

AI-Enhanced Security Assessment and Forensic Analysis of GraphQL APIs in Drone Fleet Management Systems

Automated MSc Proof-of-Concept Assessment Report

Generated: 03 October 2026, 21:51 UTC

Scope: controlled local drone-fleet GraphQL prototype. No real drones, external networks or third-party services were attacked.

Executive security posture

Captured events	Detected anomalies	Denied/failed	Evidence chain
928	834	59	VERIFIED

Enforced controls include HMAC-signed authentication, resolver-level RBAC, AST-based depth and complexity analysis, operation-batch limiting, administrator-only introspection, rate limiting, automatic request logging and chained forensic evidence.

Forensic integrity

Source digests valid: 928/928. Invalid source records: none. Broken chain positions: none.

Each event stores a SHA-256 source digest and a chain digest derived from the previous event. This exposes modification, deletion or reordering within the ordered evidence set.

AI and machine-learning evaluation

Decision Tree

Accuracy	1.0
Precision	1.0
Recall	1.0
F1-score	1.0
False positive rate	0.0
False negative rate	0.0
ROC-AUC	1.0
5-fold CV F1	0.9943 (+/- 0.0114)
Confusion matrix TN/FP/FN/TP	63/0/0/27
Feature importance	response_time_ms:0.955, query_complexity:0.045, query_depth:0.000, target_drone_id:0.000, target_mission_id:0.000, role_ADMIN:0.000, role_ANONYMOUS:0.000, role_OPERATOR:0.000
Model file	models\decision_tree.joblib
Predictions	outputs\decision_tree_test_predictions.csv

Random Forest

Accuracy	1.0
Precision	1.0
Recall	1.0
F1-score	1.0
False positive rate	0.0
False negative rate	0.0
ROC-AUC	1.0
5-fold CV F1	0.9943 (+/- 0.0114)
Confusion matrix TN/FP/FN/TP	63/0/0/27
Feature importance	response_time_ms:0.349, target_drone_id:0.171, query_complexity:0.128, role_OPERATOR:0.108, query_depth:0.043, role_VIEWER:0.028, target_mission_id:0.020, operation_name_ALLTELEMETRY:0.019
Model file	models\random_forest.joblib
Predictions	outputs\random_forest_test_predictions.csv

Logistic Regression

Accuracy	1.0
Precision	1.0
Recall	1.0
F1-score	1.0
False positive rate	0.0
False negative rate	0.0
ROC-AUC	1.0
5-fold CV F1	1.0 (+/- 0.0)
Confusion matrix TN/FP/FN/TP	63/0/0/27
Feature importance	response_time_ms:1.779, target_drone_id:1.734, role_OPERATOR:1.291, query_complexity:0.942, operation_name_TELEMETRY:0.877, role_VIEWER:0.850, role_UNKNOWN:0.728, operation_name_LOGIN:0.728
Model file	models\logistic_regression.joblib
Predictions	outputs\logistic_regression_test_predictions.csv

Extra Trees

Accuracy	1.0
Precision	1.0
Recall	1.0
F1-score	1.0
False positive rate	0.0
False negative rate	0.0
ROC-AUC	1.0
5-fold CV F1	1.0 (+/- 0.0)
Confusion matrix TN/FP/FN/TP	63/0/0/27
Feature importance	response_time_ms:0.178, target_drone_id:0.178, role_OPERATOR:0.152, query_complexity:0.097, role_VIEWER:0.054, operation_name_TELEMETRY:0.043, role_ANONYMOUS:0.036, operation_name_ALLTELEMETRY:0.029
Model file	models\extra_trees.joblib
Predictions	outputs\extra_trees_test_predictions.csv

Isolation Forest

Accuracy	0.3444
Precision	0.314
Recall	1.0
F1-score	0.4779
False positive rate	0.9365
False negative rate	0.0
ROC-AUC	0.9148
5-fold CV F1	0.4852 (+/- 0.0049)
Confusion matrix TN/FP/FN/TP	4/59/0/27
Feature importance	Not available for unsupervised Isolation Forest
Model file	models\isolation_forest.joblib
Predictions	outputs\isolation_forest_test_predictions.csv

Metrics must be interpreted in the context of a controlled synthetic dataset. Strong test scores demonstrate implementation behaviour, not guaranteed real-world generalisation.

Suspicious-event timeline

The forensic timeline reconstructs GraphQL API activity from security logs. It links user role, operation, requested resource, authorisation result, anomaly score and evidence hash. This connects API security testing with forensic-ready logging.

Timestamp	Actor / role	Operation and target	Outcome / risk	Evidence hash
2026-09-29 11:27:02	ADMIN UNKNOWN	MUTATION login API/resource not directly mapped	FAILED / ANOMALY Risk: 0.70	c79454b89ff217cf...
2026-09-29 11:26:55	ADMIN UNKNOWN	MUTATION login API/resource not directly mapped	FAILED / ANOMALY Risk: 0.70	7cebbadb790ae9d...
2026-09-29 11:26:47	adm UNKNOWN	MUTATION login API/resource not directly mapped	FAILED / ANOMALY Risk: 0.70	947c559ed88c7cf4...
2026-09-22 12:09:37	anonymous ANONYMOUS	GraphQL exportSecurityLogsCsv API/resource not directly mapped	DENIED / ANOMALY Risk: 0.70	9bc7fb9069d44b97...
2026-09-22 12:09:15	anonymous ANONYMOUS	QUERY blockedRequest API/resource not directly mapped	DENIED / ANOMALY Risk: 1.00	bb27920d85a0a0ed...
2026-09-22 12:09:15	anonymous ANONYMOUS	QUERY blockedRequest API/resource not directly mapped	DENIED / ANOMALY Risk: 1.00	fecfd6bd144f061c...
2026-09-22 12:04:22	admin ADMIN	QUERY OverviewSecurity API/resource not directly mapped	ALLOWED / ANOMALY Risk: 0.70	b59fa784f68e4b35...
2026-09-22 12:04:21	admin ADMIN	QUERY OverviewFleet API/resource not directly mapped	ALLOWED / ANOMALY Risk: 0.70	96675c9e09e92942...
2026-09-22 12:04:21	demo_student ADMIN	QUERY missions API/resource not directly mapped	ALLOWED / ANOMALY Risk: 0.70	22254fa49dcc1541...
2026-09-22 12:04:21	demo_student ADMIN	QUERY drones API/resource not directly mapped	ALLOWED / ANOMALY Risk: 0.70	a5e0fbb729f2f98b...
2026-09-22 12:04:21	admin ADMIN	MUTATION Model API/resource not directly mapped	ALLOWED / ANOMALY Risk: 0.70	59696ef32626beee...
2026-09-22 12:04:16	admin ADMIN	QUERY OverviewSecurity API/resource not directly mapped	ALLOWED / ANOMALY Risk: 0.70	f3dbb681a8adb4f2...
2026-09-22 12:04:16	admin ADMIN	QUERY OverviewFleet API/resource not directly mapped	ALLOWED / ANOMALY Risk: 0.70	a0aaf32f91156b53...
2026-09-22 12:04:16	demo_student ADMIN	QUERY missions API/resource not directly mapped	ALLOWED / ANOMALY Risk: 0.70	8619ee109fb6e501...

Limitations and future work

This is an academic proof-of-concept using simulated events, synthetic labelled data, local SQLite storage and a single-node rate limiter. Production deployment would require managed identity, TLS, distributed enforcement, immutable central evidence storage, representative traffic evaluation, privacy governance and operational monitoring.