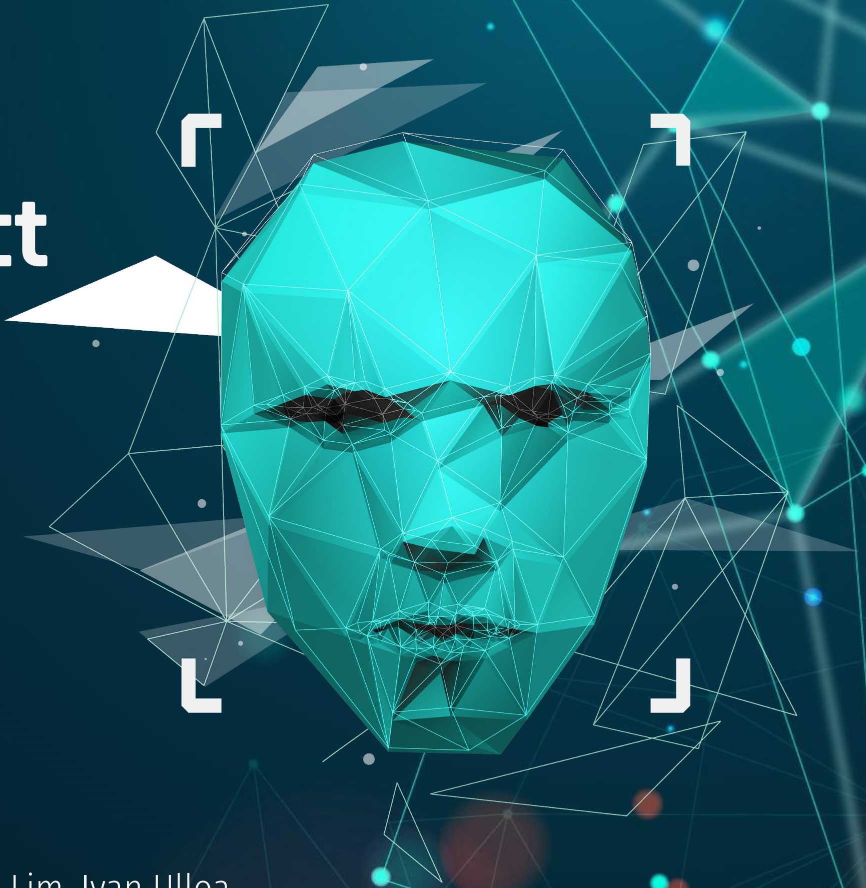
Using NLP to Predict the Severity of Cybersecurity Vulnerabilities



DSE 260 - Capstone Project
June 4, 2021
Final Presentation

Team: Saba Janamian, Bryan Cook, James Logan, Teck Lim, Ivan Ulloa
Advisors: Dr. Amarnath Gupta, Dr. Ilkay Altintas

OUR TEAM

Teck Lim: Project manager

Saba Janamian: Data engineer

James Logan: Data engineer

Ivan Ulloa: Data analyst

Bryan Cook: Solution architect

Advisor: Dr. Amarnath Gupta

01

ELEVATOR PITCH

The importance of Cyber Security

02

THE TECHNICAL DETAILS

The inner workings of the product

03

CREATING A PRODUCT

Architecture of the solution

04

DEMO AND CONCLUSION

Product showcase and final thoughts

THE ELEVATOR PITCH

01

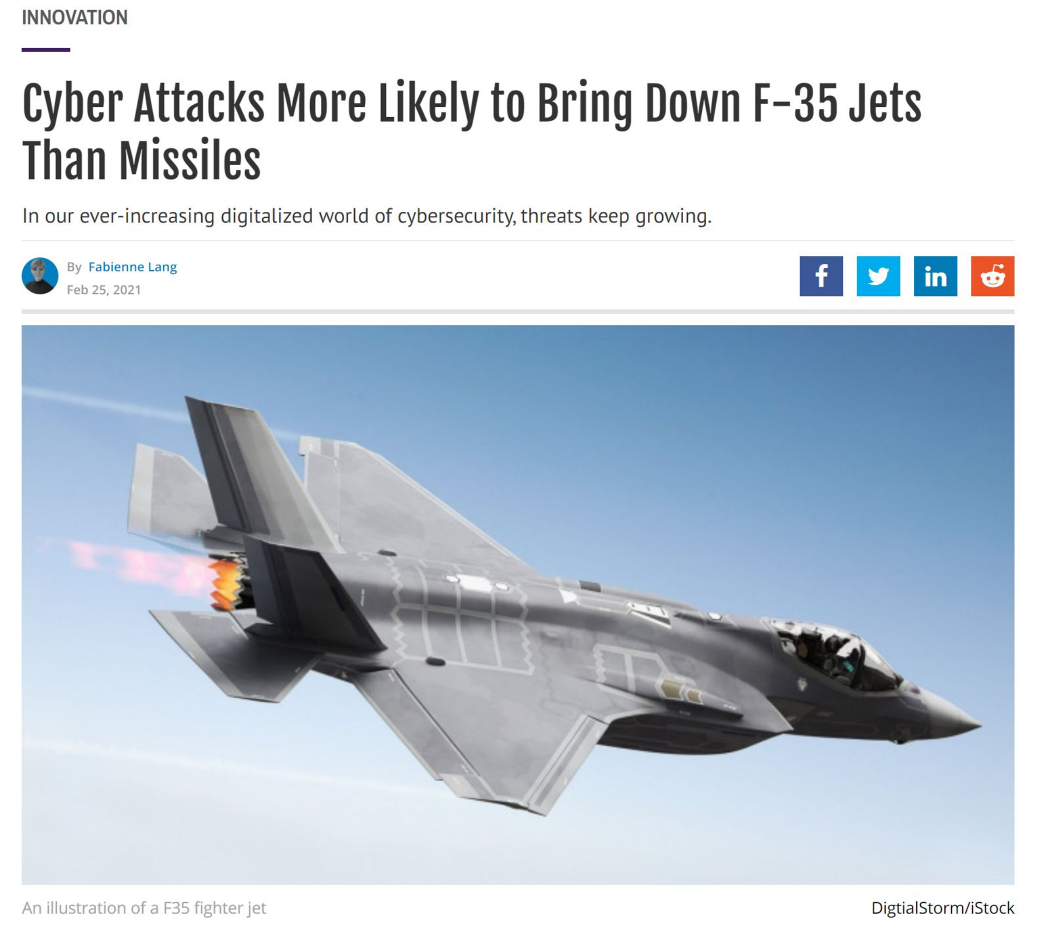
The Importance of Cybersecurity

CYBER-SECURITY IS IMPORTANT

$6,000,000,000,000

Annual Global Cybercrime Damage Cost

Source: CYBERSECURITY VENTURES



INNOVATION

Cyber Attacks More Likely to Bring Down F-35 Jets Than Missiles

In our ever-increasing digitalized world of cybersecurity, threats keep growing.

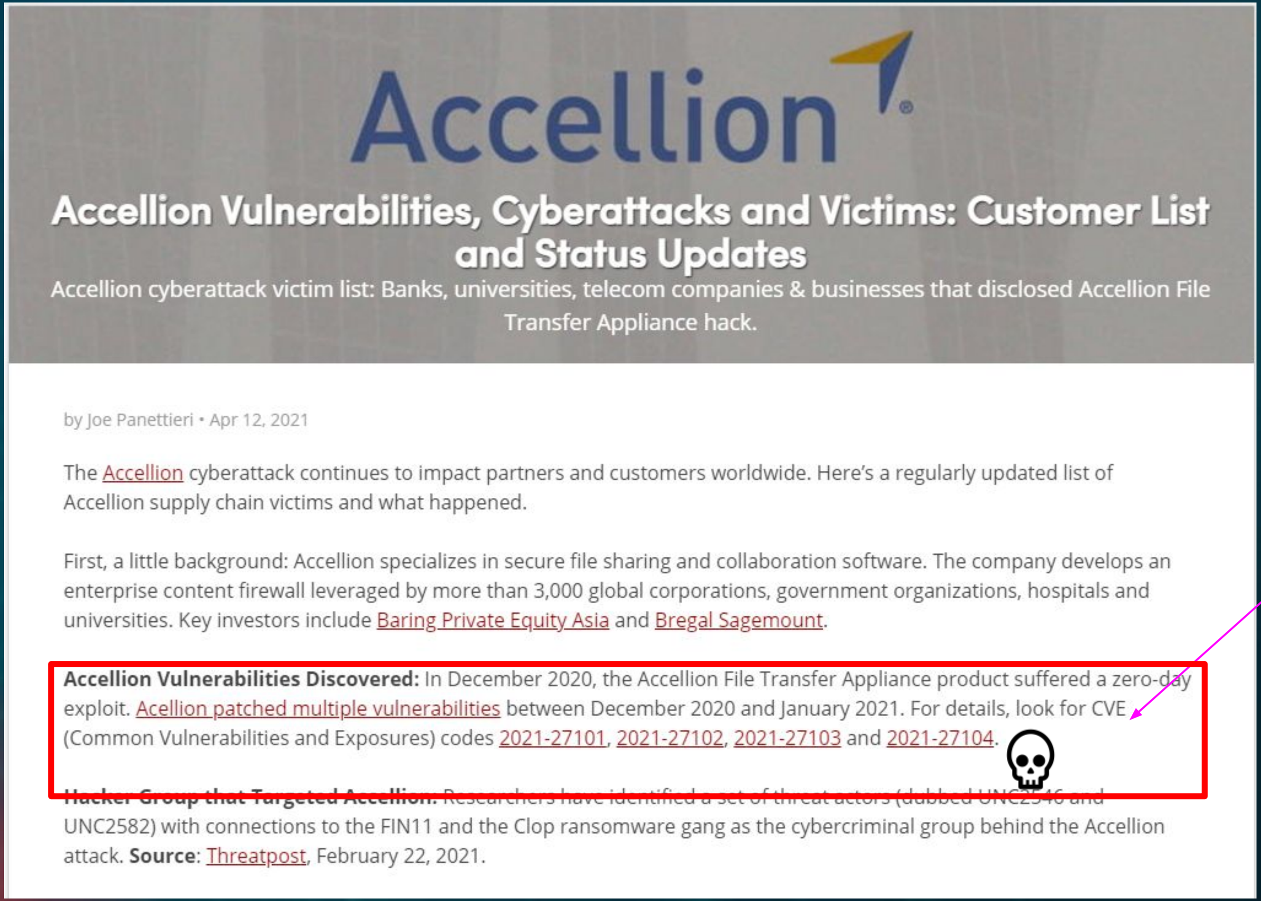
By Fabienne Lang
Feb 25, 2021

An illustration of a F35 fighter jet

DigtialStorm/iStock

COLONIAL PIPELINE CO
1473
NO SMOKING
1460
1450
1450

A PROBLEM TO SOLVE



Accellion Vulnerabilities, Cyberattacks and Victims: Customer List and Status Updates

Accellion cyberattack victim list: Banks, universities, telecom companies & businesses that disclosed Accellion File Transfer Appliance hack.

by Joe Panettieri • Apr 12, 2021

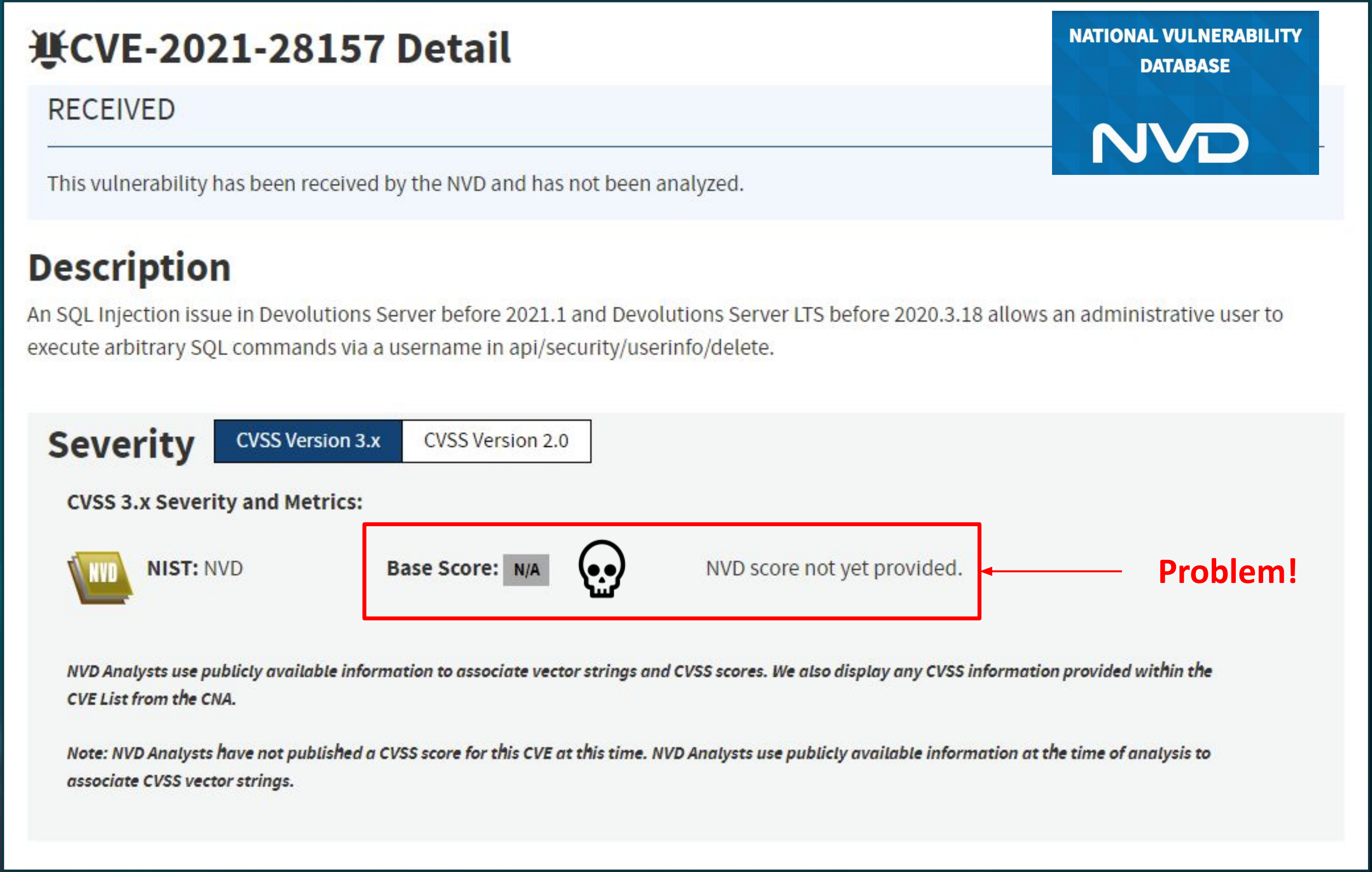
The Accellion cyberattack continues to impact partners and customers worldwide. Here's a regularly updated list of Accellion supply chain victims and what happened.

First, a little background: Accellion specializes in secure file sharing and collaboration software. The company develops an enterprise content firewall leveraged by more than 3,000 global corporations, government organizations, hospitals and universities. Key investors include Baring Private Equity Asia and Bregal Sagemount.

Accellion Vulnerabilities Discovered: In December 2020, the Accellion File Transfer Appliance product suffered a zero-day exploit. Accellion patched multiple vulnerabilities between December 2020 and January 2021. For details, look for CVE (Common Vulnerabilities and Exposures) codes 2021-27101, 2021-27102, 2021-27103 and 2021-27104. 💀

Hacker Group that Targeted Accellion: Researchers have identified a set of threat actors (dubbed UNC2546 and UNC2582) with connections to the FIN11 and the Clop ransomware gang as the cybercriminal group behind the Accellion attack. **Source**: Threatpost, February 22, 2021.

Many CVE record don’t yet have CVSS metrics!



CVE-2021-28157 Detail

NATIONAL VULNERABILITY DATABASE

NVD

RECEIVED

This vulnerability has been received by the NVD and has not been analyzed.

Description

An SQL Injection issue in Devolutions Server before 2021.1 and Devolutions Server LTS before 2020.3.18 allows an administrative user to execute arbitrary SQL commands via a username in api/security/userinfo/delete.

Severity

CVSS 3.x Severity and Metrics:

NIST: NVD   **Base Score:** N/A   NVD score not yet provided.

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have not published a CVSS score for this CVE at this time. NVD Analysts use publicly available information at the time of analysis to associate CVSS vector strings.

Problem!

Insights from a Domain Expert

Scott Pope

Director, Product Management & Business Development

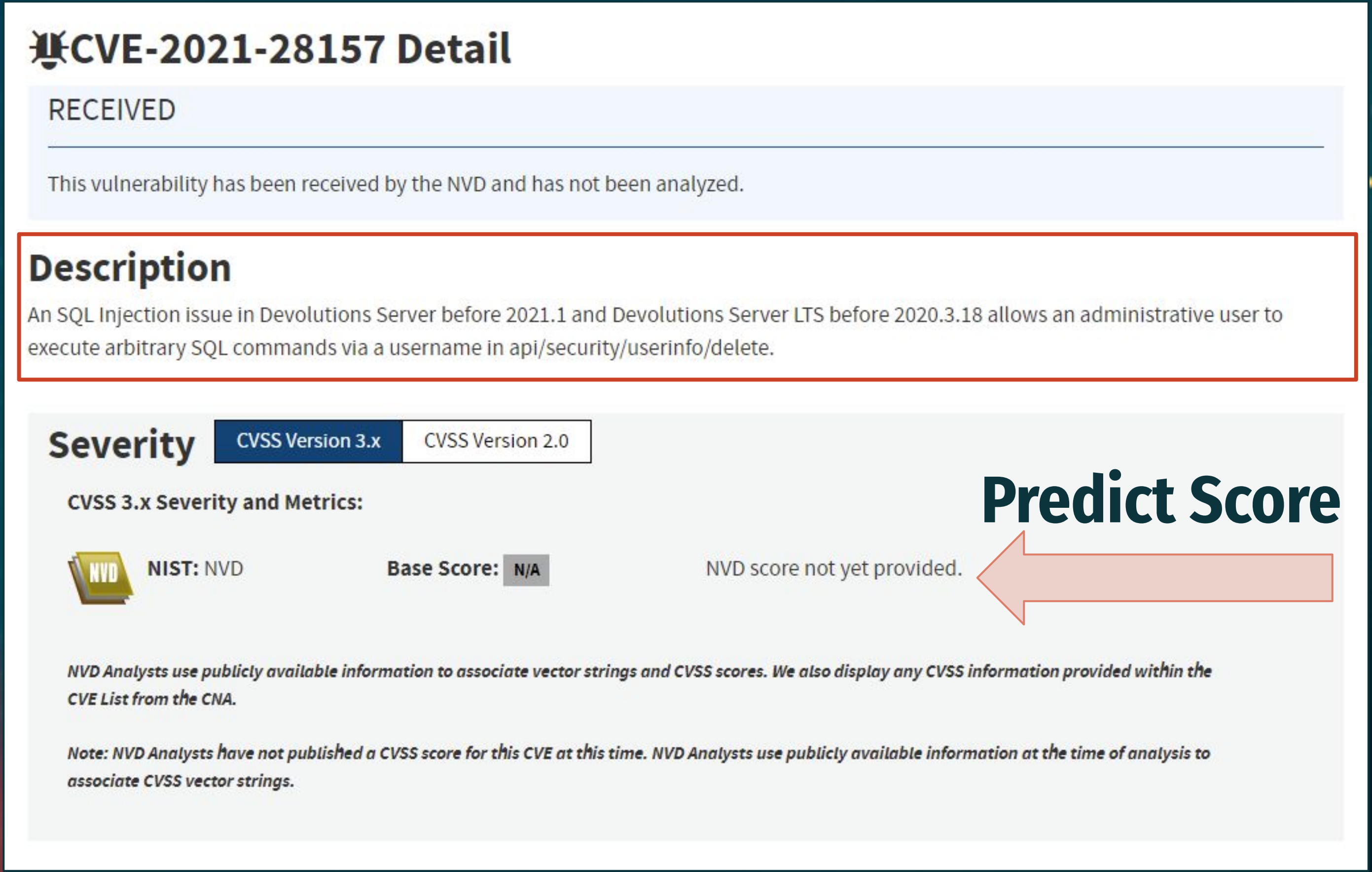
Security Technical Alliances Ecosystem

- CVEs are heavily used by cybersecurity engineers
- Most successful cyber attacks result from known, uncorrected vulnerabilities

- Missing CVSS metrics are a big problem for cybersecurity engineers!
  - Cybersecurity engineers have too much data and not enough time
  - There is no time for “data exploration”
  - False negatives are bad
  - False positives can be worse; they consume too much time

PROPOSED SOLUTION

Solution Concept



CVE-2021-28157 Detail

RECEIVED

This vulnerability has been received by the NVD and has not been analyzed.

Description

An SQL Injection issue in Devolutions Server before 2021.1 and Devolutions Server LTS before 2020.3.18 allows an administrative user to execute arbitrary SQL commands via a username in api/security/userinfo/delete.

Severity

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** N/A NVD score not yet provided.

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have not published a CVSS score for this CVE at this time. NVD Analysts use publicly available information at the time of analysis to associate CVSS vector strings.

Predict Score

Analyze text

Language Model

VulnerWatch

PRODUCT OVERVIEW

1 **PREDICTION**

Predicted CVSS scores based on description of CVEs

2 **EXPLICABILITY**

Be able to explain the prediction result

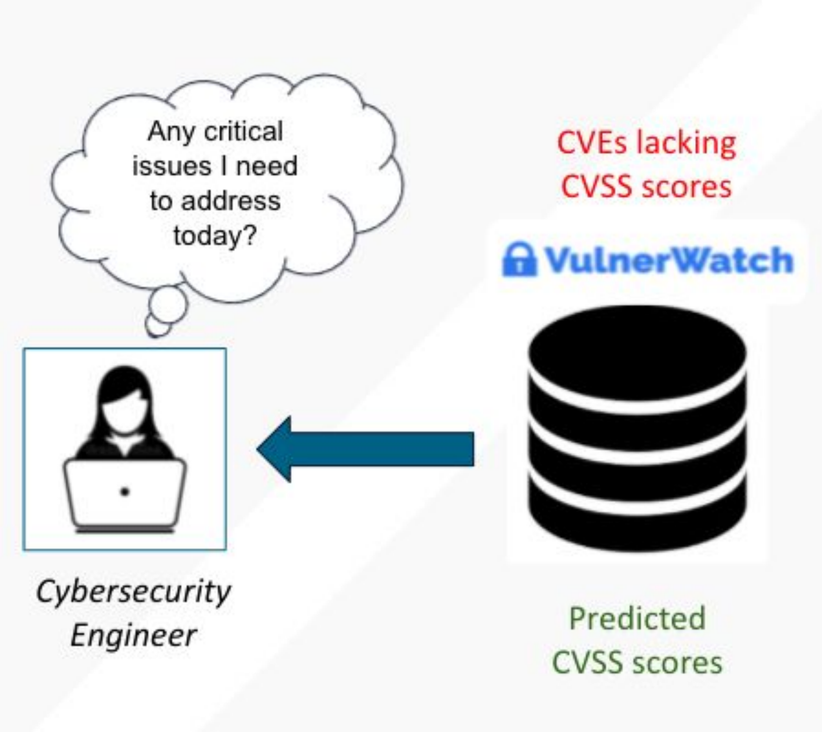
3 **EFFICIENT UX**

User-friendly graphical interface to access the application

4 **AUTONOMY**

Option to run scheduled predictions in batch without human intervention

Use Cases



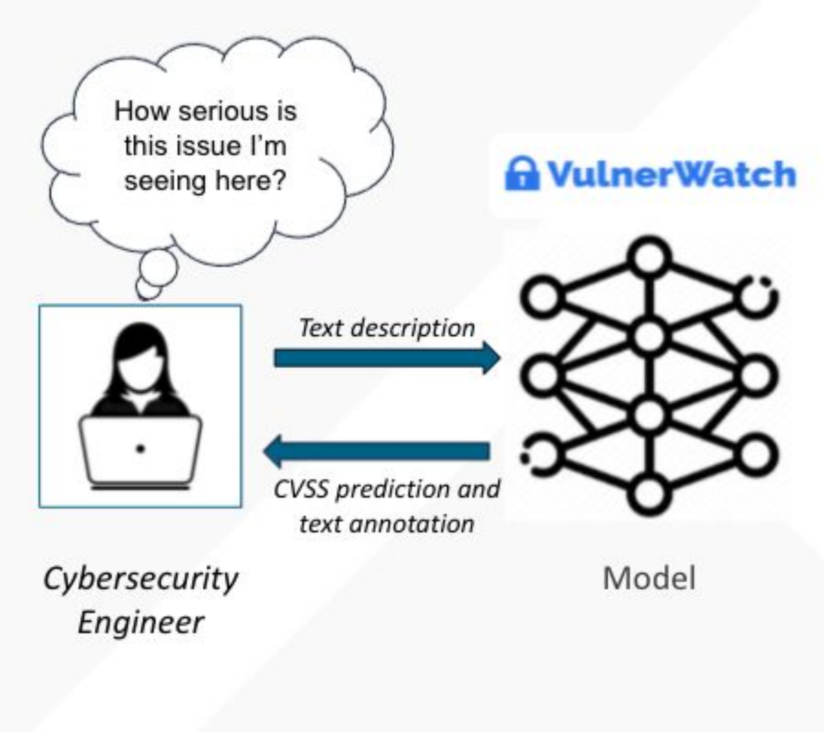
Any critical issues I need to address today?

CVEs lacking CVSS scores

VulnerWatch

Cybersecurity Engineer

Predicted CVSS scores



How serious is this issue I'm seeing here?

VulnerWatch

Text description

CVSS prediction and text annotation

Cybersecurity Engineer

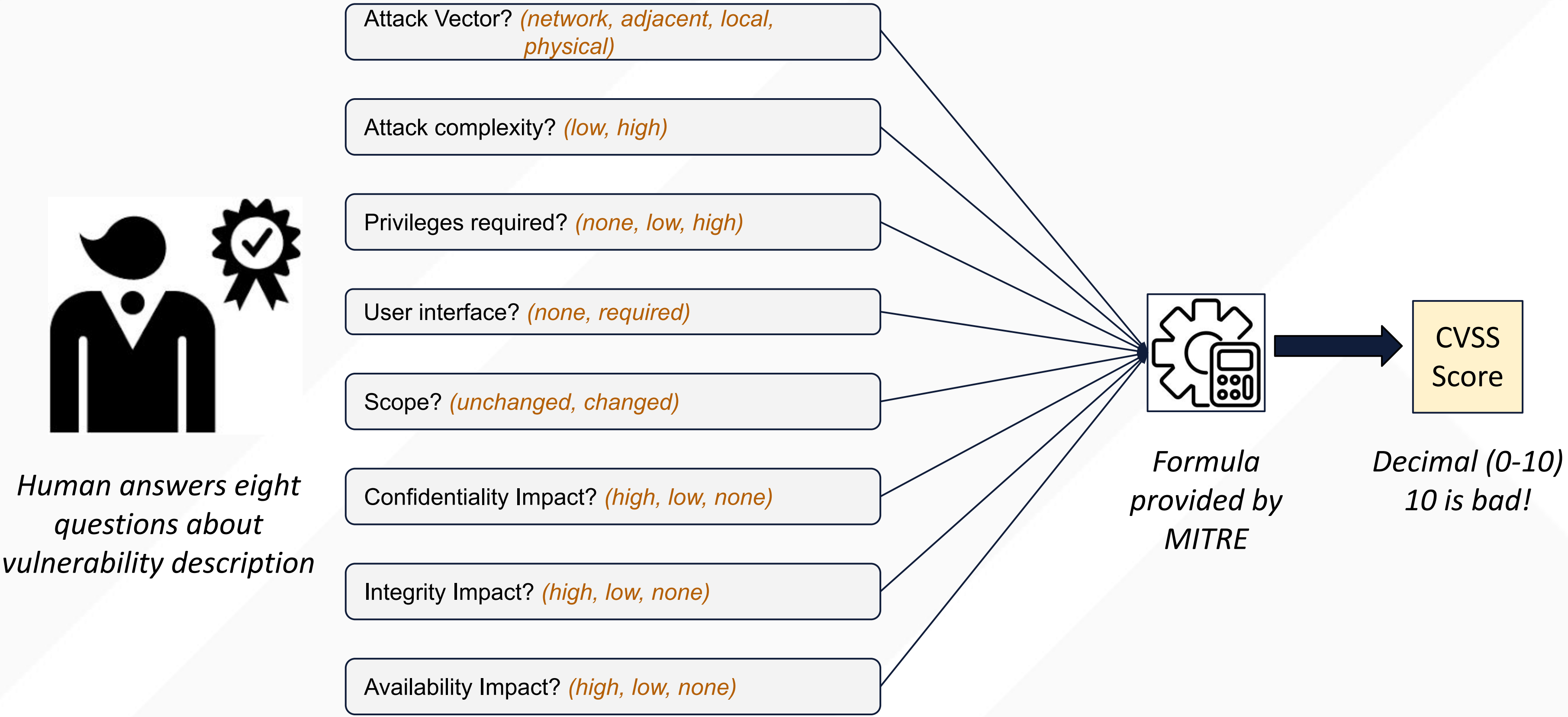
Model

THE TECHNICAL DETAILS

02

CVSS METRICS
NLP Analysis of CVE Descriptions

CVSS Calculation



Human answers eight questions about vulnerability description

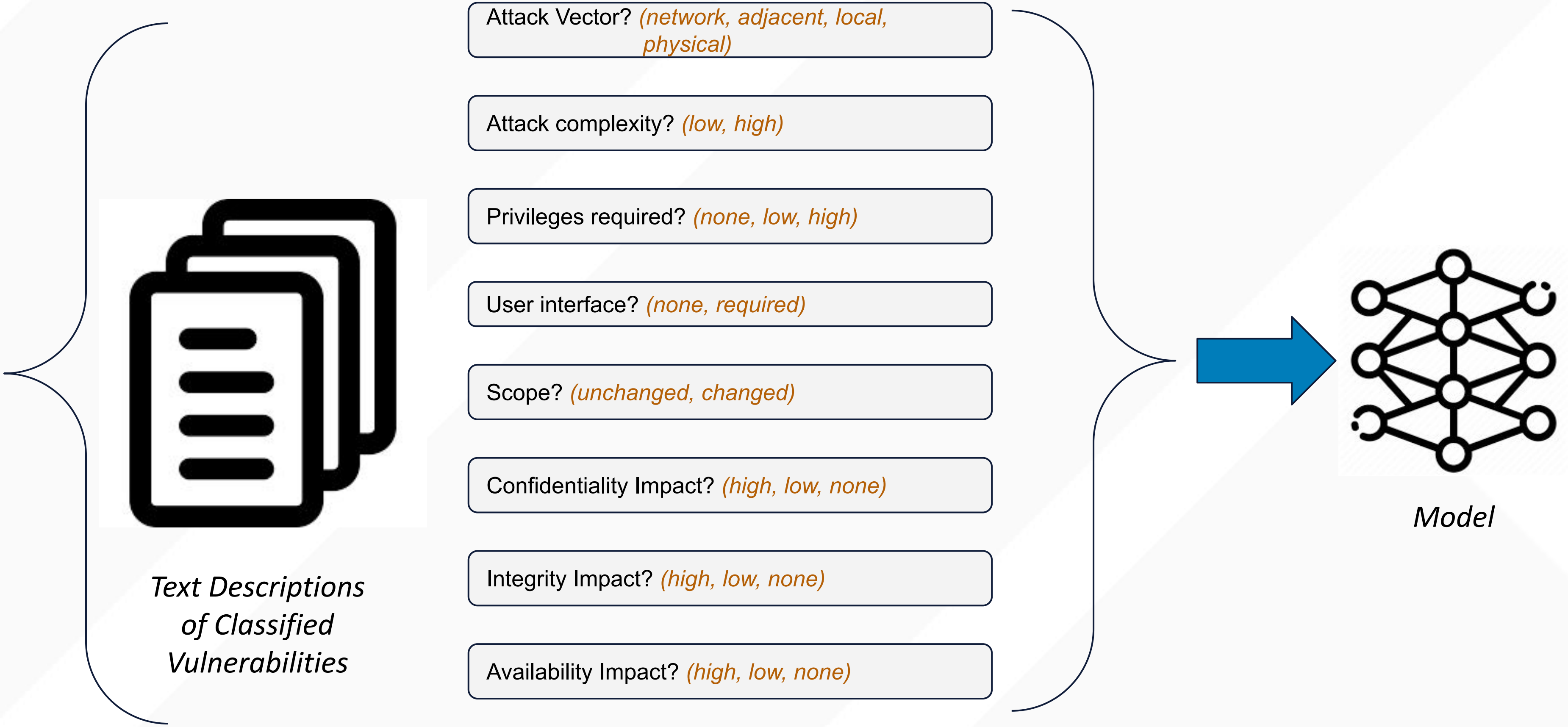
- Attack Vector? *(network, adjacent, local, physical)*
- Attack complexity? *(low, high)*
- Privileges required? *(none, low, high)*
- User interface? *(none, required)*
- Scope? *(unchanged, changed)*
- Confidentiality Impact? *(high, low, none)*
- Integrity Impact? *(high, low, none)*
- Availability Impact? *(high, low, none)*

Formula provided by MITRE

CVSS Score

Decimal (0-10)
10 is bad!

Train Using NLP Based on Text Descriptions + Answers/Classes



Text Descriptions of Classified Vulnerabilities

Attack Vector? *(network, adjacent, local, physical)*

Attack complexity? *(low, high)*

Privileges required? *(none, low, high)*

User interface? *(none, required)*

Scope? *(unchanged, changed)*

Confidentiality Impact? *(high, low, none)*

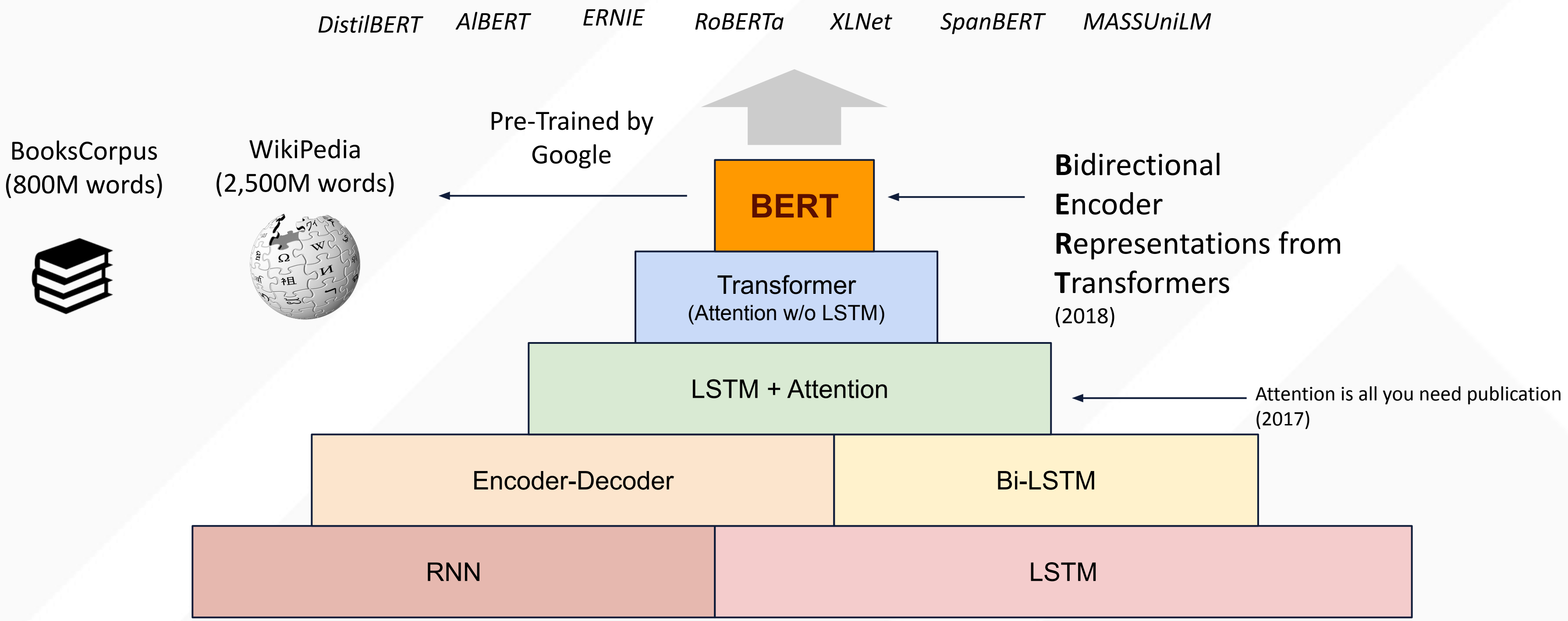
Integrity Impact? *(high, low, none)*

Availability Impact? *(high, low, none)*

Human-generated Answers/Classes

Model

Entering BERT



DistilBERT *AlBERT* *ERNIE* *RoBERTa* *XLNet* *SpanBERT* *MASSUniLM*

BooksCorpus
(800M words)

WikiPedia
(2,500M words)

Pre-Trained by
Google

BERT

Transformer
(Attention w/o LSTM)

LSTM + Attention

Encoder-Decoder

Bi-LSTM

RNN

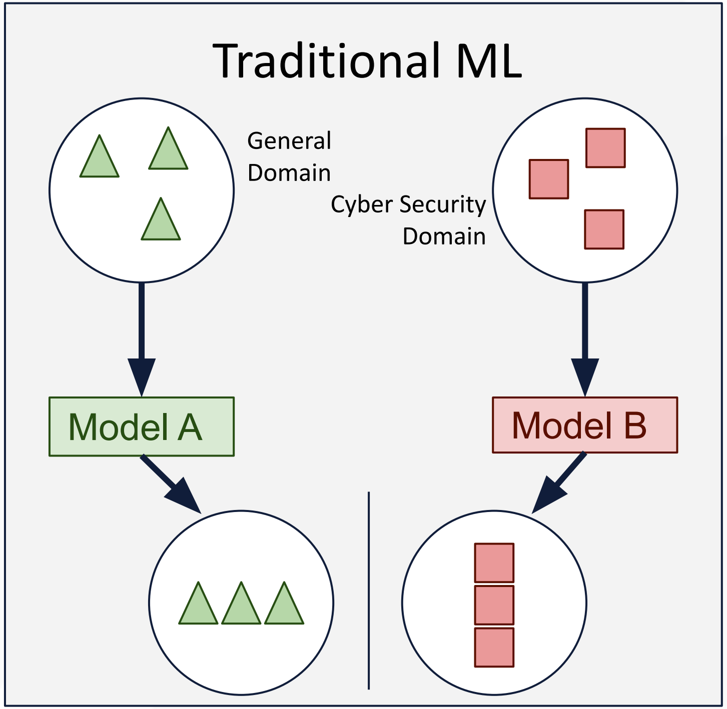
LSTM

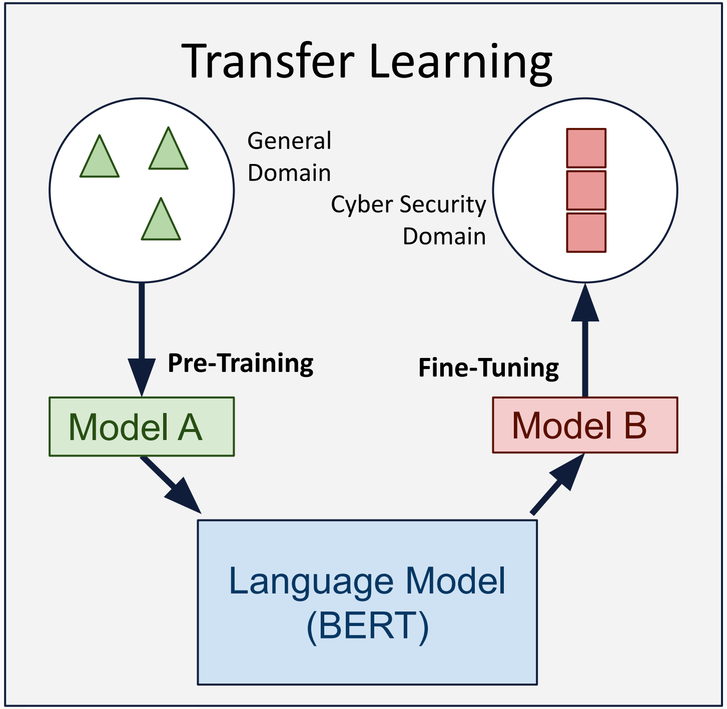
Bidirectional
Encoder
Representations from
Transformers
(2018)

Attention is all you need publication
(2017)

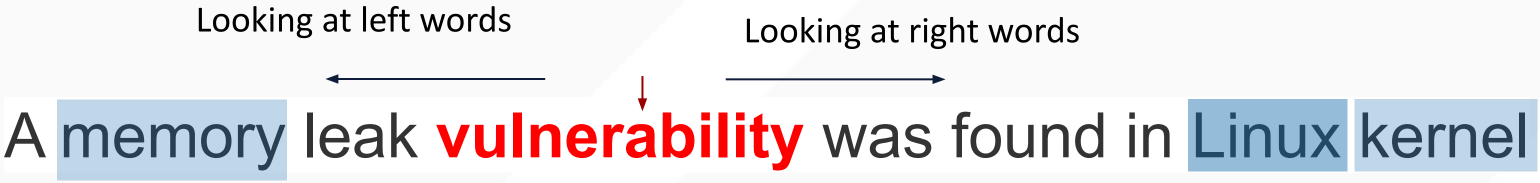
Source: https://mccormickml.com/2019/11/11/bert-research-ep-1-key-concepts-and-sources/

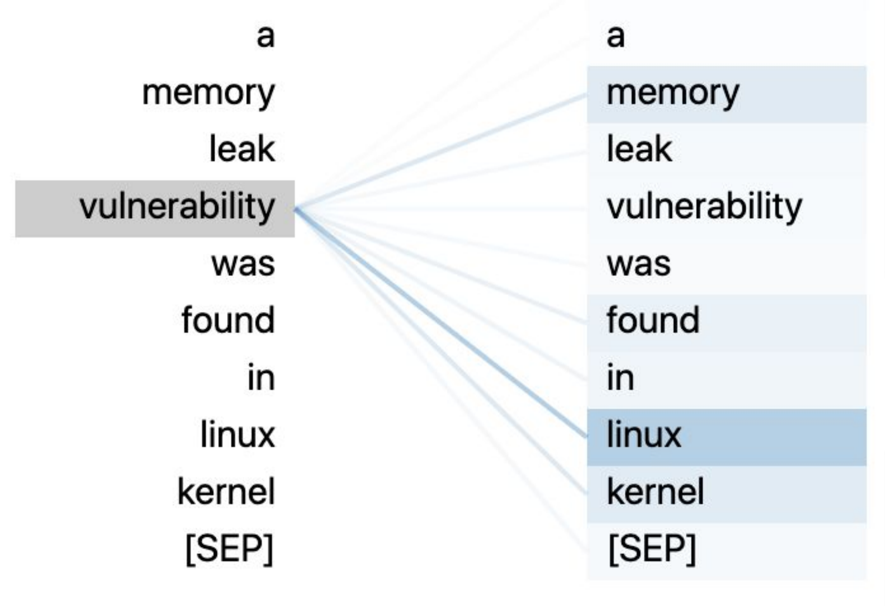
Transfer Learning





Bidirectional Language Model with Attention Weights



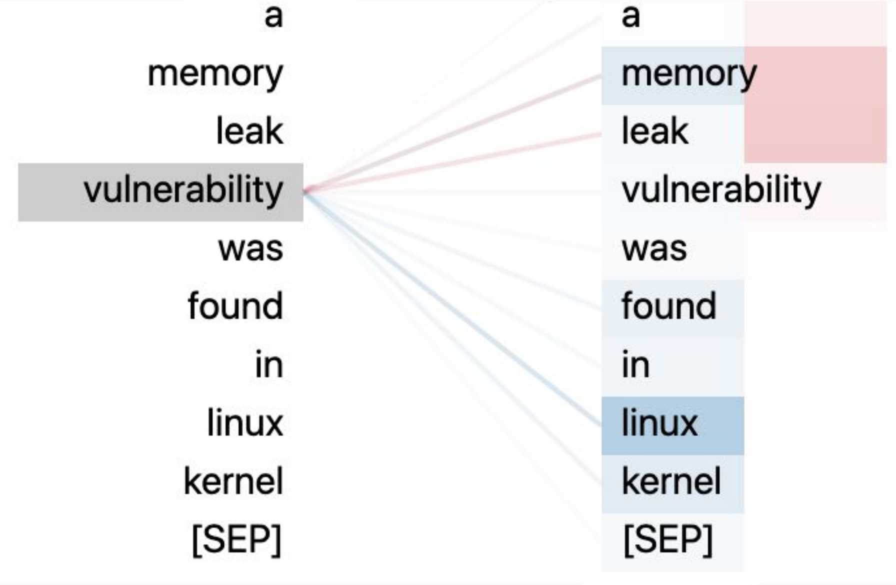


Multi Attention Head

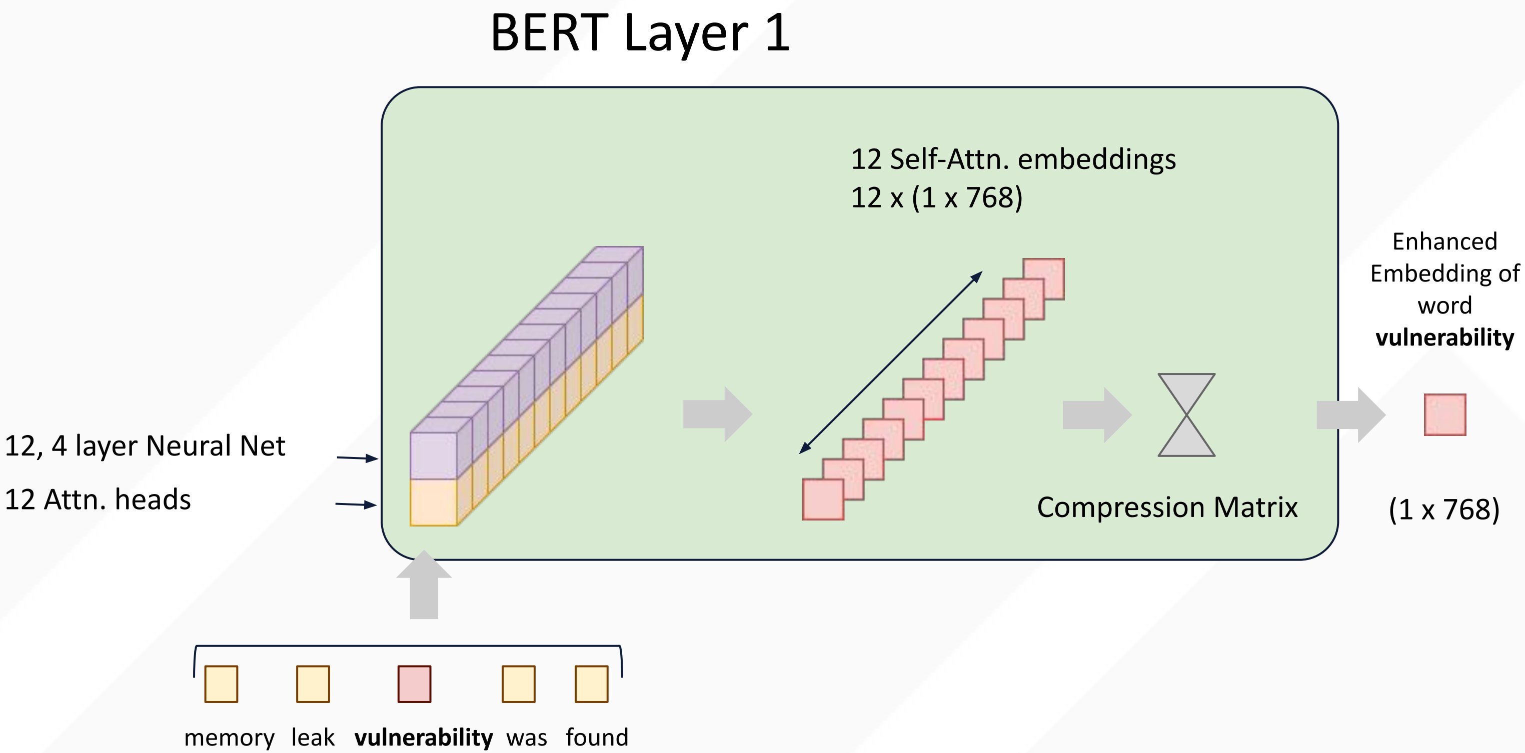
Attention from both Head 1 and 2

Attention from Head 2

A memory leak **vulnerability** was found in Linux kernel



Inner working of BERT Layer



BERT Layer 1

12 Self-Attn. embeddings
12 x (1 x 768)

Enhanced Embedding of word **vulnerability**

(1 x 768)

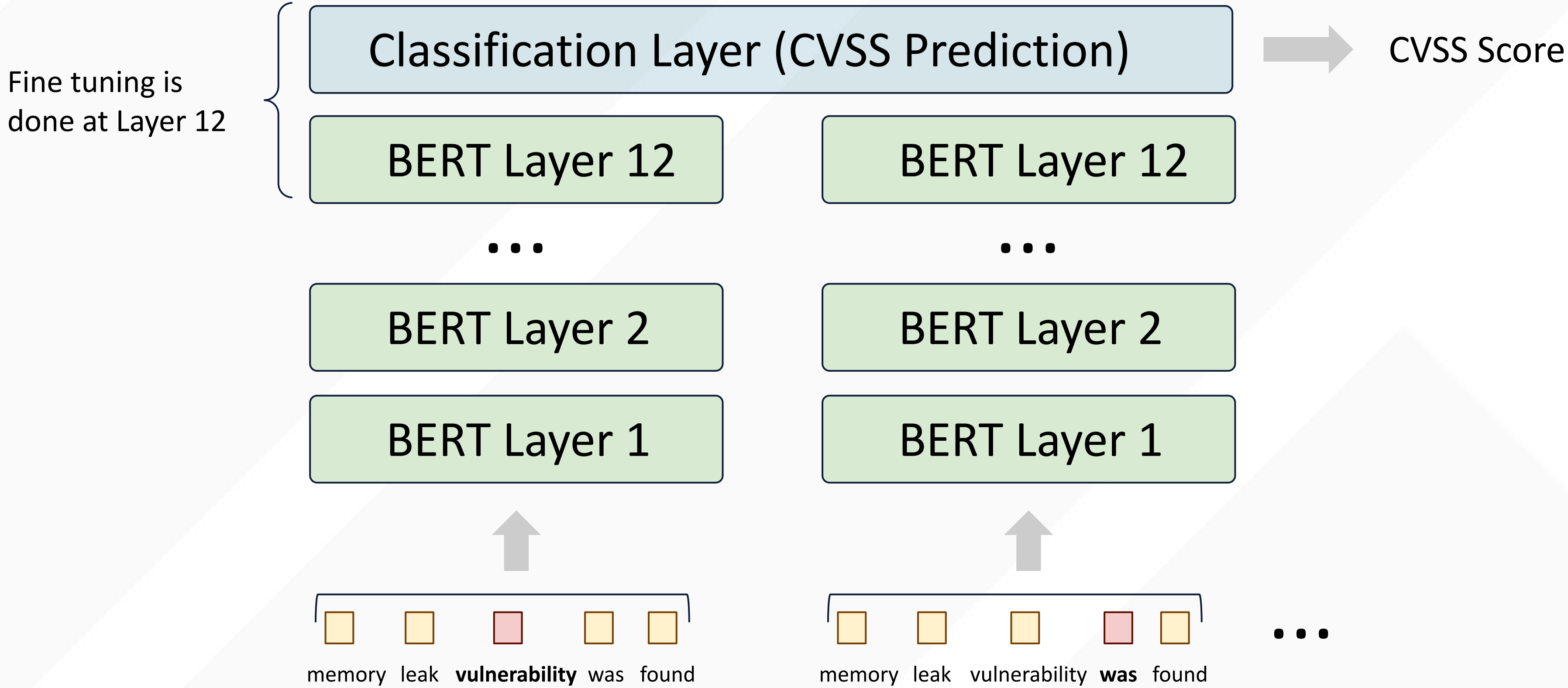
Compression Matrix

12, 4 layer Neural Net

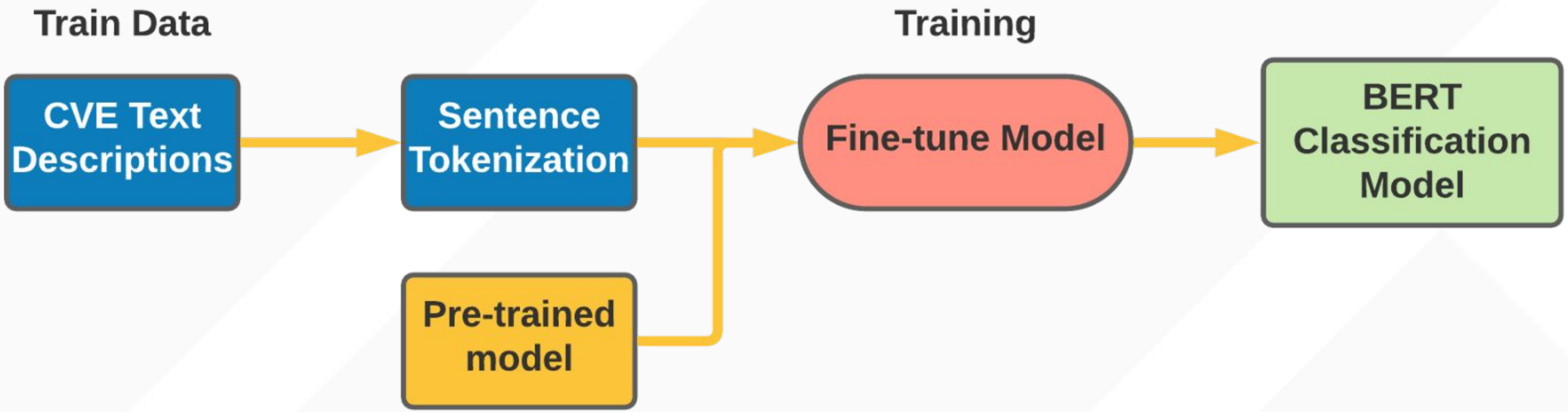
12 Attn. heads

memory leak **vulnerability** was found

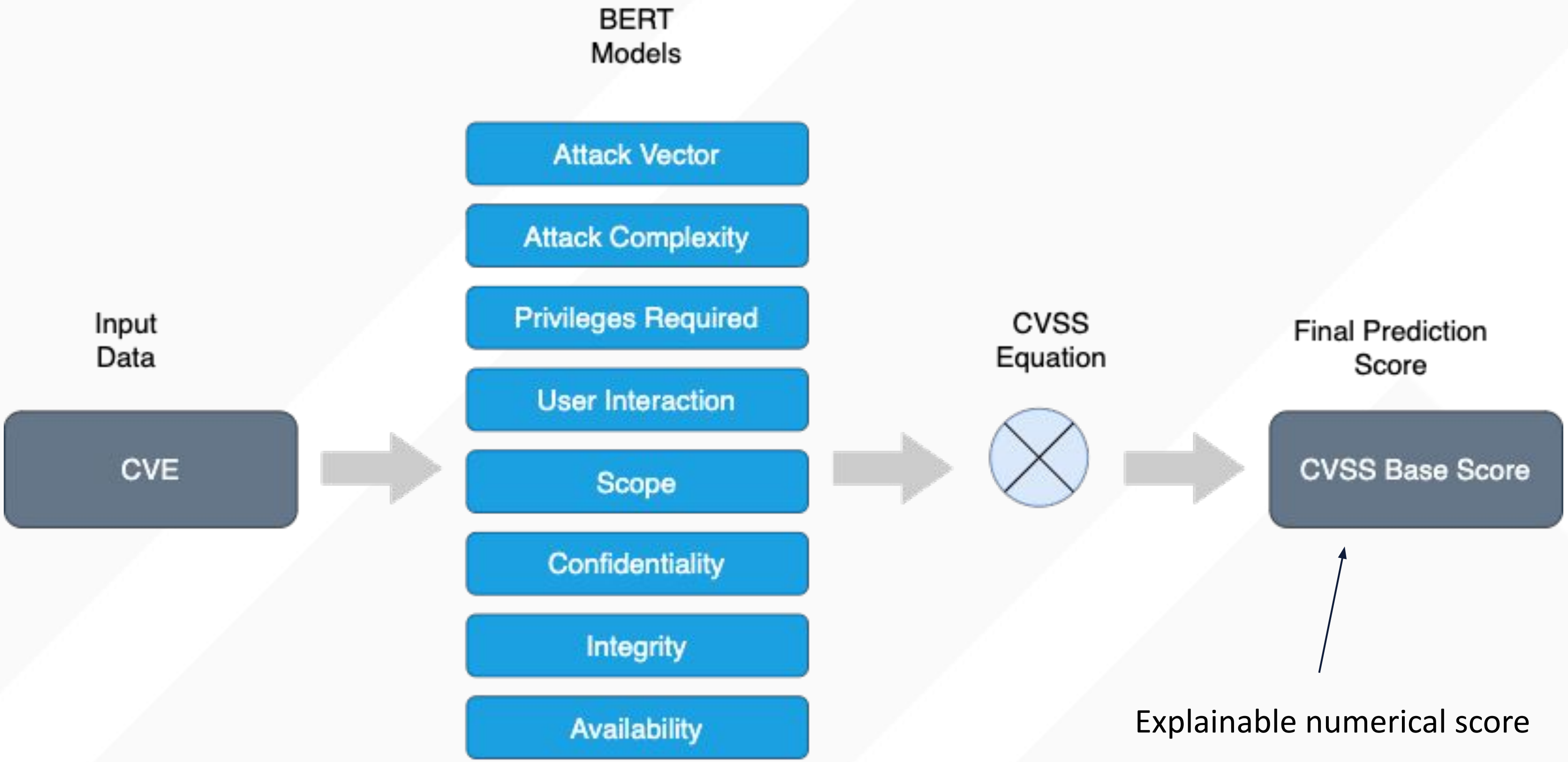
12 BERT Layers


Fine tuning is done at Layer 12
Classification Layer (CVSS Prediction)
CVSS Score
BERT Layer 12
BERT Layer 12
• • •
• • •
BERT Layer 2
BERT Layer 2
BERT Layer 1
BERT Layer 1
memory leak **vulnerability** was found
memory leak vulnerability **was** found
• • •

Pipe Line of Language Model Fine-Tuning



8 Separate BERT Models for each CVSS metric



Explainable numerical score

Modeling Results for Metrics

Train dataset: 61,616
Test dataset: 15,404

	N-Class Labels	Mean Confidence	Accuracy %	MCC	F1
Attack Vector *(network, adjacent, local, physical)*	4	0.9912	0.9257	0.8162	0.8146
Attack complexity *(low, high)*	2	0.9201	0.9518	0.6421	0.8147
Privileges required *(none, low, high)*	3	0.9498	0.8806	0.7441	0.8136
User interface *(none, required)*	2	0.9195	0.9374	0.8643	0.9129
Scope *(unchanged, changed)*	2	0.9327	0.9670	0.8801	0.8989
Confidentiality Impact *(high, low, none)*	3	0.9631	0.8915	0.8062	0.8729
Integrity Impact *(high, low, none)*	3	0.9798	0.9041	0.8413	0.8977
Availability Impact *(high, low, none)*	3	0.9612	0.9108	0.8219	0.7606

Modeling Results for Metrics

Train dataset: 61,616
Test dataset: 15,404

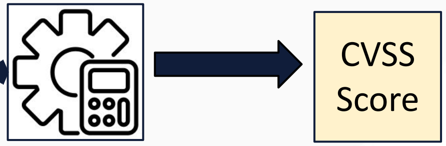
	N-Class Labels	Mean Confidence	Accuracy %	MCC	F1	F1 (>90%)
Attack Vector *(network, adjacent, local, physical)*	4	0.9912	0.9257	0.8162	0.8146	0.8675
Attack complexity *(low, high)*	2	0.9201	0.9518	0.6421	0.8147	0.9066
Privileges required *(none, low, high)*	3	0.9498	0.8806	0.7441	0.8136	0.9128
User interface *(none, required)*	2	0.9195	0.9374	0.8643	0.9129	0.9811
Scope *(unchanged, changed)*	2	0.9327	0.9670	0.8801	0.8989	0.9783
Confidentiality Impact *(high, low, none)*	3	0.9631	0.8915	0.8062	0.8729	0.9495
Integrity Impact *(high, low, none)*	3	0.9798	0.9041	0.8413	0.8977	0.9255
Availability Impact *(high, low, none)*	3	0.9612	0.9108	0.8219	0.7606	0.8243

Modeling Results for CVSS Scores

Predicted Answers

- Attack Vector *(network, adjacent, local, physical)*
- Attack complexity *(low, high)*
- Privileges required *(none, low, high)*
- User interface *(none, required)*
- Scope *(unchanged, changed)*
- Confidentiality Impact *(high, low, none)*
- Integrity Impact *(high, low, none)*
- Availability Impact *(high, low, none)*

Scores	Score Range	MSE	MAE	R2	R2 (>90%)
Impact score	0.0 - 6.0	0.8561	0.3670	0.6049	0.9114
Exploitability score	0.1 - 3.9	0.4280	0.2883	0.4887	0.8362
Base Score	**0.0 - 10.0**	**1.2760**	**0.5887**	**0.5055**	**0.8687**

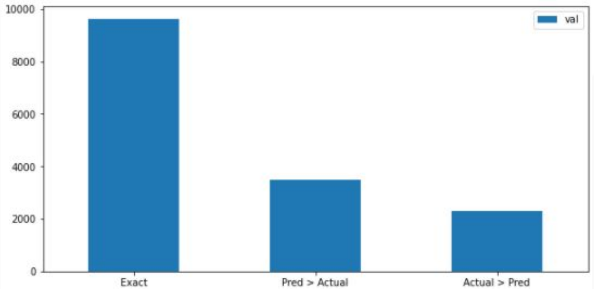


Formula provided by MITRE

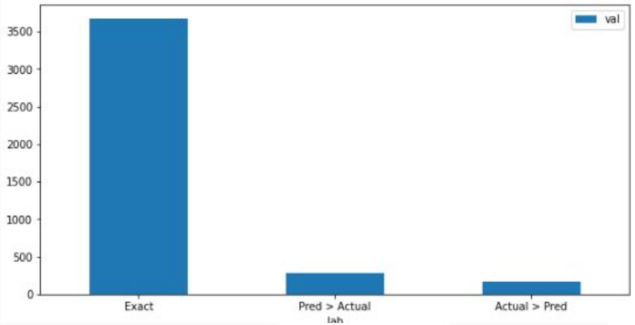
Predicted

Interpreting the Confidence

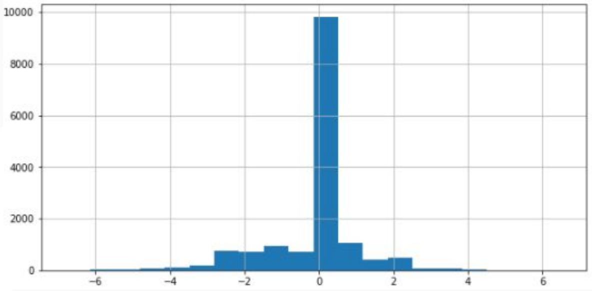
- Performance of predicted classes and CVSS scores is important
- Per domain expert, Predicted > Actual, i.e. false positives, is worse!



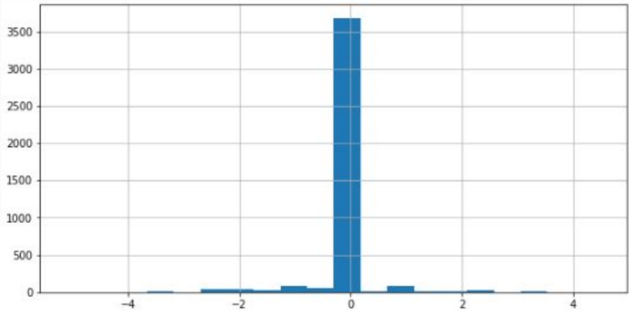
Base score prediction (All CVE)



Base score prediction (> 90%)



Base score error distribution (All CVE)



Base score error distribution (> 90%)

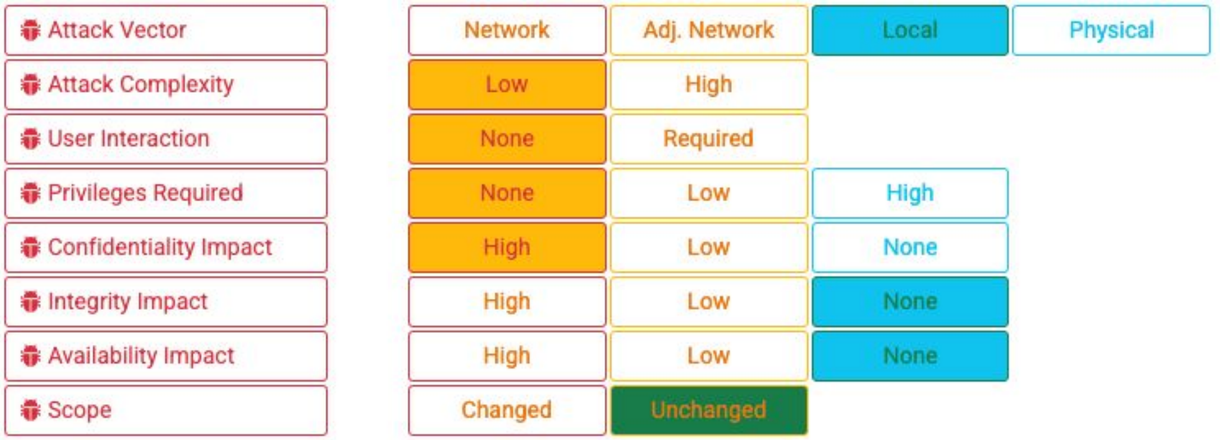
Explaining the result

CVE-2021-22739: *Information Exposure vulnerability exists in a Software which could cause a device to be compromised when it is first configured.*

What is the severity score?

Predicted: 6.2

Why?

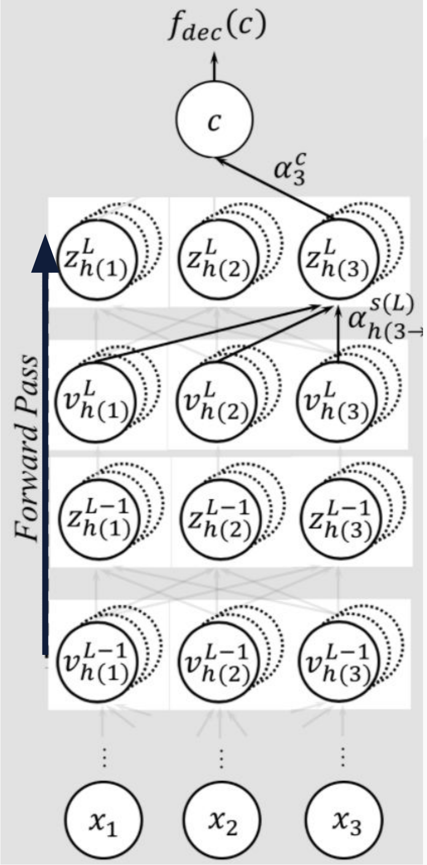


Attack Vector	Network	Adj. Network	[✓ Local]	Physical
Attack Complexity	[✓ Low]	High		
User Interaction	[✓ None]	Required		
Privileges Required	[✓ None]	Low	High	
Confidentiality Impact	[✓ High]	Low	None	
Integrity Impact	High	Low	[✓ None]	
Availability Impact	High	Low	[✓ None]	
Scope	Changed	[✓ Unchanged]		

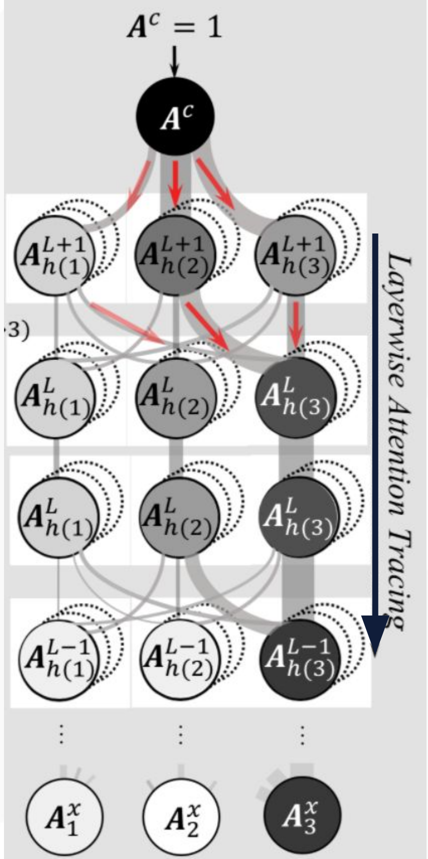
Why?

Why?

Finding Relevant Words



An open network



An open **network**

Source:https://github.com/frankaging/LAT_for_Transformer

Case Study

Originally from CVE-2021-22739

Information Exposure vulnerability exists in homeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior which could cause a device to be compromised when it is first configured.

Question:

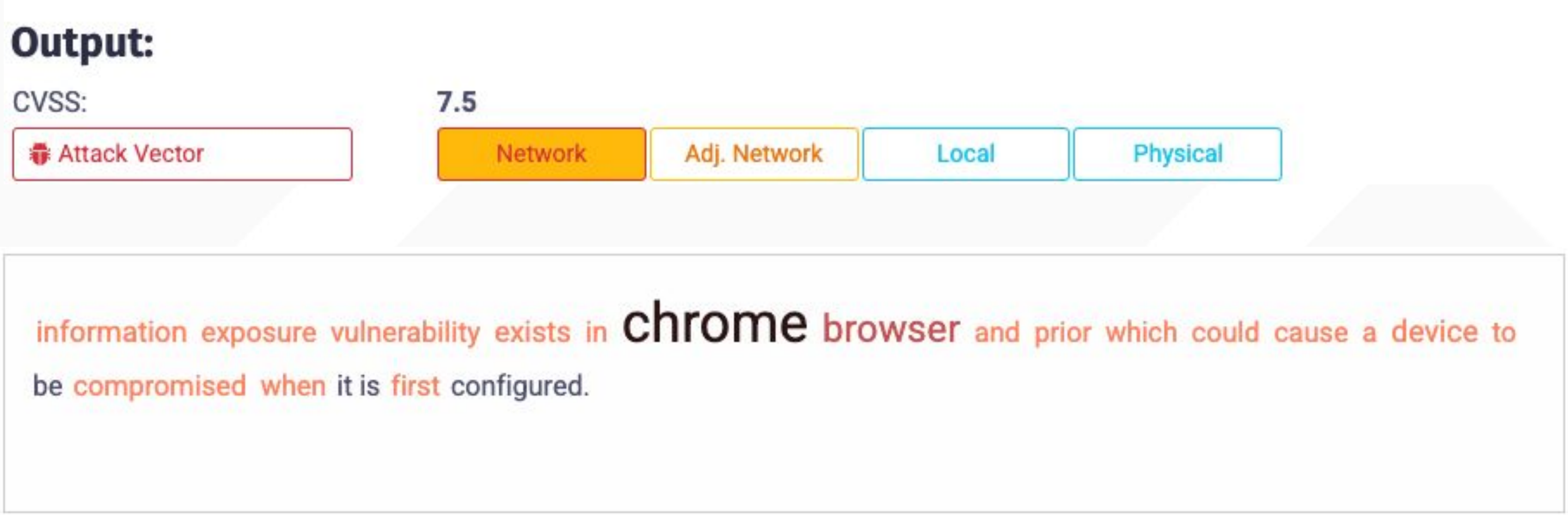
1) **What is the attack vector?**
    1. Network
    2. Adj. Network
    3. Local
    4. Physical

2) **Which word or phrases contributed the most to your decision?**

Case Study

Originally from CVE-2021-22739

Information Exposure vulnerability exists in Chrome browser which could cause a device to be compromised when it is first configured.



Output:

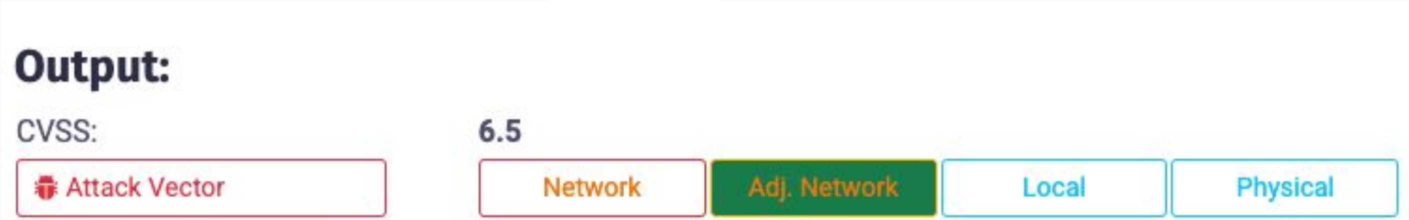
CVSS: 7.5

information exposure vulnerability exists in chrome browser and prior which could cause a device to be compromised when it is first configured.

Case Study

Originally from CVE-2021-22739

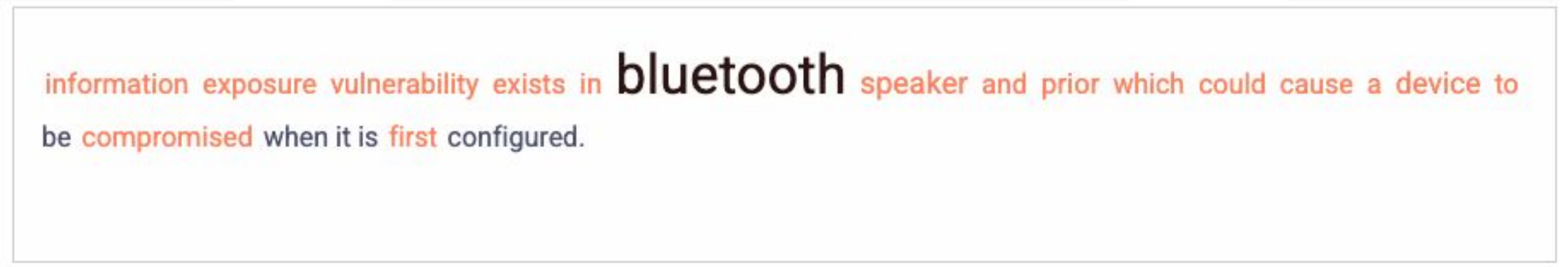
Information Exposure vulnerability exists in Bluetooth speaker which could cause a device to be compromised when it is first configured.



Output:

CVSS: 6.5

Attack Vector: Network [✓ Adj. Network] Local Physical

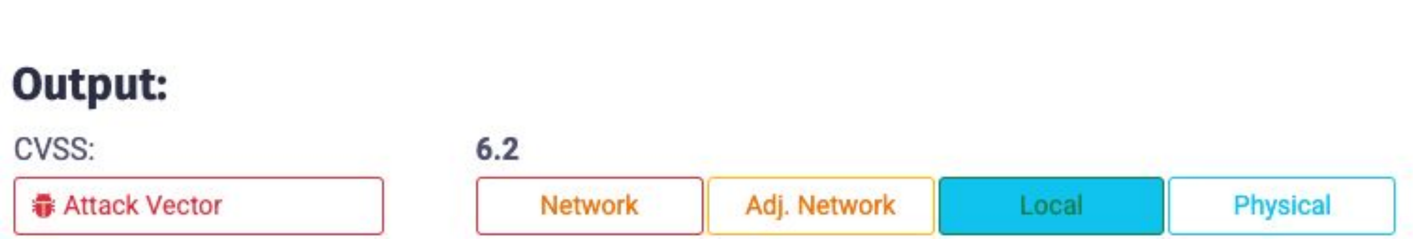


information exposure vulnerability exists in bluetooth speaker and prior which could cause a device to be compromised when it is first configured.

Case Study

Originally from CVE-2021-22739

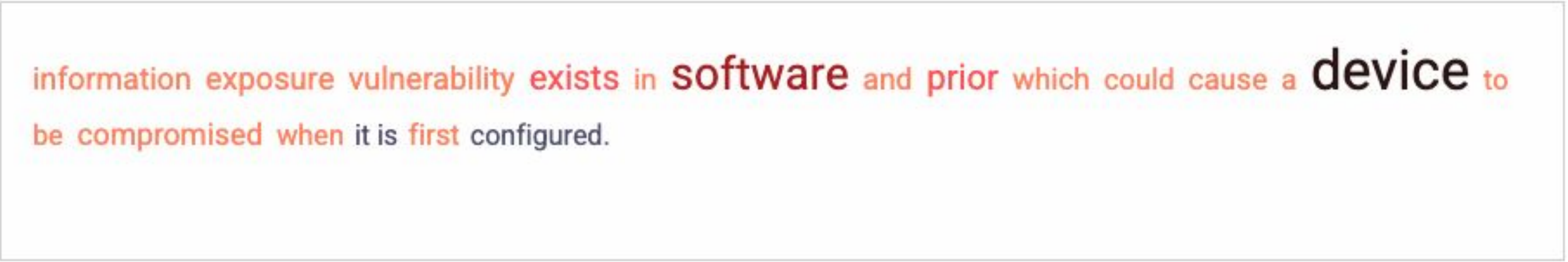
Information Exposure vulnerability exists in Software which could cause a device to be compromised when it is first configured.



Output:

CVSS: 6.2

Attack Vector: Network | Adj. Network | [✓ Local] | Physical

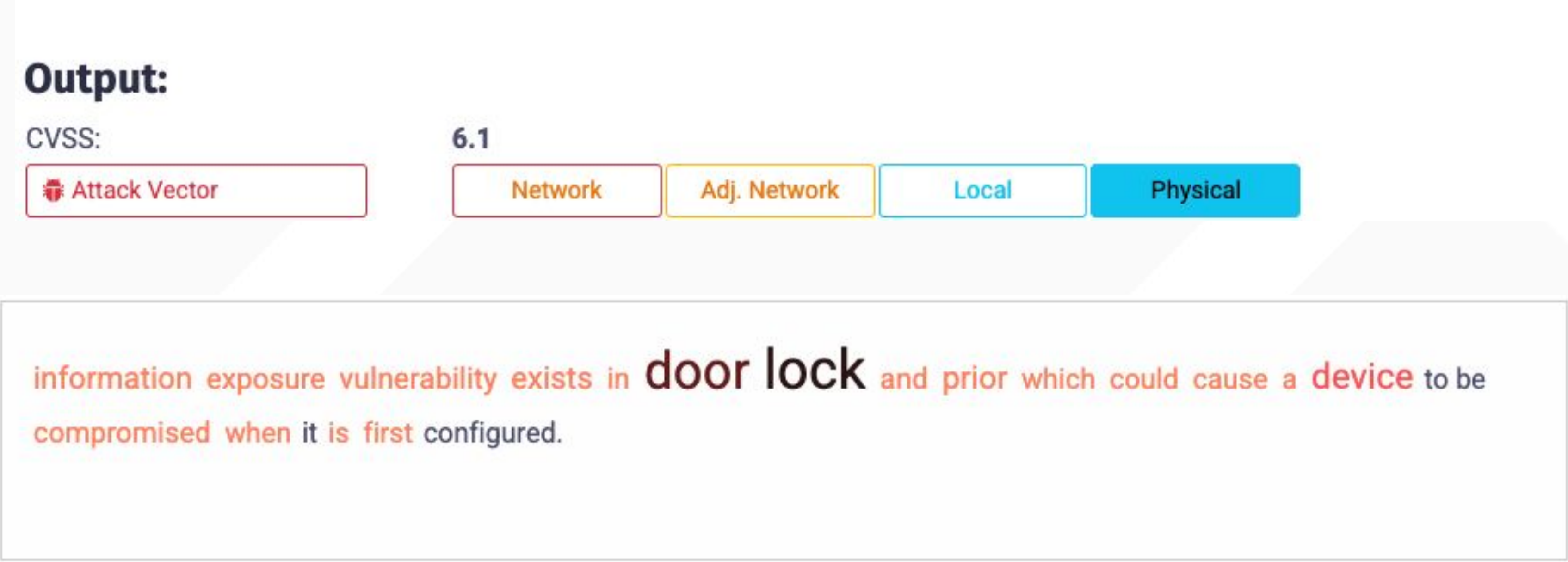


information exposure vulnerability exists in software and prior which could cause a device to be compromised when it is first configured.

Case Study

Originally from CVE-2021-22739

Information Exposure vulnerability exists in Door Lock which could cause a device to be compromised when it is first configured.



Output:

CVSS: 6.1

Attack Vector: Network | Adj. Network | Local | [✓ Physical]

information exposure vulnerability exists in door lock and prior which could cause a device to be compromised when it is first configured.

Case Study Conclusion

- Model is context aware
- Model has prior knowledge about the words

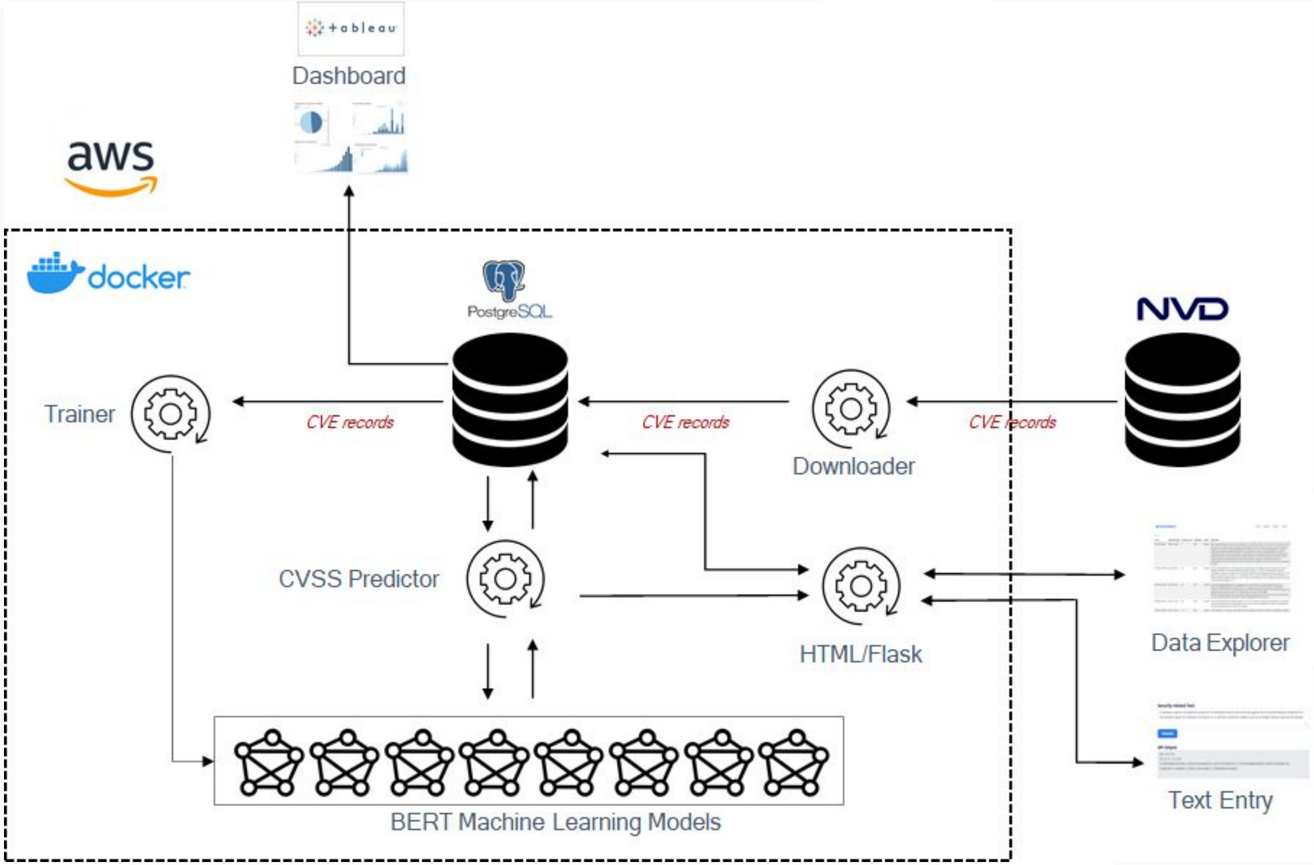
CREATING A PRODUCT

03

Implementing an Architecture

VulnerWatch

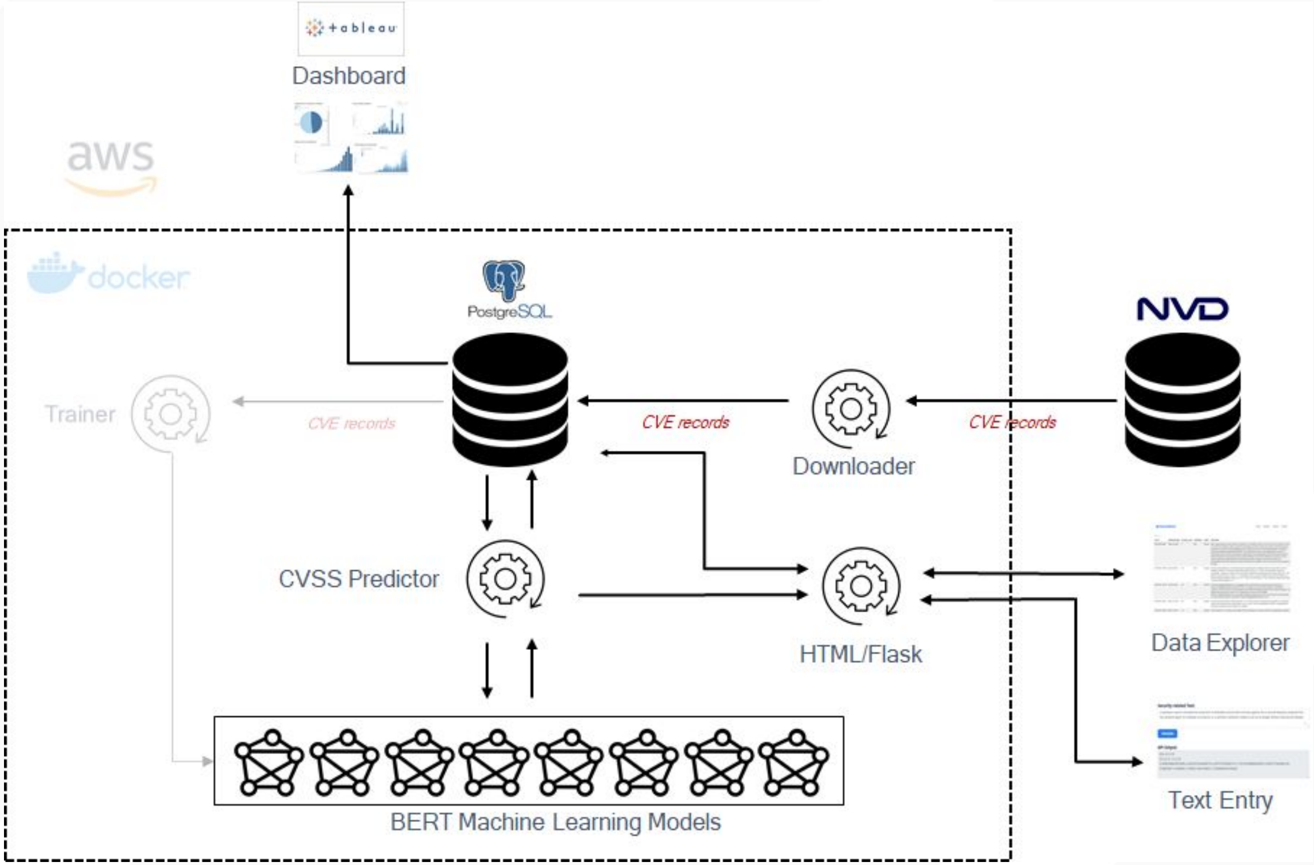
Architecture



GitHub: https://github.com/twlim1/260_capstone

VulnerWatch

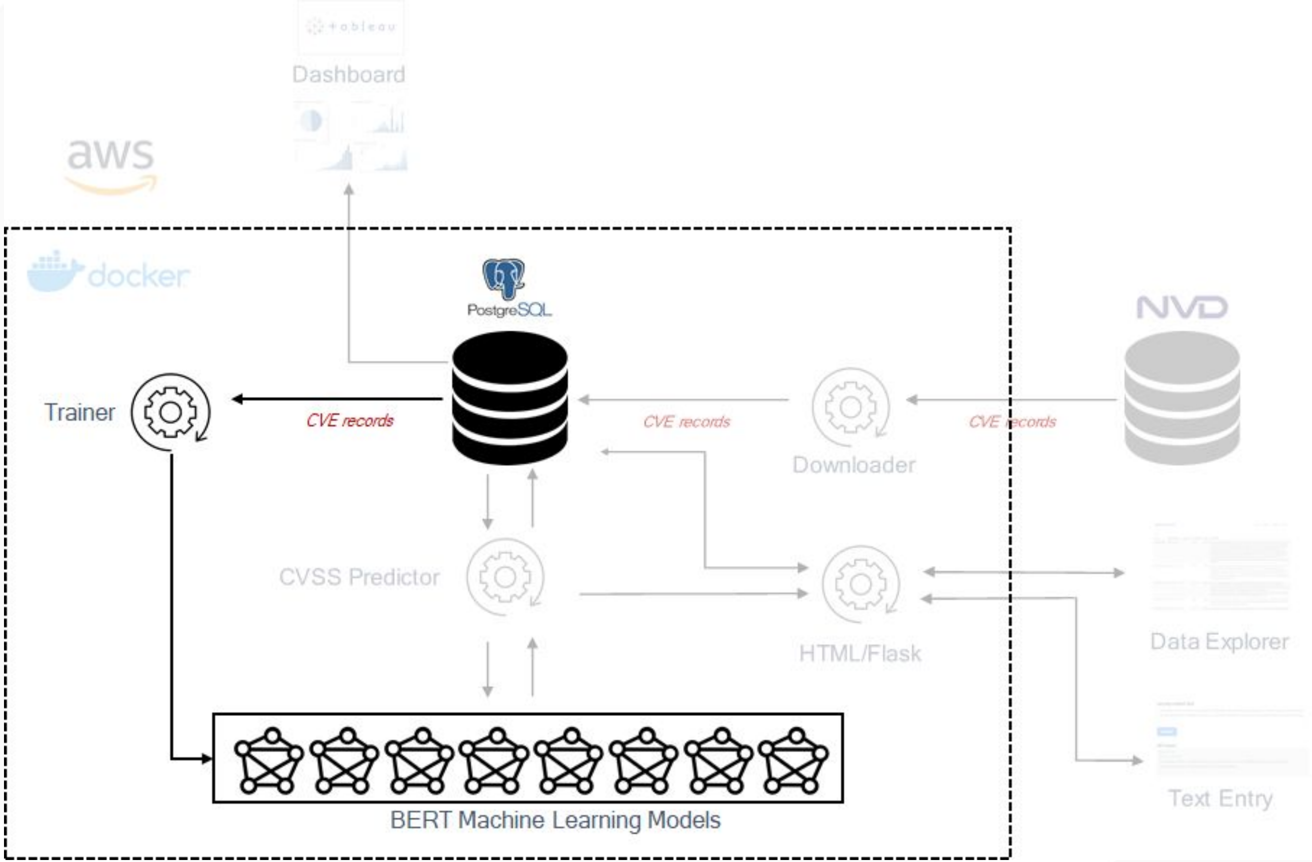
ETL Pipeline



GitHub: https://github.com/twlim1/260_capstone

VulnerWatch

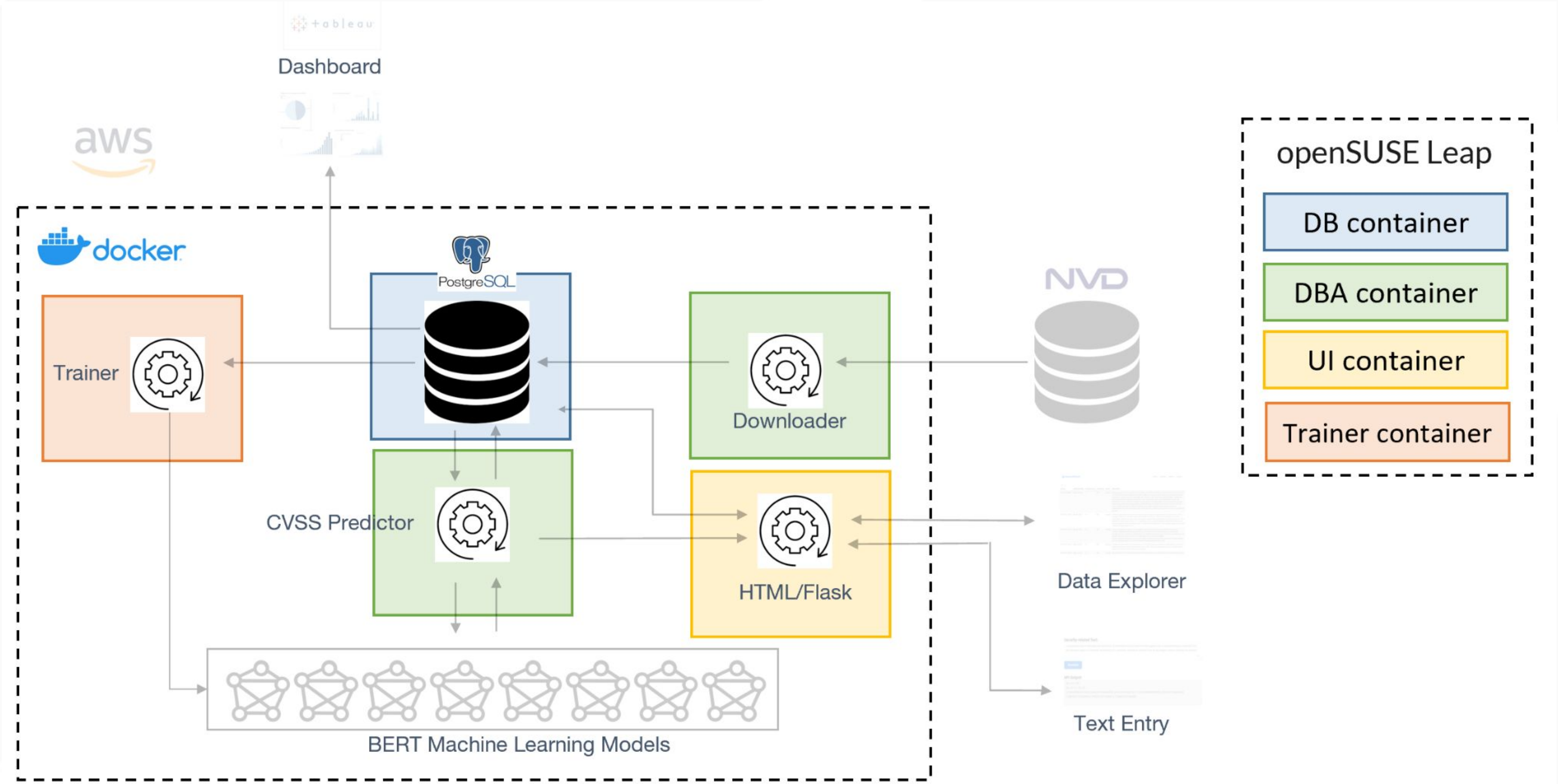
Training Pipeline



GitHub: https://github.com/twlim1/260_capstone

VulnerWatch

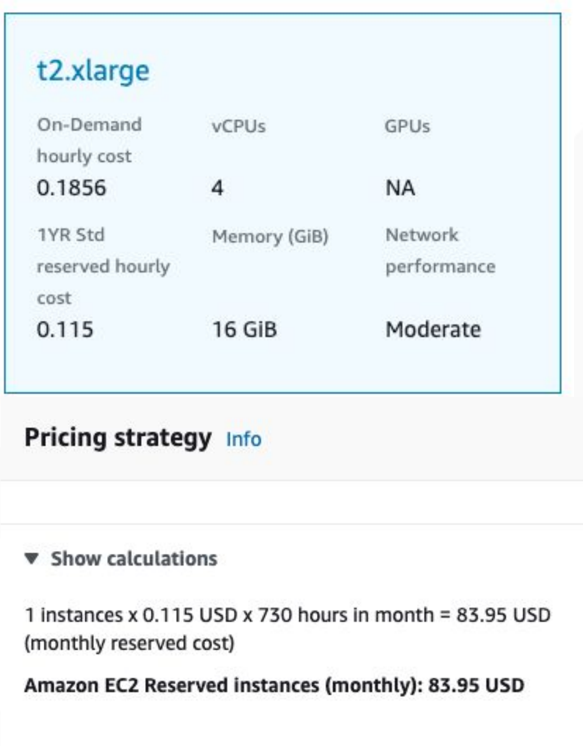
Scalability & Portability



GitHub: https://github.com/twlim1/260_capstone

System Cost

EC2 instance:
24 hrs/day



t2.xlarge

On-Demand hourly cost	vCPUs	GPUs
0.1856	4	NA
1YR Std reserved hourly cost	Memory (GiB)	Network performance
0.115	16 GiB	Moderate

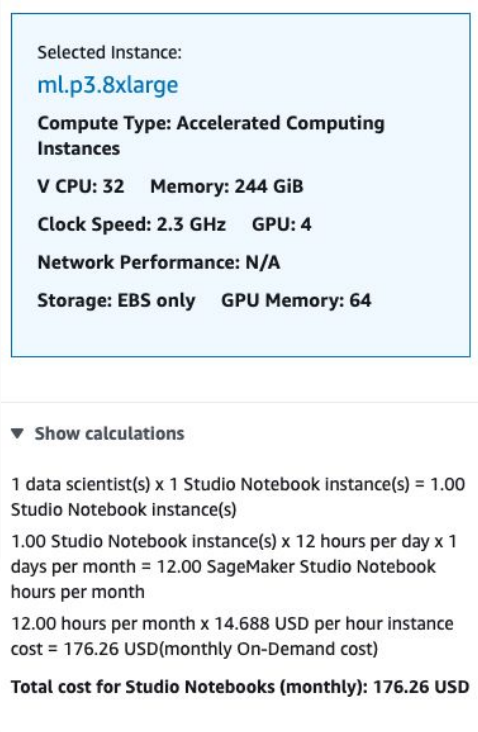
Pricing strategy Info

▼ Show calculations

1 instances x 0.115 USD x 730 hours in month = 83.95 USD (monthly reserved cost)

Amazon EC2 Reserved instances (monthly): 83.95 USD

SageMaker On-Demand GPU instance:
12 hrs fine-tuning/per month
to train 8 models. Each model takes 1.5 hr



Selected Instance:
ml.p3.8xlarge

Compute Type: Accelerated Computing Instances

V CPU: 32 Memory: 244 GiB

Clock Speed: 2.3 GHz GPU: 4

Network Performance: N/A

Storage: EBS only GPU Memory: 64

▼ **Show calculations**

1 data scientist(s) x 1 Studio Notebook instance(s) = 1.00 Studio Notebook instance(s)

1.00 Studio Notebook instance(s) x 12 hours per day x 1 days per month = 12.00 SageMaker Studio Notebook hours per month

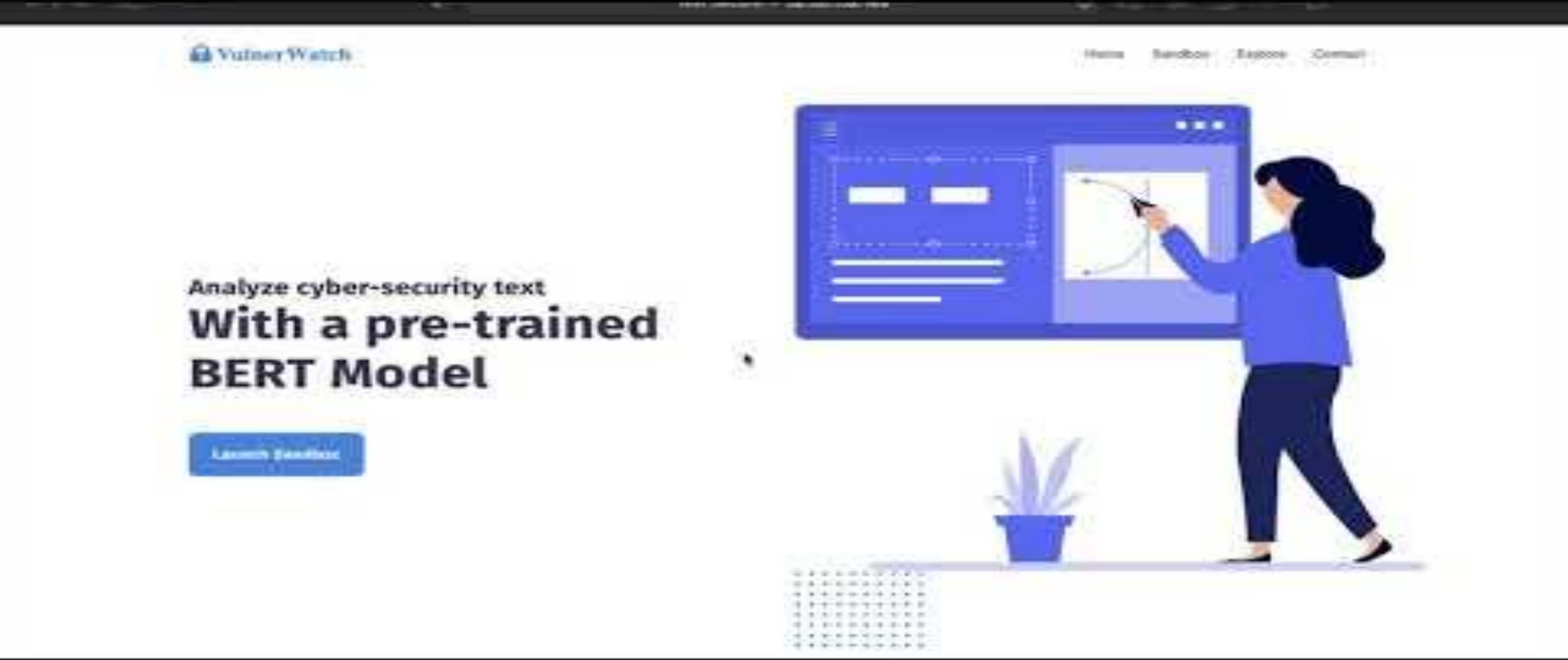
12.00 hours per month x 14.688 USD per hour instance cost = 176.26 USD(monthly On-Demand cost)

Total cost for Studio Notebooks (monthly): 176.26 USD

DEMO AND CONCLUSION

04

Product demo
Future work
Recapitulation and Conclusions

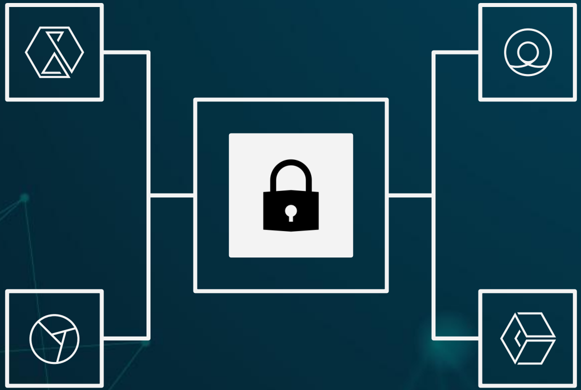


Analyze cyber-security text

With a pre-trained BERT Model

https://www.youtube.com/watch?v=rJ7rqURGZN0&t=5s

FUTURE WORK



Research if the product is commercially interesting and if that is the case make the product commercially ready

COMMERCIALLY READY

PUBLISH RESULT

Perform further analysis and share the result with scientific community as a research paper

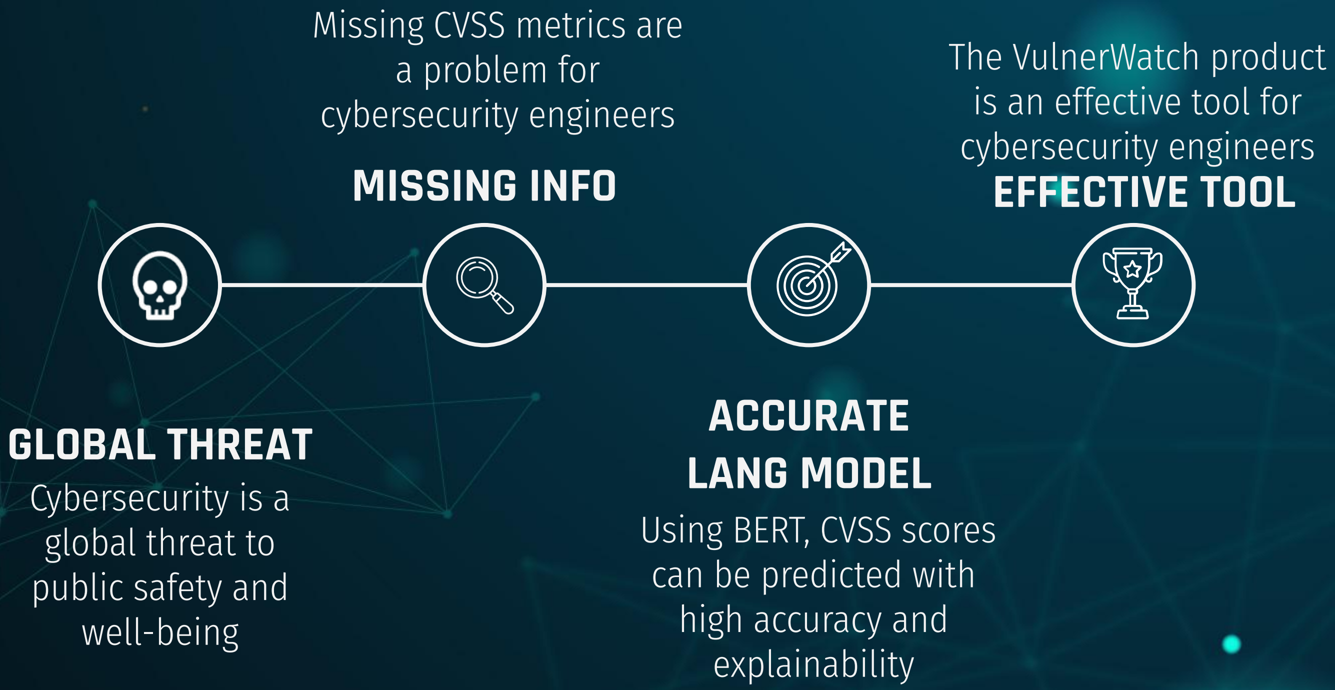
Extract long phrases instead of words and use the phrases to fine tune the language model for Question Answering

ADD QUESTION ANSWERING

PREDICTING CWEs

Use the same principle to predict Common Weakness and Enumerations (CWE)

RECAP AND CONCLUSION



GLOBAL THREAT

Cybersecurity is a global threat to public safety and well-being

MISSING INFO

Missing CVSS metrics are a problem for cybersecurity engineers

ACCURATE LANG MODEL

Using BERT, CVSS scores can be predicted with high accuracy and explainability

EFFECTIVE TOOL

The VulnerWatch product is an effective tool for cybersecurity engineers

THANKS!

Do you have any questions?

Slide template: https://slidesgo.com/theme/ai-tech-agency#search-agent