PENTESTERRA
SEE THE REAL RISK

BAS MODULE

Breach & Attack Simulation

Scenario-driven attacks mapped to MITRE ATT&CK — the same verification-first methodology as the continuous platform

REAL ATTACK SCENARIOS
CONTROL VALIDATION
CONTINUOUS CYCLES
REAL DEFENSIVE ASSURANCE

Proves whether your existing controls actually stop a real attack scenario, not just whether a vulnerability exists.

ATTACK TODAY. STRONGER TOMORROW.

PENTESTERRA — Live Simulation Platform

- Dashboard
- Vulnerability Management
- Attack Chain
- Breach & Attack Simulation
- Attack Chain Analysis
- DevGuard
- Pentest Scope
- Reports
- Integrations
- Settings

Breach & Attack Simulation

Run realistic adversary scenarios, test your controls, and prove your resilience.

Search scenarios, adversaries, techniques... | Last 30 days

48	312	186	27	285
Scenarios Run	Techniques Tested	Controls Validated	Failed Steps (Control Gaps)	Blocked Steps (Controls Working)
↑ +60%	↑ +42%	↑ +55%	↓ -35%	↑ +28%

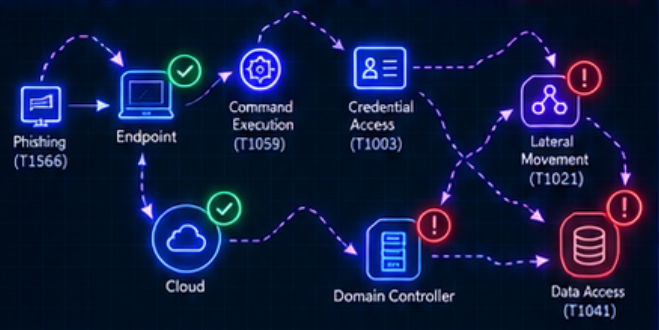
Attack Simulation: Adversary Path

Scenario-driven execution mapped to MITRE ATT&CK

Executed | Blocked | Failed

Initial Access → Execution → Persistence → Privilege Escalation → Lateral Movement → Impact

- APT29 — Stealthy access, Cloud-focused
- APT28 — Hybrid operations, Identity-focused
- Lazarus — Financial targeting, Multi-stage



Control Validation Results

Control Area	Status	Pass Rate
Endpoints (EDR)	Mostly Blocked	92%
Identity (AD)	Gaps Found	68%
Email (SEG)	Blocked	96%
Cloud (AWS/Azure)	Mostly Blocked	89%
Servers (Linux/Windows)	Gaps Found	71%
Network (FW/IDS)	Blocked	94%

Simulation Outcome

HIGH RISK

APT28 – Initial Access to Domain Admin

Phishing led to credential access, followed by lateral movement to a domain controller. Multiple controls failed to detect the activity.

View Full Simulation Report →

Recent Simulation Scenarios

View All

#	Scenario Name	Adversary Template	MITRE ATT&CK	Status	Result	Date
1	Phishing to Domain Admin	APT28 (Hybrid Ops)	T1566 → T1003 → T1021	Completed	Partial Fail	2024-09-14
2	Cloud Persistence	Lazarus (Financial)	T1566 → T1078 → T1098	Completed	Blocked	2024-09-12
3	Ransomware Simulation	APT29 (Cloud Focus)	T1566 → T1059 → T1486	Completed	Partial Fail	2024-09-10
4	Data Exfiltration (Cloud)	Lazarus (Financial)	T1078 → T1048 → T1041	Completed	Blocked	2024-09-08
5	Living-off-the-Land	APT28 (Hybrid Ops)	T1202 → T1059 → T1021	Completed	Partial Fail	2024-09-06

Continuous Simulation Cycle

Next run in 2 days

- Scheduled Re-runs
- Re-compute attack chains
- Track control performance
- Detect new exposure
- Trend over time

What it does

- Scenario-driven attack chains mapped to MITRE ATT&CK tactics/techniques
- Threat template catalogue (APT29, APT28, Lazarus...) — real adversary TTPs, not generic payloads, pulled from MITRE ATT&CK STIX + curated CVEs
- Re-runs on schedule — every cycle re-computes the attack chain engine so exposure is tracked over time, not a point-in-time snapshot
- Same non-destructive, verification-first methodology as network/web pentest — safe in production
- Part of one unified VM/ASM/BAS orchestration core — not a bolted-on separate tool
- Independently licensed — can run standalone or combined with other modules

Why Pentesterra

- BAS is not isolated — results immediately become part of Attack Chain and Vulnerability Management, not a separate report
- In 2026 Gartner grouped BAS + automated pentesting + automated red teaming into AEV — Pentesterra covers all three in one platform, while most vendors sell them separately

> *Same methodology. More confidence. Real resilience.*
> — PENTESTERRA

REAL SCENARIOS
REAL CONTROLS
REAL CONTEXT
REAL INSIGHTS
REAL ADVANTAGE

THE BAS WORKFLOW

1. **Select Scenario** — Choose from built-in or custom templates
2. **Launch Safely** — Non-destructive simulation
3. **Validate Controls** — See what's blocked vs. what gets through
4. **Re-compute Attack Paths** — Updated attack graph and exposure
5. **Track Over Time** — Scheduled re-runs and trending

MITRE ATT&CK Mapped | Threat Templates | Continuous Re-runs | Verification-first | Production-safe | Standalone or Unified | Attack Chain Ready

Validate whether your defenses really stop the scenario. Explore BAS →

REAL SECURITY FOR A MORE RESILIENT TOMORROW

PENTESTERRA

BREACH & ATTACK SIMULATION

Proves Whether Your Controls Actually Stop an Attack

Scenario-driven attacks mapped to MITRE ATT&CK - the same verification-first methodology as the continuous platform. Proves whether your existing controls actually stop a real attack scenario, not just whether a vulnerability exists.

MITRE ATT&CK

Every scenario step mapped to a tactic and technique

Recurring

Runs on a schedule or on demand, not once a year

Verified

A working exploit behind every failed control

WHY NOW

You bought EDR, a SIEM, and a firewall upgrade this year - nobody has actually tested whether they stop a real attack. A control that looks correctly configured on paper and a control that actually blocks a real technique are not the same thing - and an incident is a bad time to learn the difference.

HOW IT WORKS

Scenario-Driven Kill Chains

Each simulation runs a full attack scenario - initial access, execution, privilege escalation, lateral movement, impact - the way a real intrusion unfolds, with every step mapped to an ATT&CK tactic and technique.

→ Real adversary templates: APT29 (Cozy Bear), APT28 (Fancy Bear), Lazarus Group and more, pulled from MITRE ATT&CK + curated CVEs

→ Recurring or on-demand simulation cycles

→ Internal, external, and hybrid scenarios

Security Control Validation

The point of a simulation is not the finding - it is the answer to “did the control stop it?” Pentesterra runs the scenario against your existing controls and reports which held, which failed, and where you've drifted.

→ Preventive and detective control coverage per scenario

→ Control drift measured between assessments

→ Gaps ranked by exposure, not by scenario count

A Failed Control Comes With a Working Exploit

Simulation-only tools tell you a control did not fire. Pentesterra also verifies the underlying vulnerability with a real, non-destructive exploit.

→ Non-destructive exploit verification behind each failed control

→ Reproduction steps and evidence attached to the finding

→ Isolated staging and production scopes, human-in-the-loop option

Runs Alongside Scanning and Pentest Cycles

BAS is not isolated - results immediately become part of Attack Chain and Vulnerability Management, not a separate report.

→ Shares scope, assets, and findings with the other modules

→ No separate agent fleet to deploy for simulations

→ Feeds attack chain analysis as verified path steps

WHY PENTESTERRA

BAS, automated pentesting, and exploit verification run on the same platform, sharing scope, assets, and findings - most vendors sell these as separate products with separate agents and separate reports to reconcile.

FREQUENTLY ASKED QUESTIONS

What is breach and attack simulation?

BAS runs safe, scripted attack scenarios against your live environment to test whether your security controls actually detect and stop them. It runs continuously or on demand and measures how control effectiveness changes over time.

How is BAS different from a vulnerability scanner?

A scanner enumerates weaknesses. BAS executes a full attack path and reports whether your controls held. Pentesterra combines both: the simulation shows the control gap, and exploit verification proves the vulnerability behind it is real and reachable.

Is it safe to run against production?

Yes. Simulations and exploit verification are non-destructive by default - no data deletion, no denial-of-service payloads, and nothing that reads or moves confidential data. Staging and production are isolated, and a human-in-the-loop mode can gate active exploitation behind analyst approval.

Does BAS replace a red-team engagement?

It complements one. BAS continuously validates whether your controls stop known adversary techniques on a schedule you set; a red team engagement is still the right tool for a fully custom, human-led scenario. Many teams run BAS between red-team cycles to catch control drift in the meantime.

Validate whether your defenses really stop the scenario

Run a real adversary emulation against your own environment.

info@pentesterra.com
pentesterra.com/breach-attack-simulation