AccuKnox®

AI Security Report

Report for **Jul 12, 2025 12:00:00 (IST) to Aug 12, 2025 12:00:00 (IST)**

Prepared for

Acme Corp

Prepared by

AccuKnox

support@accuknox.com

About the Report

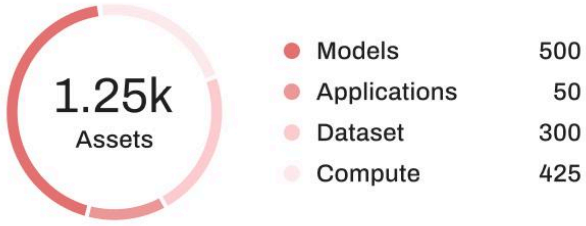
This report provides a detailed evaluation of the organization's compliance posture against applicable regulatory standards and frameworks. It identifies areas of non-compliance, highlights gaps in policies and controls, and offers actionable recommendations to address these issues. The assessment leverages industry best practices and automated compliance validation tools to ensure accuracy and completeness. This report aims to help the organization reduce compliance risk, maintain regulatory adherence, and strengthen governance practices.

Confidentiality Notice

AI Cloud Assets Scan

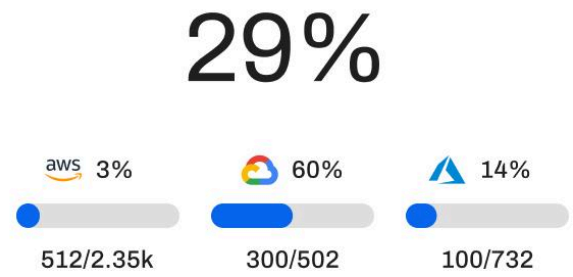
Jul 12, 2025
to **Aug 12, 2025**

AI Asset Summary



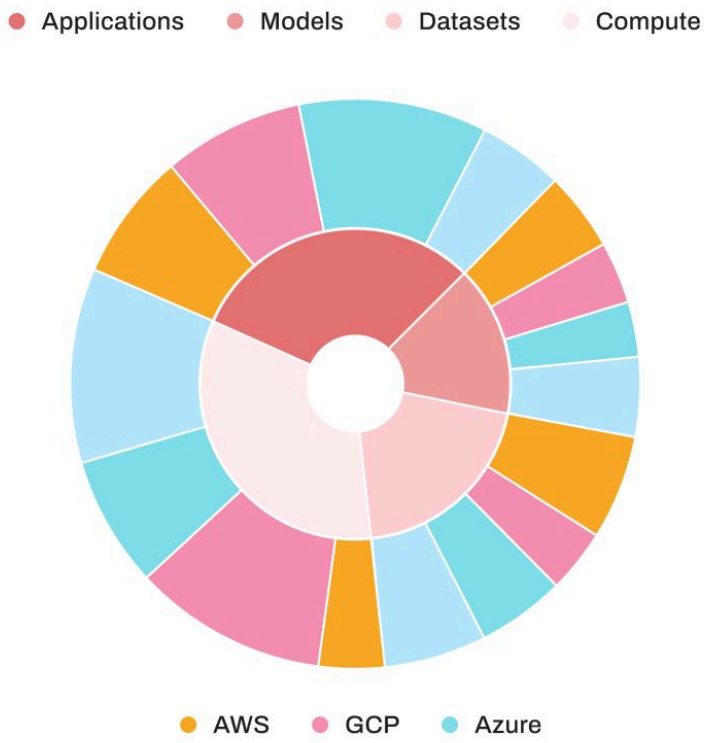
Shows the total number of AI assets, broken down by type (Models, Applications, Dataset, Compute)

AI Assets with Findings by Cloud Provider



Displays the count of AI assets with findings, segmented by cloud provider.

Asset Summary by Cloud Provider



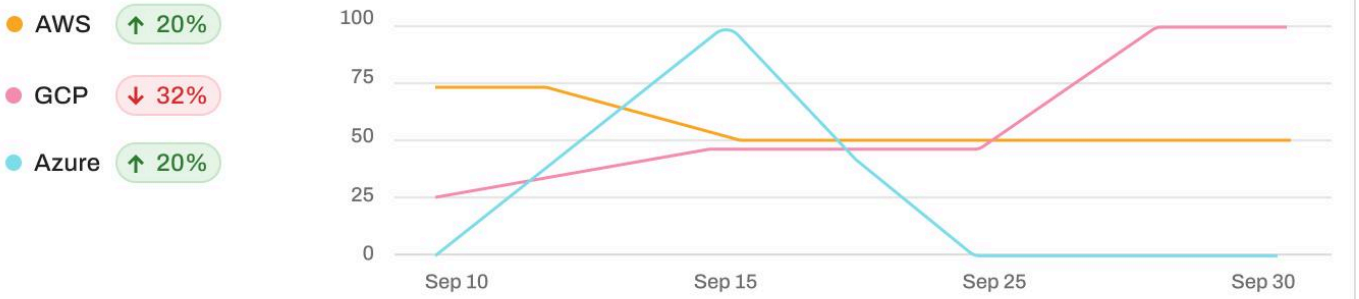
Cloud Provider	Application	Models	Dataset	Compute
AWS	20	14	19	30
GCP	36	12	15	24
Azure	24	11	20	10

Displays the distribution of assets across providers and categories for quick comparison.

AI Cloud Assets Scan

Jul 12, 2025
to **Aug 12, 2025**

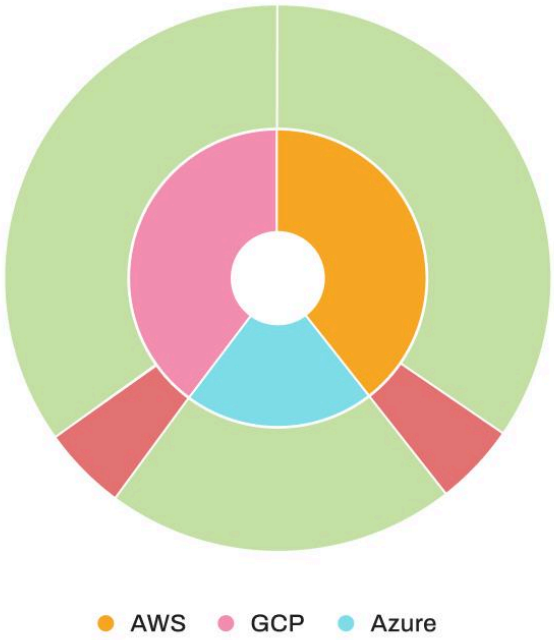
Assets Trend by Cloud Provider



Tracks asset trends over time for AWS, GCP and Azure.

Cloud Providers

20 Accounts 16 Active 4 Inactive



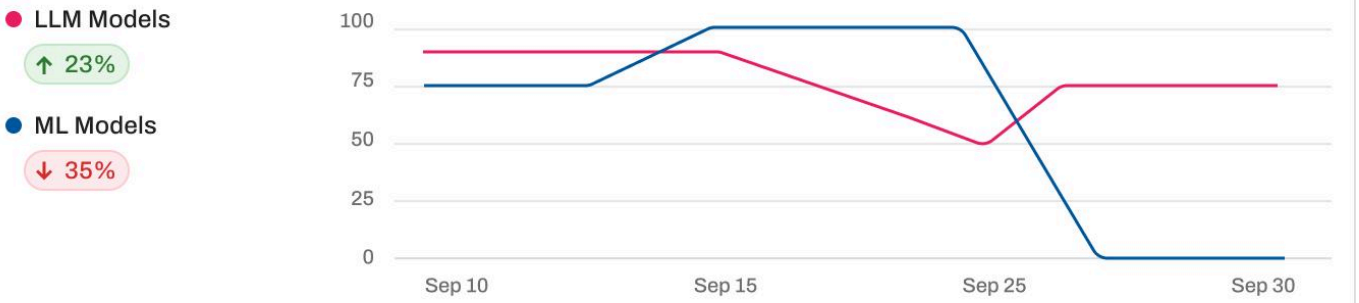
Cloud Provider	Active	Inactive
AWS	6	2
GCP	6	2
Azure	4	0

Shows the total number of connected cloud accounts, categorized by provider and their active/inactive status.

AI Cloud Assets Scan

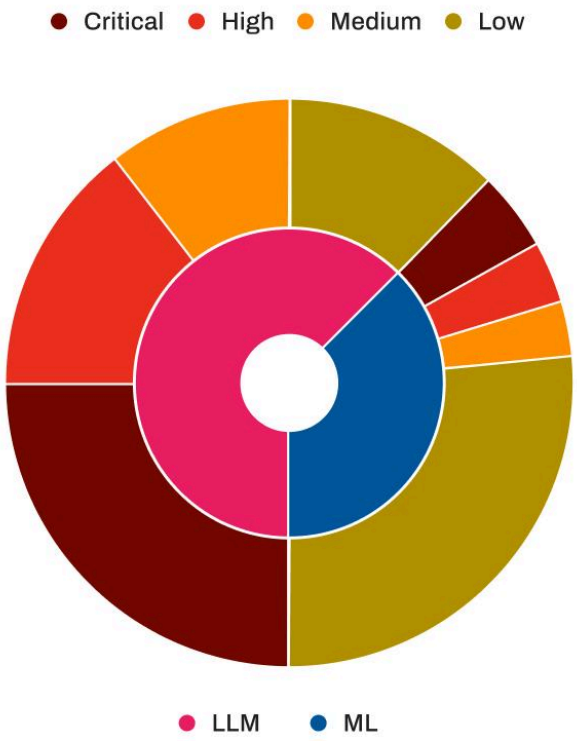
Jul 12, 2025
to **Aug 12, 2025**

Issue Distribution Trend by Models



Tracks issue trends across LLM, ML, and Custom models over time.

Issue Distribution across Models by Severity



Severity	LLM	ML
Critical	100	25
High	75	30
Medium	50	20
Low	35	100

Shows the distribution of findings across LLM & ML models by severity.

AI Cloud Assets Scan

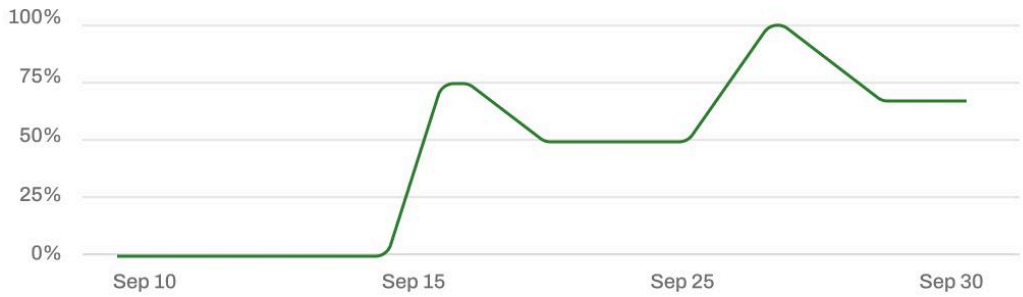
Jul 12, 2025
to **Aug 12, 2025**

Compliance Summary

65%

Moderate Risk

Checks Passed
120/200



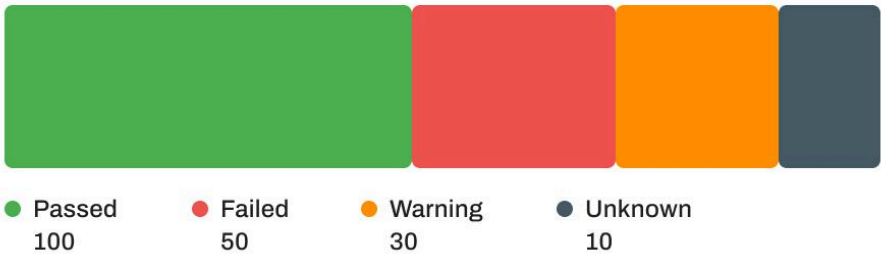
Provides overall compliance percentage and risk level.

Compliance by Framework

Singapore AI Act	EU AI Act	OWASP Top 10
55%	95%	75%
At Risk	Good Governance	Moderate Risk
Last Scan 12/08/2025	Last Scan 12/08/2025	Last Scan 12/08/2025

Shows compliance status against different regulatory frameworks.

AI Assets Compliance Status



Displays assets compliance results (Passed, Failed, Warning, Unknown).

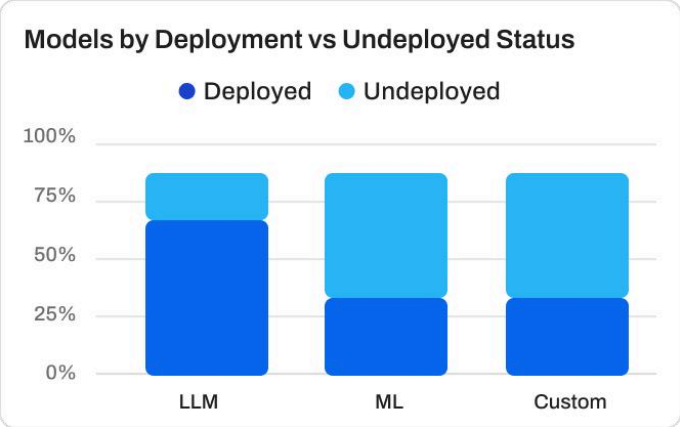
Top 10 Checks with Assets Failed

Checks	Severity	Assets
Key Vault Recovery not enabled	Critical	8
Kubernetes RBAC not enabled	Critical	98
Monitoring agent not encrypted	High	2,788
Public S3 bucket detected	Medium	23
Weak password policy in IAM	Low	2

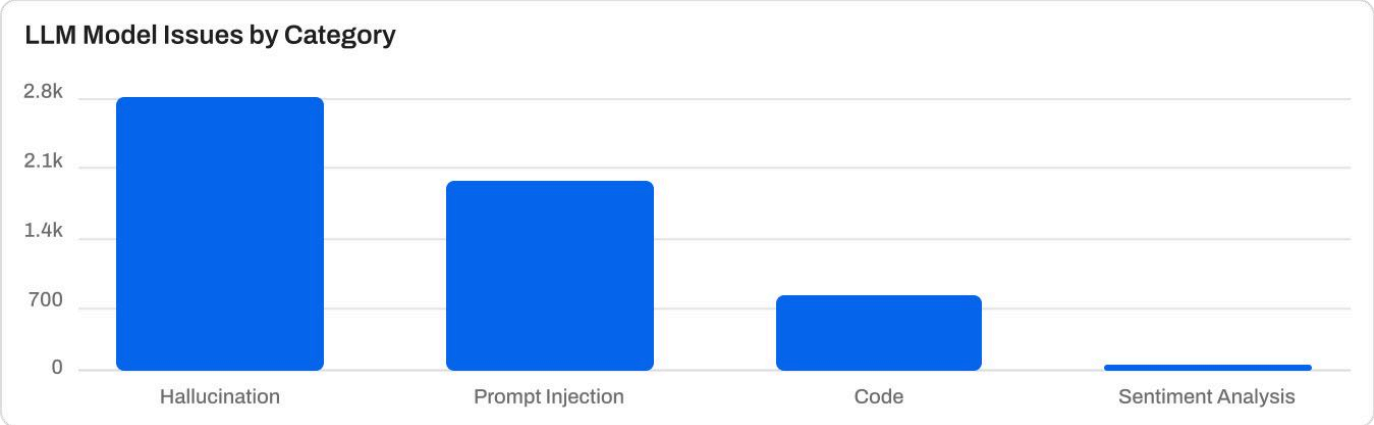
Lists the top failed checks with severity and asset count.

AI Cloud Assets Scan

Jul 12, 2025
to **Aug 12, 2025**



Shows model deployment status across model types.



Displays the number of issues grouped by model category to help identify key problem areas.

AI Cloud Assets Scan

Jul 12, 2025
to **Aug 12, 2025**

Infrastructure Issues by Category

Shows infrastructure-related issues categorized by type for easier prioritization.

Top 5 ML Models by Issues

Cloud Provider with Models	Findings	Severity							
Model Name - 2	67	2	C	5	H	40	M	20	L
Model Name-3	45	3	C	2	H	25	M	15	L
Model Name-1	1,100	100	C	300	H	400	M	300	L
Model Name -4	67	2	C	5	H	40	M	20	L
Model Name-5	45	3	C	2	H	25	M	15	L

Displays the ML models with the highest issue counts, categorized by severity to support prioritization of remediation efforts.

Top 5 LLM Models by Issues

Cloud Provider with Models	Findings	Severity							
Model Name-1	1,100	100	C	300	H	400	M	300	L
Model Name - 2	67	2	C	5	H	40	M	20	L
Model Name-3	45	3	C	2	H	25	M	15	L
Model Name -4	67	2	C	5	H	40	M	20	L
Model Name-5	45	3	C	2	H	25	M	15	L

Displays the LLM models with the highest issue counts, categorized by severity to support prioritization of remediation efforts.

AI Cloud Assets Scan

Jul 12, 2025
to **Aug 12, 2025**

Top 5 Datasets by Issues

Cloud Provider with Datasets	Findings								Severity
Model Name - 2	67	2	C	5	H	40	M	20	L
Model Name-3	45	3	C	2	H	25	M	15	L
Model Name-1	1,100	100	C	300	H	400	M	300	L
Model Name -4	67	2	C	5	H	40	M	20	L
Model Name-5	45	3	C	2	H	25	M	15	L

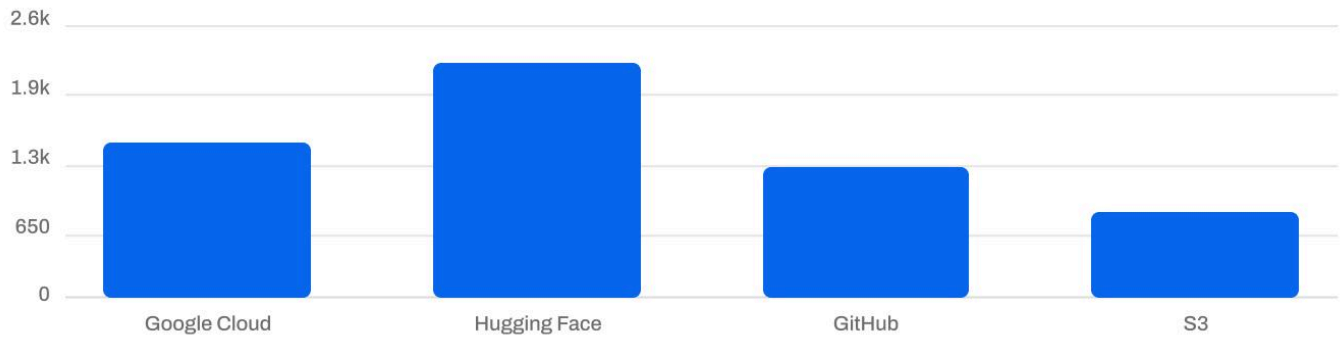
Displays the datasets with the highest issue counts, categorized by severity to support prioritization of remediation efforts.

Top 5 Computes by Issues

Cloud Provider with Computes	Findings								Severity
Model Name-1	1,100	100	C	300	H	400	M	300	L
Model Name - 2	67	2	C	5	H	40	M	20	L
Model Name-3	45	3	C	2	H	25	M	15	L
Model Name -4	67	2	C	5	H	40	M	20	L
Model Name-5	45	3	C	2	H	25	M	15	L

Displays the compute resources with the highest issue counts, categorized by severity to support prioritization of remediation efforts.

Secret Issues by Source

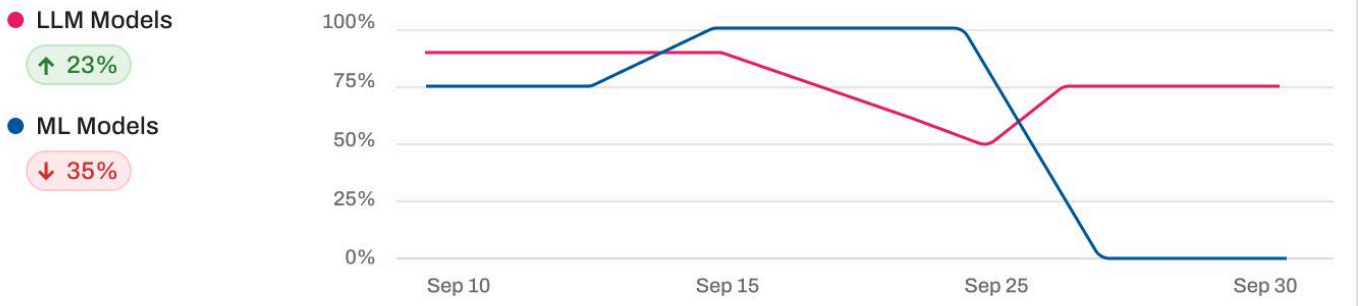


Displays the distribution of detected secrets across different sources (e.g., Google Cloud, Hugging Face, GitHub, S3) to help identify areas of exposure.

Red Teaming - On-Demand Scan

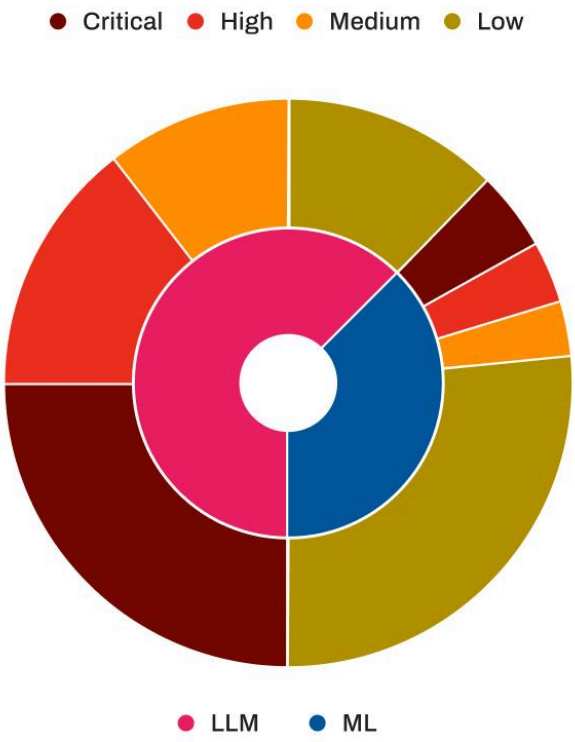
Jul 12, 2025
to **Aug 12, 2025**

Issue Distribution Trend



Tracks issue trends across LLM, ML, and Custom models over time.

Issue Distribution across Models by Severity



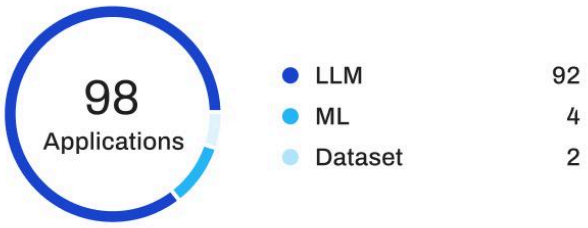
Severity	LLM	ML
Critical	100	25
High	75	30
Medium	50	20
Low	35	100

Shows the distribution of findings across LLM & ML models by severity.

Red Teaming - On-Demand Scan

Jul 12, 2025
to **Aug 12, 2025**

Applications by Category



Shows model deployment status, highlighting the count of deployed vs undeployed models.

Top 5 LLM Applications with Issues

Application	Findings								Severity
LLM Application -1	2,594	1,150	C	470	H	520	M	454	L
LLM Application -2	1,049	192	C	192	H	430	M	235	L
LLM Application -3	977	242	C	245	H	260	M	230	L
LLM Application -4	941	239	C	239	H	235	M	228	L
LLM Application -5	941	239	C	239	H	235	M	228	L

Displays the total number of LLM-related issues, broken down by severity levels (Critical, High, Medium, Low) to highlight overall risk distribution.

Red Teaming - On-Demand Scan

Jul 12, 2025
to **Aug 12, 2025**

Top 5 ML Applications with Issues

Application	Findings				Severity
ML Application -1	2,594	1,150 C	470 H	520 M	454 L
ML Application -2	1,049	192 C	192 H	430 M	235 L
ML Application -3	977	242 C	245 H	260 M	230 L
ML Application -4	941	239 C	239 H	235 M	228 L
ML Application -5	941	239 C	239 H	235 M	228 L

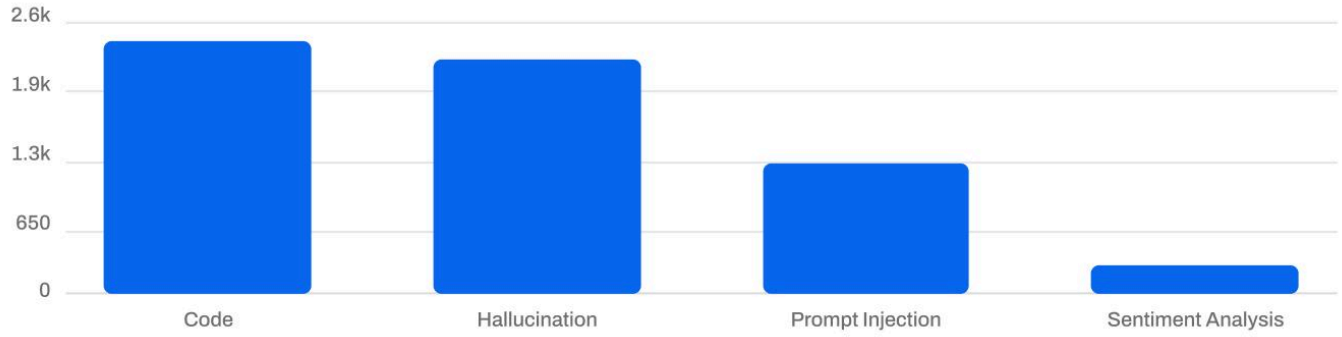
Displays the ML applications with the highest issue counts, categorized by severity to support prioritization of remediation.

Top 5 Datasets with Vulnerabilities

Dataset	Findings				Severity
Dataset-test-1	120	20 C	10 H	60 M	60 L
Dataset-test-1 - 2	80	2 C	1 H	3 M	2 L
Dataset-test-1 - 3	75	7 C	1 H	1 M	1 L
Dataset-test-4	8	8 C	0 H	0 M	0 L
Dataset-test-5	9	7 C	2 H	0 M	0 L

Displays the datasets with the highest number of vulnerabilities, categorized by severity to support remediation planning.

LLM Applications Issues by Category

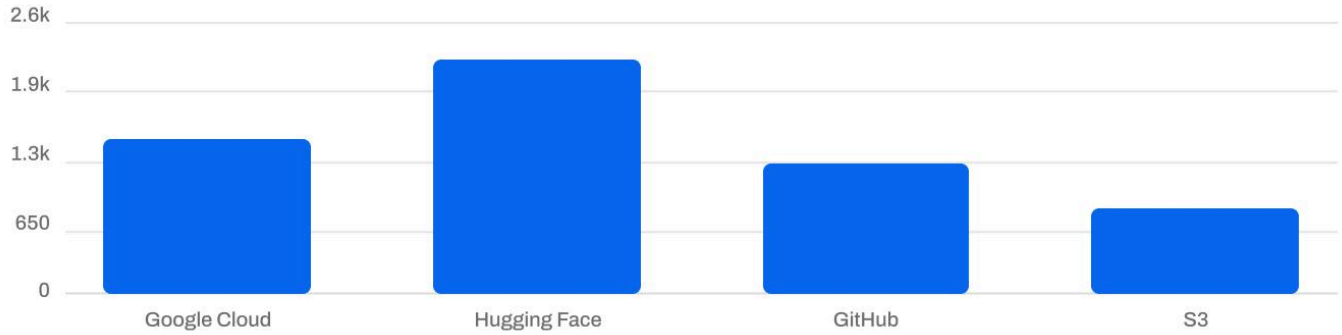


Displays application-level issues grouped by category to help identify key problem areas and prioritize remediation.

Red Teaming - On-Demand Scan

Jul 12, 2025
to **Aug 12, 2025**

Secrets by Source



Displays the distribution of detected secrets across different sources to help identify areas of exposure.

Top 5 Secret Scan Vulnerabilities

Vulnerabilities	Findings	Severity
Vulnerability - 1	120	Critical
Vulnerability - 2	80	High
Vulnerability - 3	75	Medium
Vulnerability -4	8	Low
Vulnerability -5	5	Low

Displays the most common vulnerabilities with their findings, categorized by severity to help assess and prioritize security risks.

Top 5 Assets with Issues

Asset	Findings								Severity
amazon.nova-micro-v1:0	2594	1150	C	470	H	520	M	454	L
meta.llama3-8b-instruct-v1:0	1049	192	C	192	H	430	M	235	L
mistral.mistral-7b-istruct-v0:2	977	242	C	245	H	260	M	230	L
amazon.titan-text-lite-v1	941	239	C	239	H	235	M	228	L
amazon.titan-text-lite-v2	867	242	C	250	H	245	M	130	L

Top 5 assets with most issues, ranked by severity to highlight key security risks.