GATR

Gathering Advanced Tactical Resources

Your EDR, performing advanced forensics with precision and at scale.

By seamlessly integrating with Endpoint Detection and Response (EDR) systems, GATR revolutionizes DFIR (Digital Forensics and Incident Response) capabilities, allowing professionals to dig deep into devices without the need of additional tools or physical access.

- No need for another tool setup; GATR directly integrates in your EDR solution.
- Zero code approach; no need for developing or maintaining code by your team.
- Continuous Enhancement; GATR automatically updates to incorporate the latest forensic methodologies and tools.
- Scalable collection architecture; Collect a single forensic image or take a snapshot of your full fleet, in a few steps.
- Automatic artifact processing; Get an already populated supertimeline alongside the collected raw data

Deploy with ease

GATR comes with a preset of collection configuration and allows you to create custom ones.

GATR will detect the target environment and pick the right tool automatically.

GATR setup is effortless.

Collect at scale

GATR distributed architecture allows its users to launch collection of forensic images whether targeting a single device or thousands at the same time.

GATR adapt itself to the operating condition of the targeted assets applying different error recovery technique to ensure the highest rate of success with the fewest manual steps involved.

Integrate and consume

GATR produce standard format recognized by the DFIR community such as PLASO timelines.

GATR can be integrated with other tools via its API.

www.cyberhorses.io

Zugerstrasse 72

6340 Baar, Switzerland

info@defcom.io