OFFENSIVE SECURITY

Purple Team Engagements

Turn Detection Gaps Into Validated Detection Capabilities

Detection improves fastest when offensive and defensive teams test, observe, and build together.

01 — THE CHALLENGE

Offensive and defensive security teams often operate in separate cycles. Red teams produce findings. SOC teams build queries. Detection engineers tune controls. The feedback loop is slow and frequently incomplete.

As a result, detection gaps persist and teams learn from actual incidents rather than controlled exercises.

02 — WHY ARCTIQ

Arctiq Purple Team Engagements place offensive and defensive teams in the same room.

We execute adversary techniques aligned to the threats the client faces. SOC and detection engineering teams observe what fires, what does not, and how analysts respond. Detection logic is built, tuned, and validated in real time.

> The primary output is not a report. It is a measurably stronger detection stack, improved SOC workflow, and a defensive team that has practiced against realistic techniques.

03 — ADVISORY CAPABILITIES

- Controlled MITRE ATT&CK technique execution
- EDR response validation
- SIEM correlation testing
- SOC analyst response measurement
- Playbook and automation validation
- ATT&CK coverage mapping
- Sigma, KQL, SPL, and EQL detection content
- CrowdStrike, SentinelOne, Defender for Endpoint, and Carbon Black tuning
- Microsoft Sentinel, Splunk, Google SecOps, and Elastic detection tuning
- Identity telemetry validation
- Before-and-after detection coverage measurement

DETECTION STACK

MITRE ATT&CK · Sigma · KQL · SPL · CrowdStrike · Microsoft Sentinel · Splunk

04 — BUSINESS OUTCOMES

Organizations gain:

- ✓ New, validated detections in production
- ✓ Measurable improvement in ATT&CK coverage
- ✓ Better-tuned EDR and SIEM platforms
- ✓ Stronger SOC workflows
- ✓ Improved coordination between offensive and defensive teams
- ✓ A documented before-and-after view of detection maturity

05 — WHY IT MATTERS

Detection capabilities improve when teams test them against realistic adversary behavior. Arctiq helps organizations turn offensive techniques into validated defensive improvements.

Run a purple team engagement →

www.arctiq.com