CENTRIC CONSULTING PRESENTS

KNOCK OUT HACKERS

WITH PURPLE TEAM EXERCISES

YOUR CYBER FIGHTERS

BLUE TEAM
The First Responders

Defense: 100%

Goal: Provide security monitoring and detection across different systems, networks and applications

Job titles: Security analysts, security engineers, incident response analysts, risk analysts and more

RED TEAM
The Attackers

Offense: 100%

Goal: Proactively simulate real-world attacks to identify vulnerabilities and security gaps

Job titles: Penetration testers, ethical hackers and more

PURPLE TEAM
The Tag Team

Offense: 50%

Defense: 50%

Goal: Bridge the gap between cybersecurity's respective offense and defense sides

Job titles: A combination of blue team and red team titles

TRAIN FOR YOUR CYBER FIGHT

DAILY DRILLS → Monthly Automated Testing

KEY POINTS:

- Scalability and coverage across the full MITRE ATT&CK matrix
- Repeatability for regression testing and detection tuning
- Cost efficiency through reduced labor demands
- Fast feedback loops when integrated with existing telemetry

EACH MONTHLY CYCLE SHOULD INCLUDE:

- Tool-led simulations across key TTP categories, such as credential access, execution, privilege escalation and more
- Detection gap analysis with a focus on improving rule fidelity and reducing false positives
- Detection rule tuning—for example, custom Sigma, KQL, or Sentinel logic—based on test outcomes
- Tracking key metrics like MTTD, telemetry coverage, and detection source, like EDR versus SIEM

SPARRING SESSIONS → Biannual Manual Deep Dives

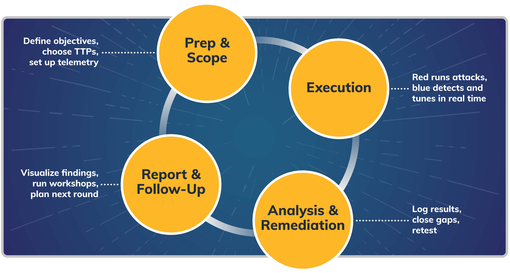
KEY POINTS:

- Realistic adversary simulation that mimics advanced threat actors
- Deeper insights into EDR bypasses and telemetry weak spots
- Adaptive engagement in which testers pivot based on detection patterns
- Hands-on collaboration that strengthens red and blue team skills

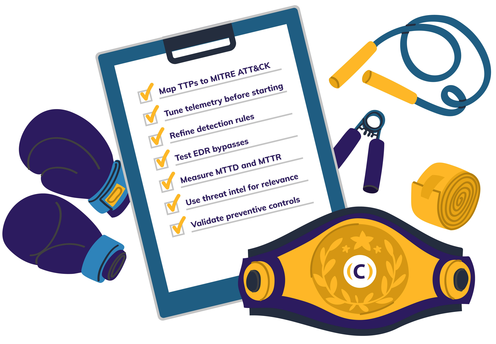
EACH ENGAGEMENT SHOULD INCLUDE:

- Custom-crafted attack chains, including techniques like process hollowing, cross-domain persistence, and EDR bypasses through direct system calls
- Blue team monitoring in real time using live telemetry from SIEMs, EDRs, and endpoint logs to assess detection and triage performance
- Tabletop components, such as injecting alerts into the SOC to simulate incident response workflows
- Post exercise reporting, including detailed findings, vulnerability documentation, and prioritized remediation recommendations

BUILD YOUR DEFENSES

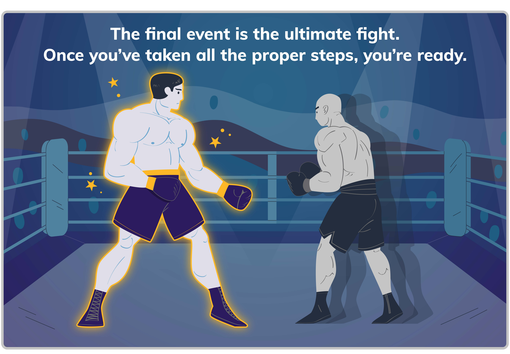


YOUR FINAL CHECKLIST



THE MAIN EVENT

The final event is the ultimate fight.
Once you've taken all the proper steps, you're ready.



Win the championship with the right sparring partner.
Contact us to build your purple team hybrid program.

((CENTRIC))

CentricConsulting.com