ChatGPT & Generative AI for Security Engineers & Analysts

Empowering Cybersecurity with Artificial Intelligence

Experience

Wednesday June 12th, 2024
In-Person at Adobe's Office in Bucharest Romania
Anchor Plaza, Bd. Timișoara 26Z, București 061331, Romania

Course Overview

The world of cybersecurity is evolving rapidly, and artificial intelligence (AI) is at the forefront of this transformation. Large Language Models (LLMs) like ChatGPT and generative AI systems are revolutionizing how security engineers and analysts approach their work. This intensive course will equip you with the knowledge and skills to harness the power of LLMs and generative AI, streamlining your tasks, enhancing your threat detection capabilities, and ultimately making you a more effective cybersecurity professional.

In this course you will learn:

- Leveraging SaaS LLMs like ChatGPT, Claude, Gemini, Perplexity AI, LLama, Copilot, and Copilot for Security for cybersecurity tasks
- Utilizing SaaS image generation tools MidJourney and DALL·E 3 for data visualization and attack scenario modeling
- Crafting effective prompts using libraries like Anthropic Prompt Library and PromptHero
- Running local LLMs such as Ollama, Open WebUI, Llama 3, Dolphin-Llama3, Hugging Face, and ChatRTX for sensitive LLM tasks
- Automating security workflows with LangChain Agents and OpenAI Assistants/GPTs
- Applying LLMs for threat intelligence gathering, malware analysis, vulnerability research, and incident response
- Generating clear technical reports, documentation, and communications assisted by AI

Key Takeaways

The primary takeaways from the training course include:

* **Practical Skills:** Gain hands-on experience using LLMs and generative AI tools like ChatGPT, Claude, MidJourney, and more to solve real-world cybersecurity challenges.
* **Prompt Engineering Mastery:** Learn how to craft effective prompts to get the most accurate and relevant responses from AI systems, maximizing their value for security tasks.
* **Threat Intelligence Enhancement:** Discover how to leverage AI to analyze threat data, identify patterns, and generate actionable insights to proactively defend against attacks.
* **Security Automation:** Explore the potential of AI agents and automation to streamline repetitive tasks, freeing up your time for more strategic security initiatives.
* **AI-Powered Creativity:** Utilize generative AI to visualize potential threats, create realistic simulations, and develop innovative security solutions.
* **Staying Ahead of the Curve:** Understand the evolving landscape of LLMs and generative AI in cybersecurity, ensuring you're equipped with the latest knowledge and tools.
* **Ethical Considerations:** Grasp the ethical implications of using AI in security, including biases, potential misuse, and responsible AI practices.

Additional takeaways from the training course include:

* Mastering prompt engineering techniques to elicit precise and actionable outputs from LLMs for cybersecurity tasks, enhancing efficiency and accuracy in threat analysis, incident response, and security research.
* Leveraging SaaS AI platforms like ChatGPT, Claude, and Copilot for Security to augment threat intelligence gathering, malware analysis, and vulnerability assessments, enabling faster identification and mitigation of security risks.
* Utilizing local LLMs and image generation tools to maintain data privacy and customize AI models for organization-specific security needs, such as generating network diagrams, attack graphs, and visualizing security data.
* Automating security workflows and building custom security chatbots/copilots using tools like LangChain Agents and OpenAI Assistants/GPTs, streamlining tasks like phishing email analysis, log analysis, and alert triage.
* Enhancing threat hunting capabilities by leveraging AI-powered pattern recognition and anomaly detection, enabling proactive identification of sophisticated threats and reducing mean-time-to-detect (MTTD).
* Generating clear, concise, and persuasive technical reports, documentation, and communications with the assistance of LLMs, improving collaboration and buy-in from stakeholders.
* Gaining hands-on experience with a wide range of SaaS and local AI tools, equipping attendees with the practical skills to integrate cutting-edge AI capabilities into their organization's security operations.

* Understanding the current capabilities and limitations of LLMs and generative AI in cybersecurity, and learning strategies to mitigate potential risks such as data leakage, bias, and adversarial attacks.

By the end of the course, security engineers and analysts will have a comprehensive understanding of how to harness the power of LLMs and generative AI to enhance their organization's security posture, streamline workflows, and stay ahead of evolving cyber threats.

Course Outline

Module 1: Fundamentals of LLMs and Generative AI
* Introduction to Large Language Models (LLMs)
* How LLMs and Generative AI work under the hood
* Key terms and concepts (e.g., prompts, tokens, fine-tuning)
* Applications of LLMs and Generative AI in cybersecurity

Module 2: SaaS LLMs: Supercharging Your Security Workflow
* **ChatGPT & OpenAI:** Conversational AI for security tasks
* **Claude & Anthropic:** Advanced reasoning and ethical AI
* **Gemini & Google:** Google's powerful LLM for research and security
* **Perplexity AI:** Conversational search engine for security intelligence
* **LLama & Meta:** Open-source LLMs for research and development
* **Copilot & Microsoft:** AI-powered code generation and security analysis
* **Copilot for Security & Microsoft:** Specialized AI for security tasks

Module 3: SaaS Image Generation: Visualizing Threats
* **MidJourney:** AI-generated images for threat modeling and simulation
* **DALL·E 3:** OpenAI's advanced image generation for creative security uses

Module 4: Mastering Prompts: The Key to Effective AI Interaction
* **Prompt Library & Anthropic:** A collection of effective prompts
* **Prompt Hero:** Resources and tools for crafting powerful prompts
* **Best Practices** for prompt engineering in a security context

Module 5: Local LLMs: Taking Control of Your AI Environment
* **Ollama:** A user-friendly platform for running local LLMs
* **Open WebUI:** A customizable interface for interacting with LLMs
* **Llama 3 & Meta:** Fine-tune and run this powerful LLM locally
* **Dolphin-Llama3:** Optimized Llama 3 for lower resource requirements
* **Hugging Face:** A vast library of LLMs and tools
* **ChatRTX:**NVIDIA's hardware-accelerated LLM for RTX GPUs

Module 6: Local Image Generation: On-Premise AI-Powered Visualization
* **Stable Diffusion:** Generate and customize images with this powerful tool

Module 7: Agents & Automation: Streamlining Security with AI
* **LangChain Agents:** Build custom AI agents for security automation
* **Assistants & OpenAI:** Design AI assistants for specific security tasks
* **GPTs & OpenAI:** Create custom GPTs for your security needs

Module 8: Hands-On Labs and Practical Applications
* Threat hunting with ChatGPT
* Vulnerability assessment with Claude
* Security report generation with Gemini
* Building custom security tools with LLMs
* Integrating LLMs into your existing security workflow

Who Should Attend

This course assumes the student already has some basic cybersecurity knowledge and would like to learn more about how to apply LLMs and Generative AI systems to existing cybersecurity challenges. This includes:

* Security Engineers
* Security Analysts
* Threat Intelligence Professionals
* SOC (Security Operations Center) Personnel
* Cybersecurity Managers and Leaders
* Anyone interested in leveraging AI for cybersecurity

Audience Skill Level

Beginner to Intermediate

Student Requirements

Students should be comfortable with:
- Using Linux and SSH
- Basic networking concepts and services (e.g. TCP/IP, DNS, DHCP, etc…)

Students will benefit from having:
- Some Python scripting knowledge is recommended, but not required.
- Some basic SaaS LLM experience (e.g. ChatGPT) is recommended, but not required.

What Students Should Bring

Students will need to bring to the class:
* A laptop with admin access to install software (e.g. PuTTY, Chrome, etc...).
* The Laptop needs to be able to join a wireless network and access cloud services hosted in common Cloud Service Providers (e.g. AWS, Azure, & GCP).

What Students Will Be Provided With

Students will need to bring to the class:
* A copy of the course slides (100+ slides)
* Access to our Discord server, to continue the conversation after the event!
* Free access to our Cloud (AWS/Azure/GCP) student training environment during the course.

Trainer

Bryce Kunz (@TweekFawkes) loves researching red team techniques for bleeding edge services (e.g. LLMs, Generative AI, Cloud, etc.). Previously Chief Strategy Officer (CSO) at Stage 2 Security // UltraViolet Cyber, supported the NSA (network exploitation & vulnerability research), Adobe (built a red teaming program for cloud services), and DHS (incident response). Bryce holds numerous certifications (e.g. OSCP, CISSP, ...), has spoken at various security conferences (i.e. BlackHat, DerbyCon, BSidesLV, etc...) and teaches classes at BlackHat (e.g. AWS & Azure Exploitation).

Benefits of Attending

* Gain a competitive edge in the cybersecurity landscape
* Streamline security tasks and workflows
* Improve threat detection and response capabilities
* Develop valuable skills in AI and machine learning
* Network with other cybersecurity professionals