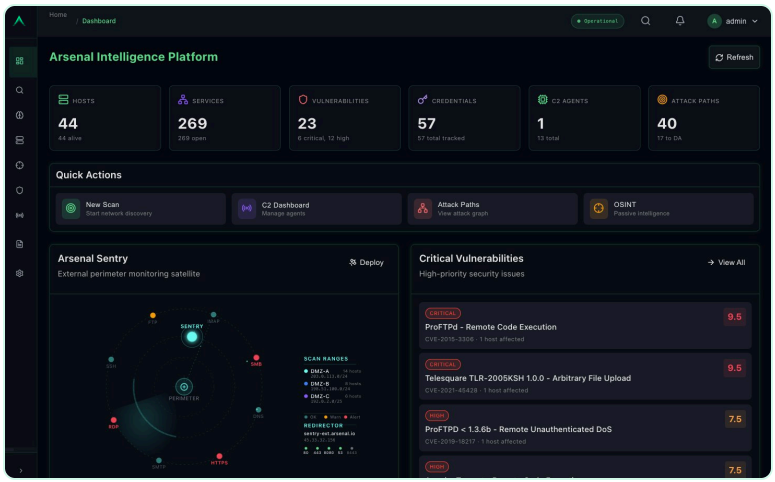
# The unified red team operations platform.

Arsenal correlates 47 integrated offensive security tools (e.g. BloodHound, Certipy, Metasploit, Impacket, Nuclei, NetExec, and more) under one operational data model. Every tool's output enriches the next. No CSV exports. No tab-switching. No lost intelligence.




## PLATFORM SUMMARY

### KEY CAPABILITIES

- Attack Path Intelligence with LLM synthesis
- Inline purple-team detection enrichment
- Active Directory + ADCS enumeration
- Unified credential vault & reuse detection
- Smart Exploit Checker & isolated Exploit Lab
- Arsenal C2 (Win / Linux / macOS agents)

### BUILT FOR

- Internal enterprise red teams
- Concurrent operator workflows
- OT environments, data centers, critical infrastructure
- On-prem & air-gapped deployment

### DEPLOYMENT

- Single hardened appliance
- Hardware sized to environment
- No SaaS · No outbound telemetry

### UNIFIED DATA MODEL

One correlated graph. Every tool reads from and writes to it. Findings carry source provenance end-to-end.

### OPERATOR-GRADE OUTPUT

Synthesized attack chains and MITRE-mapped paths, not raw scan dumps.

### DATA STAYS YOURS

Engagement data never leaves the appliance. The data sanitization engine obfuscates everything sent to frontier AI. Fail-closed.

### DETECTION-AWARE

Purple-team intelligence inline on every path: expected detections, Sigma rules, Sysmon coverage, SIEM patterns.

HOW IT WORKS

# From signal to attack path, in one workflow.

Every tool integration reads from and writes to a unified host, credential, vulnerability, and path model. UID-based deduplication prevents duplicate entities across tools. An operator working in Arsenal sees synthesized intelligence: which hosts are vulnerable, which credentials work where, which paths exist, which detections cover each step.

01
### RECONNAISSANCE
Network, web, and OSINT enumeration under one interface. Nmap, RustScan, Nuclei, httpx, FFUF, and Amass are all orchestrated, not just bundled.

02
### AD ENUMERATION
BloodHound CE for graph collection, Certipy for ADCS (ESC1–ESC13), continuous LDAP heartbeat tracking domain change.

03
### CREDENTIAL INTEL
Unified vault across SAM, LSASS, DPAPI, NTDS, Kerberos. Cross host reuse detection and validation tracking built in.

04
### ATTACK PATHS
115+ graph queries plus LLM synthesis. Paths classified VERIFIED, OPPORTUNISTIC, or THEORETICAL by evidence strength.

05
### EXPLOIT LAB
Isolated container sandbox per POC. Frontier-model safety analysis flags dangerous behaviors before any execution against a live target.

06
### ARSENAL C2
Native Windows, Linux, and macOS support. Custom C2 platform built into the unified intelligence schema, so every callback enriches the same data model.

∞
### CONTINUOUS LOOP
New BloodHound correlations and host vulnerabilities trigger automatic rediscovery. The path inventory tracks engagement state in real time.

47 INTEGRATED TOOLS

**ACTIVE DIRECTORY**
BloodHound CE · Certipy (ESC1–13) · LDAP heartbeat

**RECON & VULNERABILITY**
Nmap · RustScan · Masscan · Nuclei (10k+ templates) · SearchSploit · httpx · GoWitness · FFUF · Amass · TheHarvester · Sublist3r

**EXPLOITATION & LATERAL MOVEMENT**
Metasploit (7k+ modules) · NetExec (7 protocols) · Impacket direct-API + custom Arsenal Go (PSExec, WMIExec, SMBExec, AtExec)

**CREDENTIALS & COMMAND-AND-CONTROL**
Hashcat · John the Ripper · Arsenal C2 (native Win / Linux / macOS support)

FEATURED CAPABILITIES

# Where Arsenal goes further.

Three capabilities define the gap between Arsenal and any toolchain you assemble yourself. Each was built because no off-the-shelf tool addresses the operator-grade workflow Arsenal demands.

## Attack Path Intelligence

Two discovery modes run against the Arsenal Graph, a custom Neo4j layer combining network scan results, share enumeration, lateral-movement reachability, AD relationships, and ADCS certificate vulnerabilities into one offensive surface model. **Graph correlation** runs 115+ predefined queries (Kerberoasting, AS-REP, RBCD, DCSync, ESC1–ESC13, ACL abuse). **LLM synthesis** identifies chains pure graph traversal misses, bridging vulnerabilities, harvested credentials, accessible shares, and AD relationships into operator-grade narratives. Reactive rediscovery fires automatically on new correlation completion.

## Exploit Lab + Smart Exploit Checker

Two questions during exploitation: **is this exploit safe to run?** and **which exploits are worth running against this host?** Arsenal answers both. The Exploit Lab provides isolated, ephemeral Docker sandboxes per POC, with frontier-model safety analysis classifying the POC and flagging dangerous operations (encoded PowerShell, reverse shells to unknown infrastructure, hardcoded callbacks, credential dumping) before any run. The Smart Exploit Checker correlates enumeration results against Metasploit, ExploitDB, and the GitHub POC corpus, surfacing OPSEC-filtered exploit candidates directly on each host's detail view.

## Frontier AI Without Data Exposure

Arsenal's AI runs against current frontier models, but engagement data never leaves the appliance. Before any outbound LLM call, a Microsoft Presidio-based sanitization layer anonymizes hostnames, IPs, domains, usernames, credentials, service banners, and share paths. Entities are replaced with consistent per-engagement pseudonyms (HOST_ALPHA, USER_BETA, SHARE_GAMMA). The model reasons over the topology without ever seeing real values. **The layer is fail-closed**; if sanitization errors, the LLM call is rejected. Operators get frontier-model reasoning. Defenders get an auditable trail. Customer data stays on the appliance.

ARSENAL BY THE NUMBERS

| 47 | 115+ | 7k+ | 10k+ | ESC1–13 | 0 bytes |
|---|---|---|---|---|---|
| integrated tools | AD & ADCS queries | Metasploit modules | Nuclei templates | ADCS coverage | raw data to LLMs |

WHY THIS APPROACH WORKS

# Arsenal vs. the fragmented stack.

Most red teams run 15–20 disconnected tools. Three failure modes recur: lost intelligence between tools, operational friction from context-switching, and scattered ground truth that lives in terminal histories and notebooks. Arsenal replaces that.

| | FRAGMENTED TOOLCHAIN | ★ ARSENAL |
|---|---|---|
| **Data correlation** | Manual. CSV exports, copy-paste. | Automatic. Unified data model with UID dedup. |
| **Engagement state** | Terminal histories & operator notebooks. | Single source of truth. Survives turnover. |
| **Credential reuse detection** | Operator memory and grep. | Cross-host validation across all credential types. |
| **Attack-path synthesis** | BloodHound graph alone. | Graph + LLM across network, AD, ADCS, creds, shares. |
| **Detection awareness** | Bolted on, or absent. | Built in. Sigma + SIEM coverage inline on every path. |
| **AI on engagement data** | Raw values sent to cloud APIs, or unused. | Per-engagement pseudonymization. Fail-closed. On-prem. |

EVALUATE ARSENAL IN YOUR ENVIRONMENT

## Pre-configured appliance.

Arsenal ships as a single hardened appliance, ready to scan within hours. No cloud onboarding. No SaaS activation.

Request a Free Demo →

ABOUT ARSENAL UNIFIED INTELLIGENCE

Arsenal Unified Intelligence builds the operating system for enterprise red teams. It unifies offensive security tooling under one correlated data model, with privacy-preserving AI that fragmented toolchains can't deliver. Founded and built in the US by a military veteran and senior operator with deep experience across enterprise red teaming, regulated industries, and IT-OT boundaries inside data centers.

GET IN TOUCH

EMAIL contact@arsenalui.com
WEB arsenalui.com