THE ROLE OF AI IN CYBERSECURITY

**ENG. FATIMA ALABDULKAREEM**

K-CYBER SECURITY COMMITTEE REPRESENTATIVE

AGENDA

- INTRODUCTION

- HOW AI IS UTILIZED IN CYBERSECURITY

- RISKS/THREATS OF AI

- GENERATIVE AI USES

- CONCLUSION

Private Insensitive Data

Kuwait Petroleum Corporation and subsidiaries | مؤسسة البترول الكويتية وشركاتها

AI INTRODUCTION

AI is when you make a computer like a little brain. You help it to learn by giving it a lot of words and pictures and numbers. If the computer hears you answer a lot of questions, later on it can quickly answer your questions. But it only knows what you show it and tell it, so it's not as smart as you are.
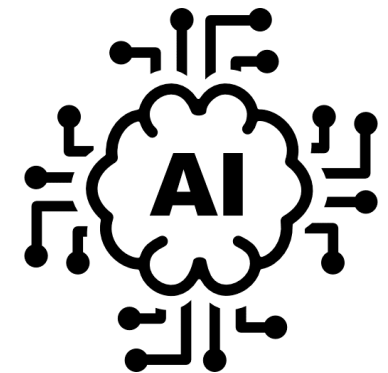
*Reference: *integrate.ai,* Roshanak Houmanfar

PREDICTIVE VS. GENERATIVE AI
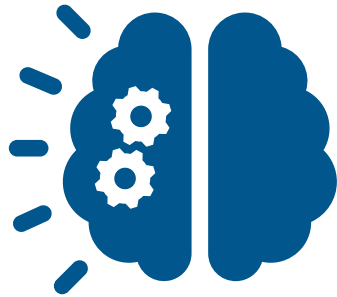
Predictive

Analyzes data to recognize behavior, make predictions, and classify information.

Generative

Consumes large quantities of data to generate new content.

PREDICTIVE AI USES IN CYBERSECURITY

01 Threat Intelligence
Scoring Indicators, Creating correlations, Identifying priority threats …etc.

02 Threat Hunting
Suggest specific hunts based on: Threat Intelligence, Network Behavior, Existing Vulnerabilities, Triggered Incidents and Offenses, Conduct Automated Hunts
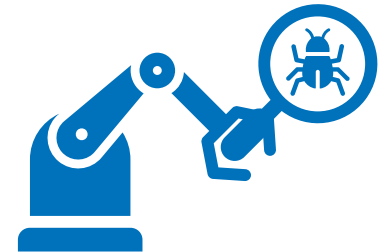
03 Cyber Risk Management
Quantify risks based on existing data

04 Firewalls
Detect and block suspicious/ harmful traffic

PREDICTIVE AI USES IN CYBERSECURITY

05 Vulnerability Management
Prioritize vulnerabilities to be patched based on likelihood & Severity
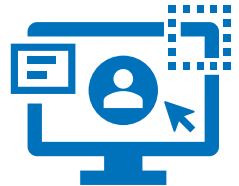
06 Email Security
Detect and block phishing emails, Detect abnormal user emailing behavior

07 SOC Operations
SIEM Incident Detections, SOAR Automated Responses

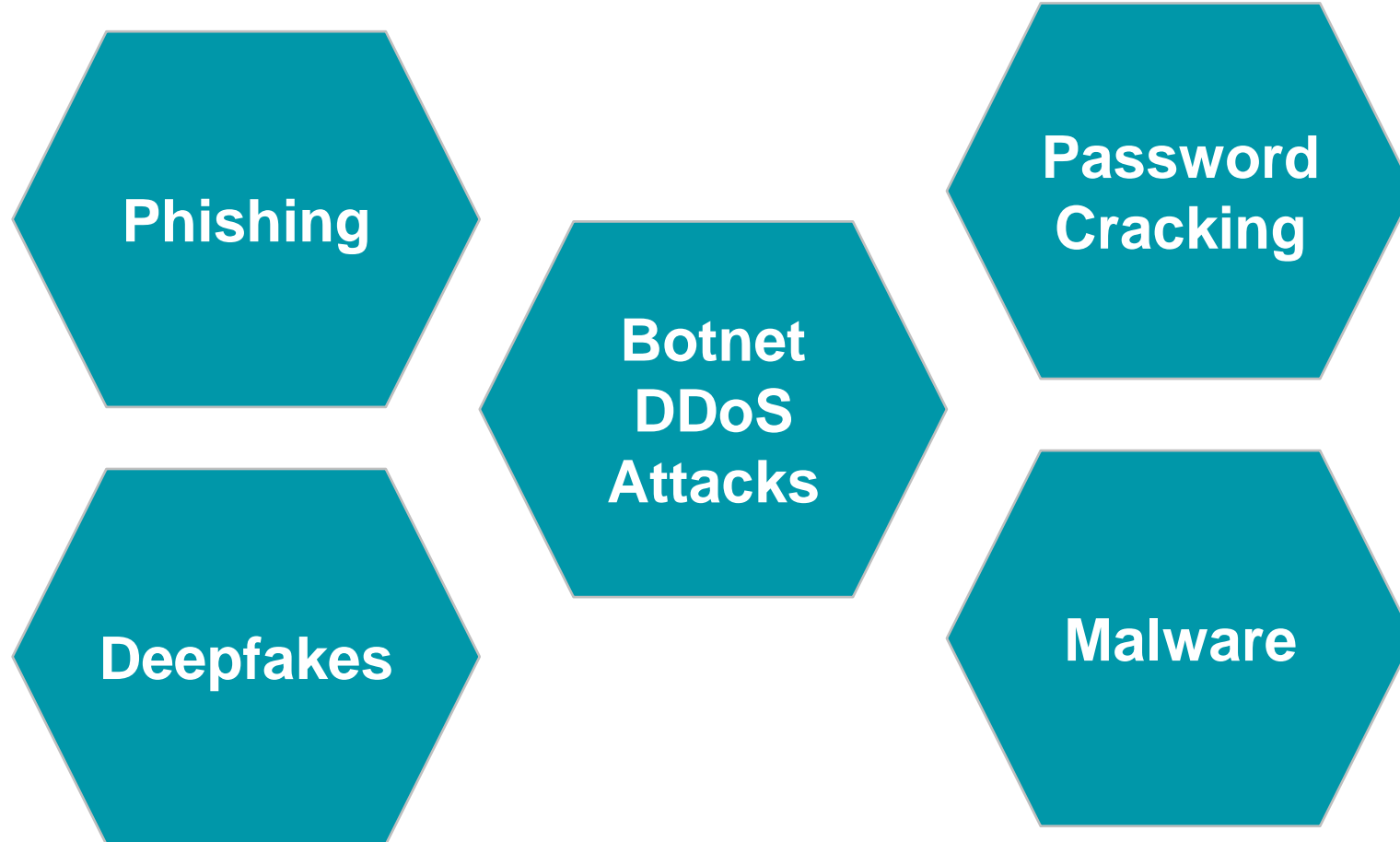## 08 Network/ Endpoint Detection & Response
Network Analysis, Abnormal Behavior Detection, Dynamic Learning, Building correlations

RISKS & THREATS OF AI

How attackers can leverage generative AI to enhance their attacks.

Phishing

Deepfakes

Botnet DDoS Attacks

Password Cracking

Malware

Private Insensitive Data

GENERATIVE AI USES

TRAINING & AWARENESS

Generate explanations for complex security topics.
Generate Phishing Emails for training.
Generate graphical content that showcase specific security topics.
Generate scenarios of cyber attacks against current infrastructure.

SOC

Generate new rules/ playbooks for detection & response.
Generate use cases

THREAT INTELLIGENCE / HUNTING

Generate analysis of specific malware or threat hunting codes.

Threat Intelligence Reporting
Insights & Trends
Specific for different parties.
Hunt and write specific YARA rules.

FINAL TIPS & TAKEAWAYS

- AI presents a lot of possibilities and uncertainties.

- Stay diligent and up-to-date with AI progress.

- Be careful with generative AI projects.

- Leverage Predictive AI in all possible security functions.

- Developing AI regulations globally and locally.

- Understand AI weaknesses.

- Use AI responsibly.

Kuwait Petroleum Corporation and subsidiaries | مؤسسة البترول الكويتية وشركاتها

THANK YOU

ENG. FATIMA ALABDULKAREEM

Senior Information Security & Network Administrator (PIC)

K-Cyber Security Committee Representative