

Predicting Cyber scores with Random Forest

Rename notebook

In this analysis, we p at containing various features related to the cybersecurity posture of different organizations. The key steps involved converting asset values from string formats (millions or billions) to numeric values, encoding categorical features into numerical values, and normalizing certain numerical features. A custom cyber score was created by combining several factors, such as threat level, vulnerability, control strength, time to remediate, security maturity, and security spending. The cyber score was then discretized into categories ranging from 1 to 10. A Random Forest Regressor model was trained to predict the cyber scores, and recommendations were generated based on the predicted scores

Importing Libraries

```
import pandas as pd
from sklearn.preprocessing import LabelEncoder, MinMaxScaler
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestRegressor
from sklearn.metrics import mean_squared_error, r2_score
import numpy as np
```

Reading the Data File

```
# Load the data

data = pd.read_excel("/content/cyber_data.xlsx")
```

EDA of the Data

```
data.head()
```



	Organization	Incident	Asset Value	Threat Level	Vulnerability	Control Strength	Details
0	Adobe	Adobe Data Breach 2024	1B	Medium	Medium	High	Customer accounts compromised, data stolen
1	Airbnb	Airbnb API Exposure 2024	850M	Medium	Medium	Medium	Host and guest information exposed through API
2	Amazon	Amazon Internal Leak 2024	1.3B	Medium	Medium	High	Internal documents accessed, data leaked
3	American Airlines	AA Payment Info Breach 2024	850M	High	Medium	Medium	Customer payment information exposed
4	Apple	Apple API Vulnerability 2024	1.6B	Medium	Medium	High	Customer information accessed through API vuln.

Exl

Exl

Next steps:

Generate code with data

View recommended plots

```
data.info()
```



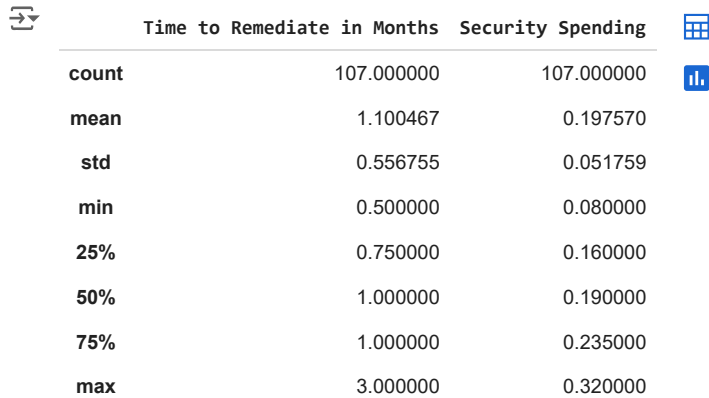
```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 107 entries, 0 to 106
Data columns (total 14 columns):
#   Column              Non-Null Count  Dtype
---  -
0   Organization         107 non-null    object
1   Incident             107 non-null    object
```

```

2  Asset Value                107 non-null  object
3  Threat Level               107 non-null  object
4  Vulnerability              107 non-null  object
5  Control Strength           107 non-null  object
6  Details                    107 non-null  object
7  Attack Type                107 non-null  object
8  Impact                     107 non-null  object
9  Root Cause                 107 non-null  object
10 Time to Remediate in Months 107 non-null  float64
11 Industry                   107 non-null  object
12 Security Maturity           107 non-null  object
13 Security Spending           107 non-null  float64
dtypes: float64(2), object(12)
memory usage: 11.8+ KB

```

```
data.describe()
```



	Time to Remediate in Months	Security Spending
count	107.000000	107.000000
mean	1.100467	0.197570
std	0.556755	0.051759
min	0.500000	0.080000
25%	0.750000	0.160000
50%	1.000000	0.190000
75%	1.000000	0.235000
max	3.000000	0.320000

Converting ASSET column string to Numerical

```

# Convert Asset Value to numeric
def convert_asset_value(value):
    if isinstance(value, str):
        if 'M' in value:
            return float(value.replace('M', '')) * 1e6
        elif 'B' in value:
            return float(value.replace('B', '')) * 1e9
    return float(value)

data['Asset Value'] = data['Asset Value'].apply(convert_asset_value)

```

Encoding Categorical columns into Numerical Values

```

# Define a function to convert categorical features to numerical values
def encode_labels(df, column):
    le = LabelEncoder()
    df[column] = le.fit_transform(df[column])
    return df

# Encode categorical features
categorical_columns = ['Threat Level', 'Vulnerability', 'Control Strength', 'Industry', 'Security Maturity']
for col in categorical_columns:
    data = encode_labels(data, col)

```

Normalizing Features: Asset Value and Time to remediate in Months

Normalization of asset value is done to make it easily comparable with other features of the dataset

```

# Normalize numerical features (excluding Security Spending)
scaler = MinMaxScaler()
numerical_columns = ['Asset Value', 'Time to Remediate in Months']
data[numerical_columns] = scaler.fit_transform(data[numerical_columns])

```

Rename notebook

	Organization	Incident	Asset Value	Threat Level	Vulnerability	Control Strength	Details	Attack Type	Impact	Root Cause	Reinforcement
0	Adobe	Adobe Data Breach 2024	0.571429	1	2	0	Customer accounts compromised, data stolen	Phishing	Financial	Social Engineering	
1	Airbnb	Airbnb API Exposure 2024	0.464286	1	2	2	Host and guest information exposed through API	API Exploitation	Reputational	Configuration Error	
2	Amazon	Amazon Internal Leak 2024	0.785714	1	2	0	Internal documents accessed, data leaked	Insider Threat	Operational	Insider Access	
3	American Airlines	AA Payment Info Breach 2024	0.464286	0	2	2	Customer payment information exposed	Malware	Financial	Malware Infection	
4	Apple	Apple API Vulnerability 2024	1.000000	1	2	0	Customer information accessed through API vuln.	API Exploitation	Reputational	Poor API Security	

Next steps: [Generate code with data](#) [View recommended plots](#)

Creating a CyberScore Formula and adding the column to the data

```
# Create the cyber score
data['cyber_score'] = (
    data['Threat Level'] +
    data['Vulnerability'] +
    (1 - data['Control Strength']) +
    data['Time to Remediate in Months'] +
    (1 - data['Security Maturity']) +
    (1 - data['Security Spending'])
)

# Discretize the cyber score into categories 1-10
data['cyber_score'] = np.ceil(MinMaxScaler((1, 10)).fit_transform(data[['cyber_score']])).astype(int)

# Prepare the data for training
X = data.drop(columns=['Organization', 'Incident', 'Details', 'Attack Type', 'Impact', 'Root Cause', 'cyber_score'])
y = data['cyber_score']
```

Splitting the Dataset into Training and Testing

```
# Split the data into training and testing sets
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)
```

Training the Model

```
# Train a Random Forest Regressor
model = RandomForestRegressor(n_estimators=100, random_state=42)
model.fit(X_train, y_train)
```

RandomForestRegressor

RandomForestRegressor(random_state=42)

```
# Predict on the test set
y_pred = model.predict(X_test)
```

Rename notebook

Model Evaluation

```
# Evaluate the model
mse = mean_squared_error(y_test, y_pred)
r2 = r2_score(y_test, y_pred)
```

```
print(f'MSE: {mse}, R2: {r2}')
```

```
➦ MSE: 0.34937727272727265, R2: 0.9181120581113802
```

The model has good Accuracy.

Generating Recommendations based on following categories:-

(1)0-2=Poor Score (2)3-5=Moderate (3)6-8=Good (4)9-10=Best Score

```
# Generate recommendations based on cyber score
def generate_recommendations(cyber_score):
    if cyber_score <= 2:
        return [
            "Critical security overhaul needed.",
            "Implement advanced security protocols immediately.",
            "Increase budget for cybersecurity improvements.",
            "Engage with top-tier cybersecurity firms for an in-depth assessment."
        ]
    elif cyber_score <= 5:
        return [
            "Immediate action required to address vulnerabilities.",
            "Implement strict access controls and monitoring.",
            "Engage with cybersecurity consultants for comprehensive risk assessment."
        ]
    elif cyber_score <= 8:
        return [
            "Conduct a thorough security audit.",
            "Increase security training for employees.",
            "Invest in advanced threat detection systems."
        ]
    else:
        return [
            "Maintain current security measures.",
            "Regularly update and review security policies."
        ]
```

```
data['recommendations'] = data['cyber_score'].apply(generate_recommendations)
```

```
# Display the updated dataframe with recommendations
data[['Organization', 'cyber_score', 'recommendations']]
```



1 to 100 of 107 entries

Filter



index	Organ	ore	recommendations
0	Adobe	7	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
1	Airbnb	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
2	Amazon	9	Maintain current security measures.,Regularly update and review security policies.
3	American Airlines	4	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
4	Apple	10	Maintain current security measures.,Regularly update and review security policies.
5	Atlassian	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
6	British Airways	2	Critical security overhaul needed.,Implement advanced security protocols immediately.,Increase budget for cybersecurity improvements.,Engage with top-tier cybersecurity firms for an in-depth assessment.
7	Capcom	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
8	Cisco	10	Maintain current security measures.,Regularly update and review security policies.
9	Discord	4	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
10	DoorDash	2	Critical security overhaul needed.,Implement advanced security protocols immediately.,Increase budget for cybersecurity improvements.,Engage with top-tier cybersecurity firms for an in-depth assessment.
11	Dropbox	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
12	eBay	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
13	Facebook	8	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
14	FedEx	2	Critical security overhaul needed.,Implement advanced security protocols immediately.,Increase budget for cybersecurity improvements.,Engage with top-tier cybersecurity firms for an in-depth assessment.
15	GitHub	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
16	GitLab	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
17	GoDaddy	6	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
18	Google	10	Maintain current security measures.,Regularly update and review security policies.
19	Hulu	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
20	IBM	10	Maintain current security measures.,Regularly update and review security policies.
21	Instagram	3	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
22	Intel	8	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
23	LinkedIn	3	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
24	Lyft	7	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
25	Marriott	4	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
26	Mastercard	9	Maintain current security measures.,Regularly update and review security policies.
27	MGM Resorts	4	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
28	Microsoft	9	Maintain current security measures.,Regularly update and review security policies.
29	MOVEit	6	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
30	NASA	4	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
31	Netflix	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
32	Oracle	10	Maintain current security measures.,Regularly update and review security policies.
33	PayPal	9	Maintain current security measures.,Regularly update and review security policies.
34	PepsiCo	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
35	Pinterest	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
36	Reddit	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
37	Salesforce	9	Maintain current security measures.,Regularly update and review security policies.
38	Samsung	6	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
39	Shopify	4	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
40	Slack	9	Maintain current security measures.,Regularly update and review security policies.
41	Snapchat	4	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.

42	Sony Pictures	7	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
43	SpaceX	8	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
44	Spotify	4	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
45	Squarespace	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
46	Tesla	7	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
47	TikTok	4	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
48	T-Mobile	6	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
49	Toyota	7	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
50	Twitter	6	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
51	Uber	7	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
52	University of Manchester	6	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
53	Verizon	8	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
54	Yahoo	4	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
55	Zoom	7	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
56	L'Oréal	3	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
57	LinkedIn Learning	8	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
58	Duolingo	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
59	Delta Airlines	8	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
60	Warner Bros.	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
61	Southwest Airlines	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
62	DreamWorks Animation	2	Critical security overhaul needed.,Implement advanced security protocols immediately.,Increase budget for cybersecurity improvements.,Engage with top-tier cybersecurity firms for an in-depth assessment.
63	YouTube	6	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
64	Unilever	2	Critical security overhaul needed.,Implement advanced security protocols immediately.,Increase budget for cybersecurity improvements.,Engage with top-tier cybersecurity firms for an in-depth assessment.
65	Skillshare	8	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
66	Procter & Gamble	8	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
67	Disney	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
68	Lionsgate	7	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
69	Universal Pictures	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
70	UPS	7	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
71	Khan Academy	7	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
72	FutureLearn	4	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
73	DHL	2	Critical security overhaul needed.,Implement advanced security protocols immediately.,Increase budget for cybersecurity improvements.,Engage with top-tier cybersecurity firms for an in-depth assessment.
74	Coursera	4	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
75	Paramount Pictures	4	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
76	Coca-Cola	3	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
77	Johnson & Johnson	7	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
78	Blackboard	7	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
79	MGM Studios	4	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.
80	Chase	5	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.

	Gregg		with cybersecurity consultants for comprehensive risk assessment.
81	Nestlé	7	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
82	Kimberly-Clark	7	Conduct a thorough security audit.,Increase security training for employees.,Invest in advanced threat detection systems.
83	Reckitt Benckiser	1	Critical security overhaul needed.,Implement advanced security protocols immediately.,Increase budget for cybersecurity improvements.,Engage with top-tier cybersecurity firms for an in-depth assessment.
84	edX	4	Immediate action required to address vulnerabilities.,Implement strict access controls and monitoring.,Engage with cybersecurity consultants for comprehensive risk assessment.