Agentic AI in AppSec

A (quick) Primer

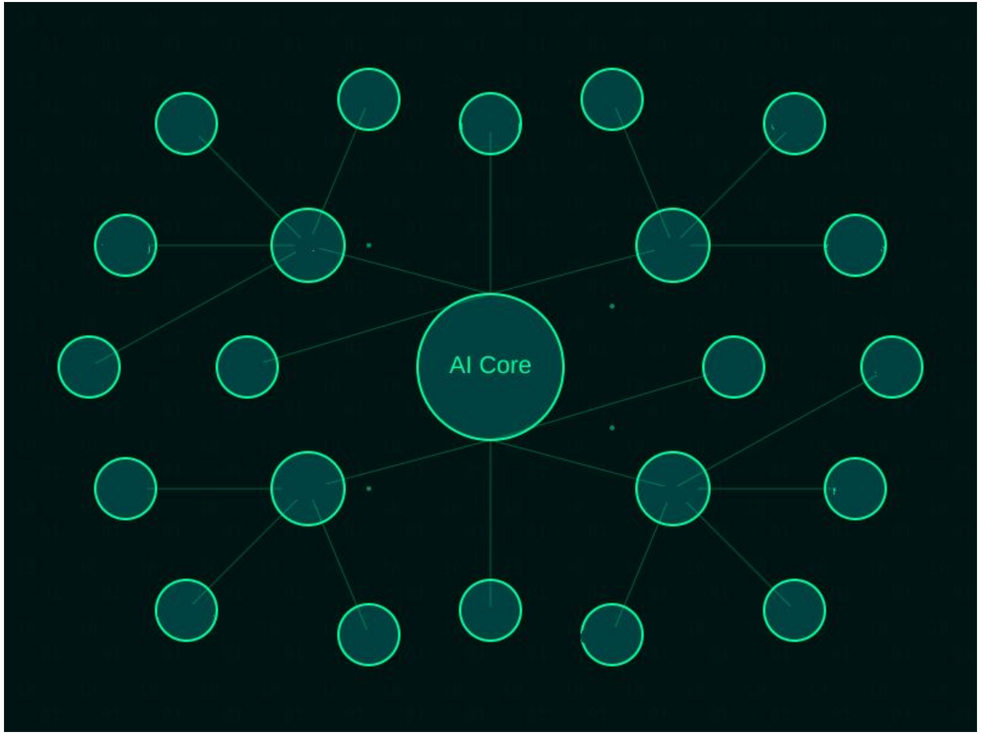
Left TODO

AI + External Tools

Capabilities

=

Use Cases

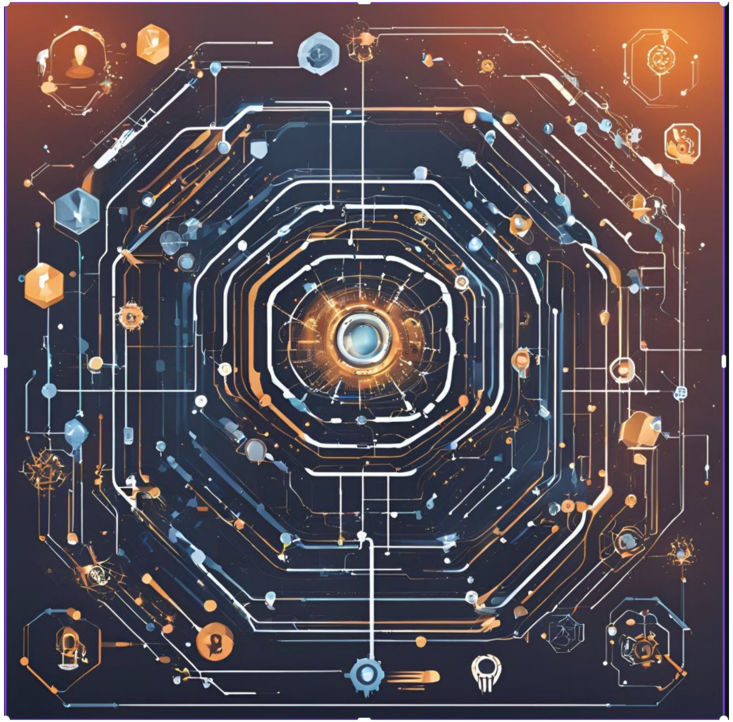


Use Cases

- Knowledge Augmentation & Training Humans
- Marketing
- Customer Service
- Continuous regulatory compliance
- Bare Metal Command and Control

Product Security Use Cases

- Automated and accurate tooling configuration



Product Security Use Cases

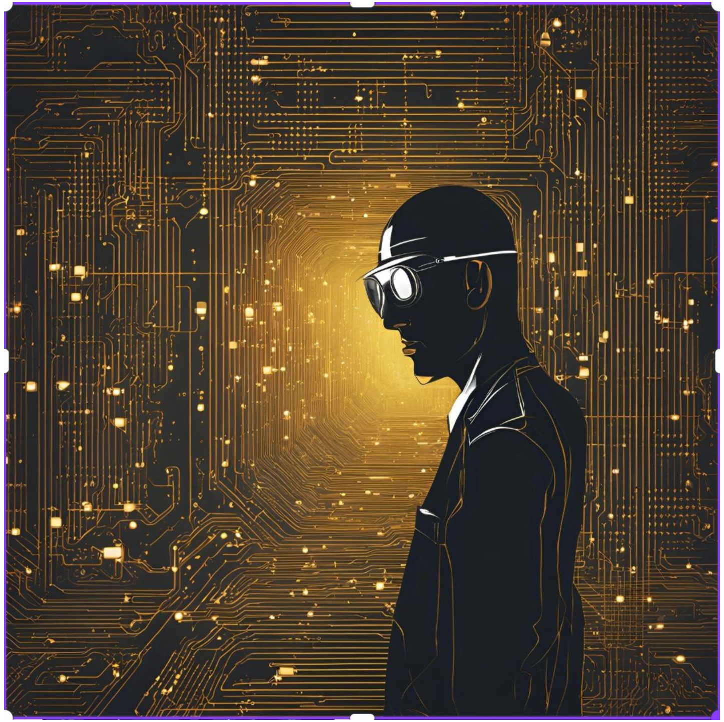
- Product Security workflow creation

Product Security Use Cases

- Remediation (with testing)

Product Security Use Cases

- False Positive detection
  - (with voting and consensus)

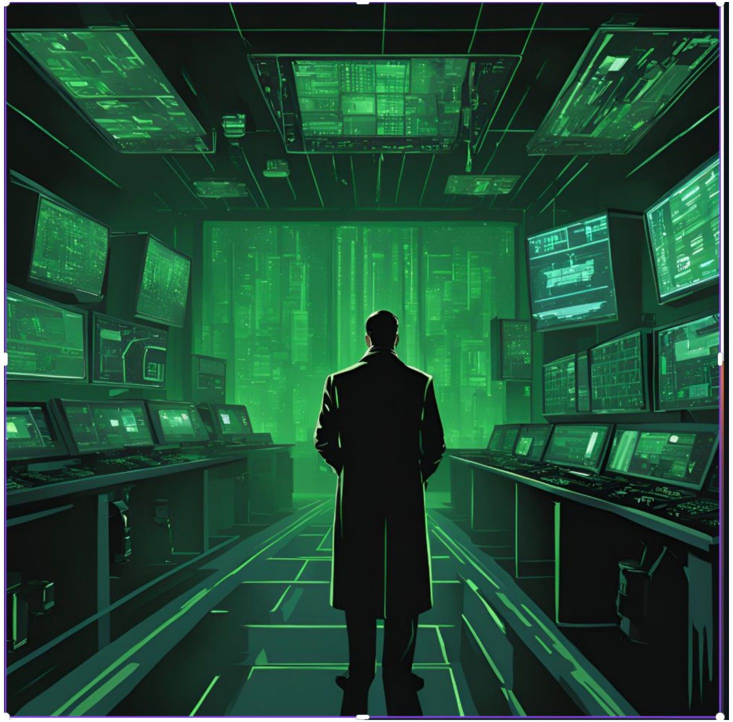


Product Security Use Cases

- Automated, Accurate Threat Modeling

Security Considerations

- Accuracy decreases with the number of tools
- Permissions
- Human in the loop
- Funds denial
- Old-Time-y injections, do not assume the LLM will give you clean arguments



Resources

OWASP AI Exchange

https://owaspai.org/

Chip Huyen’s post on Agents

https://huyenchip.com//2025/01/07/agents.html

Anthropic’s post on Agents

https://www.anthropic.com/research/building-effective-agents

Frameworks

Langgraph

https://langchain-ai.github.io/langgraph/#key-features

Autogpt

https://docs.agpt.co/

Burr

https://github.com/dagworks-inc/burr

Thank you!

SMITHY