



GDA is threat exposure validation.

Validate where AI runs. Prove what an attacker can actually reach.

An operator authorizes a named scope. GDA discovers, exploits, and publishes only evidence-graded findings.

DEPLOYMENT



Discover

Map hosts, apps, APIs, identities, and services in scope.



Exploit

Prove the path with live, bounded attacks.



Prove & fix

Evidence-graded findings, then retest the close.



Certify

A badge for that scope, bound to a UUID and hash.

WHO IT IS FOR



Security leadership

Show what an attacker could actually take — not a ranked list of unproven CVEs.



Security architects

One operation that chains web, API, identity, cloud, and the edge.



Security operators

Named scope, time box, kill switch, replayable plan, and a hash to file.



Platform security

The same class of proof in CI and on a schedule, so a fix is re-tested.

TWO NATURES OF ATTACK — ONE PLATFORM

YIN · DETERMINISTIC Deterministic

Repeatable known-attack logic. Replayable plans, no model required. Air-gap ready.



YANG · PROBABILISTIC Exploratory

Adaptive exploration. Open-weight models, opt-in and self-hosted. Cannot publish Critical without captured output.

Probabilistic exploration. Deterministic proof. You can leave exploration off. You cannot turn the evidence gate off.



HOW GDA WORKS

Discover, attack, explore, prove, revalidate — on the system as deployed.



A scanner executes a list. GDA pursues an objective.

Agents choose tools from live observation, share state, and re-plan when an action fails.



01 Port Discovery

Map reachable hosts, ports, and protocols before payload selection.



02 Recon

Fingerprint services, stacks, identities, and reachable control points.



03 Discovery

Generate and rank candidate attack paths by reachability and context.



04 Exploitation

Attempt safe, bounded exploitation and capture target-side proof.



05 Post-exploit

Reuse credentials, escalate privileges, pivot, and move laterally.



06 Collection

Grade evidence, deduplicate findings, map paths, and build reports.



Evidence doctrine

- **Exploited** — Captured target output. Only this grade can be Critical.
- **Observed** — Condition confirmed; exploit not proven.
- **Attack Path Identified** — Reachable chain proven; exploit not executed.
- **Simulated** — Modeled only; never presented as exploit proof.



Authorization & safety

- Signed envelope with named targets and expiry $\leq 24h$.
- Kill switch and fail-closed scope enforcement.
- Default-deny destructive classes; reversible probes by default.



DETERMINISTIC EXECUTION

Repeatable plans, audit replay, bounded primitives.



ADAPTIVE REASONING

Open-weight models, opt-in. Observe, re-plan, pivot.



WHAT GDA TESTS: WEB APPLICATIONS

Show the attacks the platform can execute, not vague coverage claims.

ATTACK TYPE	WHAT IT MEANS	
 01 Injection	SQL, NoSQL, command injection	PARTIAL
 02 Remote Code Execution	OS command execution and web application RCE	
 03 Server-Side Template Injection	SSTI payload injection and execution	
 04 Cross-Site Scripting	Reflected, stored, and DOM XSS	
 05 Server-Side Request Forgery	SSRF and metadata access abuse	
 06 XML External Entity	XXE and XXE-to-SSRF paths	
 07 Insecure Deserialization	Java, PHP, Python, and .NET gadget-chain probing	
 08 File Upload Attacks	Malicious upload and web-shell style abuse	
 09 Path Traversal	Directory traversal and unauthorized file access	
 10 HTTP Request Smuggling	CL.TE and TE.CL style smuggling	
 11 Open Redirect	Redirect abuse and token theft paths	
 12 CORS Misconfiguration	Origin reflection and credential leakage	
 13 CSRF	Authenticated workflow abuse	
 14 Security Misconfiguration	Dangerous methods, insecure headers, exposed admin paths	
 15 Vulnerable Components	Known-CVE exploitation against exposed software	



WHY THIS MATTERS

- A scanner may report a weakness.
- GDA shows whether it can actually be exploited.
- Evidence and attack paths help teams fix what matters first.



Mapped to OWASP Top 10 · CWE · CVE/CVSS



WHAT GDA TESTS: APIS

GDA tests API behavior, authorization, business logic, and exploit paths.

API ATTACK TYPE	WHAT IT MEANS	
 Broken Object-Level Authorization (BOLA / IDOR)	Access to objects or records that should be off limits	
 Broken Authentication	Weak login, session, or token handling	
 Broken Object Property Authorization	Unauthorized property exposure or modification	
 Resource Consumption Abuse	API calls that can exhaust resources or create denial of service	PARTIAL
 Broken Function-Level Authorization	Access to privileged or admin functions	
 Sensitive Business Flow Abuse	Multi-step workflow abuse and business-logic attacks	
 API Server-Side Request Forgery	API-driven SSRF and backend request abuse	
 Security Misconfiguration	Insecure API settings, headers, or deployment choices	
 Shadow or Outdated APIs	Hidden, forgotten, or old endpoints	
 Unsafe API Consumption	Trust issues with downstream APIs and third-party services	PARTIAL
 JWT Attacks	alg:none, algorithm confusion, and claim tampering	
 Mass Assignment	Unexpected or unauthorized property updates	
 GraphQL Attacks	Schema support and testing	
 REST API Fuzzing	Malformed and context-aware payload testing	
 Multi-Step Authenticated Testing	Role-aware testing across real user flows	



Recognizable standards

- OWASP API Security Top 10 2023
- OWASP Top 10
- CWE / CVE / CVSS



What buyers should know

- Checks real exploit paths, not only schema mistakes.
- Supports REST, GraphQL, OpenAPI, Postman, and authenticated workflows.
- Shows which API issues can lead to real impact.



WHAT GDA TESTS: IDENTITY, NETWORK, CLOUD

Start anonymous, produce credentials, re-enumerate with access, then exploit and move laterally.

ID IDENTITY & ACTIVE DIRECTORY		
Enumeration	Users, service accounts, SPNs, trusts, and policy discovery	✓
Password Spraying	Lockout-aware credential testing	✓
Kerberos Attacks	AS-REP roasting and Kerberoasting	✓
Credential Dumping	Credential extraction and reuse	✓
Pass-the-Hash / NTLM Relay	Hash reuse and relay paths	✓
DCSync	Directory replication abuse	✓
ADCS / Delegation / ACL Abuse	Privilege escalation through directory control paths	✓
Shadow Credentials / GPO / Ticket Forgery	Persistence and advanced AD abuse	✓
ID NETWORK & SERVICES		
Host and Port Discovery	Reachable hosts, open ports, and exposed services	✓
Service Fingerprinting	Identify versions, stacks, and likely attack paths	✓
SMB Attacks	Null sessions, signing weaknesses, and file-share abuse	✓
SSH / FTP / WinRM	Credential validation and remote access paths	✓
MSSQL and Service Access	Database access and command execution paths	✓
TLS and Certificate Analysis	Protocol, cipher, and certificate weaknesses	✓
Pivoting and Segmentation Validation	Can an attacker cross trust boundaries?	✓
ID CLOUD, CONTAINERS & CI/CD		
Cloud Metadata Abuse	IMDS and metadata credential access	✓
IAM Privilege Escalation	Role and permission abuse	✓
IAM Trust-Chain Attacks	Assume-role and trust-chain pivoting	✓
Secrets Access	Access to stored credentials and secrets	✓
Sensitive Cloud Data Access	Storage and database exposure validation	✓
Container Escape	Container-to-host attack paths	✓
Kubernetes Exposure	Exposed kubelet and cluster weaknesses	✓
CI/CD Compromise	Pipeline and Jenkins-style exposure	✓



WHY THIS PAGE IS IMPORTANT

These are the attack paths that turn one foothold into broader compromise.



BEYOND SCANNERS AND ANNUAL TESTS

GDA validates security controls, attacker movement, and connected systems.

SECURITY CONTROL VALIDATION		
ZTNA / Private Application Access	Can protected internal apps still be reached?	✓
SWG and URL Filtering	Can web controls be bypassed?	✓
CASB Restrictions	Are SaaS and tenant controls enforced?	✓
DLP Controls	Can sensitive data still leave the environment?	✓
Firewall / FWaaS	Do network and application controls block the path?	✓
DNS Security and C2 Controls	Can attacker callbacks still work?	✓
MFA and Identity Controls	Do step-up controls stop the attacker?	✓
GenAI Egress Controls	Can LLM or GenAI channels leak sensitive data?	✓
Network Segmentation	Do trust boundaries really hold?	✓
POST-EXPLOIT & ATTACK CHAIN		
Privilege Escalation	Can low access become admin or root access?	✓
Credential Reuse	Can found credentials unlock more systems?	✓
Lateral Movement	Can compromise spread across hosts and identities?	✓
Persistence Paths	Can the attacker maintain access?	✓
Sensitive Data Collection	Can important data be reached and read?	✓
Crown-Jewel Targeting	Can the attacker reach critical systems or assets?	✓
Attack-Path Chaining	Can separate weaknesses become one real path?	✓
Safe Proof of Impact	Can impact be shown without destructive action?	✓
ROBOTICS, IOT & CYBER-PHYSICAL		
MQTT Broker Attacks	Authentication bypass and topic abuse	✓
ROS2 / DDS Attacks	Service discovery and unauthorized commands	✓
Unsigned OTA Updates	Firmware promotion and update-path risk	✓
Firmware Analysis	Embedded secrets and hardcoded keys	✓
Fleet API IDOR	Cross-device or cross-tenant control abuse	✓
BLE / RF / Zigbee	Wireless replay and unencrypted control paths	✓
UART / JTAG / USB	Local hardware and debug-interface exposure	✓
Robot Admin Interfaces	Default credentials and privilege escalation	✓
Device Integrity / Attestation	Can identity and integrity be trusted?	✓

Not default SKU — engagement / SOW. SCADA/ICS ATT&CK is vision, not shipping.





PROOF, REPORTING, DEPLOYMENT, AND USE CASES

GDA is designed to prove exploitability and help teams act on it.



EXPLOITED

Captured target output proves the exploit worked.



OBSERVED

The condition is real, but exploitation was not completed.



ATTACK PATH IDENTIFIED

The reachable chain is proven, even if the exploit was gated.



SIMULATED

Modeled only; not presented as exploit proof.

Outputs & reporting



OCSF 1.1 JSON



Interactive HTML attack graphs



Markdown reports



DOT / Cytoscape / Neo4j graph exports



Technical findings with evidence



Executive summaries



Compliance rollups



Retest and validation output

Deployment & operations



SaaS, private cloud, and air-gap



On-demand and scheduled runs



CI/CD integration



Workflow and ticketing integration



Signed authorization and scoped runs



Global kill switch



Default non-destructive probes



Explicit approval for destructive classes

BEST-FIT USE CASES



Web and API



Internal network
and AD



Cloud and
container



Security-control
effectiveness



Robotics and IoT



Continuous
exposure
validation



Compliance rollups PCI DSS 4.0 · NIST CSF 2.0 · OWASP Top 10 · SOC 2 · HIPAA · ISO 27001:2022 · DORA · NIS2 —
finding mappings, not vendor certificates



SEE WHICH PATHS ACTUALLY LEAD TO COMPROMISE.

Learn more at gadriel.ai



WHAT GDA TESTS BEFORE ATTACKS GET IN

One product across the estate. Network to industrial.

