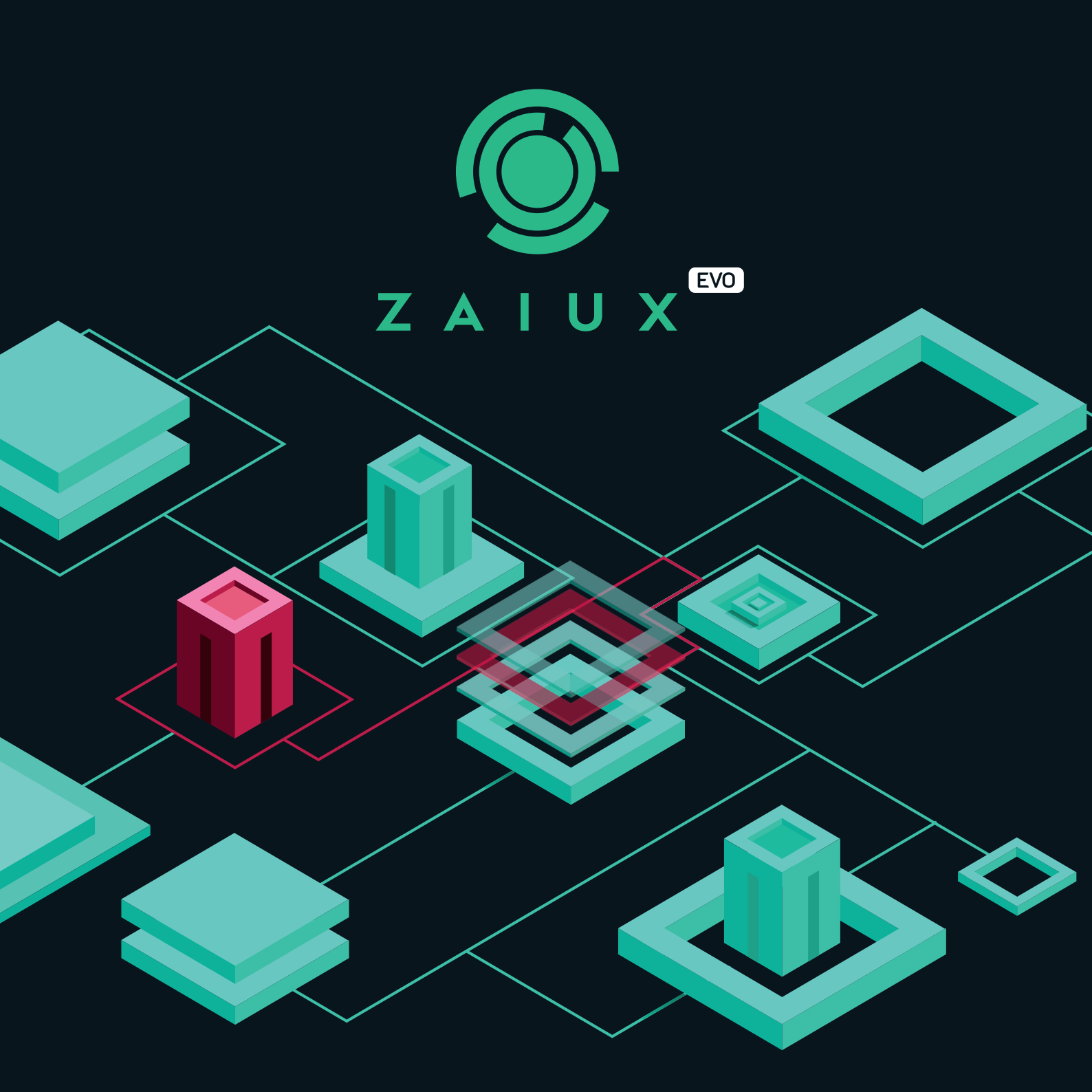
ZAIUX EVO

The AI automated Breach & Attack Simulation Solution

— Designed for MSSPs —


ZAIUX
EVO

The most suitable Cloud BAS solution for your infrastructure

ZAIUX® Evo offers a sophisticated Breach & Attack Simulation in a Microsoft Active Directory environment, employing Artificial Intelligence to analyse network behaviour and allocate resources thanks to mathematical optimization, thus executing automated hacking processes and finding security flaws in the target network.

Our BAS emulates a real intrusion: the whole defensive security toolchain is validated against a targeted attack from the outside, pointing out its blind spots both in local domain Privilege Escalation and in protection from data exfiltration.

Everything from a centralized MSSP Cloud Portal.

ZAIUX EVO

ZAIUX® Evo the AI automated cloud BAS solution

An intelligent solution that, thanks to our DPZR™ cloud engine, verifies the resilience of IT infrastructures against internal threats and generates Remediation Plans referring to the MITRE ATT&CK® framework, thus reducing execution time by more than 50% compared to a traditional Penetration Test.

How does it work?

ZAIUX® Evo makes it possible to perform a complete BAS in a Microsoft Active Directory environment with a “thinking” software, leveraging an always up-to-date range of the most modern and advanced hacking techniques, executed in stealth mode emulating a human approach. Automation is managed by the DPZR™ cloud engine that includes Machine Learning algorithms specially conceived by our expert team to emulate human intelligence, breaking the time barrier of manual execution.

ZAIUX® Evo executes sophisticated attack techniques, among which:

- EDR/XDR Evasion out-of-the-box
  - Dynamic SSN Resolution on the fly
  - Indirect System Calls
  - Unhook EDR Userland Hooks
  - Regularly updated custom Loaders & Implants
  - Sleep Obfuscation
  - Thread Stack Spoofing
  - Patchless AMSI & ETW Evasion via Hardware-Breakpoints
- C2 communication via HTTPS + SMB Pivoting
- Lateral Movement
- Privilege Escalation
- In-Process .NET Assembly execution
- Active Directory misconfiguration leveraging

ZAIUX® Evo
a unique and essential solution

Ease of use

Configure and monitor a BAS in a few simple steps, directly from the MSSP portal, without installing any agents on the endpoints.

A Virtual Red Team

Execute orchestrated techniques against weaknesses in the target network, obtaining better performances compared to a manual Penetration Test.

No false positives

Gain insight on the real critical spots, concretely exploitable by an attacker, thus prioritizing your remedial actions.

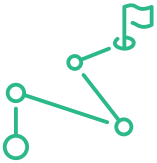
Optimized reporting

Receive a clear and concise report, which shows the attacks successfully performed, referring to the MITRE ATT&CK framework.

How we use Artificial Intelligence with ZAIUX® Evo

Dynamic analysis

Thanks to the proprietary Machine Learning algorithms integrated in the DPZR™ cloud engine, ZAIUX® Evo learns user behaviour patterns in real time and schedules techniques in an ad-hoc fashion, like a human attacker would.



Attack planning

By using optimization and heuristic search techniques, ZAIUX® Evo autonomously orchestrates context-aware attacks, thus surpassing in efficiency the human-based approach without sacrificing efficacy.

Ethical Hacking, Artificial Intelligence and Machine Learning cleverly combined by an expert team who offers cutting edge software solutions and services to mitigate Cyber Risk.

pikered

ZAIUX® Evo è una soluzione “Made in Italy”
sviluppata da Pikered | Milano | pikered.com