



LCSG

LITCHFIELD CYBER SECURITY GROUP

— DISCOVER. EXPLOIT. DEMONSTRATE. —

RED TEAM OPERATIONS

DISCOVER. EXPLOIT. DEMONSTRATE.

Objective-driven adversary simulation designed to determine how far a capable attacker can progress within an authorized environment.

REALISTIC OBJECTIVES. CONTROLLED EXECUTION. MEASURABLE IMPACT.

LCSG combines experienced human operators, threat-informed methodology and AI-accelerated analysis to test attack paths across technology, identity and people.

Test the Organization, Not Just the Vulnerability

A red team engagement begins with an objective rather than a vulnerability list. The operation is designed to determine whether an authorized adversary can establish access, expand control, cross trust boundaries and reach systems, data or business functions that matter.

OBJECTIVE DRIVEN

Engagements are built around agreed outcomes such as reaching a protected system, obtaining defined access or demonstrating control of a critical business process.

ATTACK PATH FOCUSED

Individual weaknesses are combined where appropriate to model how a real compromise can progress through multiple layers of the environment.

ADVERSARY MINDED

Operators adapt to what the environment reveals instead of following a fixed sequence of test cases.

CONTROLLED & AUTHORIZED

Rules of engagement, safety constraints, communications and stop conditions are established before operations begin.

The question is not simply 'what is vulnerable?' It is 'what can an adversary actually achieve?'

Multiple Attack Surfaces. One Objective.

Red team operations can cross technology boundaries when authorized. Scope is tailored to the client, threat model and objective rather than forcing every engagement into the same playbook.

EXTERNAL ATTACK SURFACE Internet-facing applications, APIs, services, cloud resources and exposed infrastructure that may provide an initial foothold.	APPLICATION & API EXPLOITATION Authentication, authorization, business logic and implementation weaknesses used to obtain access or expand control.
IDENTITY & ACCESS Credentials, tokens, federation, privilege relationships, role boundaries and identity-driven paths through the environment.	CLOUD & INFRASTRUCTURE Cloud services, network trust, administrative interfaces, segmentation and infrastructure relationships relevant to the objective.
SOCIAL ENGINEERING Where explicitly authorized, controlled human-targeted techniques can be incorporated to evaluate susceptibility and access pathways.	POST-COMPROMISE PROGRESSION Privilege escalation, lateral movement, persistence simulation and movement toward the agreed objective within defined rules.

MITRE ATT&CK; as a Common Language

LCSG can use MITRE ATT&CK; to structure adversary behaviors, communicate tactics and techniques, and map operational activity to a recognized threat-informed framework. MITRE describes ATT&CK; as a common language and framework that red teams can use to emulate specific threats and plan operations.

01 DEFINE THE OBJECTIVE

Agree the target outcome, scope, assumptions, safety controls, communications and evidence requirements.

02 MODEL THE ADVERSARY

Select relevant threat behaviors and techniques based on the environment, threat intelligence and engagement goals.

03 ESTABLISH ACCESS

Identify and exercise authorized initial-access paths while maintaining operational control and minimizing unnecessary impact.

04 PROGRESS

Adapt based on discovered access, privileges, trust relationships and defensive response; chain techniques where needed.

05 ACHIEVE & DEMONSTRATE

Reach the agreed objective or establish the point at which controls prevent further progression, preserving evidence.

06 DEBRIEF & IMPROVE

Explain the attack path, map relevant behaviors, identify control gaps and provide practical recommendations.

AI Supports the Operator - It Does Not Replace One

LCSG embraces AI where it improves speed, correlation and analytical reach. Red team decisions remain human-led because operational judgement, context, creativity and restraint determine whether an engagement is both useful and safe.

AI CAN ACCELERATE

- Attack-surface and data correlation
- Analysis of large technical datasets
- Research and hypothesis generation
- Protocol, API and application analysis
- Operational note and evidence organization

EXPERIENCE DIRECTS

- Objective and strategy selection
- Choosing meaningful attack paths
- Adapting to unexpected behavior
- Controlled exploitation decisions
- Determining when impact is sufficiently demonstrated

25+ YEARS OF OFFENSIVE SECURITY EXPERIENCE

Modern AI can accelerate the work. Experience determines which paths matter, how far to go and what the result means.

Realistic Does Not Mean Uncontrolled

Red team operations are designed to create realistic pressure without introducing unmanaged business risk. Engagement boundaries are agreed in advance and can be adjusted to the sensitivity of the environment.

AUTHORIZATION Written authorization, scope and designated points of contact before testing begins.	SAFETY CONTROLS Defined prohibited actions, production constraints, sensitive systems and escalation procedures.
COMMUNICATION Agreed communication cadence, emergency contacts and mechanisms for rapidly stopping or modifying activity.	DATA HANDLING Controlled collection, storage and disposal of engagement data and evidence.
DECONFLICTION Processes for distinguishing authorized activity from genuine malicious activity when required.	OPERATIONAL DISCRETION Testing can be conducted with varying levels of defender awareness depending on the engagement objective.

DELIVERABLES

Show the Path. Explain the Impact.

A red team report should reconstruct the operation so technical teams and leadership can understand how the objective was reached, which controls succeeded or failed, and where investment will materially reduce risk.

EXECUTIVE NARRATIVE A concise account of the operation, objective, outcome and major business implications.	ATTACK PATH A chronological reconstruction of initial access, privilege changes, movement and the sequence leading toward the objective.
TECHNICAL EVIDENCE Supporting evidence for significant actions and weaknesses demonstrated during the engagement.	ATT&CK; MAPPING Where appropriate, observed or emulated behaviors mapped to relevant MITRE ATT&CK; tactics and techniques.
CONTROL OBSERVATIONS What prevented, detected, delayed or failed to stop progression, without turning the report into a generic defensive audit.	PRIORITIZED ACTIONS Practical recommendations focused on breaking meaningful attack paths and reducing the likelihood or impact of similar compromise.

A successful red team engagement produces more than findings - it shows how compromise unfolds.



DISCOVER. EXPLOIT. DEMONSTRATE.

Objective-driven red team operations backed by decades of offensive security and vulnerability research experience.

RED TEAM OPERATIONS | PENETRATION TESTING | VULNERABILITY RESEARCH

M&A; CYBER DUE DILIGENCE | GOVERNMENT CYBER CAPABILITIES

LCSG.US

LITCHFIELD CYBER SECURITY GROUP