARNING MODEL



January 1, 2020

Feedback Weaponization

5- Star System



5 Stars is the best rating. These artists are highly recommended. They have shown professionalism throughout their time working for Copyartwork.

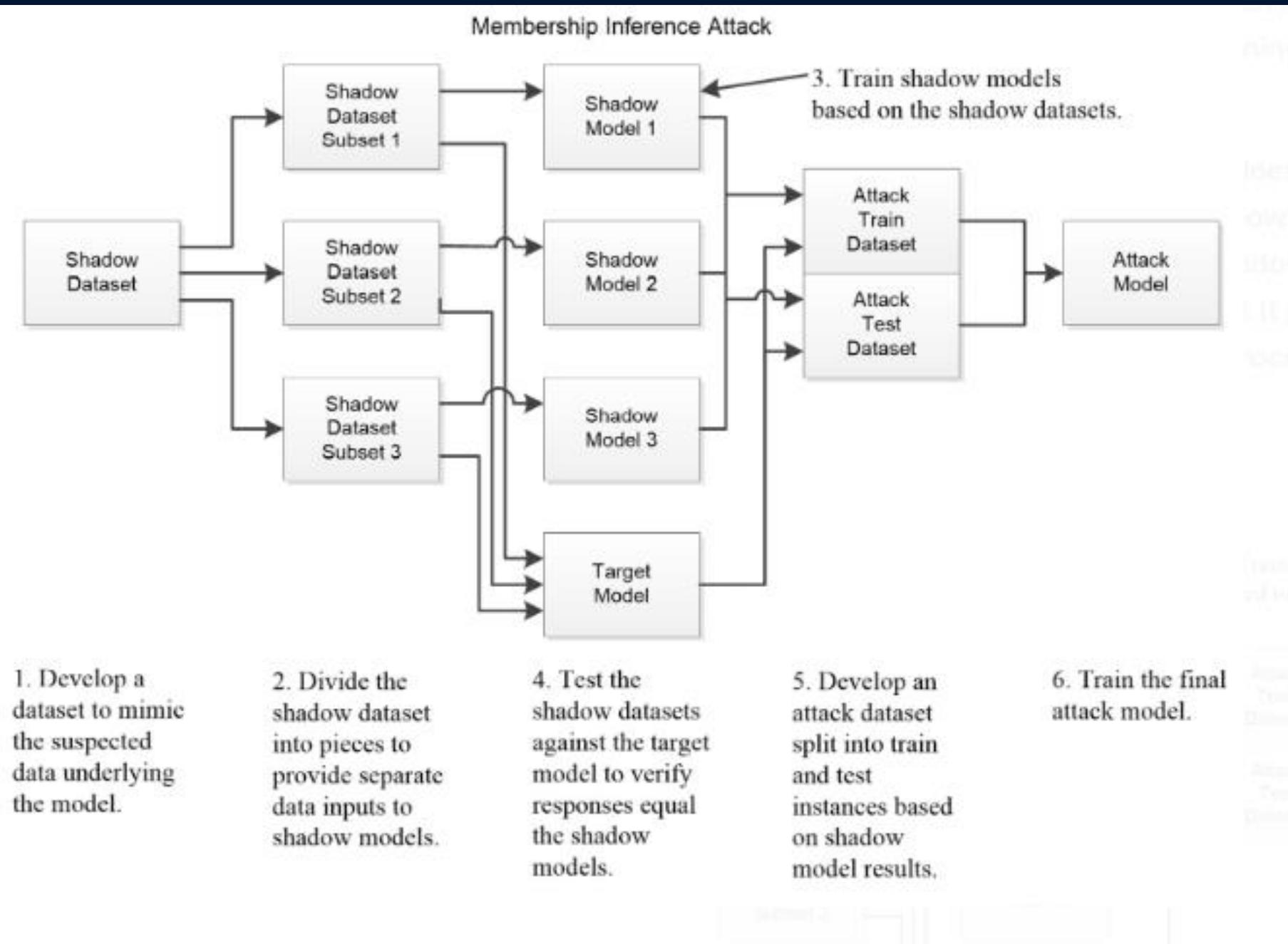
4 Stars is the second highest rating. These artists need a few more jobs under their belt to achieve 5 star status. They are still recommended by copyartwork.

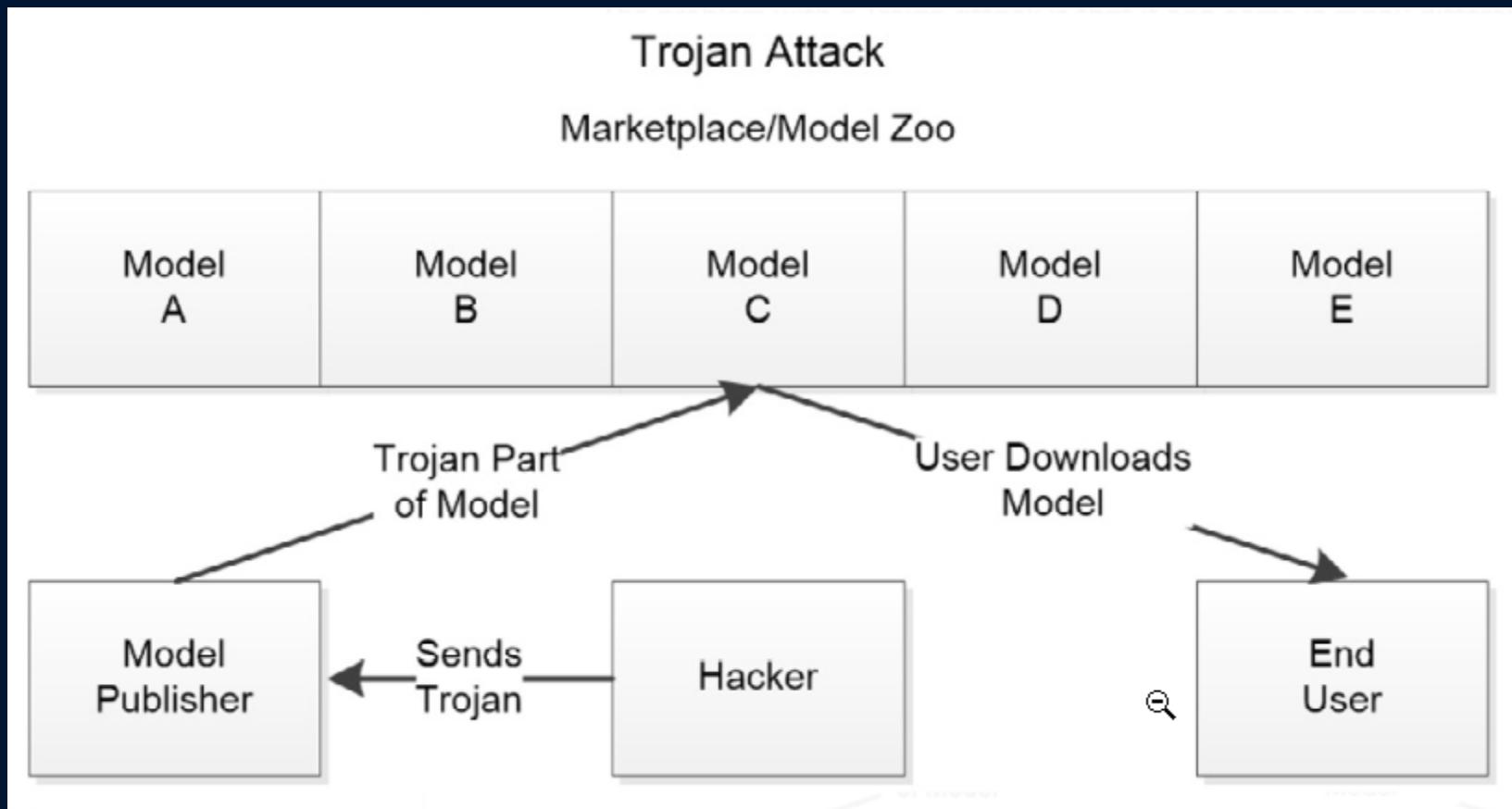
3 Stars is the rating given to the average artist. They have somewhat recently joined Copyartwork. They are still working to establish a good reputation on the site.

2 Star artists have done very few jobs with copyartwork, and are working on their reputation. They also may have a few minor mistakes in their work.

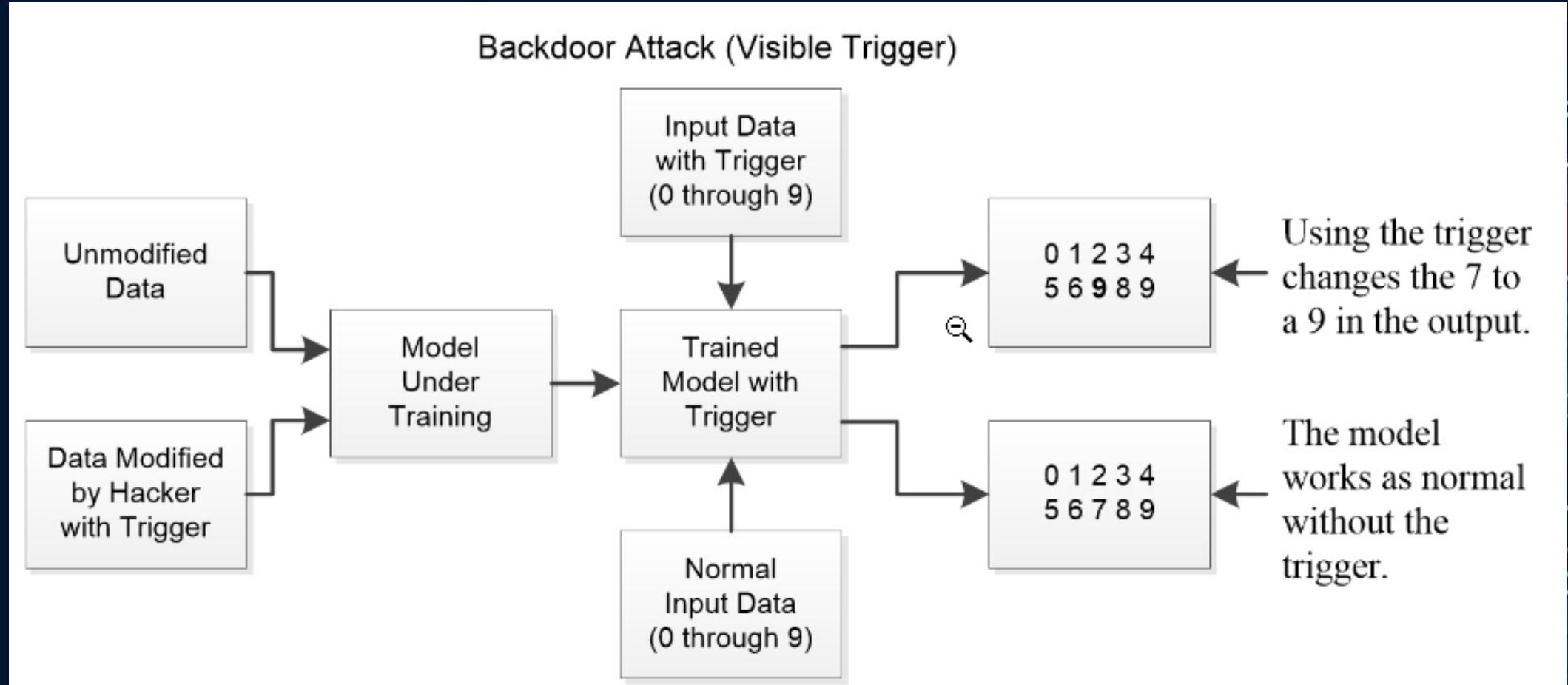
1 Star artists are brand new to copyartwork. They have completed very few jobs, so not much is known about their ability yet. Or, they have had some issues, that they need to correct

This Photo by Unknown Author is licensed under [CC BY-SA](#)

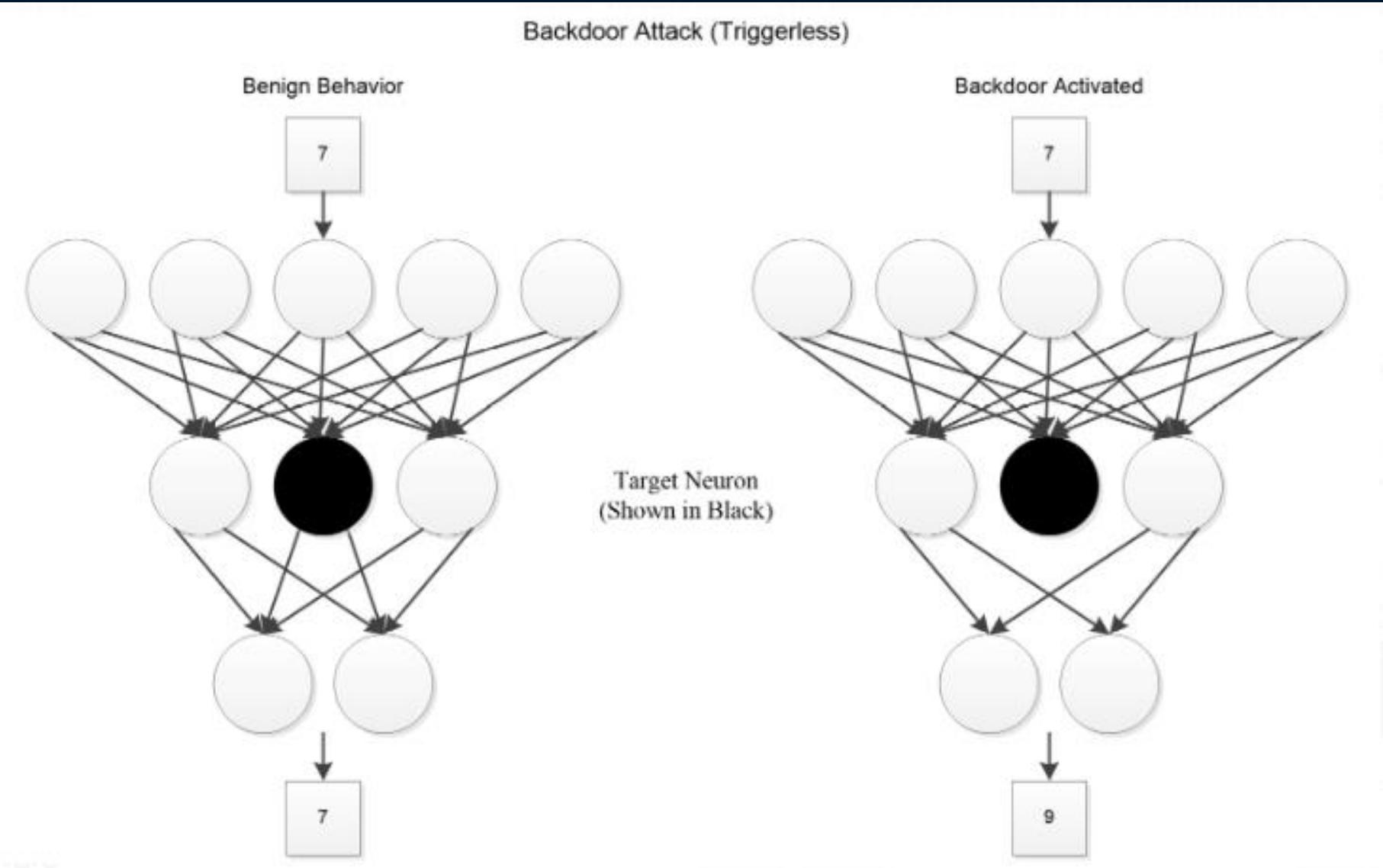




Backdoor (neural) attacks



Triggerless Backdoor Attack



See it in action...

- <https://kennysong.github.io/adversarial.js/>

Attack Types by Strength (Carlini & Wagner Strongest)

- Carlini and Wagner: See details at <https://arxiv.org/pdf/1608.04644.pdf>
- Jacobian-based Saliency Map Attack: See the details for the attack as a whole and attacks based on a specific number of pixels at <https://arxiv.org/abs/2007.06032> and <https://arxiv.org/pdf/1808.07945.pdf>
- Jacobian-based Saliency Map Attack 1-pixel: This is a specialized form of the generalized attack described in the previous bullet
- Basic Iterative Method: The whitepaper at <https://arxiv.org/pdf/1607.02533.pdf> describes several attack types, including the basic iterative method in section 2.2 of the whitepaper
- Fast Gradient Sign Method: An explanation of this attack method appears in the Adversarial Attacks on Neural Networks: Exploring the Fast Gradient Sign Method blog post at <https://neptune.ai/blog/adversarial-attacks-on-neural-networks-exploring-the-fast-gradient-sign-method>

ML Security in the Real World

- Ensuring user authentication (the validation that the user's identity is real) and authorization (giving the user the correct rights) go as planned
- Filtering out potentially hazardous data before the user even gets to see it

Understanding the kinds of App Security

- Role Based
- Attribute Based
- Resource Based
- Group Based
- Identity Based

The Minimum

1. Requesting authorization
2. Authenticating the individual
3. Monitoring and logging their access
4. Verifying that each action is allowed by the application security profile

Code Along...

Summary

Lab: None for this section

Hands-on Lab: Please refer to your Lab Guide
and follow the instructions provided by your Instructor

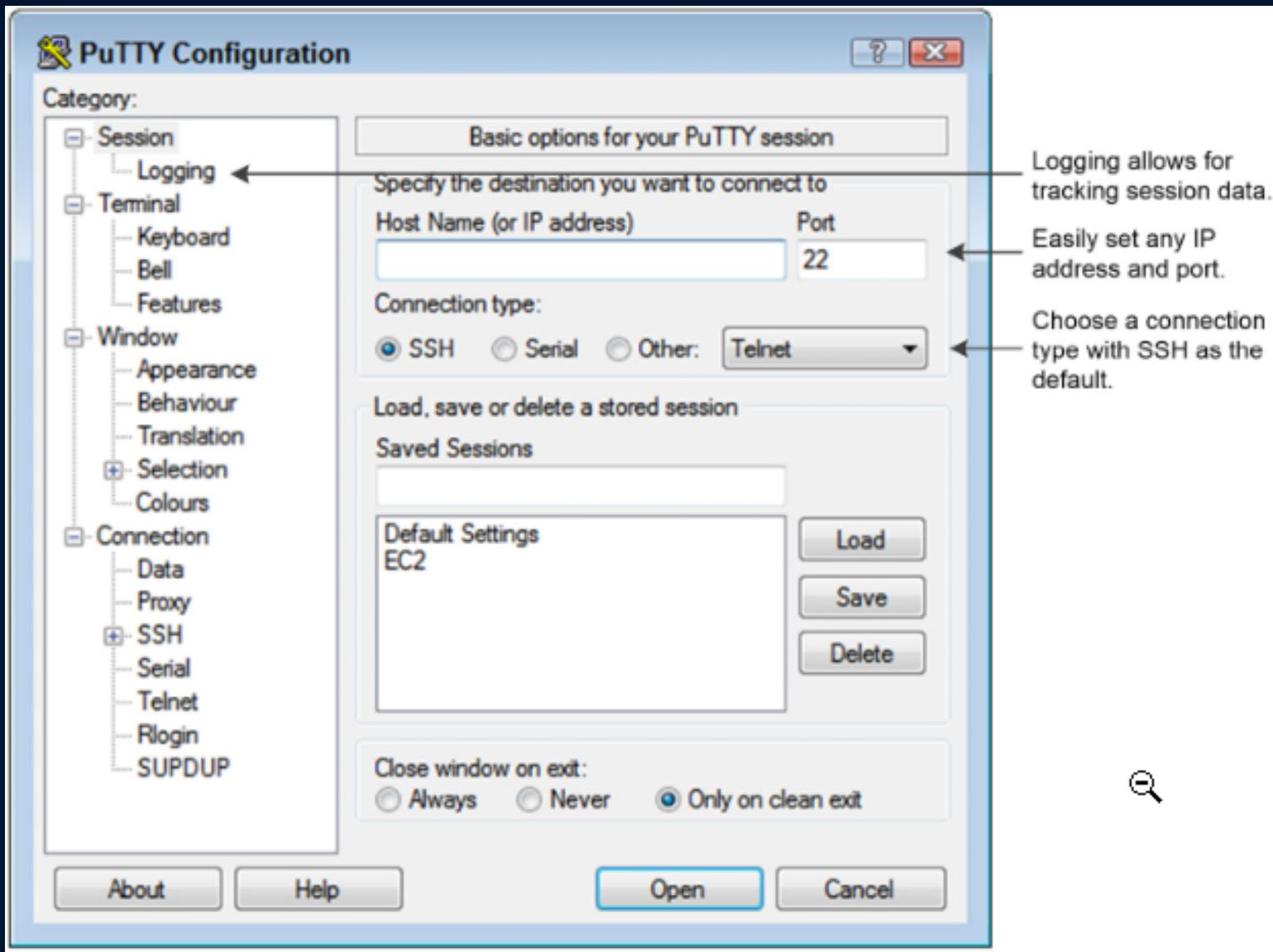
Chapter 4:

CSI Cyber

Keep Your Network Clean

Experience is

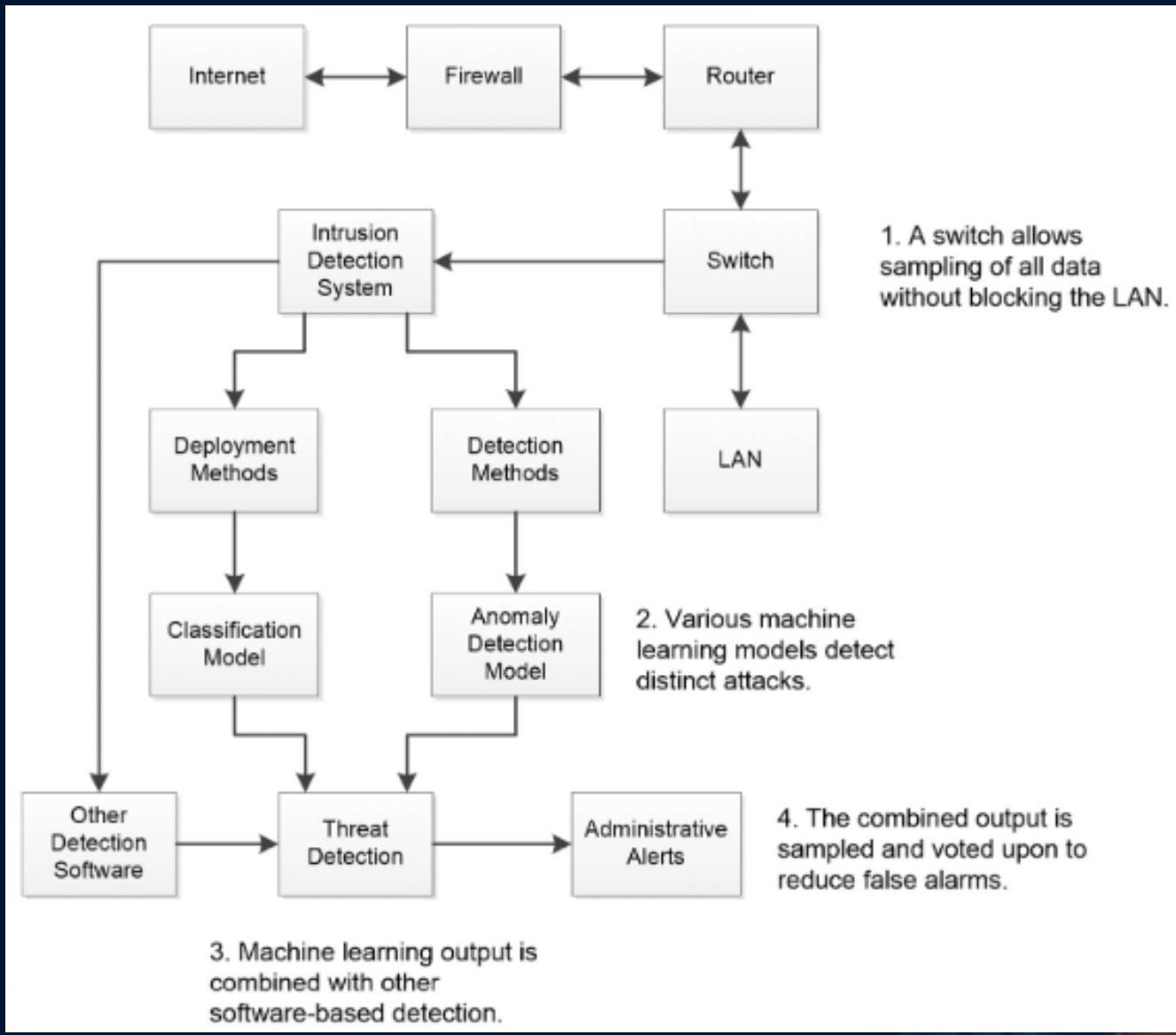
Access Control



Authentication

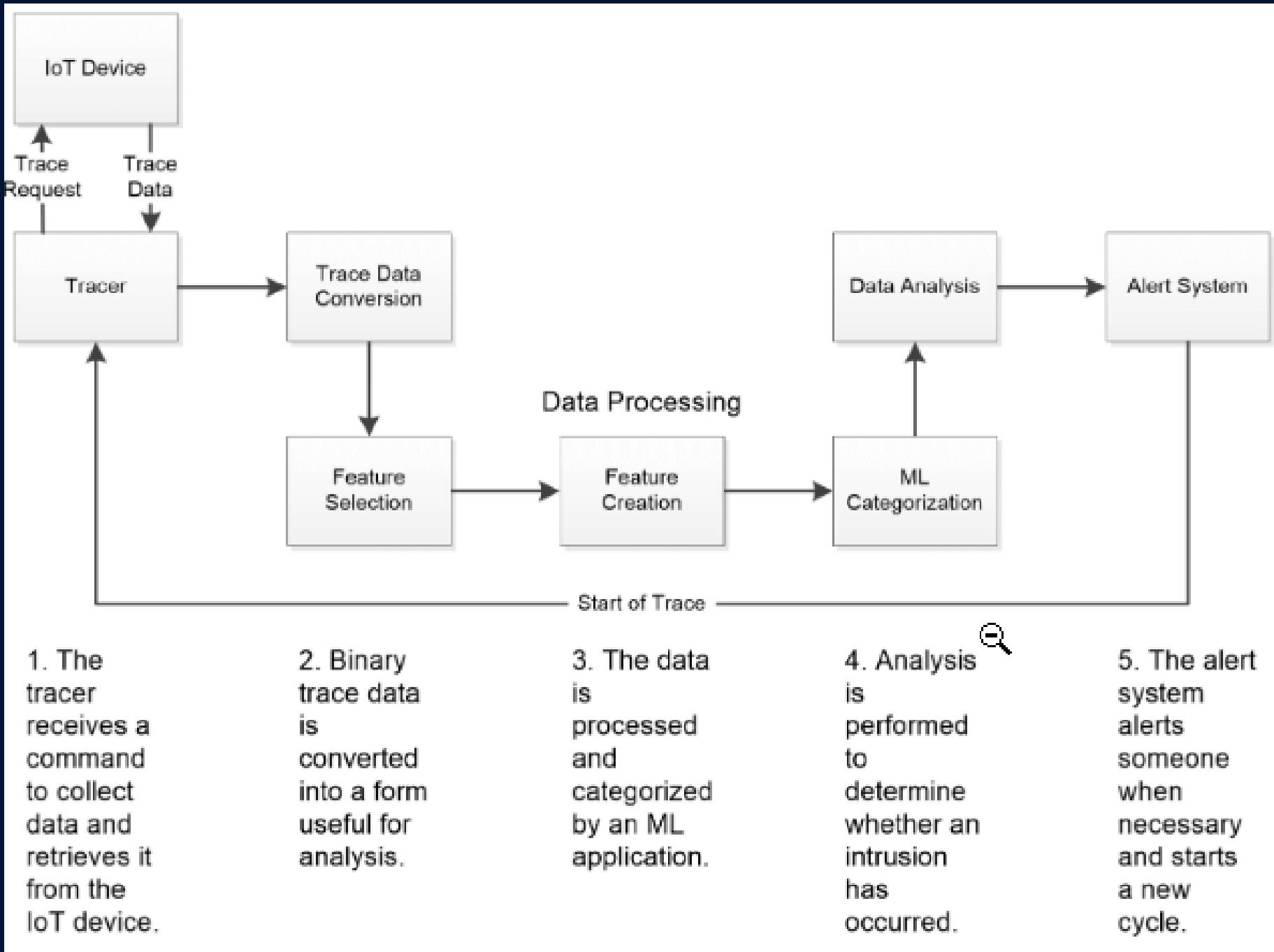
- Device type and/or name
- Location
- Network type
- Operating system
- User risk profile
- User tendencies

Intrusion Detection



Subtle Intrusion Detectors

1. A hacker gains entry to a smart device connected to the internet for monitoring purposes.
2. The hacker changes data in an unobtrusive manner on the device, such that the data will produce an unexpected result when processed by analytics software.
3. The user or host service accesses the device from a desktop system, tablet, or other device attached to the network.
4. The data modifications produce an unexpected result.
5. The network is now potentially open to attack due to the result produced by the analytics software.



Add ML to the AI Security Mix

- Perform regression analysis to determine whether certain packets are somehow flawed compared to normal packets from a given source. In other words, you're not dealing with absolutes but, rather, determining what is normal from a particular sender. Anything outside the normal pattern is suspect.
- Rely on classification to detect whether incoming data matches particular suspect patterns. Unlike signature matching, this form of analysis relies on training a neural network to recognize classes of data that it hasn't seen before. Consequently, even if an attacker changes a signature, the model can still likely recognize the data class.
- Use clustering to detect attack patterns and as part of forensic analysis in real time. For example, suddenly seeing groups of requests from a particular set of IP addresses that all have the same characteristics is a type of suspect pattern.

Develop an Updated Security Plan

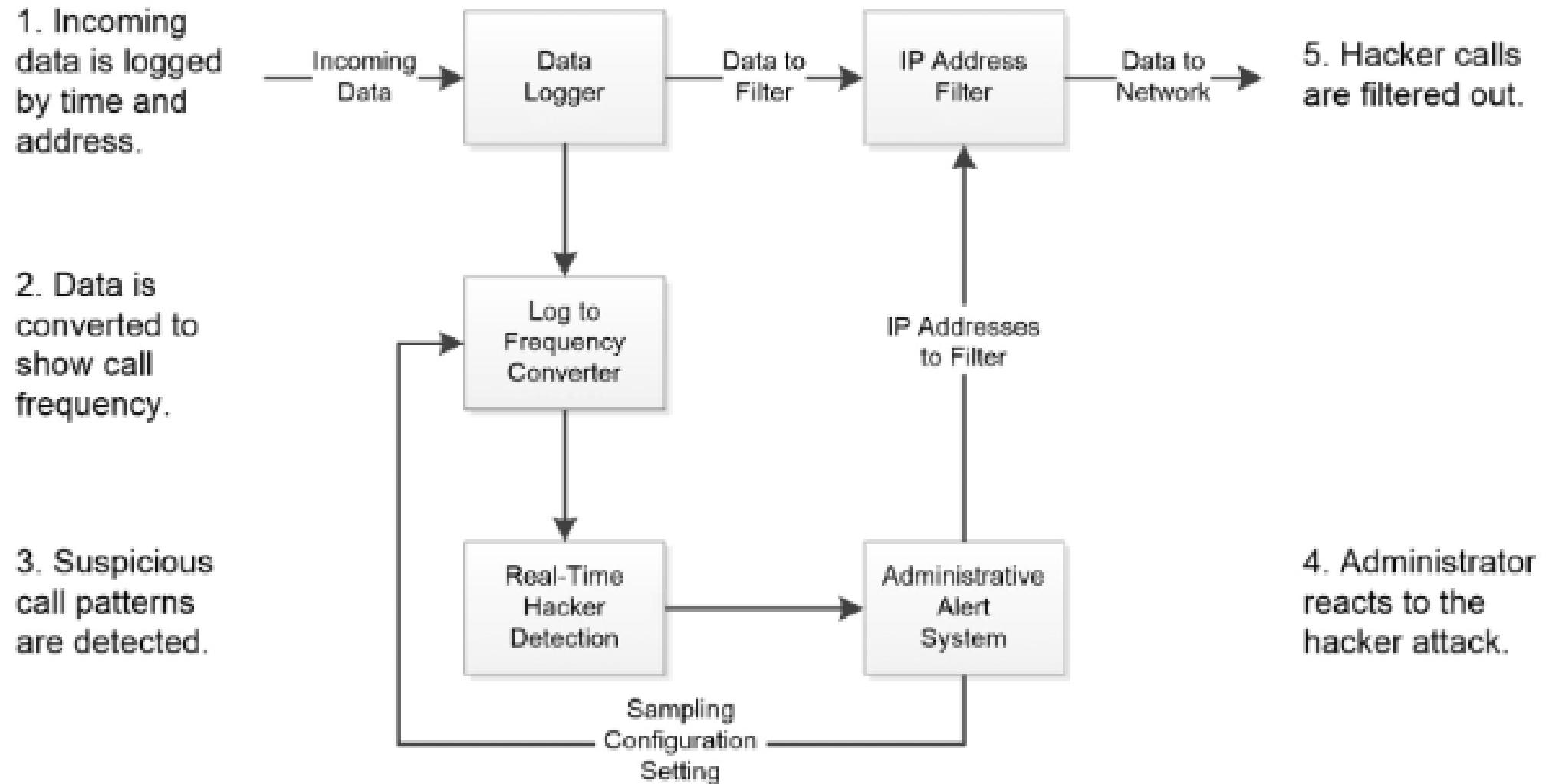
- Determining what sort of data to collect before, during, and after an attack
- Tracking user activities for analysis as part of detecting attack vectors
- Creating and testing models specifically designed for security needs and then providing instructions for deploying them during an attack

Which Features to Track

- Track user behaviors such as login time, the time between breaks, and other factors using regression
- Employ known user factors, such as meeting times, to classify users by peer group (such as a workgroup or users who exercise during lunch)
- Use clustering techniques to detect users who have unusual habits or aren't part of known groups (the outliers)

Real Time Defenses

- Detect
- Analyze
- Mitigate
- (DAM)



Code Along...



Lab: Lab Name (or Demo)

Hands-on Lab: Please refer to your Lab Guide
and follow the instructions provided by your Instructor

Chapter 5:

AI Adversarial Attacks and Defenses

Exploring Strategies and Defenses

Assessing the Vulnerability of Your Algorithms, Models, and AI Environments

- Reviewing the Azure Machine Learning life cycle
- Introducing an ML project
- Exploring the Zero Trust model
- Assessing the vulnerability of ML assets and apps

Cloud Machine Learning (Azure)

Microsoft Azure Search resources, services, and docs (G+/-)

Home > Create a resource > Marketplace >

Azure Machine Learning

Create a machine learning workspace

Basics Networking Advanced Tags Review + create

Resource details

Every workspace must be assigned to an Azure subscription, which is where billing happens. You use resource groups like folders to organize and manage resources, including the workspace you're about to create.
[Learn more about Azure resource groups](#)

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Workspace details

Configure your basic workspace settings like its storage connection, authentication, container, and more. [Learn more](#)

Workspace name * ⓘ ✓

Region * ⓘ ✓

Storage account * ⓘ [Create new](#)

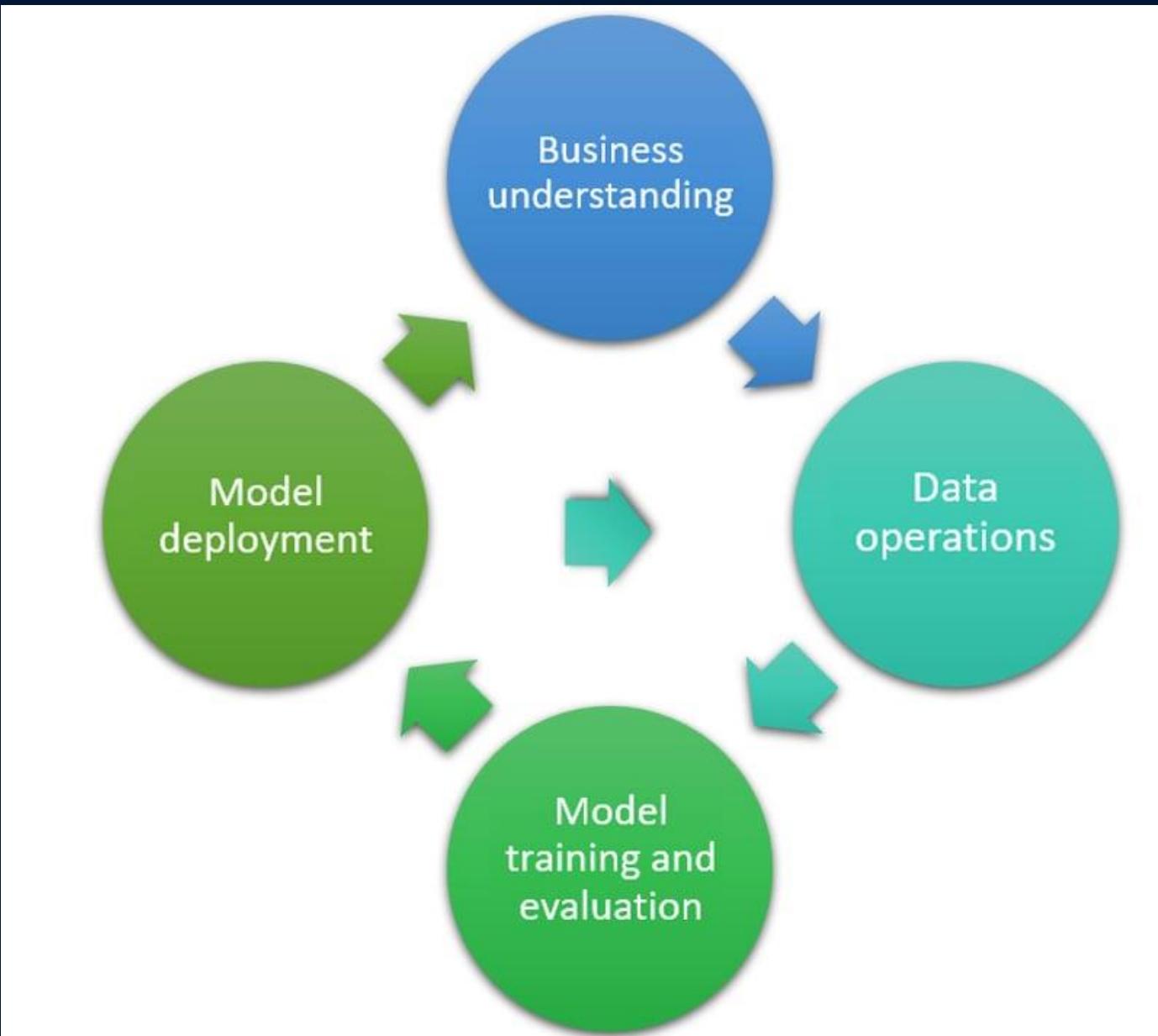
Key vault * ⓘ [Create new](#)

Application insights * ⓘ [Create new](#)

Container registry * ⓘ [Create new](#)

[Review + create](#) [< Previous](#) [Next : Networking](#)

Cloud ML Life Cycle



[All workspaces](#)[Home](#)[Model catalog PREVIEW](#)[Authoring](#)[Notebooks](#)[Automated ML](#)[Designer](#)[Prompt flow PREVIEW](#)[Assets](#)[Data](#)[Jobs](#)[Components](#)[Pipelines](#)[Environments](#)[Models](#)[Endpoints](#)[Manage](#)[Compute](#)[Monitoring PREVIEW](#)[Data Labeling](#)[Linked Services](#)

Azure Machine Learning

[+ New](#)

Generative AI with Prompt flow PREVIEW ...



Chat With Wikipedia

ChatGPT-based chatbot that leverages Wikipedia data to ground the responses.

[Start](#)

Vector DB QnA Step 1

Build Faiss index used for Vector DB QnA

[Start](#)

Web Classification

Create flows that use large language models to classify URLs into multiple categories.

[Start](#)

Generative AI models PREVIEW ...

openai-whisper-large

Speech recognition

databricks-dolly-v2-12b

Text generation

Notebook samples ...



Get started: Train and deploy a model

Train and deploy a sample image classification model.



Arbitration agents using LangChain

Demonstration of LangChain agent to implement the ReAct logic using Azure OpenAI endpoints.



Index and search your own data with GPT

Bring your own data to look up using GPT with LangChain



Distributed GPU training

Run a sample multi-GPU image classification experiment.

[All workspaces](#)[Home](#)[Model catalog](#)[Authoring](#)[Notebooks](#)[Automated ML](#)[Designer](#)[Assets](#)[Data](#)[Jobs](#)[Components](#)[Pipelines](#)[Environments](#)[Models](#)[Endpoints](#)[Manage](#)[Compute](#)[Linked Services](#)[Data Labeling](#)

Create data asset

1 Data type

2 Data source

3 Azure Open Dataset

4 Review

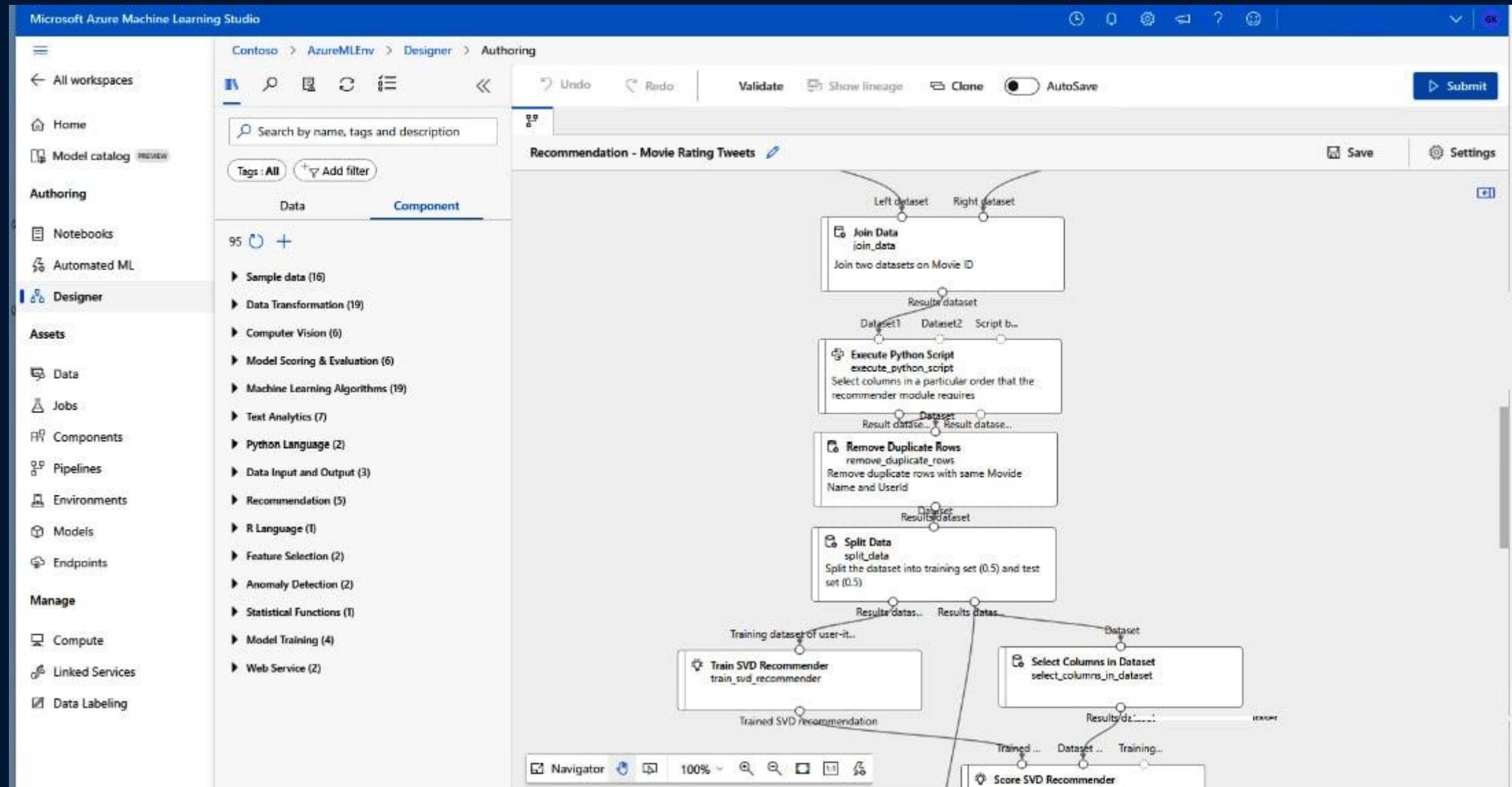
Choose a source for your data asset

Choose the data source you want to create your asset from. A data source can be from a local storage location on your computer, from an attached datastore, from Azure storage, or from a public web URL.

**From Azure storage****From SQL databases****From Azure Open Datasets****From local files****From web files**

Create a dataset with one-click from pre-made data sets. These data sets are created by the general public and published as Azure Open Datasets

[Back](#)[Next](#)



- [All workspaces](#)
- [Home](#)
- [Model catalog](#)
- Authoring**
- [Notebooks](#)
- Automated ML**
- [Designer](#)
- Assets**
- [Data](#)
- [Jobs](#)
- [Components](#)
- [Pipelines](#)
- [Environments](#)
- [Models](#)
- [Endpoints](#)
- Manage**
- [Compute](#)
- [Linked Services](#)
- [Data Labeling](#)

Create a new Automated ML job

- 1 Select data asset
- 2 Configure job
- 3 Select task and settings**
- 4 Hyperparameter configuration
(Computer Vision only)
- 5 Validate and test

Select task and settings

Select the machine learning task type for the experiment. To fine tune the experiment, choose additional configuration or featurization settings.



Classification

To predict one of several categories in the target column. yes/no, blue, red, green.



Regression

To predict continuous numeric values.



Time series forecasting

To predict values based on time.



Natural language processing

Predict based on text-only data types using multi-class or multi-label classification.



Computer vision

Multi-class or multi-label image classification, object detection, and instance segmentation.

[View additional configuration settings](#) [View featurization settings](#)

Notebooks

The screenshot shows the Microsoft Azure Machine Learning Studio interface. The left sidebar contains a navigation tree with categories such as 'All workspaces', 'Home', 'Model catalog', 'Authoring', 'Notebooks' (which is selected), 'Automated ML', 'Designer', 'Assets', 'Data', 'Jobs', 'Components', 'Pipelines', 'Environments', 'Models', 'Endpoints', 'Manage', 'Compute', 'Linked Services', and 'Data Labeling'. The main content area is titled 'Notebooks' and shows a list of notebooks under the 'Samples' category. One notebook, 'quickstart.ipynb', is currently selected and displayed. The notebook content starts with a section titled 'Create training script' with the following text: 'Let's start by creating the training script - the `main.py` Python file.' Below this, it says 'First create a source folder for the script:' followed by a code snippet:

```
1 import os
2
3 train_src_dir = "./src"
4 os.makedirs(train_src_dir, exist_ok=True)
```

Further down, there is more text: 'This script handles the preprocessing of the data, splitting it into test and train data. It then consumes this data to train a tree based model and return the output model. MLFlow will be used to log the parameters and metrics during our pipeline run.' At the bottom, it says 'The cell below uses IPython magic to write the training script into the directory you just created.' followed by another code snippet:

```
1 %%writefile {train_src_dir}/main.py
2
3 import os
4 import argparse
5 import pandas as pd
6 import mlflow
7 import mlflow.sklearn
8 from sklearn.ensemble import GradientBoostingClassifier
9 from sklearn.metrics import classification_report
10 from sklearn.model_selection import train_test_split
11
12 def main():
13     """Main function of the script"""
14
15     # Read the data
16     df = pd.read_csv("adult.csv")
```

ML Project

AzureML Azure Machine Learning workspace

Search Download config.json Delete

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Events

Networking Properties Locks

Alerts Metrics Diagnostic settings

Essentials

Resource group :	ML	Studio web URL :	https://ml.azure.com/?tid=9ee746b-3eeb-
Location :	West Europe	Container Registry :	azuremlhub
Subscription :		Key Vault :	azuremlkeyvault
Subscription ID :		Application Insights :	azuremlinsights
Storage :	azuremlfs	MLflow tracking URI :	azureml://westeurope.api.azureml.ms/mlflow/v1.0/subscription...

Work with your models in Azure Machine Learning Studio

The Azure Machine Learning Studio is a web app where you can build, train, test, and deploy ML models. Launch it now to start exploring, or [learn more about the Azure Machine Learning Studio](#)

[Launch studio](#)

Please complete Lab 1: Setup your Azure Environment

- We will break into groups of 2 or 3
- Please download the Lab 1 Lab Guide from here:
- <https://github.com/fenago/ai-security/tree/main/lab-guides>

[All workspaces](#)[Home](#)[Model catalog](#)[Authoring](#)[Notebooks](#)[Automated ML](#)[Designer](#)[Assets](#)[Data](#)[Jobs](#)[Components](#)[Pipelines](#)[Environments](#)[Models](#)[Endpoints](#)[Manage](#)[Compute](#)[Linked Services](#)[Data Labeling](#)

Create data asset

1 Data type

2 Data source

Set the name and type for your data asset

Name *

*

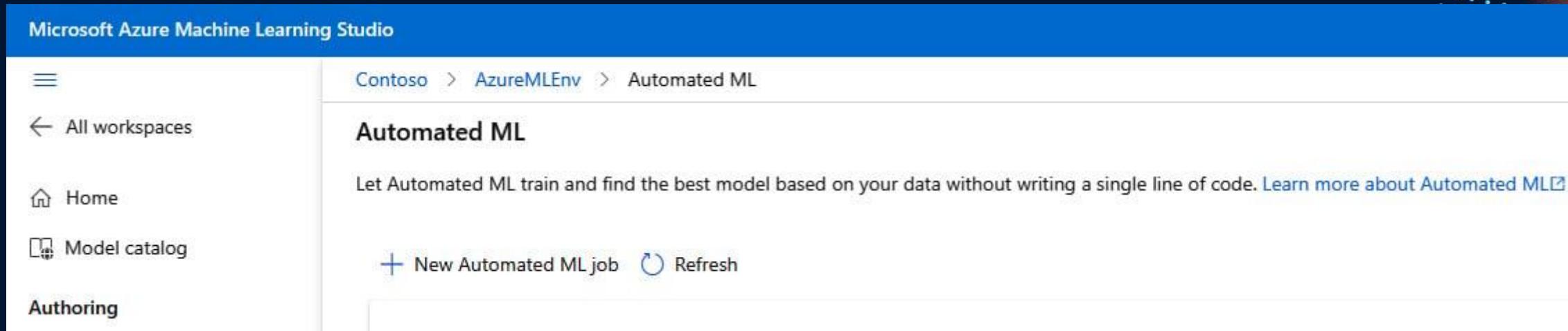
Description

The Diabetes dataset has 442 samples with 10 features, making it ideal for getting started with machine learning algorithms.

Type * ⓘ

[Back](#)[Next](#)

Training the Model in the Cloud



The screenshot shows the Microsoft Azure Machine Learning Studio interface. The top navigation bar is blue with the text "Microsoft Azure Machine Learning Studio". Below it, the breadcrumb navigation shows "Contoso > AzureMLEnv > Automated ML". On the left, there is a sidebar with icons for "All workspaces", "Home", "Model catalog", and "Authoring". The main content area is titled "Automated ML" and contains the sub-instruction: "Let Automated ML train and find the best model based on your data without writing a single line of code. [Learn more about Automated ML](#)". At the bottom of this section are two buttons: "+ New Automated ML job" and "⟳ Refresh".

☰
← All workspaces

HomeAs

Model catalog PREVIEW

Authoring

Notebooks

Automated ML

Designer

Assets

Data

Jobs

Components

Pipelines

Environments

Models

Endpoints

Contoso > AzureMLEnv > Automated ML > diabetes-automl > bold_chayote_ycdd48jr

bold_chayote_ycdd48jr edit star checkmark Completed

Overview Data guardrails Models Outputs + logs Child jobs

⟳ Refresh ⏪ Deploy ⏴ Download ⏷ Explain model # View generated code ⏮ View options

Search

Algorithm name	Explained	Normalized ro...	Sampling	Created on
VotingEnsemble	View explanation	0.16786	100.00 %	May 5, 2023
StackEnsemble		0.17017	100.00 %	May 5, 2023
StandardScalerWrapper, ElasticNet		0.17039	100.00 %	May 5, 2023
StandardScalerWrapper, ElasticNet		0.17039	100.00 %	May 5, 2023
StandardScalerWrapper, ElasticNet		0.17039	100.00 %	May 5, 2023
MaxAbsScaler, ElasticNet		0.17039	100.00 %	May 5, 2023
RobustScaler, ElasticNet		0.17041	100.00 %	May 5, 2023

Make Predictions from the Deployed Model

Microsoft Azure Machine Learning Studio

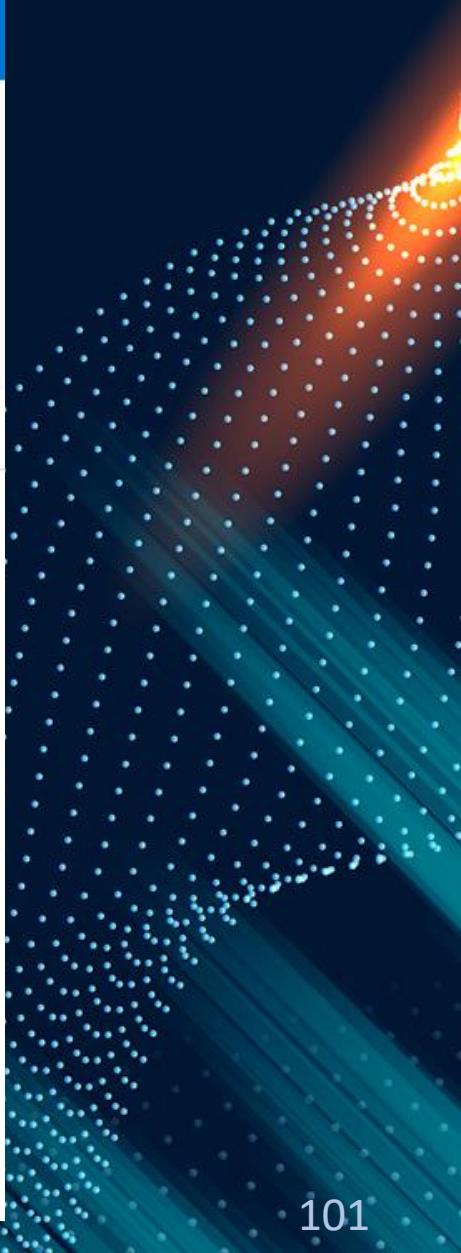
Contoso > AzureMLEnv > Endpoints > diabetes-automl-v2

diabetes-automl-v2

Details Test Consume Deployment logs

Endpoint attributes

Service ID	diabetes-automl-v2
Description	--
Deployment state	Healthy 
Operation state	Succeeded
Compute type	Container instance
Created by	System Administrator
Model ID	AutoML2362f010042:1

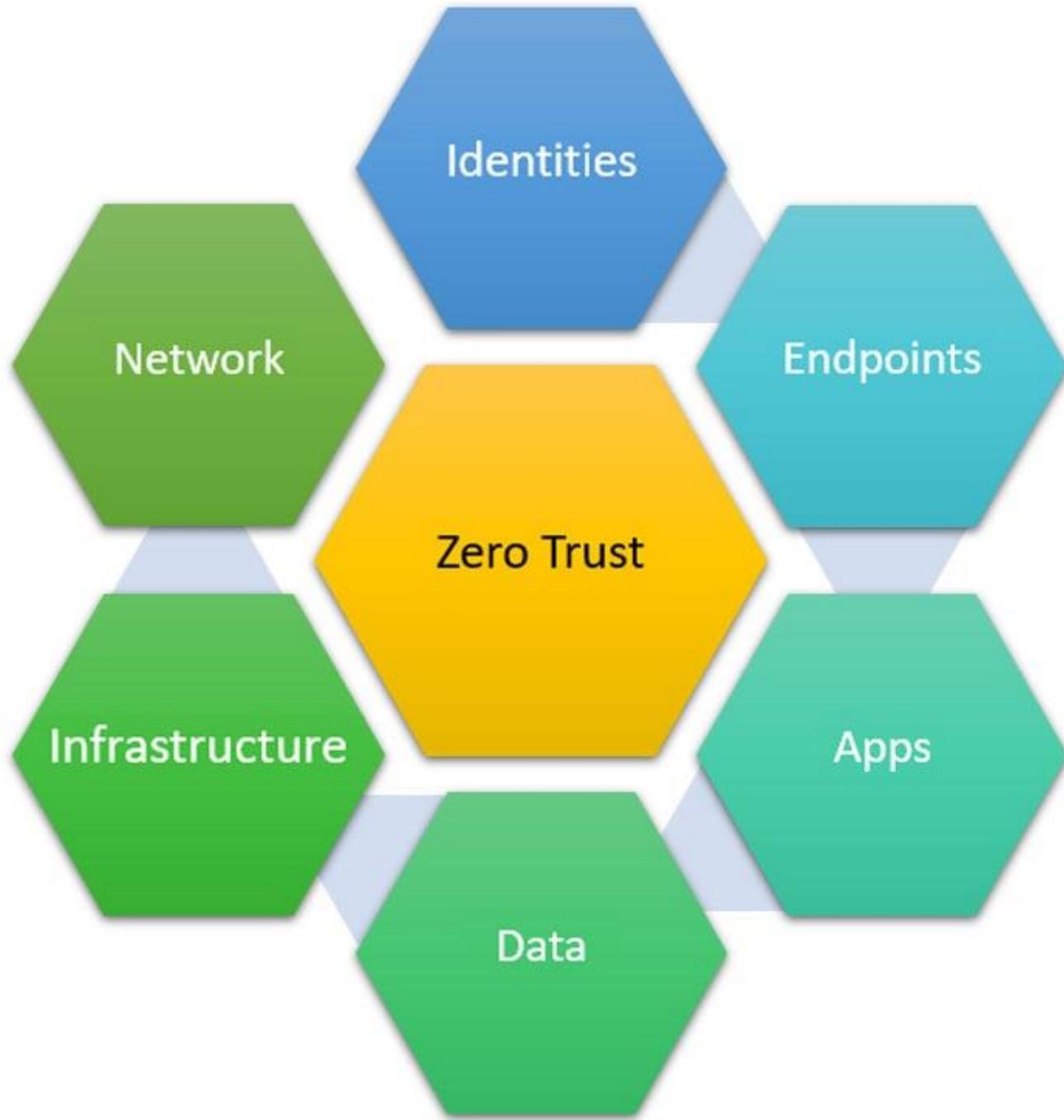


Copyright © 2024 Trivera Technologies LLC. | www.triveratech.com

Labs 2,3,4

Zero Trust Model

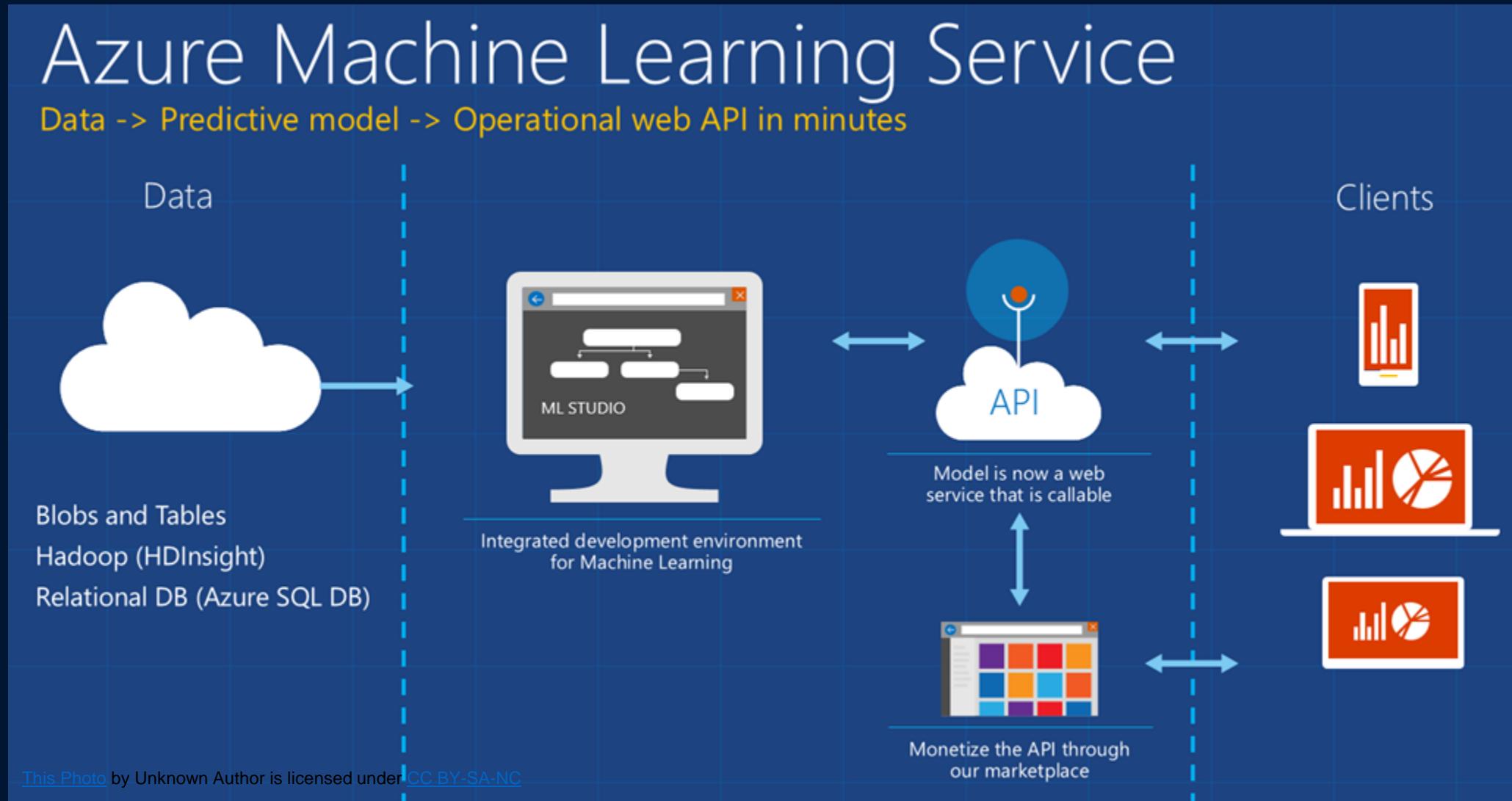
- Verify Explicitly
- Use Least Privilege Access
- Assume Breach



Assessing the vulnerability of ML assets and apps

1. Identity Management
2. Data and Data Sources
3. Infrastructure
4. Network and End-Points
5. Monitoring and Maintenance

AI/ML Applications



Lab 5

Summary

Experience is

Chapter 6:

Crisis Averted: AI Incident Response Planning

Develop and Implement effective incident response plans for AI system breaches:
Compliance and Regulatory

Compliance and Regulatory

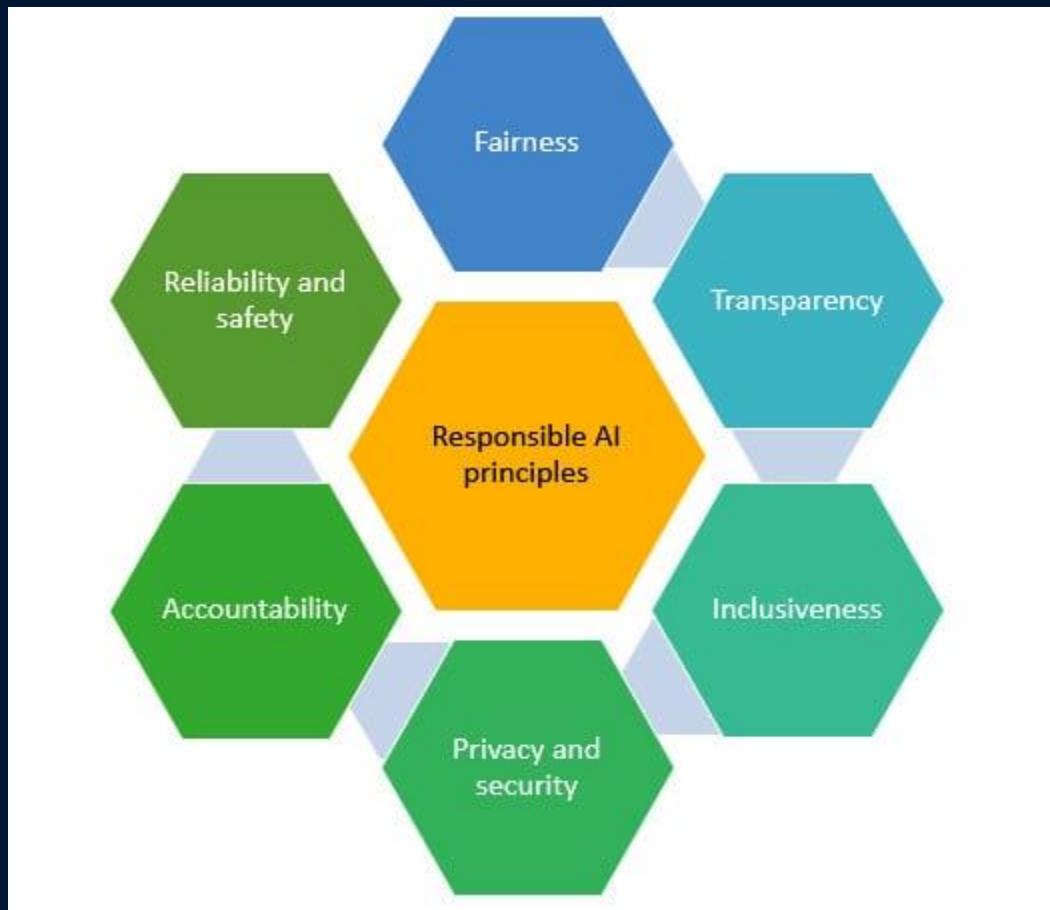
- Exploring Responsible AI development
- Regulatory compliance in Azure Policy for Azure Machine Learning
- Compliance auditing and reporting
- Compliance automation in Azure

Re

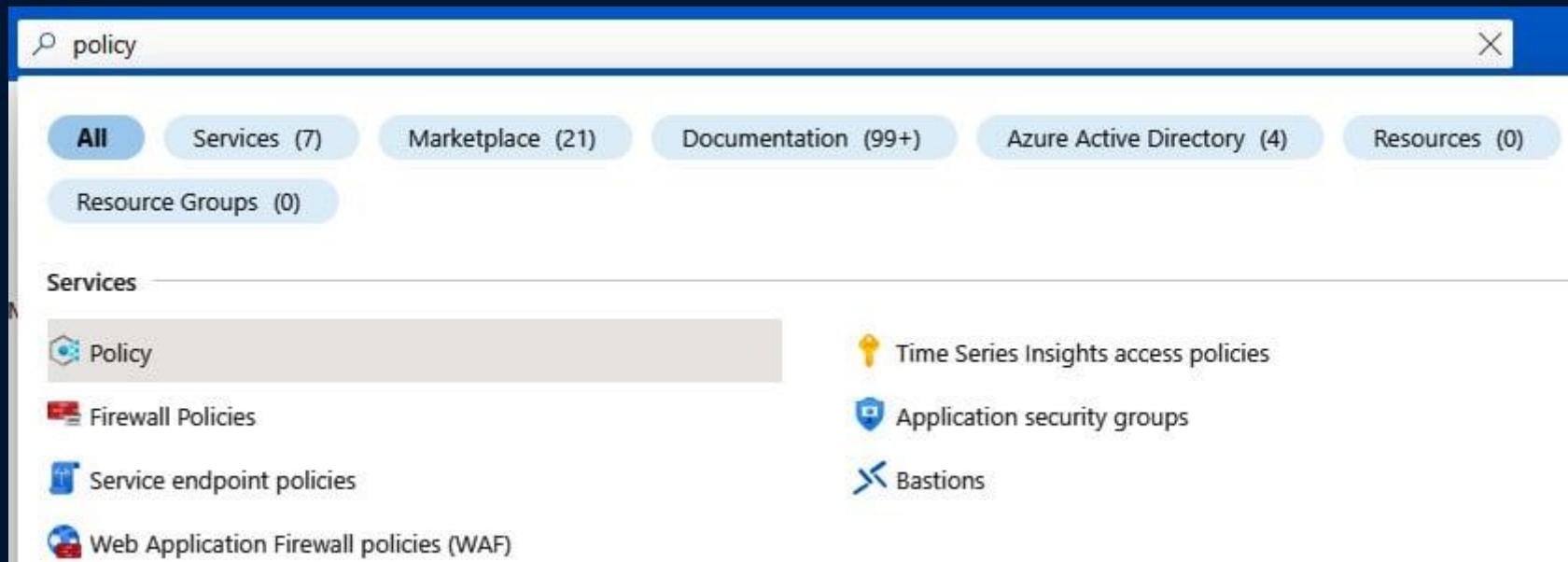


RESPONSIBLE

Responsible AI Principles



Regulatory Compliance in Azure Policy for Azure ML



Lab 6



Microsoft Compliance Ecosystem



Service Trust Portal
Audit Reports



Microsoft Defender for Cloud
Workload/Posture Protection

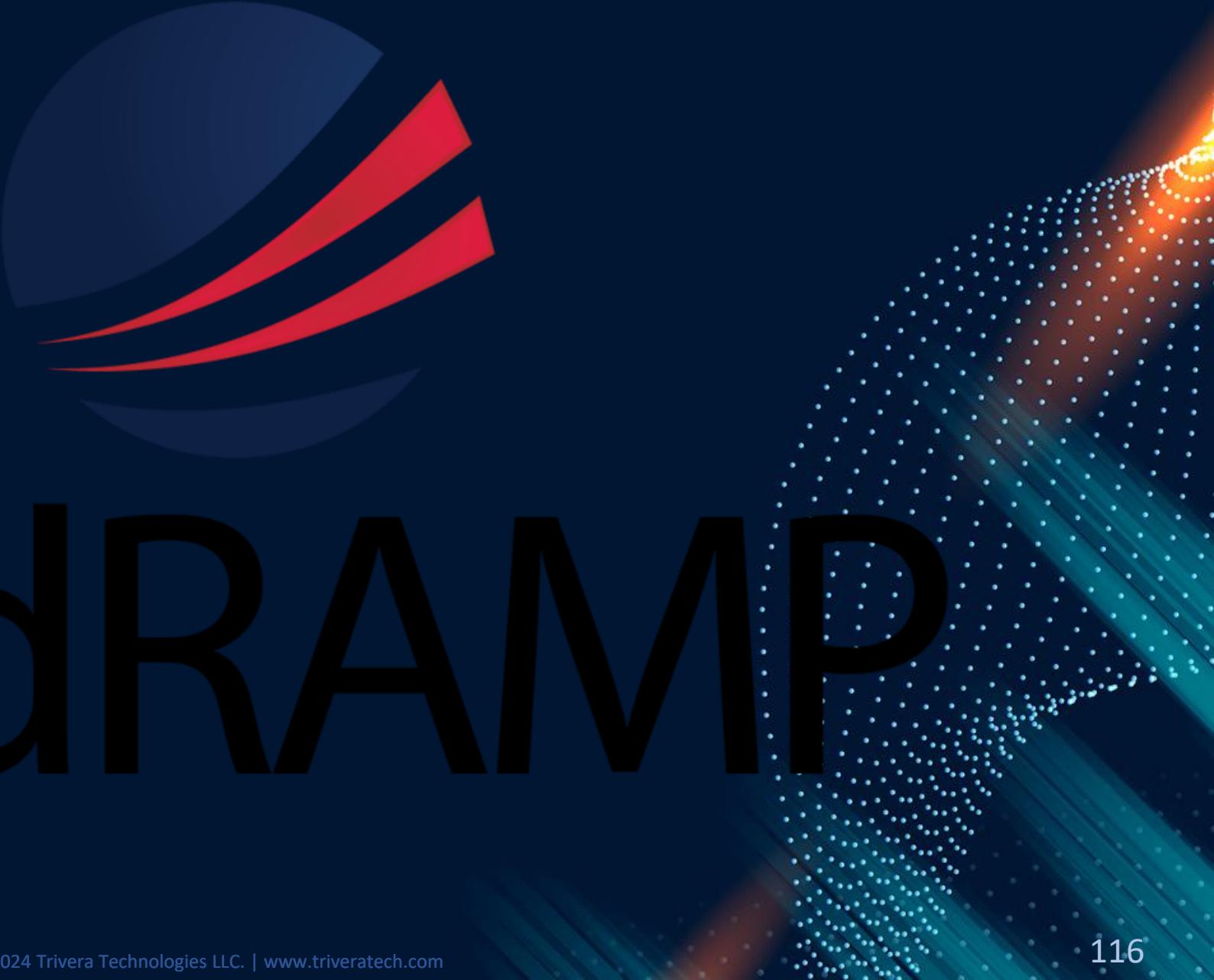


Microsoft Sentinel
Monitoring



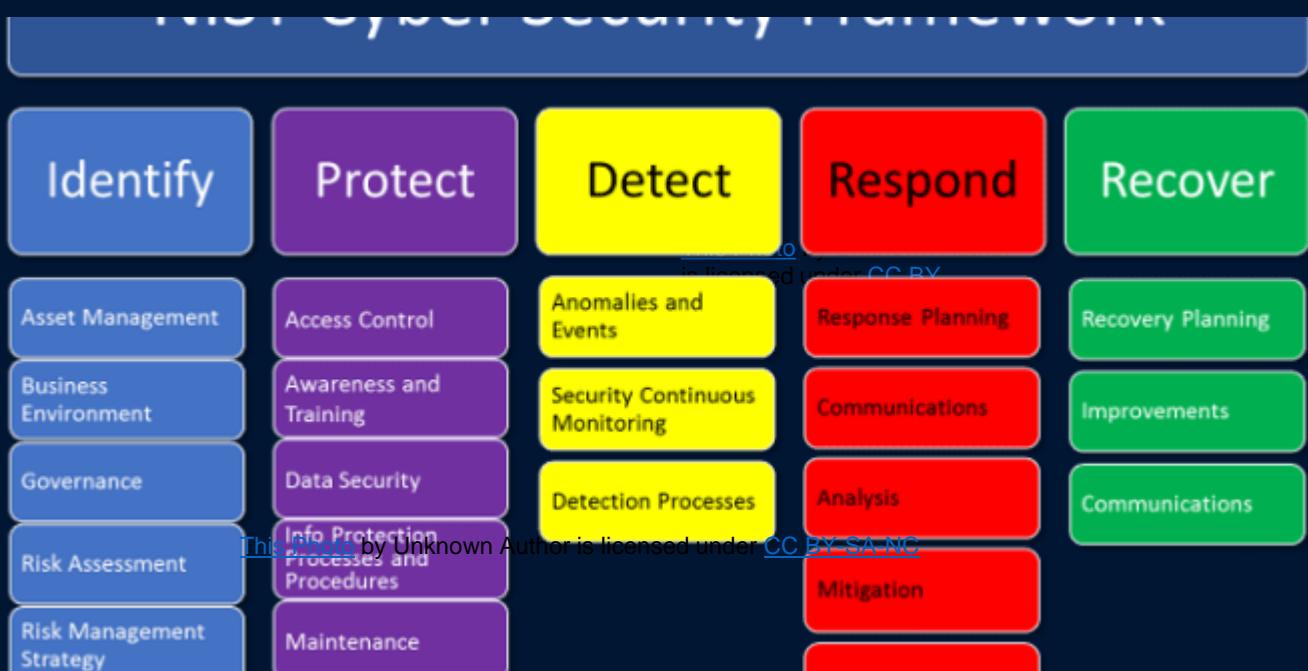
Microsoft 365 Compliance Manager
Compliance Management

FedRAMP



FedRAMP

NIST SP 800-53 rev. 5





AUDIT

Azure Portal

Microsoft Azure Search resources, services, and docs (G+) Home Policy X

Scope: 2 selected

Compliance state change events are now available at the management group level. Use event-based architecture to react to notifications with an Azure Function, Logic App, or any other supported event handler. Learn more <https://aka.ms/policyPlusEventGrid>

Overall resource compliance: 57% (8 out of 14)

Resources by compliance state: 8 - Compliant (green), 6 - Non-compliant (red)

Non-compliant initiatives: 1 out of 1

Non-compliant policies: 62 out of 222

LEARN MORE: [Learn about Policy](#) [Onboarding tutorial](#)

Name	Scope	Compliance state	Resource compliance	Non-Compliant Resources	Non-compliant policies	Actions
ASC Default (subscription: ...)	MSDN Platforms Subscription	Non-compliant	0% (0 out of 6)	6	62	...
Allowed locations	MSDN Platforms Subscription	Compliant	100% (13 out of 13)	0	0	...

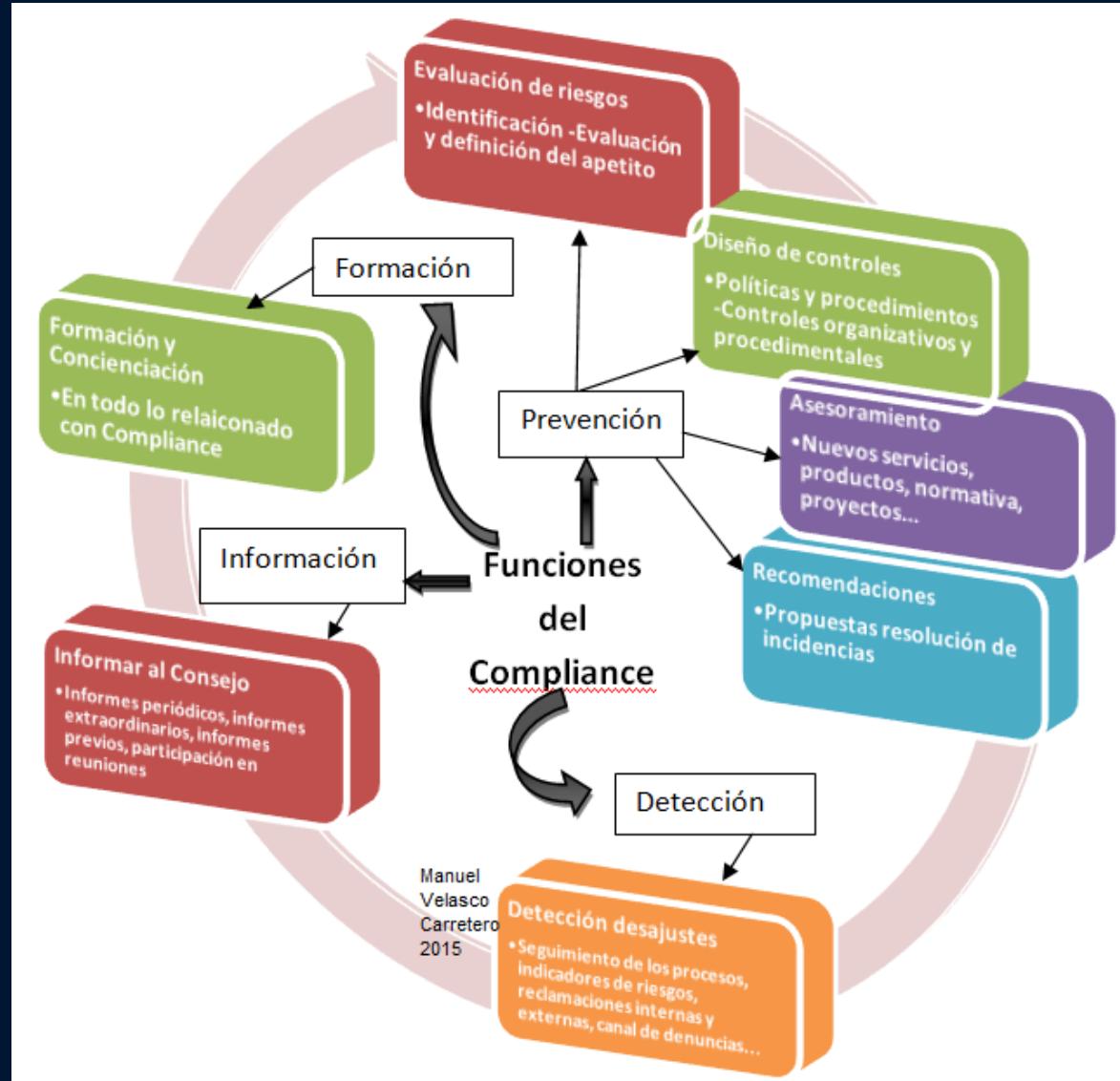
[View all](#)

ASSIGNMENTS BY COMPLIANCE (LAST 7 DAYS)

Date	ASC Default...	Allowed loc...
5/1/2023	6	0
6/1/2023	6	0
6/3/2023	6	0

Lab 7: Azure Resource Graph Explorer

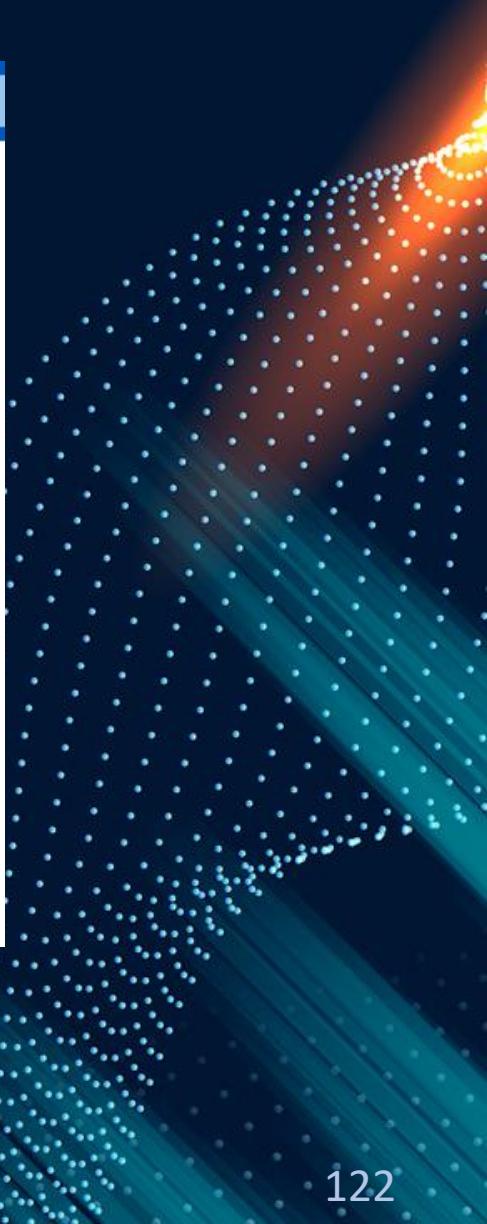
Compliance Automation



This Photo by Unknown Author is licensed under [CC BY-ND](#)

Copyright © 2024 Trivera Technologies LLC. | www.triveratech.com

Azure Blueprints



Microsoft Azure

Search resources, services, and docs (G+)

Home > Blueprints | Getting started >

Create blueprint

Basics Artifacts

Blueprint name * ⓘ

 ✓

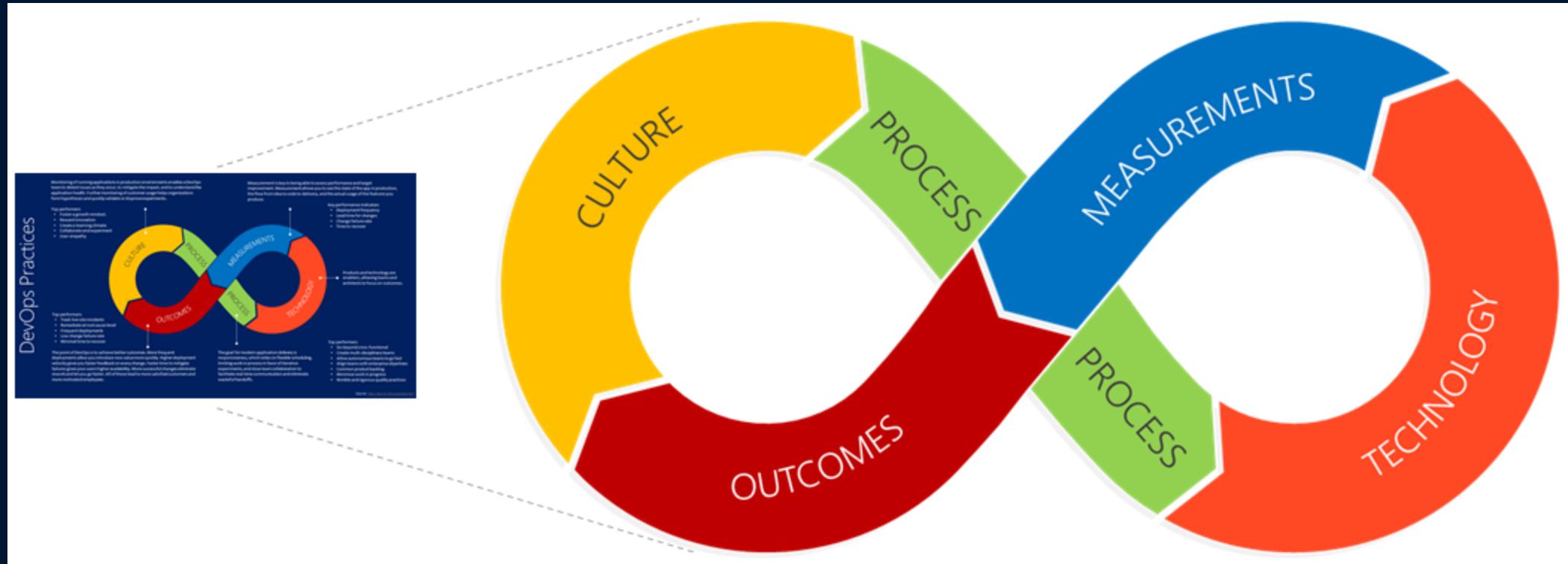
Blueprint description

Configures a virtual network with a subnet and an NSG.

Definition location * ⓘ

MSDN Platforms Subscription ✓ ...

The Definition Location is the place in the management group hierarchy where this blueprint definition will be stored. Once the definition is created, a blueprint assignment can be created at or below this location in the management group hierarchy. Management groups are groups that can contain subscriptions, or other management groups. You can learn more at: aka.ms/BlueLocation



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

Summary

Chapter 7:

AI Privacy & Ethical Considerations

Data Privacy and Responsible AI Best Practices

- Discovering and protecting sensitive data
- Introducing differential privacy
- Mitigating fairness
- Working with model interpretability
- Exploring FL and secure multi-party computation

Lab 9

Discovering and protecting sensitive data

- **Personally identifiable information (PII)**: Information that can be used to identify an individual, such as full name, date of birth, social security number, driver's license number, passport number
- **Financial information**: Credit card numbers, bank account details, financial transaction records, and so on
- **Health information**: Medical records, health insurance information, mental health records, and other health-related data
- **Passwords and authentication data**: Usernames, passwords, security questions, or any other credentials used to access systems or accounts
- **Biometric data**: Fingerprints, retinal scans, facial recognition data, and other biometric identifiers
- **Confidential business information**: Trade secrets, intellectual property (IP), financial reports, customer lists, proprietary algorithms, and so on
- **Government classified information**: Information classified by governments for national security reasons
- **Personal communications**: Private messages, emails, and other communications that individuals expect to be confidential
- **Social and demographic information**: Race, ethnicity, religion, sexual orientation, and other sensitive demographic data
- **Geolocation data**: Precise location data of individuals or assets

Data Anonymization

- Removing direct identifiers
- Pseudonymization
- Data masking / Tokenization
- Generalization / Aggregation

Differential Privacy



Chapter 8: What's Next?

Preparing for Future AI Security Challenges:
Managing and Securing Access

Experience is

Lesson Agenda: What We Will Cover

- Working with the PoLP
- Authenticating with Microsoft Entra ID
- Implementing RBAC
- Authenticating with application identities
- Enhancing access security

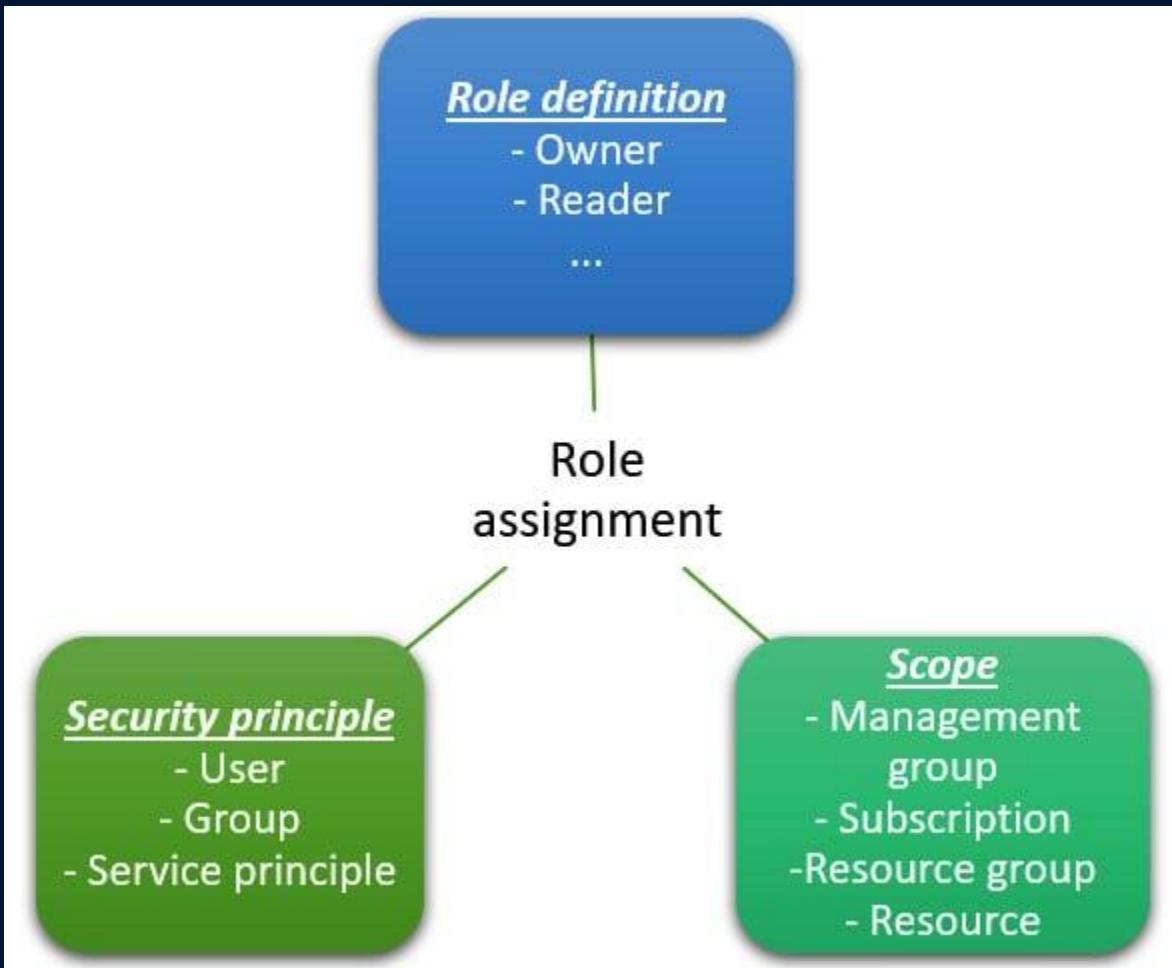
PoLP

- Application Inventory
- RBAC
- Regular reviews
- Automated tools
- Zero Trust Architecture
- Continuous Monitoring
- Training!

Microsoft Entra ID

- Previously Azure Active Directory (Azure AD)

RBAC



Built in Roles

Check access Role assignments **Roles** Deny assignments Classic administrators

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles.

Search by role name, description, or ID Type : All Category : All

<input type="checkbox"/> Name ↑↓	Description ↑↓
<input type="checkbox"/> Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
<input type="checkbox"/> Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC.
<input type="checkbox"/> Reader	View all res

+ Add Download role assignments Edit columns Refresh Remove Feedback



Check access Role assignments **Roles** Deny assignments Classic administrators

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

AzureML Type : All Category : All

Showing 4 of 465 roles

<input type="checkbox"/> Name ↑↓	Description ↑↓
<input type="checkbox"/> AzureML Compute Operator	Can access and perform CRUD operations on Machine Learning Services managed comput.

Add a Role Assignment

The screenshot shows the Microsoft Azure Access control (IAM) blade for the "MSDN Platforms Subscription". The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Security, Events, and Cost Management. The main area has tabs for Check access, Role assignments, Roles, and Deny assignments, with "Check access" being the active tab. Under "My access", there is a "View my access" button. Below it, under "Check access", there is a "Check access" button.

Lab 11, 12

Create a Service Principle

- In order to authenticate when working with applications or scripts that train and test a model, for example, you can use service principal authentication. To achieve this, we need to create a service principal in the Microsoft Entra ID workspace. If you are creating a service principal, you need to create an application registration.

```
georgia [ ~ ]$ az ad sp create-for-rbac --sdk-auth --name azuremldataScientist --role Reader --scopes /subscriptions/
Option '--sdk-auth' has been deprecated and will be removed in a future release.
Creating 'Reader' role assignment under scope '/subscriptions/
The output includes credentials that you must protect. Be sure that you do not include these credentials in your code
{
  "clientId": "[REDACTED]",
  "clientSecret": "[REDACTED]",
  "subscriptionId": "[REDACTED]",
  "tenantId": "[REDACTED]",
  "activeDirectoryEndpointUrl": "https://login.microsoftonline.com",
  "resourceManagerEndpointUrl": "https://management.azure.com/",
  "activeDirectoryGraphResourceId": "https://graph.windows.net/",
  "sqlManagementEndpointUrl": "https://management.core.windows.net:8443/",
  "galleryEndpointUrl": "https://gallery.azure.com/",
  "managementEndpointUrl": "https://management.core.windows.net/"
}
```


Managed Identities

Home > GeneralVM > CodestoriesLab

CodestoriesLab | Identity

Virtual machine

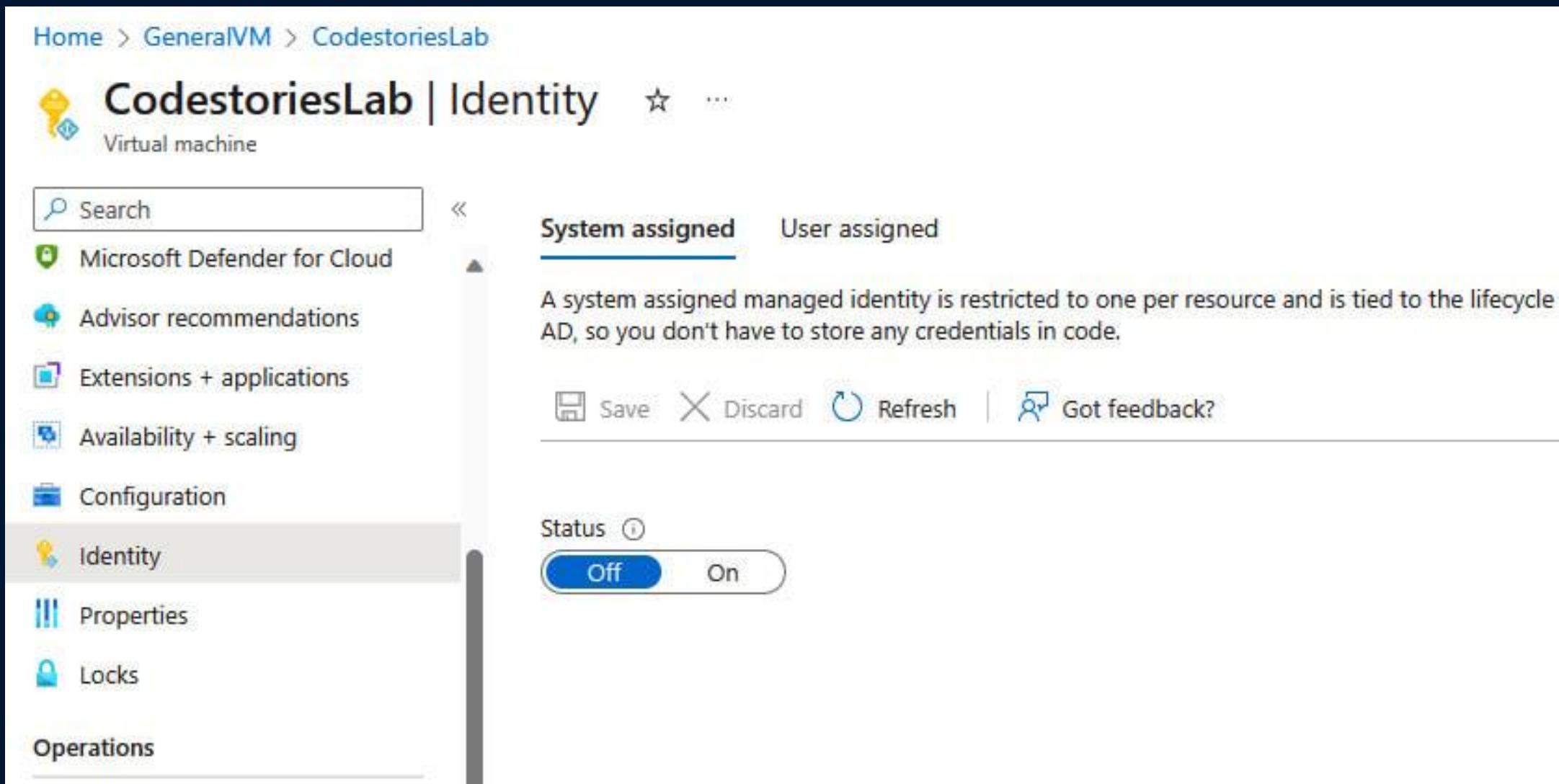
Search Microsoft Defender for Cloud Advisor recommendations Extensions + applications Availability + scaling Configuration Identity Properties Locks Operations

System assigned User assigned

A system assigned managed identity is restricted to one per resource and is tied to the lifecycle AD, so you don't have to store any credentials in code.

Save Discard Refresh Got feedback?

Status Off On



Conditional Access

- Requiring for multi-factor authentication (MFA) to be enabled for users with highly privileged roles or from unrecognized locations
- Blocking users that are flagged by the system as high risk
- Allowing or blocking access from specific IPs or countries
- Requiring a password change to allow access

Summary

Chapter 9:

Managing Your Cloud Workspace

Azure ML Workspace

Experience is

Lesson Agenda: What We Will Cover

- Exploring network security
- Working with Azure Machine Learning compute
- Managing container registries and containers

ML Network Security



Secure the ML Workspace

AzureML | Networking ⭐ ...

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Events

Settings

Networking

Public access Private endpoint connections Workspace managed outbound access

Save Discard changes Refresh

Public network access

Disabled

All networks

Public access Private endpoint connections Workspace managed outbound access

+ Private endpoint ✓ Approve ✘ Reject ━ Remove Refresh

Filter by name... All connection states

This screenshot shows the 'Networking' settings for an Azure Machine Learning workspace. The 'Public access' tab is active, indicating that public network access is disabled. The 'Private endpoint connections' tab is also visible. A 'Discard changes' button is present. The left sidebar shows other workspace settings like Overview, Activity log, and Access control (IAM). The 'Networking' tab is highlighted.

Securing Associated Resources

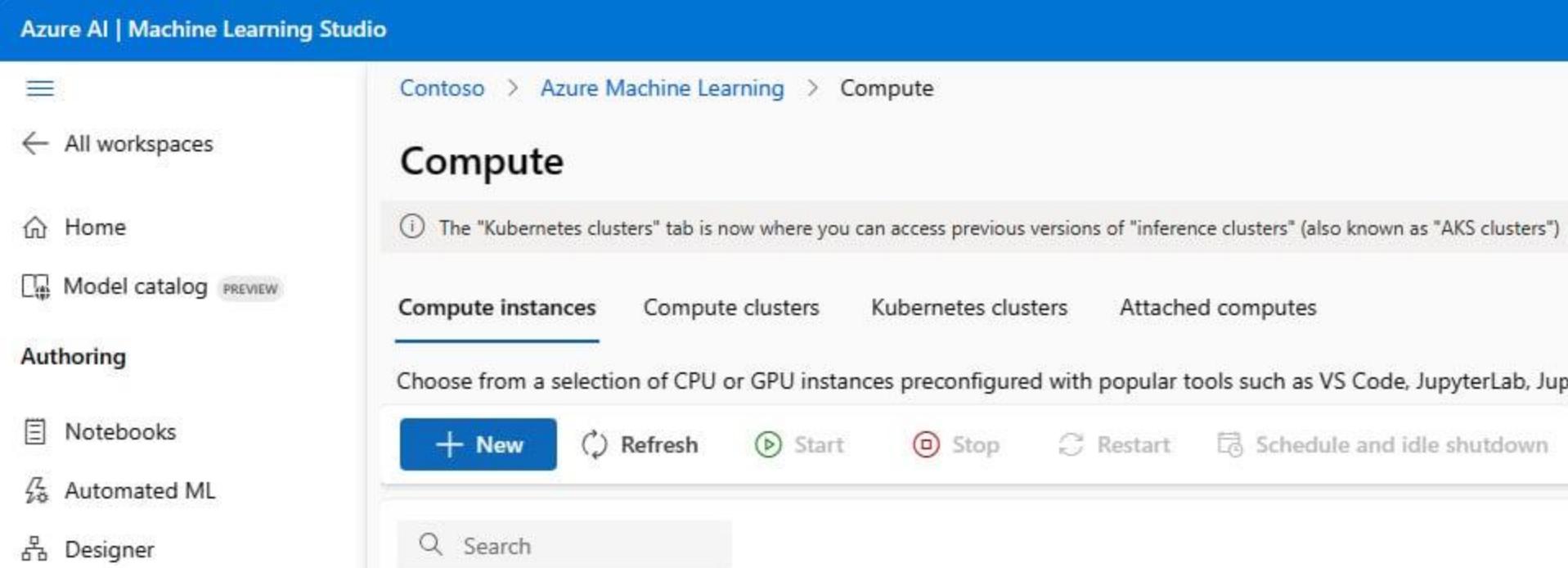
The screenshot shows the Azure Storage account 'azureml' settings page under the 'Networking' tab. The left sidebar lists 'Storage account', 'Data migration', 'Events', 'Storage browser', and 'Storage Mover'. Under 'Data storage', there are links for 'Containers', 'File shares', 'Queues', and 'Tables'. Under 'Security + networking', 'Networking' is selected, while 'Front Door and CDN' and 'Access keys' are also listed. The main content area has tabs for 'Firewalls and virtual networks' (selected), 'Private endpoint connections', and 'Custom domain'. Below these are buttons for 'Save', 'Discard', 'Refresh', and 'Give feedback'. A note states: 'Firewall settings restricting access to storage services will remain in effect for up to a minute after saving updated settings allow'. The 'Public network access' section shows three options: 'Enabled from all networks' (radio button), 'Enabled from selected virtual networks and IP addresses' (radio button, selected), and 'Disabled'. A link to 'Configure network security for your storage accounts' is provided. The 'Virtual networks' section includes 'Add existing virtual network' and 'Add new virtual network' buttons. A table lists one virtual network: 'AzureMLVNet' with one subnet and an address range. The 'Endpoint Status' column shows a green 'OK' status.

Virtual Network	Subnet	Address range	Endpoint Status
> AzureMLVNet	1		OK

Validate Access



Working with Azure ML Compute



The screenshot shows the Azure AI | Machine Learning Studio interface. The top navigation bar includes 'Contoso > Azure Machine Learning > Compute'. The left sidebar has a 'Compute' section with 'Compute instances' selected, along with other options like 'Compute clusters', 'Kubernetes clusters', and 'Attached computes'. Below this, there's a note: 'The "Kubernetes clusters" tab is now where you can access previous versions of "inference clusters" (also known as "AKS clusters")'. A 'Compute instances' table is shown with columns for 'Name', 'Type', 'Status', and 'Actions'. The first row is a 'New instance' entry. At the bottom of the table are buttons for '+ New', 'Refresh', 'Start', 'Stop', 'Restart', and 'Schedule and idle shutdown'. A search bar is also present at the bottom.

Secure Compute Instances

Create compute instance

1 Scheduling optional
2 Security optional
3 Applications optional
4 Tags optional
5 Review

Security
Configure security settings such as SSH, virtual network, root access, and managed identity for your compute instance.

User assignment
 Assign to another user (i)

Assigned identity
 Assign a managed identity (i)

Identity type
 System-assigned User-assigned

SSH
 Enable SSH access (i)

Virtual network
 Enable virtual network (i)

(i) Your workspace is linked to a virtual network using a private endpoint connection. In order to communicate properly with the workspace,

Virtual network *
AzureMLVNet (ML)

Subnet *
default
 No public IP (i)

Secure Compute Clusters

Compute

The "Kubernetes clusters" tab is now where you can access previous versions of "inference clusters" (also known as "compute clusters").

Compute instances **Compute clusters** Kubernetes clusters Attached computers

Create a single or multi node compute cluster for your training, batch, or inference needs.

+ New Refresh Delete View options

Create compute cluster

Virtual Machine Advanced Settings

Maximum number of nodes *

Idle seconds before scale down *

Enable SSH access

Advanced settings

Enable virtual network

Virtual network *

Refresh virtual networks

Subnet *

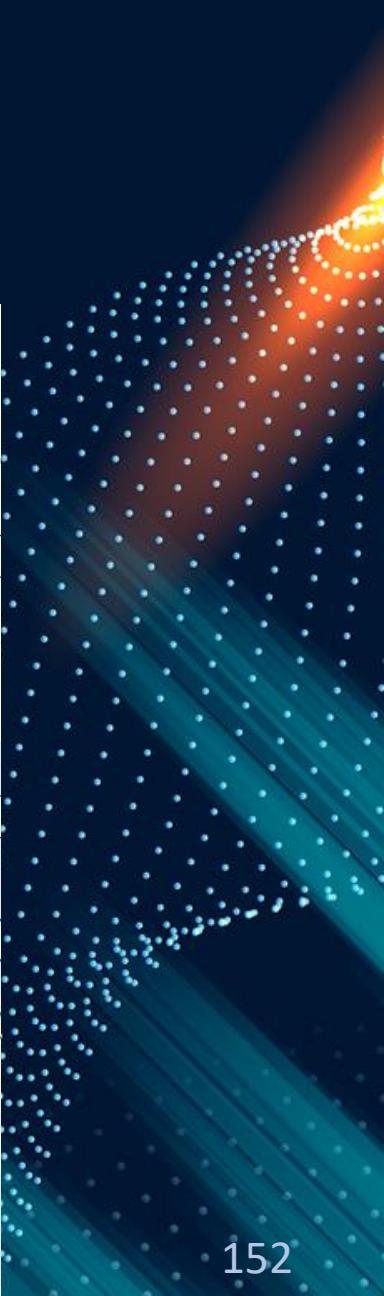
No public IP

SharedAccessKeyDisallowed: Azure Storage AD authorization for requests to Blob and Queue storage only. Please allow Shared Key access for requests to Azure Files or

Assign a managed identity

Identity type

System-assigned User-assigned



Copyright © Microsoft Corporation. All rights reserved.

Securing with Container Registry

Home > Container registries >

 **azureml** | Properties ☆ ...

<< Save Discard

Encryption azurecr.io

Identity

Networking

Microsoft Defender for Cloud

Properties Admin user

Locks Pricing plan Premium

Services

Repositories When turned on, soft delete provides save and recovery for your images, tags, and other deletion from your registry. If you have items you've already deleted that you want to items before the purge day arrives. [Learn more](#)

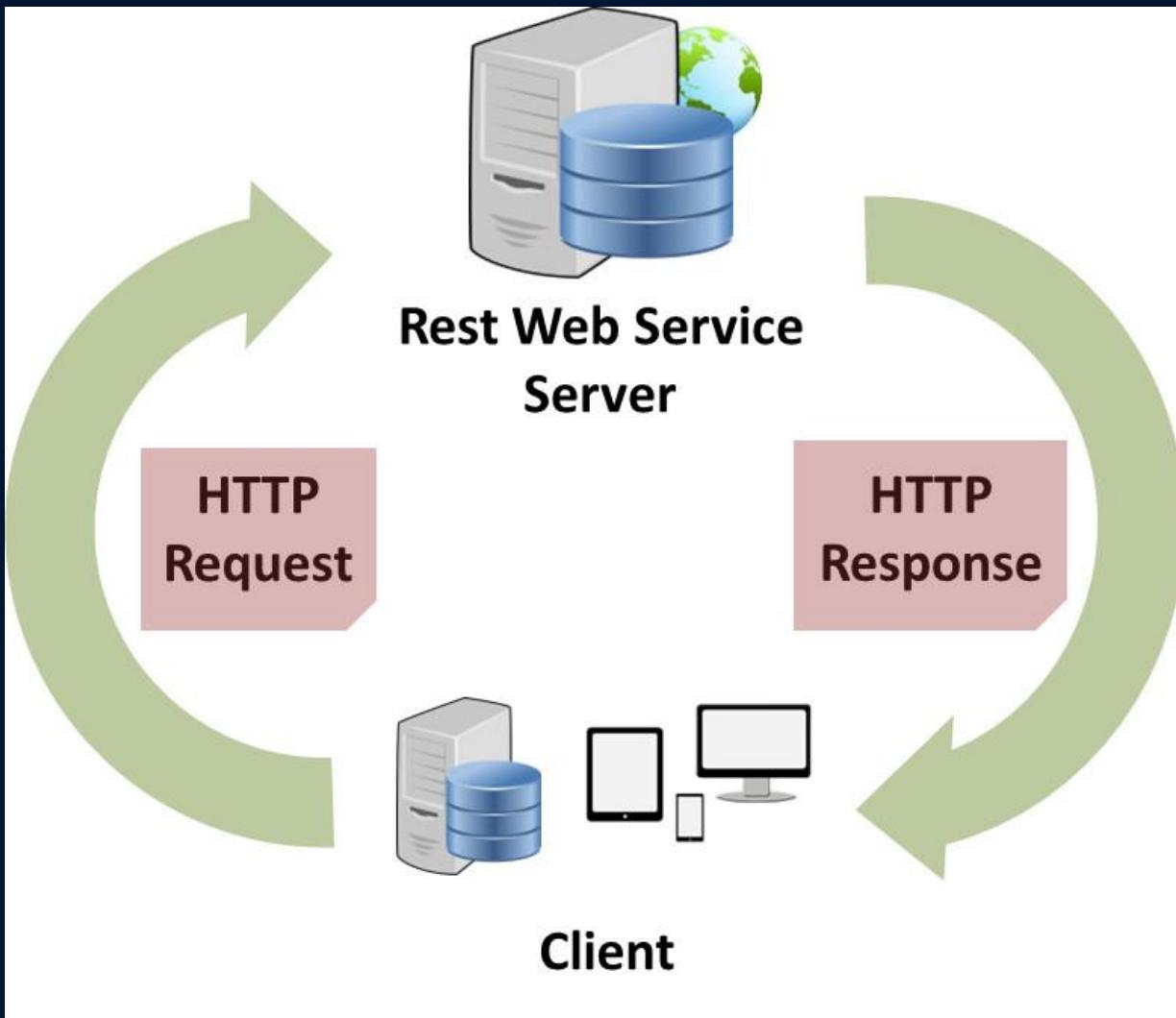
Webhooks

Geo-replications

Soft delete

Retention days before purge * 7

ML Endpoints



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

ML Endpoints

Chapter 10:

MLOps

Azure MLFlow

Experience is

Lesson Agenda: What We Will Cover

- Working with MLOps in Azure Machine Learning
- Leveraging IaC
- Implementing CI/CD
- Exploring event-driven workflows in Azure

MLOps

- Collaboration
- Versioning
- Model Validation
- CI/CD
- Monitoring and Logging
- Scalability
- Reproducibility
- Automation

IaC

- ARM
- Bicep
- CLI
- Blueprints
- Terraform

IaC with Azure ML

- Infrastructure
- Datastores / Datasets
- Model Deployment
- Automation and Orchestration

CI/CD with ML

- Training the model
- Logging metrics
- Retrieving the registered model
- Packaging and deploying the model

Azure DevOps

- Azure Boards: This provides work tracking with Kanban boards, backlogs, team dashboards, and custom reporting. It allows teams to plan, track, and discuss work across the entire development life cycle.
- Azure Repos: This is a version control system that provides Git repositories for source control. It supports pull requests, branching, and searching.
- Azure Pipelines: This is a CI/CD platform for deploying and testing applications to different platforms both for cloud and on-premises offerings.
- Azure Test Plans: This is a platform that includes multiple testing tools for different scenarios such as exploratory or continuous testing.
- Azure Artifacts: This allows collaboration between teams to share packages from private or public repositories such as NuGet or Maven into their pipelines.

Free Azure DevOps

<https://learn.microsoft.com/en-us/azure/devops/user-guide/sign-up-invite-teammates?view=azure-devops>

Event Grid

- Azure Event Grid is a fully managed event routing service.
- It enables you to easily build applications that react to changes or events happening within Azure services or even on-premises.

Event Handlers

TOPIC DETAILS

Pick a topic resource for which events should be pushed to your destination. [Learn more](#)

Topic Types

Subscription *

Resource Group *

Resource *

Azure Function

Web Hook

Storage Queues

Event Hubs

Hybrid Connections

Service Bus Queue

Service Bus Topic

Partner Destination

EVENT TYPES

Pick which event types get pushed to your dest

Filter to Event Types *

ENDPOINT DETAILS

Pick an event handler to receive your events. Le

Endpoint Type *

Summary

Chapter 11:

Monitoring

Azure Monitoring, Logging, Threat Detection

Experience is

Lesson Agenda: What We Will Cover

- Enabling logging and configuring data retention for Azure services
- Securing resources with Microsoft Defender
- Exploring threat management with Sentinel

«

 The Log Analytics agents, used by VM Insights, won't be supported as of August 31, 2024. Plan to migrate to VM Insights on Azure Monitor agent prior to this date. →

[Overview](#) [Tutorials](#)

Insights

Use curated monitoring views for specific Azure resources. [View all insights](#)

Application insights

Monitor your app's availability, performance, errors, and usage.

[View](#) [More](#)

Container Insights

Gain visibility into the performance and health of your controllers, nodes, and containers.

[View](#) [More](#)

VM Insights

Monitor the health, performance, and dependencies of your VMs and VM scale sets.

[View](#) [More](#)

Network Insights

View the health and metrics for all deployed network resources.

[View](#) [More](#)

Detection, triage, and diagnosis

Visualize, analyze, and respond to monitoring data and events. [Learn more about monitoring](#) ↗

Metrics

Create charts to monitor and investigate the usage and performance of your Azure resources.

[View](#) [More](#)

Alerts

Get notified and respond using alerts and actions.

[View](#) [More](#)

Logs

Analyze and diagnose issues with log queries.

[View](#) [More](#)

Workbooks

View, create and share interactive reports.

[View](#) [More](#)

Change Analysis

Investigate what changed to triage

Diagnostic Settings

Route monitoring metrics and logs to

Azure Monitor SCOM managed instance

SCOM management instance

Managed Prometheus

Collect Prometheus metrics from your



Metrics

Azure Monitoring

...

X

+ New chart ⏪ Refresh ⏪ Share ⏪ Feedback ⏪

UTC Time: Last 24 hours (Automatic - 5 minutes)

Memory Usage

>Add metric Add filter Apply splitting

Line chart ⏪ Drill into Logs ⏪ New alert rule Save to dashboard ⏪ ...

gkcache, Used Memory, Max



Used Memory (Max)
gkcache

476 kB

Home >

Log Analytics workspaces



...

Create

Open recycle bin

Manage view

Refresh

Export to CSV

Open query

Assign tags

Filter for any field...

Subscription equals all

Resource group equals all

Location equals all

Add filter

Showing 1 to 5 of 5 records.

Name ↑↓

Resource group ↑↓

Diagnostic setting

...

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name *

Allsettings



Logs

Category groups ⓘ

allLogs

audit

Categories

AmIComputeClusterEvent

AmIComputeClusterNodeEvent

AmIComputeJobEvent

AmIComputeCpuGpuUtilization

AmIRunStatusChangedEvent

ModelsChangeEvent

ModelsReadEvent

ModelsActionEvent

Destination details

Send to Log Analytics workspace

Subscription

Log Analytics workspace

AzureMLAnalytics (westeurope)

Archive to a storage account

Stream to an event hub

Send to partner solution

Monitor | Alerts

Microsoft



Search



View as timeline (preview)



Create



Alert rules



Action groups



Alert processing rules

Overview

Activity log

Alerts

Metrics

Logs

Change Analysis

Service health

Workbooks

Insights

Applications



Search

Subscription :

Time range : Past 24 hours

Total alerts



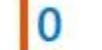
0

Critical



0

Error



0

Warning



0

Informational



0

Verbose



0

Name ↑↓

Severity ↑↓

Affected resource ↑↓

Action Groups

Home > Monitor | Alerts >

Create action group

...

Basics Notifications Actions Tags Review + create

An action group invokes a defined set of notifications and actions when an alert is triggered. [Learn more](#)

Project details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription ⓘ



Resource group * ⓘ

(New) Alerts

Create new

Region *

Global

Instance details

Action group name * ⓘ

Email Administrators

Display name * ⓘ

EmailAdmins

The display name is limited to 12 characters

Managing Alerts

Home > Monitor

Monitor | Alerts

Microsoft

Search View as timeline (preview) Create Alert rules Action groups Alert processing rules ...

New: View alerts visualized on a timeline for a clearer picture of your events. You can switch between views anytime. [View as timeline \(preview\)](#)

Overview Activity log Alerts Metrics Logs Change Analysis Service health Workbooks

Search Subscription : Time range : Past 24 hours Alert condition : all Severity : all Add filter Less

Total alerts Critical Error Warning Informational Verbose

No grouping

Name ↑↓	Severity ↑↓	Affected resource ↑↓	Alert condition ↑↓	User response ↑↓	1
Azure ML Administrative ...	4 - Verbose	azureml	Fired	New	1... ⏮
Azure ML Administrative ...	4 - Verbose	azureml:	Fired	New	1... ⏮
Azure ML Administrative ...	4 - Verbose	delete (azureml) /...	Fired	New	1... ⏮
Azure ML Administrative ...	4 - Verbose	azureml	Fired	New	1... ⏮
Azure ML Administrative ...	4 - Verbose	delete (azureml) /...	Fired	Acknowledged	1... ⏮

Application Insights

Deploy a model

Select entry script file [Browse](#)

Conda dependencies file * [i](#)

Select conda dependencies file * [Browse](#)

Dependencies

[Add File](#)

[▼ Advanced](#)

Enable Application Insights diagnostics and data collection [i](#)

Enable Application Insights diagnostics and data collection

Scoring timeout [i](#)

Auto scale enabled [i](#)

Auto scale enabled

Min replicas [i](#)

Search

Subscriptions

What's new

General

Overview

Getting started

Recommendations

Attack path analysis

Security alerts

Inventory

Cloud Security Explorer

Workbooks

Community

Diagnose and solve problems

Cloud Security

Security posture

Regulatory compliance

Workload protections

Data security (Preview)

Firewall Manager

DevOps security (preview)

Management

Environment settings

Security solutions

Workflow automation

1

Azure subscriptions

96

Assessed resources

20

Active recommendations

--

Attack paths

--

Security alerts



Security posture

20/20

Unassigned recommendation

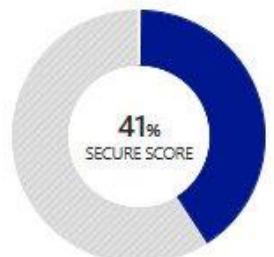
0/0

Overdue recommendations

0

Attack paths

Secure score



[Explore your security posture >](#)



Regulatory compliance

Microsoft cloud security benchmark

34 of 63 passed controls

Lowest compliance regulatory standards by passed controls



No additional standards are currently monitored.

[Open policy settings to manage additional compliance policies](#)

[Improve your compliance >](#)



Workload protections

Resource coverage

100% For full protection, enable 1 resource plans



Inventory

Unmonitored VMs

3

To better protect your organization, we recommend installing agents

Security posture



Secure score over time Governance report Guides & Feedback

Azure environment

Azure

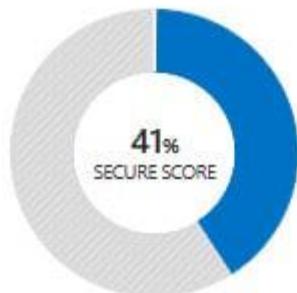
AWS

GCP

Azure DevOps



Secure score



Environment



1 Management groups



1 Subscriptions



28/46 Unhealthy resources



59 Recommendations

Governance



Assign ownership and drive recommendations remediation using governance. To create your first rule, [click here](#).

Environment Owner

Search by name

Environment == All

Group by environment

Name ↑↓

Secure score ↑↓

Unhealthy resour... ↑↓

Attack paths ↑↓

Recommendations



Azure subscription



41%

28 of 46

0

[View recommendations...](#)

Home >

Microsoft Sentinel



...

[+ Create](#)

[Manage view](#) ▾

[Refresh](#)

[Export to CSV](#)

[Open query](#)

[View incidents](#)

[Filter for any field...](#)

Subscription equals **all**

Resource group equals **all**

Location equals **all**

[+ Add filter](#)

Showing 1 to 1 of 1 records.

[Name ↑](#)

[Resource group ↑](#)

[Location ↑](#)

[MyWorkspace](#)

[logs](#)

[West Europe](#)

Summary

Chapter 12:

Baseline

Secure Baseline

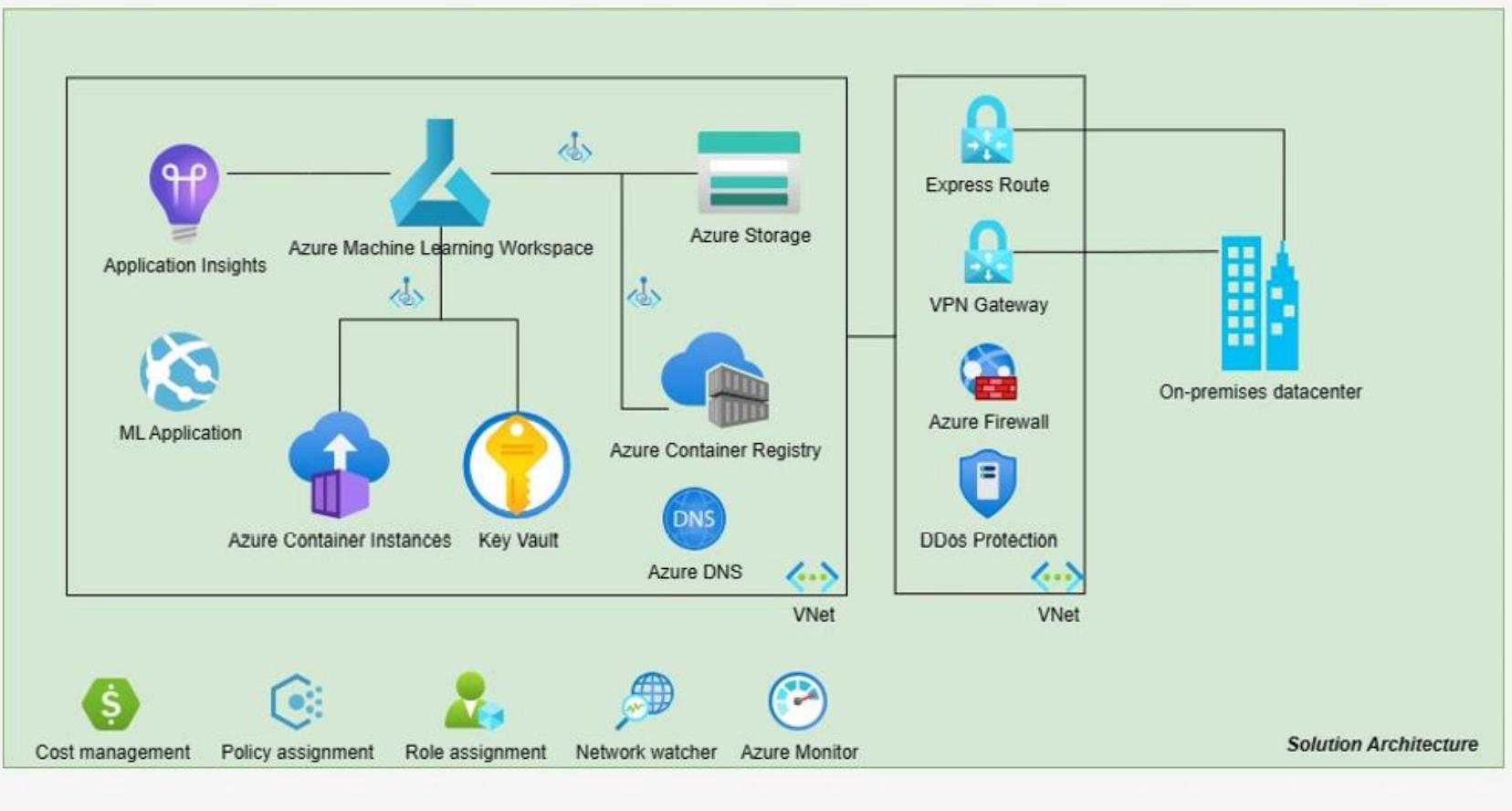
Experience is

Lesson Agenda: What We Will Cover

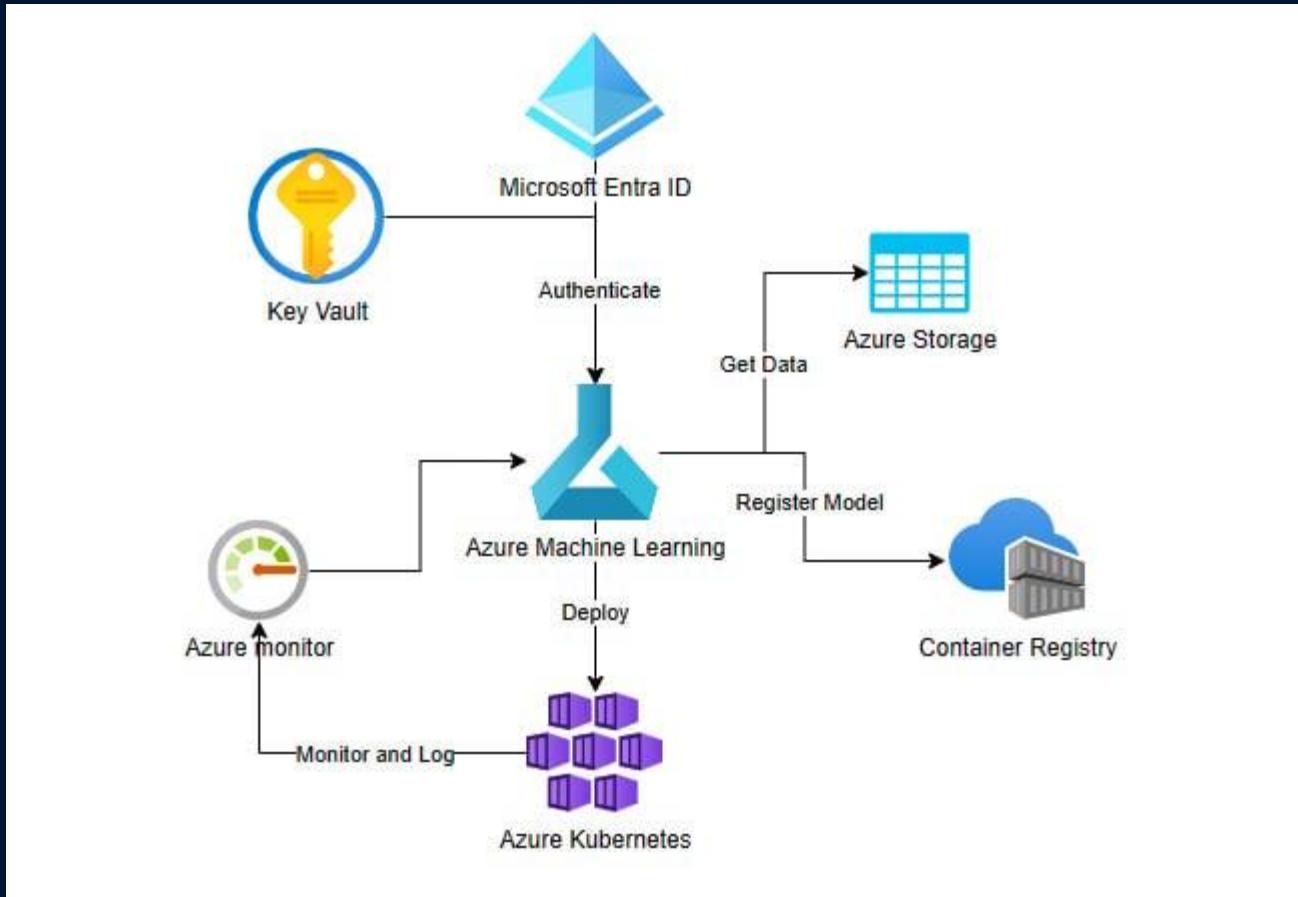
- Setting a baseline for Azure Machine Learning
- Threat modeling for Azure Machine Learning
- Reviewing the shared responsibility model for cloud security

Discover Services for Added Security

- NSG
- VPN Gateways
- ExpressRoute
- Azure Firewall
- VWAN
- WAF
- DDoS
- Azure Front Door
- Defender
- Azure Site Recovery







MICROSOFT THREAT MODELING TOOL



Version: 7.3.31026.3

Threat Model:

Create A Model

Model your system by drawing diagram(s). Make sure you capture important details.

Open A Model

Open an existing model file and analyze threats against your system.

Getting Started Guide

A step-by-step guide to help you get up and running now.

Template For New Models

Azure Threat Model Template(1.0.0.33) [Browse...](#)

Recently Opened Models

[Sample Threat Model.tm7](#)

Threat Modeling Workflow

1. Select your template.
2. Create your data flow diagram model.
3. Analyze the model for potential threats.
4. Determine mitigations.

Template:

Create New Template

Define stencils, threat types and custom threat properties for your threat model from scratch.

Open Template

Open an existing Template and make modifications to better suit your specific threat analysis.

Template Workflow

Use templates to define threats that applications should look for.

1. Define stencils
2. Define categories
3. Define threat properties
4. Define threat
5. Share your template

Responsibility	SaaS	PaaS	IaaS	On-Premises
Information and data	Customer	Customer	Customer	Customer
Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
Accounts and identities	Customer	Customer	Customer	Customer
Identity and directory infrastructure	Shared	Shared	Shared	Customer
Applications	Provider	Shared	Shared	Customer
Network controls	Provider	Shared	Shared	Customer
Operating system	Provider	Provider	Shared	Customer
Physical hosts	Provider	Provider	Provider	Customer
Physical network	Provider	Provider	Provider	Customer
Physical datacenter	Provider	Provider	Provider	Customer

Summary

Thanks again for joining us!

- We truly appreciate your time. Please complete the End of Course Survey.
- Any questions?
 - Review the full Course Guide for Course Tips, Resources & Next Step Learning Plans
 - Feel Free to Reach Out: Info@triveratech.com / Dr.Lee@triveratech.com
 - See full list of AI, Python, Coding, Security & Full Stack Courses & SkillJourneys: www.triveratech.com
- Free Courses, Articles, Resources & Offers



Let's Connect! Follow Us for Free Courses, Articles, Resources & Offers:
LinkedIn: @TriveraTech



Subscribe to our Channel for Free Courses & Events
YouTube: @TriveraTech