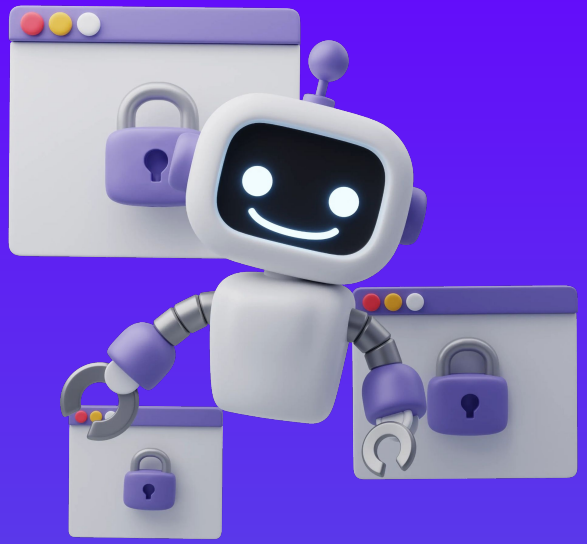
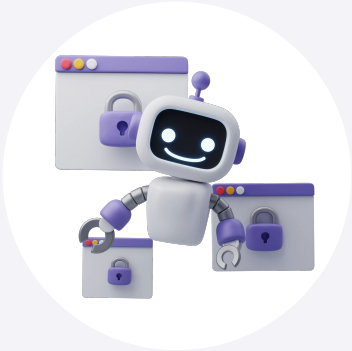


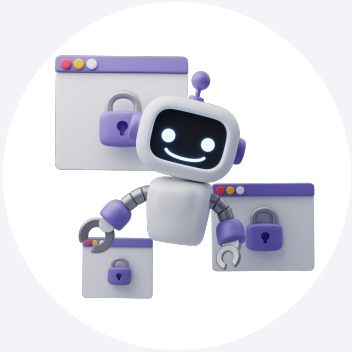
AppSec Robots Masterclass

Last updated: March 2026



Security work today is fragmented across tools and stages with threat modeling, code analysis, runtime testing, and infrastructure audits all running as separate efforts. Each step depends on manual execution, which slows teams down and makes it harder to maintain consistency across environments.

This course focuses on building systems that connect and run these workflows end-to-end. Instead of treating each activity in isolation, the training walks through how to design agents that handle the full security lifecycle, from understanding architecture and code to testing applications and auditing infrastructure, using real inputs and practical integrations.



Day 1: Building Core AppSec Systems

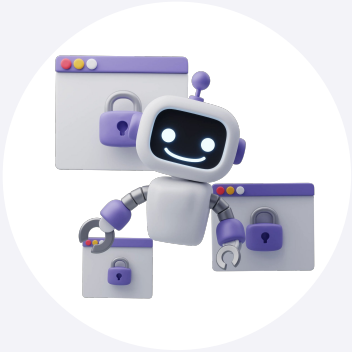
Section 1: Foundations of Security Agents

What you'll learn

- How agents move from prompts to systems that take action
- How reasoning, tool usage, and memory enable multi-step workflows
- Where agents fit into real security operations

Hands-On

- Build agents that call tools and execute actions through APIs
- Implement reasoning workflows for complex security tasks
- Add memory to retain context across runs



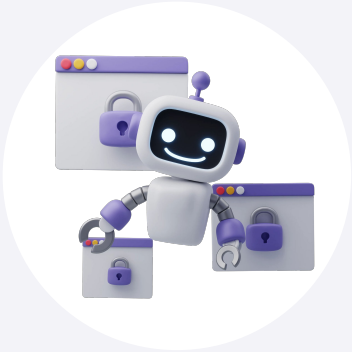
Section 2: Connecting Agents to Data and Tools

What you'll learn

- How agents use real data instead of generating generic outputs
- How to integrate agents with tools and systems
- Why grounding and context matter in security workflows

Hands-On

- Implement RAG to connect agents to documents and code
- Set up MCP servers for tool and API integration
- Build data pipelines using vector databases



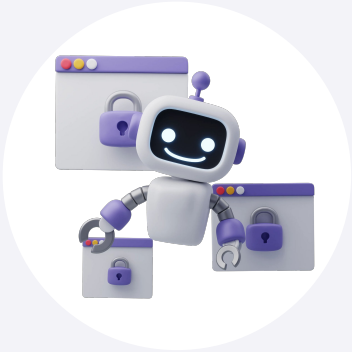
Section 3: Threat Modeling Agents (Documents + Architecture)

What you'll learn

- How to turn architecture and documentation into threat models
- How to ground analysis in real system context
- How to map threats to standard frameworks

Hands-On

- Build agents that ingest architecture docs and diagrams
- Generate threat vectors mapped to STRIDE and MITRE ATT&CK
- Create research agents to pull in current threat intelligence
- Generate reports for developers, security teams, and leadership



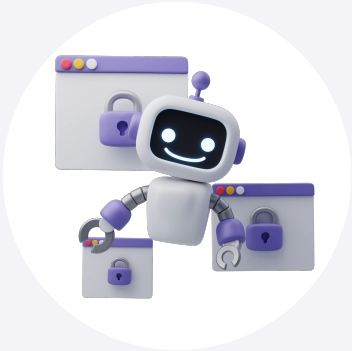
Section 4: Code-Driven Threat Modeling Agents

What you'll learn

- Why documentation alone is not enough for threat modeling
- How to extract security insights directly from code
- How to map real data flows and attack surfaces

Hands-On

- Build agents that scan codebases and identify abstractions
- Map relationships, trust boundaries, and data flows
- Generate diagrams and attack surface maps
- Feed outputs into threat modeling systems



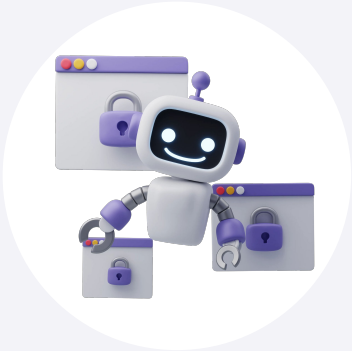
Section 5: SAST Agents (Static Analysis Systems)

What you'll learn

- How static analysis fits into automated workflows
- How to trace real data flows instead of pattern matching
- How to reduce noise and prioritize real vulnerabilities

Hands-On

- Build reconnaissance agents to identify stack and entry points
- Implement taint analysis for source-to-sink tracking
- Classify vulnerabilities and assign severity
- Generate structured reports with remediation guidance



Day 2: Runtime, Infrastructure, and Scaled Workflows

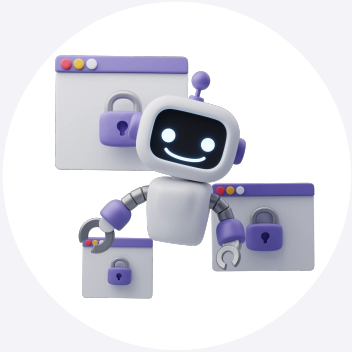
Section 6: DAST Agents (Runtime Testing Systems)

What you'll learn

- How to validate vulnerabilities at runtime
- How agents explore applications and execute attacks
- How to reduce manual testing effort

Hands-On

- Build agents that crawl applications and map attack surfaces
- Generate and execute context-aware attack payloads
- Validate vulnerabilities through response analysis
- Generate reports with confirmed findings



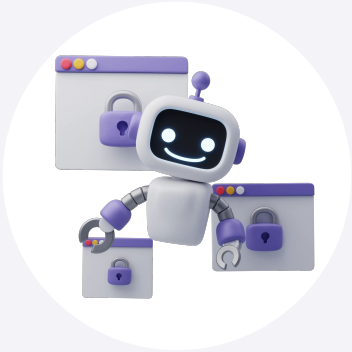
Section 7: Kubernetes Security Agents

What you'll learn

- How to audit Kubernetes environments at scale
- Where misconfigurations and risks exist
- How to continuously monitor cluster security

Hands-On

- Connect agents to Kubernetes using MCP
- Analyze RBAC configurations and privilege risks
- Evaluate network policies and workload exposure
- Detect insecure container and secret configurations



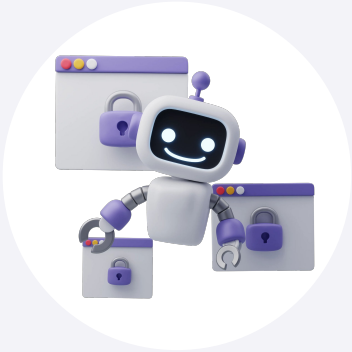
Section 8: Cloud Security Agents (AWS)

What you'll learn

- How to audit cloud environments consistently
- How to identify identity and infrastructure risks
- How to enforce security checks across accounts

Hands-On

- Build agents to audit IAM users and roles
- Detect risky permissions and escalation paths
- Analyze S3 exposure and encryption gaps
- Evaluate security group configurations



Section 9: Multi-Agent Workflows and System Design

What you'll learn

- How to connect agents into coordinated systems
- How to design workflows across the security lifecycle
- How to move from tools to systems

Hands-On

- Design multi-agent workflows across security stages
- Connect agents to share context and outputs
- Build systems that run continuously
- Structure outputs for integration into existing processes