Supervised Learning Models:

Model	Example Use Case
Logistic Regression	Phishing email detection
Decision Trees	Malware classification
Random Forests	Intrusion detection
Gradient Boosting Machines	Predicting malicious URLs
Support Vector Machines (SVMs)	Network traffic classification
K-Nearest Neighbors (KNN)	Classifying types of network traffic
Linear Regression	Predicting the time to next security breach
Neural Networks	Spam email classification
Convolutional Neural Networks	Analyzing security camera footage for suspicious activities
Recurrent Neural Networks (RNNs)	Predicting sequences of security incidents based on historical data
Transformers	Analyzing sequences of security logs for threats
Named Entity Recognition (NER)	Identifying sensitive information in documents
Sentiment Analysis	Detecting threatening communications
Text Classification	Classifying emails as spam or phishing

Unsupervised Learning Models:

Model	Example Use Case
Isolation Forest	Anomaly detection in network traffic
One-Class SVM	Detecting unusual login activities
Autoencoders	Detecting unusual patterns in log files
K-Means Clustering	Grouping similar security incidents
DBSCAN	Identifying noise in network traffic data
Principal Component Analysis	Reducing dimensionality of security feature sets
Q-Learning	Adapting firewall rules dynamically
Deep Q-Networks (DQN)	Dynamic intrusion detection system configurations

Summary:

- **Supervised Learning Models**:
    - Logistic Regression, Decision Trees, Random Forests, Gradient Boosting Machines, Support Vector Machines (SVMs), K-Nearest Neighbors (KNN), Linear Regression, Neural Networks (including Convolutional and Recurrent Neural Networks), Transformers, Named Entity Recognition (NER), Sentiment Analysis, Text Classification.
- **Unsupervised Learning Models**:
    - Isolation Forest, One-Class SVM, Autoencoders, K-Means Clustering, DBSCAN, Principal Component Analysis, Q-Learning, Deep Q-Networks (DQN).