



RED TEAM · ADVERSARY SIMULATION · PURPLE TEAM

Authorized adversaries. Measurable defense.

We emulate real adversaries – with written authorization, inside a signed scope – and measure what your defenders saw. Every engagement ends in detections you can prove and fixes you can assign.

01 SERVICES

- ▶ **Red team adversarial simulation**
Objective-based, threat-informed campaigns.
- ▶ **Assumed breach**
Start from an authorized foothold; measure how far and how fast.
- ▶ **Purple team**
Execute, observe, tune and re-run with your SOC in the room.
- ▶ **External / internal assessment**
Prioritized, actionable findings.
- ▶ **Social engineering (authorized)**
Written approval plus HR / legal sign-off.
- ▶ **Wireless / RF assessment**
Authorized testing of in-scope infrastructure.
- ▶ **Reporting & detection validation**
ATT&CK mapping, coverage scorecards, retest.

02 PROCESS

- 01 **Scope & RoE** objectives, threat model, in/out of scope, stop word, sign-off
- 02 **Recon** passive intelligence gathering and planning
- 03 **Emulation** controlled, authorized adversary behaviour
- 04 **Objective** simulated markers only; detection measured at every step
- 05 **Reporting** exec summary, narrative, ATT&CK heatmap, owners
- 06 **Debrief & retest** purple-team walkthrough, tuning, validation

03 ENGAGEMENT TYPES

ENGAGEMENT	ANSWERS THE QUESTION	BEST FOR	PRICING
Scoping call	What should we test first, and why?	Everyone, before anything else	Free · 30 min
Assumed breach	Once someone is in, how far do they get – and do we notice?	First red team; post-compliance programs	Contact for quote
Purple-team sprint	Do our detections actually fire? Can we tune them now?	SOCs with new tooling or gaps to close	Contact for quote
Objective-based red team	Could a realistic adversary reach what matters most?	Mature programs; board-level assurance	Contact for quote
Assessment + retest	What's exposed, what's fixed, and can we prove it?	External / internal / wireless scope	Contact for quote

04 PRINCIPLES

- ▶ **Authorized only.** Signed by an accountable owner. No signature, no activity.
- ▶ **Safety first.** Non-destructive by default, named deconfliction contacts, an emergency stop word either side can use.
- ▶ **Detection validation.** Every simulated action is mapped to ATT&CK and marked detected, alerted, contained or missed.
- ▶ **AI is advisory only.** It helps analyze and draft; a human authorizes every active action.
- ▶ **Evidence handled carefully** and destroyed on schedule.

05 CONTACT

Michael M Schlosser (0gr3n) · Senior Offensive Security Consultant

Email 0gr3n1nj4@pm.me

Web <https://0gr3security.com/>

X [@0gr3n1nj4](https://twitter.com/0gr3n1nj4)

LinkedIn [linkedin.com/in/michael-m-schlosser-0gr3](https://www.linkedin.com/in/michael-m-schlosser-0gr3)

PGP 0A23 D92A 531E F397 A51A 920B 363D 0146 7053 3B40 · 0gr3security.com/pgp.asc

Location US East · remote engagements worldwide

Bring your objectives, constraints and timeline. We reply with a scoping call.