HACKPROVE

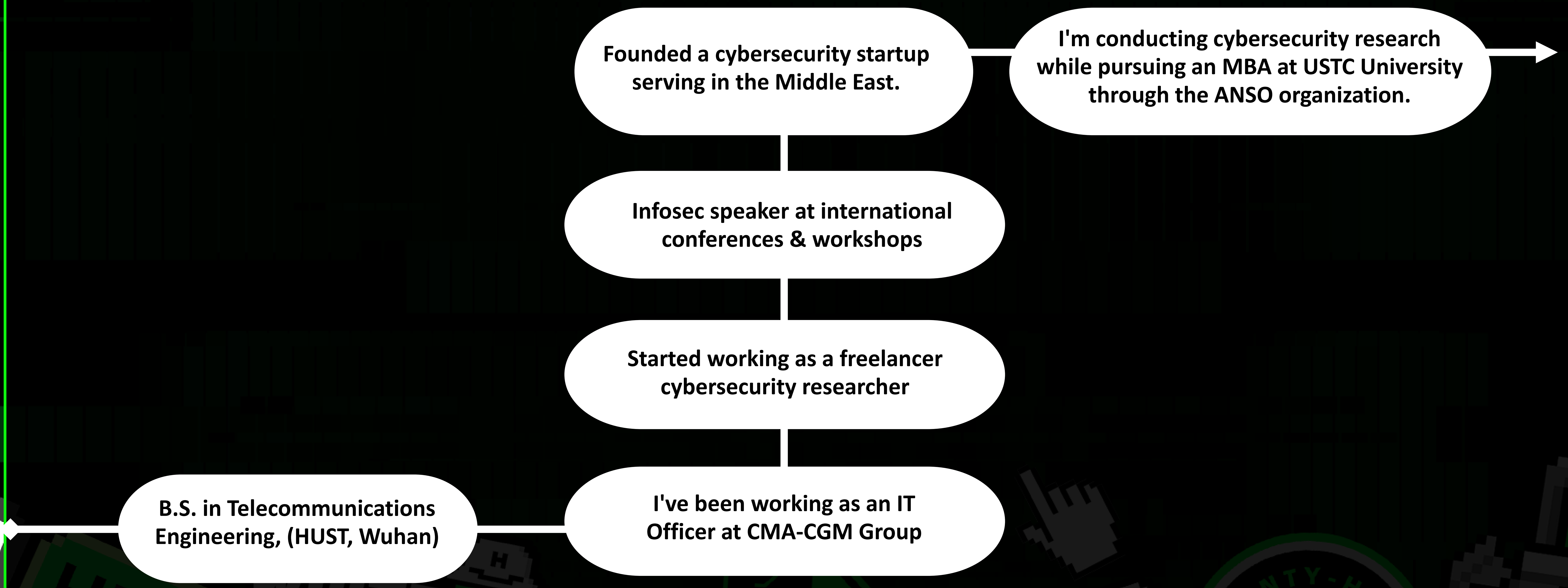
2025 HACKPROVE WORLD

# LEVERAGING AI & MACHINE LEARNING TO STAY AHEAD OF EMERGING CYBER THREATS

2025/01/10

Ismail Ahmed

# WHO AM I



B.S. in Telecommunications Engineering, (HUST, Wuhan)

I've been working as an IT Officer at CMA-CGM Group

Started working as a freelancer cybersecurity researcher

Infosec speaker at international conferences & workshops

Founded a cybersecurity startup serving in the Middle East.

I'm conducting cybersecurity research while pursuing an MBA at USTC University through the ANSO organization.

# CONTENTS

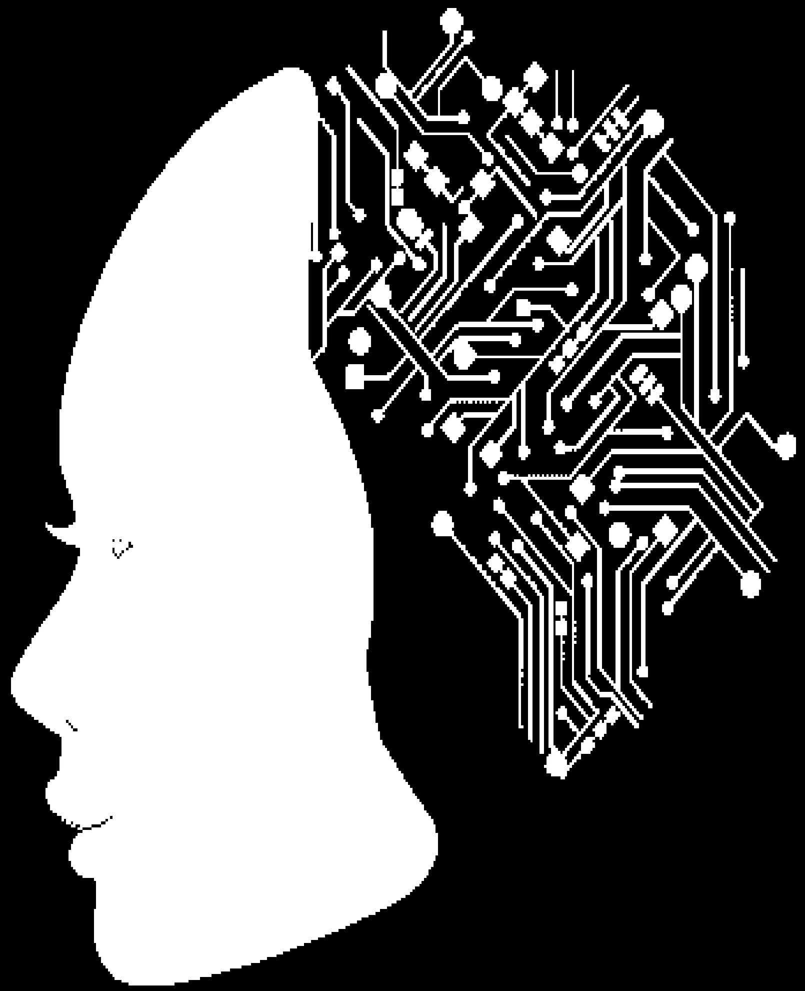
01 Introduction to AI & ML in Cybersecurity

02 Core Applications & challenge's

03 The Cyber Threat Landscape

04 Practical Demo & Conclusion

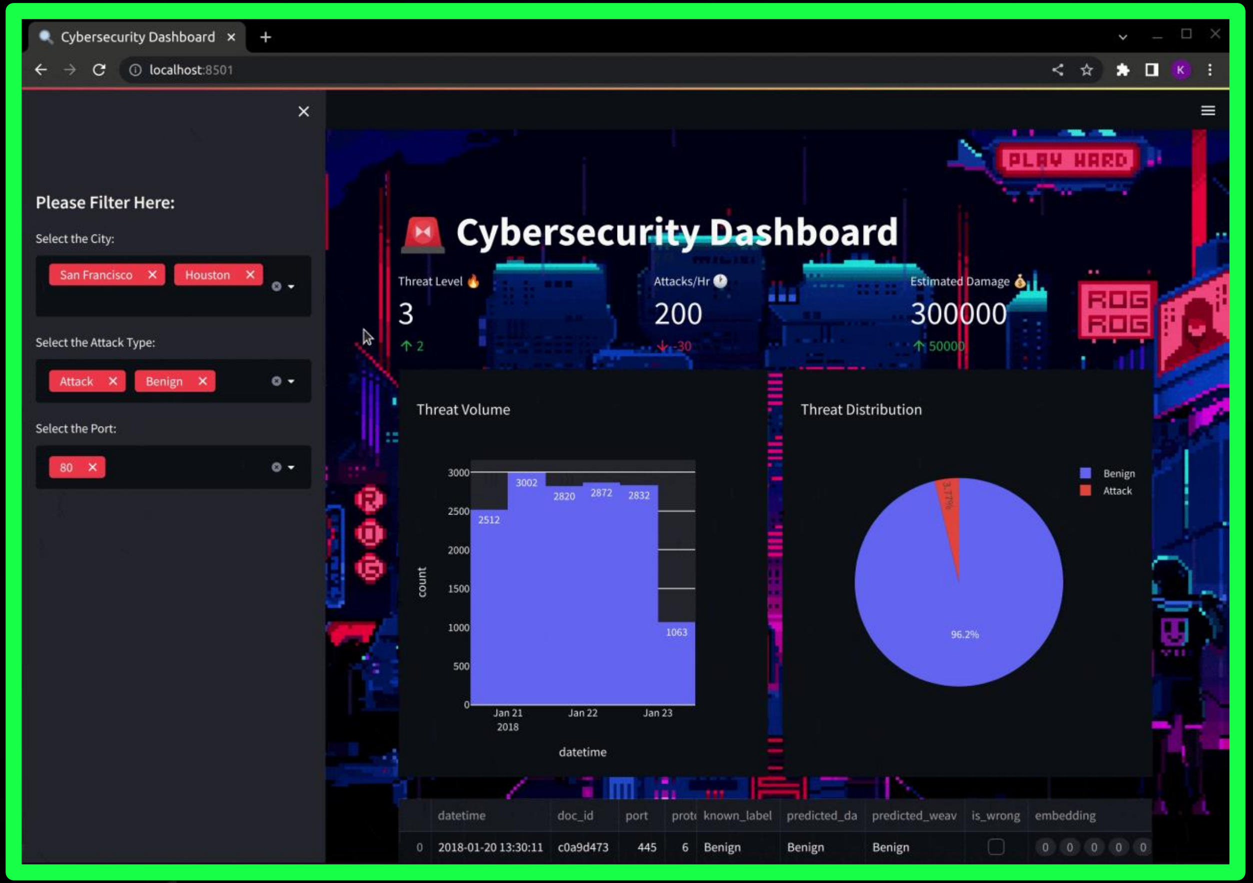
# INTRODUCTION



The integration of AI in cyber security represents a dynamic shift in how organizations defend against evolving threats. This combination of big data and AI/ML has enhanced cybersecurity defenses by empowering organizations to analyze and respond to security incidents more effectively, mitigate risks, and adapt to evolving cyber threats.

# THE GROWING OF CYBER THREATS

Cyber threats are becoming increasingly sophisticated, with cybercriminals using advanced techniques to breach security systems and steal data. These threats include phishing, ransomware, advanced persistent threats (APTs), and zero-day exploits. The rise of artificial intelligence and machine learning has further enhanced these attacks, making them harder to detect. Organizations must stay vigilant and adapt to protect against these evolving threats.



Please Filter Here:

Select the City: San Francisco, Houston

Select the Attack Type: Attack, Benign

Select the Port: 80

Cybersecurity Dashboard

Threat Level 🔥 3 ↑ 2

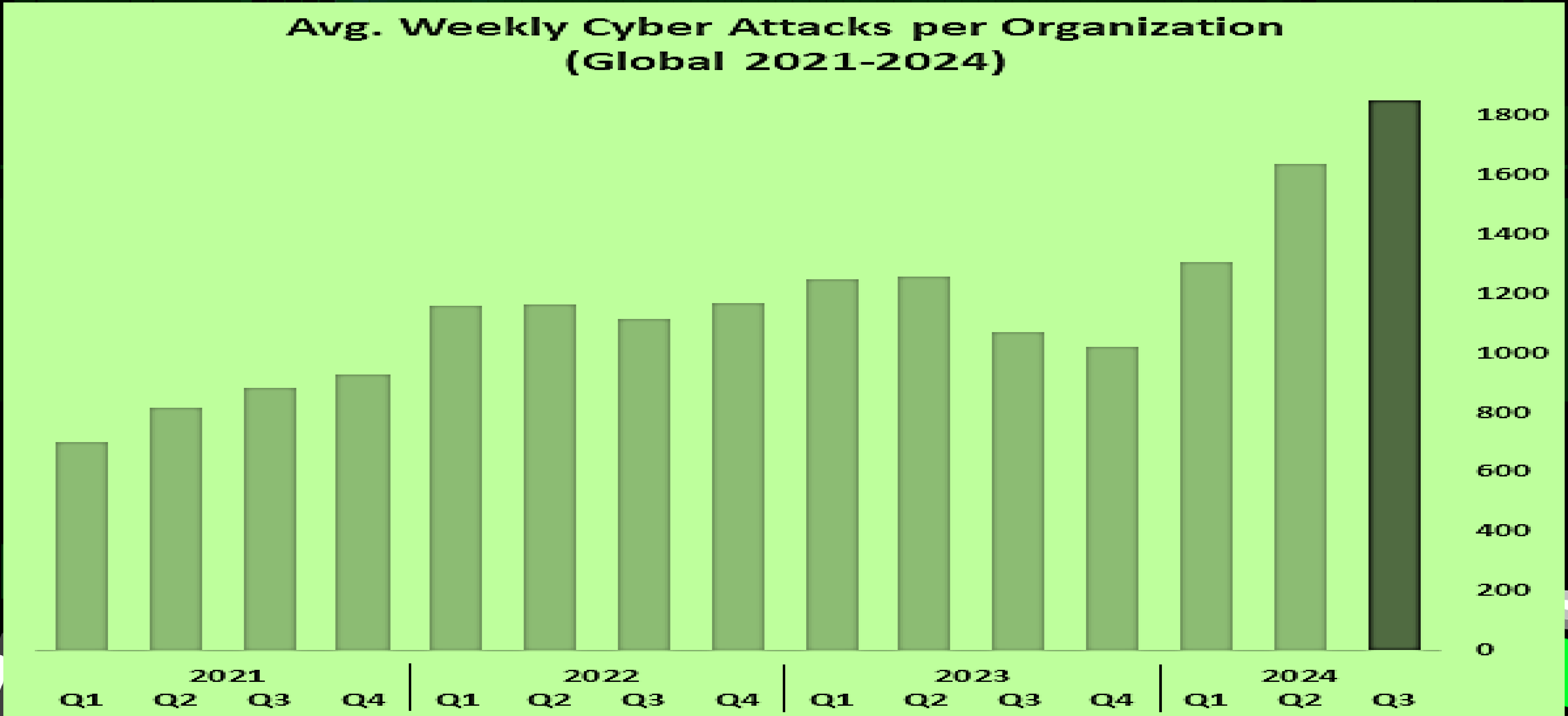
Attacks/Hr 200 ↓ -30

Estimated Damage 💰 300000 ↑ 50000

|  | datetime | doc_id | port | prot | known_label | predicted_da | predicted_weav | is_wrong | embedding |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 2018-01-20 13:30:11 | c0a9d473 | 445 | 6 | Benign | Benign | Benign | □ | 0 0 0 0 0 |

HACKPROVE

2025 HACKPROVE WORLD

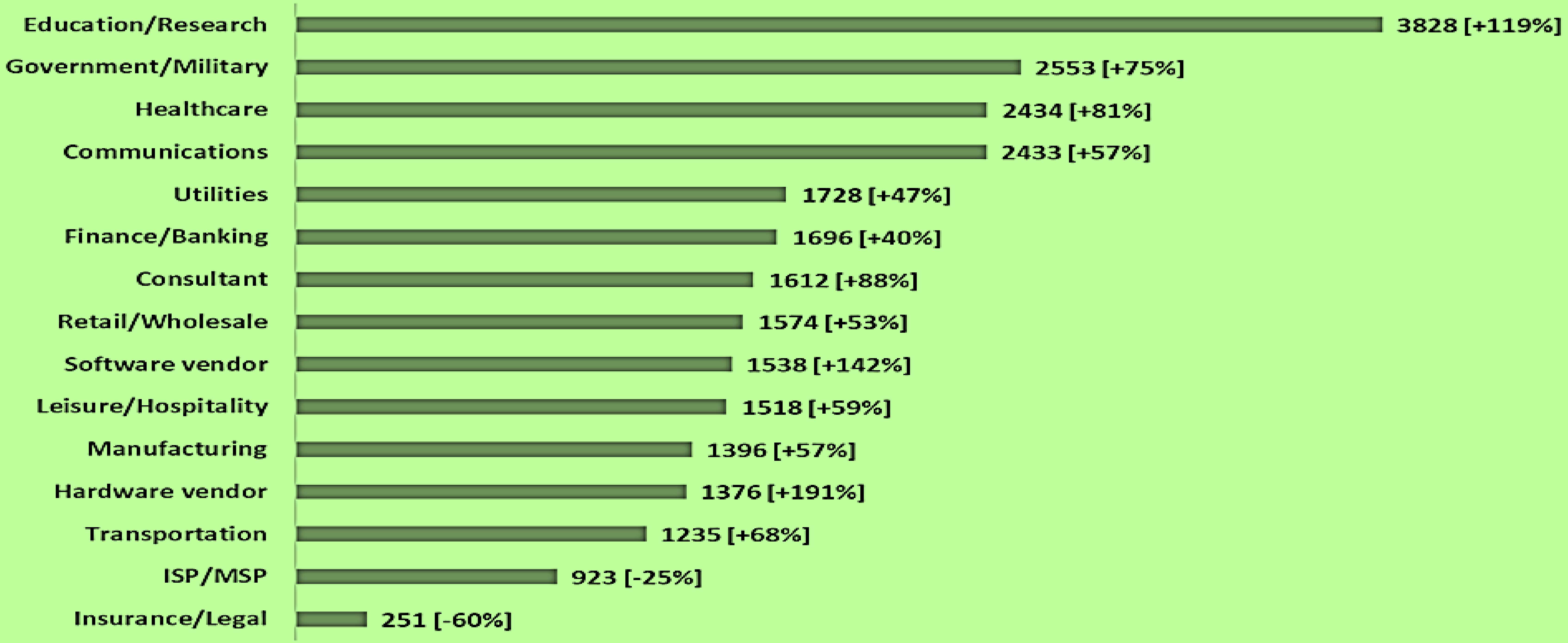

Avg. Weekly Cyber Attacks per Organization (Global 2021-2024)

Source: https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/

HACKPROVE

2025 HACKPROVE WORLD

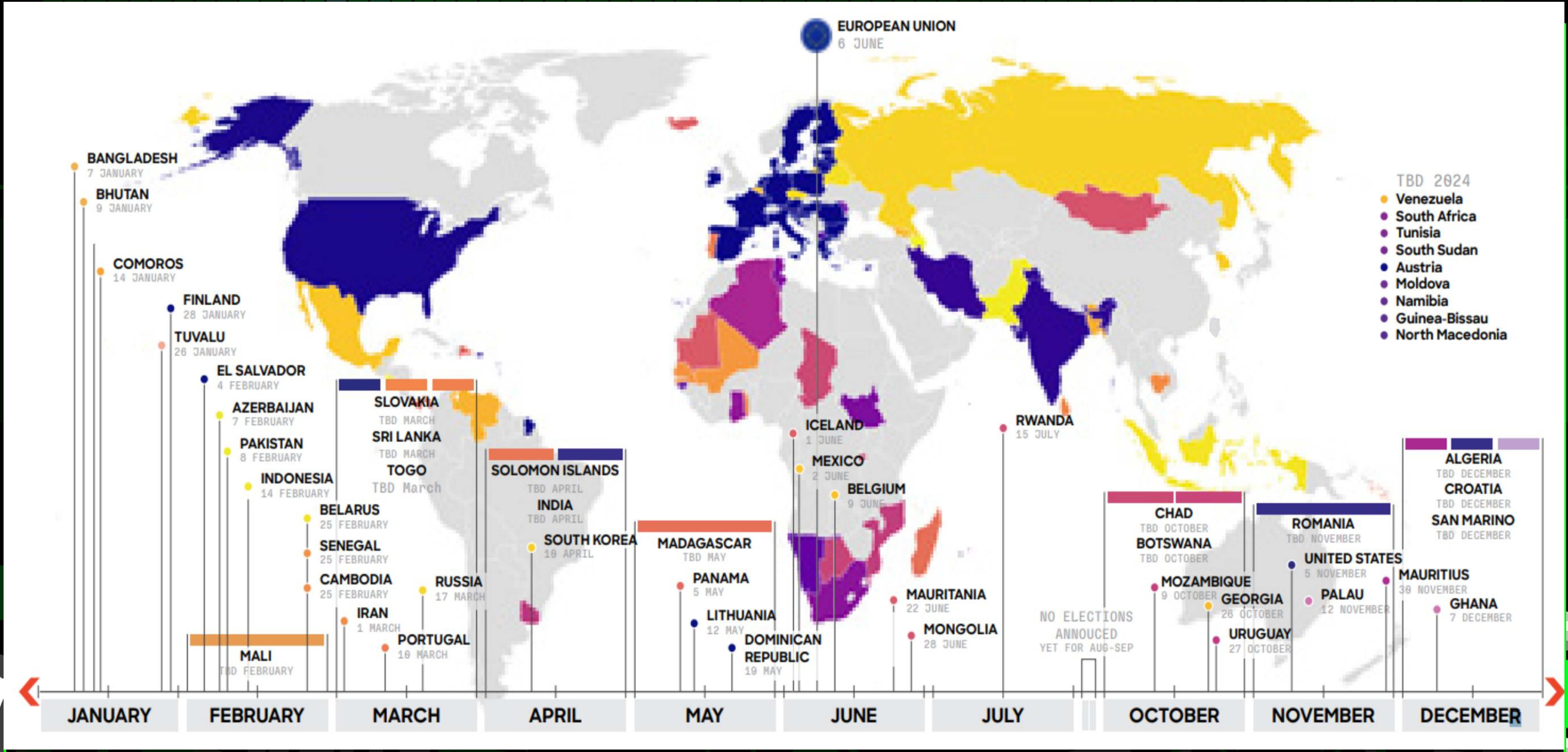
## Global Avg. Weekly Cyber Attacks per Industry
(Q3 2024 Compared to Q3 2023)



Source: https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/

HACKPROVE

2025 HACKPROVE WORLD



Source: CROWDSTRIKE Countries holding presidential, parliamentary or general elections in 2024 -

# CHALLENGES IN TRADITIONAL CYBERSECURITY APPROACHES

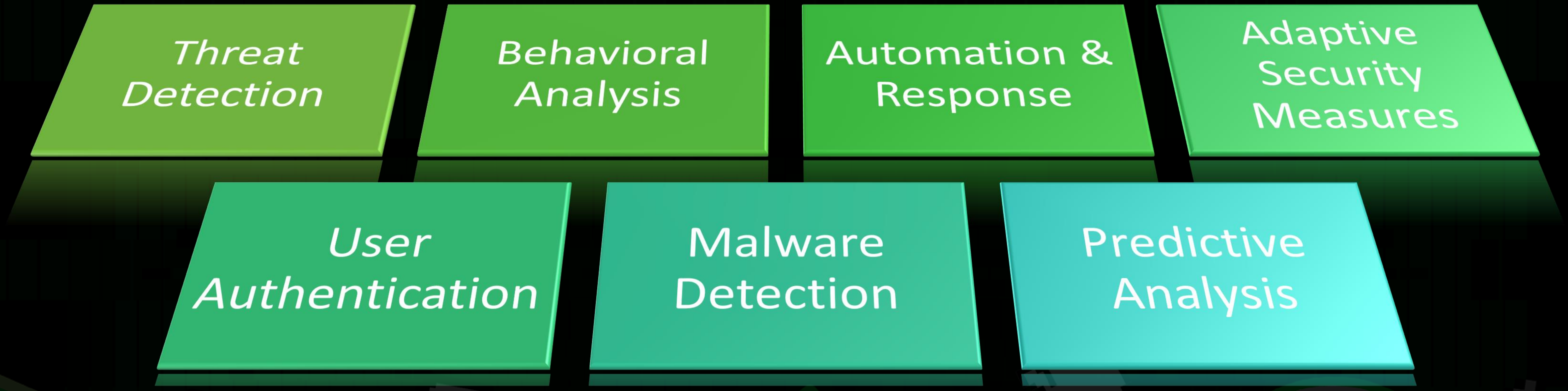
Traditional cybersecurity approaches face several significant challenges in today’s evolving threat landscape :

- Budget Constraints
- Skill shortages
- Emergence of APT’S
- Lack of Visibility
- The Explosion of Data
- Rise of Ransomware

# WHY AI AND ML ARE CRITICAL IN THIS DOMAIN

# WHY AI AND ML ARE CRITICAL IN THIS DOMAIN

AI and ML are critical for achieving unprecedented levels of efficiency and accuracy in this domain



*Threat Detection*

Behavioral Analysis

Automation & Response

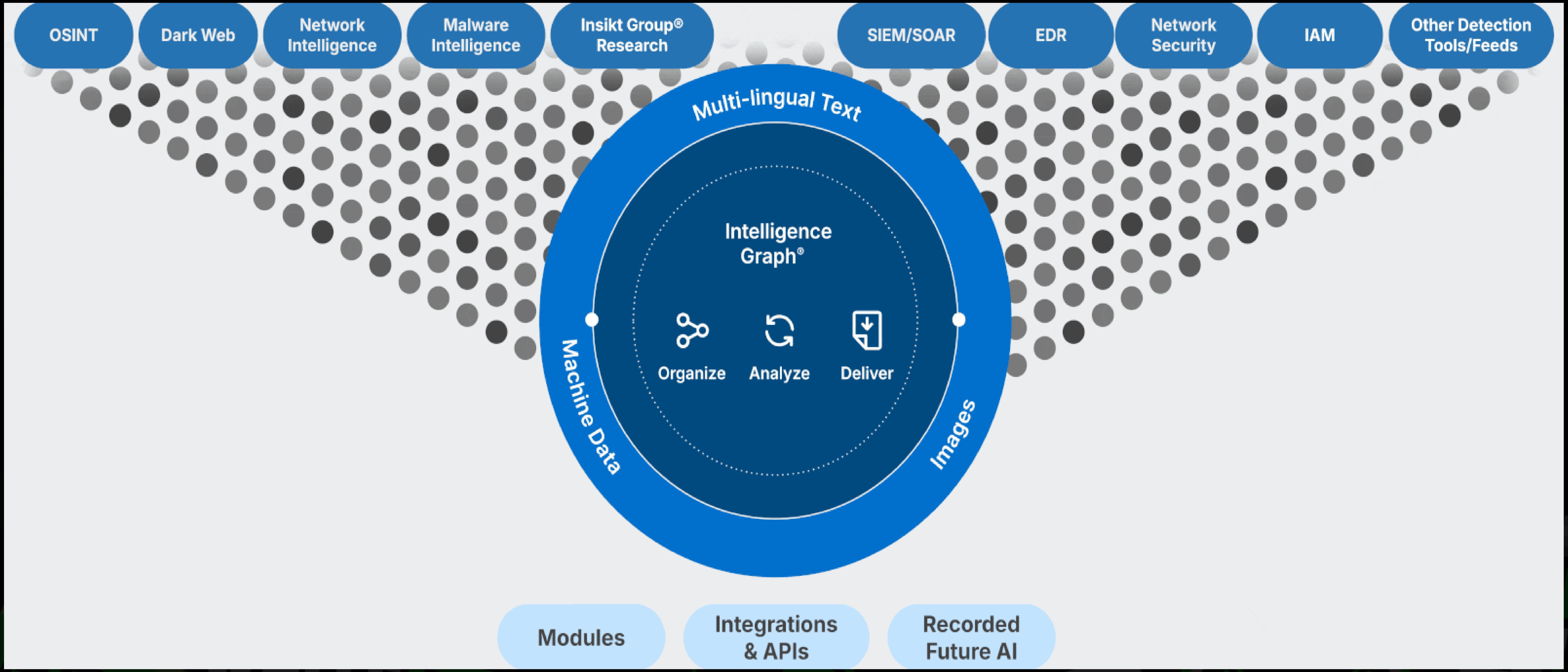
Adaptive Security Measures

*User Authentication*

Malware Detection

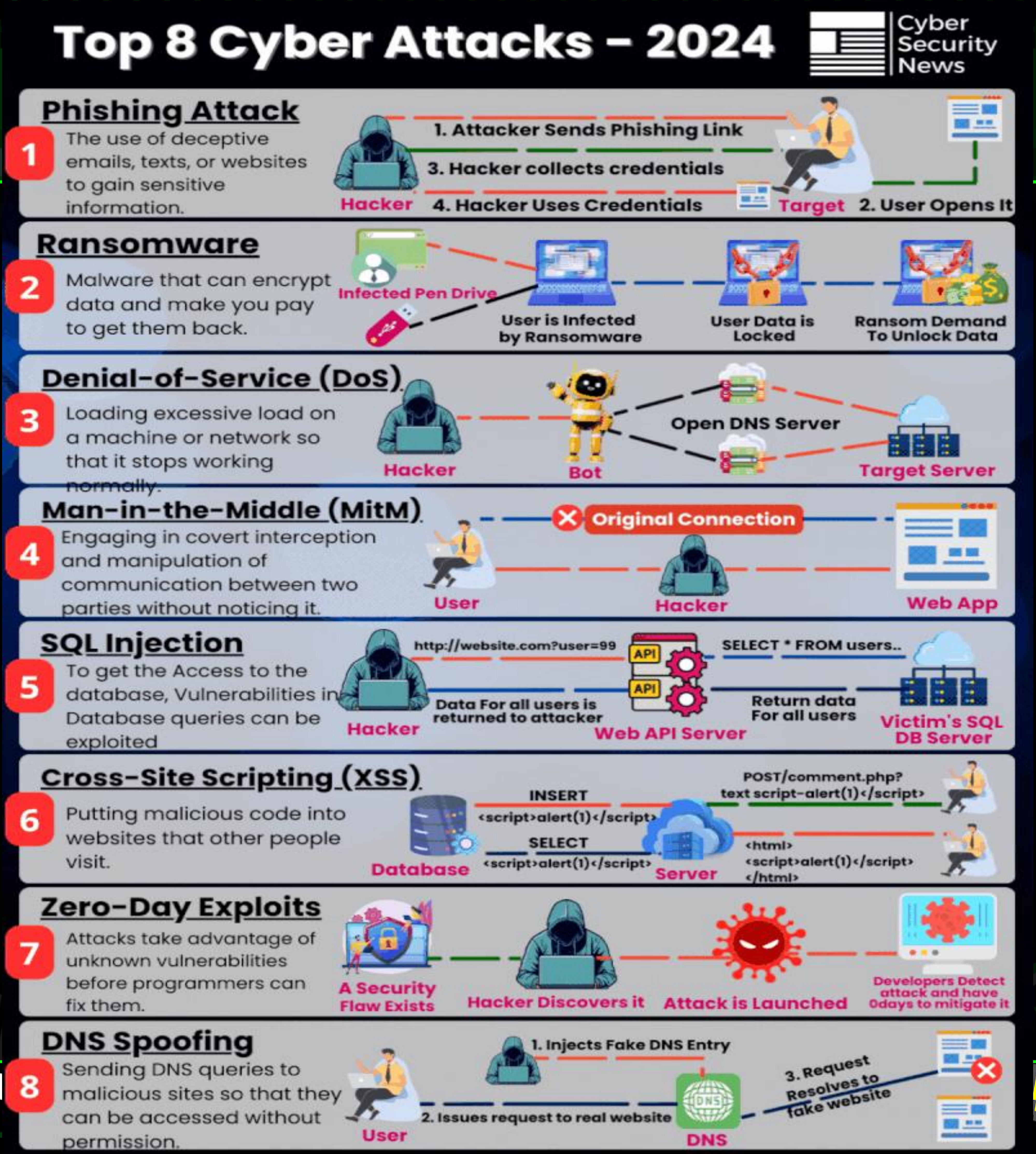
Predictive Analysis

However, with the power of AI and ML, you'll be able to track the world's threats effectively !



HACKPROVE

2025 HACKPROVE WORLD



# Top 8 Cyber Attacks - 2024

Cyber Security News

## 1 Phishing Attack

The use of deceptive emails, texts, or websites to gain sensitive information.

Hacker
1. Attacker Sends Phishing Link
3. Hacker collects credentials
4. Hacker Uses Credentials
Target
2. User Opens It

## 2 Ransomware

Malware that can encrypt data and make you pay to get them back.

Infected Pen Drive
User is Infected by Ransomware
User Data is Locked
Ransom Demand To Unlock Data

## 3 Denial-of-Service (DoS)

Loading excessive load on a machine or network so that it stops working normally.

Hacker
Bot
Open DNS Server
Target Server

## 4 Man-in-the-Middle (MitM)

Engaging in covert interception and manipulation of communication between two parties without noticing it.

## 5 SQL Injection

To get the Access to the database, Vulnerabilities in Database queries can be exploited

http://website.com?user=99
API
API
SELECT * FROM users..
Hacker
Data For all users is returned to attacker
Web API Server
Return data For all users
Victim's SQL DB Server

## 6 Cross-Site Scripting (XSS)

Putting malicious code into websites that other people visit.

INSERT
<script>alert(1)</script>
SELECT
<script>alert(1)</script>
Database
Server
POST/comment.php?
text script-alert(1)</script>
<html>
<script>alert(1)</script>
</html>

## 7 Zero-Day Exploits

Attacks take advantage of unknown vulnerabilities before programmers can fix them.

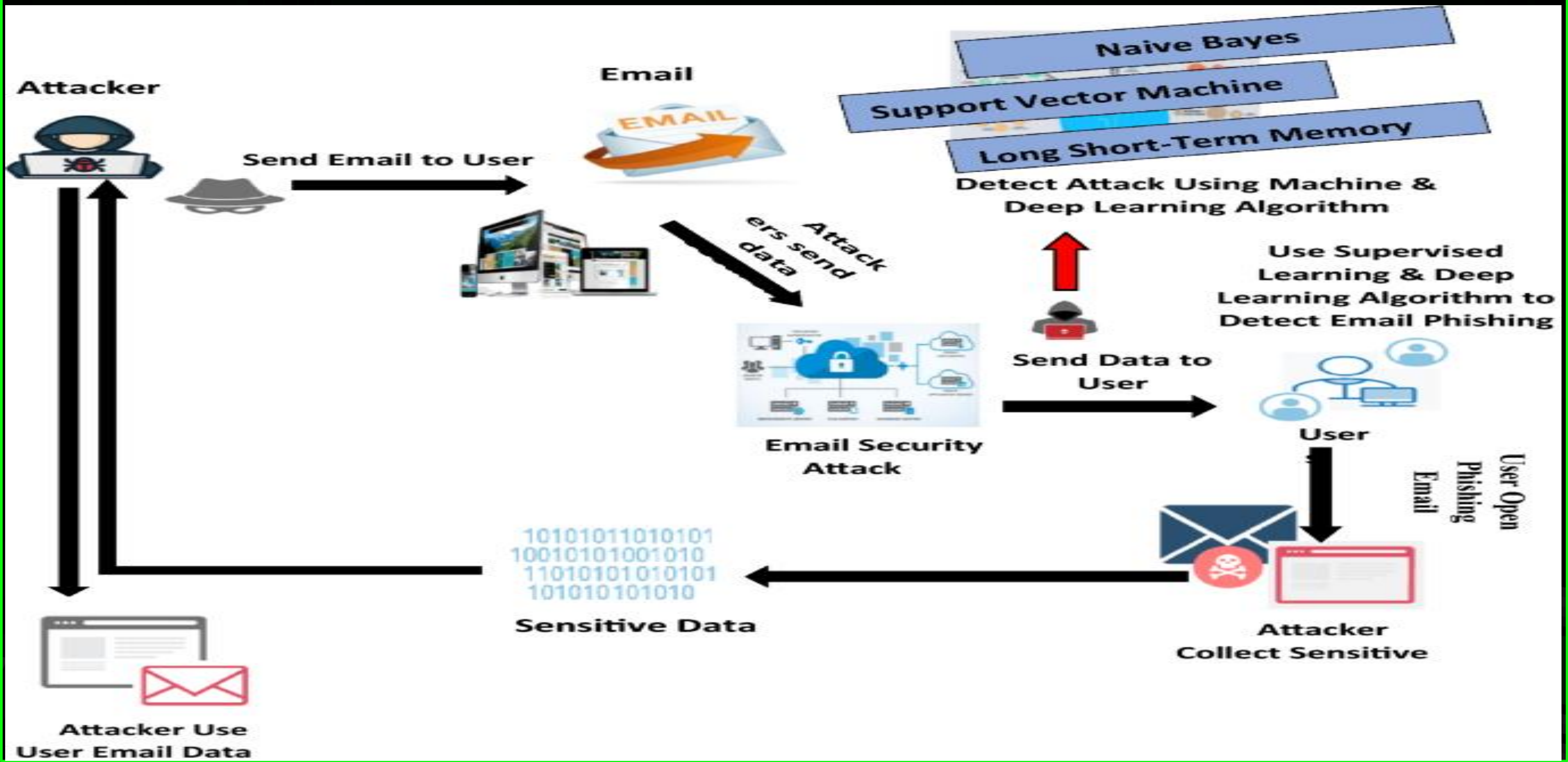
## 8 DNS Spoofing

Sending DNS queries to malicious sites so that they can be accessed without permission.

1. Injects Fake DNS Entry
User
2. Issues request to real website
DNS
3. Request Resolves to fake website

Source: Cyber Security News

# Detecting Phishing Attacks With AI



# AI-POWERED CYBERSECURITY TOOLS

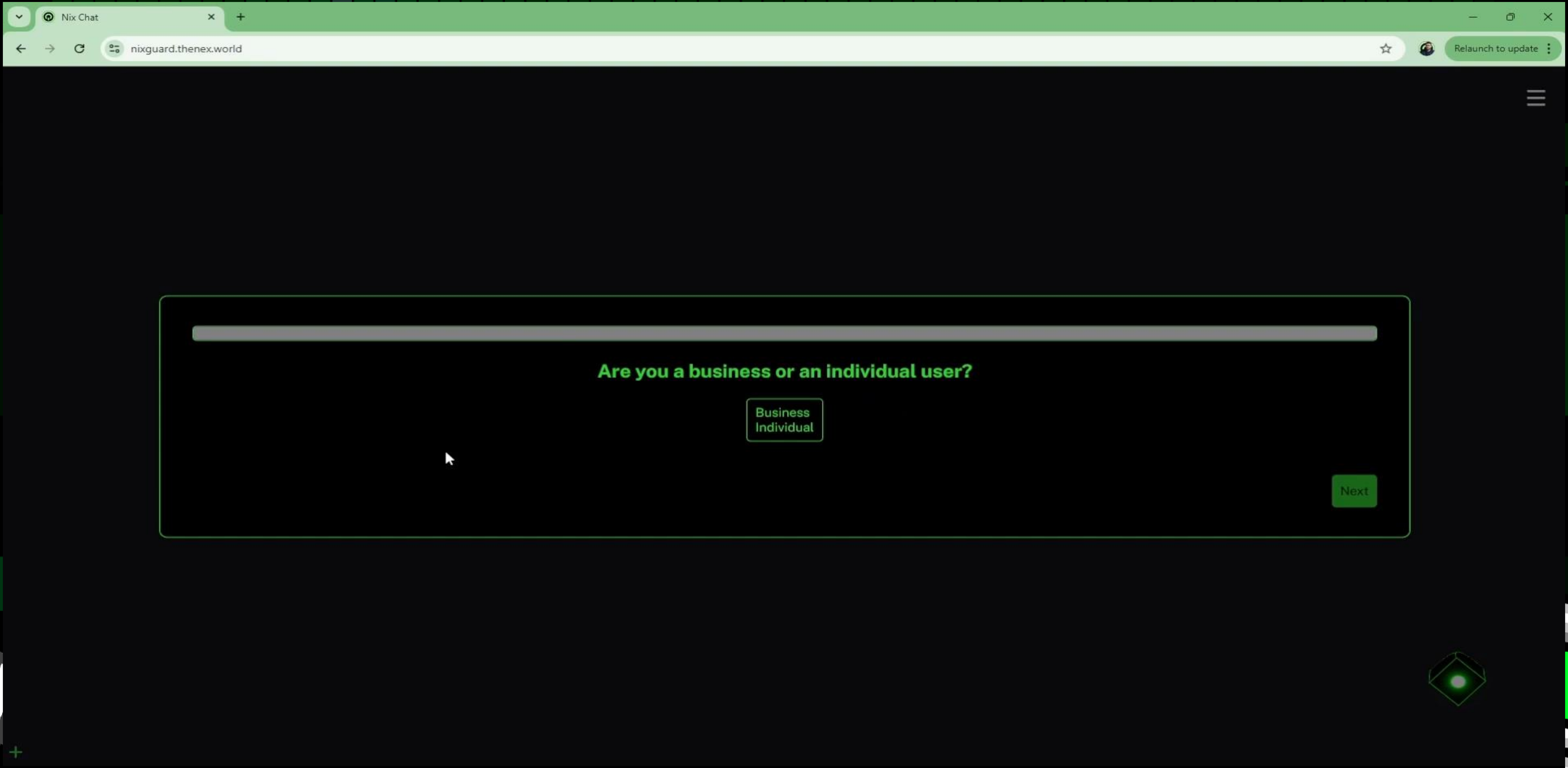
CROWDSTRIKE

deep instinct™

SentinelOne®

DARKTRACE

CYLANCE PROTECT



Are you a business or an individual user?

# CONCLUSION

Organizations must prioritize investing in cutting-edge threat detection systems. These systems should leverage the power of artificial intelligence to identify anomalies and analyze user behavior patterns.

Concurrently, continuous employee training programs are essential. This is because AI-powered attacks frequently exploit human vulnerabilities, such as susceptibility to phishing scams.

Finally, implementing adaptive security measures is crucial. These measures must be dynamic and capable of evolving alongside the constantly changing threat landscape.

HACKPROVE

2025 HACKPROVE WORLD

# Q & A

HACKPROVE

2025 HACKPROVE WORLD

# Thanks for your attention ^_^

🌐 Yalla-Hack.net

✉ cn.ismail@yalla-hack.net

☎ +8618326095404

in https://www.linkedin.com/in/engismail2020/