Course:
Cybersecurity in the age of GenAI: Understanding Generative AI and its impact on cybersecurity

Course Description

In the ever-evolving landscape of cybersecurity, the stakes have never been higher. With cyber threats becoming more sophisticated and elusive, how can individuals and organizations stay one step ahead? The answer lies in harnessing the groundbreaking potential of Generative AI (GenAI). As the digital realm faces an unprecedented wave of challenges, this comprehensive course serves as your beacon through the complexities of GenAI in cybersecurity.

Why is the convergence of Generative AI and cybersecurity more relevant today than ever? In an age where digital transformation accelerates at breakneck speeds, adversaries are also leveraging AI to orchestrate more complex and stealthy attacks. Understanding and utilizing GenAI in defense mechanisms has become indispensable. This course unravels GenAI's capabilities, challenges, and the ethical landscape, preparing you to leverage its power responsibly and effectively.

Embark on a captivating journey through our curriculum, meticulously designed to address the nuances of GenAI in cybersecurity. You'll delve into the impact of GenAI on cyber threats, exploring both the opportunities and the challenges it presents.

Through comparative analyses, this course dissect the differences between traditional and AI-enhanced cyber threats, providing you with a comprehensive understanding of the evolving threat landscape.

An entire section is devoted to AI-specific vulnerabilities, where you'll explore the mechanics of AI-powered malware, unravel the intricacies of data poisoning, and study real-world cases of AI-specific cyberattacks. This prepares you to recognize and tackle sophisticated threats that leverage AI technologies.

Defensive strategies are a cornerstone of this course. From principles of secure prompt engineering to implementing adversarial testing, we guide you through strategies that fortify AI systems against potential breaches. Detailed modules on detecting and mitigating deepfakes and preventing AI-enhanced phishing attacks are designed to equip you with potent countermeasures against these emerging threats.

Leveraging GenAI for defense is an empowering journey we embark on together. You'll learn how to enhance threat detection, automate response strategies, and use GenAI for realistic incident simulation. By studying real-world case studies, you'll see the transformative impact GenAI can have on enhancing cybersecurity posture, providing you with practical insights to apply in your endeavors.

Ethical and legal considerations are interwoven throughout the coursework, ensuring you're well-versed in navigating the complexities of deploying GenAI solutions responsibly. From data privacy concerns to formulating policies that govern GenAI utilization in cybersecurity, this course addresses the critical legal and ethical dimensions that underpin all technological deployments.

In advancing through the program, you'll tackle advanced topics such as the role of quantum computing and the future of encryption in the age of GenAI. This not only broadens your understanding of cybersecurity but also equips you with knowledge about the horizon of cyber defense technologies.

Practical application is a key emphasis. Sections on AI-driven threat intelligence, vulnerability management, and cybersecurity operations are interspersed with project-based learning opportunities. Whether optimizing SOC operations with GenAI or automating patch management, you'll engage in hands-on projects that refine your skills and enhance your portfolio.

What sets our course apart is not only the depth and breadth of content but also the unique blend of theoretical knowledge and practical application. Unlike any other course available, we take you beyond the surface, offering insights into securing high-risk AI systems, developing AI-powered security training programs, and leveraging GenAI in digital forensics. Each module is a step on a ladder, elevating your expertise and preparing you for the challenges of tomorrow.

As the demand for skilled cybersecurity professionals surges, this course stands as a pivotal stepping stone in your career. Whether you're a budding professional eager to make your mark in cybersecurity or an experienced practitioner looking to expand your arsenal with GenAI knowledge, this course is designed to cater to a wide audience.

By the end of this comprehensive journey, you'll not only possess a thorough understanding of GenAI's impact on cybersecurity but also have a portfolio of projects that attest to your newly acquired capabilities. This not only enhances your employability but also prepares you to contribute meaningfully to the cybersecurity community.

In a world where cyber threats loom larger by the day, equipping yourself with the knowledge and skills to wield GenAI in defense is more than a professional advantage - it's a necessity.

Learning objectives

- Define the role of GenAI in cybersecurity.
- Explain the evolution of cyber threats with GenAI.
- Compare traditional vs. GenAI-enhanced cyber threats.
- Evaluate the ethical implications of GenAI in cybersecurity.
- Identify AI-specific threats such as deepfakes and AI-phishing.
- Describe the concept of prompt injection attacks.
- Analyze the development process of AI-powered malware.
- Explain the impact of data poisoning on AI models.
- Apply secure prompt engineering principles.
- Detect and mitigate deepfakes using strategic approaches.
- Prevent AI-enhanced phishing attacks through innovative methods.
- Implement adversarial testing in AI systems for better security.
- Use GenAI for realistic incident simulation in cybersecurity practice.
- Automate response strategies to cybersecurity incidents with AI.
- Assess ethical and legal considerations in deploying GenAI.
- Develop secure AI models following best practices.
- Protect AI intellectual property and secure AI coding practices.
- Explore the impact of quantum computing on GenAI security.
- Utilize GenAI for enhanced cyber threat intelligence.
- Apply AI-driven techniques for effective vulnerability management.

Topics covered

The course is split into the following sections:

Section 1: Introduction to Generative AI in Cybersecurity

- Understanding Generative AI and Its Impact on Cybersecurity
- The Evolution of Cyber Threats with GenAI
- Generative AI: Friend or Foe in Cyber Defence
- Comparative Analysis: Traditional vs GenAI-Enhanced Cyber Threats

- The Ethical Landscape of GenAI in Cybersecurity

Section 2: AI-Specific Threats and Vulnerabilities

- Introduction to AI-Specific Threats: Deepfakes, AI-Phishing
- Understanding Prompt Injection Attacks
- The Mechanics of AI-Powered Malware Development
- Data Poisoning and Its Impact on AI Models
- Case Studies: Major AI-Specific Cyberattacks

Section 3: Defensive Strategies against GenAI Threats

- Principles of Secure Prompt Engineering
- Strategies for Detecting and Mitigating Deepfakes
- Preventing AI-Enhanced Phishing Attacks
- Data Hygiene Practices for AI Security
- Implementing Adversarial Testing in AI Systems

Section 4: Leveraging GenAI for Cybersecurity Defense

- GenAI in Threat Detection and Analysis
- Using GenAI for Realistic Incident Simulation
- Automating Response Strategies with AI
- Enhancing Cybersecurity Posture with GenAI
- Case Studies: Successful GenAI Implementation in Cyber Defense

Section 5: Ethical and Legal Considerations in GenAI

- Ethical Deployment of GenAI in Cybersecurity
- Navigating the Legal Landscape of GenAI
- Data Privacy Concerns with GenAI Technologies
- Building Trust in GenAI Cybersecurity Solutions
- Framework for Ethical Generative AI Use in Cybersecurity

Section 6: Secure Development of AI Systems

- Best Practices in Secure AI Model Development
- Mitigating Risks in AI Supply Chain
- Protecting AI Intellectual Property
- Secure Coding Practices for Generative AI
- Case Studies: Securing High-Risk AI Systems

Section 7: Advanced Topics in GenAI and Cybersecurity

- Quantum Computing and Its Impact on GenAI Security
- The Future of Encryption in the Age of Generative AI
- Advanced Persistent Threats (APTs) and GenAI
- AI-driven Security Orchestration, Automation, and Response (SOAR)
- Future-Proofing Cybersecurity for GenAI Advances

Section 8: Innovations in AI-Driven Threat Intelligence

- The Role of GenAI in Cyber Threat Intelligence
- Automating Threat Intelligence with Generative AI

- Enhancing Predictive Capabilities with AI
- Integrating GenAI with Existing Threat Intelligence Platforms
- Real-World Applications of AI-Driven Threat Intelligence

Section 9: GenAI in Vulnerability Management

- AI-Powered Vulnerability Identification
- Automating Patch Management with GenAI
- Risk Assessment and Prioritization with AI
- Enhancing Vulnerability Management through GenAI
- Case Studies on AI-Driven Vulnerability Management

Section 10: Cybersecurity Operations and GenAI

- Optimizing SOC Operations with Generative AI
- AI in Incident Detection and Response
- Using GenAI for Security Log Analysis
- Streamlining Compliance using AI Technologies
- The Role of AI in Continuous Security Monitoring

Section 11: Training and Awareness with GenAI

- Developing AI-Powered Security Training Programs
- Using GenAI to Simulate Phishing Attacks for Training
- Gamifying Cybersecurity Training with AI
- Measuring Training Effectiveness with AI Analytics
- Case Studies: GenAI in Security Awareness Campaigns

Section 12: Privacy Enhancements through GenAI

- Using GenAI to Strengthen Data Privacy
- AI-Driven Anonymization Techniques
- Generative AI in GDPR Compliance
- Balancing Data Utility and Privacy with AI
- Privacy by Design in Generative AI Applications

Section 13: AI-Driven Digital Forensics

- The Role of GenAI in Digital Forensics
- Automating Evidence Collection with AI
- Enhancing Analytical Capabilities in Forensics with AI
- GenAI in Fraud Detection and Investigation
- Case Studies: AI-Driven Successes in Digital Forensics

Section 14: Cybersecurity Policy and GenAI

- Formulating Cybersecurity Policies for GenAI Utilization
- Global Regulations Affecting GenAI in Cybersecurity
- AI Ethics and Governance in Cybersecurity
- Collaborating with International Bodies on GenAI Security
- Strategic Planning for GenAI in National Security

Section 15: The Socioeconomic Impact of GenAI on Cybersecurity

- Analyzing the Job Market Evolution with GenAI in Cybersecurity
- Economic Considerations of GenAI in Security
- Public Perception and Trust in GenAI-Enhanced Cybersecurity
- The Influence of GenAI on Cyber Crime Economics
- Preparing Cybersecurity Workforces for the GenAI Era

Section 16: GenAI and Identity Management

- Advancements in AI-Powered Biometric Systems
- GenAI in Behavioral Biometrics for Authentication
- Challenges in AI-Driven Identity Verification
- Using GenAI to Combat Identity Theft
- Real-World Implementations of GenAI in Identity Management

Section 17: Future Technologies in GenAI Security

- Exploring the Intersection of IoT and GenAI in Cybersecurity
- The Role of 5G in Enabling AI-Enhanced Cyber Threats
- Nanotechnology and GenAI in Cybersecurity
- Anticipating the Next Wave of GenAI Technologies
- Preparing for Unknown Future GenAI Threats

Section 18: GenAI in Cyber Incident Response

- AI-Powered Crisis Management and Recovery
- Using Generative AI for Faster Root Cause Analysis
- Automated Remediation with AI
- Bridging the Gap Between Incident Response and GenAI
- Success Stories in AI-Enhanced Cyber Response

Section 19: Benchmarking GenAI Cybersecurity Solutions

- Evaluating GenAI Cybersecurity Tools and Platforms
- Best Practices for Testing GenAI Security Solutions
- The Role of Open Source in Advancing GenAI Security
- Establishing Industry Standards for GenAI in Cybersecurity
- Leveraging Competitions and Challenges to Improve AI Sec Solutions

Section 20: Emerging Threats and Future Directions

- Speculative Threats in the Future of GenAI and Cybersecurity
- Adapting to the Evolving GenAI Threat Landscape
- Emerging Trends in Generative AI and Cyber Defense
- Preparing for the Next Decade of Cybersecurity with GenAI
- Closing Thoughts: The Never-Ending Cycle of Innovation in Cybersecurity

Course duration

This course may take up to 5 hours to be completed. However, actual study time differs as each learner uses their own training pace.

Course pre-requisites

There are no requirements or pre-requisites for this course, but the items listed below are a guide to useful background knowledge which will increase the value and benefits of this course:

- Basic understanding of cybersecurity principles and practices.
- Familiarity with AI and machine learning concepts.
- Experience with programming or scripting languages (Python preferred).

The course is addressed to:

- Cybersecurity professionals seeking to update their knowledge on the latest AI threats and defense strategies.
- IT managers responsible for safeguarding their organizations' digital assets against advanced cyber threats.
- AI researchers focusing on cybersecurity applications and looking to understand the latest trends and threats in the field.
- Software developers working on cybersecurity solutions who need to incorporate generative AI capabilities into their products.
- Cybersecurity policy makers and strategists interested in the ethical, legal, and socioeconomic implications of utilizing GenAI in defense mechanisms.
- Students and academicians pursuing studies in cybersecurity, AI, or a related field, who wish to gain a comprehensive understanding of how generative AI impacts cybersecurity.

Training Method

The course is offered fully online using a self-paced approach. The learning units consist of videos. Learners may start, stop and resume their training at any time.

At the end of the course, participants take a Quiz to complete the course and earn a Certificate of Completion once the quiz has been passed successfully.

Registration and Access

To register to this course, click on the *Take this course* button to pay online and receive your access instantly. If you are purchasing this course on behalf of others, please be advised that you will need to create or use their personal profile before finalizing your payment.

Access to the course is valid for 90 days.

If you wish to receive an invoice instead of paying online, please Contact us by email. Talk to us for our special Corporate Group rates.

Instructor

Peter Alkema is a highly accomplished Business and IT leader specialising in large scale technology delivery and digital transformation strategy implementation for leading financial services business. A proven record in driving the full development lifecycle at all levels across large and complex banking enterprises ensures a deep understanding of the challenges, opportunities and pathways to success for digital transformation in banking. By utilising innovation, awareness, and knowledge, able to drive high-level business strategy formulation, product and platform development, and change management.

Teaching 500k online students about Data Science, Machine Learning, Digital Transformation, Business, Academic, Self Development and Technology skills.

Business & IT leader specialising in large scale technology delivery, digital transformation and Agile software engineering (PhD). 24 years in the banking industry; 10 years consulting (Accenture) and 14 years working in banking (Absa & FNB).

Won the ITWeb Gartner Visionary CIO Of The Year in 2016 & featured on CNBC Africa. Founded and led the largest banking hackathon in South Africa which was featured on Harvard Business Review.

Professional skills: Digital Transformation, Technology, Agile, ERP, Programme Management, Innovation, Thought Leadership, Communication, Process Engineering, Online Training.