SCEN&R

Toward an Open Standard for Realistic Adversary Emulation Scenarios

One campaign file. Any engine.



Frédéric Guihery · Damien Crémilleux

M&NTIS Team, Almond R&D · with Théo Vieugué and Thibault Lefrançois

M&NTIS PLATFORM · Almond

01 Why

Sharing executable attack campaigns

A real campaign is a chain: darupel crosses 3 hosts in 9 steps

CTI REPORT → ATTACK CAMPAIGN → CYBER RANGE → SOC / CERT ANALYSTS



darupel is one of our M&NTIS cyber-range training campaigns, taken here as the running example: from a vulnerable WordPress plugin to ransomware on the database server.

darupel only ran on M&NTIS; another engine meant a rewrite

M&NTIS
Python kill chain + **9 attack workers**: ≈3,200 lines.

CALDERA
Abilities, facts, profile: a second implementation.

Red team
A runbook: a third, not replayable.

same campaign, written three times

Costly. Rebuilt for every engine.

Locked in. Stuck in its tool.

Not shared. No campaign catalog.

Three requirements for a shareable campaign

	Engine-independent	Executable	Campaign state
Atomic Red Team	✓	✓	×
Attack Flow	✓	×	partial
CALDERA	×	✓	✓
SCEN&R	✓	✓	✓

Campaign state: **where** each step runs, **what** it hands on, **when** the next step fires.

TEST CASE · DARUPEL STEP 4 → STEP 5

Can step 5 reuse the password step 4 stole?

Atomic Red Team	×	Static inputs
Attack Flow	×	Prose only
CALDERA	partial	Only inside CALDERA
SCEN&R	✓	On any engine

02 SCEN&R

What does a portable campaign look like?

SCEN&R moves the campaign logic out of the engine into one file

Atomic tests

What runs: one test per technique (Atomic Red Team format).

SCEN&R scenario

How steps connect: sessions, data, conditions, infrastructure.

Engine

Where it runs: M&NTIS, CALDERA, or yours.

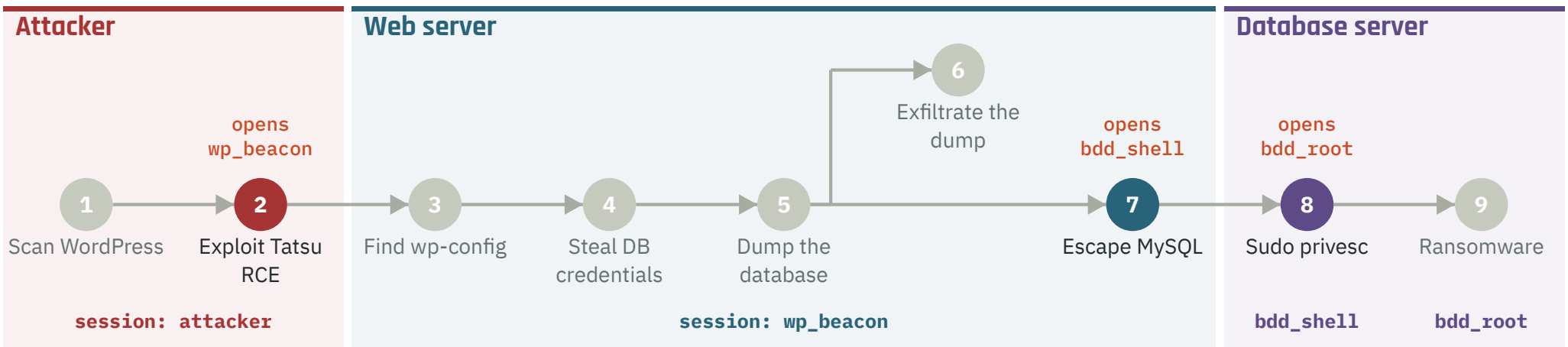
TRAVELS WITH THE FILE

Steps, sessions, extractions, conditions, IOCs

STAYS WITH THE ENVIRONMENT

Target hosts, pacing

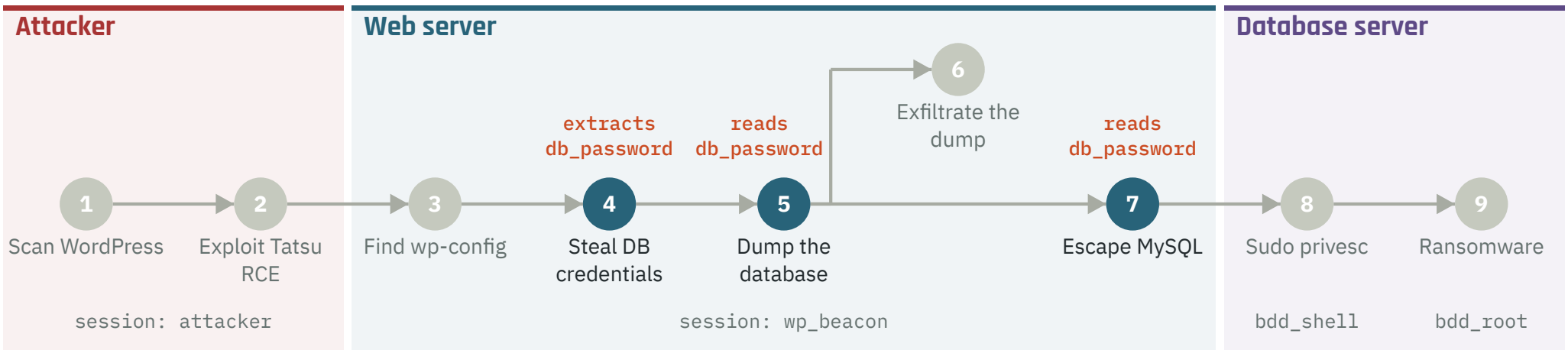
Each step declares the foothold it opens; the engine picks the transport




```yaml
darupel.yaml
- id: escape_mysql_cli
  session: wp_beacon              # runs here
  procedure: {file: T1068/T1068.yaml, guid: …}
  produces:
    session:
      bdd_shell: {host: WebBDD}   # opens this
```

The file says **where** the attacker stands.
The engine picks **how**: shell, beacon, agent.

The stolen password reaches the next step without an operator

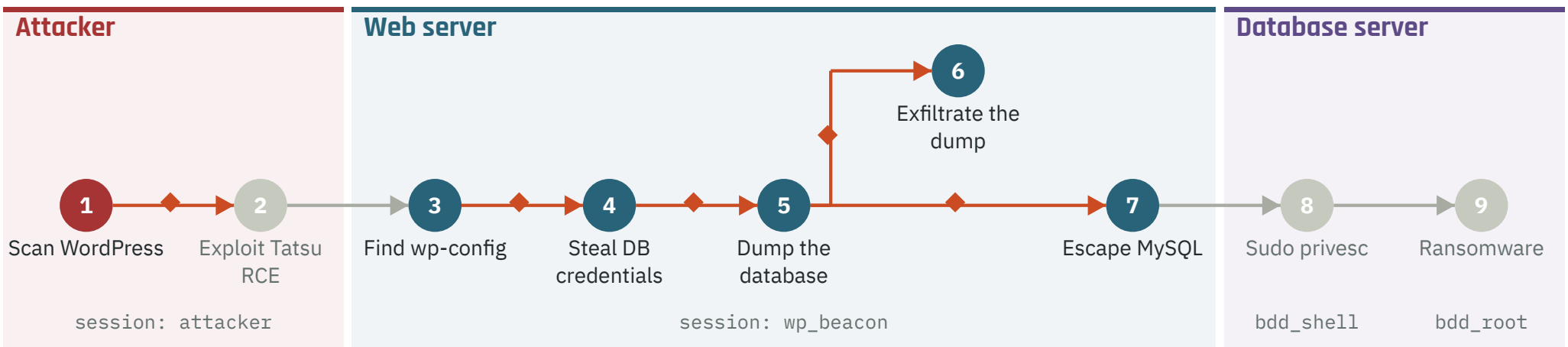



```
beside the test · then in darupel.yaml
db_password:                    # T1552.001.procedure.yaml
  extract: "'DB_PASSWORD',\s*'([^']+)'"

mysql_password_b64: >-          # step dump_remote_database
  {{steal_wp_db_credentials.db_password | b64encode}}
```

Written **once, beside the test**. Every scenario using it gets db_password.

No credentials, no pivot: the campaign reacts to what it obtained




```
darupel.yaml · graph
- from_: steal_wp_db_credentials
  to: dump_remote_database
  condition: steal_wp_db_credentials.db_password != null
```

◆ guarded edge.
Fallbacks (PsExec, else WMI) are just more edges.

Pinned infrastructure tests IOC detection, not just behaviour


```
infra · pinned from a CTI report
infra:
  c2_server:         # pinned: CISA AA23-353A, C2
    ip: "5.199.168.24"
  c2_relay:          # pinned: same report, C2
    domain: "resources.docusong.com"
  payload_server:    # free: the range chooses
```

```
upload_url: >-       # step exfiltrate_database_dump
  http://{{infra.payload_server.ip}}/upload
```

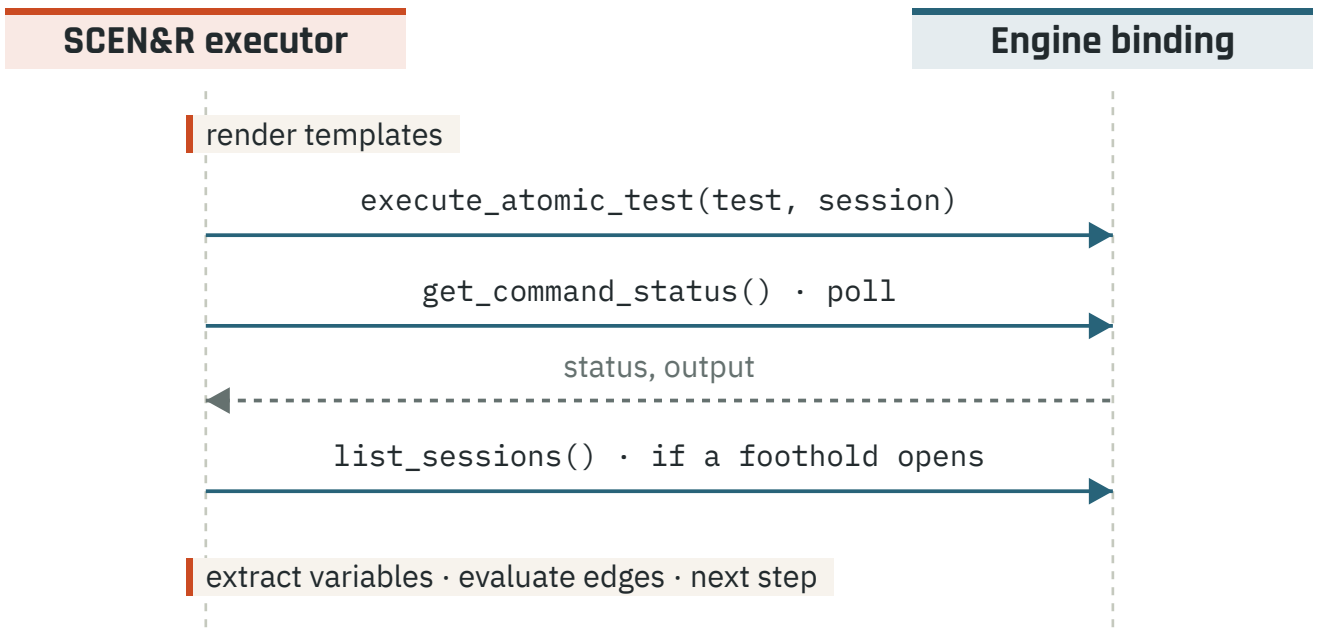
Pinned: deployed at that exact IP or domain.

Free: the range picks; the scenario reads it back.

ALPHV/BlackCat: pin the advisory's C2, and detections fire on the **real IOCs**.

IOCs: CISA #StopRansomware AA23-353A (ALPHV Blackcat), Table 4. The scenario states them; it does not fetch them.

A new engine costs about 250 lines once, then runs any SCEN&R campaign



BINDING SIZE, PYTHON

146 lines · M&NTIS

244 lines · CALDERA

Non-blank, non-comment lines in `scenar/backends/`. `prepare_session` is optional.

```
scenar run darupel.yaml --backend caldera --session attacker=<agent>
```

03 Proof

Running SCEN&R

The file under test: one campaign, nine atomic tests

darupel.scenar.yaml — 143 lines

```yaml
schema_version: "2.0"
scenario:
  id: darupel-scenar
variables:
  wordpress_root: "/srv/www/wordpress"
steps:
  - id: list_web_root_files
    session: wp_beacon
    procedure:
      file: "T1083/T1083.yaml"
      guid: "783150c3-fab1-…"
      parameters:
        search_path: "{{wordpress_root}}"
    timeout: "1m"
  # … 8 more steps
graph:
  - from_: exploit_tatsu_rce
    to: list_web_root_files
  - from_: list_web_root_files
    to: steal_wp_db_credentials
    condition:
      list_web_root_files.wp_config_path != null
  # … 6 more edges, 4 of them guarded
```

file + GUID →

atomics/ — 9 tests

```
├─ T1595.002/
│  ├─ T1595.002.yaml
│  └─ T1595.002.procedure.yaml
├─ T1190/
│  └─ T1190.yaml
├─ T1083/
│  ├─ T1083.yaml
│  └─ T1083.procedure.yaml
├─ T1552.001/
│  ├─ T1552.001.yaml
│  └─ T1552.001.procedure.yaml
├─ T1005/
│  ├─ T1005.yaml
│  └─ T1005.procedure.yaml
├─ T1048.003/
│  └─ T1048.003.yaml
├─ T1068/
│  └─ T1068.yaml
├─ T1548.003/
│  └─ T1548.003.yaml
└─ T1486/
   └─ T1486.yaml
```

What runs, in Atomic Red Team format.

same GUID →

T1083.procedure.yaml — 1 of 4

```yaml
procedures:
  - guid: "783150c3-fab1-…"
    produces:
      variable:
        wp_config_path:
          extract:
            "(.*/wp-config\\.php)$"
```

7 variables across the 4 companions, each extracted beside its test.

Same file, two engines, same campaign

M&NTIS

TITLE	TYPE	STATUS	ALERTS	START	DURATION	MITRE TAGS
WordPress plugin scan with wpscan	Attack (manual)	Success	—	13:30:18	4 s	T1595_002_000
WordPress Tatsu Builder RCE (CVE-2021-25094)	Attack (manual)	Success	—	13:30:22	19 s	T1190_000
Discover configuration files in web root	Attack (manual)	Success	—	13:30:43	4 s	T1083_000
Extract WordPress database credentials from wp-config.php	Attack (manual)	Success	—	13:30:49	3 s	T1552_001_000
Dump remote MySQL database with mysqldump	Attack (manual)	Success	—	13:30:53	5 s	T1005_000
HTTP file exfiltration via multipart upload	Attack (manual)	Success	—	13:30:59	5 s	T1048_003_000
MySQL UDF library injection to system shell	Attack (manual)	Success	—	13:31:05	5 s	T1068_000
Baron Samedit privilege escalation (CVE-2021-3156)	Attack (manual)	Success	—	13:31:12	4 s	T1548_003_000

CALDERA

Status	Ability Name	Host
success	WordPress plugin scan with wpscan	RedTeamHost
success	WordPress Tatsu Builder RCE (CVE-2021-25094)	RedTeamHost
success	Discover configuration files in web root	WebServerUbuntu
success	Extract WordPress database credentials from wp-config.php	WebServerUbuntu
success	Dump remote MySQL database with mysqldump	WebServerUbuntu
success	HTTP file exfiltration via multipart upload	WebServerUbuntu
success	MySQL UDF library injection to system shell	WebServerUbuntu
success	Baron Samedit privilege escalation (CVE-2021-3156)	WebBDD

9 / 9
steps successful on each engine

4
sessions opened

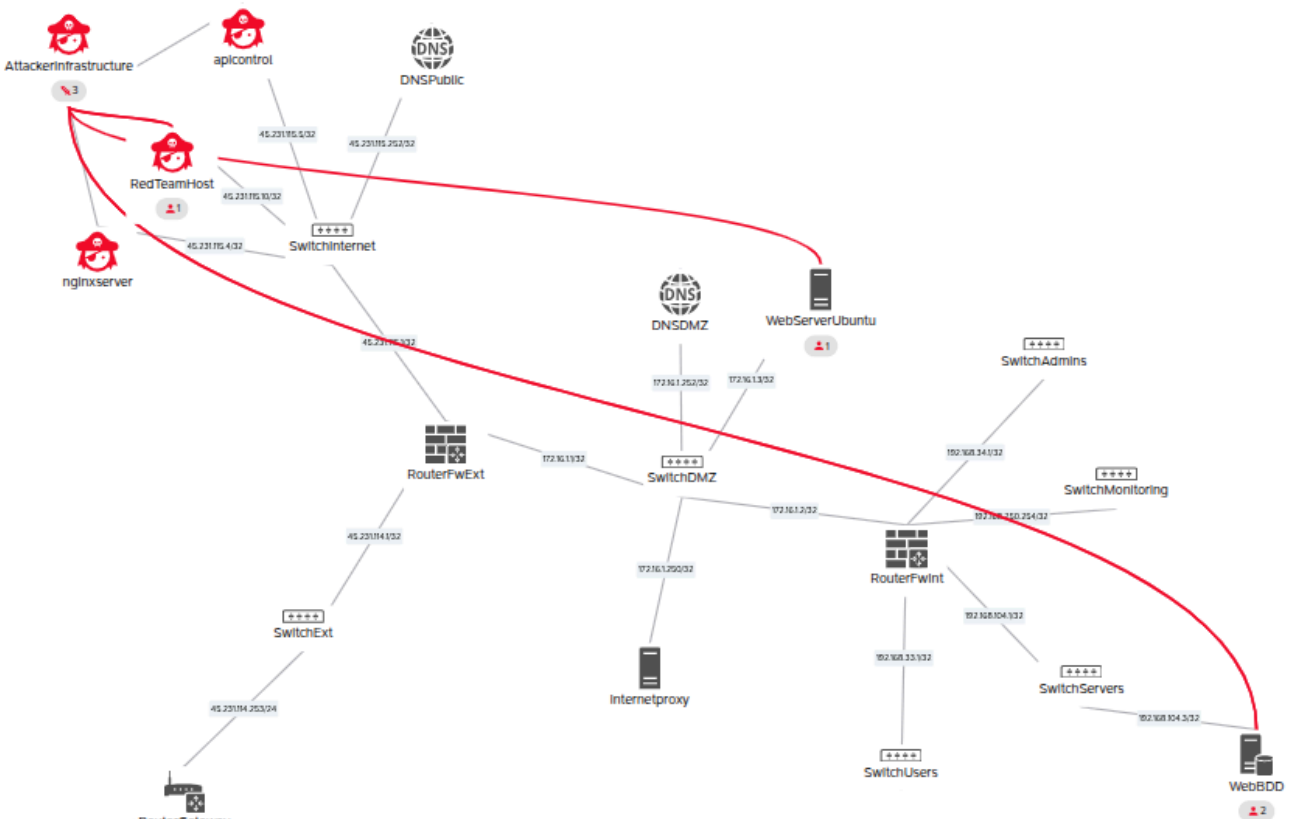
3
hosts crossed

0
lines changed in the scenario

Same behaviour, same footholds. Only the implant differs: CALDERA agent, M&NTIS beacon.

darupel runs of 9 Nov 2026. Rows compacted; the ninth step (ransomware) is in both run logs.

The range deploys the attacker's infrastructure



DEPLOYED ON M&NTIS

Node	IOC
Payload	45.231.115.4 zxfamen.com
C2	45.231.115.5 bbyeenhancedysb.com

Red line: darupel's path, attacker → web → database.

04 Next

Where do we take it, together?

Today, any analyst can write, test and share a campaign

WHAT WORKS TODAY

Write
Your own campaign, in plain YAML, for the threat you choose.

→

Test
Train analysts or challenge your defense, on your range or engine.

→

Share
The same file, to partners and the community.

Proven on darupel: **9/9** steps on M&NTIS and CALDERA, **0** lines changed.

A portable format can be generated

From a recent threat — turn a fresh exploit into a campaign and challenge your defense against what attackers use **now**.

IN USE

Recent exploit
Advisory, CVE, report

→

AI drafts SCEN&R
Steps mapped to atomic tests

→

Validate
Schemas, references, graph

→

Replay
Range or your own lab

From production IT — turn attack paths inferred in a real system into campaigns, to test defense against attacks that fit **your** environment.

NEXT

Production IT
Security data collected

→

Attack paths
From M. Poisson's PhD

→

One SCEN&R file
Per inferred path

→

Replay
Range, or production via a beacon

One portable output: every generator targets every engine.

Attack-path inference: results of Manuel Poisson's recently completed PhD thesis.

Generate once from a fresh threat; every team tests its own defense


```
gitlab-cicd-regexp-rce.yaml · generated, then ✓ validated
scenario:
  id: gitlab-cicd-regexp-rce
  name: GitLab CI/CD regex RCE to repository theft
infra:
  exfil_server:              # free: range supplies
steps:
  - id: exploit_gitlab_cicd_rce     # T1190, CVE-2026-97229
    session: attacker
    procedure: {file: T1190/T1190.yaml, guid: …}
    produces:
      session: {gitlab_shell: {host: GitLabServer}}
  - id: locate_gitlab_secrets       # T1083
  - id: read_db_credentials         # T1552.001
  - id: archive_private_repo        # T1213.003
  - id: exfiltrate_repo_archive     # T1048.003
graph: [ … 4 edges, guarded on extracted state … ]
```

FROM OUR THREAT WATCH

CVE-2026-97229: GitLab CI/CD regex RCE.

CISA KEV 29 Oct · Metasploit 6 Nov

1. **AI drafts** the 5-step kill chain from the advisory
2. **DeepSeek** adapts the real CVE exploit into the scenario
   DeepSeek V4 Flash · open model · $16.54
3. **Validated, run live: 5/5** steps, live RCE → exfil
4. **Share** the same file with every team

> One file per fresh threat: every team tests its own defense, on its own engine.

Toward an open standard: join us

Available today

- Specification 2.x
- JSON Schemas
- Python reference executor
- M&NTIS and CALDERA bindings

We ask you

- Write a binding for your engine or range
- Contribute campaigns
- Challenge the specification

Next for the format

COMING SOON

- A public campaign catalog

EXPLORING

- IOCs from MISP / OpenCTI
- Draft scenarios from published Attack Flows



One campaign file. Any engine.

Write it · **test** it · **share** it.

gitlab.com/scenar/scenar

Frédéric Guihery · Damien Crémilleux · M&NTIS Team, Almond R&D

M&NTIS PLATFORM Almond