Generative AI in Cybersecurity

Information Systems Security Association – Northern Virginia Chapter (ISSA-NOVA)

December14th, 2023
6:00 pm to 7:00 pm EDT

Jim Wiggins
Chief Executive Officer
Federal IT Security Institute

FITSI
FEDERAL IT SECURITY INSTITUTE
HELPING SECURE THE NATION'S FEDERAL INFORMATION SYSTEMS

Overview

- Overview of Artificial Intelligence and Generative AI
- Introduction to Generative AI in Cybersecurity
- Foundations of Generative AI
- Common Platforms
- Types of Use
- Generative AI for Enhanced Threat Intelligence
- Policy Optimization through Generative AI
- Generative AI in Cybersecurity Training
- Other Possible Cybersecurity Use Cases
- Ethical and Privacy Concerns in Generative AI
- Limitations and Challenges of Generative AI
- Real-world Applications and Case Studies
- Collaborative Defense: Human and Generative AI Synergy
- Q&A Session

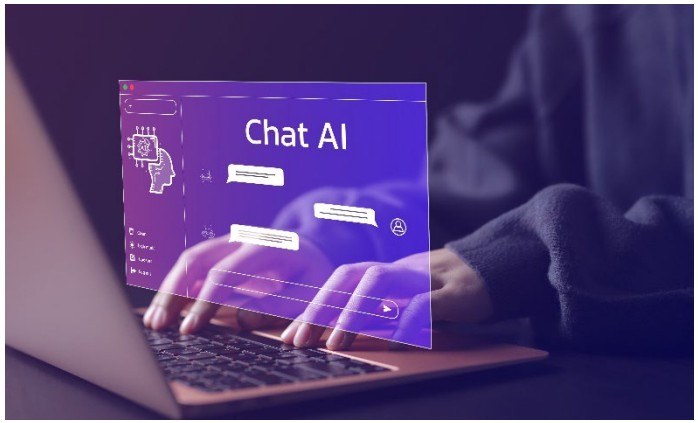
Overview of Artificial Intelligence and Generative AI

- Artificial Intelligence
  - Simulation of human intelligence processes by machines, especially computer systems to include learning, reasoning and self-correction.
- Examples
  - Healthcare
    - Diagnose a disease with medical images
  - Transportation
    - Self driving cars
  - Manufacturing
    - Optimize assembly lines

Foundations of Generative AI

- Overview of Generative AI and its significance.
- The increasing relevance of Generative AI in the cybersecurity landscape.

Foundations of Generative AI

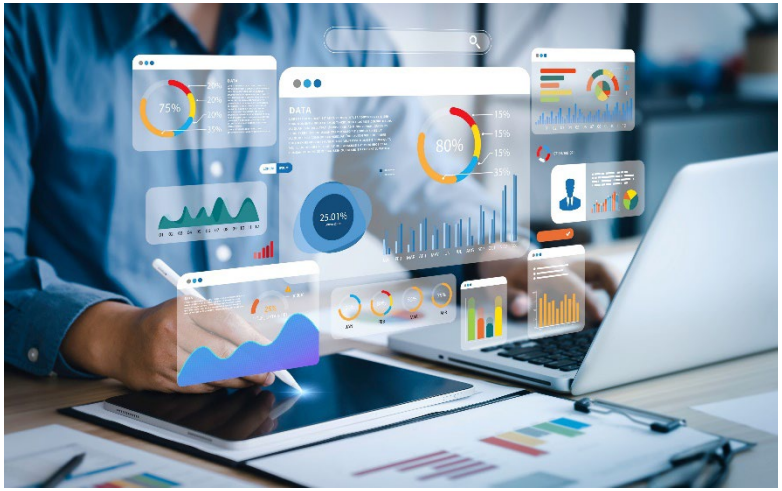


- Core principles behind Generative AI.
- Introduction to Generative Adversarial Networks (GANs) and their mechanics.
- Other generative models and their implications in cybersecurity.

Common Platforms

- Current Generative AI Players:
  - Text
    - OpenAI
      - ChatGPT
    - Google
      - Bard
    - Microsoft
      - Bing
  - Graphics
    - OpenAI
      - Dalle-2/3
    - Midjourney

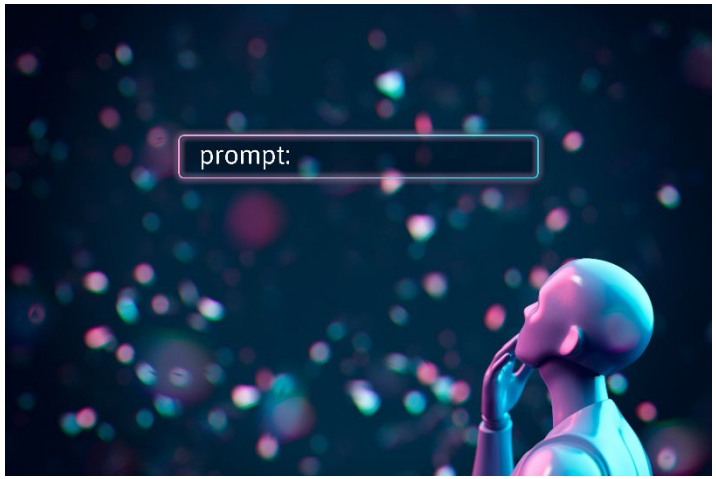
Types of Uses of Generative AI



- Brainstorming
- Content Creation
- Proofing
- Learning

Prompting

- Prompt: A question or a statement that you provide to ChatGPT or Bard to start a conversation or ask for information.



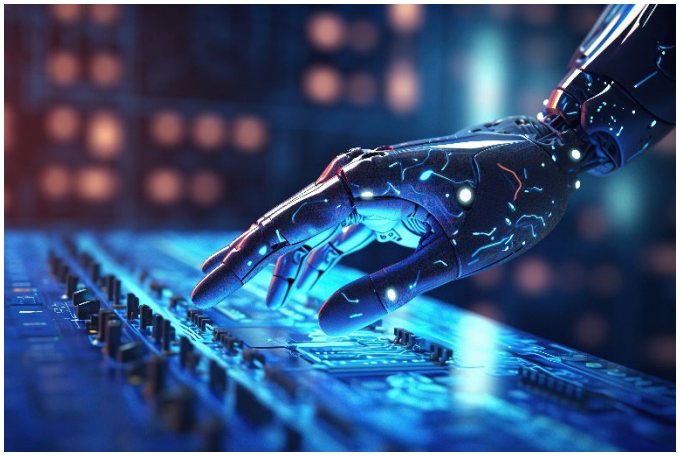
- Quality of the prompt matters!

Limitations and Challenges of Generative AI

- Potential biases in AI outputs.
- Vulnerabilities specific to Generative AI.
- Addressing the risks of AI misuse (e.g., deepfakes in phishing).

Generative AI for Enhanced Threat Intelligence

- Using Generative AI to simulate cyber threats.
- Advantages of predictive threat modeling.
- Improving threat detection through AI-generated patterns.



Policy Optimization through Generative AI

- Crafting and refining cybersecurity policies with AI insights.
- Simulating policy impacts using Generative AI.
- Continuous policy adaptation based on AI-driven feedback.

Generative AI in Cybersecurity Training

- AI-augmented training scenarios.
- Role-playing and simulations powered by Generative AI.
- Continuous learning modules adapted to evolving AI-generated threats.

Other Possible Cybersecurity Use Cases

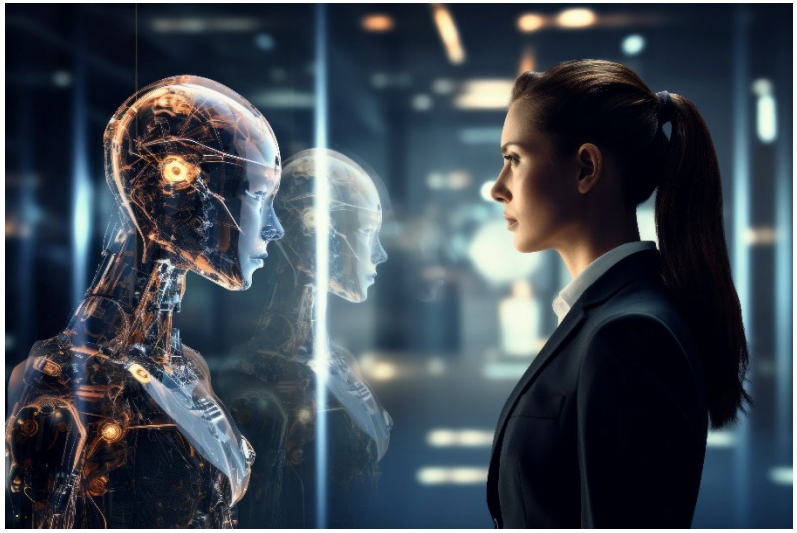
- Threat Intelligence Analysis
- Incident Response Communication
- Training and Simulation
- Public Awareness Campaigns
- Policy and Regulation Drafting
- Automated Vulnerability Assessments
- Visual Threat Representations
- Predictive Analysis
- Social Media Monitoring
- AI-Assisted Forensics
- Disaster Response Coordination
- Enhancing Internal Operations
- Research and Development
- Stakeholder Engagement
- Customized Learning and Development

Ethical and Privacy Concerns in Generative AI

- Addressing data privacy in Generative AI models.
- Ethical implications of AI-generated content.
- Ensuring responsible use of Generative AI in cybersecurity.

Collaborative Defense: Human and Generative AI Synergy

- Balancing human expertise with AI capabilities.
- Enhancing decision-making processes with AI insights.
- Best practices for effective collaboration.



Q&A Session

Recap

- Overview of Artificial Intelligence and Generative AI
- Introduction to Generative AI in Cybersecurity
- Foundations of Generative AI
- Common Platforms
- Types of Use
- Generative AI for Enhanced Threat Intelligence
- Policy Optimization through Generative AI
- Generative AI in Cybersecurity Training
- Other Possible Cybersecurity Use Cases
- Ethical and Privacy Concerns in Generative AI
- Limitations and Challenges of Generative AI
- Real-world Applications and Case Studies
- Collaborative Defense: Human and Generative AI Synergy
- Q&A Session