# Navigating the New Frontier:

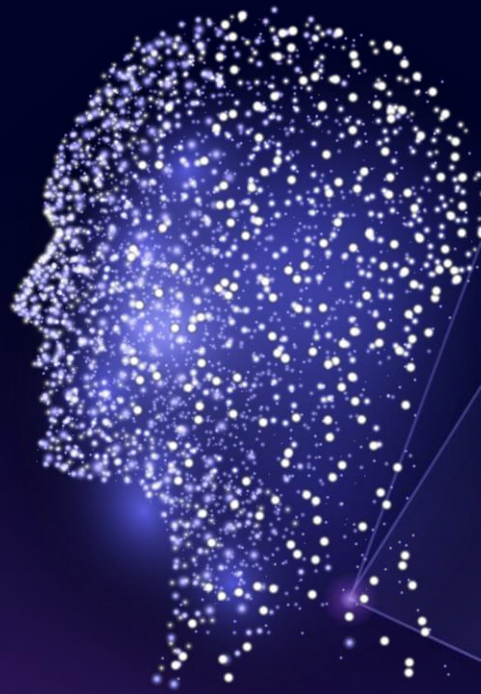
## Penetration Testing in the AI/ML Era

# About Me

## Herman Cowart

A veteran of the U.S. Army, he is the Founder and CEO of Paradoxical Security, specializing in offensive security across various sectors. He leads the company in delivering tailored cybersecurity solutions to tackle complex security challenges.

He manages a team of 18 penetration testers on a government contract, overseeing 170 to 190 penetration tests and red team engagements annually. His expertise in both military operations and cybersecurity ensures robust protection for critical infrastructures.



# Agenda

01 Introduction to Penetration Testing

02 The AI/ML Buzz/Craze

03 AI/ML in Application Development

04 Impact of AI/ML on Security Vulnerabilities

05 Conclusion

06 Q/A

# Introduction to Penetration Testing

**Beyond Vulnerability Scanning:** Distinguishes itself from vulnerability assessments by not relying on automated scanners to find known weaknesses

**Manual Testing Approach:** Involves hands-on techniques to simulate real-world attacks, beyond automated scanning

**Focus on Zero-Day Vulnerabilities:** Identifies previously unknown and unpatched security flaws

**Exploit Validation:** Confirms whether identified vulnerabilities are exploitable, providing a clear view of potential risks

**Prioritization of Remediation:** Helps organizations prioritize fixes based on the severity and exploitability of discovered vulnerabilities

# The AI/ML Buzz/Craze


## Artificial Intelligence (AI):

AI is a broad field of computer science focused on creating systems capable of performing tasks that would typically require human intelligence. These tasks include decision-making, object detection, speech recognition, and language translation.

## Machine Learning (ML):

ML is a subset of AI that involves training a model using large amounts of data and algorithms that give the system the ability to learn how to perform a task without being explicitly programmed to do so.

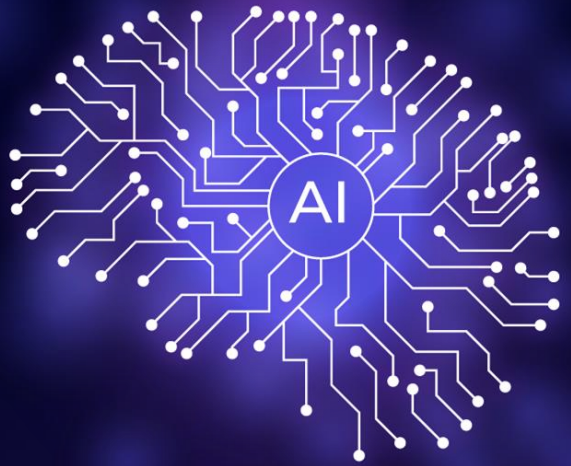
## Deep Learning (DL):

Deep learning is a specialized subset of ML that uses layered neural networks to analyze various factors of data. It mimics the human brain's ability to recognize patterns and classify various types of information.

## Natural Language Processing (NLP):

NLP is a branch of AI that gives machines the ability to read, understand, and derive meaning from human languages.

# The AI/ML Buzz/Craze




Artificial Intelligence and Machine Learning revolutionize industries by automating tasks and enhancing data analysis, leading to more accurate and faster decision-making. These technologies improve efficiency and productivity, freeing up resources for strategic work. They also personalize user experiences, increasing customer satisfaction and enabling new business models in various sectors like healthcare and finance.

# AI/ML in Application Development

| | |
|---|---|
| **Complexity of AI/ML Models** | AI and ML models are inherently complex, and their internal workings can often be opaque, even to their developers. This nature can make it difficult to predict or understand behavior, leading to unexpected outcomes or decisions. |
| **Data Quality and Bias** | Models are only as good as the data they are trained on. Poor quality, biased, or insufficient training data can lead to inaccurate models that make flawed decisions or exhibit biased behavior, affecting application reliability and fairness. |
| **Lack of Expertise** | Implementing AI/ML requires a certain level of expertise not only in machine learning but also in application security. Without this expertise, the integration of these technologies can be mishandled, leaving applications vulnerable to both conventional and AI-specific attacks. |
| **Challenges in Understanding AI-Generated Code** | Applications developed with the assistance of AI/ML can include code that is auto-generated. This code can be complex and not easily understood by human developers, which poses significant challenges when trying to apply updates or patches. |
| **Security Vulnerabilities** | When developers without a deep understanding of AI/ML technologies or security principles utilize these models in applications, they can inadvertently introduce security vulnerabilities. |
| **Remediation Complexity for AI-Induced Vulnerabilities** | AI/ML-generated code can introduce vulnerabilities that are non-intuitive and difficult to trace to their origin. Developers may find it particularly challenging to patch these vulnerabilities due to the complex and opaque logic that AI algorithms create. |

# Impact of AI/ML on Security Vulnerabilities

01. Emergence of New Vulnerability Types

02. Increased Complexity of Applications

03. Vulnerability Proliferation AI/ML Code

# Impact of AI/ML on Security Vulnerabilities

## Emergence of New Vulnerability Types

Integrating Artificial Intelligence (AI) and Machine Learning (ML) into application development inherently increases complexity across several dimensions.

First, AI/ML models require layers of data processing—from collection to analysis and inference—each introducing potential points of vulnerability.

Additionally, these applications often need to interact dynamically with existing systems, presenting integration challenges that can obscure potential security weaknesses. The adaptability of AI/ML models, while a strength, also allows the system's behavior to evolve unpredictably as new data is processed, complicating consistent security evaluation.

# Impact of AI/ML on Security Vulnerabilities

## Increased Complexity of Applications

The unique characteristics of AI/ML-driven applications give rise to new forms of vulnerabilities.

For instance, data poisoning can subtly corrupt the training process, resulting in a model that performs incorrectly or maliciously under specific conditions.

Adversarial attacks are another significant concern, where minimal, carefully crafted perturbations to input data can lead models to make erroneous predictions or classifications.

# Impact of AI/ML on Security Vulnerabilities

## Vulnerability Proliferation AI Code

The integration of AI and ML into application development often involves the use of shared datasets and pre-trained models. This practice, while efficient, can also be a vector for widespread security vulnerabilities. If a vulnerability is discovered in a common model or dataset, it can affect all applications that utilize these shared resources.

As AI/ML applications proliferate, the propagation of vulnerabilities through shared resources necessitates a more vigilant and proactive approach to security. This includes not only identifying and patching known vulnerabilities but also monitoring the behavior of deployed AI models to detect and mitigate emerging security threats.

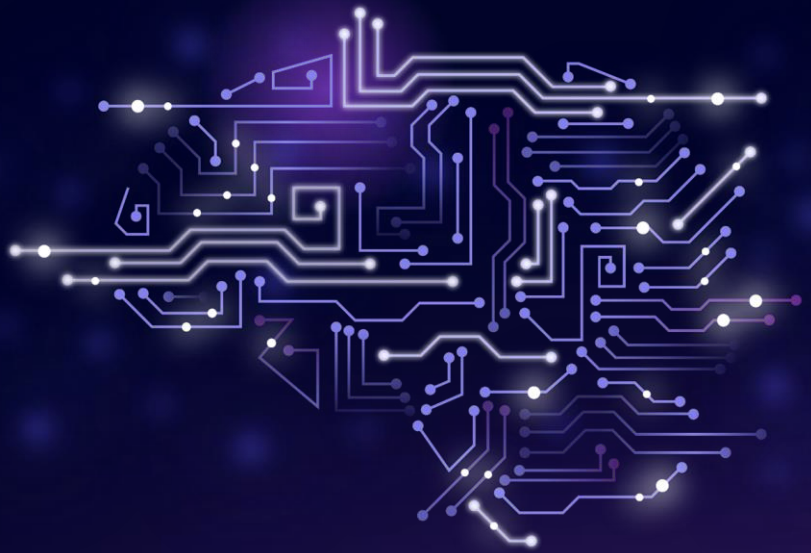
# Conclusion

While AI and ML technologies offer transformative potential for innovation and efficiency, they also introduce heightened risks and complexities, particularly in the realm of cybersecurity. The adoption of AI/ML by developers with limited understanding in secure coding practices can inadvertently amplify these risks.

A significant concern arises from the gap in developers' knowledge regarding not only the underlying mechanisms of AI/ML but also fundamental principles of secure application development. This discrepancy can lead to the deployment of AI systems fraught with vulnerabilities, making them susceptible to a new spectrum of cyber threats.

It is essential to enhance the education and training of developers in secure coding practices, specifically tailored to the integration of AI/ML technologies. Ensuring that developers understand both the power and the pitfalls of AI/ML will be crucial in mitigating risks effectively.

# Any Questions?



# THANK YOU

Herman Cowart
Herman.Cowart@ParadoxicalSecurity.com

https://paradoxicalsecurity.com

PARADOXICAL SECURITY