Becoming the Trainer: Attacking ML Training Infrastructure

TROOPERS

Brett Hawkins (@h4wkst3r)

Adversary Services, IBM X-Force Red

IBM

Blog Post and Tool

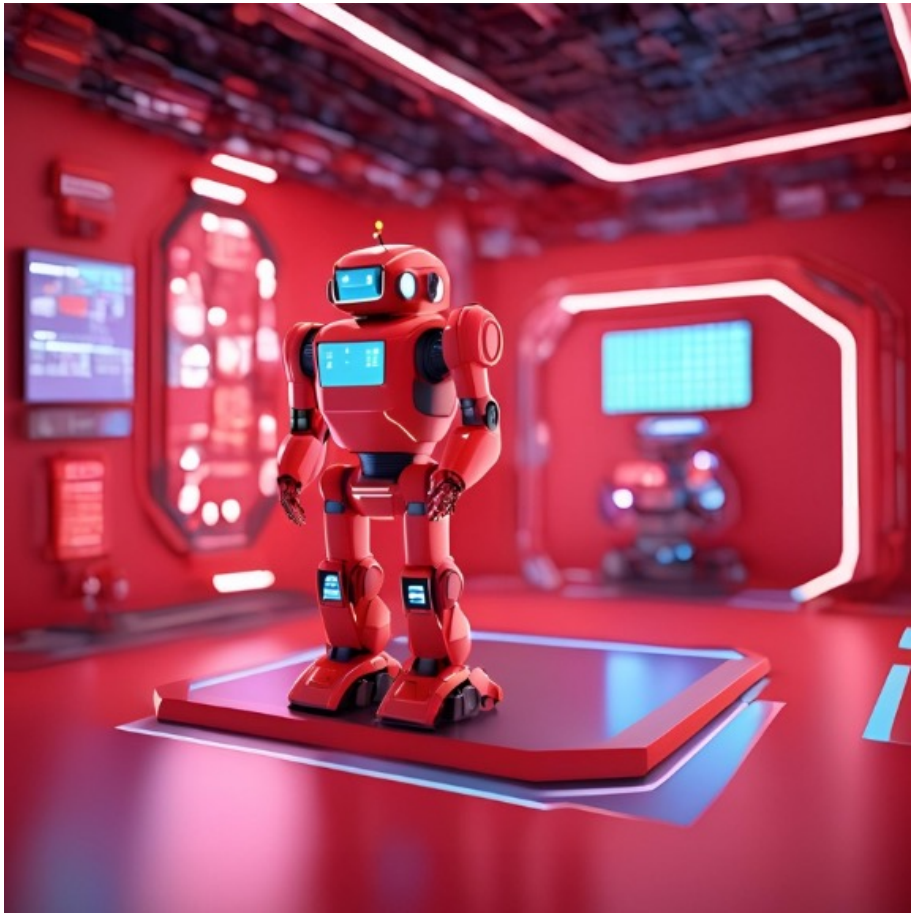
Blog Post

MLOKit

Agenda

1. Introduction
2. Background
3. Attacking ML Training Environments
   - Attack Scenarios
   - Demos
4. Protecting ML Training Environments
5. Conclusion
6. Q&A

Introduction



Who am I – Brett Hawkins

https://h4wkst3r.github.io

Current Role
Team Lead, Adversary Services
IBM X-Force Red

Open-Source Tool Author
SharPersist, InvisibilityCloak, SCMKit, ADOKit, MLOKit

Conference Speaker
Black Hat (US & EU), BlueHat, ShmooCon, DerbyCon, Wild West Hackin' Fest, BSides, Hackers Teaching Hackers

Research Drivers

Threat actors targeting AI/ML environments

Lack of research on attacking and defending ML infrastructure

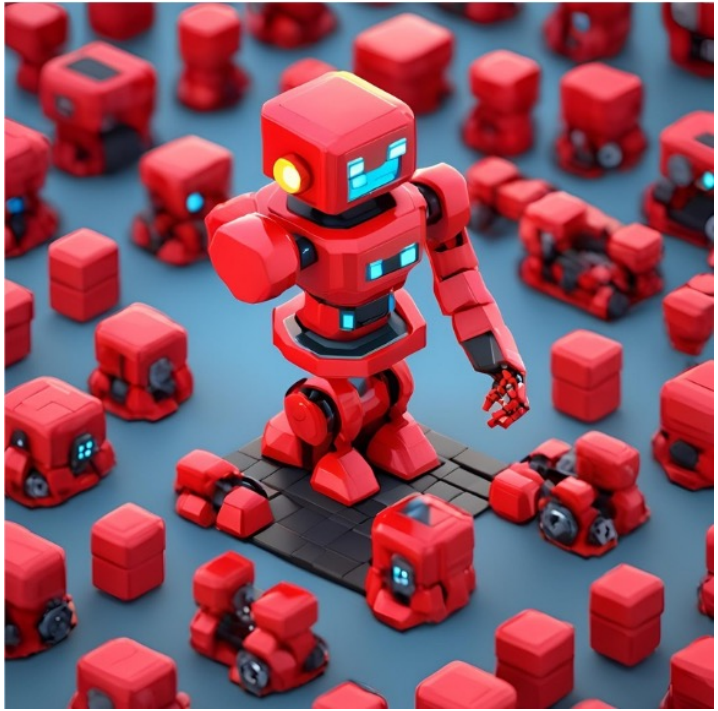
Adoption of ML technologies by enterprises

Lack of tooling to simulate attacks against platforms used in ML training envs

Threat Actor Motivation

Theft of models and weights, backdooring models for initial access or persistence, expanding access via lateral movement and privesc, sensitive data theft or deploying ransomware, model modification/poisoning for misclassification, degradation, fraud or ml-based detection evasion.

Attendee Takeaways



How to steal models from model registries

How to poison models within ML training platforms

How to defend key components of ML training infrastructure

How to get code execution via attacks on ML training infrastructure

What is new in this research?

```
[*] INFO: Listing Model Artifact Location Info:

Account Name: testworkspace5178193999

Datastore Type: AzureBlob

Container Name: azureml

Path: ExperimentRun/dcid.AutoML_91114fd1-6657-4bf0-b51d-6f868e2c2033_42/outputs/mlflow-m

[*] INFO: Getting associated datastore for model artifacts:

                  Account Name |                                    Container Name |  D
-------------------------------------------------------------------------------------
       testworkspace5178193999 |                                           azureml |

[*] INFO: Uploading model artifacts

[*] INFO: Uploading: conda.yaml

[*] INFO: Uploading: MLmodel

[*] INFO: Uploading: model.pkl

[*] INFO: Uploading: python_env.yaml

[*] INFO: Uploading: requirements.txt

[+] SUCCESS: Model has been poisoned with model artifacts specified in source directory
```

Advanced attacks against ML training environments

New detection rules (Azure ML and SageMaker)

MLOKit tool updates – NEW supported platforms and attacks

My Perspective

I am

Offensive Cybersecurity Specialist

I am not

Data Scientist

AI/ML Engineer

Cloud Engineer

Detection Engineer

DevOps Engineer

Software Engineer

Background

Prior Work

Links to prior work are provided in appendix slides

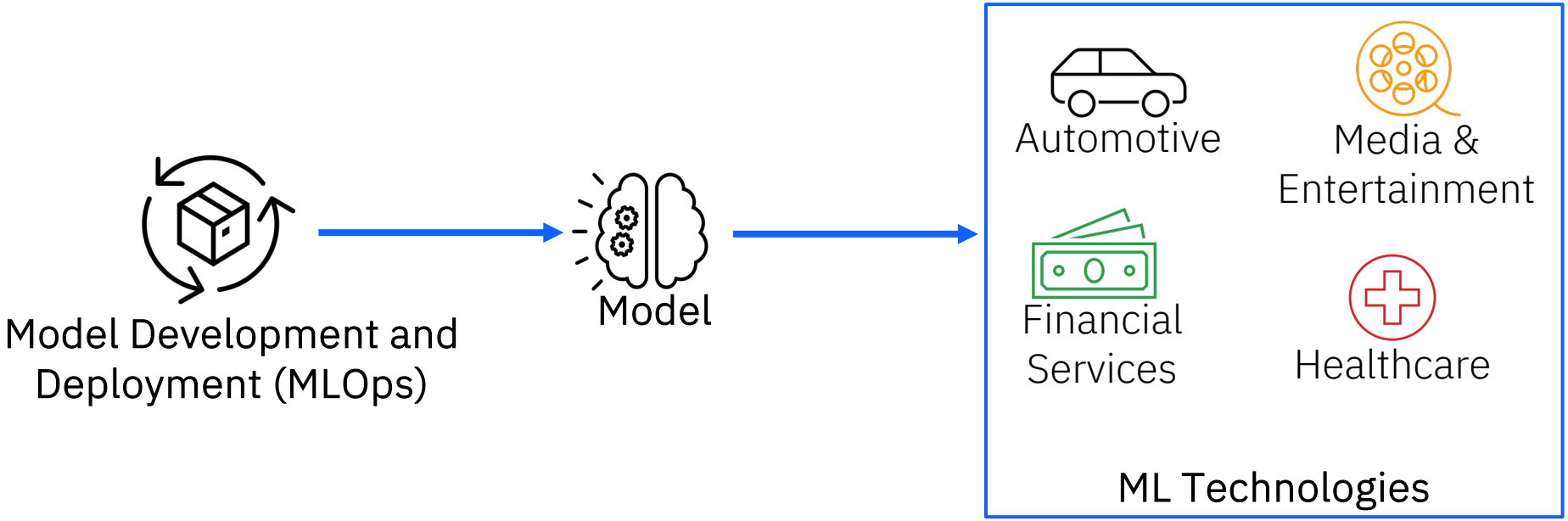
Chris Thompson (@retBandit) & I – ShmooCon 2025

Disrupting the Model: Abusing MLOps Platforms to Compromise ML Models and Enterprise Data Lakes

Or Azarzar (@azarzaror) – Blog Post (2021)

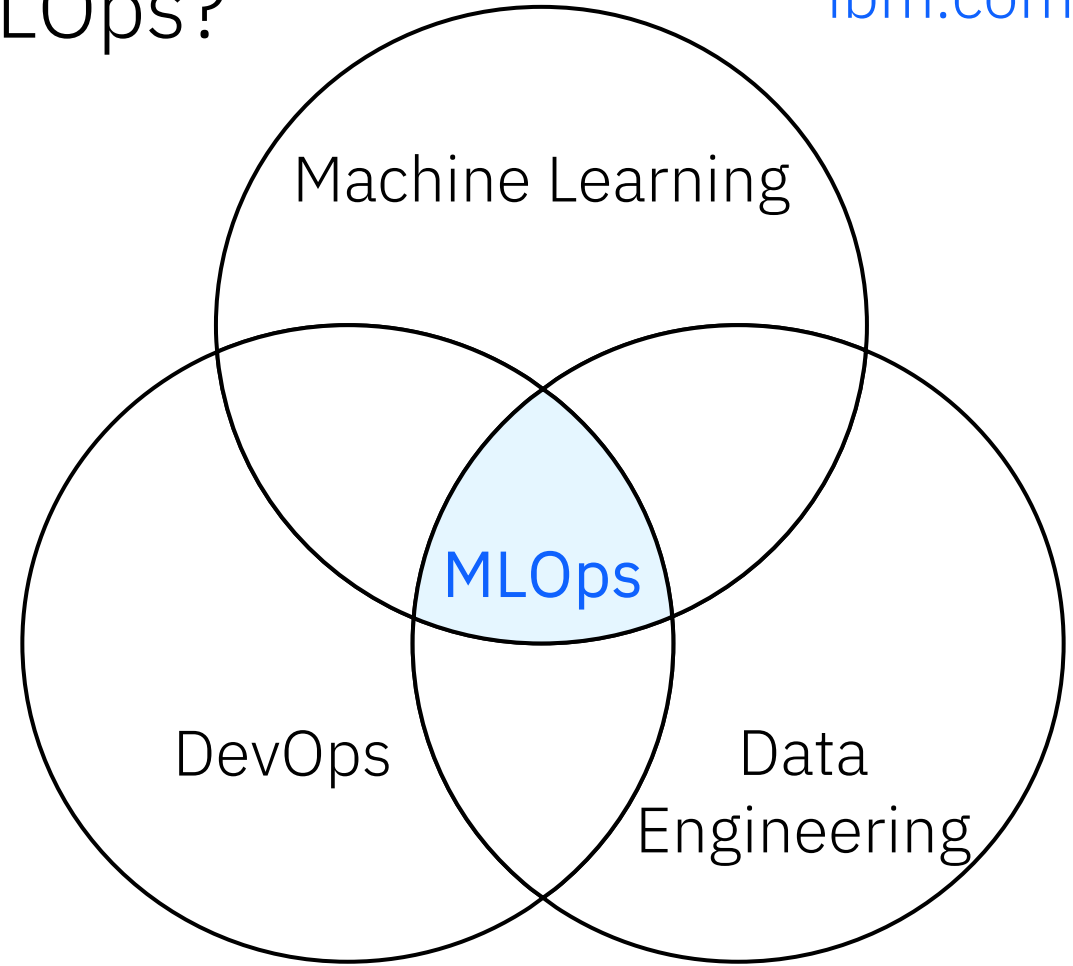
Protect Your Environment When Working with Amazon SageMaker

ML Technology Use Cases

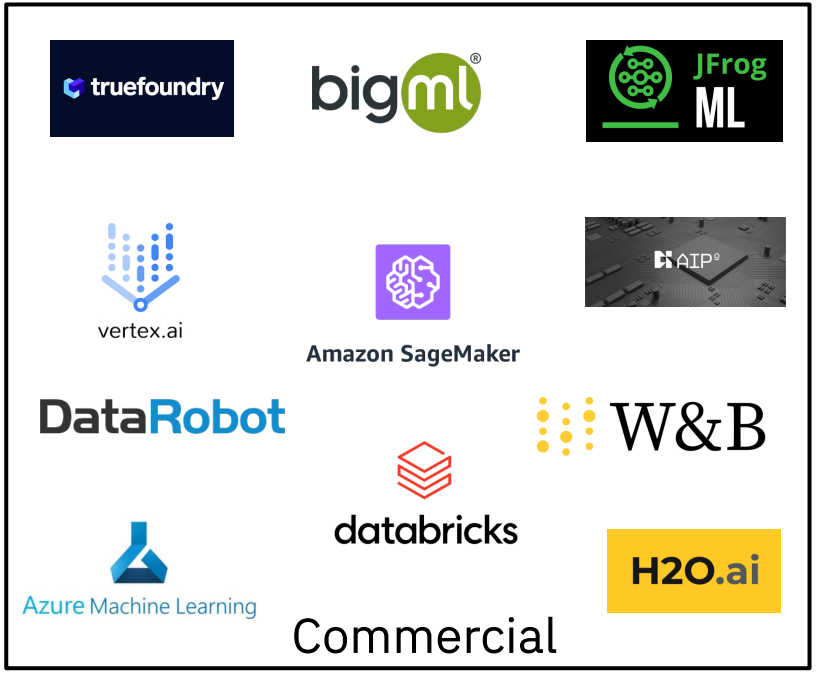


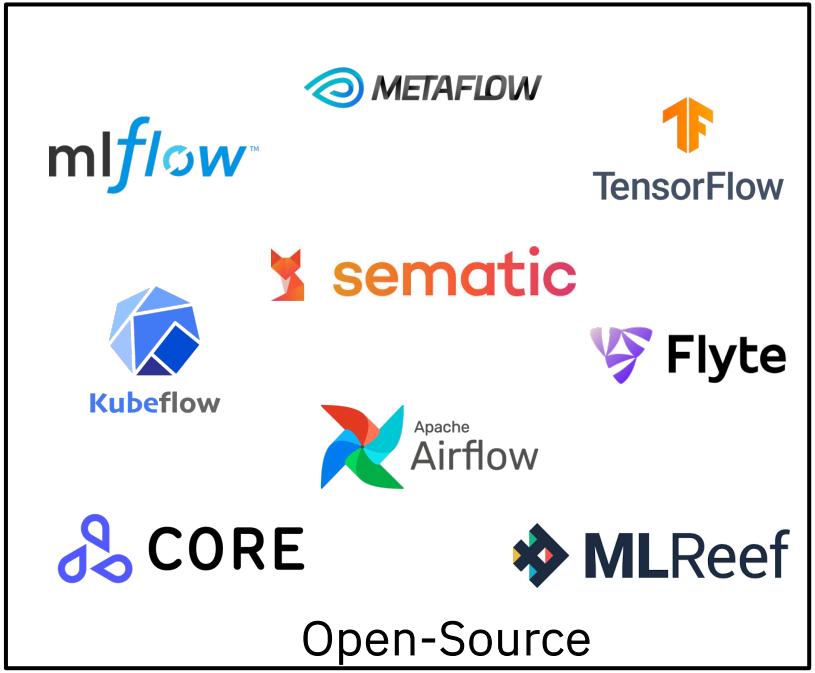
What is MLOps?

ibm.com/topics/mlops

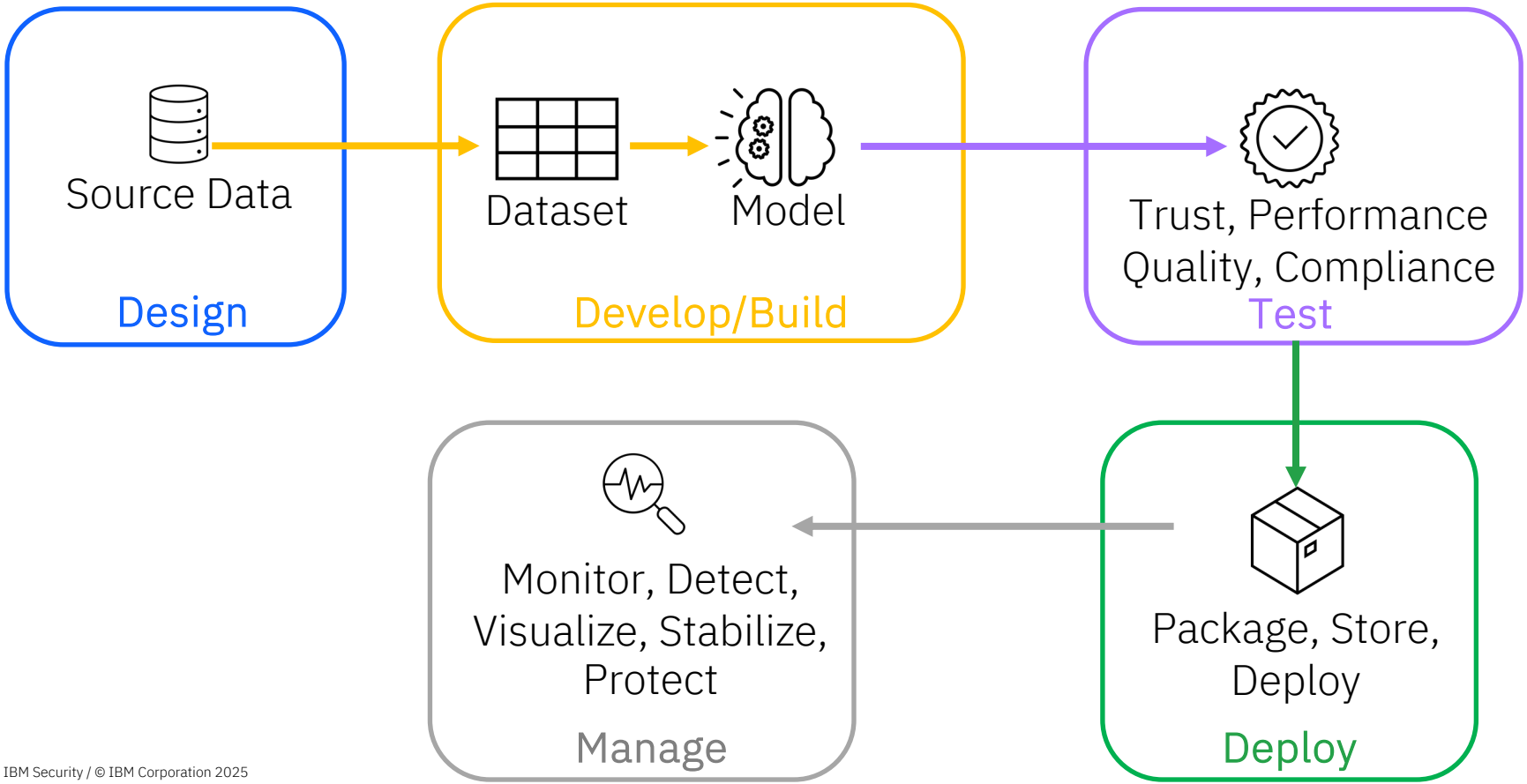


Popular MLOps Platforms

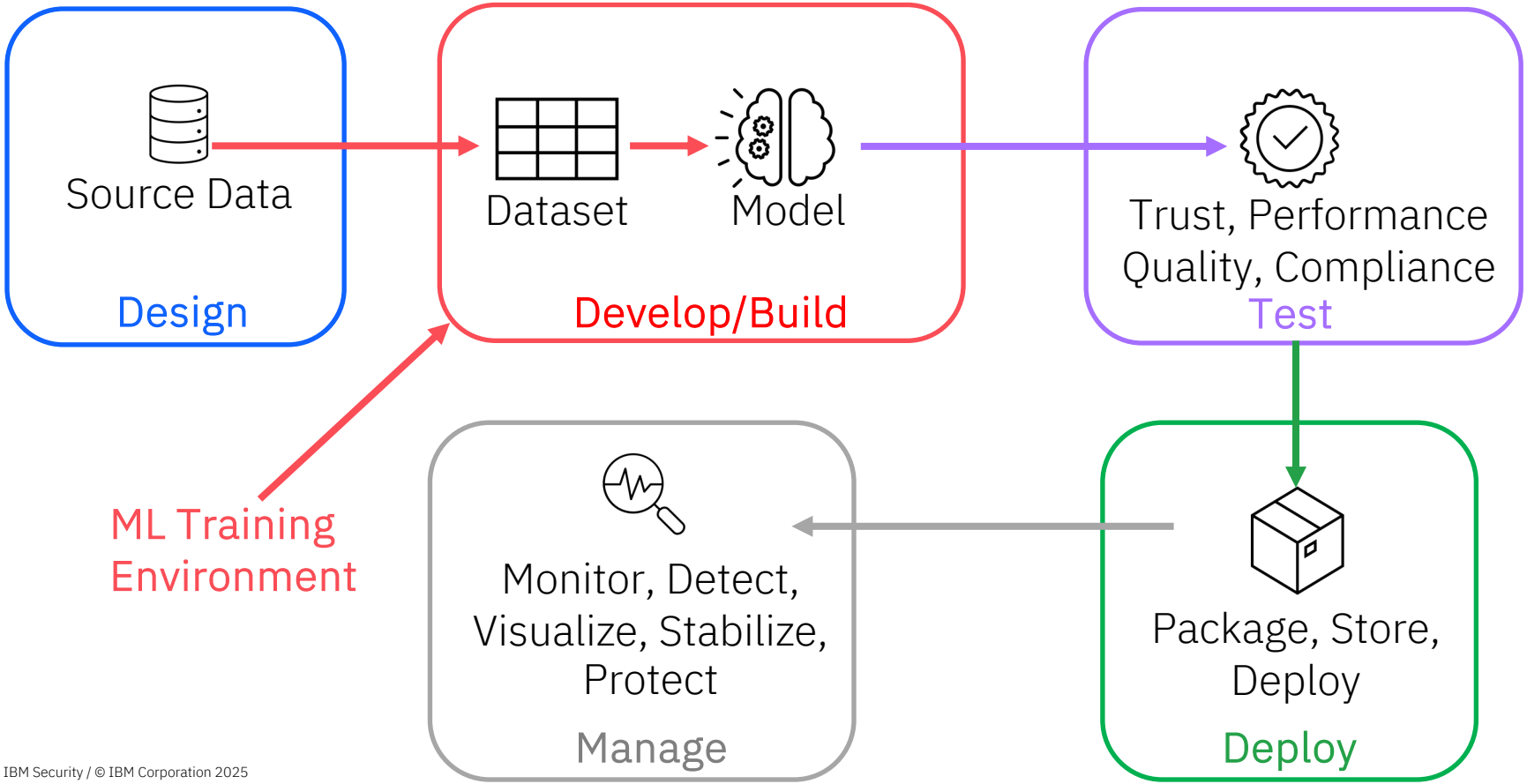




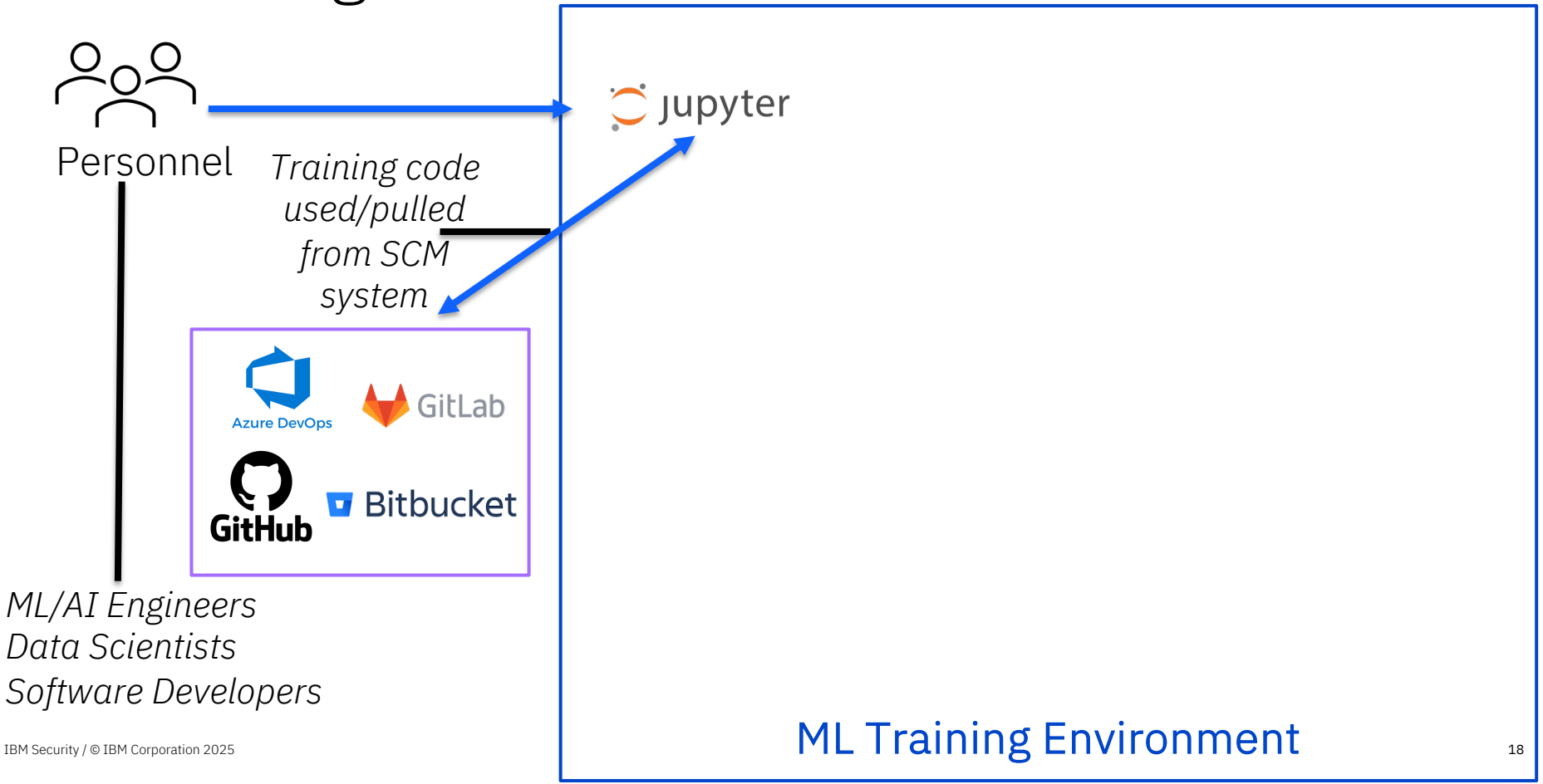
MLOps Lifecycle



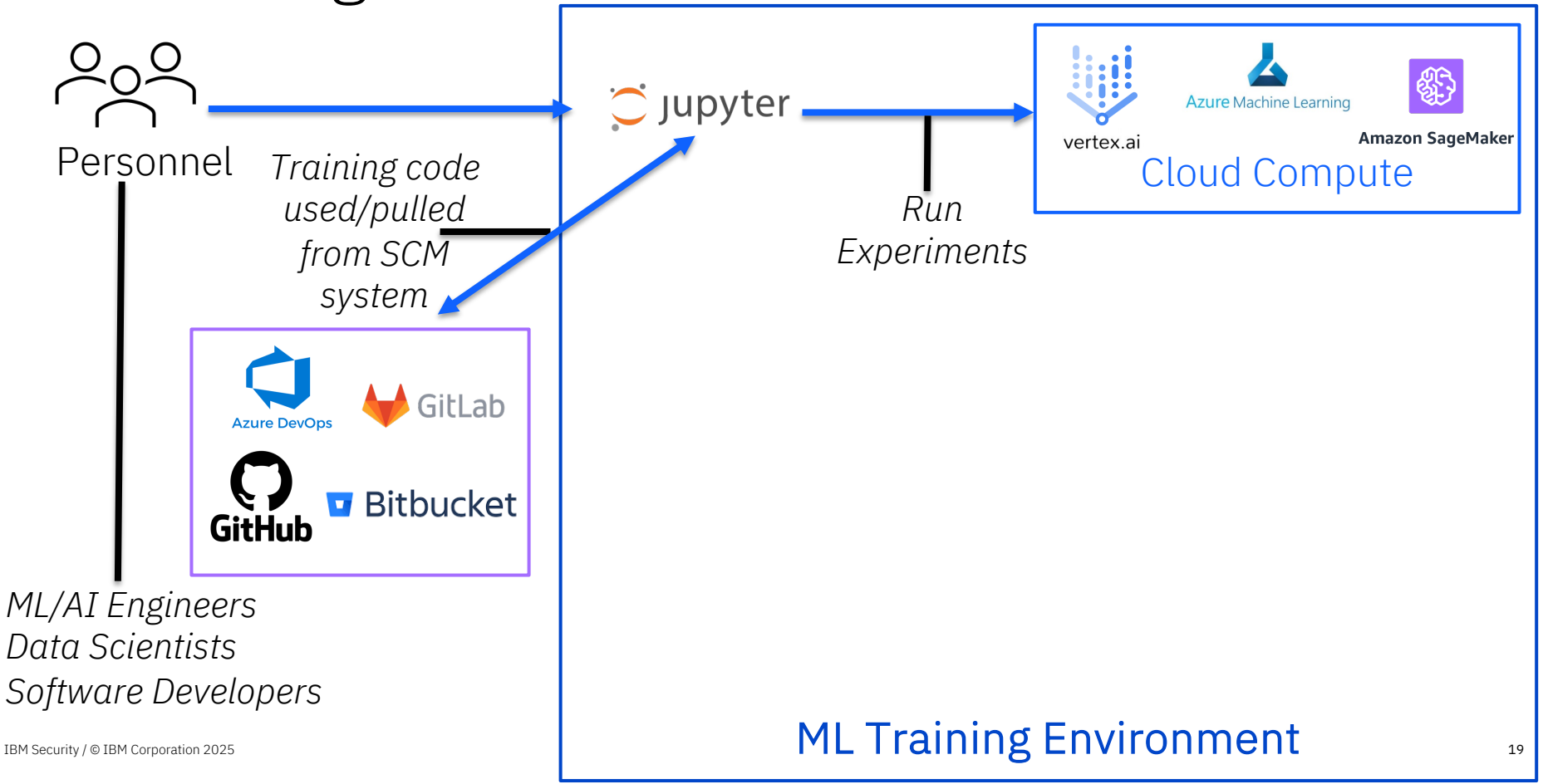
MLOps Lifecycle - ML Training Environment



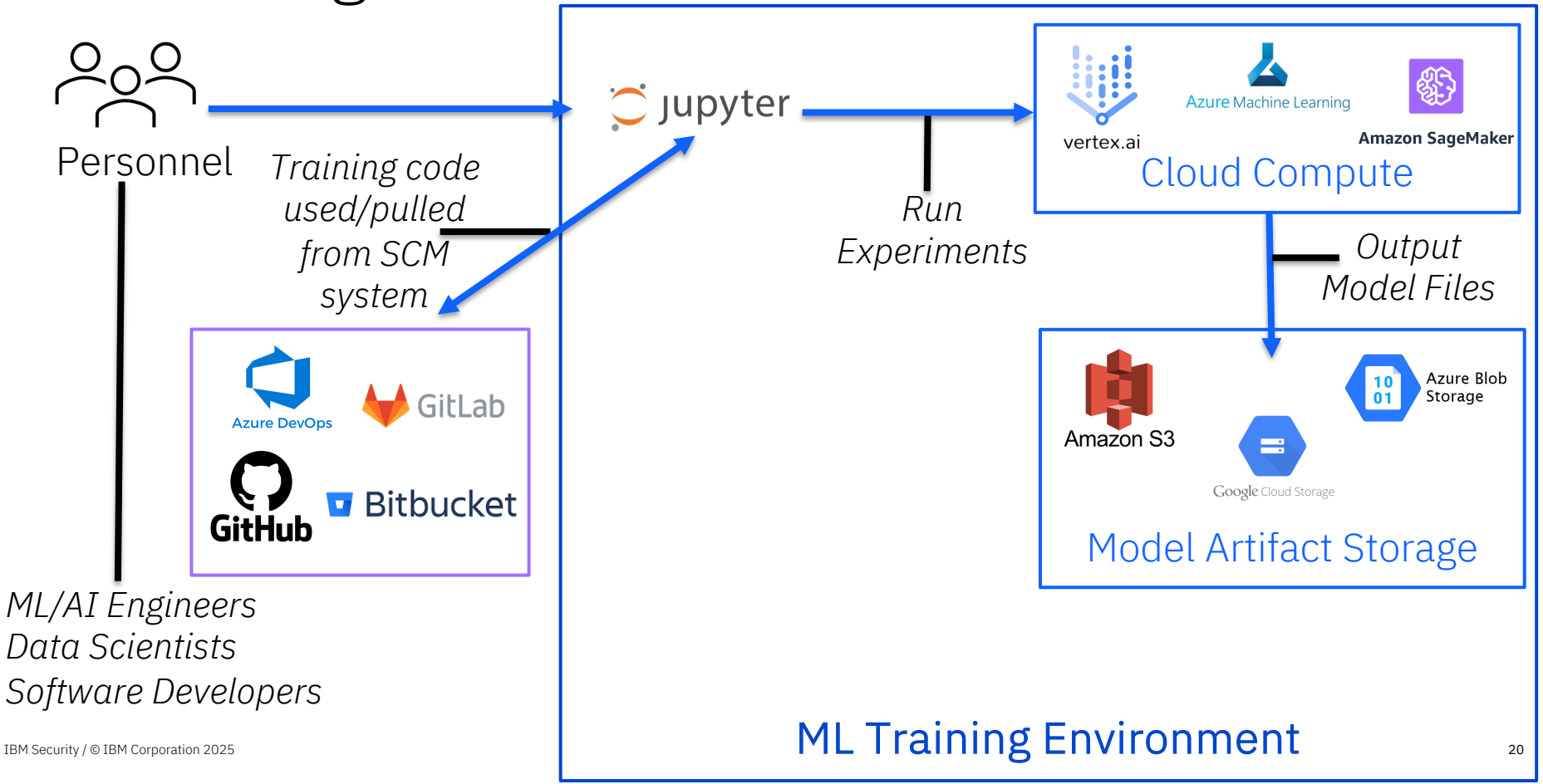
ML Training Environment Infrastructure



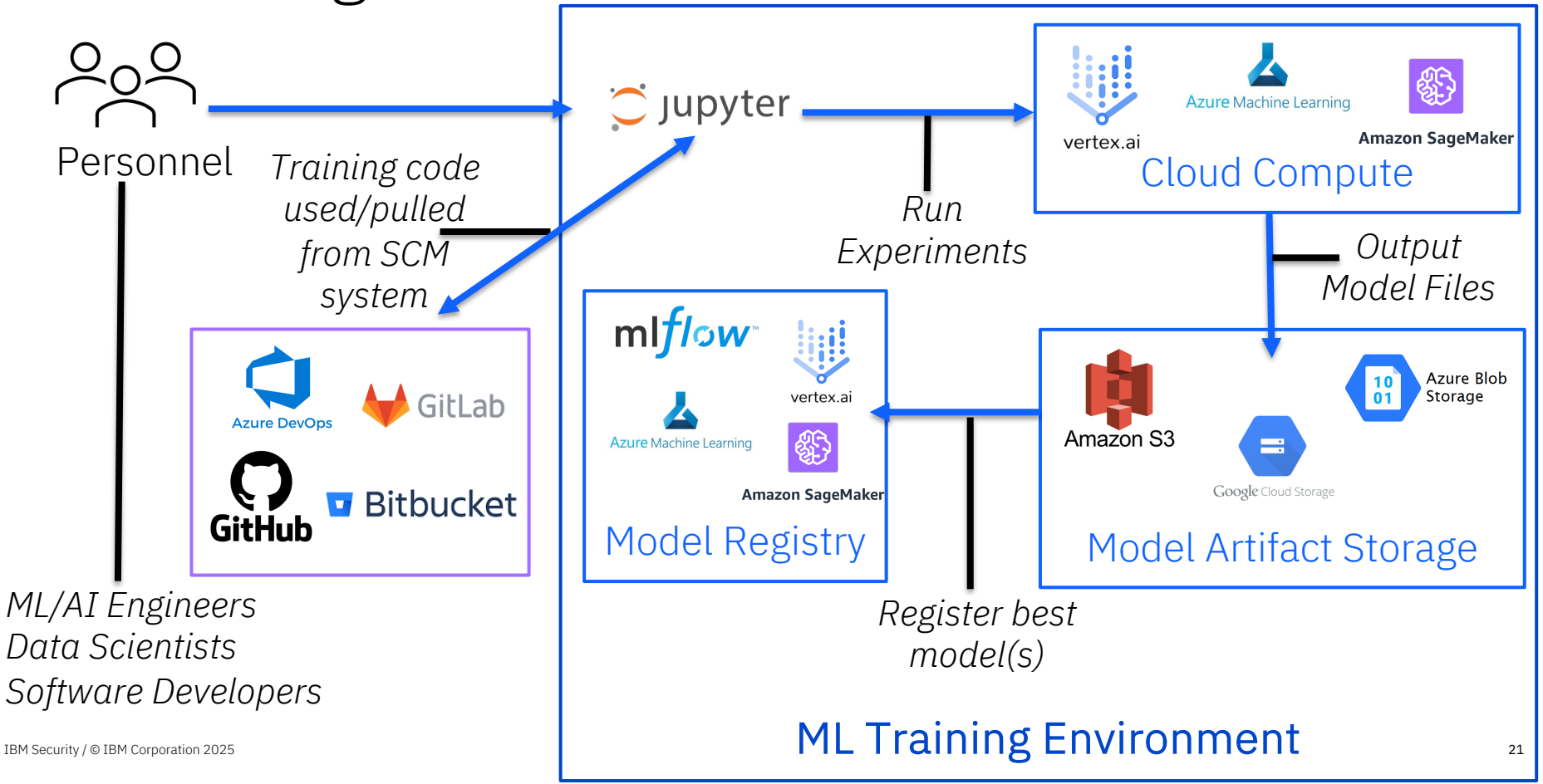
ML Training Environment Infrastructure



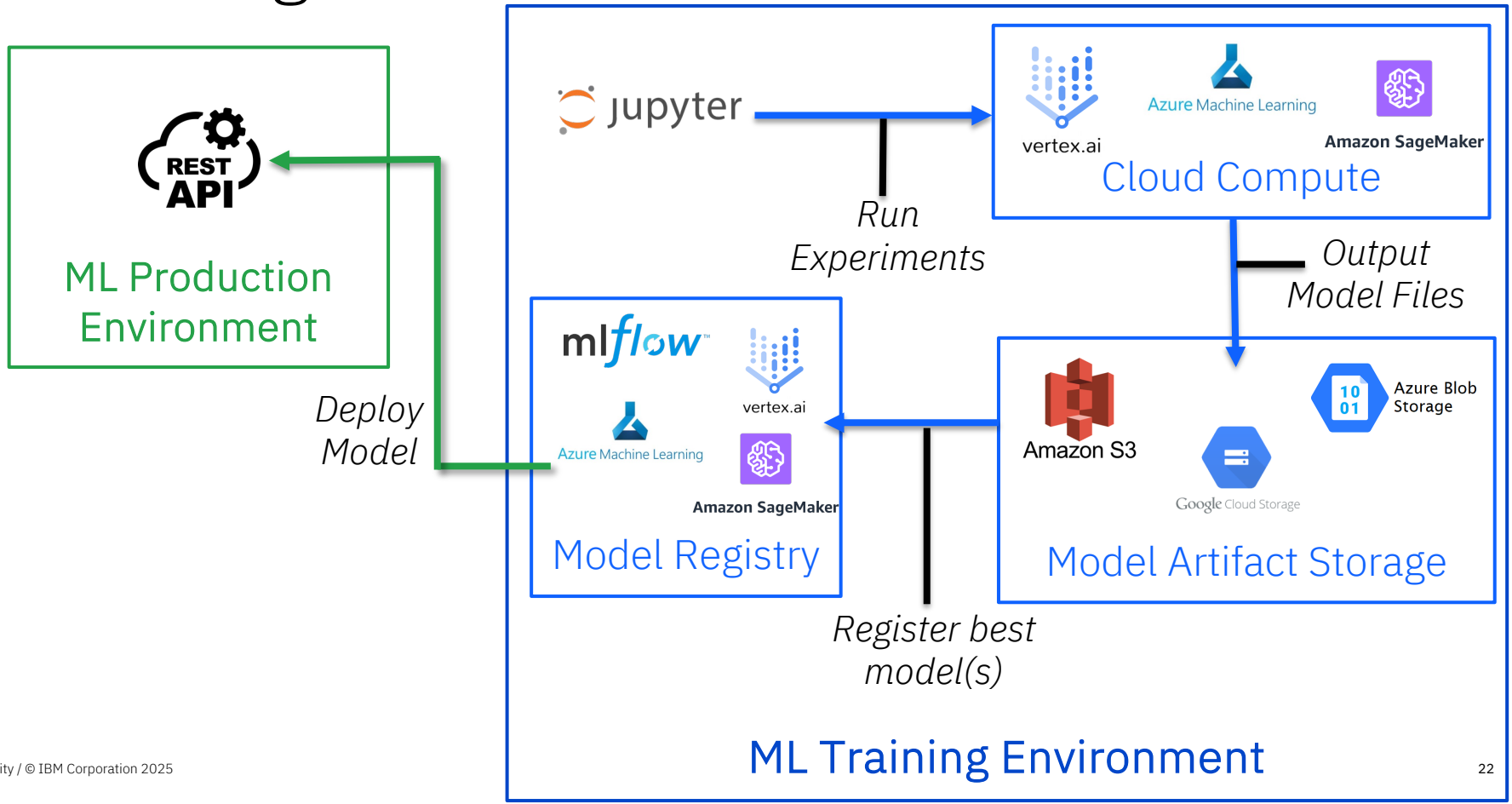
ML Training Environment Infrastructure



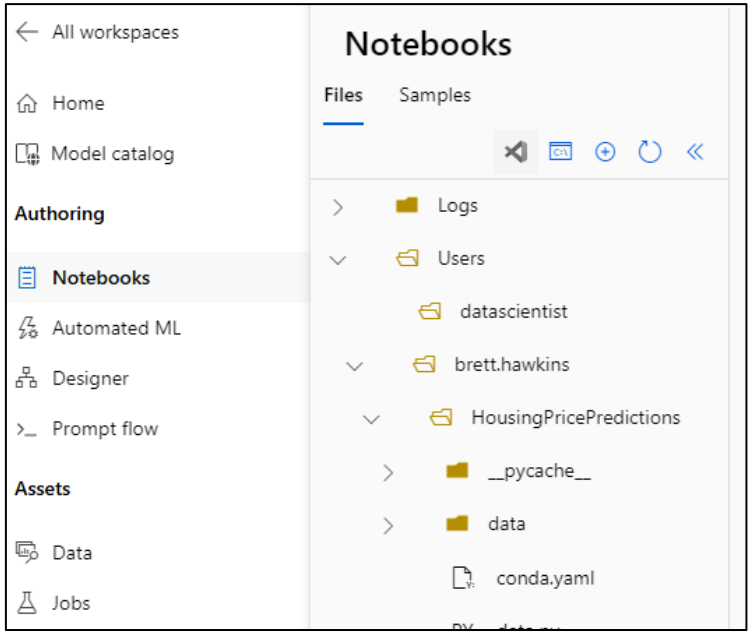
ML Training Environment Infrastructure



ML Training Environment Infrastructure



ML Training Infrastructure Components



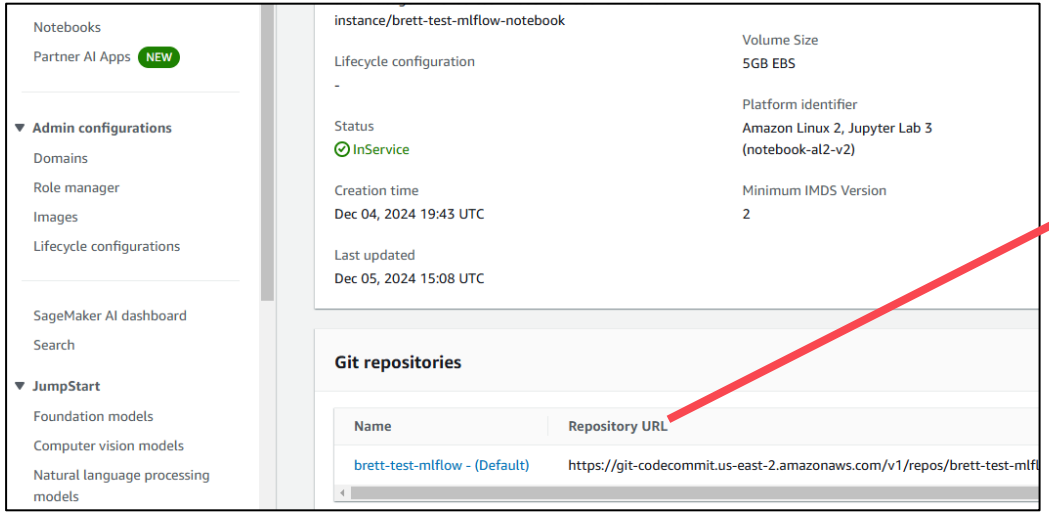
Notebook Env
Contains ML training code

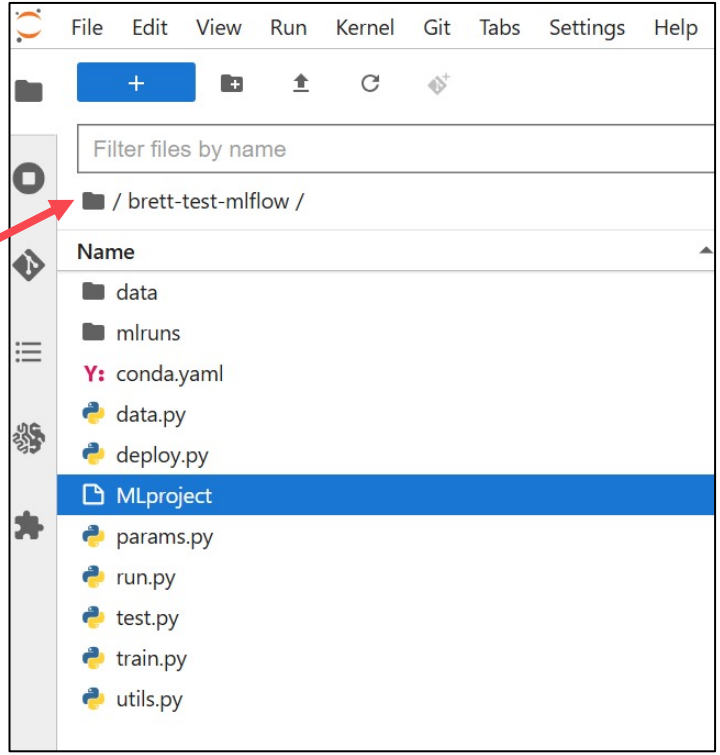
Model Registry
Track and version models

Cloud Compute
Infrastructure that performs ML training from ML training code

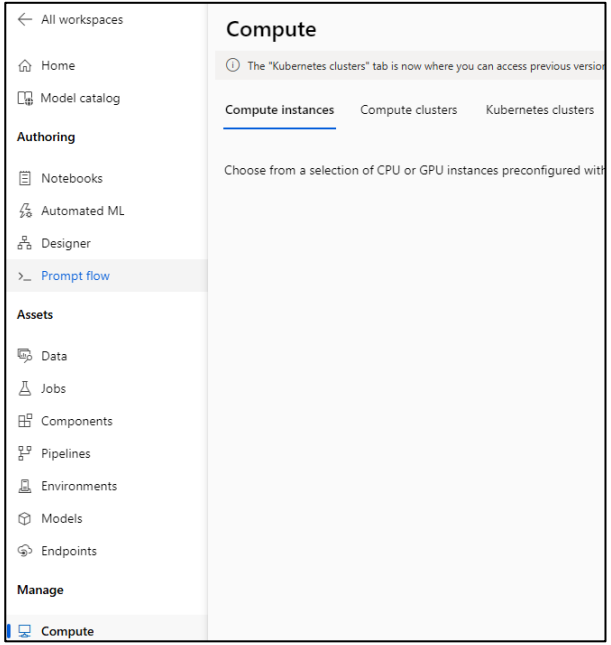
Model Artifact Storage
ML training artifact outputs (model weights, model files, etc.)

Notebook Env- SageMaker





ML Training Infrastructure Components



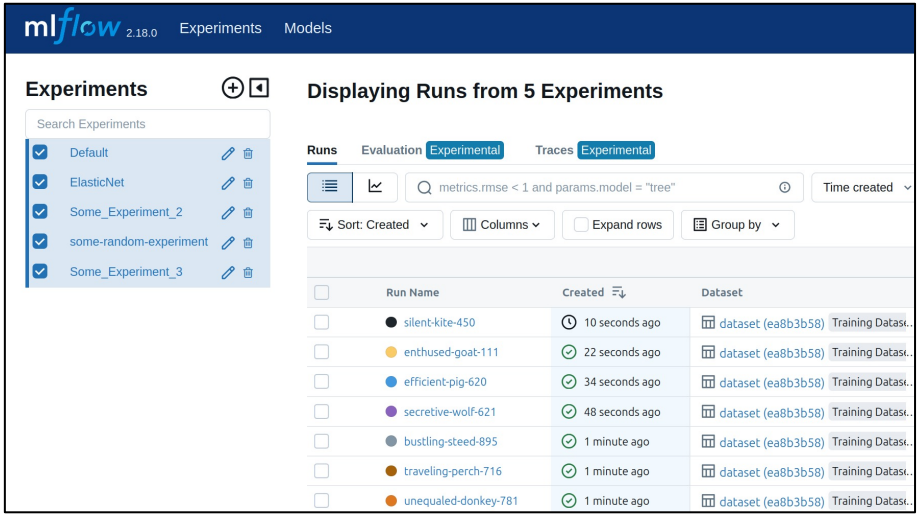
Notebook Env
Contains ML training code

Model Registry
Track and version models

Cloud Compute
Infrastructure that performs ML training from ML training code

Model Artifact Storage
ML training artifact outputs (model weights, model files, etc.)

ML Training Infrastructure Components



Notebook Env
Contains ML training code

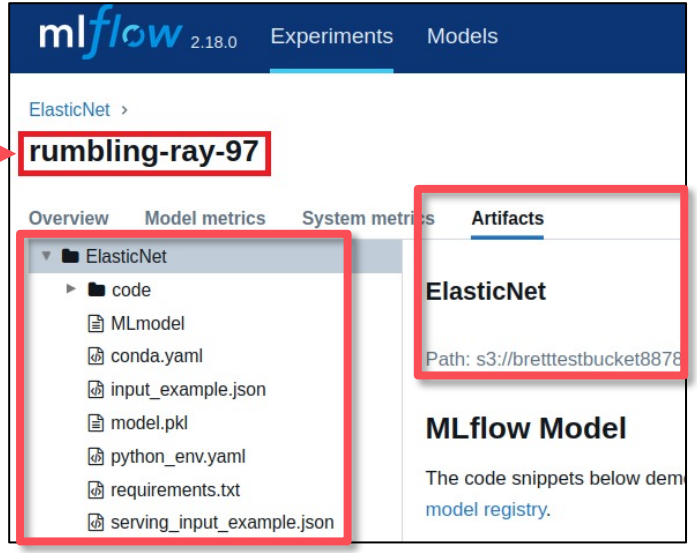
Model Registry
Track and version models

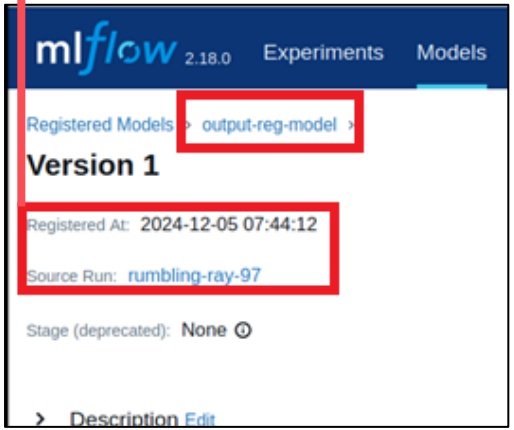
Cloud Compute
Infrastructure that performs ML training from ML training code

Model Artifact Storage
ML training artifact outputs (model weights, model files, etc.)

Model Registry and Artifact Storage - MLFlow

Points to Experiment Run

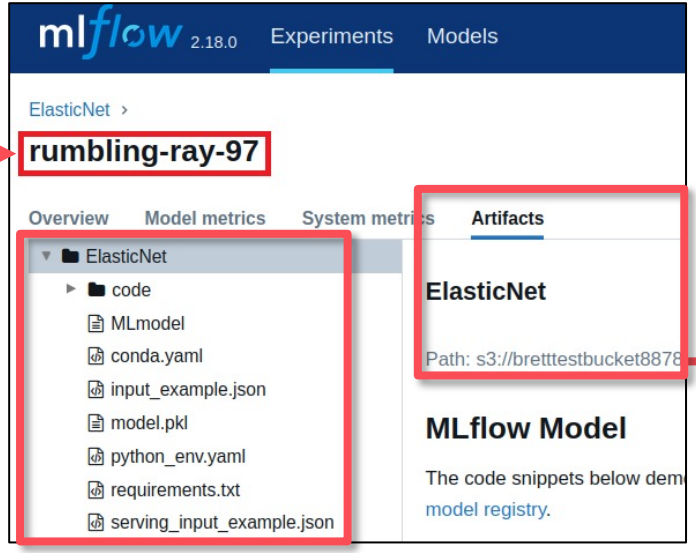


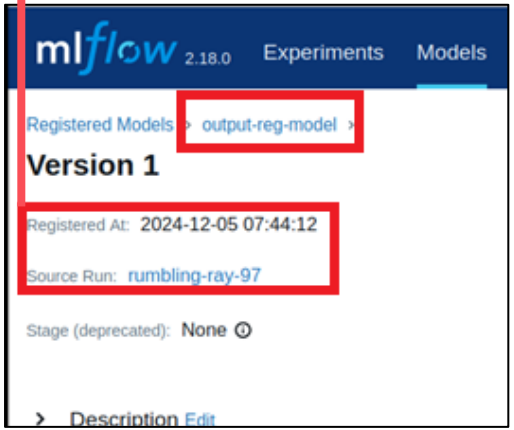


Model Registry

Model Registry and Artifact Storage - MLFlow

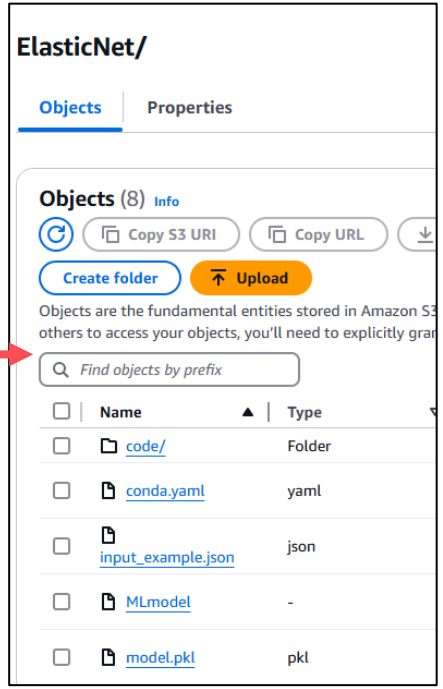
Points to Experiment Run





Model Registry

Model Artifacts from Experiment Run



Artifact Storage (S3)

Model Registry and Artifact Storage - SageMaker

Points to Training Job

Amazon SageMaker AI > Models

Models

Search models

Name
housing-price-prediction
employee-salary-model
model-employee-salary-2
test-model-employee-salary

Model Registry

Amazon SageMaker AI > Training jobs

Training jobs Info

Search training jobs

Name
Canvas1737552693229-t1-1-abc7ba0d24a949c1b71e3068f6818d5dbaa024
Canvas1737498359380-t1-1-3cd30f983f574fa981d972b73671b6009d1aa4
linear-learner-2025-01-14-17-48-39-098
Canvas1736861646394-t1-1-e9af1f274ed743d7854a6f5b74d3175a8b8311

Model data location

s3://sagemaker-us-east-2-339713155979/Canvas/default-20250121T171825/Training/output/Canvas1
candidates/model/Canvas1737552693229-trial-t1-1/model.tar.gz

Scanning status

-

Model Registry and Artifact Storage - SageMaker

Points to Training Job

Amazon SageMaker AI > Models

Models

Search models

Name
housing-price-prediction
employee-salary-model
model-employee-salary-2
test-model-employee-salary

Model Registry

Amazon SageMaker AI > Training jobs

Training jobs Info

Search training jobs

Name
Canvas1737552693229-t1-1-abc7ba0d24a949c1b71e3068f6818d5dbaa024
Canvas1737498359380-t1-1-3cd30f983f574fa981d972b73671b6009d1aa4
linear-learner-2025-01-14-17-48-39-098
Canvas1736861646394-t1-1-e9af1f274ed743d7854a6f5b74d3175a8b8311

Model data location

s3://sagemaker-us-east-2-339713155979/Canvas/default-20250121T171825/Training/output/Canvas
candidates/model/Canvas1737552693229-trial-t1-1/model.tar.gz

Scanning status

-

Artifact Storage (S3)

Canvas1737552693229-trial-t1-1/

Objects | Properties

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You c

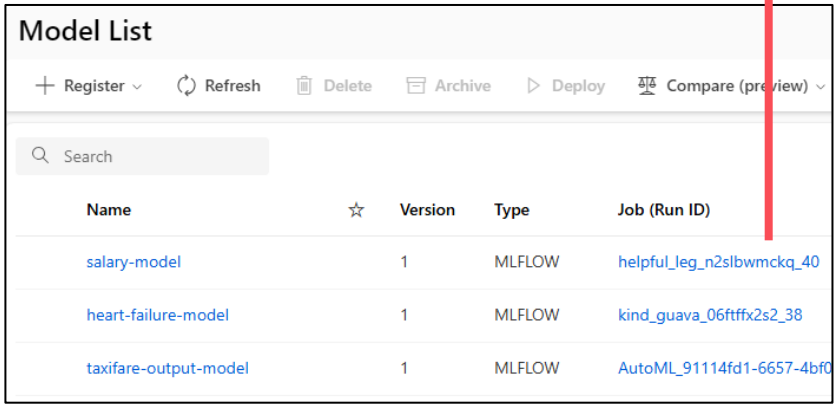
Find objects by prefix

Name	Type
model.tar.gz	gz

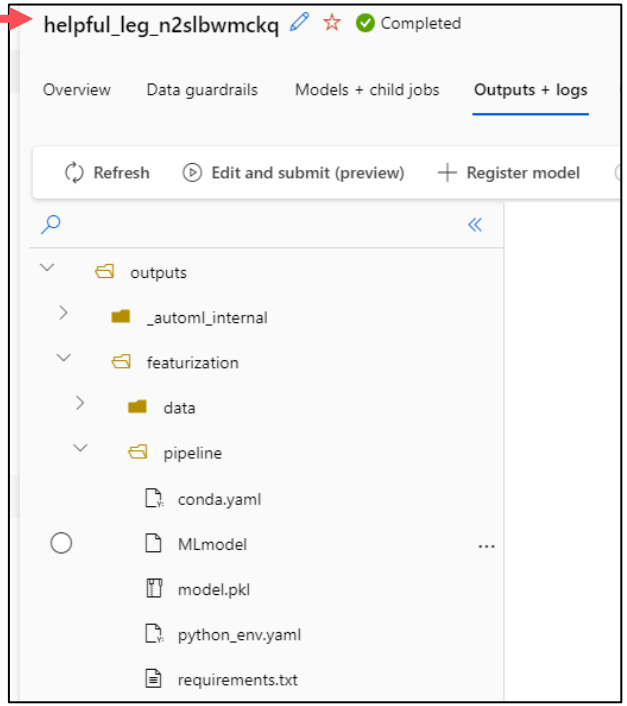
Model Artifacts from Training Job Run

Model Registry and Artifact Storage – Azure ML

Points to Training Job

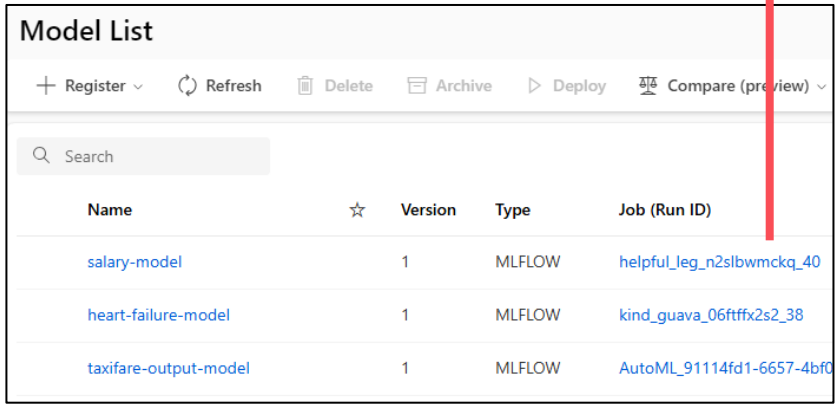


Model Registry

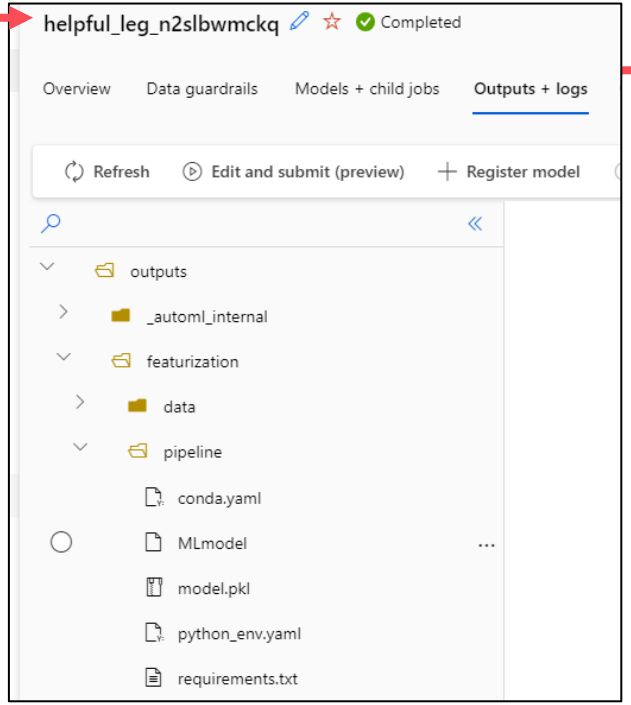


Model Registry and Artifact Storage – Azure ML

Points to Training Job



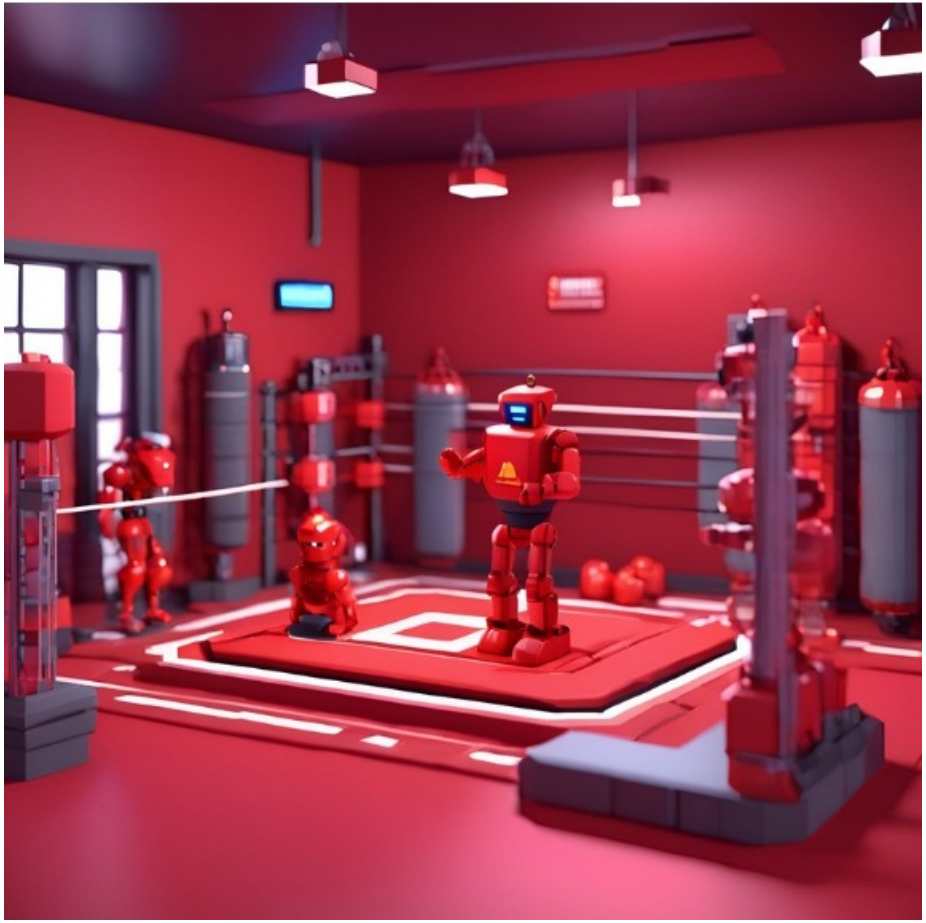
Model Registry



Azure Blob Storage

Model Artifacts from Training Job Run

Attacking ML Training Environments



Key Components – Attacker Perspective

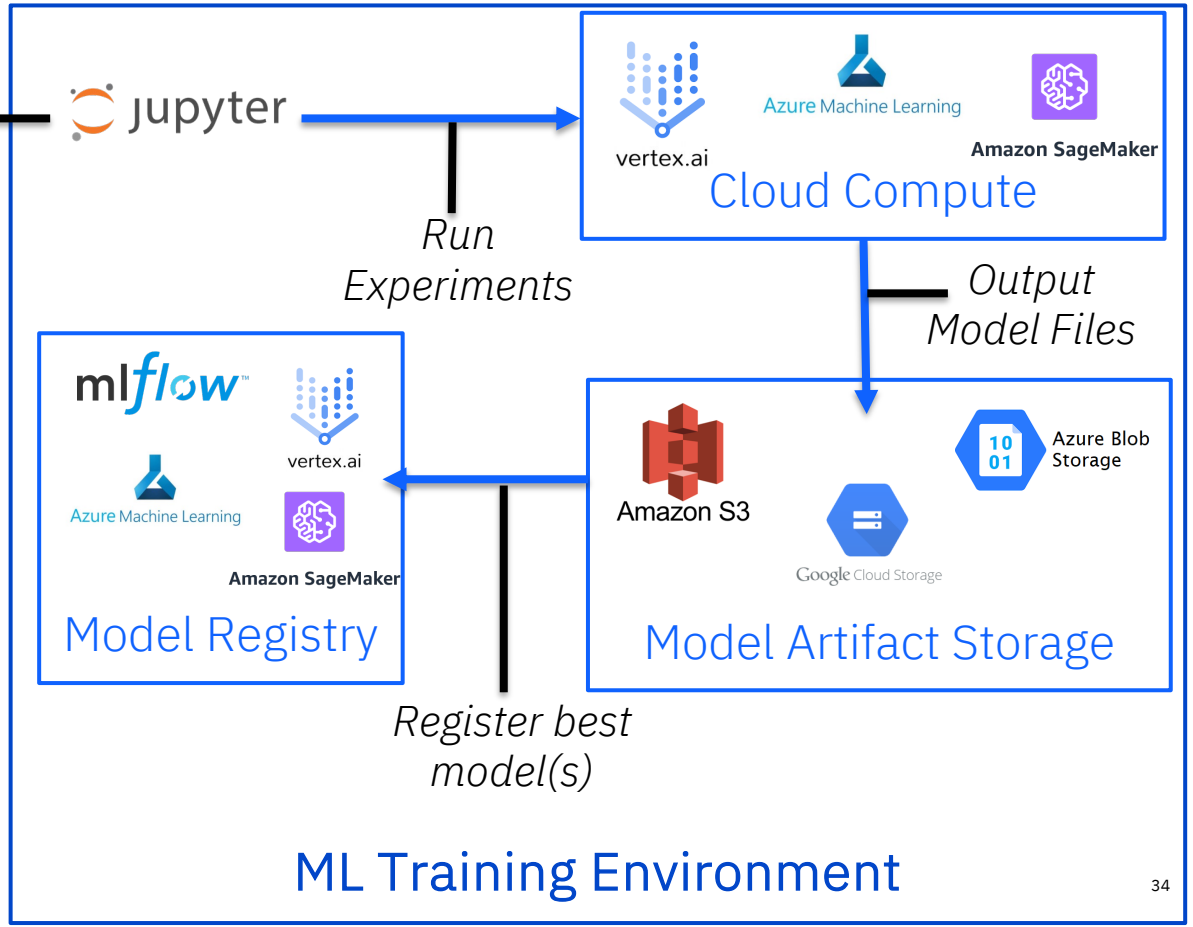
Credentials and info on other infrastructure

2:BrettComputeTest | test.ipynb

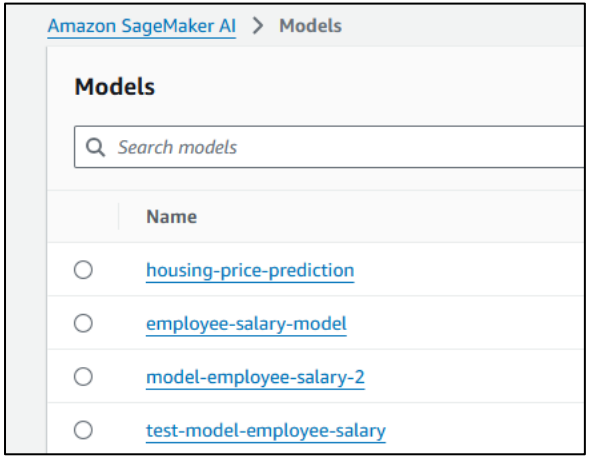
Edit in

BrettComputeTest · Kernel idle CPU 0% RAM 2%

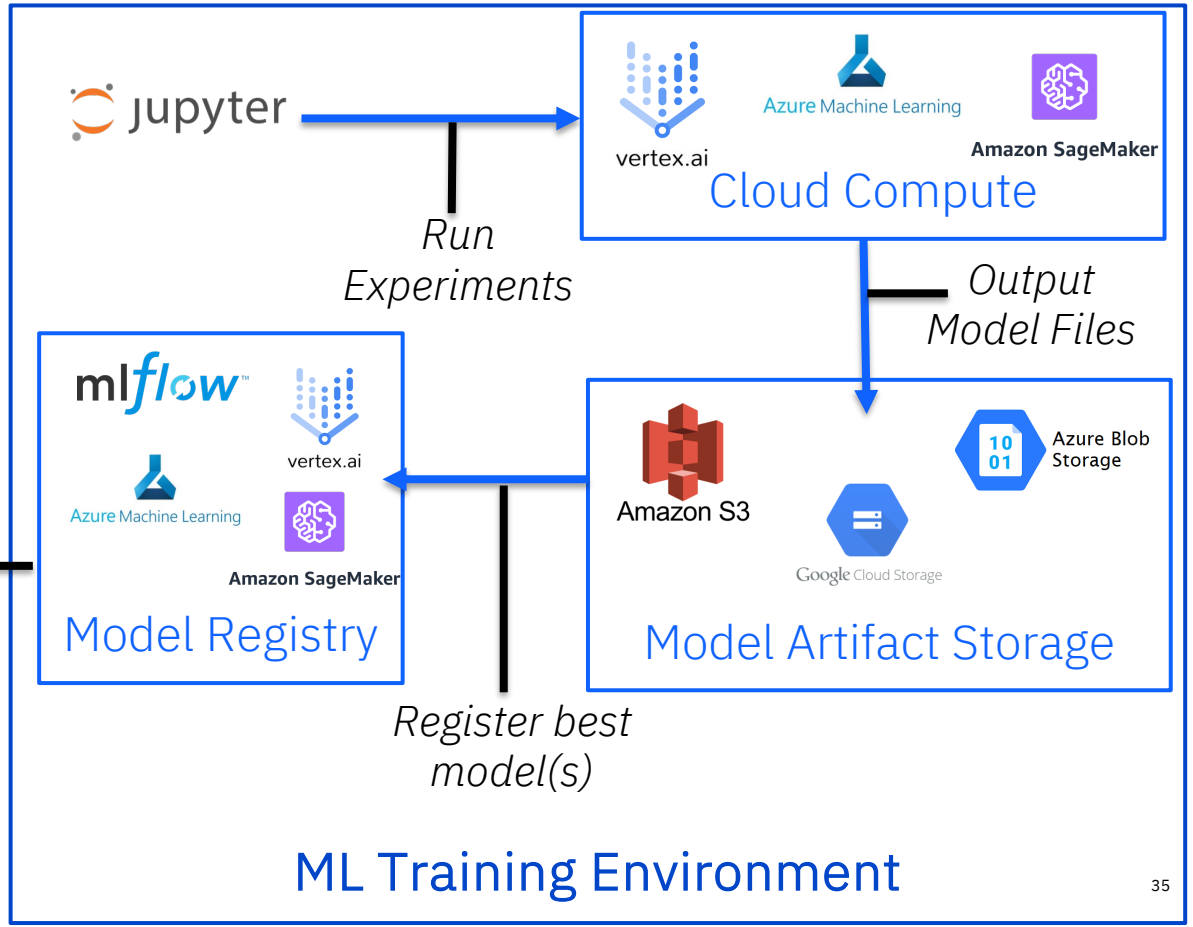
```python
import mlflow
import os

experiment_name = "ImportantExperiment"
entry_point = "Training"

# Set environment variables for MLflow tracking
os.environ['MLFLOW_TRACKING_USERNAME'] = 'admin'
os.environ['MLFLOW_TRACKING_PASSWORD'] = 'password'

mlflow.set_tracking_uri("http://13.58.45.122:5000")

mlflow.projects.run(
    uri=".",
    entry_point=entry_point,
    experiment_name=experiment_name,
    env_manager="conda"
    )
```



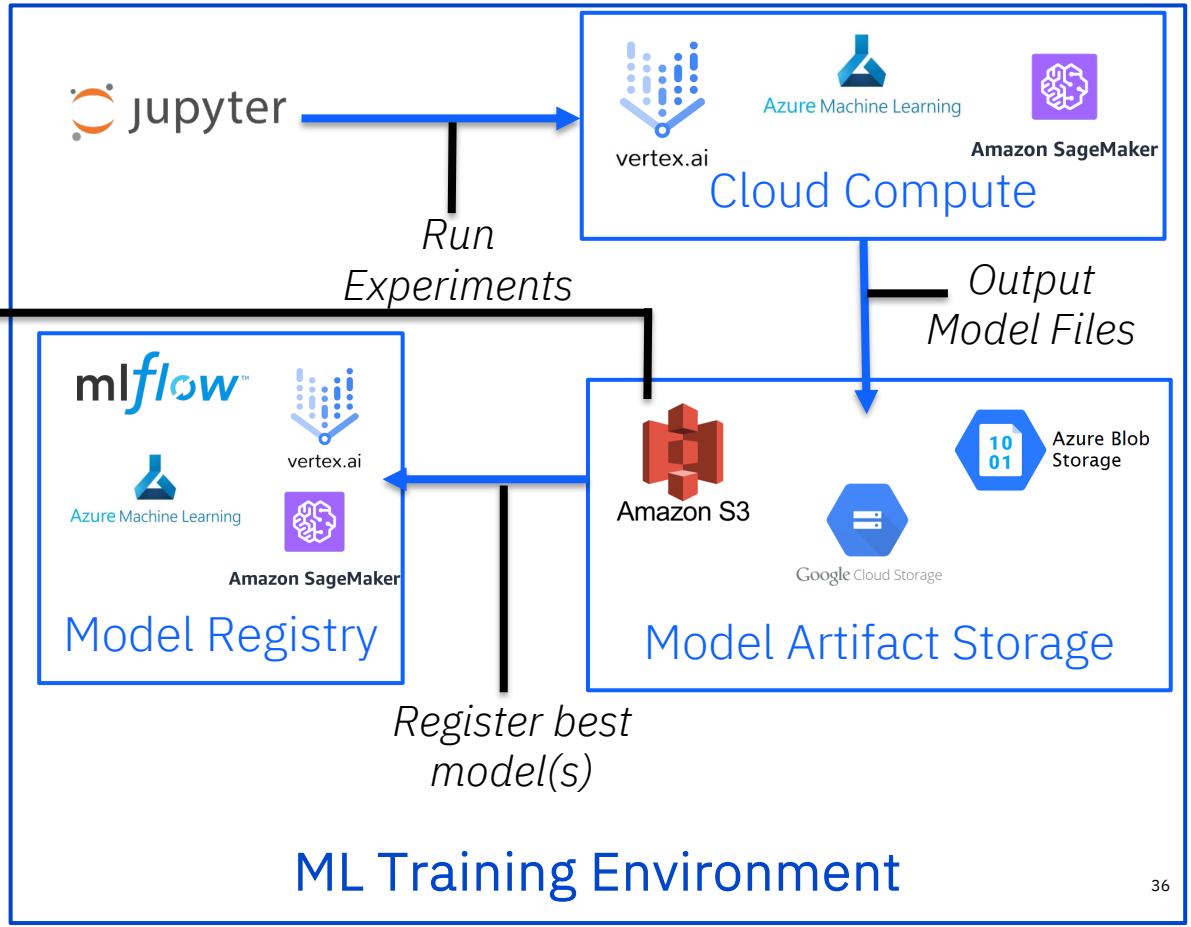
Key Components – Attacker Perspective



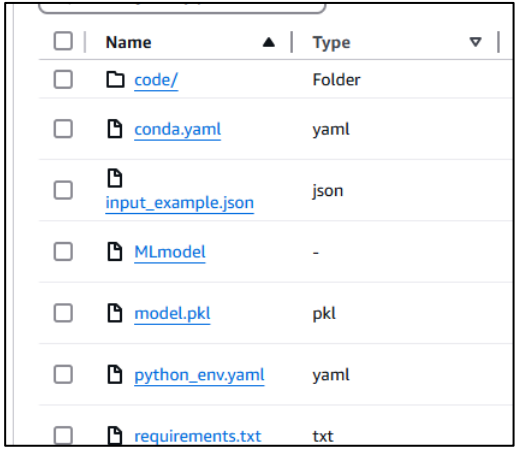
Useful for model reconnaissance



Key Components – Attacker Perspective



Fully trained model and model weights

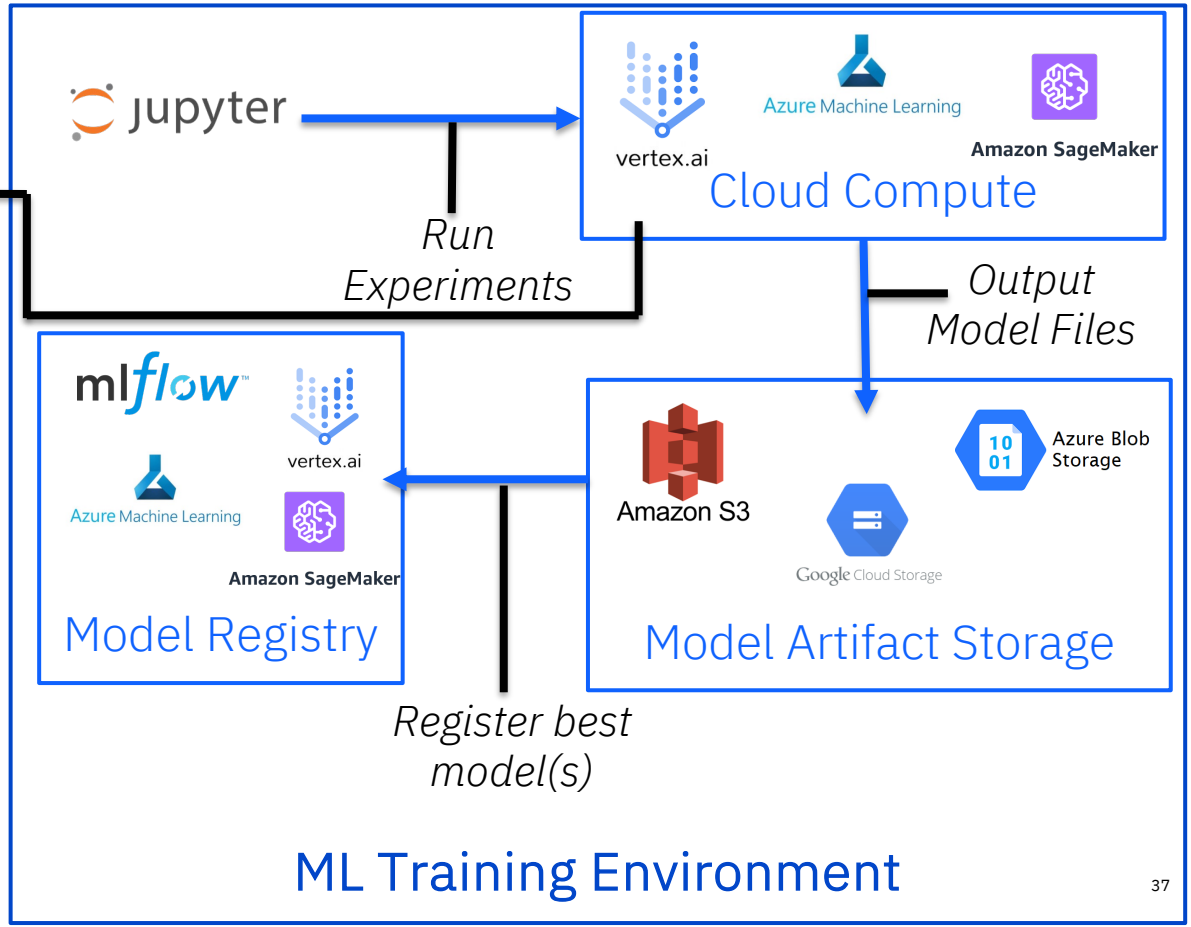


Name	Type
code/	Folder
conda.yaml	yaml
input_example.json	json
MLmodel	-
model.pkl	pkl
python_env.yaml	yaml
requirements.txt	txt

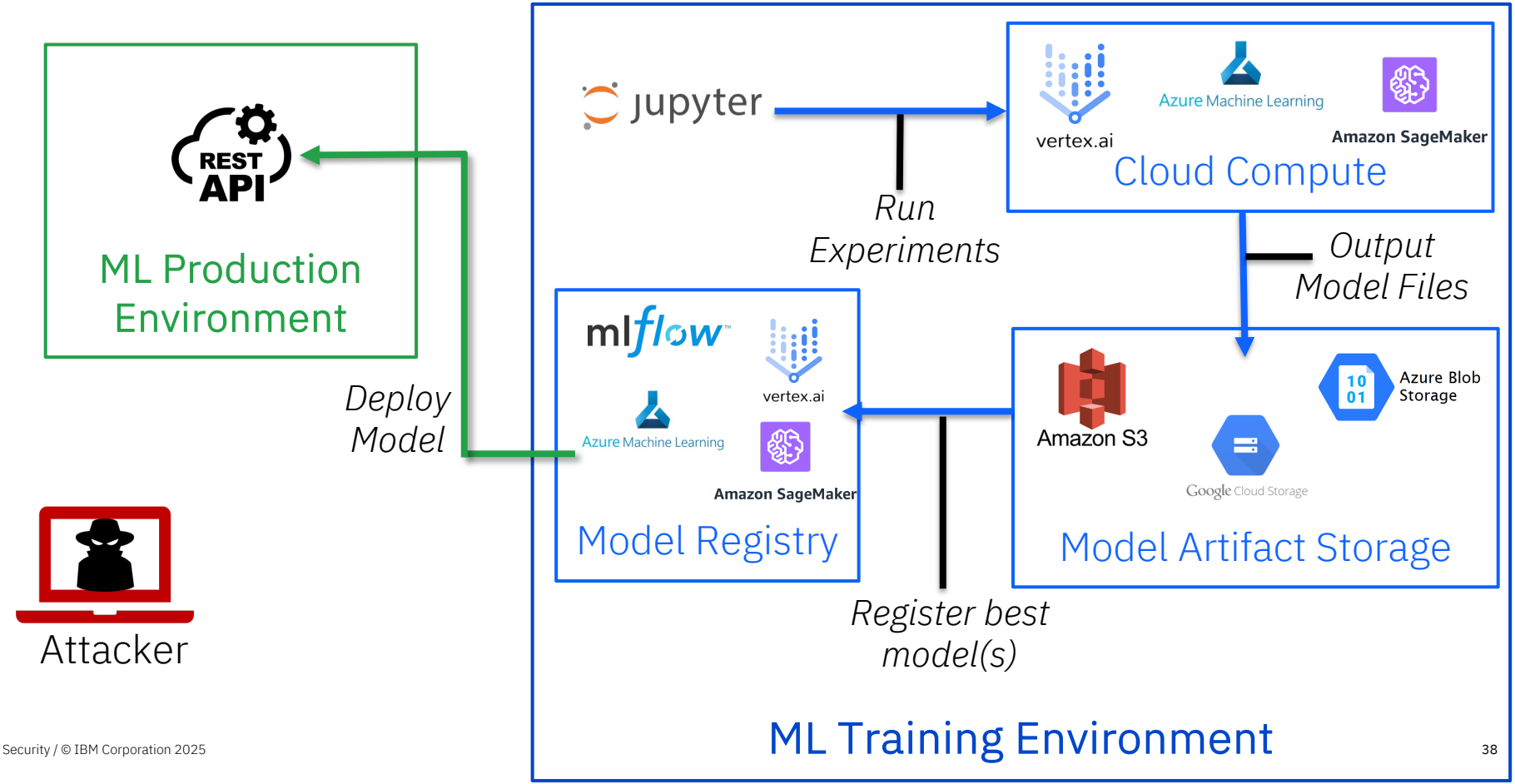
Key Components – Attacker Perspective

Sensitive environment variables and ML training code

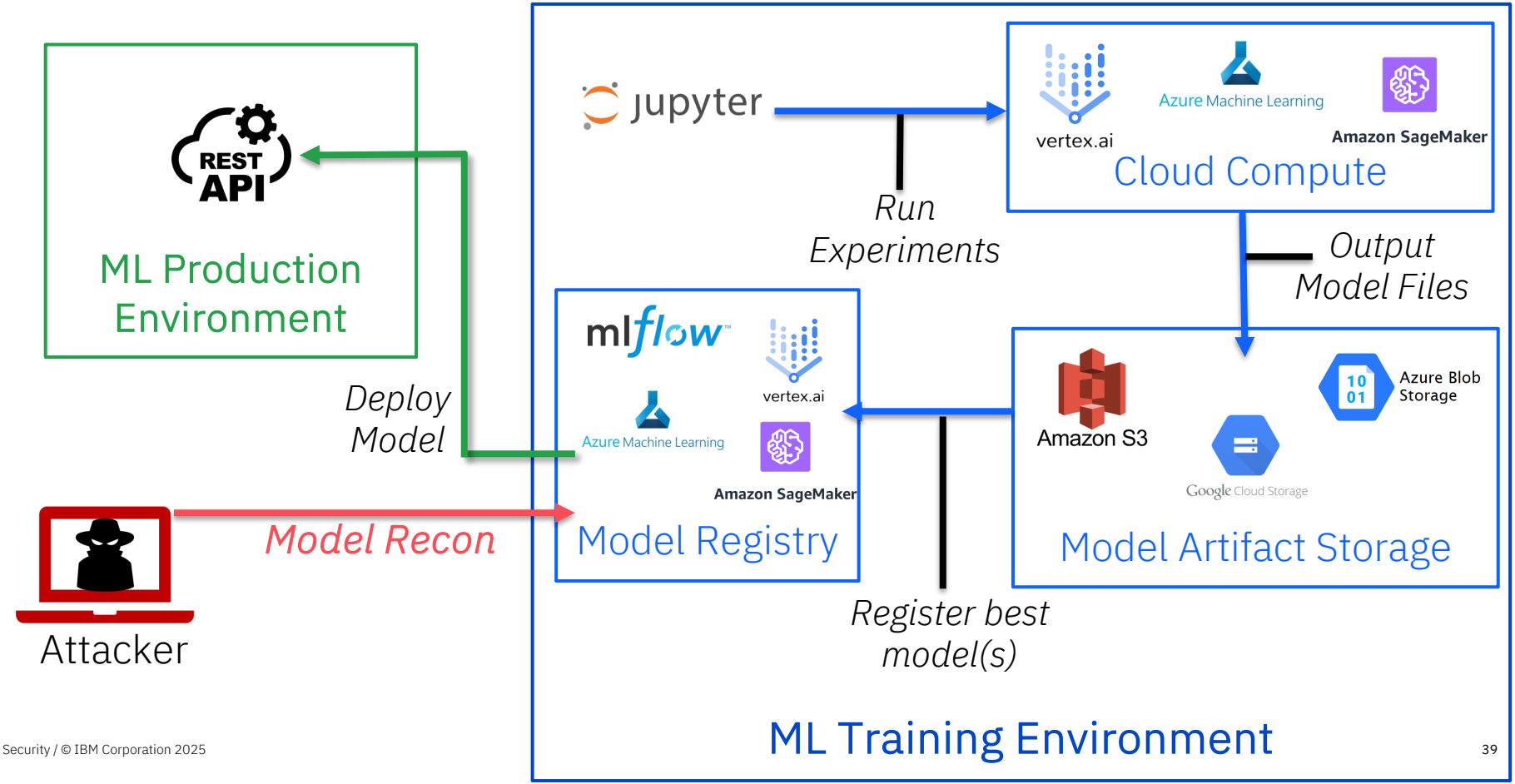
```
(base) [ec2-user@ip-172-16-11-6 brett-test-mlflow]$ ls -la
ls -la
total 64
drwxrwxr-x 7 ec2-user ec2-user 4096 Dec  5 15:35 .
drwxr-xr-x 6 ec2-user ec2-user 4096 Dec  5 15:08 ..
-rw-rw-r-- 1 ec2-user ec2-user 1292 Dec  4 19:48 conda.yaml
drwxrwxr-x 2 ec2-user ec2-user 4096 Dec  4 19:48 data
-rw-rw-r-- 1 ec2-user ec2-user 1485 Dec  4 19:48 data.py
-rw-rw-r-- 1 ec2-user ec2-user  879 Dec  4 19:48 deploy.py
drwxrwxr-x 8 ec2-user ec2-user 4096 Dec  5 15:35 .git
drwxrwxr-x 2 ec2-user ec2-user 4096 Dec  5 14:30 .ipynb_checkpoints
-rw-rw-r-- 1 ec2-user ec2-user  131 Dec  5 15:35 MLproject
drwxrwxr-x 4 ec2-user ec2-user 4096 Dec  5 15:15 mlruns
-rw-rw-r-- 1 ec2-user ec2-user  986 Dec  4 19:48 params.py
drwxrwxr-x 2 ec2-user ec2-user 4096 Dec  4 19:58 __pycache__
-rw-rw-r-- 1 ec2-user ec2-user  270 Dec  5 14:30 run.py
-rw-rw-r-- 1 ec2-user ec2-user  520 Dec  4 19:48 test.py
-rw-rw-r-- 1 ec2-user ec2-user 1342 Dec  4 19:48 train.py
-rw-rw-r-- 1 ec2-user ec2-user  409 Dec  4 19:48 utils.py
(base) [ec2-user@ip-172-16-11-6 brett-test-mlflow]$ ls -la data
ls -la data
total 904
drwxrwxr-x 2 ec2-user ec2-user   4096 Dec  4 19:48 .
drwxrwxr-x 7 ec2-user ec2-user   4096 Dec  5 15:35 ..
-rw-rw-r-- 1 ec2-user ec2-user 452865 Dec  4 19:48 test.csv
-rw-rw-r-- 1 ec2-user ec2-user 462137 Dec  4 19:48 train.csv
(base) [ec2-user@ip-172-16-11-6 brett-test-mlflow]$
```



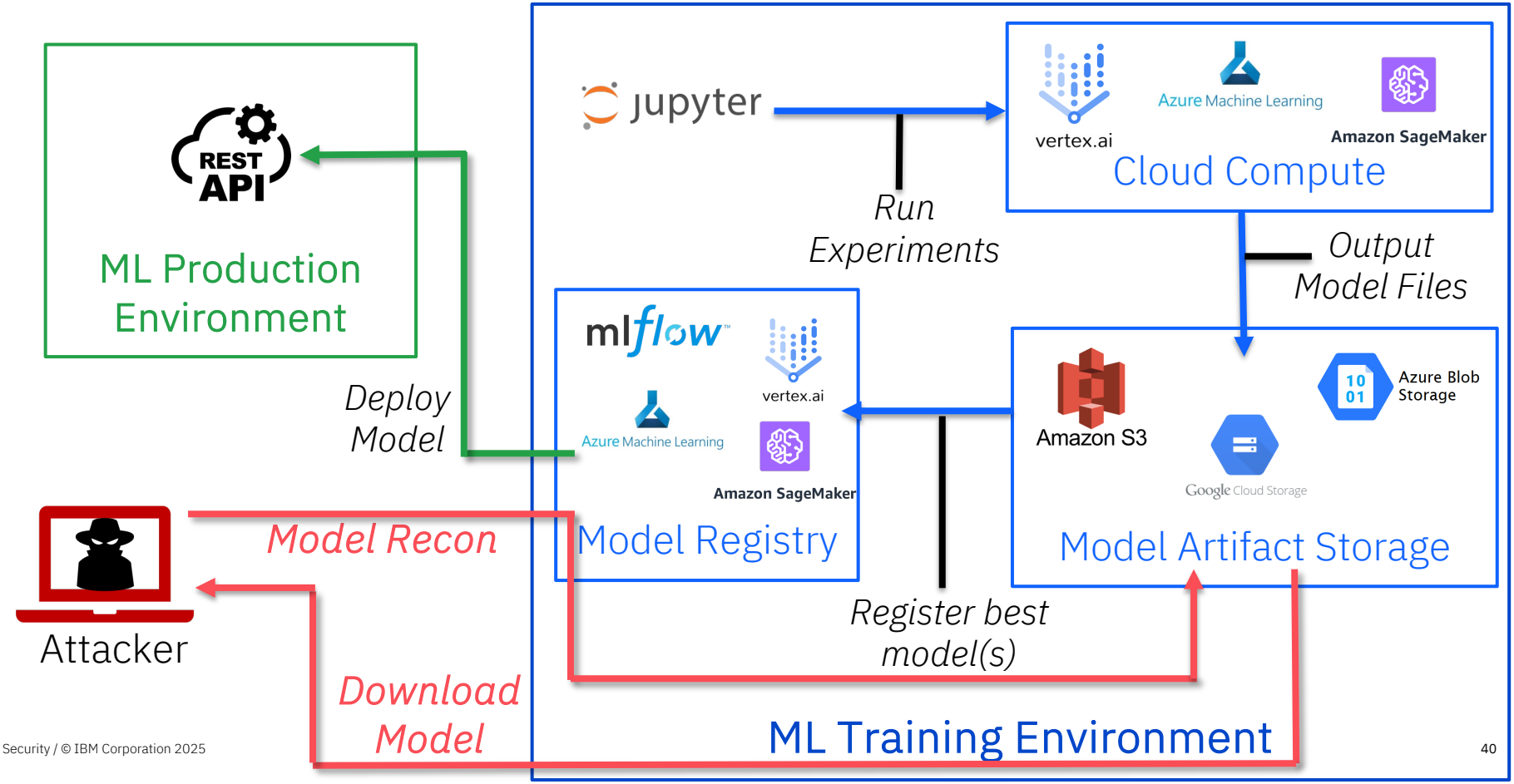
Model Theft


REST API
ML Production Environment
Deploy Model
jupyter
Run Experiments
vertex.ai
Azure Machine Learning
Amazon SageMaker
Cloud Compute
Output Model Files
mlflow
vertex.ai
Azure Machine Learning
Amazon SageMaker
Model Registry
Amazon S3
Azure Blob Storage
Google Cloud Storage
Model Artifact Storage
Register best model(s)
ML Training Environment
Attacker

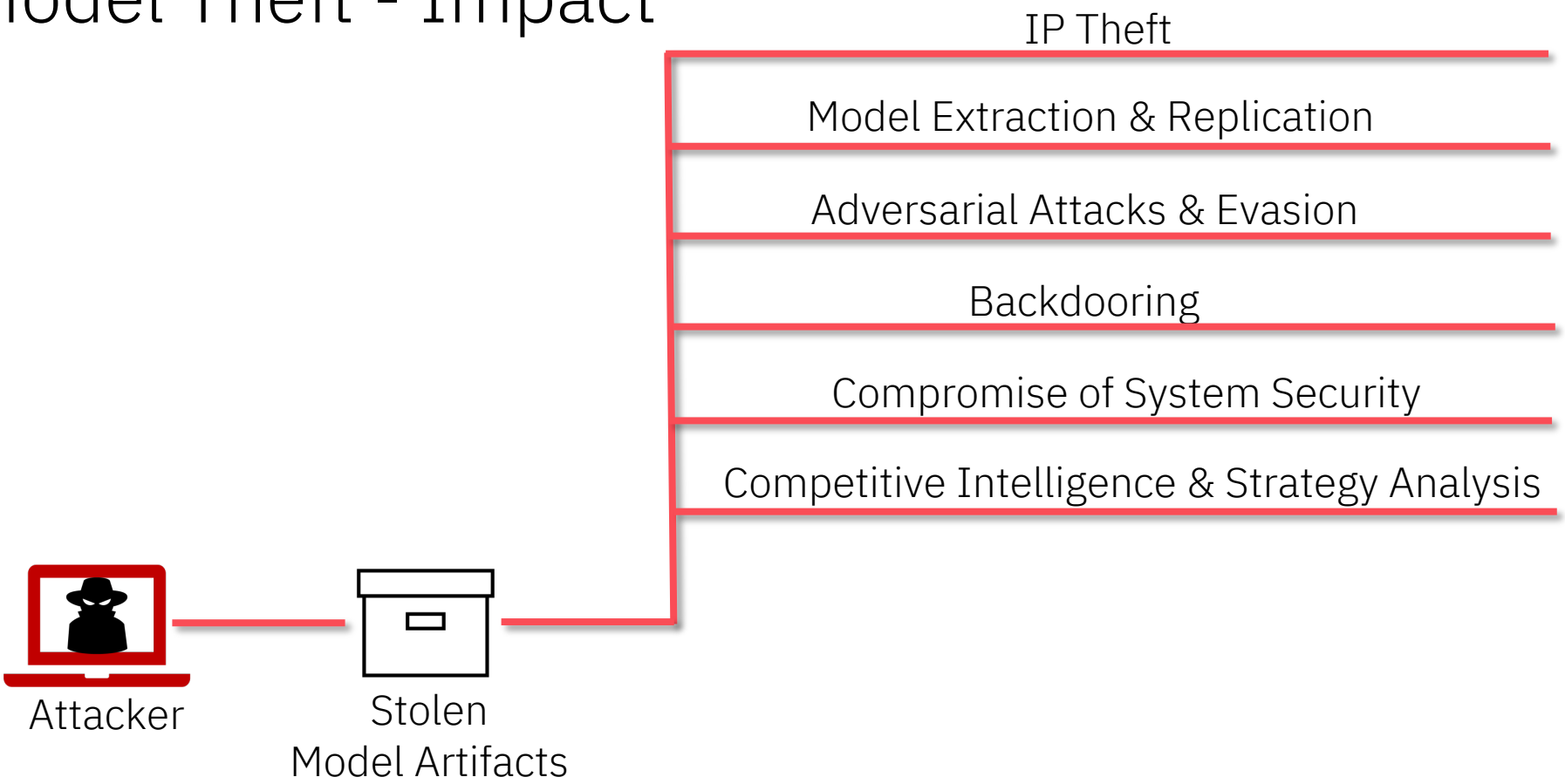
Model Theft


REST API
ML Production Environment
jupyter
vertex.ai
Azure Machine Learning
Amazon SageMaker
Cloud Compute
Run Experiments
Output Model Files
mlflow
vertex.ai
Azure Machine Learning
Amazon SageMaker
Model Registry
Deploy Model
Amazon S3
Azure Blob Storage
Google Cloud Storage
Model Artifact Storage
Model Recon
Attacker
Register best model(s)
ML Training Environment

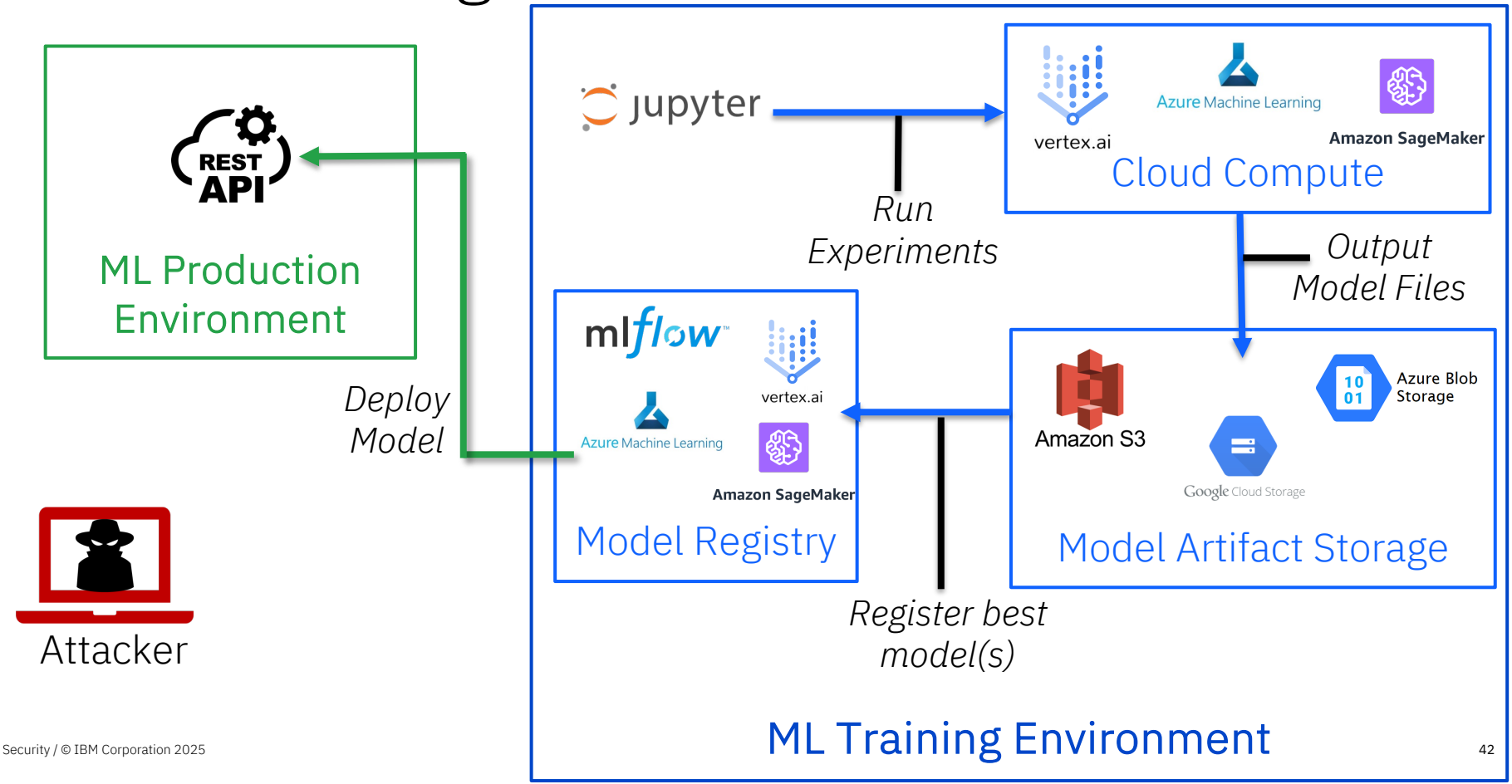
Model Theft


REST API
ML Production Environment
jupyter
vertex.ai
Azure Machine Learning
Amazon SageMaker
Cloud Compute
Run Experiments
Output Model Files
mlflow
vertex.ai
Azure Machine Learning
Amazon SageMaker
Model Registry
Amazon S3
Azure Blob Storage
Google Cloud Storage
Model Artifact Storage
Deploy Model
Model Recon
Attacker
Download Model
Register best model(s)
ML Training Environment

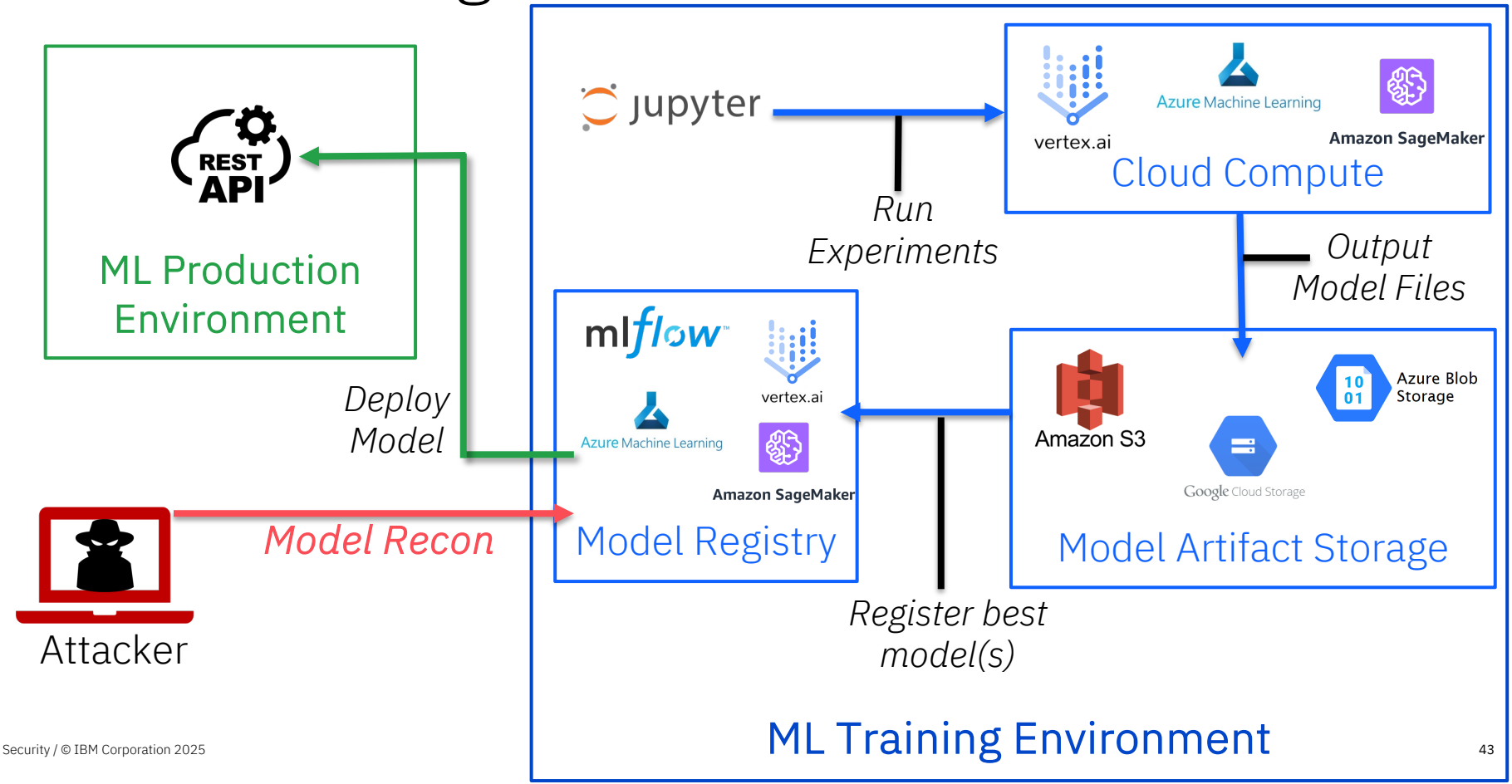
Model Theft - Impact



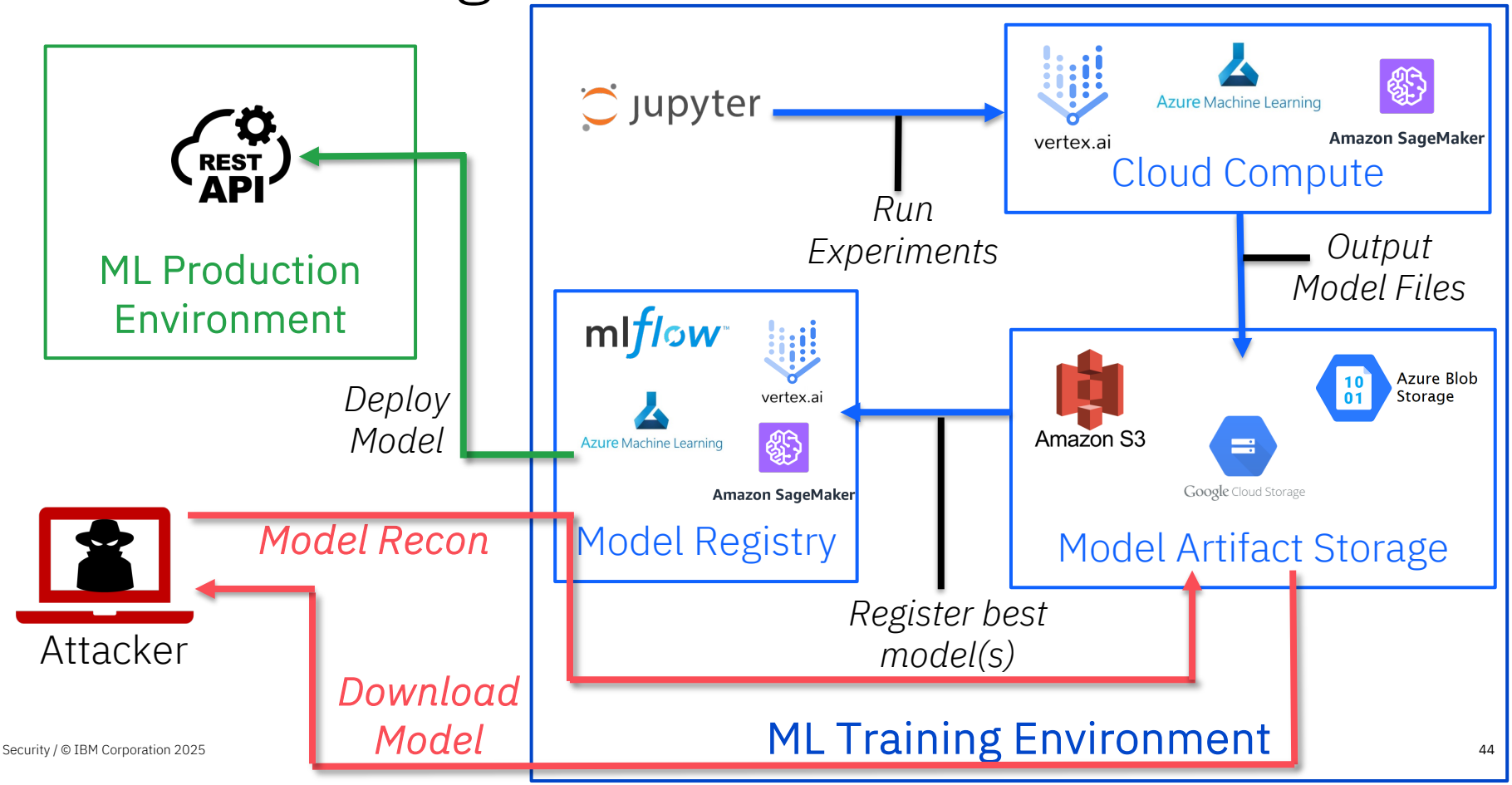
Model Poisoning – Code Execution



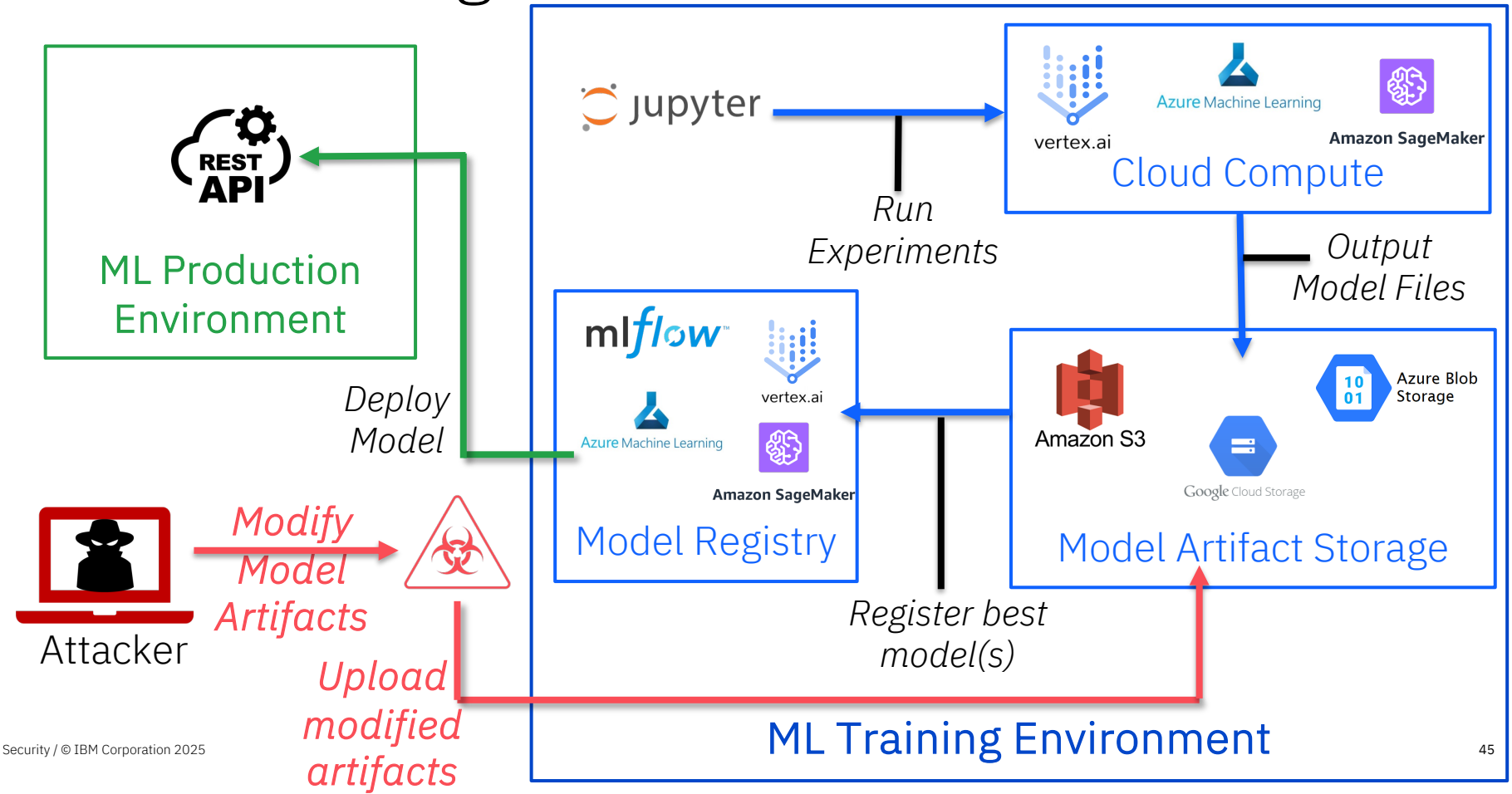
Model Poisoning – Code Execution



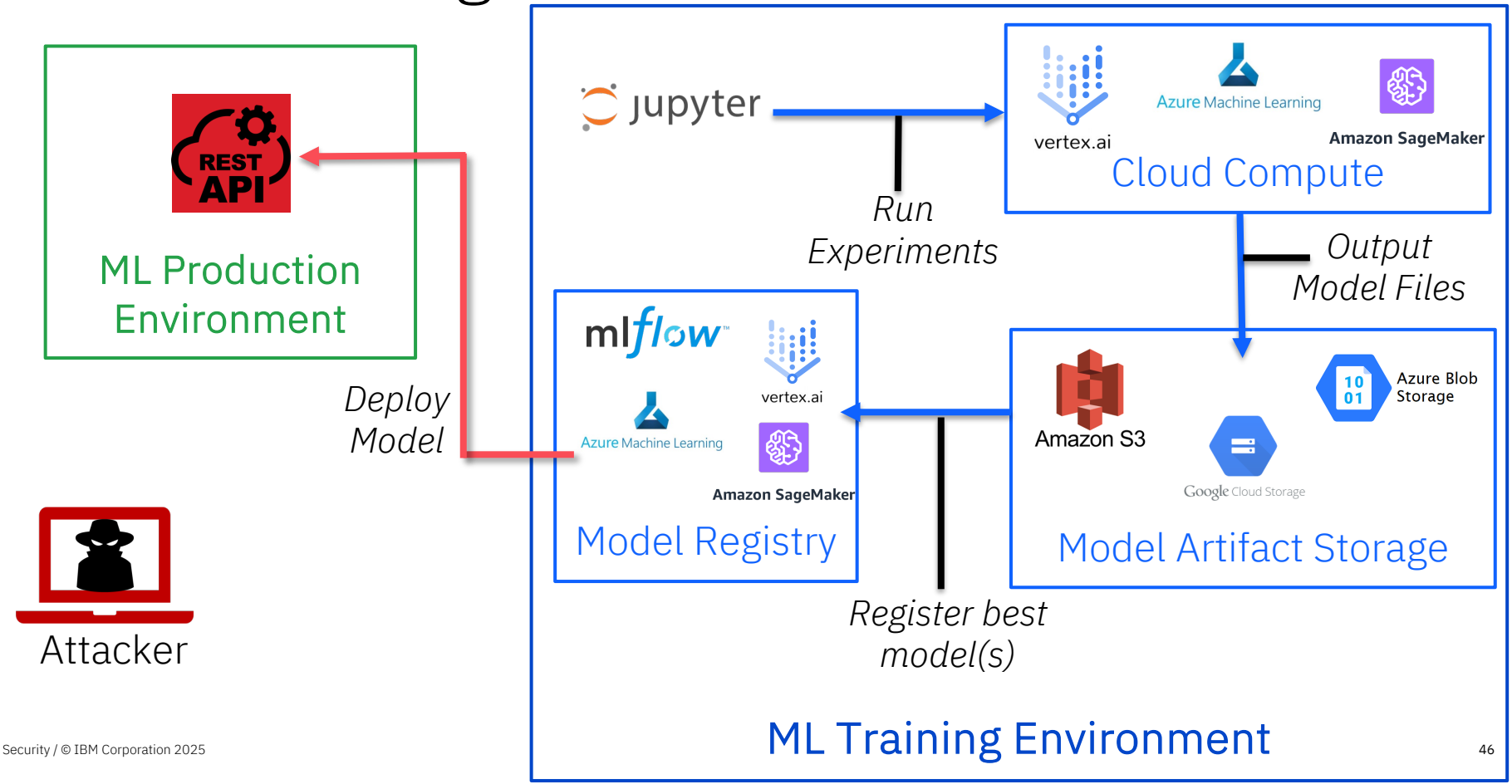
Model Poisoning – Code Execution



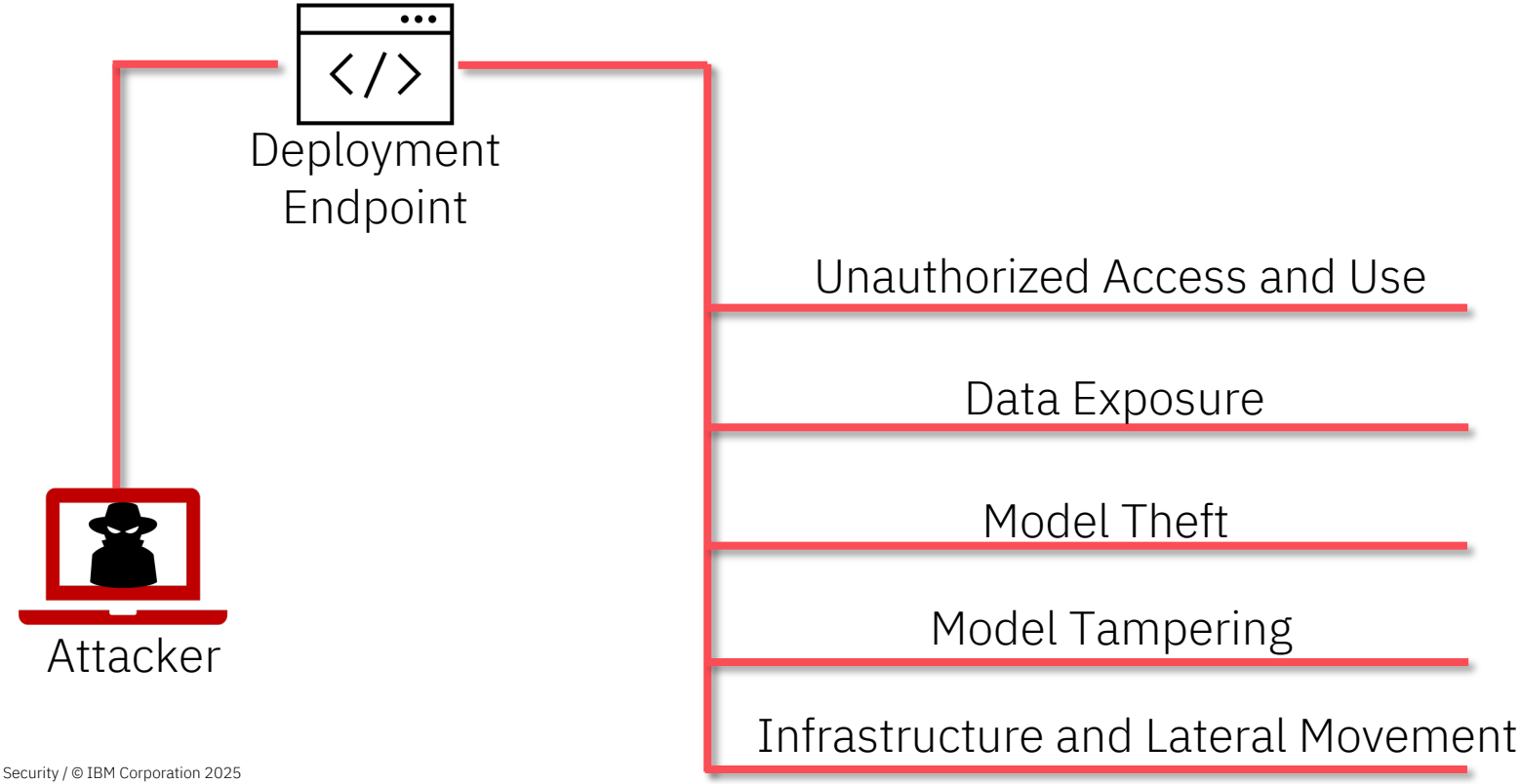
Model Poisoning – Code Execution



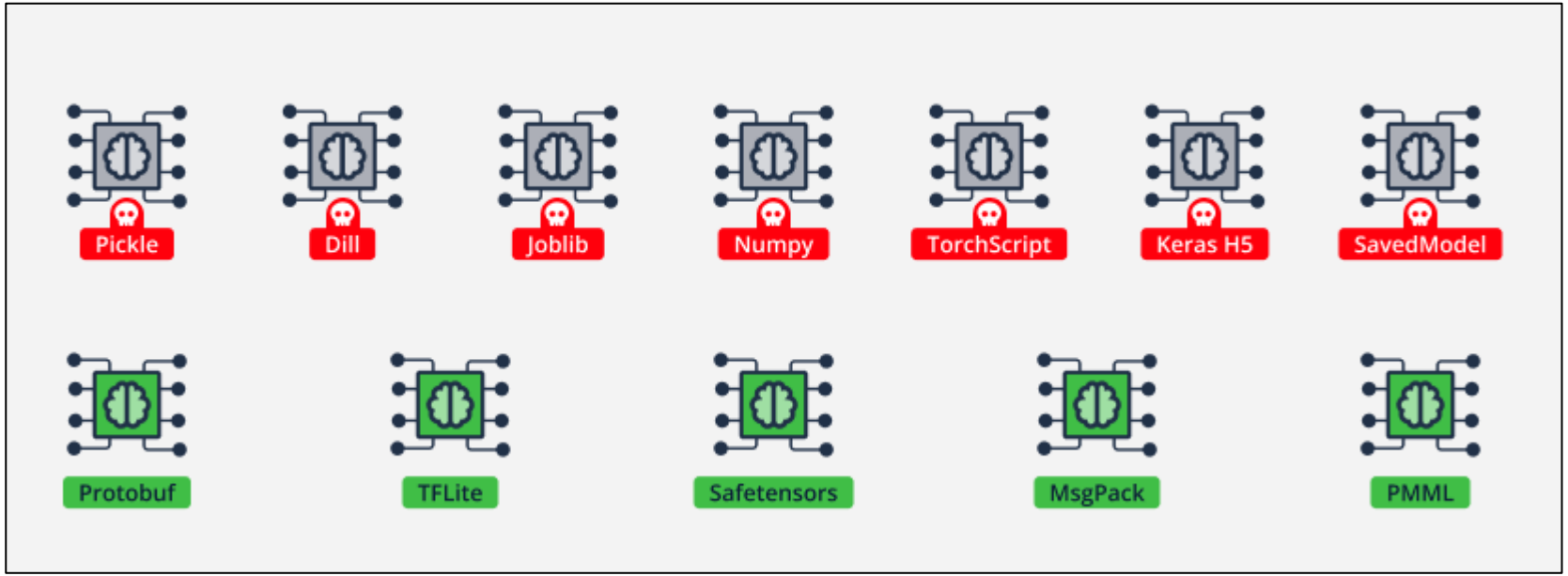
Model Poisoning – Code Execution



Model Poisoning – Code Execution - Impact



Model Formats – Support Code Execution on Load



https://jfrog.com/blog/from-mlops-to-mloops-exposing-the-attack-surface-of-machine-learning-platforms/

Creating Malicious Models for Code Execution

- MaliciousPickles - https://github.com/coldwaterq/MaliciousPickles
- Charcuterie - https://github.com/moohax/Charcuterie
- Fickling - https://github.com/trailofbits/fickling
- HiddenPickle - https://github.com/hiddenlayerai/HiddenPickle

MLOKit

github.com/xforcered/MLOKit

```
[*] INFO: Performing download-model module for sagemaker

[*] INFO: Checking credentials provided

[+] SUCCESS: Credentials are valid

                                        Model Name |        Creation Date
-------------------------------------------------------------------------------
                              employee-salary-model |            1/22/2025

[*] INFO: Downloading model artifacts

[*] INFO: Model artifacts location

s3://sagemaker-us-east-2-339713155979/Canvas/default-20250121T171825/Train:
1/model.tar.gz

[*] INFO: Checking access to S3 bucket with name: sagemaker-us-east-2-3397:

[+] SUCCESS: You have access to S3 bucket with name: sagemaker-us-east-2-3:

[*] INFO: Listing all files in prefix of: Canvas/default-20250121T171825/T:
-t1-1/

Canvas/default-20250121T171825/Training/output/Canvas1737498359380/sagemak

[*] INFO: Downloading file at: Canvas/default-20250121T171825/Training/out
.tar.gz

[+] SUCCESS: model.tar.gz written to: C:\Demo\MLOKit-OiEJQGbz
```

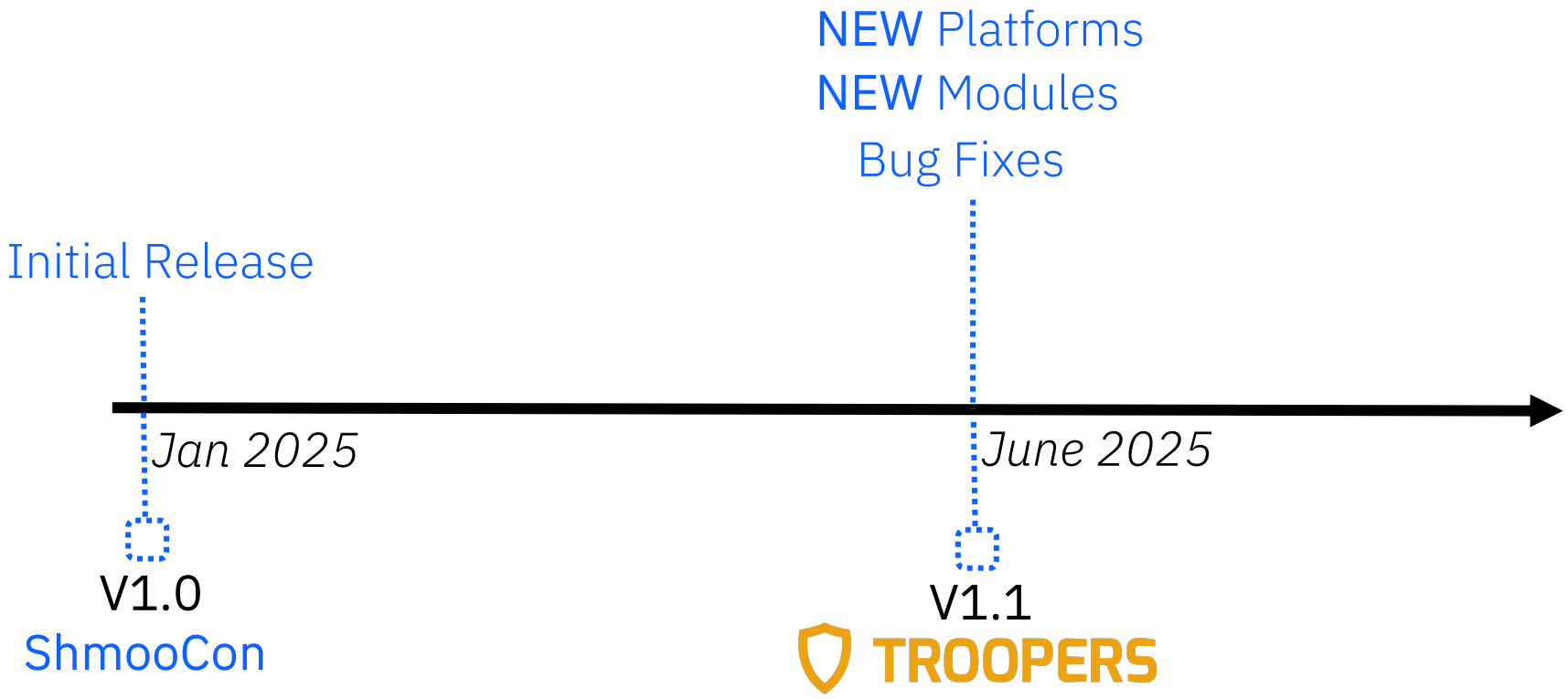
REST API Abuse
Conduct actions programmatically

Authentication
API Key, Access Token, Security Creds, User/Pass

9 Modules
Recon, Training Data Theft, Model Theft, Model Poisoning, Notebook Attacks

5 Supported Platforms
Azure ML, BigML, Vertex AI, MLFlow, SageMaker

MLOKit - History

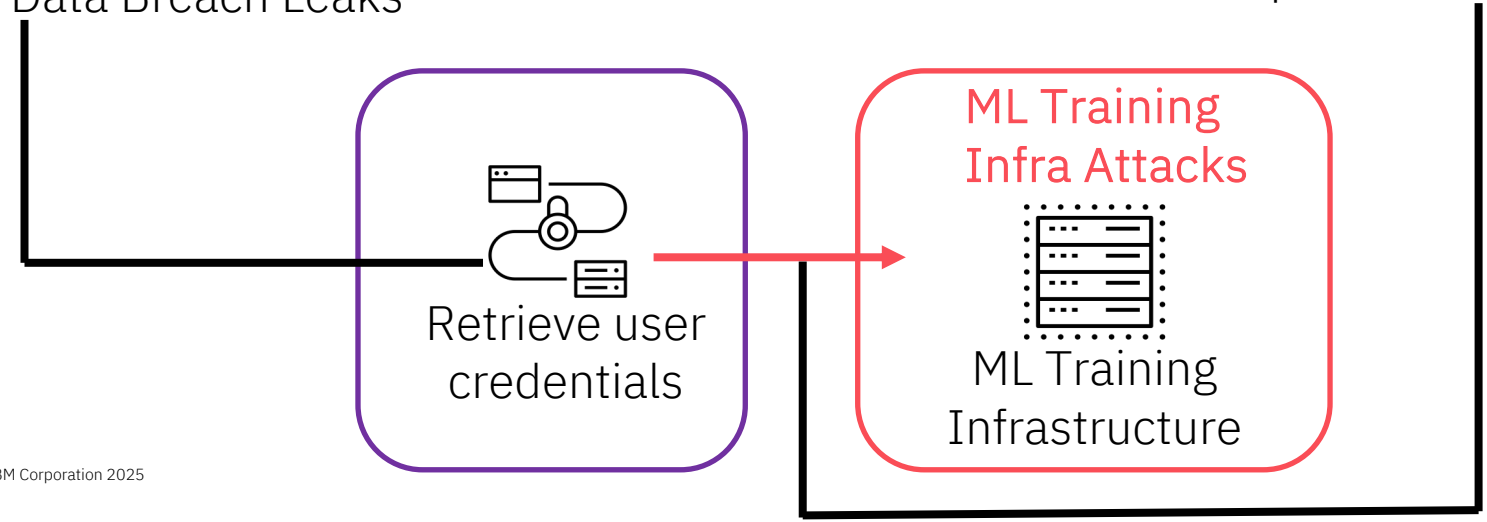


Demos: Attack Scenarios

Obtaining Credentials

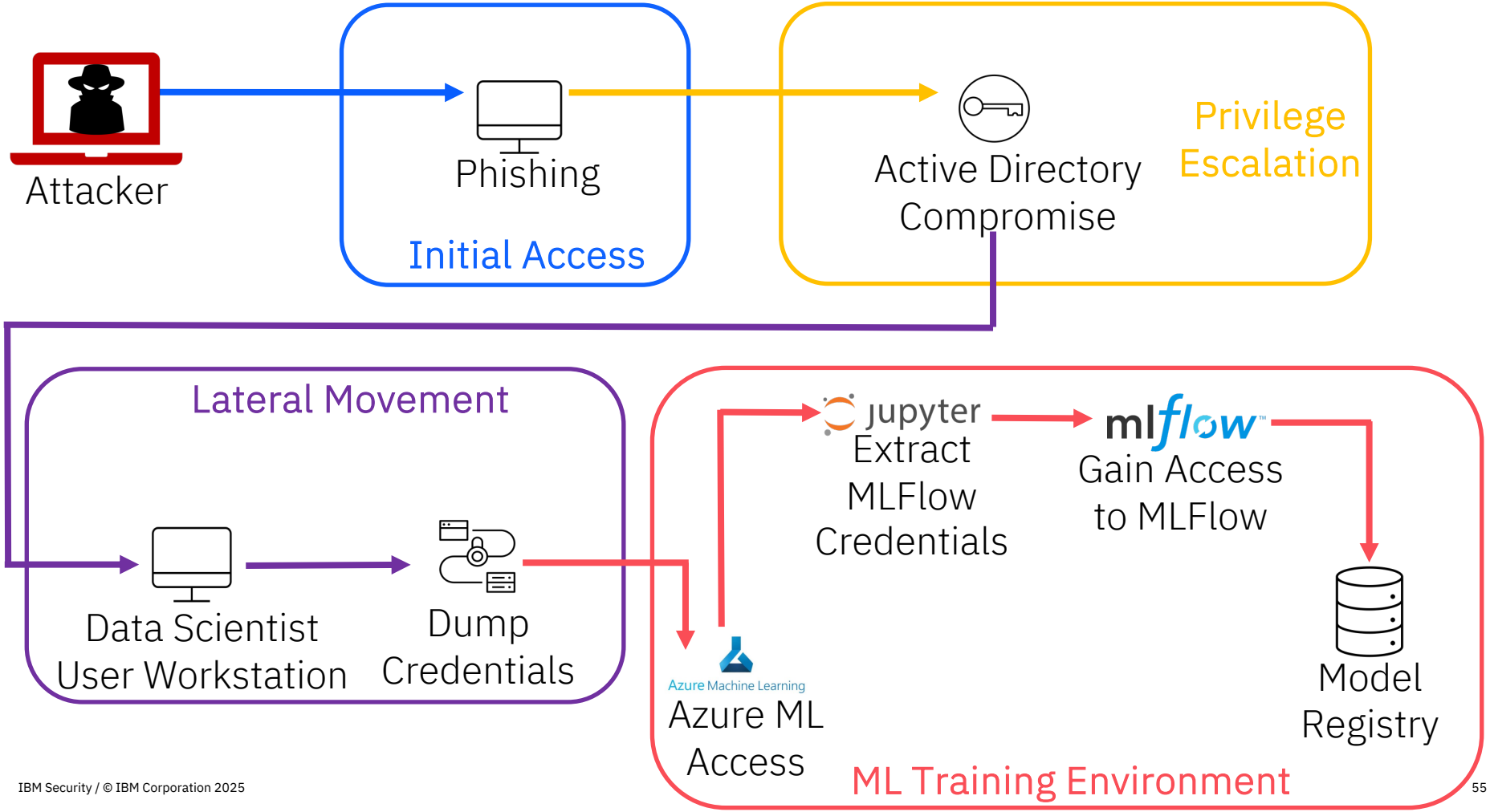
File Shares
Intranet Sites (e.g., internal wikis)
User Workstations
Social Engineering
Public Resources (e.g., Code Repos)
Unauthenticated Access
Public Data Breach Leaks

This research focuses on attack paths possible from here



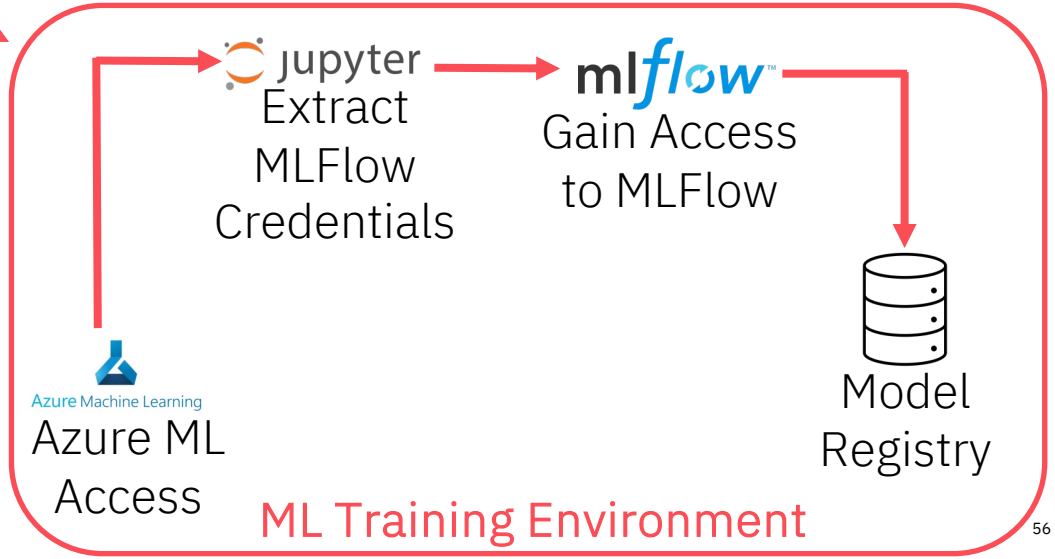
Demos: Attack Scenarios

#1: MLFlow - Initial Access and Model Theft from Model Registry
#2: SageMaker - Lateral Movement from SCM System to Cloud Compute
#3: SageMaker - Lateral Movement to Cloud Compute using Malicious Lifecycle Configuration
#4: SageMaker - Model Theft from Model Registry
#5: SageMaker - Model Poisoning to gain Code Execution
#6: Azure ML - Model Poisoning to gain Code Execution


Attacker
Phishing
Initial Access
Active Directory
Compromise
Privilege
Escalation
Lateral Movement
Data Scientist
User Workstation
Dump
Credentials
jupyter
Extract
MLFlow
Credentials
mlflow
Gain Access
to MLFlow
Azure Machine Learning
Azure ML
Access
Model
Registry
ML Training Environment

Attacker

Demo



Command Prompt

```
C:\Demo>
```

Demos: Attack Scenarios

#1: MLFlow - Initial Access and Model Theft from Model Registry

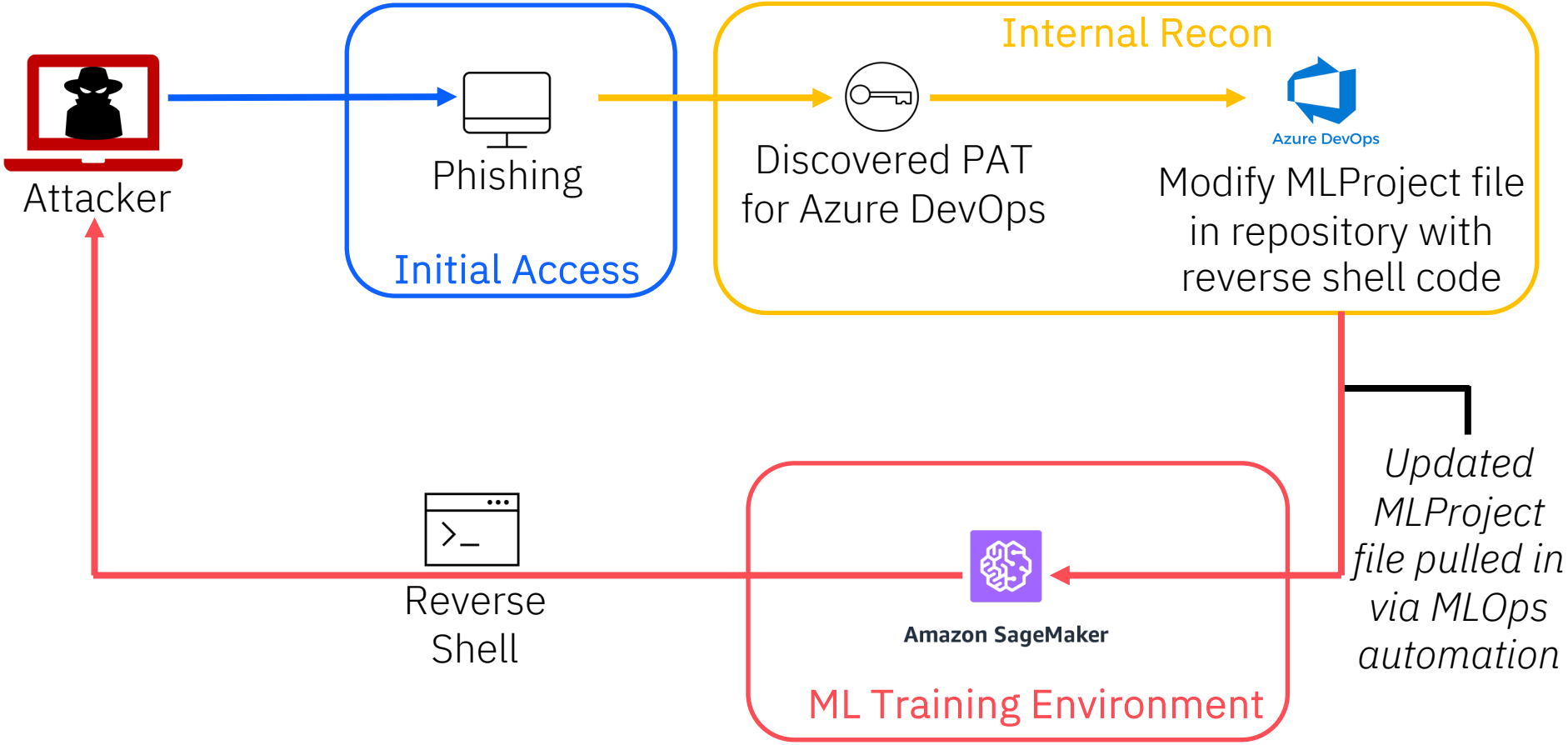
#2: SageMaker - Lateral Movement from SCM System to Cloud Compute

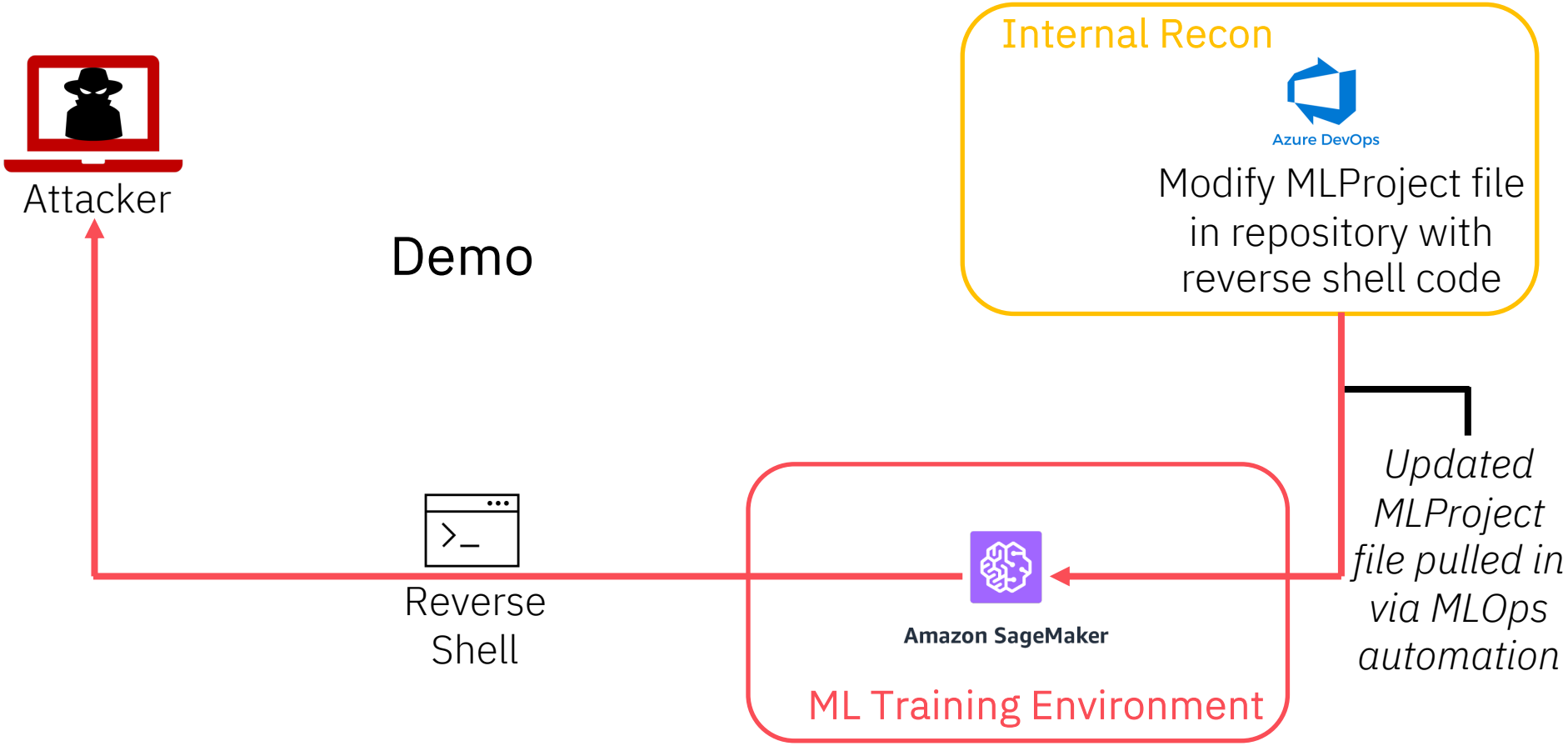
#3: SageMaker - Lateral Movement to Cloud Compute using Malicious Lifecycle Configuration

#4: SageMaker - Model Theft from Model Registry

#5: SageMaker - Model Poisoning to gain Code Execution

#6: Azure ML - Model Poisoning to gain Code Execution


Attacker
Phishing
Initial Access
Internal Recon
Discovered PAT for Azure DevOps
Azure DevOps
Modify MLProject file in repository with reverse shell code
Updated MLProject file pulled in via MLOps automation
Reverse Shell
Amazon SageMaker
ML Training Environment


Attacker
Demo
Internal Recon
Azure DevOps
Modify MLProject file in repository with reverse shell code
Updated MLProject file pulled in via MLOps automation
Reverse Shell
Amazon SageMaker
ML Training Environment

hawk@research-box: ~/demo

hawk@research-box: ~/demo

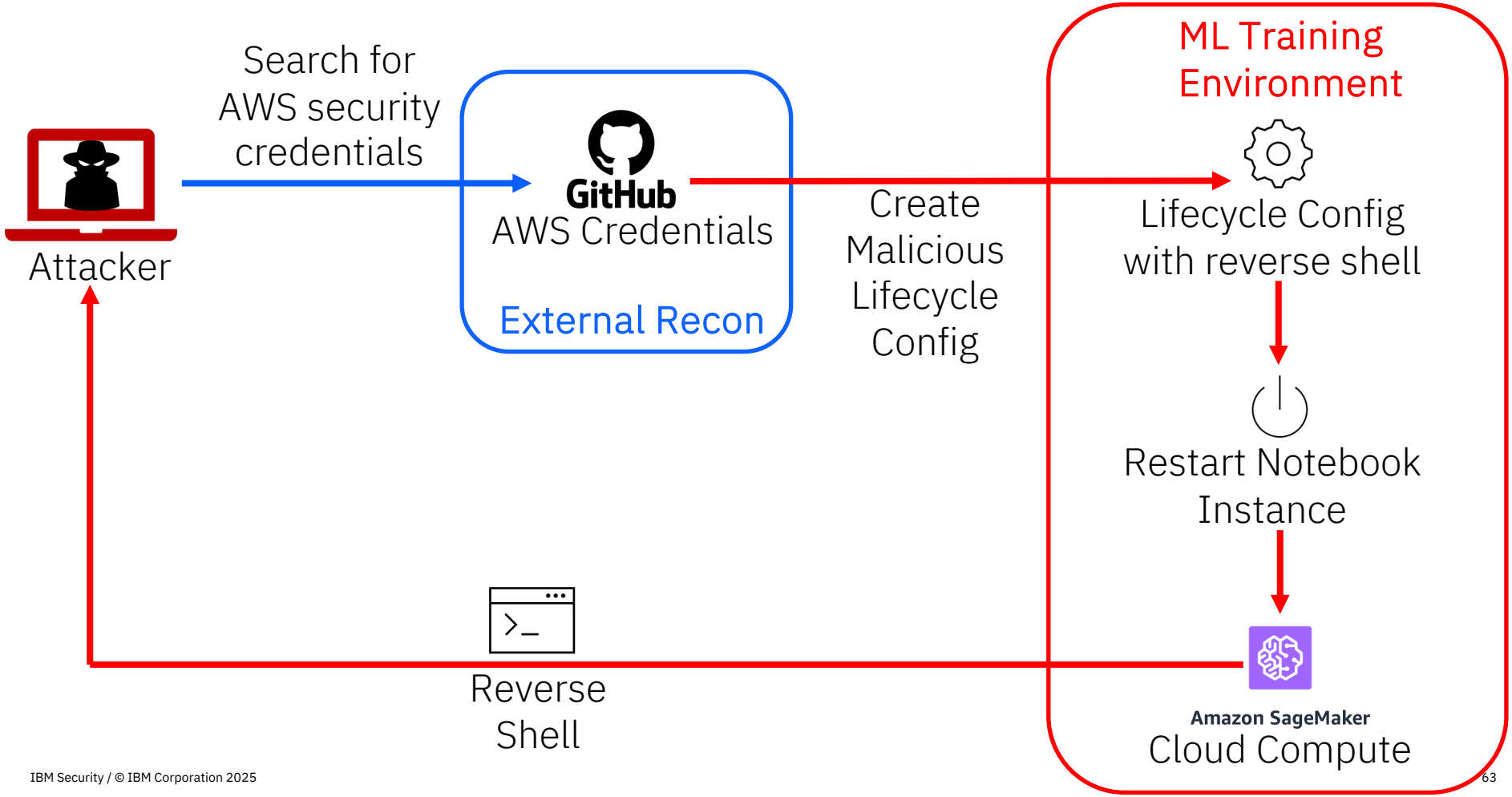
ubuntu@ip-172-31-1-70: ~

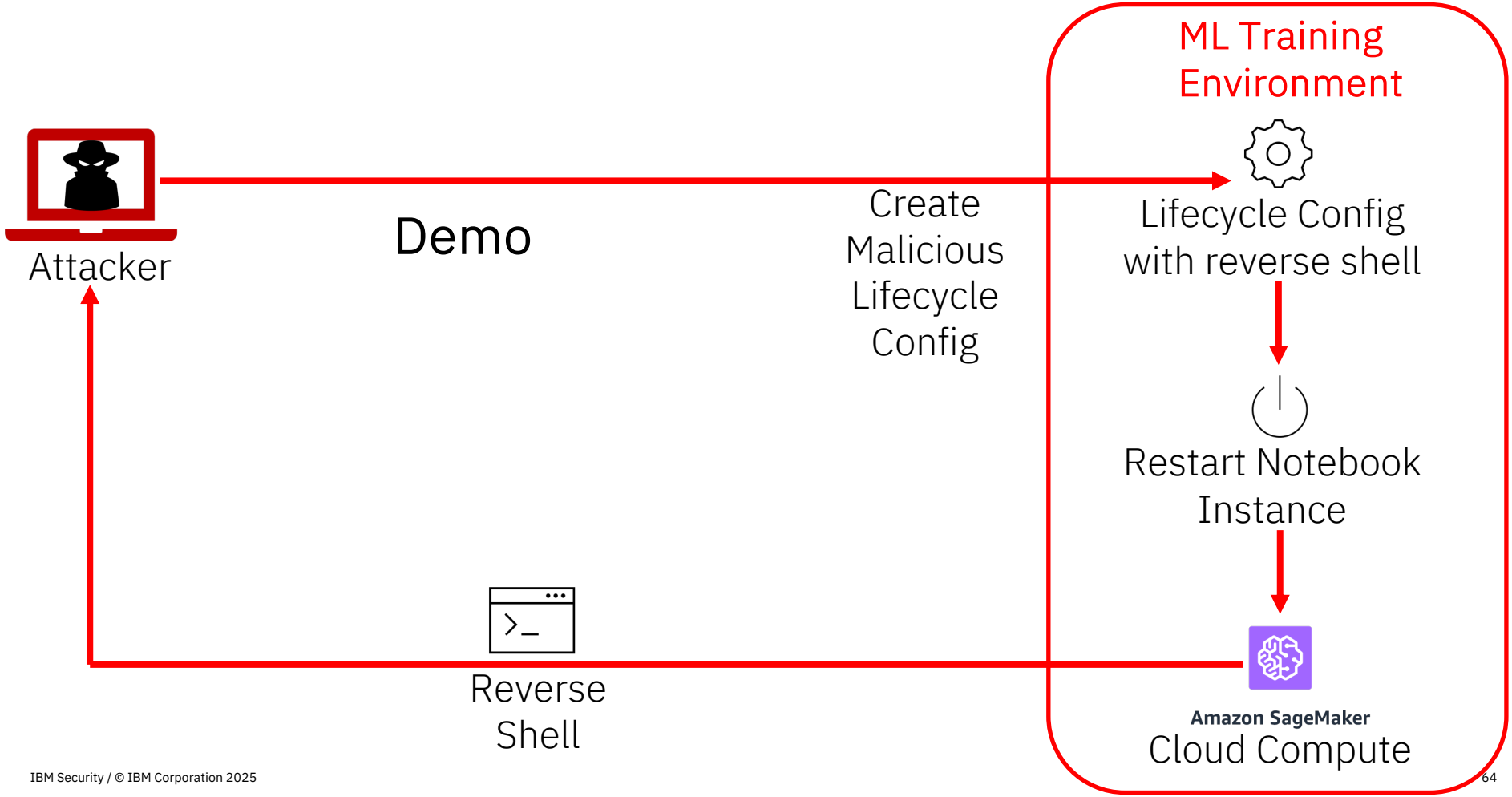
```
hawk@research-box:~/demo$
```

Clone ML training code repo using stolen PAT

Demos: Attack Scenarios

#1: MLFlow - Initial Access and Model Theft from Model Registry
#2: SageMaker - Lateral Movement from SCM System to Cloud Compute
#3: SageMaker - Lateral Movement to Cloud Compute using Malicious Lifecycle Configuration
#4: SageMaker - Model Theft from Model Registry
#5: SageMaker - Model Poisoning to gain Code Execution
#6: Azure ML - Model Poisoning to gain Code Execution


Search for AWS security credentials
Attacker
GitHub
AWS Credentials
External Recon
Create Malicious Lifecycle Config
ML Training Environment
Lifecycle Config with reverse shell
Restart Notebook Instance
Amazon SageMaker
Cloud Compute
Reverse Shell

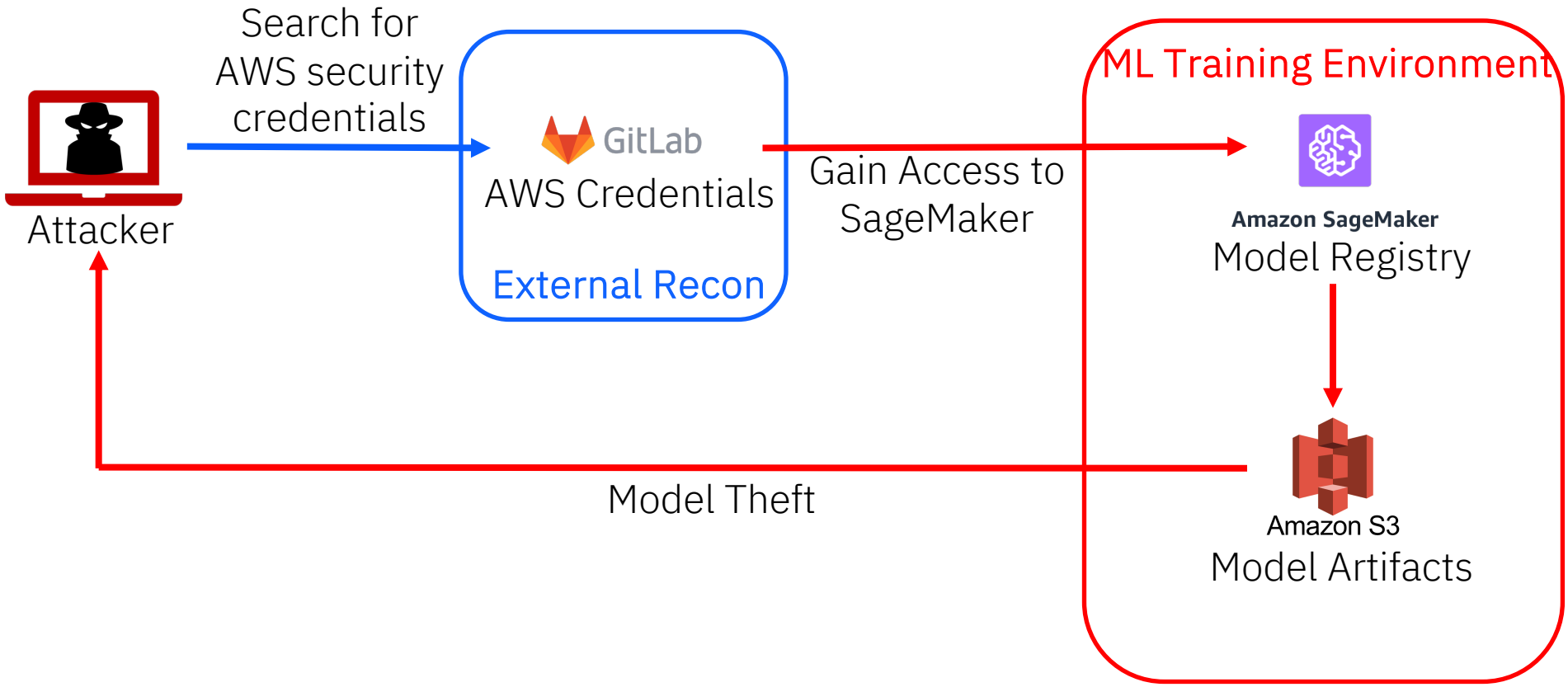

ML Training Environment
Attacker
Demo
Create Malicious Lifecycle Config
Lifecycle Config with reverse shell
Restart Notebook Instance
Reverse Shell
Amazon SageMaker
Cloud Compute

Command Prompt

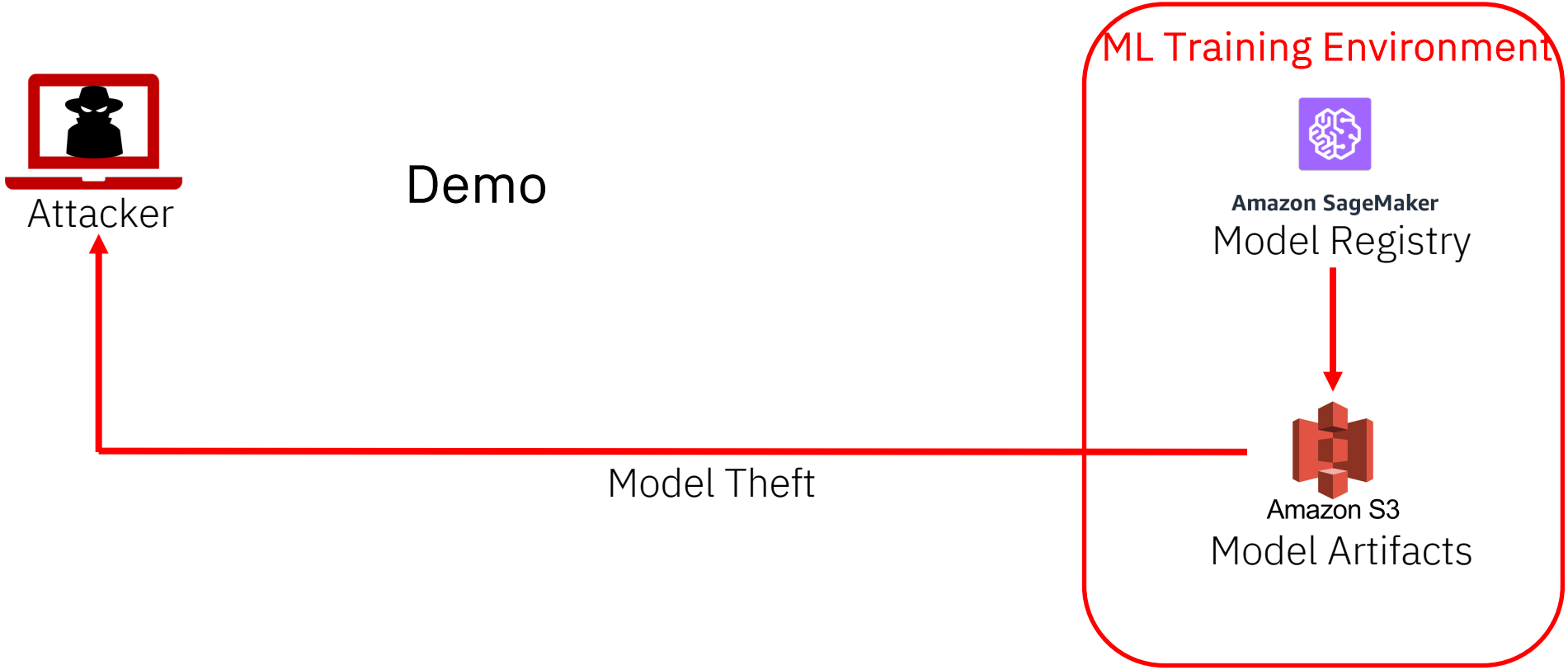
```
C:\Demo>
```

Demos: Attack Scenarios

#1: MLFlow - Initial Access and Model Theft from Model Registry
#2: SageMaker - Lateral Movement from SCM System to Cloud Compute
#3: SageMaker - Lateral Movement to Cloud Compute using Malicious Lifecycle Configuration
#4: SageMaker - Model Theft from Model Registry
#5: SageMaker - Model Poisoning to gain Code Execution
#6: Azure ML - Model Poisoning to gain Code Execution


Search for
AWS security
credentials
Attacker
GitLab
AWS Credentials
External Recon
Gain Access to
SageMaker
ML Training Environment
Amazon SageMaker
Model Registry
Amazon S3
Model Artifacts
Model Theft

Demo

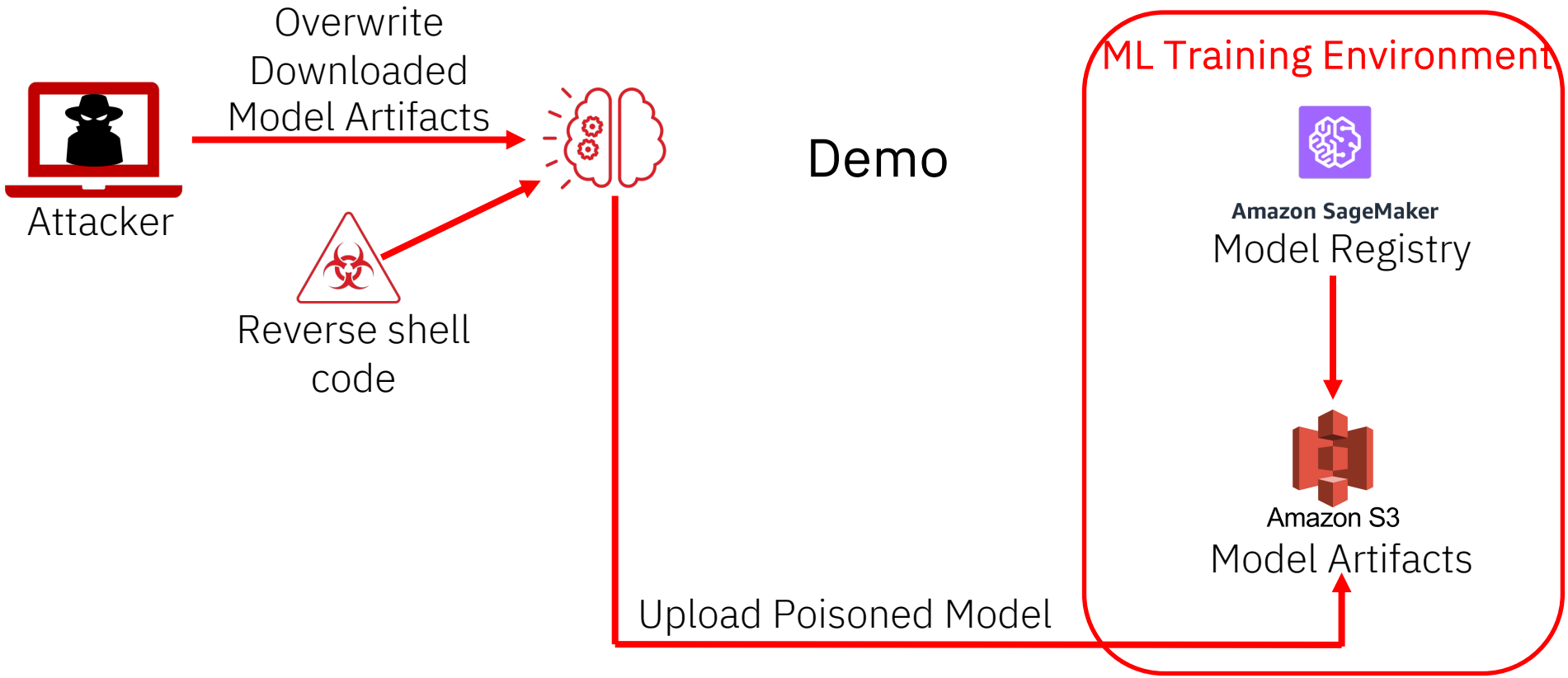

Attacker
ML Training Environment
Amazon SageMaker
Model Registry
Amazon S3
Model Artifacts
Model Theft

Command Prompt

```
C:\Demo>
```

Demos: Attack Scenarios

#1: MLFlow - Initial Access and Model Theft from Model Registry
#2: SageMaker - Lateral Movement from SCM System to Cloud Compute
#3: SageMaker - Lateral Movement to Cloud Compute using Malicious Lifecycle Configuration
#4: SageMaker - Model Theft from Model Registry
#5: SageMaker - Model Poisoning to gain Code Execution
#6: Azure ML - Model Poisoning to gain Code Execution


Overwrite
Downloaded
Model Artifacts
Attacker
Reverse shell
code
Demo
ML Training Environment
Amazon SageMaker
Model Registry
Amazon S3
Model Artifacts
Upload Poisoned Model

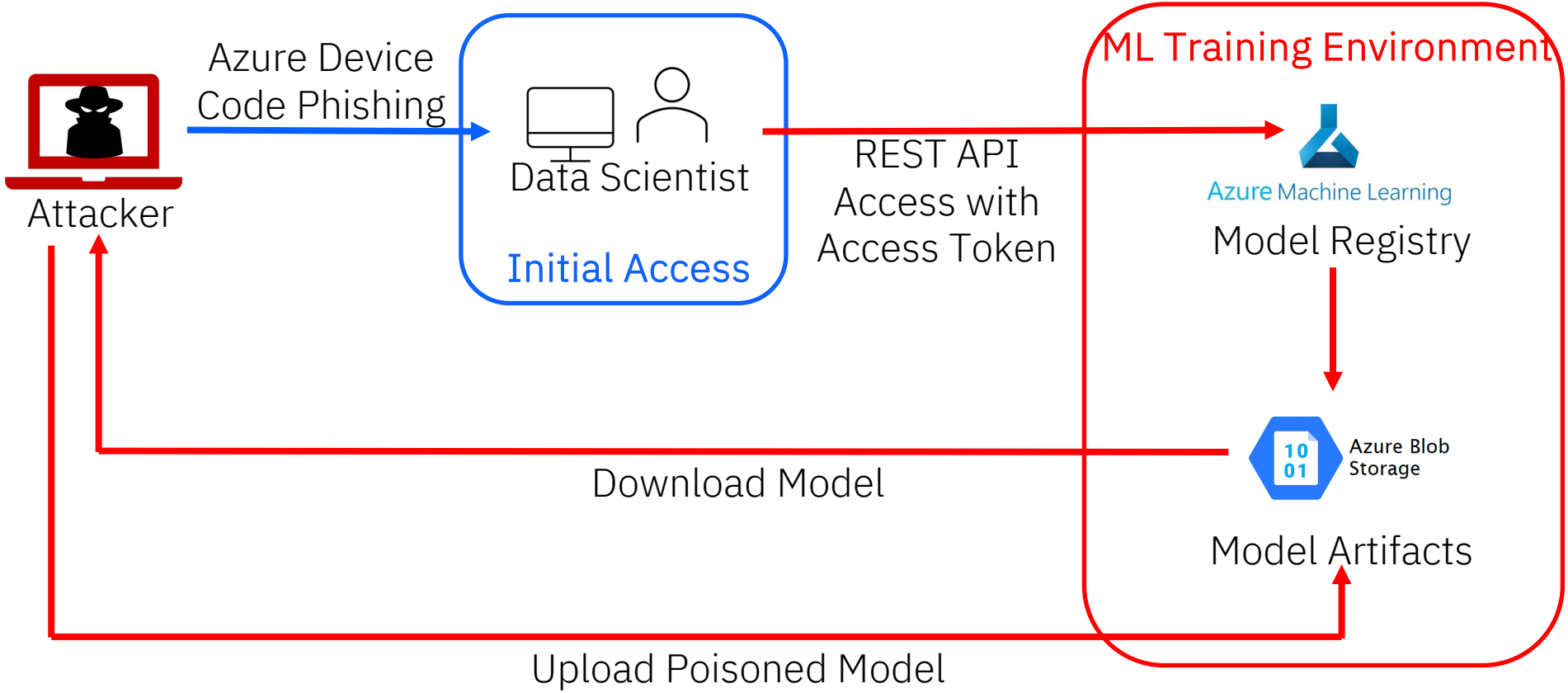
Command Prompt

```
C:\Demo>
```

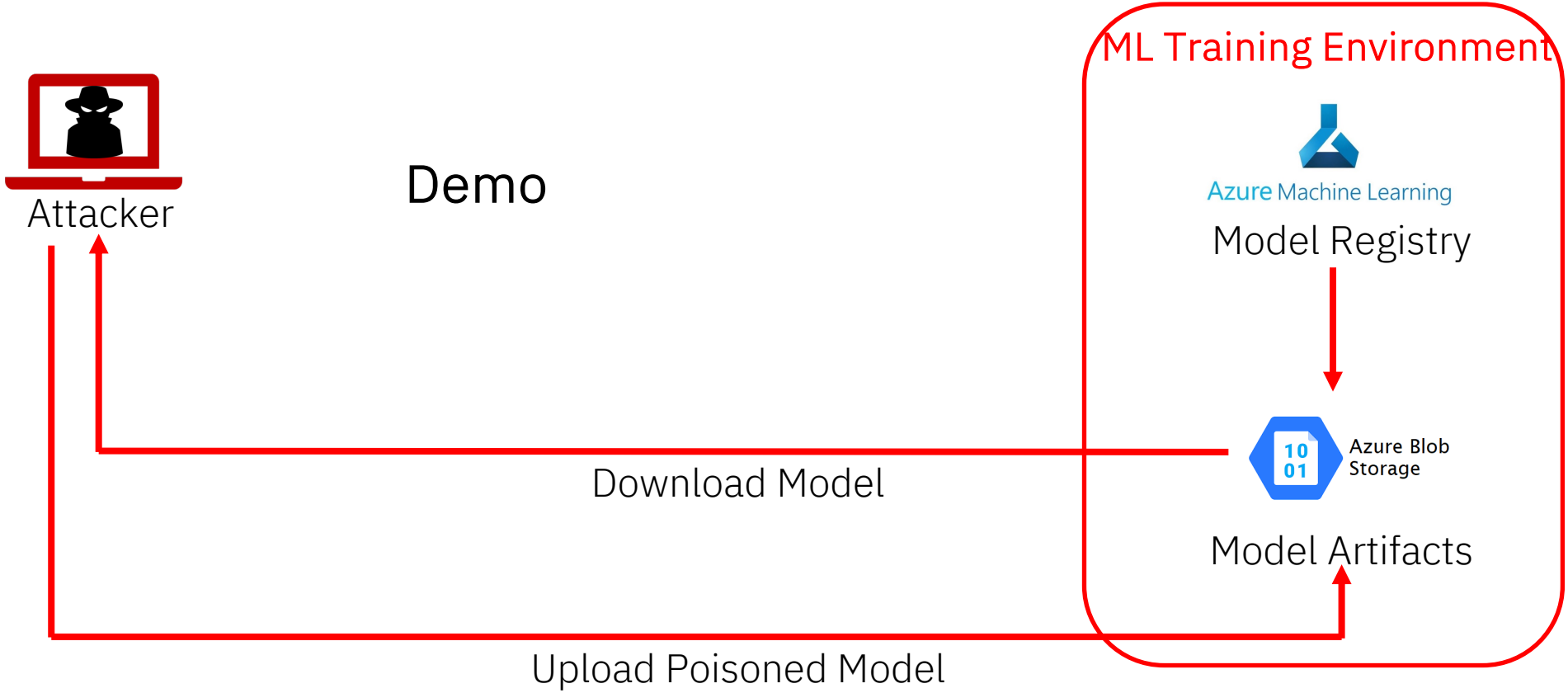
Showing model artifacts of model we previously downloaded

Demos: Attack Scenarios

#1: MLFlow - Initial Access and Model Theft from Model Registry
#2: SageMaker - Lateral Movement from SCM System to Cloud Compute
#3: SageMaker - Lateral Movement to Cloud Compute using Malicious Lifecycle Configuration
#4: SageMaker - Model Theft from Model Registry
#5: SageMaker - Model Poisoning to gain Code Execution
#6: Azure ML - Model Poisoning to gain Code Execution


Azure Device
Code Phishing
Attacker
Data Scientist
Initial Access
REST API
Access with
Access Token
ML Training Environment
Azure Machine Learning
Model Registry
Azure Blob
Storage
Model Artifacts
Download Model
Upload Poisoned Model

Demo


ML Training Environment
Attacker
Azure Machine Learning
Model Registry
Azure Blob Storage
Model Artifacts
Download Model
Upload Poisoned Model

C:\Users\hawk\Desktop\Demo.txt - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

Demo.txt | poison_model.py

```
===Azure ML===

MLOKit.exe check /platform:azureml /credential:%CRED%

MLOKit.exe list-projects /platform:azureml /subscription-id:47c5aaab-dbda-44ca-802e-00

MLOKit.exe list-models /platform:azureml /credential:%CRED% /subscription-id:47c5aaab-

MLOKit.exe download-model /platform:azureml /credential:%CRED% /subscription-id:47c5aa

MLOKit.exe poison-model /platform:azureml /credential:%CRED% /subscription-id:47c5aaab
```

Normal text file | length : 886 lines : 28 | Ln : 7 Col : 12 Pos : 206 | Windows (CR LF) | UTF-8 | INS

Protecting ML Training Environments

Users

Use password management system

Separate admin account

Additional monitoring controls

Security Awareness Training

MFA enabled and in use

PATs with expiration dates

Azure Machine Learning

jupyter

Amazon S3

Amazon SageMaker

mlflow™

Azure Blob Storage

Notebook Environments

- Password protect notebook
- IP address restrictions
- Limits to kernel execution times
- Use virtual environment
- Run as non-root account
- No cleartext credentials/secrets

jupyter

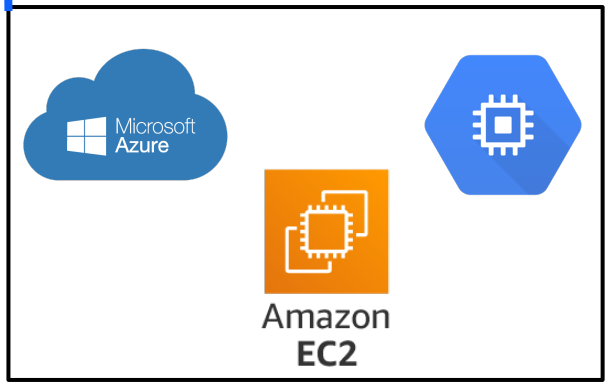
Cloud Compute

Enable auto-shutdown and auto-start schedule

Delete compute if no longer needed

Disable unneeded services

Configure role-based access



Model Artifact Storage and Registry

- Cleanup/delete old model artifacts
- Restrict access to backend storage
- IP-address restrictions
- Enable logging and apply detection rules
- Implement model integrity verification

Azure Machine Learning

Amazon S3

Amazon SageMaker

mlflow™

Azure Blob Storage

Detection Guidance – Summary

Azure ML Detections

https://github.com/h4wkst3r/KQL-Queries

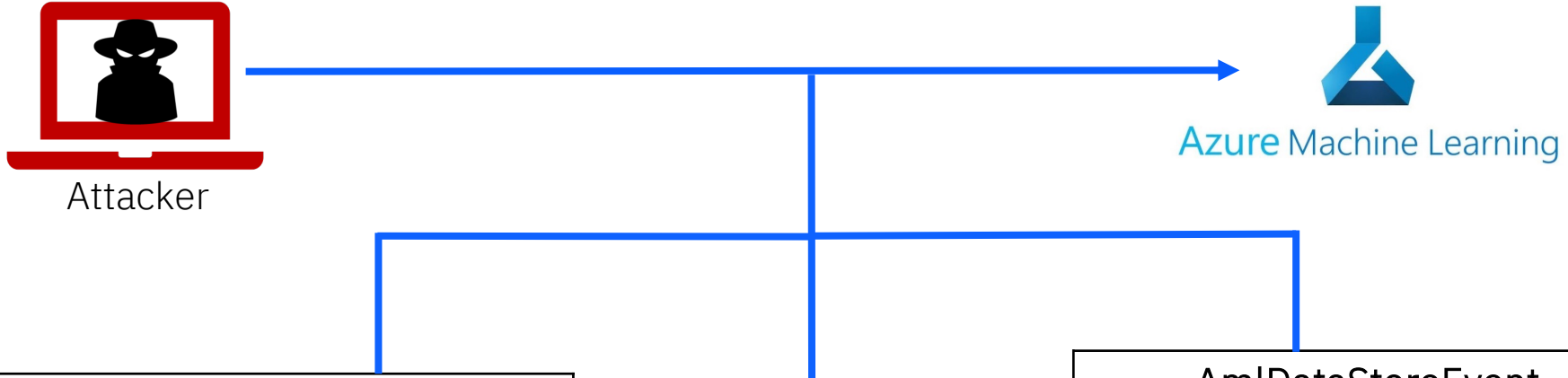
Dataset Poisoning
Dataset Recon
Dataset Theft
Model Poisoning
Model Recon
Model Theft

SageMaker Detections

https://github.com/h4wkst3r/CloudTrail-Queries

Model Poisoning
Model Theft
Malicious Lifecycle Config

Detection Guidance – Azure ML Model Poisoning

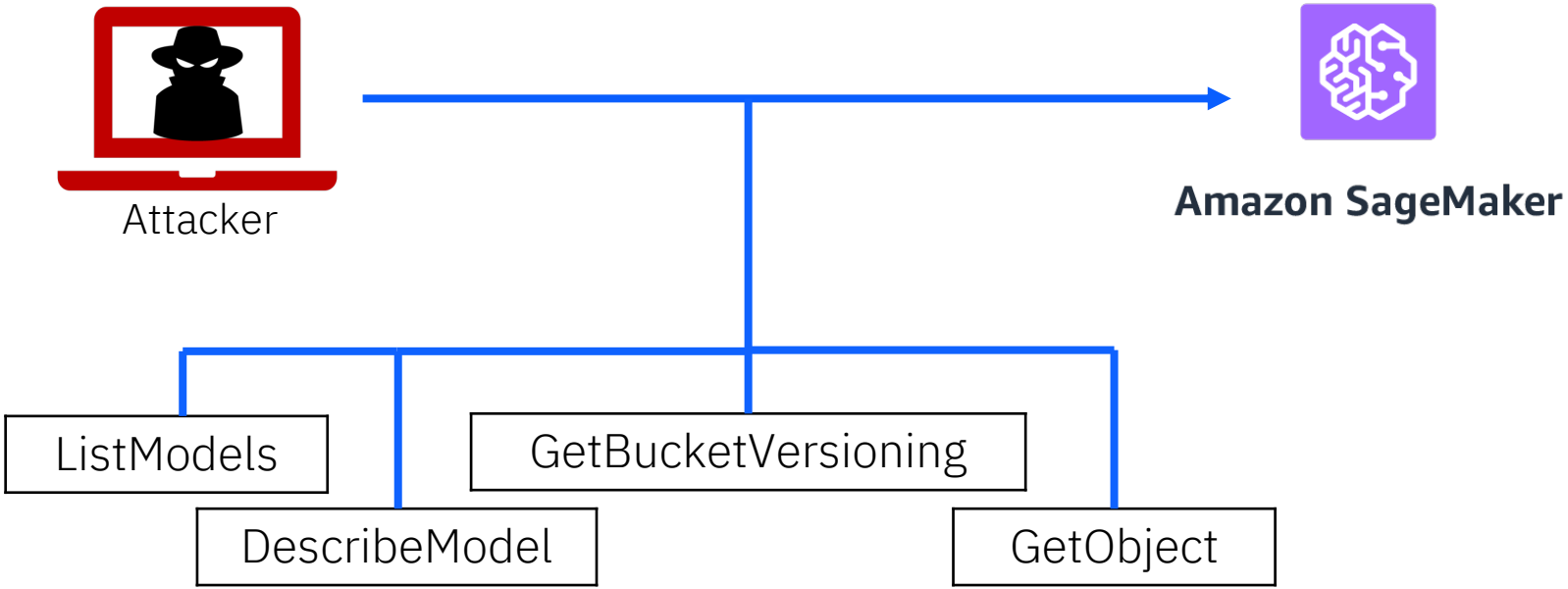


AmlModelsEvent
MICROSOFT. MACHINELEARNINGSERVICES/ WORKSPACES/Models/READ

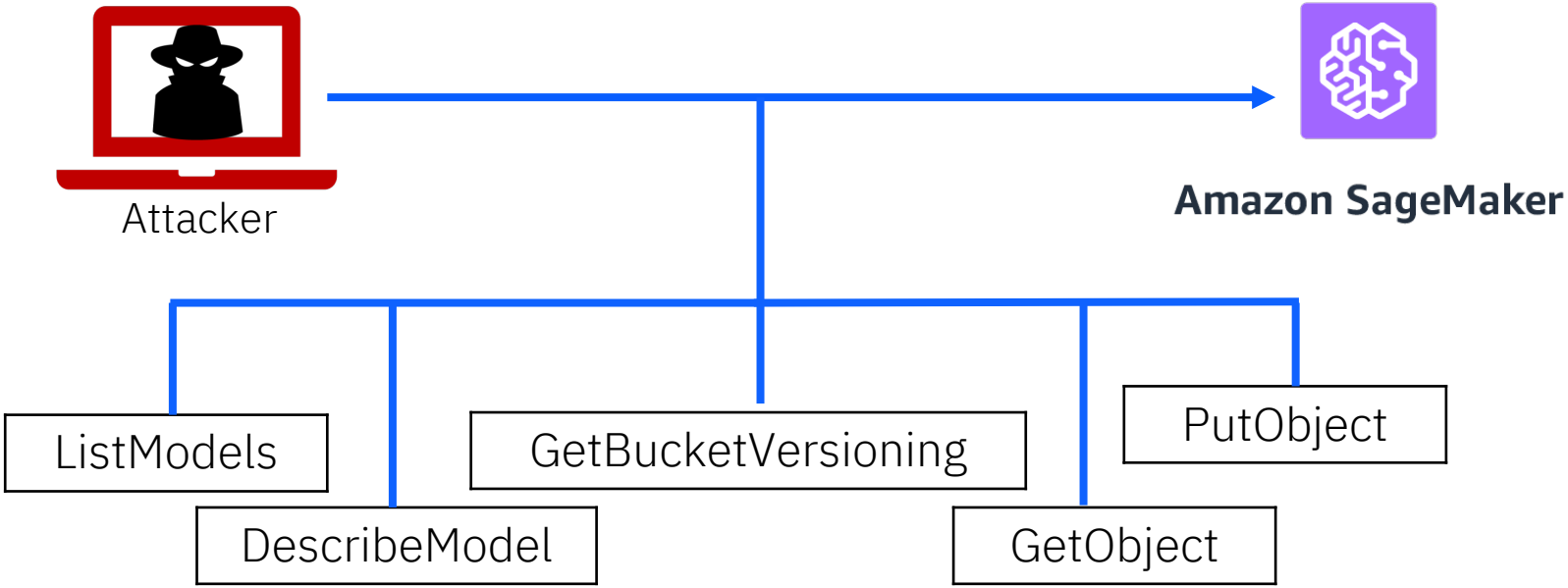
StorageBlobLogs
PutBlob AND GetBlob

AmlDataStoreEvent
MICROSOFT. MACHINELEARNINGSERVICES/ WORKSPACES/DATASTORES/ READ

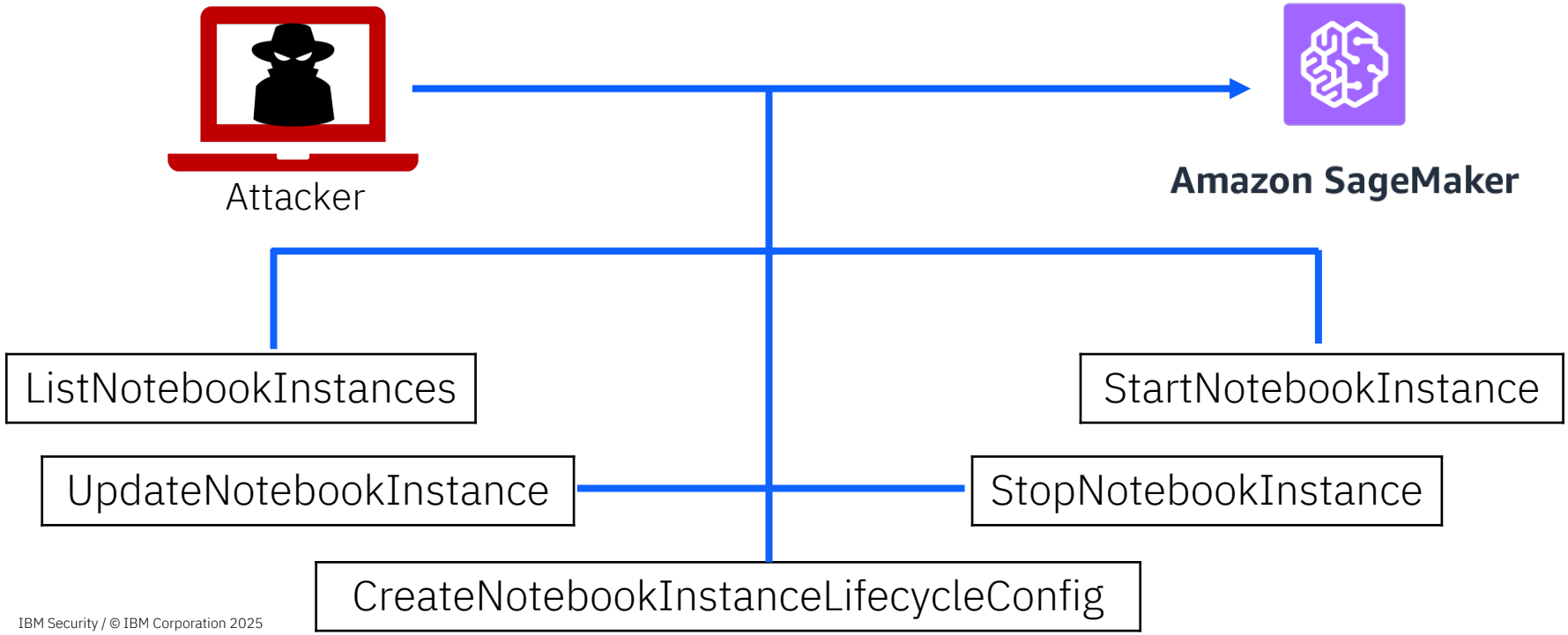
Detection Guidance – SageMaker Model Theft



Detection Guidance – SageMaker Model Poisoning



Detection Guidance – SageMaker Malicious Lifecycle Configuration



Detection Guidance – MLFlow

Attacker

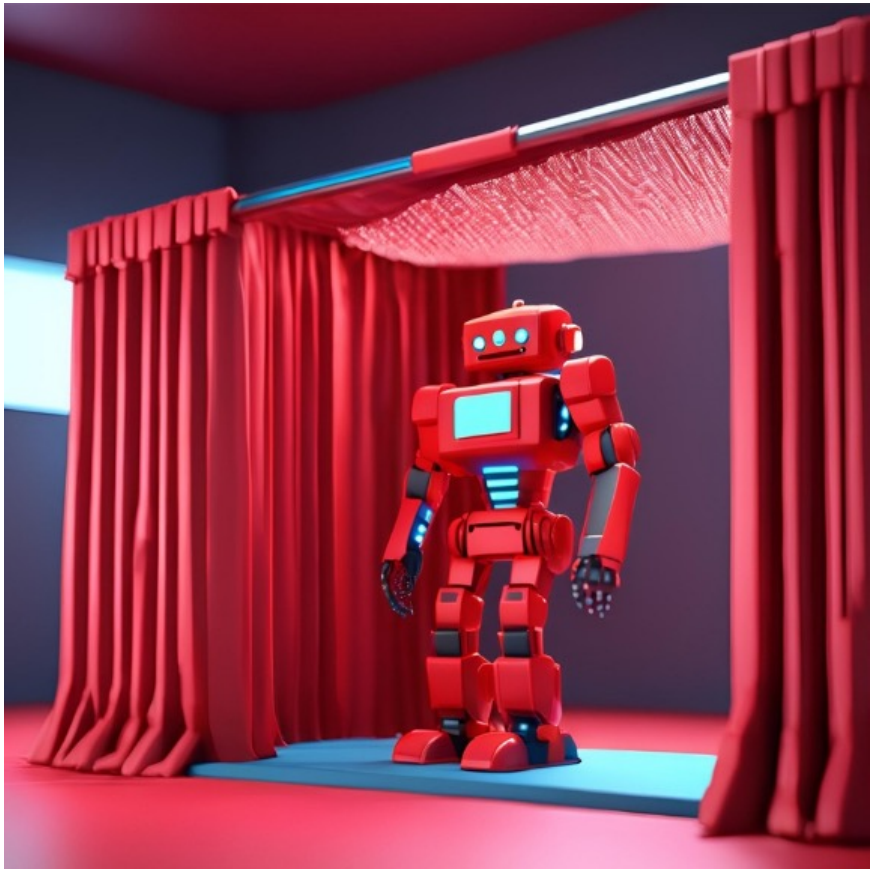
/api/2.0/mlflow/model-versions/search

/get-artifact

```
grep -i /api/2.0/mlflow/model-versions/search access.log
/2025:20:59:42 -0500] "GET /api/2.0/mlflow/model-versions/search HTTP/1.1" 200 904 "-" "MLOKit-e977ac02118a3cb2
/2025:20:59:42 -0500] "GET /api/2.0/mlflow/model-versions/search HTTP/1.1" 200 904 "-" "MLOKit-e977ac02118a3cb2
```

```
grep -i /get-artifact access.log
/2025:21:05:59 -0500] "GET /get-artifact?path=ElasticNet/code/data.py&run_id=f0b129a5e11c4bb6b1c0459a2f5ae7f6 HTTP/1.1" 200 0 "-" "MLOKit-e97
/2025:21:06:00 -0500] "GET /get-artifact?path=ElasticNet/code/params.py&run_id=f0b129a5e11c4bb6b1c0459a2f5ae7f6 HTTP/1.1" 200 0 "-" "MLOKit-e
/2025:21:06:01 -0500] "GET /get-artifact?path=ElasticNet/code/train.py&run_id=f0b129a5e11c4bb6b1c0459a2f5ae7f6 HTTP/1.1" 200 0 "-" "MLOKit-e9
/2025:21:06:01 -0500] "GET /get-artifact?path=ElasticNet/code/utils.py&run_id=f0b129a5e11c4bb6b1c0459a2f5ae7f6 HTTP/1.1" 200 0 "-" "MLOKit-e9
/2025:21:06:02 -0500] "GET /get-artifact?path=ElasticNet/conda.yaml&run_id=f0b129a5e11c4bb6b1c0459a2f5ae7f6 HTTP/1.1" 200 0 "-" "MLOKit-e977a
/2025:21:06:02 -0500] "GET /get-artifact?path=ElasticNet/input_example.json&run_id=f0b129a5e11c4bb6b1c0459a2f5ae7f6 HTTP/1.1" 200 0 "-" "MLOK
/2025:21:06:03 -0500] "GET /get-artifact?path=ElasticNet/model.pkl&run_id=f0b129a5e11c4bb6b1c0459a2f5ae7f6 HTTP/1.1" 200 0 "-" "MLOKit-e977ac
```

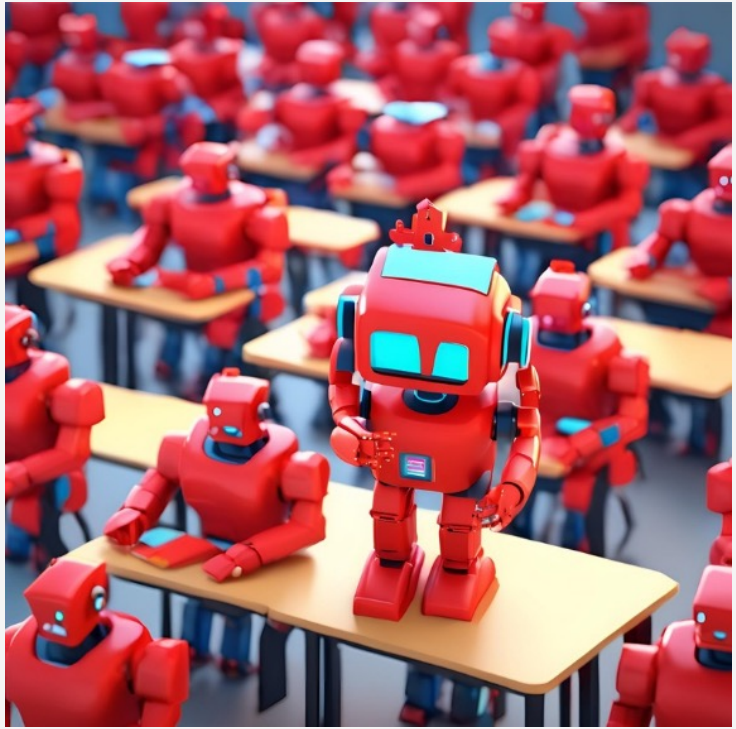
Conclusion



Conclusion

01	02	03
ML training environments contain highly sensitive and business critical data	We need to understand these systems so we can protect them	Unauthorized access to these environments could be significant

Questions?



Brett Hawkins
@h4wkst3r

Blog Post -

MLOKit Tool -

IBM

References

- https://twitter.com/retBandit
- https://twitter.com/h4wkst3r
- https://www.ibm.com/downloads/documents/us-en/11630e2cbc302316
- https://github.com/xforcered/MLOKit
- https://twitter.com/azarzaror
- https://web.archive.org/web/20241214000321/https:/www.panoptica.app/blog/protect-your-environment-when-working-with-amazon-sagemaker
- https://www.ibm.com/topics/mlops
- https://neptune.ai/blog/mlops-tools-platforms-landscape
- https://www.databricks.com/glossary/jupyter-notebook
- https://www.ibm.com/docs/en/z-devops-guide?topic=applications-source-code-management
- https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing
- https://mlflow.org/docs/latest/tracking/artifacts-stores.html

References

- https://wandb.ai/site/articles/what-is-an-ML-model-registry/
- https://learn.microsoft.com/en-us/azure/devops/user-guide/what-is-azure-devops
- https://about.gitlab.com/
- https://github.com/
- https://aws.amazon.com/sagemaker/
- https://learn.microsoft.com/en-us/azure/machine-learning/overview-what-is-azure-machine-learning
- https://mlflow.org/
- https://docs.aws.amazon.com/sagemaker/latest/dg/model-registry.html
- https://learn.microsoft.com/en-us/azure/machine-learning/how-to-manage-models?view=azureml-api-2&tabs=cli
- https://aws.amazon.com/s3/
- https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction
- https://www.ibm.com/services/adversary-simulation

References

- https://mlflow.org/docs/latest/rest-api.html
- https://learn.microsoft.com/en-us/azure/devops/organizations/accounts/use-personal-access-tokens-to-authenticate?view=azure-devops&tabs=Windows
- https://mlflow.org/docs/latest/projects.html
- https://github.com/xforcered/ADOKit
- https://aws.amazon.com/blogs/machine-learning/build-an-end-to-end-mlops-pipeline-using-amazon-sagemaker-pipelines-github-and-github-actions/
- https://docs.aws.amazon.com/IAM/latest/UserGuide/security-creds.html
- https://docs.aws.amazon.com/sagemaker/latest/dg/security-iam-awsmanpol.html
- https://docs.aws.amazon.com/sagemaker/latest/dg/nbi.html
- https://docs.aws.amazon.com/sagemaker/latest/dg/notebook-lifecycle-config.html
- https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-iam-awsmanpol.html
- https://jfrog.com/blog/from-mlops-to-mloops-exposing-the-attack-surface-of-machine-learning-platforms/

References

- https://docs.python.org/3/library/pickle.html
- https://gist.githubusercontent.com/h4wkst3r/2c30a3d39e20b7cd8606211ba3132d85/raw/e4e253b052f5b916134409fcb61b91c49b91d912/CreatePickle.py
- https://github.com/coldwaterq/MaliciousPickles
- https://github.com/moohax/Charcuterie
- https://github.com/trailofbits/fickling
- https://github.com/hiddenlayerai/HiddenPickle
- https://docs.aws.amazon.com/sagemaker/latest/dg/how-it-works-deployment.html
- https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/
- https://learn.microsoft.com/en-us/entra/identity-platform/access-tokens
- https://learn.microsoft.com/en-us/rest/api/azureml/
- https://learn.microsoft.com/en-us/azure/machine-learning/concept-workspace?view=azureml-api-2
- https://docs.gunicorn.org/en/stable/settings.html

References

- https://learn.microsoft.com/en-us/microsoft-365/enterprise/subscriptions-licenses-accounts-and-tenants-for-microsoft-cloud-offerings?view=o365-worldwide
- https://learn.microsoft.com/en-us/azure/machine-learning/concept-data?view=azureml-api-2
- https://learn.microsoft.com/en-us/azure/machine-learning/concept-endpoints?view=azureml-api-2
- https://blog.gitguardian.com/how-to-handle-secrets-in-jupyter-notebooks/
- https://medium.com/@techlatest.net/security-best-practices-for-ai-ml-in-jupyter-notebooks-a-blog-post-on-the-security-best-practices-c0e0659cfccb
- https://github.com/h4wkst3r/KQL-Queries
- https://github.com/h4wkst3r/CloudTrail-Queries
- http://www.ibm.com/downloads/documents/us-en/11630e2cbc302316
- https://github.com/aws-samples/aws-customer-playbook-framework/blob/main/docs/Responding to SageMaker.md
- https://aws.amazon.com/blogs/machine-learning/securing-mlflow-in-aws-fine-grained-access-control-with-aws-native-services/

References

- https://learn.microsoft.com/en-us/azure/storage/blobs/monitor-blob-storage?tabs=azure-portal
- https://learn.microsoft.com/en-us/azure/machine-learning/monitor-azure-machine-learning?view=azureml-api-2
- https://github.com/h4wkst3r/KQL-Queries/blob/main/AzureML/AzureMLModelPoisoning.kql
- https://github.com/h4wkst3r/CloudTrail-Queries/blob/main/SageMakerModelTheft.sql
- https://github.com/h4wkst3r/CloudTrail-Queries/blob/main/SageMakerModelPoisoning.sql
- https://github.com/h4wkst3r/CloudTrail-Queries/blob/main/SageMakerMaliciousLifecycleConfig.sql
- https://www.ibm.com/think/x-force/becoming-the-trainer-attacking-ml-training-infrastructure