Models for Cyber Threat Analysis

Cyber threat analysis models are structured methods used to understand, detect, analyze, and prevent cyber attacks. These models help security professionals study attacker behavior, identify vulnerabilities, assess risks, and predict future threats.

Cyber threat analysis uses two major types of models:

1. **Security Framework Models (Conceptual models)**
2. **Data Analytics / Statistical Models (Data-driven models)**

Security Framework Models (Conceptual Models)

These models help in understanding how cyber attacks happen, how attackers behave, and how organizations should respond.

1.Cyber Kill Chain Model

The Cyber Kill Chain model was developed by Lockheed Martin.

This model explains that every cyber attack happens in stages. It divides an attack into seven steps, starting from collecting information about the target and ending with stealing data or damaging the system.

First, the attacker gathers information (reconnaissance). Then they prepare malware (weaponization). After that, they send it through email or links (delivery). If the system has a weakness, they enter the system (exploitation). Then they install malware, control the system remotely, and finally achieve their goal like stealing data.

This model helps organizations stop the attack at an early stage.

2 .MITRE ATT&CK Framework

The MITRE ATT&CK framework was developed by MITRE Corporation.

This model is like a big list of real attack techniques used by hackers. It explains:

- What the attacker wants to do (tactics)
- How the attacker does it (techniques)

For example, if the attacker wants to steal passwords, they may use phishing or credential dumping. This model helps security teams understand real-world attack methods and improve detection systems.

3. STRIDE Model

The STRIDE model was developed by Microsoft.

This model is used when designing software. It helps developers think about possible threats.

STRIDE stands for:

- Spoofing (pretending to be someone else)
- Tampering (changing data)
- Repudiation (denying actions)
- Information Disclosure (leaking data)
- Denial of Service (stopping services)
- Elevation of Privilege (getting higher access)

It helps prevent security problems before software is released.

4. Diamond Model

The Diamond Model explains cyber attacks using four parts:

- Attacker
- Tools used
- Infrastructure (servers, domains)
- Victim

It helps understand the relationship between the attacker and the target system.

5. NIST Risk Management Framework

This framework was developed by National Institute of Standards and Technology.

It helps organizations manage cyber risk step by step. It includes identifying risks, applying security controls, checking if they work, and continuously monitoring systems.

It is mainly used in companies and government organizations.

Data Analytics / Statistical Models (Used to Analyze Cyber Data)

These models use mathematics and statistics to study cyber data like logs, traffic, login attempts, and attack reports.

1. Descriptive Statistical Analysis

Descriptive statistics help summarize and understand past cyber incidents. It includes measures such as mean, median, mode, variance, and standard deviation.

For example, an organization may calculate the average number of failed login attempts per day. It may also find the most common type of malware detected in a month. This model does not predict future attacks, but it helps understand historical data and create dashboards for visualization.

2.Inferential Statistics

Inferential statistics help draw conclusions from sample data. It includes hypothesis testing and confidence intervals.

For example, if a company wants to know whether cyber attacks increased after launching a new website, analysts can test the hypothesis using statistical methods. This helps in decision-making and evaluating security policies.

3.Time Series Analysis

Time series analysis studies data collected over time. Cyber attacks usually follow patterns such as daily, weekly, or seasonal trends.

For example, phishing attacks may increase during festive seasons. By using time series models like moving averages and ARIMA, analysts can predict future attack patterns and prepare defenses in advance.

This model is very useful in cyber threat visualization dashboards.

4 .Regression Analysis

Regression analysis identifies the relationship between dependent and independent variables.

Linear regression predicts continuous outcomes, such as the expected number of attacks next month. Logistic regression predicts binary outcomes, such as whether traffic is malicious or normal.

This model helps build predictive intrusion detection systems.

5.Correlation Analysis

Correlation analysis measures how strongly two variables are related.

For example, analysts may find that high network traffic correlates with an increase in intrusion attempts. This helps in identifying factors that influence cyber attacks.

6.Clustering Techniques

Clustering is an unsupervised learning method that groups similar data together.

For example, network traffic can be grouped into normal user behavior and suspicious behavior. Malware samples can also be grouped based on similarity.

Common clustering algorithms include K-Means and Hierarchical Clustering. This method is useful for discovering unknown threats.

7. Classification Algorithms

Classification models categorize data into predefined classes such as malicious or safe.

Common algorithms include:

- Decision Trees
- Random Forest
- Support Vector Machine (SVM)
- Naïve Bayes

These models are widely used in spam detection, malware detection, and intrusion detection systems.

8.Anomaly Detection Models

Anomaly detection identifies unusual behavior that does not follow normal patterns.

For example, if an employee suddenly downloads large amounts of data at midnight, the system flags it as suspicious.

Techniques include:

- Z-score analysis
- Isolation Forest
- One-Class SVM

This model is very important for detecting zero-day attacks.

9.Bayesian Statistical Models

Bayesian models use probability theory to calculate the likelihood of a cyber attack.

For example, in spam detection, Bayesian models calculate the probability that an email is spam based on certain keywords.

These models update their predictions when new data is received.

10. Markov Models

Markov models analyze sequences of events and transitions between system states.

For example, if a user fails login attempts multiple times and then suddenly gains administrator access, this sequence may indicate a cyber attack.

Markov models help detect multi-stage attacks.

11. Principal Component Analysis (PCA)

PCA is a dimensionality reduction technique. In cybersecurity, there may be thousands of features in network traffic data. PCA reduces the number of variables while keeping important information.

This helps improve the performance of machine learning models and detect patterns more efficiently.

12. Neural Networks and Deep Learning

Neural networks are advanced models inspired by the human brain. They can detect complex patterns in large cybersecurity datasets.

Deep learning models such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) are used for malware detection and network traffic analysis.

They are highly accurate but require large datasets.