ANOMALY DETECTION IN DNS TRAFFIC FOR CYBERSECURITY

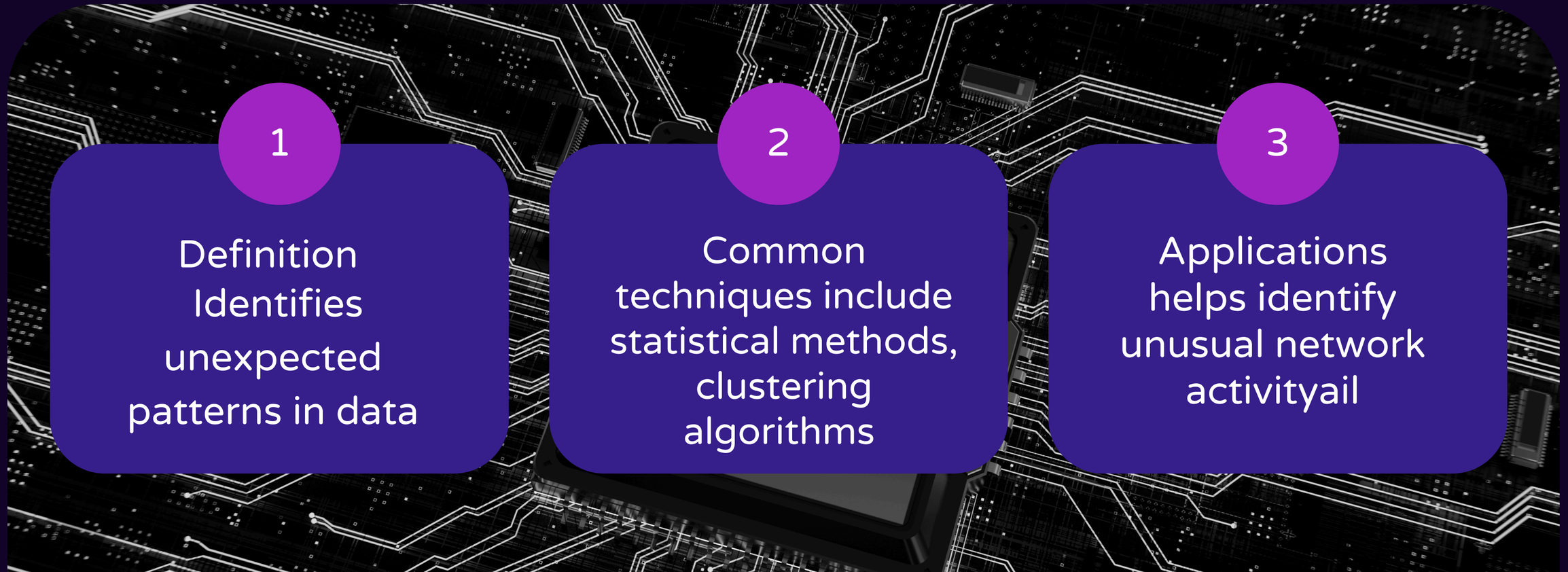
Machine Learning in Detection

HANNAH EMAD 2205123
MARIAM MOSTAFA 2205084
NADA MOHAMED 2205173

What is Anomaly Detection?

The process of identifying patterns or instances in data that deviate significantly from the expected or normal behavior. What is considered "normal" or anomalous can vary based on the context.

Anomaly Detection Basics



1

Definition Identifies unexpected patterns in data

2

Common techniques include statistical methods, clustering algorithms

3

Applications helps identify unusual network activityail

Types of Anomaly Detect in DNS

1. Machine Learning-based Methods
2. Clustering-based Methods
3. Statistical Methods

Identifying unusual patterns or behaviors that deviate from normal traffic

DNS Traffic Data & Feature

- Understanding DNS Traffic Data
- Analyzing DNS Flow Patterns
- Key Features in DNS Traffic for Anomaly Detection
- Feature Selection for DNS Traffic Analysis

Cybersecurity Threats & Challenges

1. High Volume of Traffic
2. Complexity of Attack Patterns
3. Dynamic and Evolving Threats
4. False Positives & Negative Detection

Protect Anomaly Detection

1

Encrypt
sensitive data

2

Model
Obfuscation and
Access Control

3

Regular Updates
and Monitoring

Cache Poisoning Detection

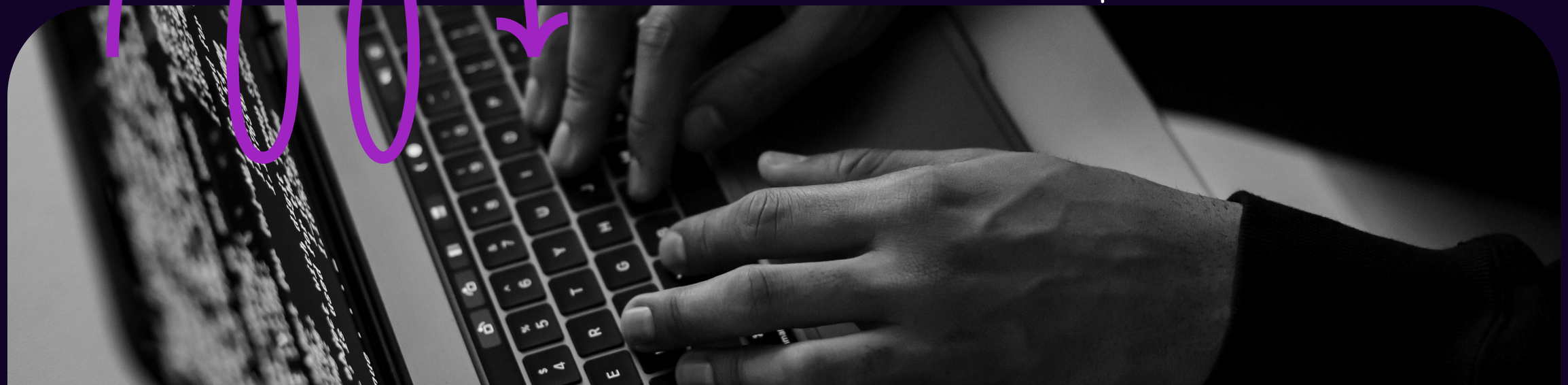
Understanding Cache Poisoning in DNS Systems

Techniques for Detecting Cache Poisoning Attacks

Mitigation Strategies for Cache Poisoning Prevention

Conclusion and Future Work

Early anomaly detection helps prevent DNS cache poisoning by identifying threats early and improving network security. Continuously updating models with new data is essential to adapt to evolving threats. Expanding detection capabilities and integrating them into broader security frameworks strengthens overall protection.



THANK YOU!