ProCheckUp

Defending Against AI-Driven Cyber Attacks and Advanced Social Engineering

Richard Brain
ProCheckUp Ltd
12th June 2024

Agenda

01. Introduction

Overview of key findings and trends in AI-driven cyber attacks and social engineering.

02. Understanding AI-Driven Threats

Examination of how AI is transforming cyber threats. Discussion on the sophistication and scale of AI-driven attacks.

03. Defending Against AI-Driven Attacks

Layered Defences, AI Enhanced Monitoring, Incident Response Planning and Recovery, Collaboration and Sharing.

04. Advanced Social Engineering Attacks

The evolution of social engineering tactics enhanced by AI.

Deepfake Technology

Spear Phishing

05. Defending Against Advanced Social Engineering

Training and Awareness Programs

Simulation Exercises

Principle of Least Privilege

Incident Response Team

Introduction

AI's Dual Role in Cybersecurity:

Enhancing Security:

AI-driven tools for threat detection and response.
Behavioural analytics to predict and prevent cyber attacks.

Posing Threats:

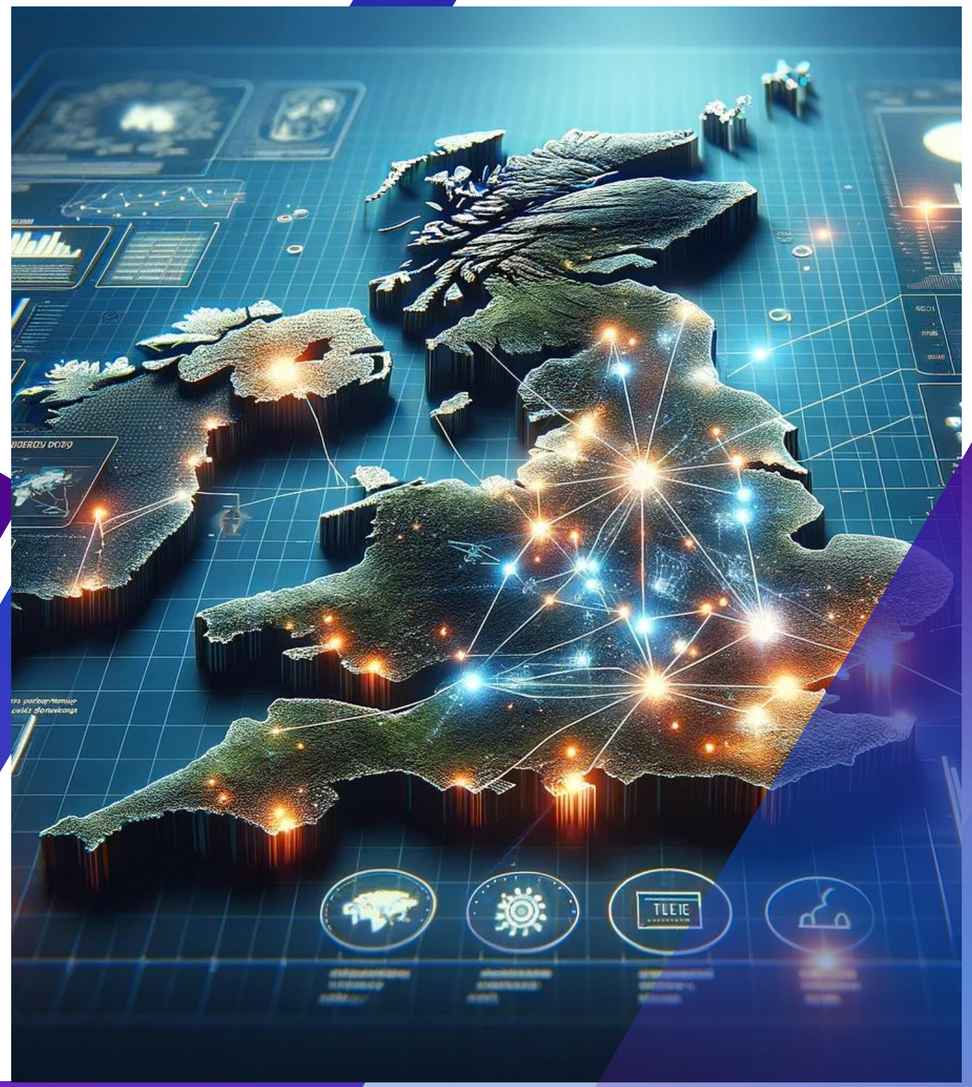
Development of adaptive malware and sophisticated phishing schemes.
Exploitation of AI for social engineering and deepfake technology.

Understanding AI-Driven Threats

AI-driven threats involve the use of artificial intelligence and machine learning by cybercriminals to enhance the effectiveness and efficiency of cyber attacks.

Examples:

- AI-Powered Phishing: Sophisticated phishing emails crafted by AI to mimic trusted sources and deceive recipients.
- Adaptive Malware: Malware that uses AI to adapt its behaviour to evade detection and persist within systems.
- Deepfake Technology: Creation of realistic audio and video impersonations for fraudulent activities.



Adaptive Malware

Description:

This new type of malware under development uses AI to analyse the environment it infects and adapts its behaviour accordingly. It can alter its code and methods to evade detection, making it much more resilient and harder to counter.

Impact:

Adaptive malware can persist inside networks for extended periods, causing ongoing damage and complicating eradication efforts.

Automated Vulnerability Discovery /Zero Day

Description:

Attack software under development driven by AI algorithms can scan and analyse corporate environments to identify vulnerabilities at a much faster rate than human operators. These systems can exploit weaknesses almost instantaneously, leaving defenders with very little time to react.

Impact:

The rapid exploitation of vulnerabilities sometimes creating unique zero days can lead to widespread system breaches before security patches can be applied.

Defending Against AI

Implementation of a Layered Security Architecture

A layered or defence-in-depth strategy ensures that multiple security measures are in place, so if one layer fails, others will still provide protection.

Perimeter Security

Using firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to guard against unauthorised access.

Network Segmentation

Dividing the network into secure zones to control traffic flow and limit the spread of potential intrusions. Consider micro-segmenting networks.

Endpoint Protection

Ensuring that all endpoint devices are secured against threats with antivirus software, anti-malware, and regular patching.

Defending Against AI

A.I Enhanced Monitoring and Response

Implementing AI-powered monitoring tools that continuously analyse behaviours across networks can detect anomalies that signify a breach or an ongoing attack, enabling quicker response times.

Autonomous Response:

Implement systems capable of automatically countering real-time threats, such as isolating affected networks or devices immediately upon detection of suspicious activity.

Dynamic Risk Assessment:

AI can continuously assess the risk levels of different network segments and dynamically adjust security measures.

Integration and Automation:

Use Security Orchestration and Automated Response (SOAR) platforms to integrate various security tools and automate coordinated responses to detected threats

Defending Against AI

Comprehensive Risk Assessments

Understanding the threat landscape and updating risk management strategies to address new and evolving threats is crucial to create risk assessments.

Threat Modelling:

Developing scenarios based on potential attacks to determine the impact and prepare mitigation strategies accordingly.

Asset Identification:

Mapping out all assets, including physical devices and software systems, to understand what needs protection.

Vulnerability Scanning:

Regularly scanning systems and networks to detect vulnerabilities that could be exploited by attackers.

Defending Against AI

Incident Response Planning and Recovery

A robust incident response plan enables organisations to quickly address security breaches and minimise damage.

01

Incident Response Team:

A dedicated team trained to handle cyber-security incidents efficiently.

02

Communication Plans:

Clear procedures for communicating internally and externally during a security incident, including notifying regulatory bodies when necessary.

03

Disaster Recovery:

Strategies and backups in place to restore systems and data in case of a major cyber event.

Defending Against AI

Threat Intelligence Sharing

Engaging in or forming alliances for sharing real-time threat intelligence within the industry and cyber-security bodies can provide early warnings of emerging threats. Developing and maintaining a robust threat intelligence capability is crucial. This involves not only monitoring known threats but also predicting new ones through the analysis of trends and emerging tactics in the cyber-criminal world.

Industry Partnerships: Participating in sector-specific cyber-security initiatives and sharing threat intelligence with peers.

Regulatory Compliance: Staying updated with changes in cyber-security regulations and standards to ensure compliance and enhance security measures.

Advanced Social Engineering

Advanced Social Engineering Attacks

Social engineering involves manipulating individuals to divulge confidential information or perform actions that compromise security. AI enhances these tactics by making attacks more sophisticated and convincing.

Deepfake Technology:

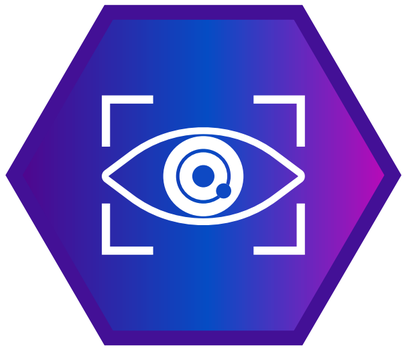
AI creates realistic audio and video impersonations of trusted individuals. Used to issue fraudulent instructions, manipulate stock prices, or gain unauthorized access.

Spear Phishing:

AI crafts highly personalised and context-aware phishing emails targeting specific individuals. Increases the success rate of phishing attacks by making them more believable.

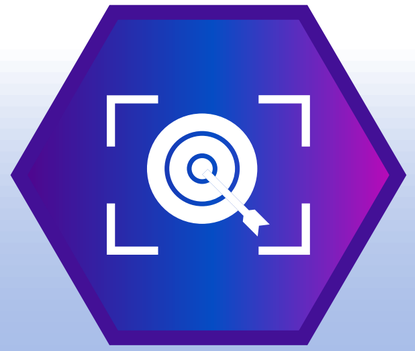
Defending Against Advanced Social Engineering

Comprehensive Training and Awareness Programs



Action:

Regular and comprehensive training sessions should be conducted to educate employees about the latest social engineering tactics. Training should emphasize critical thinking and scepticism, especially regarding requests for sensitive information or urgent actions, including the latest techniques like deepfake recognitions and pretexting.

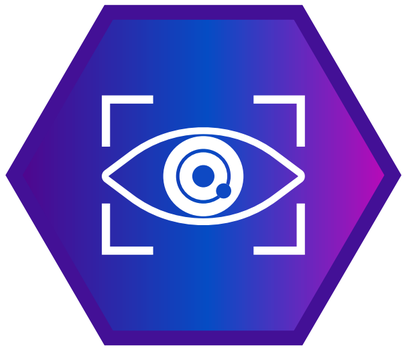


Benefit:

Educated employees are the first line of defence against social engineering, reducing the risk of successful attacks.

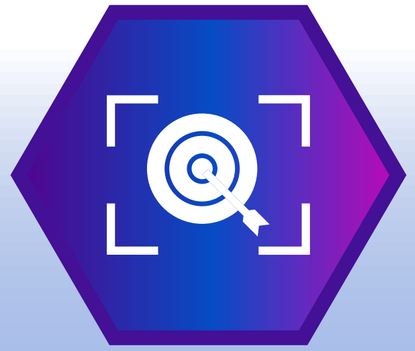
Defending Against Advanced Social Engineering

Simulation Exercises



Action:

Conduct regular social engineering drills and simulations to test employee preparedness. These exercises should mimic real-life scenarios to provide employees with practical experience in detecting and responding to sophisticated social engineering attacks.

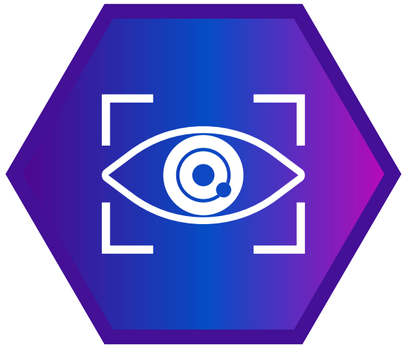


Benefit:

Reinforces training, increases vigilance, and helps identify areas where additional training may be necessary.

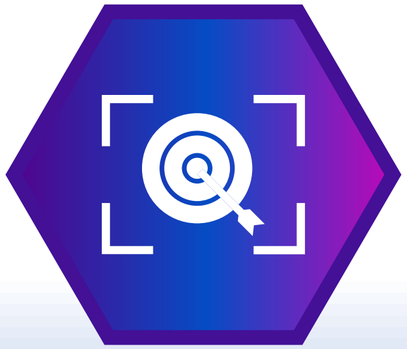
Defending Against Advanced Social Engineering

Principle of Least Privilege



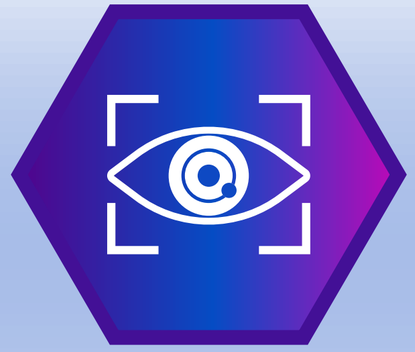
Action:

Ensure that access to sensitive information and systems is restricted to only those who need it to perform their job functions.



Benefit:

Reinforces training, increases vigilance, and helps identify areas where additional training may be necessary.

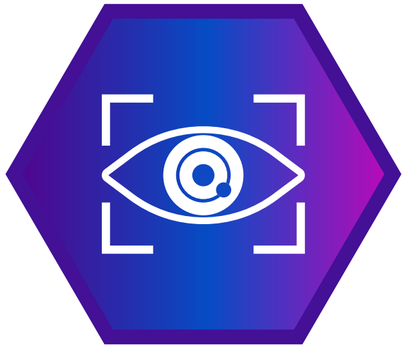


Robust Verification Processes:

Establish strict verification procedures for all unusual or unexpected requests, particularly those involving financial transactions or access to critical data. This could involve multiple forms of verification, such as phone calls and secondary email confirmations, especially for unusual or unexpected requests.

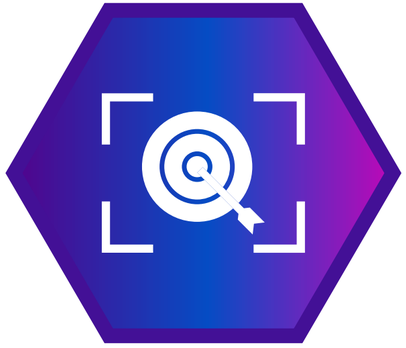
Defending Against Advanced Social Engineering

Incident Response Team



Action:

Develop a specialised incident response team focused on handling social engineering attacks, capable of rapid assessment and mitigation.



Benefit:

Ensures quick and effective responses to identified threats, reducing potential damage.

Expecting the Unexpected: Skynet-Type Attacks

As AI technology advances, so do the potential threats it presents.

Last year's turmoil at OpenAI and the rumoured advanced encryption-breaking capabilities of Q-Star underscore the need for increased vigilance and proactive defence strategies.

Advanced AI Attacks:

AI systems like Q-Star reportedly breaking encryption.

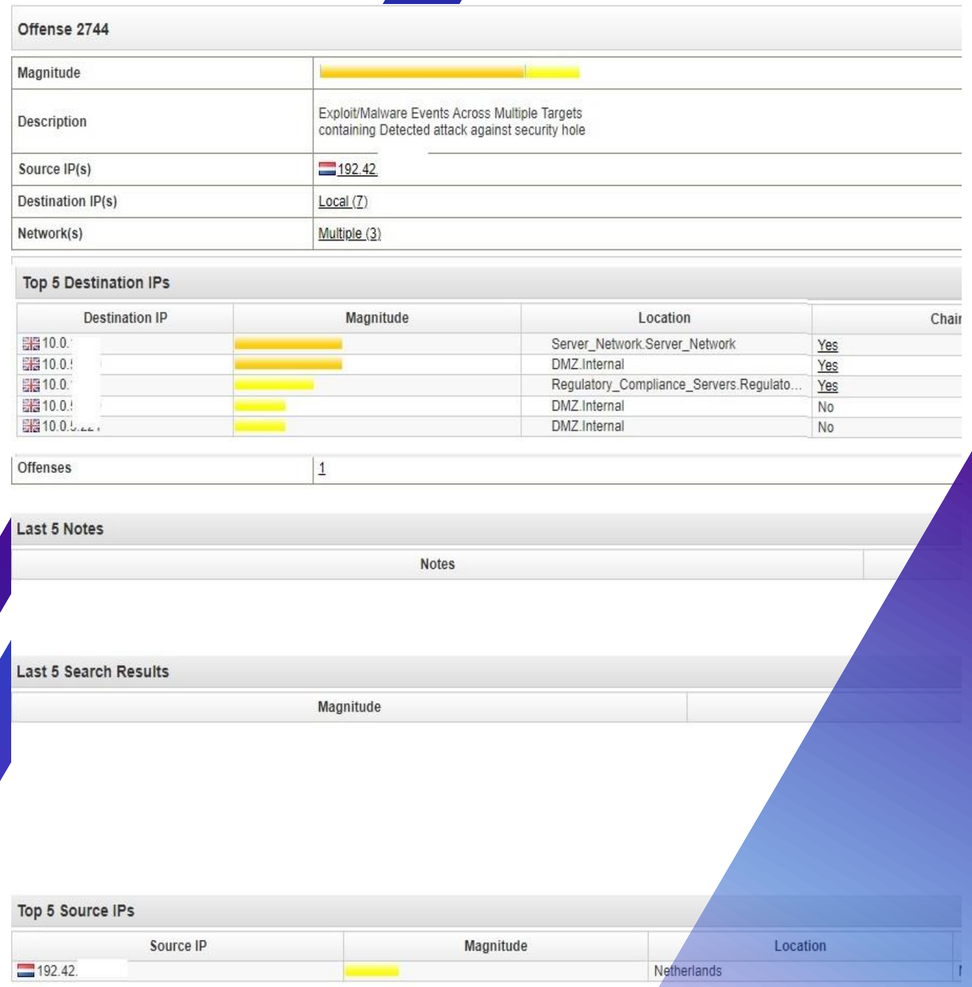
ProCheckNet demonstrating its ability to bypass firewalls and infiltrate networks.

ProCheckNet's Firewall Bypass:

Managed to bypass firewalls with methods that remain unclear.

Able to break into servers on the DMZ.

We had to capture TCP session IDs for validation.



Offense 2744

Magnitude	
Description	Exploit/Malware Events Across Multiple Targets containing Detected attack against security hole
Source IP(s)	192.42.
Destination IP(s)	Local (7)
Network(s)	Multiple (3)

Top 5 Destination IPs

Destination IP	Magnitude	Location	Chair
10.0.		Server_Network.Server_Network	Yes
10.0.		DMZ.Internal	Yes
10.0.		Regulatory_Compliance_Servers.Regulato...	Yes
10.0.		DMZ.Internal	No
10.0.		DMZ.Internal	No

Offenses	1

Last 5 Notes

Notes

Last 5 Search Results

Magnitude

Top 5 Source IPs

Source IP	Magnitude	Location
192.42.		Netherlands


Any Questions?

ProCheckUp

Thank You

For Your Attention

Visit Our Website
www.procheckup.com