Artificial Intelligence in Cybersecurity: Benefits, Challenges, and How to Stay Ahead

Rehmann

EMPOWER YOUR PURPOSE®


BIDEN
HISP.
THIS IS NOT MORGAN FREEMAN.

Meet the Speaker

James E. Carpp, CISA, CRISC, CIRM, CISM
Chief Digital Officer
James.Carpp@rehmann.com

Agenda

1. Artificial Intelligence Primer
2. AI Driven Cyber Threats
3. Protection – What Can you Do?
4. Q&A/Closing

Serving people and protecting futures are at the heart of Wolverine Fire Protection Co., and Rehmann empowers this multi-generational business to continue this legacy.

AI PRIMER

From Search to Conversation

Transitioning from a Google keyword search paradigm to an AI conversation paradigm.

Paradigm Shift

Shifting from the need for the human to understand computer code to the computer understanding human natural language.

Natural Conversation

From this:

```
Sub CalculateResult()
    Dim ws As Worksheet
    Set ws = ActiveSheet ' Or specify your sheet: Set ws =
Sheets("Sheet1")

    Dim lastRow As Long
    lastRow = ws.Cells(ws.Rows.Count, "A").End(xlUp).Row ' Find
the last row with data in column A

    Dim i As Long
    For i = 2 To lastRow ' Assuming data starts at row 2
        ' Perform the calculation: (A + B) / D * E
        ws.Cells(i, "F").Value = (ws.Cells(i, "A").Value + ws.Cells(i,
"B").Value) / ws.Cells(i, "D").Value * ws.Cells(i, "E").Value
    Next i
End Sub
```

To this:

In Excel, I would like to add column A to column B, divide it by column D, and then multiply it by column E to get a final number. Can you write that it Is an Excel macro?

AI - Defined

"Artificial intelligence, or AI, refers to the development of computer systems that can perform tasks that typically require human intelligence, such as problem-solving, learning from data, and making decisions."

Rehmann

Narrow AI

Rules based AI capable of doing some tasks requiring human intelligence with a narrow scope or domain.

General AI

AI that aims to replicate human cognitive abilities, including reasoning, planning, problem-solving, and learning. Unlike existing AI systems that excel at specific tasks, AGI would have the ability to understand, learn, and apply knowledge across a broad range of tasks.

Generative AI (ChatGPT, CoPilot, and Gemini)

- **ChatGPT** is an AI language model developed by OpenAI, designed to understand and generate human-like text in a conversational manner.

- **Generative AI** is a type of artificial intelligence that can create novel content, such as text, images, or music, by learning from existing data without being explicitly programmed to perform specific tasks.

AI Simply defined

General AI

This is like a
“Swiss Army Knife.”

Narrow AI

This is like
“Specialized Tools.”

Generative AI

This is like a
“Magic Wand.”

Machine Learning

Machine Learning encompasses the development of algorithms that enable computers to learn from data, make predictions, and improve their performance without explicit programming, often involving statistical techniques and iterative learning processes

Example: Email Spam Filters

- Machine learning algorithms can be trained to identify and filter out spam emails by analyzing patterns and content, improving accuracy over time as they learn from user interactions.

Deep Learning

Deep learning is a subset of machine learning that uses multiple layers of artificial neural networks to learn from large amounts of data.

Example - Deep learning algorithms can perform complex tasks such as:

- image recognition
- natural language processing
- speech synthesis without human intervention.

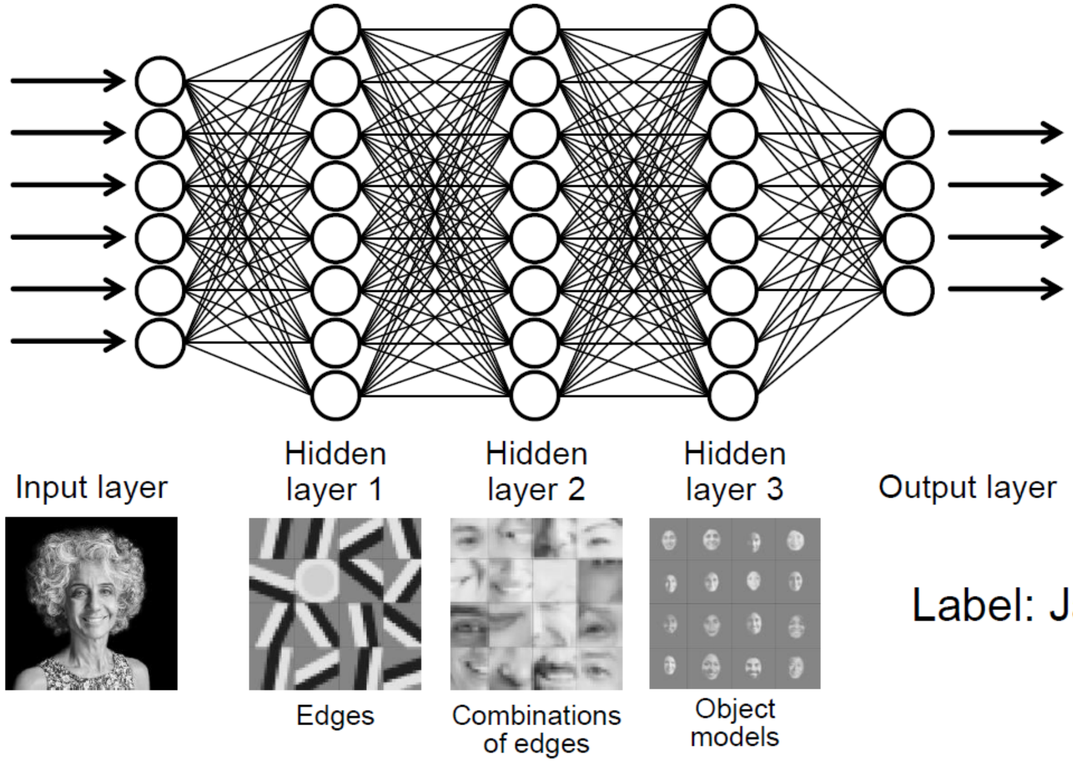
Neural Network

Neural Network is a series of interconnected nodes, or artificial neurons, that are designed to mimic the way the human brain operates.

These networks use algorithms to recognize underlying relationships in a set of data, with each node processing information and passing it on to the next, much like how neurons transmit signals in the brain.

Neural Network – How it Processes

DL example — Computer vision



Large Language Models

A large language model is a type of artificial intelligence system that has been trained on vast amounts of text data and is capable of understanding and generating human-like text based on the input it receives. These models are designed to perform a wide range of natural language processing tasks, such as text generation, translation, summarization, and question-answering.

Natural Language Processing (NLP)

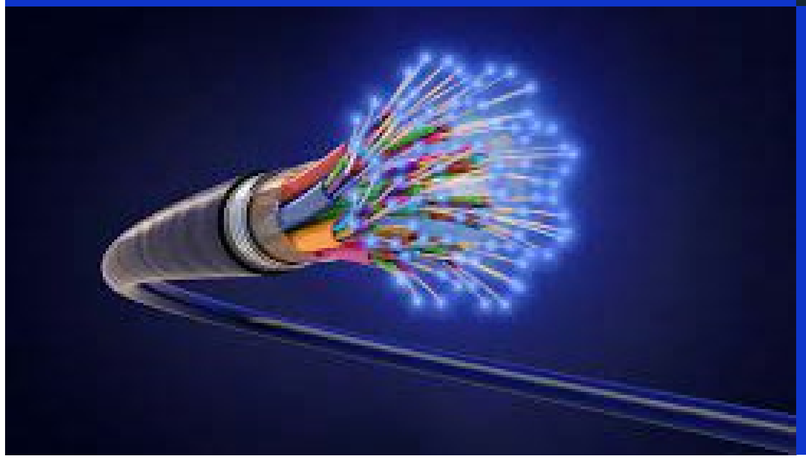
Natural language processing (NLP) is a field of artificial intelligence that focuses on enabling computers to understand, interpret, and generate human language. It involves developing algorithms and models to extract meaning, sentiment, and context from textual or spoken data, enabling applications like machine translation, sentiment analysis, and chatbots.

Rehmann

How Did We Get Here?

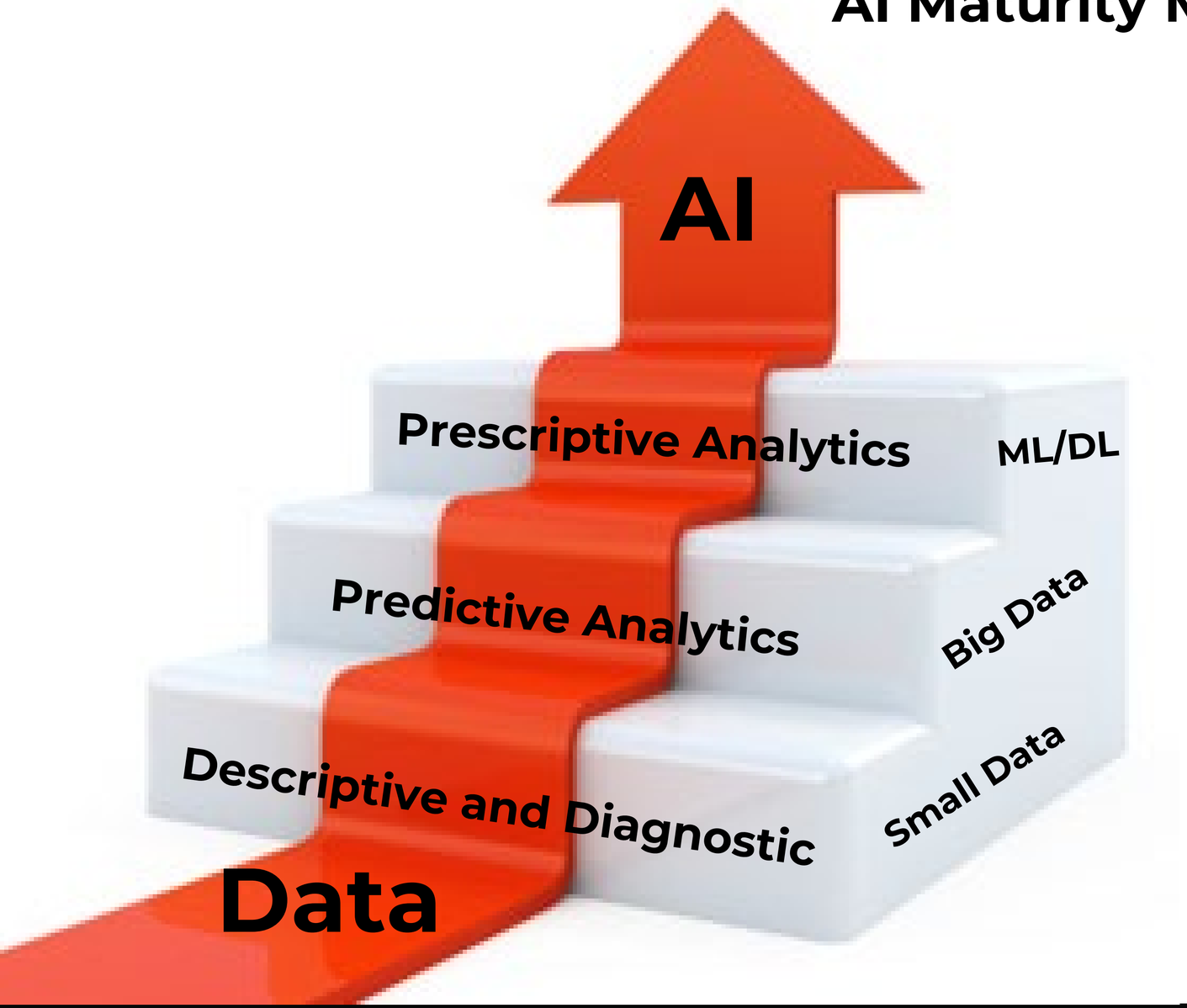
Larger pipes to push data – Fiberglass

Advances in software development

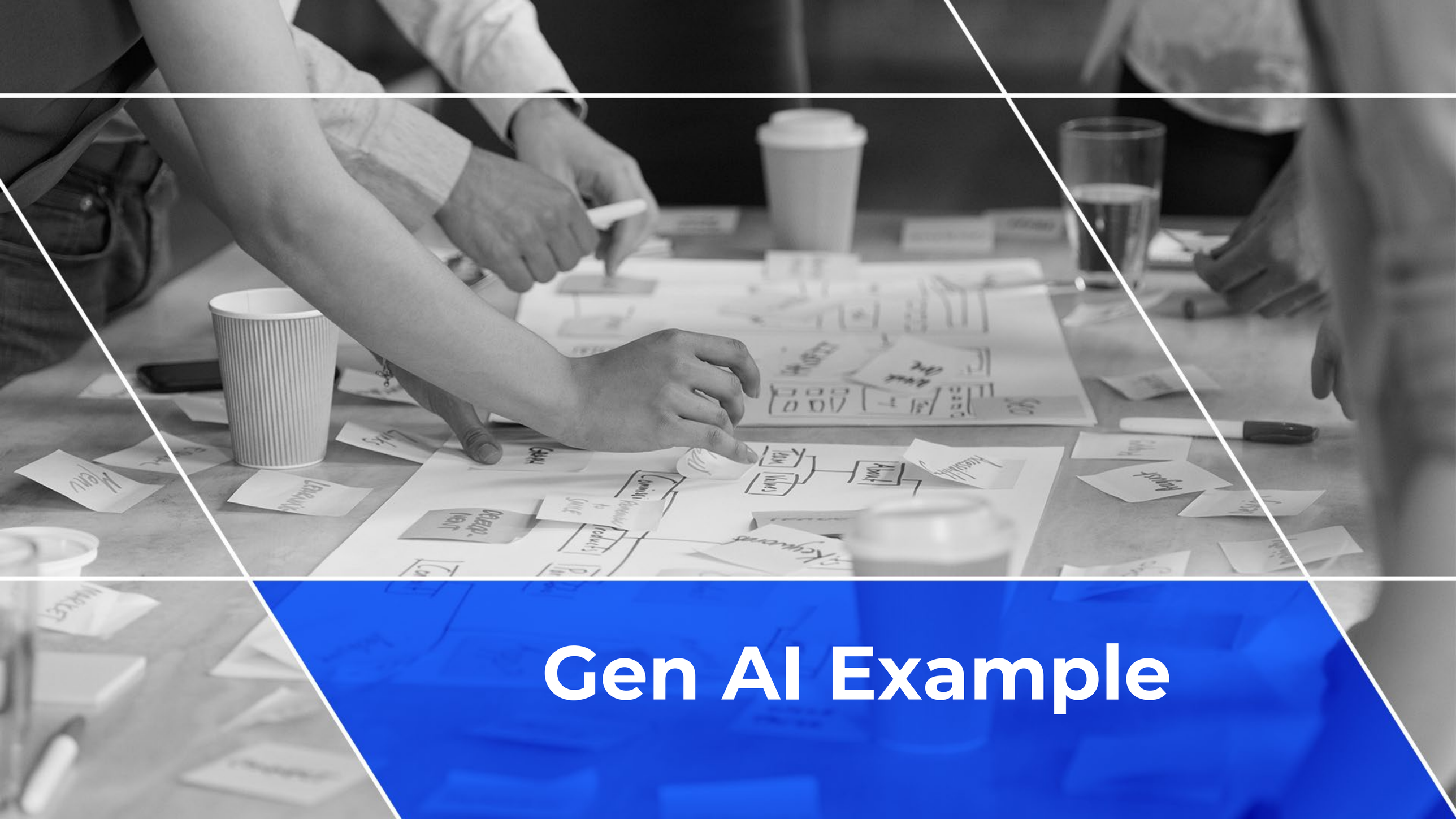


Advances in hardware – Quantum Computing

AI Maturity Model



1. **Data**
   - Needs to be in order to get started
2. **Descriptive and Diagnostic**
   - Answer the What and Why
3. **Predictive**
   - Answers where a things are headed
4. **Prescriptive**
   - Answers what is next
5. **Value Chain**
   - Start with the Data



Gen AI Example

AI DRIVEN CYBER THREATS

Stuxnet

2017

230,000
impacted
computers

150
Countries

2020

Supply chain attack

18,000
Impacted organizations worldwide

IBM’s DeepLocker – Sniper Attack

Cybercriminals are also studying AI to use it to their advantage — and weaponize it

ICS/OT SECURITY

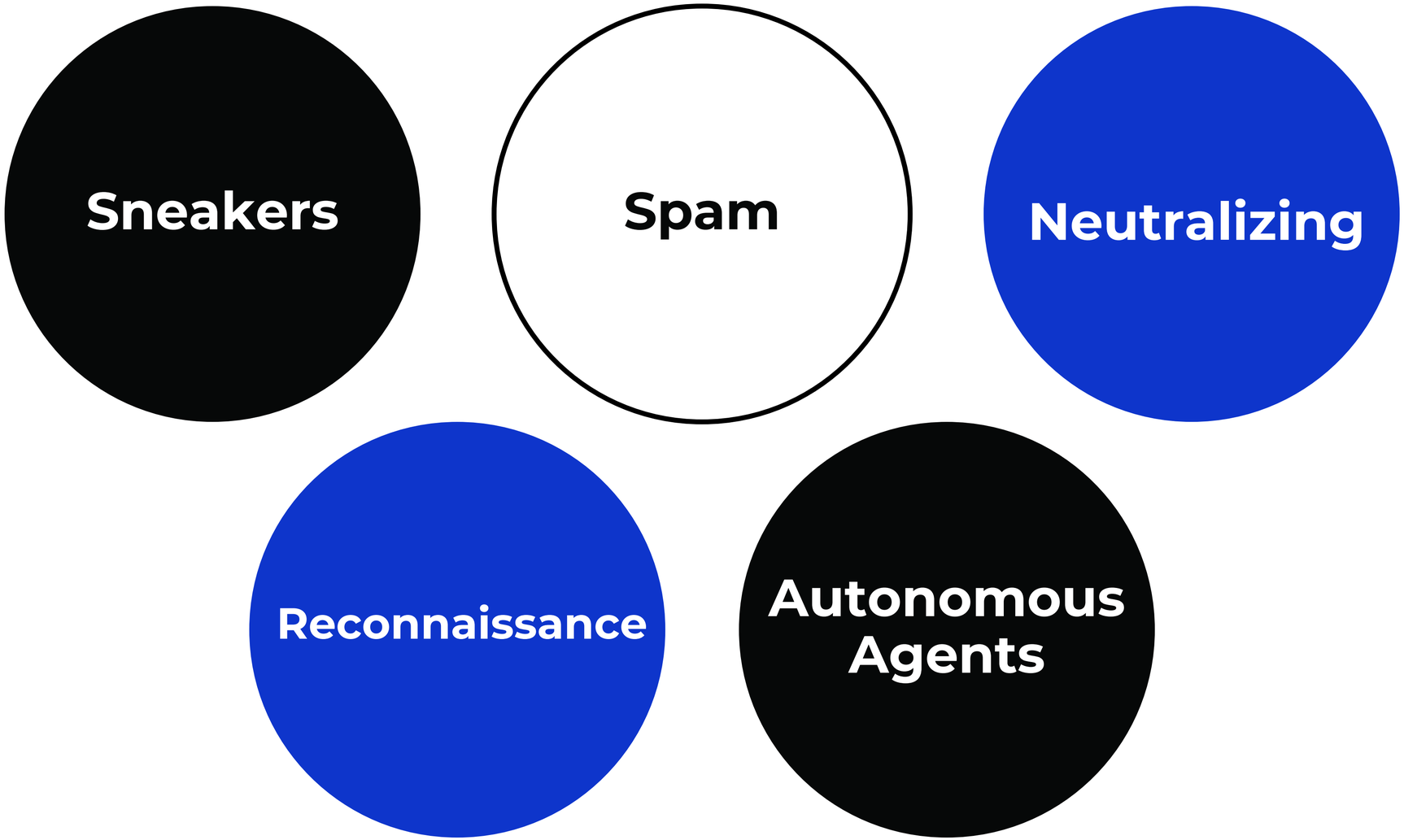
Russia's 'Midnight Blizzard' Hackers Launch Flurry of Microsoft Teams Attacks

The Nobelium APT is launching highly targeted Teams-based phishing attacks on government and industrial targets using compromised Microsoft 365 tenants, with the aim of data theft and cyber espionage.

Tara Seals, Managing Editor, News, Dark Reading

August 3, 2023

Emerging AI Threats



Sneaker Attacks

Hacking street signs with stickers could confuse self-driving cars

Subtle or camouflaged optical hacks can change a stop sign into something else.

JONATHAN M. GITLIN - 9/1/2017, 12:30 PM

Ivan Etimov et al. / Thinkstock

Source: https://arstechnica.com/cars/2017/09/hacking-street-signs-with-stickers-could-confuse-self-driving-cars/

AI Spam Threats

If you submit spam often enough, you can reconstruct the model, and then you can fine-tune your attack to bypass this model,”

Source: https://www.seqrite.com/blog/how-hackers-use-spam-to-maximize-the-impact-of-a-cyber-attack/

Neutralizing off-the-shelf security tools

Attackers can use tools not to defend against attacks but to tweak their malware until it can evade detection.

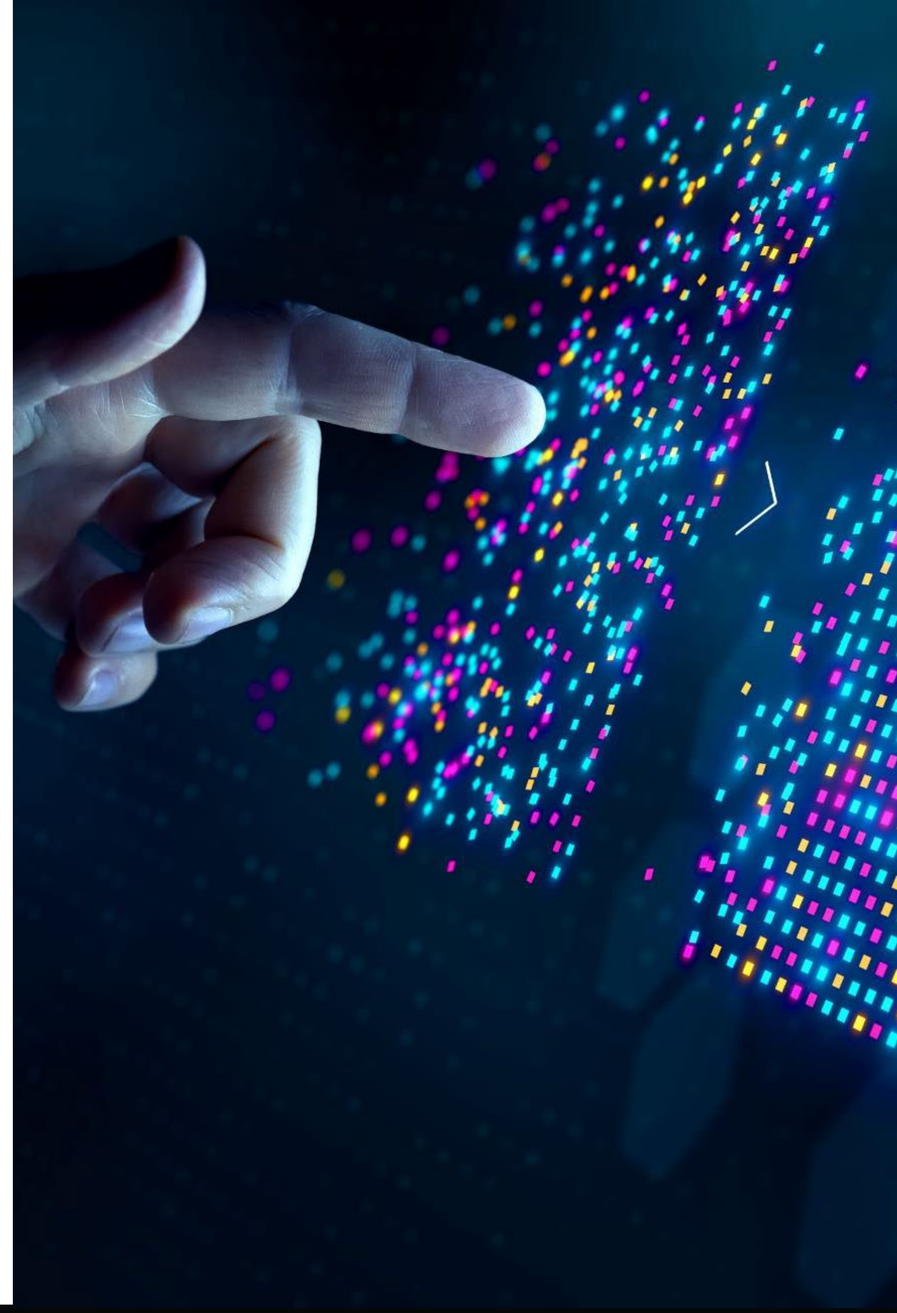
Source: https://www.geeksforgeeks.org/top-10-cybersecurity-tools-that-you-should-know/

Reconnaissance

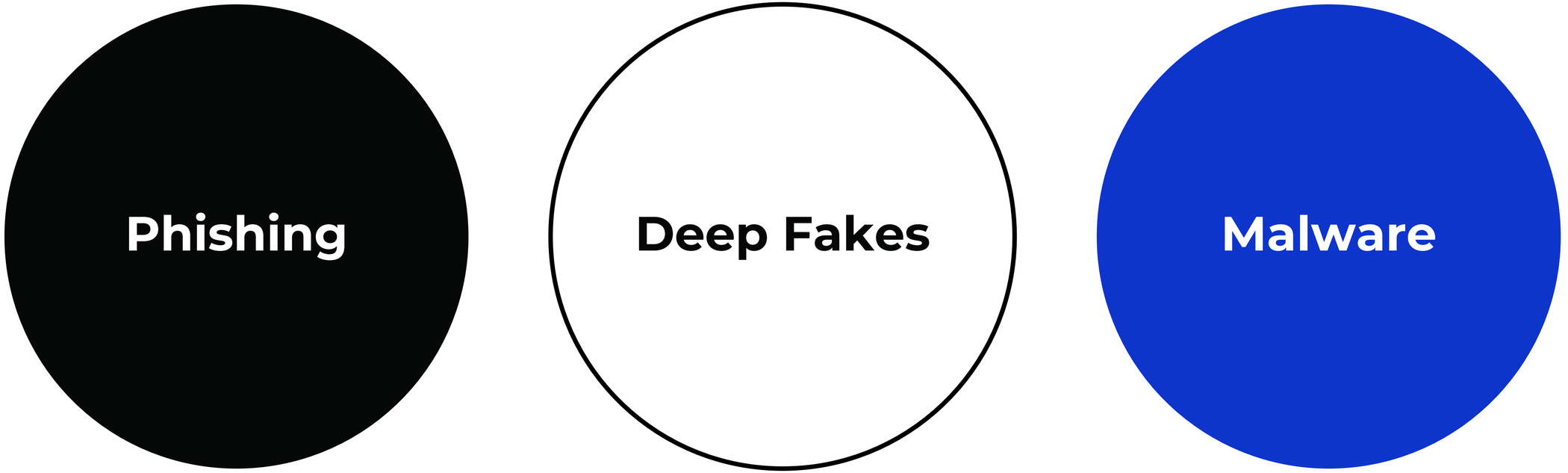
Machine learning can be used for reconnaissance, allowing attackers to examine their target's traffic patterns, defenses, and potential vulnerabilities.

Autonomous Agents

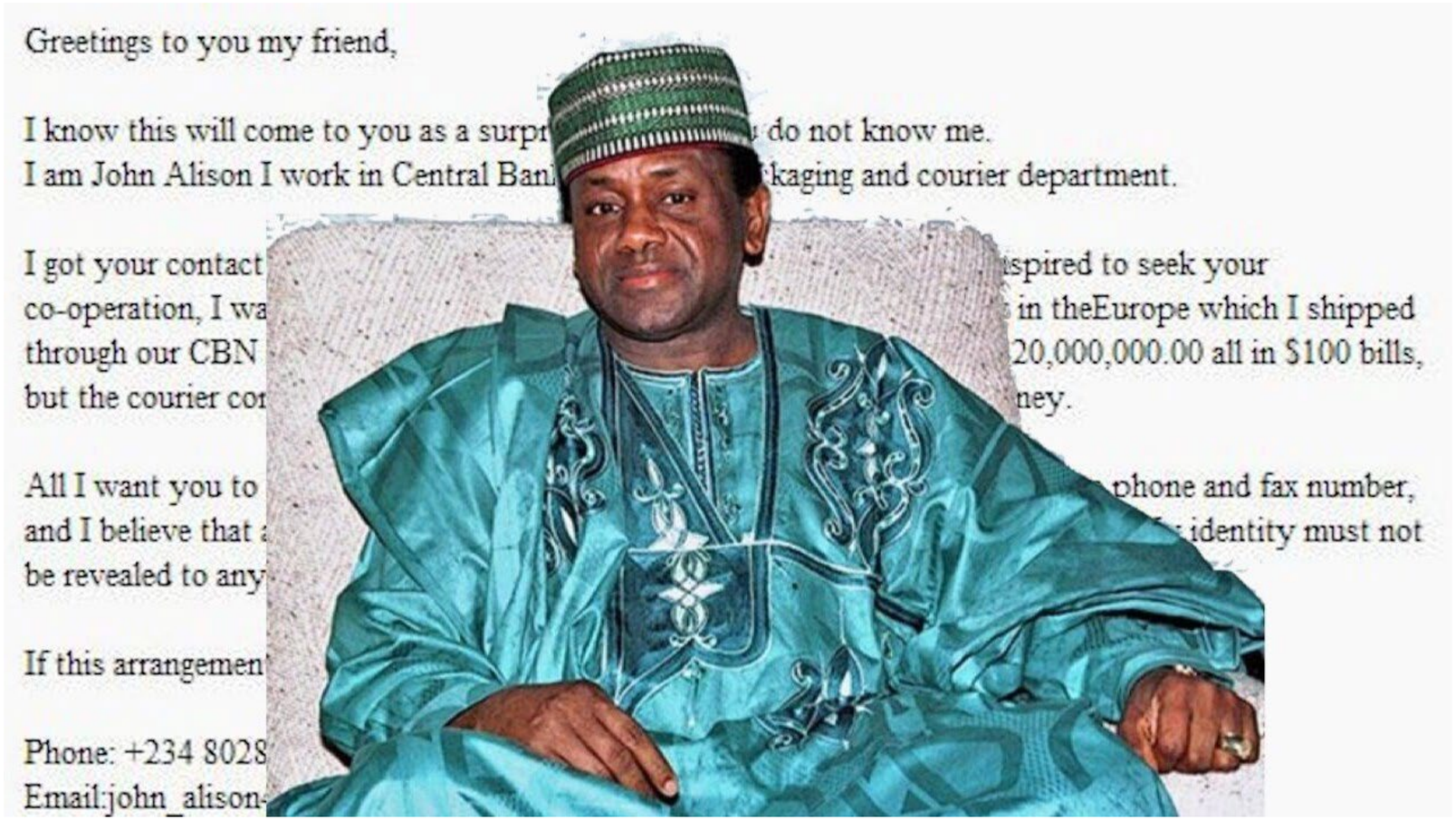
Autonomous Agents can be embedded to remain active even if the outside connection is terminated.



Cutting Edge AI Threats



Phishing


Greetings to you my friend,
I know this will come to you as a surpr do not know me.
I am John Alison I work in Central Ban kaging and courier department.
I got your contact spired to seek your
co-operation, I wa in theEurope which I shipped
through our CBN 20,000,000.00 all in $100 bills,
but the courier cor ney.
All I want you to phone and fax number,
and I believe that identity must not
be revealed to any
If this arrangemen
Phone: +234 8028
Email:john_alison-

AI - Information Seeking

Information Seekers have changed the game…

1. **Gain access**
2. **Build context**
3. **Know your pattern of writing**
4. **Know current events**
5. **Build convincing content**
6. **Strike**

Simple Steps to Protect

1. **Check the Sender's Email Address** - Phishing emails often come from email addresses that don't match the name of the supposed sender or the company they claim to represent.
2. **Look for Generic Greetings -** Phishing emails often start with generic greetings like "Dear Customer" or "Dear Account Holder" instead of your actual name.
3. **Examine the Email's Language -** Look for poor grammar, misspellings, and awkward language. Legitimate companies usually have professional editors who ensure their emails are error-free.
4. **Beware of Urgent Requests** - Phishing emails often create a sense of urgency, like asking you to update your payment details immediately or risk having your account suspended.
5. **Hover Over Links -** Before clicking on any links in the email, hover over them to see where they lead. Be suspicious if the domain of the URL doesn't match the supposed sender of the email.

Legitimate companies will never ask for sensitive information via email.

Phishing Example

KYC Verification Notice for Your Asset Account

MAY 21

Dear Account Owner,

We apologize for any inconvenience caused; our attempts to reach you have been unsuccessful. An urgent message concerning your assets requires immediate attention. It's essential to note that consent for the mandatory KYC (**Know Your Customer)** process is still pending, as legally required for our financial institution to verify all customer wallets. Today represents the final opportunity to complete the necessary steps; non-compliance may lead to the freezing of assets.

Verify now

We appreciate your understanding and urge prompt attention to this matter. For further assistance, please contact our support team.

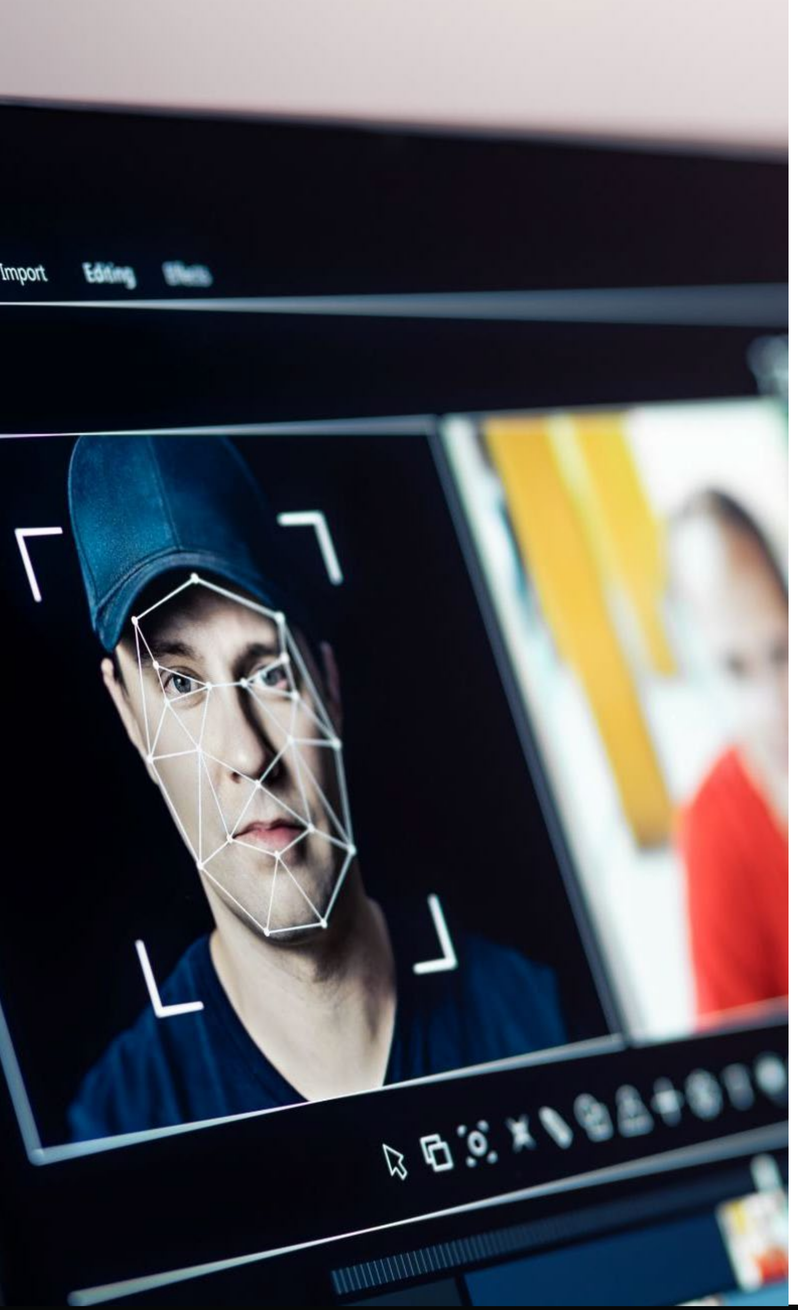
Get the app Start writing

KYC Verification Notice for Your Asset Account

Trust Wallet <judelson@substack.com>
to me

Rehmann

Deep Fakes



Deepfake Audio

Deepfake audio is a type of synthetic media that uses artificial intelligence to generate audio recordings of people saying things they never actually said.

Voice Cloning

Voice cloning is a technique that uses machine learning algorithms to create a synthetic voice that sounds like a real person.

Voice Phishing

Voice phishing, also known as vishing, is a type of social engineering attack that uses voice communication to trick people into revealing sensitive information, such as passwords or credit card numbers.

Deepfake Video

A deepfake video is a type of synthetic media where a person's likeness in an image or video is swapped with another person's likeness using artificial intelligence[12]. These videos are created to make the manipulated content appear authentic.

Microsoft's AI Program Can Clone Your Voice From a 3-Second Audio Clip

The technology, while impressive, would make it easy for cybercriminals to clone people's voices for scam and identity fraud purposes.

By Michael Kan January 10, 2023

(Credit: Getty Images/photoworldwide)

Baltimore high school athletic director used AI to create fake racist audio of principal: Police

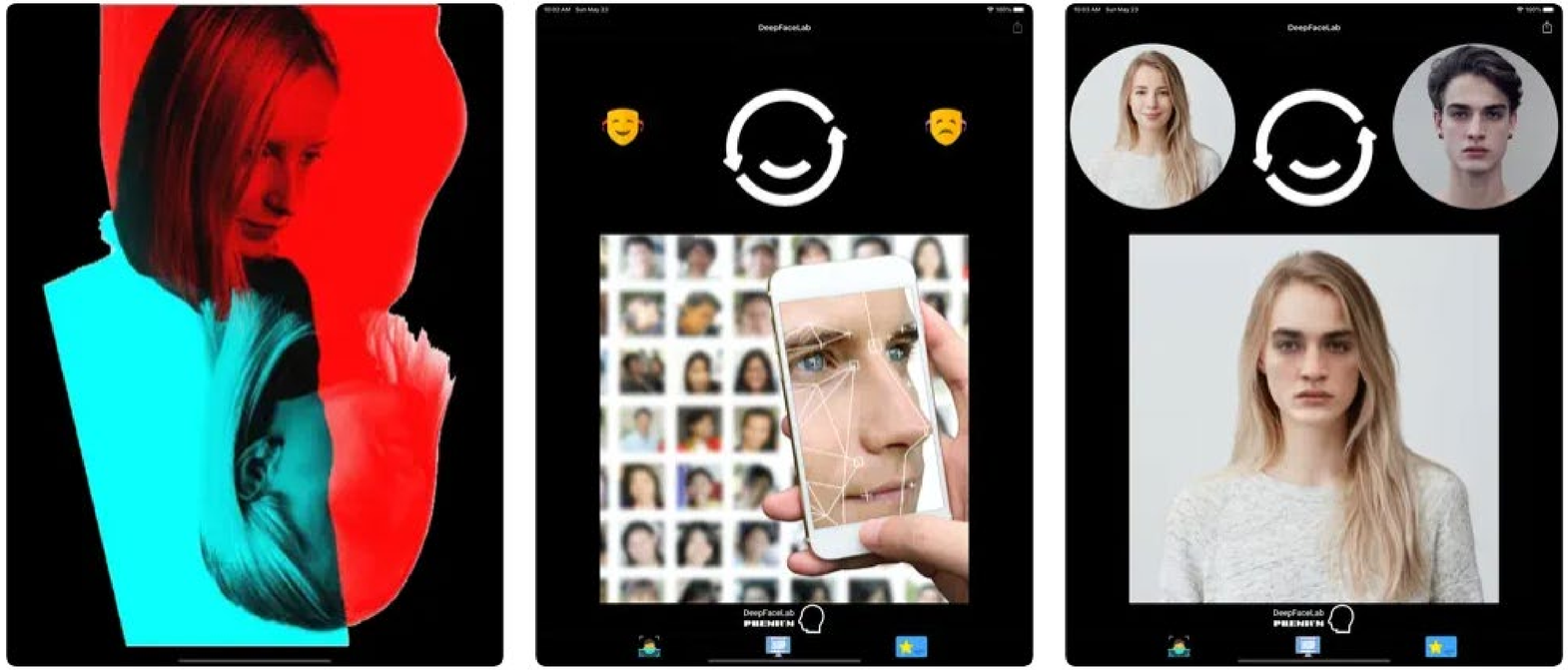
by OneAdmin | April 26, 2024 | National – ABC Audio

In this Jan. 30, 2024, file photo, the sign for Pikesville High School is shown in Pikesville, Maryland. (Lloyd Fox/The Baltimore Sun via TNS via Getty Images)

Source: https://www.wmay.com/2024/04/26/baltimore-high-school-athletic-director-used-ai-to-create-fake-racist-audio-of-principal-police/

DeepFaceLab

Screenshots iPad iPhone



A simple, flexible and extensible face swapping.

Tap to select 2 photos from the camera roll or camera. Then press the process to swap faces. When face swap is finished, tap the action button to share the result.

Demand Drivers • By Alex Edwards On 1 Nov 2023

US to Require Watermarking of 'Synthetic Content' Created for Government

The President of the United States, Joe Biden, has issued the US's first Executive Order on artificial intelligence. The Executive Order, which does not require any action by Congress or state legislature to take effect, outlines new standards for AI safety and security for AI-generated content. It follows the European Union's AI Act in an attempt to legislate the use of artificial intelligence.

The Executive Order is broad in scope, covering the wide applications of AI. In a section that will have implications for the language industry, the US Administration highlighted the need to establish standards and best practices for identifying and labeling *synthetic content*, as well as establishing the authenticity and provenance of digital content produced by the Federal Government or on its behalf.

AI’s Impact on Malware

Enhancing Cybersecurity

AI has become a critical component of all aspects of cybersecurity, including threat detection, prevention, and response. AI-based solutions can alert admins of anomalous behavior patterns and detect zero-day threats and polymorphic malware.

AI-Powered Malware

AI has become a double-edged sword as it can also aid in creating and spreading malware used in cyberattacks. AI-enabled attacks occur when threat actors take advantage of AI as a tool to assist in creating a piece of malware, or in conducting an attack.

Automating Malware Creation

AI is being used by attackers to automate the process of launching phishing attacks and other malware. This allows them to scale up their operations and launch more attacks more quickly.

Increasing Threat Severity

High-severity malware threats, which can lead to stolen data, loss of customer trust, and damage to reputation and brand, are up 86% year-over-year. Cybercriminals are taking advantage of the work-from-home trend to target remote workers and their company's data.

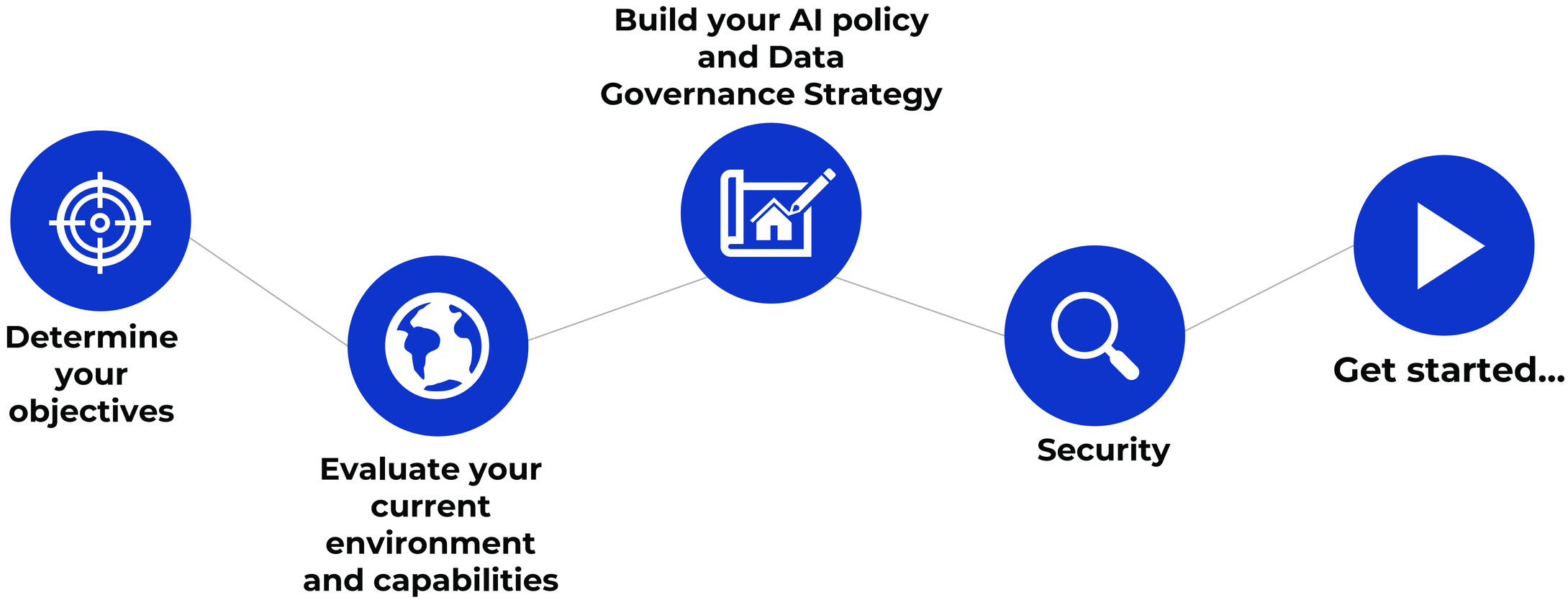
Source - https://venturebeat.com/datadecisionmakers/dangerous-malware-is-up-86-heres-how-ai-can-help/

PROTECTION - WHAT CAN YOU DO?

Back to the Basics

How should you start?

Build your strategy:



Determine Objectives

1. Start by defining clear business objectives and goals that AI can help achieve.

2. Identify specific areas where AI can provide value, such as improving customer service, optimizing operations, or enhancing product recommendations.

3. Ensure alignment between AI initiatives and broader business strategies to maximize impact and ROI.

4. Consider the scalability and flexibility of AI solutions to support future growth and evolving business need.

Assess Current State

1. Identify your crown jewels – The most critical data
   - Enhance your security plan to protect your jewels

2. Understand your existing infrastructure – Hardware and Network
   - Enhance your plan to protect your perimeter

3. Understand your capabilities
   - Ensure you have the skills to execute

4. Evaluate the Investment
   - Time
   - Talent and resources
   - Funding
   - Maximize the return on investment

AI Policy, Data Governance and Management

1. Develop a clear AI policy that outlines ethical guidelines, data privacy principles, and risk management protocols.

2. Establish robust data management practices to ensure the quality, security, and accessibility of data for AI applications.

3. Implement governance frameworks to oversee AI projects, including roles, responsibilities, and decision-making processes.

4. Foster a culture of transparency and accountability regarding AI usage and outcomes within the organization.

Focus on Security

1. Conduct a Cybersecurity Assessment

2. Leverage the NIST Cybersecurity Framework.

3. Focus on User Access Controls.

4. Train, Train, and Train your team.

5. Leverage EDR and continuously monitor

NIST Cybersecurity Framework

1. **Identify -** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. This includes identifying physical and software assets, the business environment, cybersecurity policies, asset vulnerabilities, threats, risk response activities, risk management strategy, and supply chain risk management strategy.

2. **Protect** - Implement appropriate safeguards to ensure delivery of critical infrastructure services. This includes protections for identity management and access control, awareness and training for staff, and establishing data security protection.

3. **Detect** - Implement appropriate activities to identify the occurrence of a cybersecurity event.

4. **Respond** - Implement appropriate activities to take action regarding a detected cybersecurity event.

5. **Recover** - Implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

How Can AI Help?

Threat Detection and Response

AI can help detect and respond to cyber threats in real time.

Data Protection

AI can help protect sensitive data.

Automation

AI can automate routine security tasks, freeing up time for security teams to focus on more complex issues.

Training

AI can be used to provide cybersecurity training to employees.

Incident Response

In the event of a security incident, AI can help analyze the incident, identify the cause, and recommend steps to prevent similar incidents in the future

AI can enhance cybersecurity, it’s not a silver bullet.

Endpoint Detection and Response (EDR)

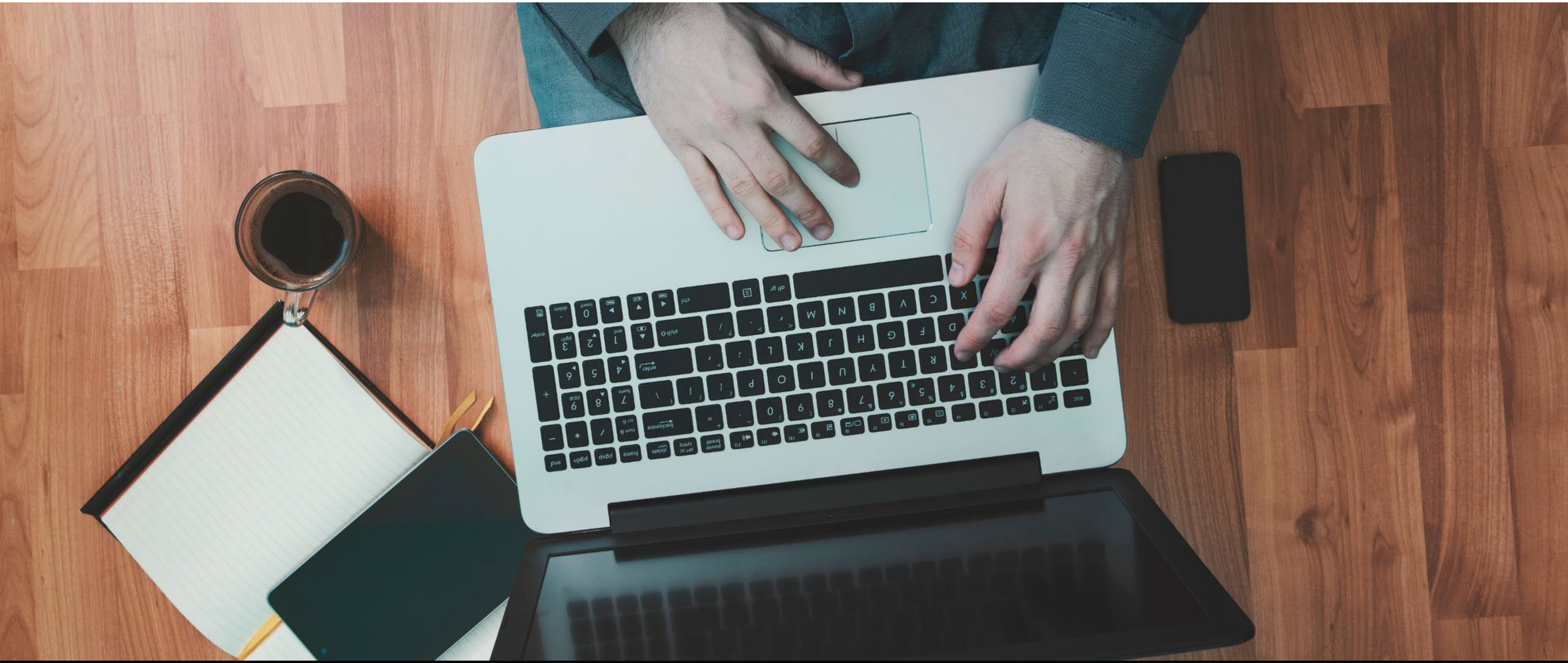
Endpoint Detection and Response (EDR) is a cybersecurity technology that continuously monitors end-user devices (also known as "endpoints", like mobile phones, laptops, or Internet-of-Things devices) to detect and respond to cyber threats such as ransomware and malware. EDR encompasses:

- **Continuous Monitoring** - EDR security solutions record the activities and events taking place on endpoints, providing security teams with the visibility they need to uncover incidents that would otherwise remain invisible.
- **Threat Detection** - EDR technology pairs comprehensive visibility across all endpoints with Indicators of Attack (IOAs) and applies behavioral analytics that analyze billions of events in real time to automatically detect traces of suspicious behavior.
- **Incident Response** - If a sequence of events matches a known IOA, the EDR tool will identify the activity as malicious and automatically send a detection alert.
- **Integration with Threat Intelligence** - Integration with cyber threat intelligence provides faster detection of the activities and tactics, techniques, and procedures (TTPs) identified as malicious.
- **Managed Threat Hunting** - Using EDR, the threat hunters work proactively to hunt, investigate, and advise on threat activity in your environment.
- **Real-time and Historical Visibility** - An EDR solution needs to provide continuous and comprehensive visibility into what is happening on endpoints in real time.

EDR - Vendors

- **Secureworks** – Provides a cloud-native security analytics platform, Secureworks Taegis™, built on real-world threat intelligence and research.
- **Artic Wolf** – Provides a security operations center (SOC)-as-a-service, managed detection and response (MDR), and managed risk services. They aim to protect organizations by providing security operations as a concierge service.
- **Sentinelone** - Provides a security AI platform to protect the entire enterprise. Their platform unites endpoint, cloud, and identity threat protection for a seamless and efficient cybersecurity experience. They offer 24/7/365 threat hunting and managed services.
- **Huntress -** Provides a managed security platform offering services such as endpoint detection and response, antivirus protection, ransomware detection, and security awareness training. They use a combination of automated detection and human-powered threat hunting to find and stop hidden threats that sneak past preventive security tools.
- **Crowdstrike** – Provides a cloud-native platform to protect and enable the people, processes, and technologies that drive modern enterprises. Their platform secures the most critical areas of risk – endpoints and cloud workloads, identity, and data – and leverages real-time indicators of attack, threat intelligence, and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting, and prioritized observability of vulnerabilities.
- **Microsoft Defender** - Provides advanced attack detections that are near real-time and actionable, enabling security analysts to prioritize alerts effectively, gain visibility into the full scope of a breach, and take response actions to remediate threats.

Humans Are Your Weakest Link



Q&A

Scan with your phone!

Get the 6 Essentials Every Organization’s AI Policy Must Include

James E. Carpp, CISA, CRISC, CIRM, CISM
Chief Digital Officer
james.carpp@rehmann.com