AIVRM

Presented by Team JISK
University of California, Berkeley
Berkeley, CA, USA
School of Information / MICS

The AIVRM Team

Yun-Hsi Tsai (Jimmy)
University of California, Berkeley
jimmy60814@ischool.berkeley.edu
School of Information / MICS

David (Ian) Clark
University of California, Berkeley
david.ian.clark@ischool.berkeley.edu
School of Information / MICS

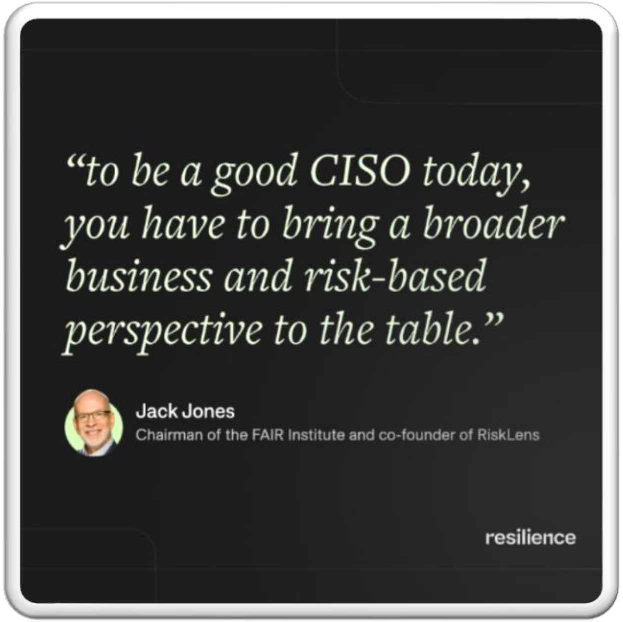
Shashank Kotturi
University of California, Berkeley
shashankkotturi@ischool.berkeley.edu
School of Information / MICS

Karim Elghobashi
University of California, Berkeley
happymeal@ischool.berkeley.edu
School of Information / MICS

Agenda

- Project motivation
- Problem Statement / Our Solution
- Hypothetical Company
- Live Demo
- AIVRM Architecture / Threat Modeling
- Q and A

The Motivation

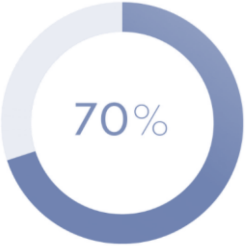


"to be a good CISO today, you have to bring a broader business and risk-based perspective to the table."

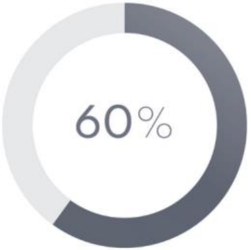
Jack Jones
Chairman of the FAIR Institute and co-founder of RiskLens

resilience

- According to a survey by the Ponemon Institute:



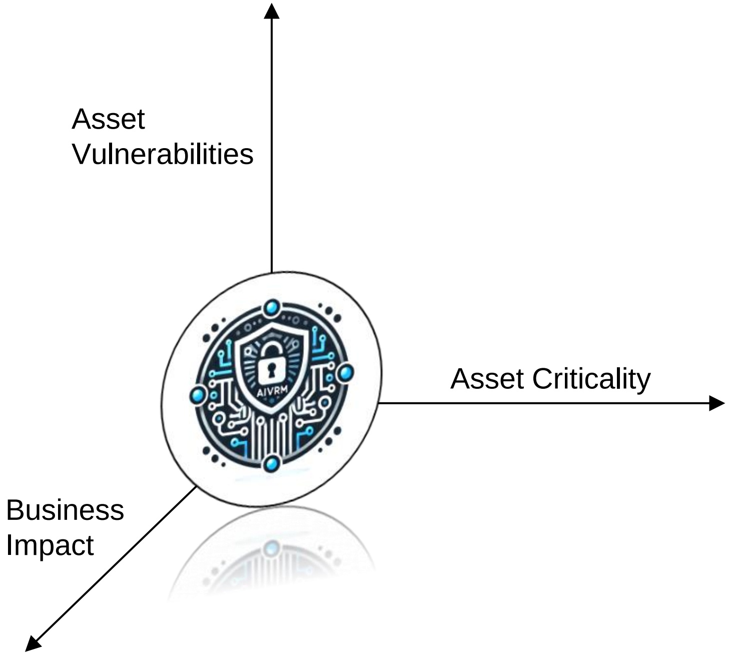
IT professionals believe financial quantification of cyber risk is inadequate.



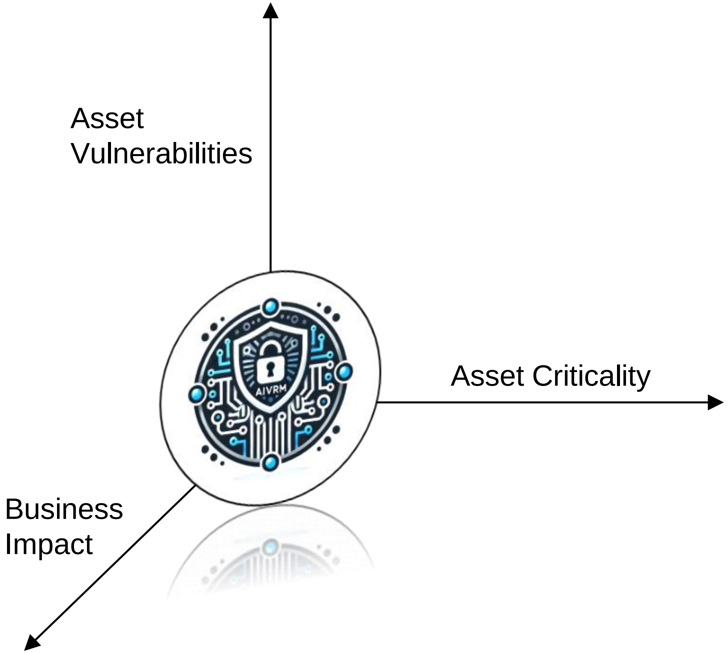
Organizations that do not calculate business impact during cyber risk assessment.

The Problem / Our Solution

- **The Problem is Strategic Disconnect:** Leadership focuses on business impact, while security teams prioritize technical vulnerabilities, causing misalignment.
- **AIVRM Solution:** Provides business impact insights on vulnerabilities, helping prioritize threats that affect critical assets.
- **Unified Approach:** Aligns security team efforts with leadership goals, enhancing organizational resilience and cybersecurity.
- **The AIVRM Triad:** Builds on three core principles: asset criticality, asset vulnerabilities, and business impact.



AIVRM Triad



- Leverage Machine Learning to analyze network traffic and score assets based on criticality metrics defined.
- Ingest vulnerability scanning reports and asset information.
- Define business impact of assets unique to an organization.
- Create scoring system which clearly defines both the technical and business impact of assets.

Demo Company – ACME Inc.

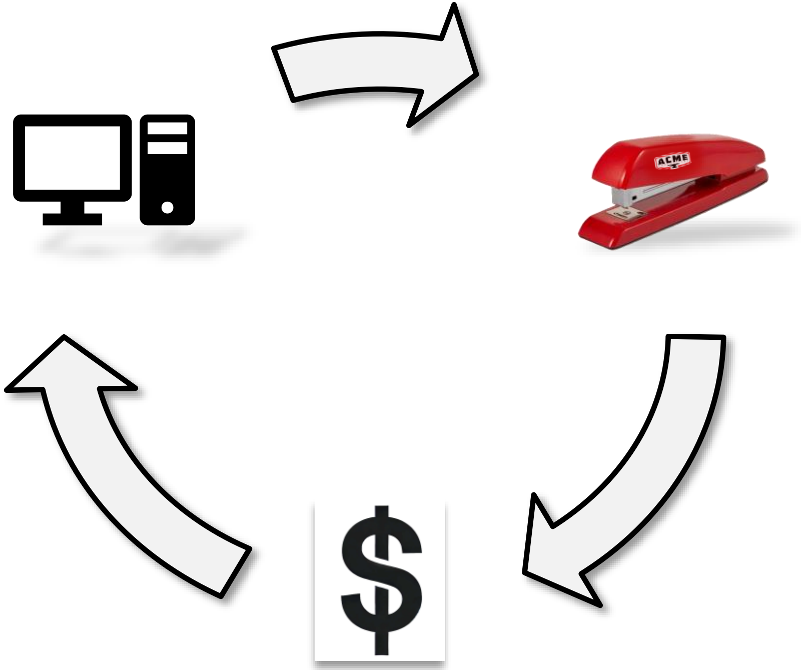
- Manufacturer of widgets and widget accessories.
- AIVRM installed on-premise.
- Data ingested from the following sources:
    - ManageEngine AssetExplorer
    - Nessus Vulnerability Scanner
    - PCAPs from perimeter Palo Alto firewall.

ACME Inc. Company Profile

- CISO: Bill Lumbergh
- # of Employees: 104
- # of Customers: 957
- Company Sales: Business to Business
- Top selling widget in 2024: Milton’s Red Stapler
- Total Yearly Company Revenue: $10,134,576

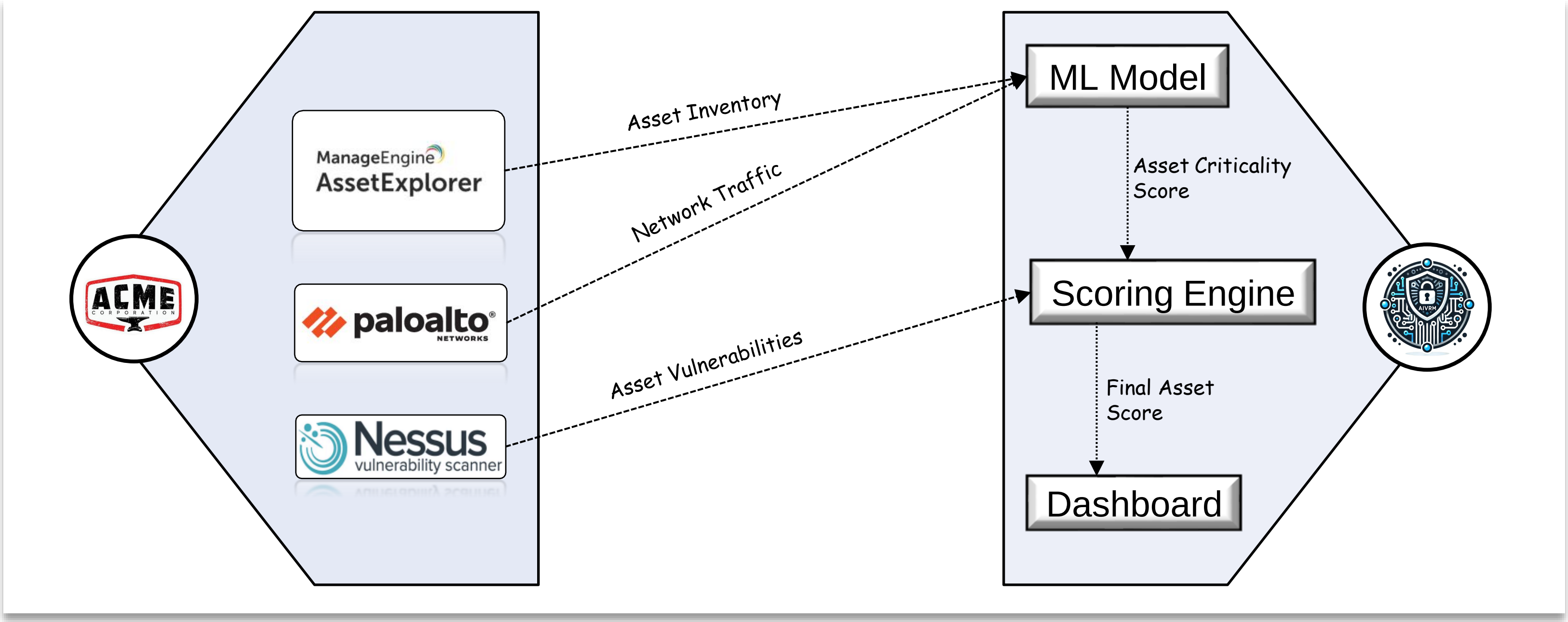
ACME Inc. Data Sources (Assets)

- Ten machines evaluated for demonstration purposes:
  - 4 Linux / 6 Windows Operating Systems
- To provide use-case clarity, the “Red Stapler” business line and associated machines will be examined further.

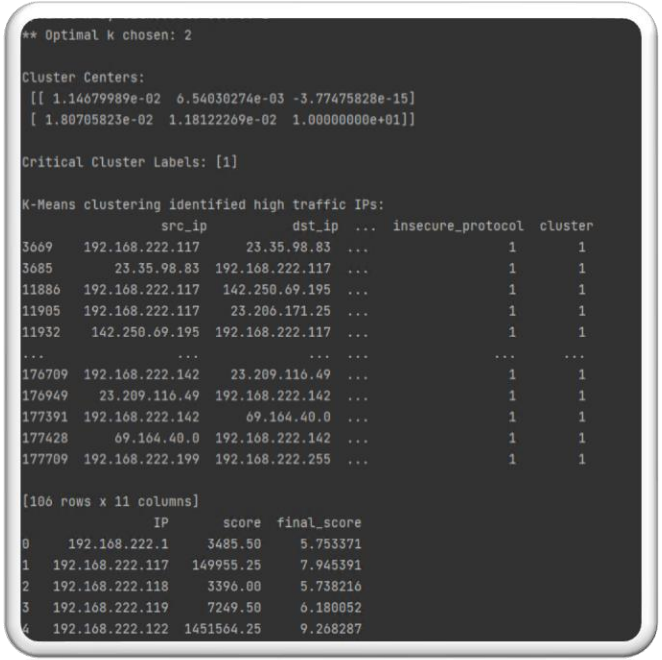


Live Demo

AIVRM System Overview

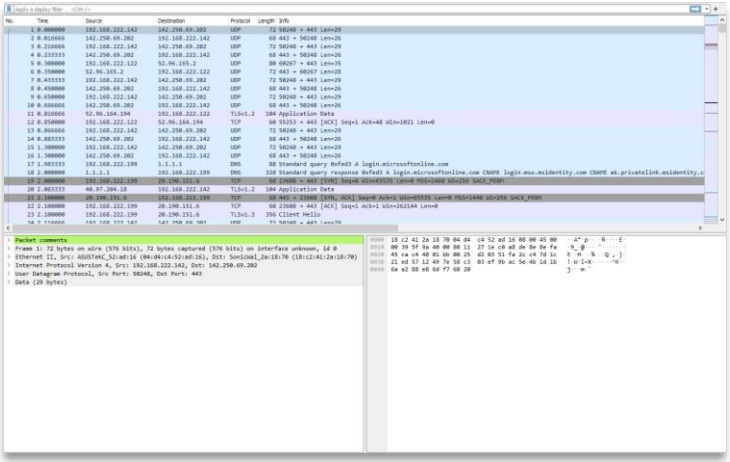


Defining Asset Criticality



```
** Optimal k chosen: 2

Cluster Centers:
 [[ 1.14679989e-02  6.54030274e-03 -3.77475828e-15]
 [ 1.80705823e-02  1.18122269e-02  1.00000000e+01]]

Critical Cluster Labels: [1]

K-Means clustering identified high traffic IPs:
                 src_ip           dst_ip  ...  insecure_protocol  cluster
3669    192.168.222.117      23.35.98.83  ...                  1        1
3685        23.35.98.83  192.168.222.117  ...                  1        1
11886   192.168.222.117   142.250.69.195  ...                  1        1
11905   192.168.222.117    23.206.171.25  ...                  1        1
11932    142.250.69.195  192.168.222.117  ...                  1        1
...                 ...              ...  ...                ...      ...
176709  192.168.222.142    23.209.116.49  ...                  1        1
176949    23.209.116.49  192.168.222.142  ...                  1        1
177391  192.168.222.142      69.164.40.0  ...                  1        1
177428      69.164.40.0  192.168.222.142  ...                  1        1
177709  192.168.222.199  192.168.222.255  ...                  1        1

[106 rows x 11 columns]
                IP       score  final_score
0     192.168.222.1     3485.50     5.753371
1   192.168.222.117   149955.25     7.945391
2   192.168.222.118     3396.00     5.738216
3   192.168.222.119     7249.50     6.180052
4   192.168.222.122  1451564.25     9.268287
```

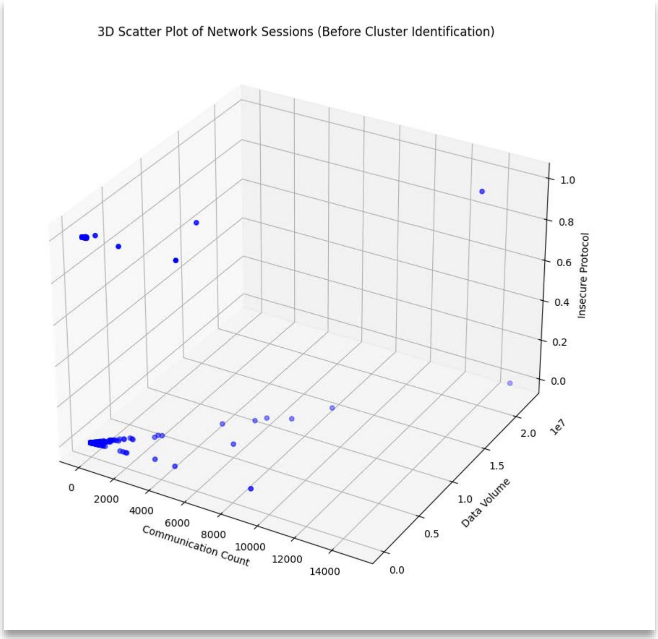
ML Model – Parse Network Traffic



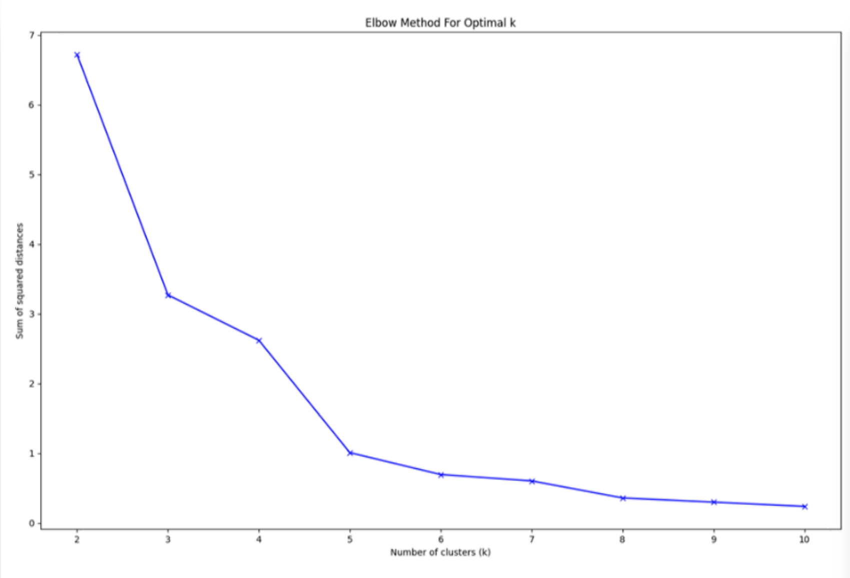
```
Apply a display filter ... <Ctrl-/>
No.   Time      Source            Destination       Protocol  Length Info
    1 0.000000  192.168.222.142   142.250.69.202    UDP           72 50248 → 443 Len=29
    2 0.016666  142.250.69.202    192.168.222.142   UDP           68 443 → 50248 Len=26
    3 0.216666  192.168.222.142   142.250.69.202    UDP           72 50248 → 443 Len=29
    4 0.233333  142.250.69.202    192.168.222.142   UDP           68 443 → 50248 Len=26
    5 0.300000  192.168.222.122   52.96.165.2       UDP           80 60267 → 443 Len=35
    6 0.350000  52.96.165.2       192.168.222.122   UDP           72 443 → 60267 Len=28
    7 0.433333  192.168.222.142   142.250.69.202    UDP           72 50248 → 443 Len=29
    8 0.450000  142.250.69.202    192.168.222.142   UDP           68 443 → 50248 Len=26
    9 0.650000  192.168.222.142   142.250.69.202    UDP           72 50248 → 443 Len=29
   10 0.666666  142.250.69.202    192.168.222.142   UDP           68 443 → 50248 Len=26
   11 0.816666  52.96.164.194     192.168.222.122   TLSv1.2      104 Application Data
   12 0.850000  192.168.222.122   52.96.164.194     TCP           60 55253 → 443 [ACK] Seq=1 Ack=48 Win=1021 Len=0
   13 0.866666  192.168.222.142   142.250.69.202    UDP           72 50248 → 443 Len=29
   14 0.883333  142.250.69.202    192.168.222.142   UDP           68 443 → 50248 Len=26
   15 1.300000  192.168.222.142   142.250.69.202    UDP           72 50248 → 443 Len=29
   16 1.300000  142.250.69.202    192.168.222.142   UDP           68 443 → 50248 Len=26
   17 1.983333  192.168.222.199   1.1.1.1           DNS           88 Standard query 0xfed3 A login.microsoftonline.com
   18 2.000000  1.1.1.1           192.168.222.199   DNS          328 Standard query response 0xfed3 A login.microsoftonline.com CNAME login.mso.msidentity.com CNAME ak.privatelink.msidentity.c
   19 2.000000  192.168.222.199   20.190.151.6      TCP           68 23608 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   20 2.083333  40.97.204.18      192.168.222.142   TLSv1.2      104 Application Data
   21 2.100000  20.190.151.6      192.168.222.199   TCP           68 443 → 23608 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
   22 2.100000  192.168.222.199   20.190.151.6      TCP           60 23608 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
   23 2.100000  192.168.222.199   20.190.151.6      TLSv1.3      356 Client Hello
   24 2.116666  192.168.222.142   142.250.69.202    UDP           72 50248 → 443 Len=29
```

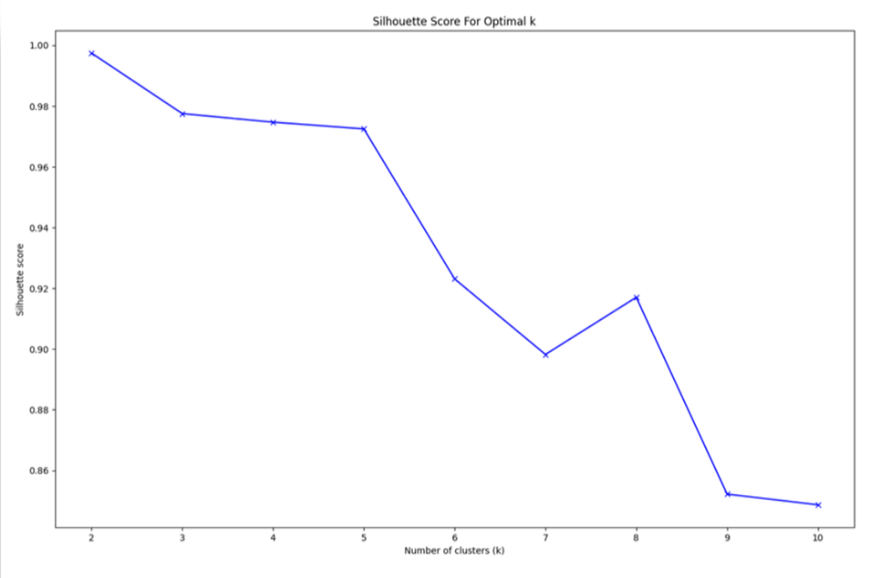
```
> Packet comments
> Frame 1: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface unknown, id 0
> Ethernet II, Src: ASUSTekC_52:ad:16 (04:d4:c4:52:ad:16), Dst: SonicWal_2a:18:70 (18:c2:41:2a:18:70)
> Internet Protocol Version 4, Src: 192.168.222.142, Dst: 142.250.69.202
> User Datagram Protocol, Src Port: 50248, Dst Port: 443
> Data (29 bytes)
```

```
0000  18 c2 41 2a 18 70 04 d4  c4 52 ad 16 08 00 45 00   ··A*·p·· ·R····E·
0010  00 39 5f 9a 40 00 80 11  27 1e c0 a8 de 8e 8e fa   ·9_·@··· '·······
0020  45 ca c4 48 01 bb 00 25  d2 03 51 fa 2c c4 7d 1c   E··H···% ··Q·,·}·
0030  21 ed 57 12 49 7e 58 c3  03 ef 9b ac 5e 4b 1d 1b   !·W·I~X· ····^K··
0040  6a a2 88 e8 6d f7 60 20                            j···m·`
```

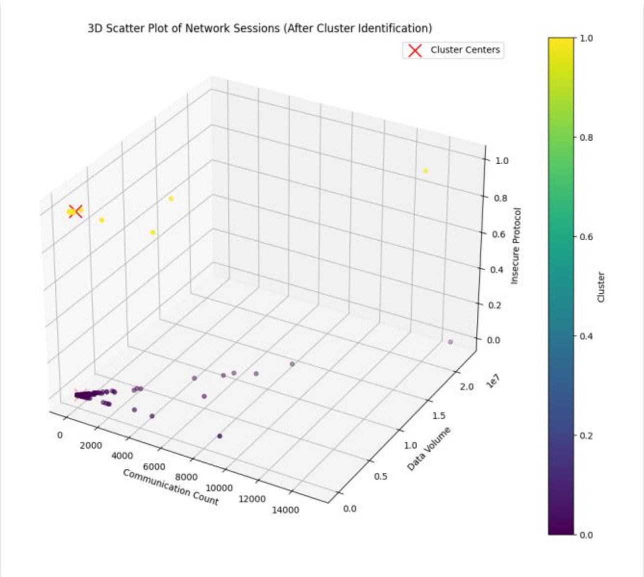


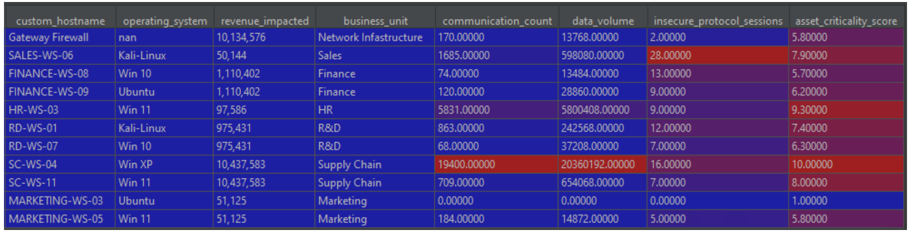
ML Model – Identify Critical Clusters of Data





ML Model – Output Asset Score

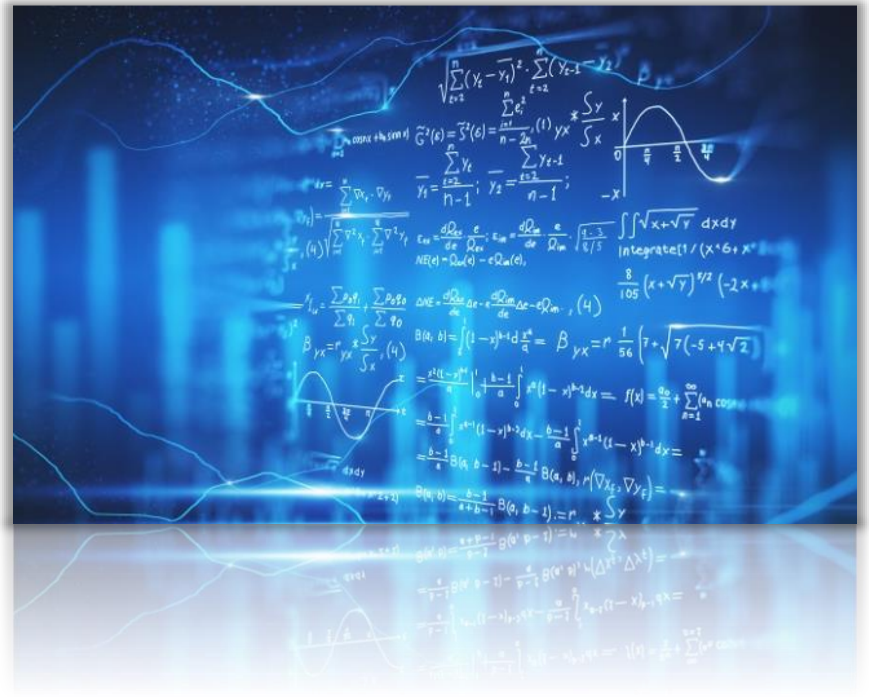




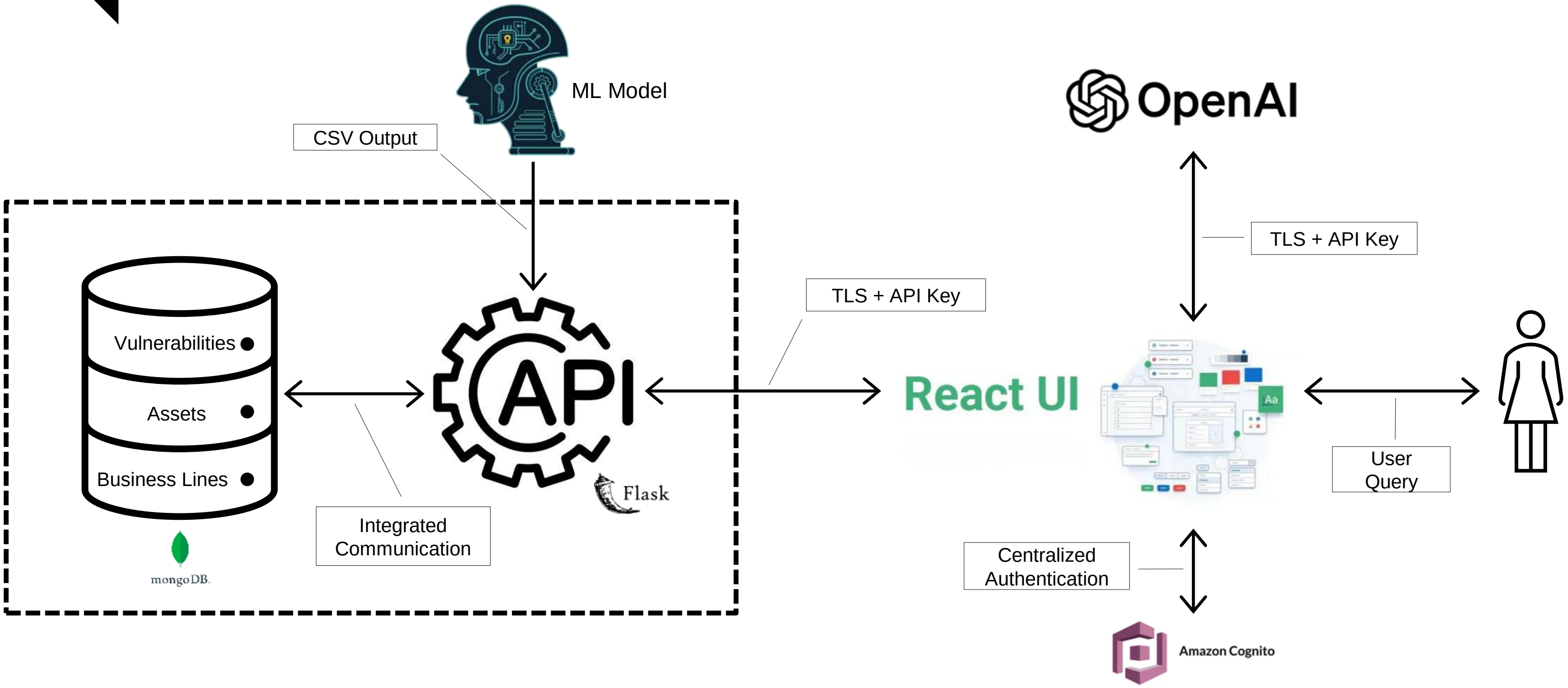
custom_hostname	operating_system	revenue_impacted	business_unit	communication_count	data_volume	insecure_protocol_sessions	asset_criticality_score
Gateway Firewall	nan	10,134,576	Network Infastructure	170.00000	13768.00000	2.00000	5.80000
SALES-WS-06	Kali-Linux	50,144	Sales	1685.00000	598080.00000	28.00000	7.90000
FINANCE-WS-08	Win 10	1,110,402	Finance	74.00000	13484.00000	13.00000	5.70000
FINANCE-WS-09	Ubuntu	1,110,402	Finance	120.00000	28860.00000	9.00000	6.20000
HR-WS-03	Win 11	97,586	HR	5831.00000	5800408.00000	9.00000	9.30000
RD-WS-01	Kali-Linux	975,431	R&D	863.00000	242568.00000	12.00000	7.40000
RD-WS-07	Win 10	975,431	R&D	68.00000	37208.00000	7.00000	6.30000
SC-WS-04	Win XP	10,437,583	Supply Chain	19400.00000	20360192.00000	16.00000	10.00000
SC-WS-11	Win 11	10,437,583	Supply Chain	709.00000	654068.00000	7.00000	8.00000
MARKETING-WS-03	Ubuntu	51,125	Marketing	0.00000	0.00000	0.00000	1.00000
MARKETING-WS-05	Win 11	51,125	Marketing	184.00000	14872.00000	5.00000	5.80000

Scoring Engine

- Combines asset criticality score from ML model and asset vulnerabilities (e.g., Nessus), to output the propriety ACE score.
- Optimized through numerous iterations to seamlessly integrate business and technical priorities.



AIVRM Architecture / Threat Modeling



References

- Jones, Jack. (2024). Resilience's Post. LinkedIn. https://www.linkedin.com/posts/resilience-cyber_riskmanagement-riskquantification-ciso-activity-7212107436973834240-yeT5/?utm_source=share&utm_medium=member_ios
- CVE. (2024). [CVE Logo]. https://www.cve.org/
- Fictional Companies Wiki. (n.d.). [ACME Corporation Logo]. https://fictionalcompanies.fandom.com/wiki/ACME
- Luele, Marcus. (2019). [Bill Lumbergh Image]. *'Office Space': 20 Years Later*. https://filmdaze.net/office-space-20th-anniversary/
- Office Space Wiki. (n.d.). [Red Stapler Image]. https://officespace.fandom.com/wiki/Red_Stapler
- Creamer, Lanette. (2019). [ManageEngine AssetExplorer Logo]. PCMag. *ManageEngine AssetExplorer Review*. https://www.pcmag.com/reviews/manageengine-assetexplorer
- PaloAlto Networks. (2024). [PaloAlto Networks Logo]. https://www.paloaltonetworks.com/company/brand
- Collins, Jennifer. (2013). [Nessus Vulnerability Scanner Logo]. Tenable. *Nessus Product Names Simplified.* https://www.tenable.com/blog/nessus-product-names-simplified
- Adobe Stock. (n.d.). [API Image]. https://stock.adobe.com/search/images?k=api+logo
- Mak, Yue Weng. (2020). [Flask Logo]. Medium. *Beautify Flask Web App using CSS, HTML.* https://medium.com/an-idea/beautify-flask- web-app-using-css-html-d574332f710f
- Bhargava, Akshay. (2022). [Amazon Cognito Logo]. Medium. *AWS Cognito | Understanding User Pool | Part-1*. https://aws.plainenglish.io/aws-cognito-understanding-user-pool-part-1-67f9d3adef5a
- Daley, Sam. (2022). [Machine Learning]. BuiltIn. *Machine Learning Technology*. https://builtin.com/machine-learning
- AHT Tech. (n.d.). [React UI Image]. *React UI component: Top best libraries and framework you should know.* https://blog.arrowhitech.com/react-ui-component-top-best-libraries-and-framework-you-should-know/
- Carpena, Maria. (2023). [OpenAI Logo]. *What is OpenAI? Here's Everything a Marketer Needs to Know.* https://www.webfx.com/blog/marketing/what-is-openai/
- Onejohi. (2019). [Flask Logo]. Medium. *Building a simple REST API with Python and Flask.* https://medium.com/@onejohi/building-a-simple-rest-api-with-python-and-flask-b404371dc699
- DTEX. (2024). *2023 Cost of Insider Risks Global Report*. https://www.dtexsystems.com/resource-ponemon-insider-risks-global-report/

Special Thanks!

Ryan Liu
Lecturer – Cyber 295, Capstone
University of California, Berkeley
School of Information / MICS

Sekhar Sarukkai
Lecturer – Cyber 295, Capstone
University of California, Berkeley
School of Information / MICS

Clarence Chio
Lecturer – Cyber 207, Applied
Machine Learning for Cybersecurity
University of California, Berkeley
School of Information / MICS

Q and A