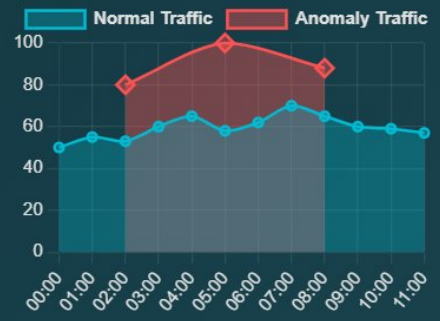
Detecting Cyber Threats Through Anomaly Detection in Network Traffic Data

1. Introduction to Network Traffic Anomaly Detection

Network traffic anomaly detection involves monitoring data flow within a network to identify patterns that deviate significantly from expected behavior. These anomalies can indicate potential cyber threats such as intrusions, denial of service attacks, or unauthorized access. This process helps in early threat detection and prevention.

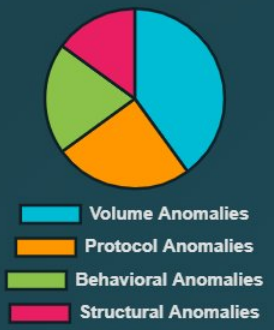


2. Types of Anomalies in Network Traffic

Anomalies in network traffic can be classified into several types such as:

- Volume anomalies - sudden spikes or drops in traffic volume
- Protocol anomalies - use of unusual protocol types
- Behavioral anomalies - unexpected access patterns or flow
- Structural anomalies - unexpected connection topology

Understanding these types helps in identifying the nature of the threat.

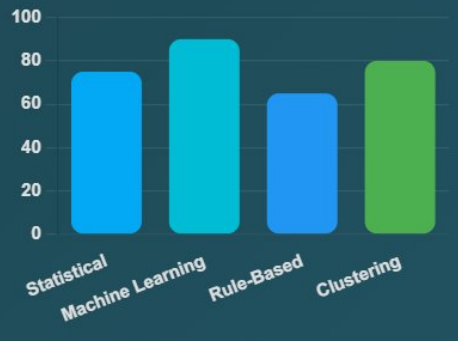


3. Techniques for Anomaly Detection

Various techniques are used to detect anomalies, including:

- Statistical Methods - detect deviations from statistical norms
- Machine Learning - use models to classify normal and abnormal traffic
- Rule-Based Detection - use predefined patterns and heuristic rules
- Clustering Algorithms - group similar traffic and highlight outliers

The effectiveness of these techniques varies based on network complexity and threat type.



Statistical
Machine Learning
Rule-Based
Clustering

4. Visualization of Anomalies Using Graphs

Visualizing network traffic anomalies helps analysts quickly identify threats and understand their characteristics. Scatter plots, line graphs, and heatmaps are common tools to represent traffic volume, anomaly scores, and time patterns. Effective visualization supports faster and more accurate response to cyber threats.