**Security Orchestration & Risk Platform  
Extended Development Tables**

Backlog Breakdown • Timelines • Responsibilities • Dependencies

*August 22, 2025*

# 1. Backlog Breakdown by Module

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Module | Phase | Tech Stack | Owner(s) | Estimated Duration |
| Core Engine & Dashboard | MVP | Spring Boot + React | Tech Lead + 2 Devs | 4 weeks |
| SAST/SCA Module | MVP | Semgrep, Dependency-Check | 2 Devs + Security Eng. | 3 weeks |
| IaC Module | MVP | Checkov, Trivy Config | 2 Devs + Security Eng. | 3 weeks |
| CI/CD Security | MVP | TruffleHog, Semgrep rules | 2 Devs + Security Eng. | 2 weeks |
| Integrations | MVP | Jira, Slack connectors | 1 Dev | 2 weeks |
| Risk Scoring v1 | MVP | Severity × Exposure | Tech Lead | 1 week |
| SBOM & Image Scanning | Phase 2 | Syft, Grype, Trivy Images | 2 Devs | 3 weeks |
| Policy-as-Code Packs | Phase 2 | OPA/Rego | 1 Dev + Security Eng. | 2 weeks |
| Graph & Attack Paths | Phase 2 | Graph DB, Neo4j/Postgres | 2 Devs | 3 weeks |
| CSPM/KSPM | Phase 3 | kube-bench, Polaris | 2 Devs + Cloud Eng. | 4 weeks |
| Admission Control & Autofix | Phase 3 | OPA Gatekeeper/Kyverno | 2 Devs | 3 weeks |
| Provenance & Signing | Phase 3 | in-toto, cosign, SLSA | 1 Dev + Security Eng. | 3 weeks |
| DAST & API Security | Phase 4 | OWASP ZAP, OpenAPI linting | 2 Devs | 3 weeks |
| Runtime Security | Phase 4 | Falco | 1 Dev + Ops Eng. | 3 weeks |

# 2. Responsibilities by Role

|  |  |
| --- | --- |
| Role | Responsibilities |
| Product Owner | Define backlog, prioritize features, ensure compliance requirements are captured. |
| Tech Lead / Architect | Oversee architecture, API contracts, design reviews, ensure cross-cutting concerns. |
| Developers | Implement backend (Spring Boot) and frontend (React), integrate scanners, build APIs. |
| Security Engineers | Tune scanners, write custom Semgrep/OPA rules, ensure exploitability context. |
| DevOps / SRE | Build IaC, manage CI/CD, observability, performance scaling, DR/BCP. |
| QA / Test Automation | Regression, security testing, validate findings lifecycle, acceptance tests. |

# 3. Dependencies

|  |  |
| --- | --- |
| Module | Dependency |
| Core Engine | Must be implemented before any scanner modules; provides API contracts. |
| Dashboard | Depends on Core Engine APIs for data visualization. |
| SAST/SCA | Requires repo ingestion pipeline from Core Engine. |
| IaC Module | Depends on repo ingestion + object store for IaC files. |
| CI/CD Security | Depends on connectors to GitHub/GitLab/Jenkins. |
| SBOM/Image Scanning | Requires artifact registry access + CI/CD integration. |
| Policy-as-Code | Requires Policy Engine base in Core Engine. |
| Graph & Attack Paths | Requires asset + findings entities in DB first. |
| CSPM/KSPM | Requires cloud IAM read-only roles + connectors. |
| Admission Control | Requires IaC + K8s baseline policies. |
| Provenance/Signing | Requires CI/CD pipelines stable for signing attestations. |

# 4. Development Timeline (Gantt Chart)

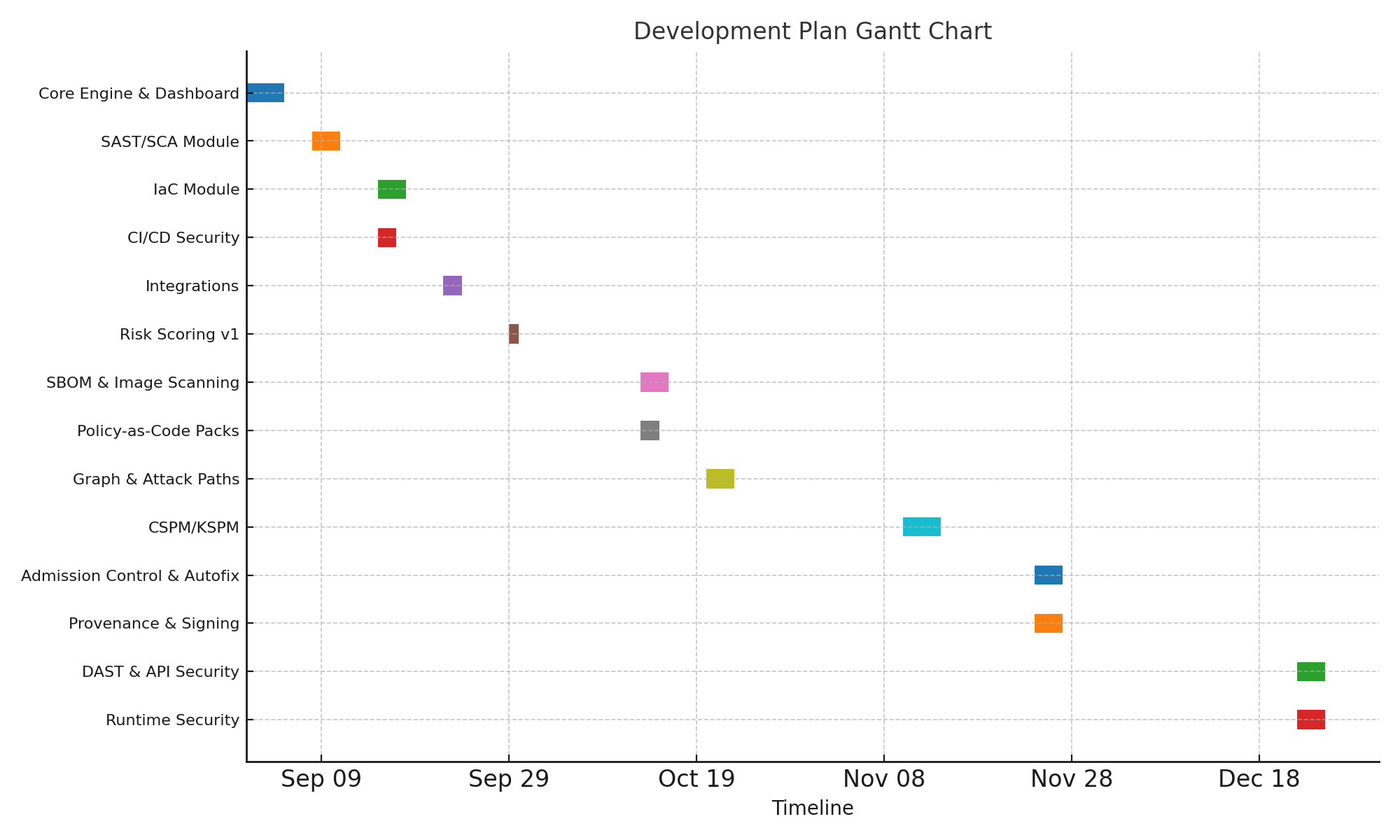


Figure: Gantt-style visualization of module development plan.