OWASP | GenAI SECURITY PROJECT

TOP 10 FOR LLM AND GENERATIVE AI

AI SECURITY SOLUTIONS INITIATIVE

Q2/Q3 2025

AI Security Solutions Landscape

For LLM and Gen AI Apps

https://genai.owasp.org/ai-security-solutions-landscape/

OWASP | GenAI SECURITY PROJECT

TOP 10 FOR LLM AND GENERATIVE AI

AI SECURITY SOLUTIONS INITIATIVE

Q2/Q3 2025

AI Security Solutions Landscape

For LLM and Gen AI Apps

The Solutions Landscape monitors and maps the full LLM and Generative AI lifecycle, focusing on the DevOps–SecOps intersection to meet evolving security needs. Guided by the OWASP Top 10 Risks and Mitigations for LLM and Gen AI and SecOps tasks, it highlights open-source and commercial solutions by stage, identifying their coverage of LLM and Gen AI SecOps duties and Top 10 threat mitigation, and leverages industry and community input as a peer-reviewed resource for navigating the growing number of LLM and Gen AI security solutions. Updated Quarterly.

https://genai.owasp.org/ai-security-solutions-landscape/

OWASP | GenAI SECURITY PROJECT
TOP 10 FOR LLM AND GENERATIVE AI

CHEAT SHEET

LLM & GenAI Security Landscape – 2025, Q2/Q3

https://genai.owasp.org/ai-security-solutions-landscape/

Operate

AI Validation, KNOSTIC, Prediction Guard, preamble, aqua, aim security, PRISMA, paloalto, Pillar, Dynamo AI, Straiker, cloudsineAI, INFOTECT, Skyrelis, NOMA, f5, ZenGuard AI, TREND MICRO, LLM GUARD, IRONCORE LABS, Llama Guard Meta, Infosys, Microsoft Security, NRI SECURE AI Blue Team, TROJ.AI, dreadnode, securiti AI Security & Governance, BLUETEAM AI

Deploy

TROJ.AI, Infosys, aim security, cisco AI Firewall®, Meta, BLUETEAM AI, securiti AI Security & Governance, Prediction Guard, PRISMA, Operant, LASSO, Teleport, IRONCORE LABS, NOMA, preamble, paloalto

Release

NOMA, CycloneDX, PRISMA, LEGIT AI-SPM, paloalto, securiti AI Security & Governance, Pillar, Calypso AI, AI Validation, aqua

Test & Evaluate

AIShield Powered by Bosch, SPLX, securiti AI Security & Governance, ZenGuard AI, AIM, promptfoo, Infosys, Giskard, Enkrypt AI, LangCheck, MODELSCAN, DRYRUN SECURITY, ADVERSA LLM vulnerability scanner, Synack, Prompt Fuzzer, aqua, Calypso AI, FUJITSU, NOMA, CYBERSECEVAL Meta, Pillar, Dynamo AI, Prediction Guard, ai+ me, TROJ.AI, KELA, Cobalt, Cymetrics, Straiker, AI Validation, PROTECT AI, WATCHTOWER BY AISHIELD, PRISMA, MINDGARD, HARMBENCH, Citadel AI, eRoom&company, TREND MICRO

Develop & Experiment

Meta, authzed, Pillar, TRAIL OF BITS, cisco AI Validation, Mend.io, ai+ me, TROJ.AI, NOMA, securiti AI Security & Governance, snyk, Operant, aqua, HoundDog.ai, Cloaked AI, PRIVACY Raven, PRISMA, pangea, Infosys

Augment, Fine Tune Data

Prediction Guard, UNSTRUCTURED.IO, securiti AI Security & Governance, BLUETEAM AI, Cloaked AI, Pillar, PRISMA

Scope & Plan

securiti, Prediction Guard, authzed, BLUETEAM AI, NOMA, Microsoft Security, STRIDE GPT, MITRE ATLAS, Seezo, Pillar, PRISMA, paloalto

Monitor

AI Validation, BLUETEAM AI, INFOTECT, KELA, LAKERA, Operant, fiddler, aim security, HIDDENLAYER, Dynamo AI, NOMA, preamble, Meta Prompt Guard, Calypso AI, aqua, Pillar, paloalto, AIShield Powered by Bosch, Prediction Guard, Teleport, TROJ.AI, securiti, PRISMA, ai+ me, TREND MICRO, APEX, Straiker, Skyrelis, SPLX, GuardionAI, PROTECT AI, ZenGuard AI

Govern

Teleport, AI Validation, BLUETEAM AI, INFOTECT, CRANIUM, Calypso AI, aim security, NOMA, securiti, paloalto, Pillar, POMERIUM, Prompt:, Dynamo AI, Skyrelis, LASSO, PRISMA, Tumeryk AI GUARD, unbound security, VERIFY FOUNDATION

Open Source Gold Sponsors Silver Sponsors

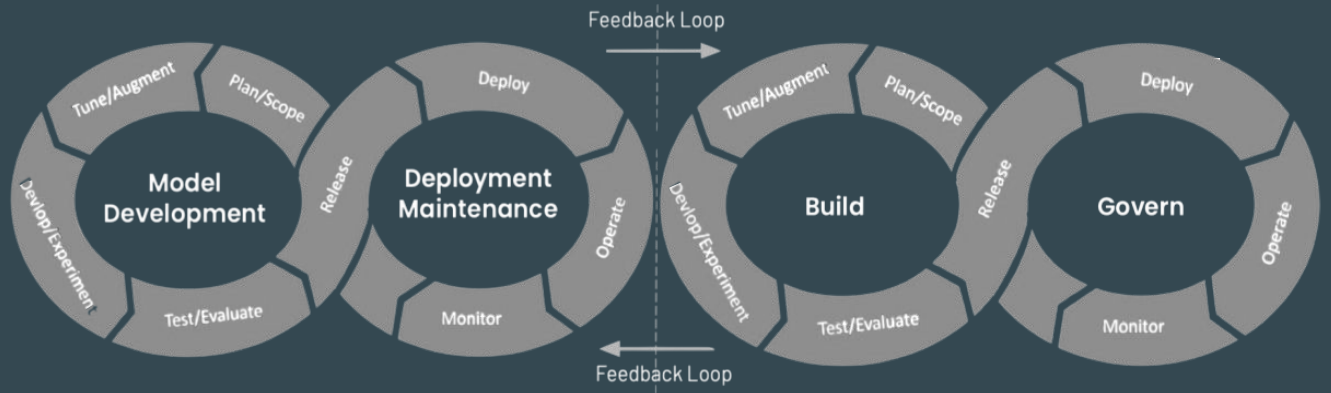
Source; OWASP Gen AI Security Solutions Landscape Guide 2025.Q2/Q31

OWASP | GenAI SECURITY PROJECT
TOP 10 FOR LLM AND GENERATIVE AI

https://genai.owasp.org/ai-security-solutions-landscape/

CHEAT SHEET

LLM and Gen AI App SecOps Framework



The OWASP LLMSecOps Framework was captured to help better align LLMOps processes and the security roles and dependencies for each stage. While LLMOps and MLOps are rooted in the same foundational principles of lifecycle management, they can diverge significantly in their focus and requirements, as one is focused primarily on model development, while the other extends DevOps to include support for various LLM, Gen AI and application patterns.

Plan & Scope

- Access Control and Authentication Planning
- Compliance and Regulatory Assessment
- Data Privacy and Protection Strategy
- Early Identification of Sensitive Data
- Third-Party Risk Assessment (Model, Provider, etc.)
- Threat Modeling

Augment & Fine Tune Data

- Data Source Validation
- Secure Data Handling
- Secure Output Handling
- Adversarial Robustness Testing
- Model Integrity Validation (ex: serialization scanning for malware)
- Vulnerability Assessment

Dev & Experiment

- Access, Authentication, and Authorization (MFA)
- Experiment Tracking
- LLM & App Vuln Scanning
- Model and Application Interaction Security
- SAST/DAST
- Secure Coding Practices
- Secure Library/Code Repository
- Software Comp Analysis

Test & Evaluation

- Adversarial Testing
- Application Security Orchestration and Correlation
- Bias and Fairness Testing
- Final Security Audit
- Incident Simulation, Response Testing
- LLM Benchmarking
- Penetration Testing
- IAST
- Vulnerability Scanning

Release

- AI/ML Bill of Materials (BOM)
- Digital Model\Dataset Signing
- Model Security Posture Evaluation
- Secure CI/CD pipeline
- Secure Supply Chain Verification
- Static and Dynamic Code Analysis
- User Access Control Validation
- Model Serialization Defenses

Deploy

- Compliance Verification
- Deployment Validation
- Digital Model\Dataset Verification
- Encryption, Secrets management
- Multi-factor Authentication
- Network Security Validation
- Secure API Access
- Secure Configuration
- User and Data Privacy Protections

Operate

- Adversarial Attack Protection
- Automated Vuln Scanning
- Data Integrity and Encryption
- LLM Guardrails
- LLM Incident Detection and Response
- Patch Management
- Privacy, Data Leakage Protection
- Prompt Security
- Runtime Self-Protection
- Secure Output Handling

Monitor

- Adversarial Input Detection
- Model Behavior Analysis
- AI/LLM Secure Posture Management
- Patch and Update Alerts
- Regulatory Compliance Tracking
- Security Alerting
- Security Metrics Collection
- User Activity Monitoring
- Observability
- Data Privacy and Protection
- Ethical Compliance

Govern

- Bias and Fairness Oversight
- Compliance Management
- Data Security Posture Management
- Incident Governance
- Risk Assessment and Management
- User/Machine Access audits

Source; OWASP Gen AI Security Solutions Landscape Guide 2025.Q2/Q31

OWASP | GenAI SECURITY PROJECT
TOP 10 FOR LLM AND GENERATIVE AI

CHEAT SHEET

LLM & GenAI Security Landscape - 2025, Q2

https://genai.owasp.org/ai-security-solutions-landscape/

Scope & Plan

authzed
Prediction Guard
PRISMA BY PALO ALTO NETWORKS
securiti
Seezo
MITRE ATLAS
Pillar
BLUETEAM AI
NOMA
Microsoft Security
PILLAR
paloalto NETWORKS
STRIDE GPT

Open Source Gold Sponsors Silver Sponsors

The focus is on defining the application's goals, understanding the specific needs the LLM will address, and determining how the pre-trained model will be integrated into the larger system. This stage involves gathering requirements, assessing potential ethical and compliance considerations, and setting clear objectives for performance, scalability, and user interaction. The outcome is a detailed project plan that outlines the scope, resources, and timelines needed to implement the LLM-powered application successfully.

LLMOps	LLMSecOps
• Data Suitability • Model Selection • Requirements Gathering (business, technical, and data) • Task Identification • Task Suitability	• Access Control and Authentication Planning • Compliance and Regulatory Assessment • Data Privacy and Protection Strategy • Early Identification of Sensitive Data • Third-Party Risk Assessment (Model, Provider, etc.) • Threat Modeling

*Source; OWASP Gen AI Security Solutions Landscape Guide 2025.Q2/Q3*1

OWASP | GenAI SECURITY PROJECT
TOP 10 FOR LLM AND GENERATIVE AI

CHEAT SHEET

LLM & GenAI Security Landscape - 2025, Q2

https://genai.owasp.org/ai-security-solutions-landscape/

Augment, Fine Tune Data

UNSTRUCTURED.IO

securiti
AI Security & Governance

Cloaked AI

Pillar

PRISMA
BY PALO ALTO NETWORKS

BLUETEAM AI

Prediction Guard

Open Source Gold Sponsors Silver Sponsors

The focus is on customizing the pre-trained model to better suit the specific application needs. This involves augmenting the original dataset with additional domain-specific data, enhancing the model's ability to generate accurate and contextually relevant responses. Fine-tuning is then conducted by retraining the LLM on this enriched dataset, optimizing its performance for the intended use case. This stage is critical for ensuring that the LLM adapts effectively to the unique challenges of the target domain, improving both accuracy and user experience with fewer instances of hallucination.

LLMOps	LLMSecOps
• Data Integration • Retrieval Augmented Generation (RAG) • Fine Tuning • In-context Learning and Embeddings • Reinforcement Learning with Human Feedback	• Data Source Validation • Secure Data Handling • Secure Data Pipeline • Secure vector database • Secure Output Handling • Adversarial Robustness Testing • Model Integrity Validation (ex: serialization scanning for malware) • Vulnerability Assessment

*Source; OWASP Gen AI Security Solutions Landscape Guide 2025.Q2/Q3*1

OWASP | GenAI SECURITY PROJECT
TOP 10 FOR LLM AND GENERATIVE AI

CHEAT SHEET

LLM & GenAI Security Landscape – 2025, Q2

https://genai.owasp.org/ai-security-solutions-landscape/

Develop & Experiment

Cisco AI Validation
NOMA
Mend.io
authzed
TROJ.AI
Pillar
Meta
AI+ME
Operant
Trail of Bits
aqua
Cloaked AI
Privacy Raven
HoundDog.ai
snyk
securiti AI Security & Governance
pangea
PRISMA
Infosys

Open Source Gold Sponsors Silver Sponsors

The focus shifts to integrating the fine-tuned model into the application's architecture. This stage involves building the necessary interfaces, user interactions, and workflows that leverage the LLM's capabilities. Developers experiment with different configurations, testing the model's performance within the application and refining the integration based on user feedback and real-world scenarios. This iterative process is crucial for optimizing the user experience and ensuring the LLM functions effectively within the broader application context.

LLMOps	LLMSecOps
• Agent Development • Experimentation, Iteration • Prompt Engineering	• Access, Authentication, and Authorization (MFA) • Experiment Tracking • LLM & App Vulnerability Scanning • Model and Application Interaction Security • SAST/DAST/ IAST • Secure Coding Practices • Secure Library/Code Repository • Software Composition Analysis

Source; OWASP Gen AI Security Solutions Landscape Guide 2025.Q2/Q3

OWASP | GenAI SECURITY PROJECT
TOP 10 FOR LLM AND GENERATIVE AI

CHEAT SHEET

LLM & GenAI Security Landscape – 2025, Q2/Q3

https://genai.owasp.org/ai-security-solutions-landscape/

Test & Evaluate

Straiker · SPLX · KELA · securiti AI Security & Governance · ZenGuard AI · AIM · MODELSCAN · DRYRUN .SECURITY · LLM vulnerability scanner · Synack · CYBERSECEVAL Meta · HARMBENCH · Prediction Guard · Prompt Fuzzer · cisco AI Validation · PROTECT AI · WATCHTOWER BY AISHIELD · PRISMA · MINDGARD · promptfoo · Infosys · Giskard · Enkrypt AI · LangCheck · Pillar · aqua · Cobalt · ADVERSA · NOMA · ai+ me · Calypso AI · Dynamo AI · FUJITSU · AIShield Powered by Bosch · Cymetrics · TROJ.AI · Citadel AI · eROUN&company · TREND MICRO

Open Source · Gold Sponsors · Silver Sponsors

At this stage in the LLM SDLC/Ops process, the focus is on assessing performance, security, and reliability through comprehensive functional, security, and usability testing. Metrics track accuracy, speed, and user interactions for fine-tuning. This phase ensures issues are resolved before deployment, enabling secure, effective real-world operation.

LLMOps	LLMSecOps
• Evaluate the model on validation and test datasets. • Integration Testing • Perform bias and fairness checks. • Stress / Performance Testing • Use cross-validation and other techniques to ensure robustness. • Validate the model's interpretability and explainability.	• Adversarial Testing • Application Security Orchestration and Correlation • Bias and Fairness Testing • Final Security Audit • Incident Simulation, Response Testing • LLM Benchmarking • Penetration Testing • SAST/DAST/IAST • Vulnerability Scanning • Available Agent Scanning

Source; OWASP Gen AI Security Solutions Landscape Guide 2025.Q2/Q31

OWASP | GenAI SECURITY PROJECT
TOP 10 FOR LLM AND GENERATIVE AI

CHEAT SHEET

LLM & GenAI Security Landscape – 2025, Q2

https://genai.owasp.org/ai-security-solutions-landscape/

Release

NOMA

securiti
AI Security & Governance

paloalto NETWORKS

PRISMA BY PALO ALTO NETWORKS

cisco AI Validation

Pillar

Calypso AI

LEGIT SECURITY AI-SPM

aqua

CycloneDX

Open Source Gold Sponsors Silver Sponsors

The focus shifts to deploying the finalized application to the production environment. This stage involves finalizing the deployment strategy, configuring the infrastructure for scalability and security, and ensuring that all components, including the LLM, are integrated and functioning as intended. Critical tasks include setting up monitoring and alerting systems, conducting a final security review, and preparing for user onboarding. The goal is to ensure a smooth and secure transition from development to production, making the application available to users with minimal risk and downtime.

LLMOps	LLMSecOps
• Enable continuous delivery of model updates • Integrate security checks and automated testing in the pipeline. • Package the model for deployment (e.g., using Docker, Kubernetes). • Set up CI/CD pipelines to automate application and model training, testing, and deployment.	• AI/ML Bill of Materials (BOM) • Digital Model\Dataset Signing • Model Security Posture Evaluation • Secure CI/CD pipeline • Secure Supply Chain Verification • Static and Dynamic Code Analysis • User Access Control Validation • Model Serialization Defenses

*Source; OWASP Gen AI Security Solutions Landscape Guide 2025.Q2/Q3*1

OWASP | GenAI SECURITY PROJECT
TOP 10 FOR LLM AND GENERATIVE AI

CHEAT SHEET

LLM & GenAI Security Landscape - 2025, Q2

https://genai.owasp.org/ai-security-solutions-landscape/

Deploy

TROJ.AI
BLUETEAM AI
Infosys
LASSO
IRONCORE LABS
securiti AI Security & Governance
Prediction Guard
PRISMA
Meta
cisco AI Firewall®
Teleport
aim security
Operant
paloalto NETWORKS
NOMA
preamble

Open Source Gold Sponsors Silver Sponsors

The focus is on securely launching the LLM and its associated components into the production environment. This stage involves configuring the deployment infrastructure for scalability and reliability, ensuring that all security measures are in place, and validating the integration of the LLM with other application components. Key activities include setting up real-time monitoring, conducting final checks to prevent any vulnerabilities, and implementing fallback mechanisms to ensure continuous operation. The goal is to smoothly transition from development to live operation, ensuring that the application is ready to handle real-world usage.

LLMOps	LLMSecOps
• Infrastructure Setup • Integrate with existing systems or applications. • Model and App Deployment • Set up APIs or services for access • User access and role management • Agent Permission and Ownership Control • Agentic Registry	• Compliance Verification • Deployment Validation • Digital Model\Dataset Signing Verification • Encryption, Secrets management • LLM Enabled Web Application Firewall • Multi-factor Authentication • Network Security Validation • Secrets Management • Secure API Access • Secure Configuration • User and Data Privacy Protections

Source; OWASP Gen AI Security Solutions Landscape Guide 2025.Q2/Q3

OWASP | GenAI SECURITY PROJECT
TOP 10 FOR LLM AND GENERATIVE AI

CHEAT SHEET

LLM & GenAI Security Landscape - 2025, Q2

https://genai.owasp.org/ai-security-solutions-landscape/

Operate

Open Source Gold Sponsors Silver Sponsors

The focus at this stage in the LLM SDLC and Ops process is on managing and maintaining the application in a live production environment. This stage involves continuous monitoring of the application's performance, security, and user interactions to ensure it operates smoothly and securely. Key activities include responding to incidents, applying updates or patches, and refining the model based on real-world data and feedback. The goal is to maintain high availability, optimize performance, and ensure the application remains secure and effective over time.

LLMOps	LLMSecOps
• Feedback Collection • Iterative Enhancements • Model Maintenance • Performance Management • Scalability and Infrastructure Management • User Support and Issue Resolution	• Adversarial Attack Protection • Automated Vulnerability Scanning • Data Integrity and Encryption • LLM Guardrails • LLM Incident Detection and Response • Patch Management • Privacy, Data Leakage Protection • Prompt Security • Runtime Application Self-Protection • Secure Output Handling • Anomaly Detection in Agent Chains • Runtime Agent Policy Validation

Source; OWASP Gen AI Security Solutions Landscape Guide 2025.Q2/Q3

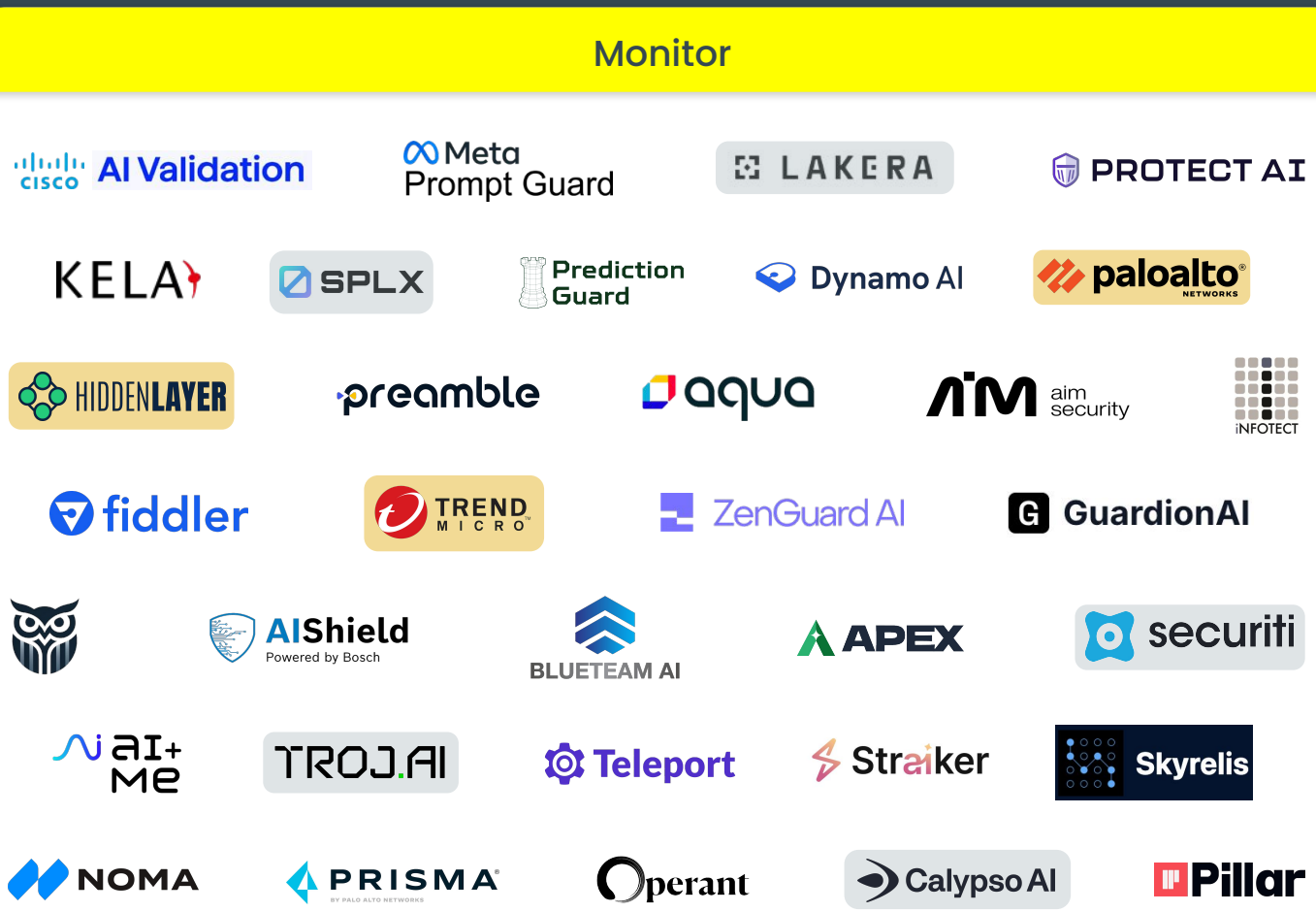
OWASP | GenAI SECURITY PROJECT
TOP 10 FOR LLM AND GENERATIVE AI

CHEAT SHEET

LLM & GenAI Security Landscape – 2025, Q2

https://genai.owasp.org/ai-security-solutions-landscape/

Monitor



Open Source Gold Sponsors Silver Sponsors

The focus at this stage is on real-time monitoring of performance, security, and user interactions. Key metrics are tracked to detect anomalies, ensure components work as expected, and maintain compliance. Data is gathered for improvement, issues are addressed proactively, and stability, security, and efficiency are maintained throughout the application's lifecycle.

LLMOps	LLMSecOps
• Automate retraining processes based on new data. • Detect and respond to model drift or degradation. • Manage model versioning and rollback if necessary • Monitor model performance (e.g., latency, accuracy, user interactions).	• Adversarial Input Detection • Model Behavior Analysis • AI/LLM Secure Posture Management • Patch and Update Alerts • Regulatory Compliance Tracking • Security Alerting • Security Metrics Collection • User Activity Monitoring • Agents Activity Monitoring • Observability • Data Privacy and Protection • Ethical Compliance

Source; OWASP Gen AI Security Solutions Landscape Guide 2025.Q2/Q3

OWASP | GenAI SECURITY PROJECT
TOP 10 FOR LLM AND GENERATIVE AI

CHEAT SHEET

LLM & GenAI Security Landscape - 2025, Q2

https://genai.owasp.org/ai-security-solutions-landscape/

Govern

BLUETEAM AI
Prompt:
cisco AI Validation
CRANIUM
POMERIUM
Calypso AI
Pillar
NOMA
securiti
Teleport
Skyrelis
paloalto NETWORKS
aim security
PRISMA BY PALO ALTO NETWORKS
iNFOTECT
Dynamo AI
unbound security
Tumeryk AI GUARD
LASSO
AI VERIFY FOUNDATION

Open Source Gold Sponsors Silver Sponsors

At this stage in the LLMOps process, the focus is on establishing and enforcing policies, standards, and best practices to ensure the application operates securely and ethically throughout its lifecycle. This stage involves setting governance frameworks that oversee data usage, model management, compliance, and security controls. Key activities include auditing, risk management, and ensuring the application adheres to regulatory requirements and organizational policies.

LLMOps	LLMSecOps
• Conduct regular audits for compliance (e.g., GDPR, CCPA). • Data Governance • Document model decisions, datasets used, and model versions. • Implement model governance frameworks.	• Bias and Fairness Oversight • Compliance Management • Data Security Posture Management • Incident Governance • Risk Assessment and Management • User/Machine Access audits • Agent Action Audit

*Source; OWASP Gen AI Security Solutions Landscape Guide 2025.Q2/Q3*1

Acknowledgement

OWASP Gen AI Solutions Landscape Initiative : https://genai.owasp.org/ai-security-solutions-landscape/

Lead: Scott Clinton

Initiative Slack Channel: #team-genai-ai-solutions-landscape-initiative

Contributors

Aurora Starita
Bryan Nakayama
Dennys Pereira
Emmanuel Guilherme
Fabrizio Cilli
Garvin LeClaire
Helen Oakley
Ishan Anand
Jason Ross
Marcel Winandy
Markus Hupfauer
Migel Fernandes
Mohit Yadav
Rachel James
Rico Komenda
Talesh Seeparsan
Teruhiro Tagomori
Todd Hathaway
Ron F. Del Rosario
Vaibhav Malik

Reviewers

Andy Smith
Arun John
Aurora Starita
Blanca Rivera Campos
Bryan Nakayama
Dan Guido
Dennys Pereira
Emmanuel Guilherme
Fabrizio Cilli
Garvin LeClaire
Heather Linn
Helen Oakley
Ishan Anand
Jason Ross
Joshua Berkoh
Marcel Winandy
Markus Hupfauer
Migel Fernandes
Mohit Yadav
Rachel James
Rammohan Thirupasur
Rico Komenda
Rammohan Thirupasur
Talesh Seeparsan
Teruhiro Tagomori
Todd Hathaway
Ron F. Del Rosario
Vaibhav Malik

Source; OWASP Gen AI Security Solutions Landscape Guide 2025.Q2/Q31

OWASP | GenAI SECURITY PROJECT
TOP 10 FOR LLM AND GENERATIVE AI

https://genai.owasp.org/ai-security-solutions-landscape/

Gen AI Security Project Sponsors

Supporting Community Operations And Outreach Through Direct Financial Sponsorship

GenAI SECURITY PROJECT — GOLD PROJECT SPONSOR — TOP 10 for LLM and Generative AI

ByteDance
HIDDENLAYER
Mend.io
snyk
paloalto NETWORKS
TREND MICRO

GenAI SECURITY PROJECT — SILVER PROJECT SPONSOR — TOP 10 for LLM and Generative AI

SPLX
Calypso AI
Acuvity
pangea
Cobalt
LAKERA
Synack
ActiveFence
Prompt:
TROJ.AI
LASSO
PROTECTO
PROMPTARMOR
securiti
GT cyber

Source; OWASP Gen AI Security Solutions Landscape Guide 2025.Q2/Q3

https://genai.owasp.org/ai-security-solutions-landscape/

Contributing to the Landscape Guide

Use the **QR Code** and associated form to submit an Agentic AI Security Landscape entry

Source; OWASP Gen AI Security Solutions Landscape Guide 2025.Q2/Q31