# Additional Learning Resources

## Recommended Reading

* **The DevSecOps Handbook** by Gene Kim, Patrick Debois, John Willis, and Jez Humble  
  Comprehensive strategies for integrating security into modern software delivery workflows.
* **Machine Learning and Security** by Clarence Chio and David Freeman  
  Practical insights into adversarial AI, anomaly detection, and the intersection of machine learning and security.
* **OWASP Top 10**  
  The industry-standard list of the most critical web application security risks.  
  <https://owasp.org/www-project-top-ten/>
* **OWASP Proactive Controls**  
  A list of security techniques for developers to proactively prevent vulnerabilities.  
  <https://owasp.org/www-project-proactive-controls/>
* **Microsoft Security Blog**  
  Updates and insights on DevSecOps, GitHub Copilot, Defender, and more.  
  <https://www.microsoft.com/security/blog/>
* **Google AI Security Papers**  
  Whitepapers and research on AI security, including large language models and red teaming.  
  <https://ai.google/responsibility/safety/>
* **OpenAI Blog**  
  Updates on GPT models, AI safety, and responsible AI practices.  
  <https://openai.com/news/>
* **OWASP GenAI Blog**  
  Community-driven updates on tools, practices, and events.  
  [https://genai.owasp.org/blog/](https://owasp.org/blog/)

## Tools and Platforms to Experiment With

* **OWASP ZAP**  
  Open-source dynamic application security testing (DAST) tool.  
  <https://www.zaproxy.org/>
* **Trivy**  
  Open-source vulnerability scanner for containers, dependencies, and Infrastructure as Code.  
  <https://aquasecurity.github.io/trivy/>
* **Semgrep**  
  Fast, developer-friendly static analysis tool with customizable rules.  
  <https://semgrep.dev/>
* **GitHub Copilot**  
  AI-powered code suggestion and security fix tool for IDEs.  
  <https://github.com/features/copilot>
* **Snyk**  
  Scans open-source libraries, containers, and IaC for known vulnerabilities.  
  <https://snyk.io/>
* **CodeQL**  
  Semantic code analysis engine used by GitHub Advanced Security.  
  <https://codeql.github.com/>
* **ChatGPT**  
  Use for generating security-focused test cases, summarizing scan results, and writing policy-as-code.  
  <https://chat.openai.com/>

## Learning Platforms and Certifications

* **EC-Council**
  + Certified DevSecOps Engineer (ECDE): <https://www.eccouncil.org/programs/certified-devsecops-engineer-ecde/>
  + Certified Ethical Hacker (CEH): <https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>
* **Linux Foundation – Implementing DevSecOps**  
  https://training.linuxfoundation.org/training/implementing-devsecops-lfs262/
* **CompTIA Security+**  
  <https://www.comptia.org/certifications/security>
* **AWS Certified Security – Specialty**  
  <https://aws.amazon.com/certification/certified-security-specialty/>
* **Google Cloud Security Engineer**  
  <https://cloud.google.com/certification/cloud-security-engineer>
* **Certified Kubernetes Security Specialist (CKS)**  
  <https://training.linuxfoundation.org/certification/certified-kubernetes-security-specialist-cks/>

## Communities and Events

* [**Cloud**](http://DevSecOps.org) **Security Alliance Slack**  
  [#devsecops-working-group](https://devsecops.org/slack/) channel
* **Reddit Communities**
  + r/devsecops: <https://www.reddit.com/r/devsecops/>
  + r/cybersecurity: <https://www.reddit.com/r/cybersecurity/>
  + r/MachineLearning: <https://www.reddit.com/r/MachineLearning/>
* **Discord Servers**
  + OpenAI: <https://discord.gg/openai>
  + Hugging Face: <https://discord.gg/hugging-face-879548962464493619>
* **Events**
  + DEF CON: <https://defcon.org/>
  + Black Hat: <https://www.blackhat.com/>
  + DevSecCon: <https://www.devseccon.com/>
  + GitHub Universe: <https://githubuniverse.com/>

## Personal Projects and Practice

* Build a CI/CD pipeline that includes Trivy or Semgrep; use ChatGPT to explain scan results.
* Use ChatGPT to help write a threat model for a mock application or personal project.
* Start a GitHub repository to document experiments and lessons learned.
* Write a blog post about your learning journey to clarify and share your understanding.

***Note:*** *All links and resources have been validated as accurate and up to date as of April 2025.*

⁂