

Build & prove technical team readiness with Dynamic Threat Ranges

Exercise your defensive, offensive, and developer teams against real attacks, and prove they can perform under pressure.

Guided training tells you who checked the box. It doesn't prove your team can do the job when the alert is ambiguous, the deadline is real, and nobody is confirming they're on the right track.

Dynamic Threat Ranges are built for teams who are past that stage. We drop technical teams into on-demand, real enterprise environments and run genuine, full-chain attacks against them. Your teams do the job with real tools, submit findings based on the evidence they uncover, and get their results in the debrief afterwards.

Set the scenario and environment and have teams work against the clock to complete the exercise. Every session pits your teams against a full-chain attack using their own tools, then hands you objective numbers and framework-mapped evidence for your next board or audit review.

BUILT FOR TEAMS
ACROSS THE
SECURITY LIFECYCLE:

DEFENSIVE SECURITY TEAMS

SOC analysts, threat hunters, and incident responders exercise in your SIEM: Splunk, Microsoft Sentinel, Elastic, or CrowdStrike Falcon Next-Gen SIEM.

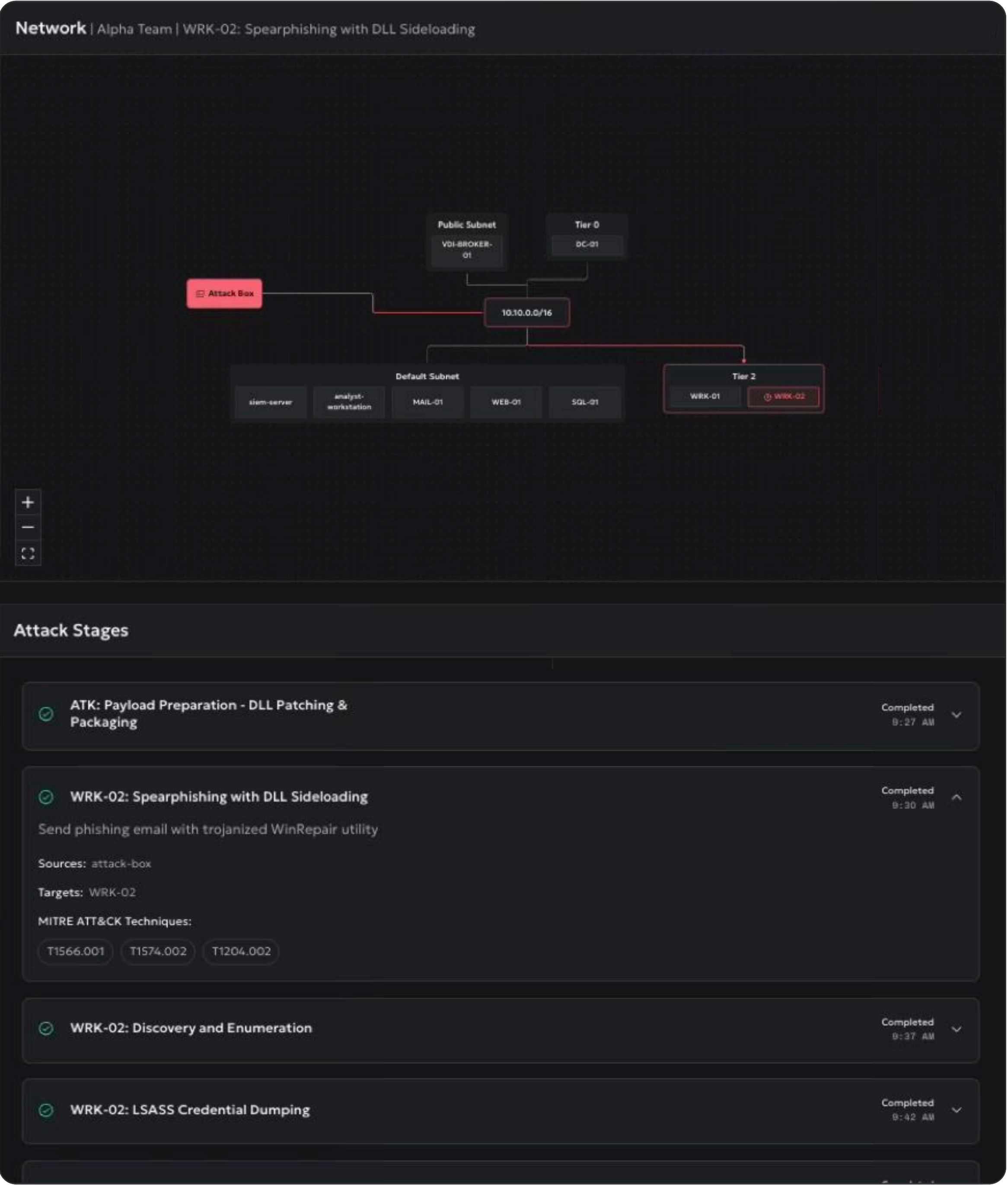


OFFENSIVE SECURITY TEAMS

Red teamers and penetration testers work a black-box engagement from a dedicated Kali attack box and offensive AI frameworks inside the target network.

REMEDIATION TEAMS

Developers and application security engineers fix real vulnerabilities leveraging AI in a running application, in a browser-based IDE with a live repository and ticket board.



Four ways into the same attack

Each exercise drops your team in at a different stage, with metrics that prove resilience.

01 THREAT HUNTING

The attack is running now.
Your team starts from threat intelligence and hunts for indicators across the environment to determine if something is there.

Measured by:

- Time to Detect
- Tasks Completed
- Time to Escalate
- Accuracy

02 INCIDENT RESPONSE

The attack is over.
Your team must reconstruct the timeline from the evidence the adversary left behind.

Measured by:

- Time to Investigate
- Accuracy
- Tasks Completed

03 DEVELOPER

There is an issue in the code base.
Your team starts from a ticket board of real vulnerabilities in a running application and uses AI to fix them until tests pass.

Measured by:

- Time to Complete
- Accuracy
- Tasks Completed
- Token Spend

04 RED TEAM

Your team is the attack.
They start from a set of targets, a deadline, and limited inside knowledge, with an aim to compromise a set of machines.

Measured by:

- Time to Complete
- Accuracy
- Tasks Completed
- Token Spend

FACILITATORS SELECT THE SCENARIO AND THE ENVIRONMENT AT SETUP

Up to five teams of 15 can run the same scenario at once, in parallel or head-to-head, with scores held back until the debrief.

Why enterprise organizations trust Immersive

Immersive provides continuous, empirical evidence to verify that an organization's, people, workflows, and AI agents hold up under pressure. Through live-fire cyber ranges, simulations, and deep capability analytics, Immersive enables the world's largest organizations to accelerate digital innovation securely.

 #1 In The Forrester Wave™ 2026 

 Trusted By 30%+ Of The Fortune 100 

