AWS re:Invent

WPS402

Threat detection using artificial intelligence

Ankush Chowdhary
Principal Security Advisor
Amazon Web Services

Sirikarn Pukkawanna
Security Data Scientist
Amazon Web Services

AWS re:Invent

aws

Agenda

Workshop overview

Solution walkthrough

Understanding the AI-based Threat Detection framework

Prework and prerequisites

Workshop activities

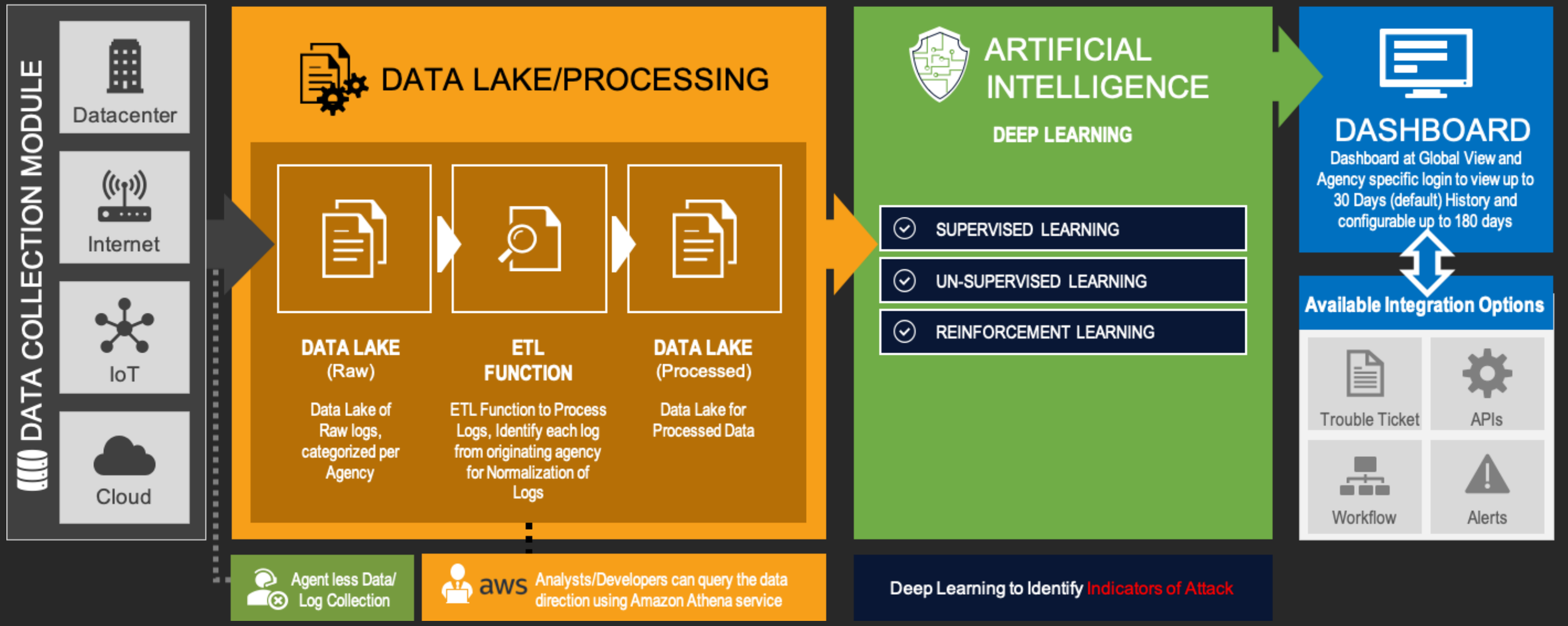
Workshop overview

- You will be using the “Threat Detection Using Artificial Intelligence” solution to detect attacks generated in a simulated environment running on AWS

- Learn to use the AI-based threat detection framework to simulate attacks, generate telemetry, test the data against ML models, and view the results on the dashboard

- Outcome: Using the threat detection solution and its accompanying framework, you can build ML-based detection models or improve the detection confidence of existing models packaged with the solution

Solution walkthrough



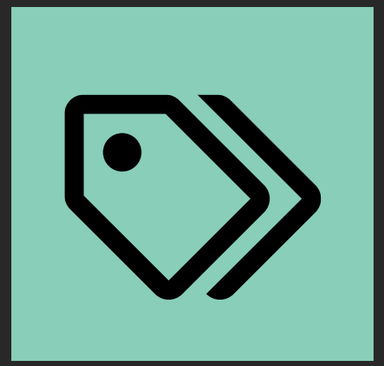
Demo

Understanding the AI-based Threat Detection framework

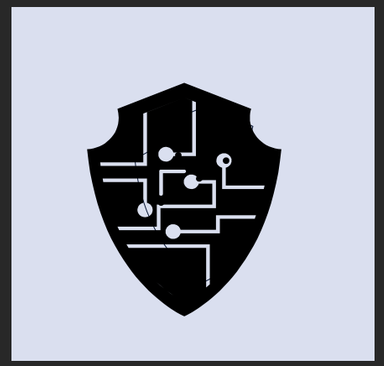
Simulated attack

Data generation/ collection

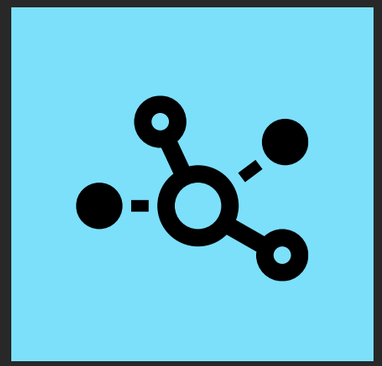
Data Lake/ ETL



Data labeling



Ml model build/test



Visualizing

Prework and prerequisites

- Individual laptops with internet connectivity
- Activate the AWS account provided to you (follow the instructions in the participant guide)
- Access your account and add yourself as a customer to the Threat Detection solution (refer to your participant guide)

Activity 1: Round 1

Activity 1: Attack simulation and display findings

- Round 1
  - Deploy the AWS CloudFormation template
  - Scan the environment
  - Navigate to the Threat Detection dashboard
  - View the findings on the analytics dashboard

Please refer to the participant guide

Activity 1: Round 2

Activity 1: Attack simulation and display findings

- Round 2
  - Run exploits on the identified vulnerabilities
  - Navigate to the Threat Detection dashboard
  - View the findings on the Deep Learning dashboard

Please refer to the participant guide

Activity 2

Activity 2: Build detection module

- Deploy AWS Lambda template
- Access logs for Amazon S3 bucket
- Search for findings in the logs
- Review findings in AWS Lambda console

Please refer to the participant guide

Q&A

Thank you!

AWS re:Invent

aws

Please complete the session survey in the mobile app.