ARANCIA

STRENGTHENING SECURITY THROUGH STRATEGIC SIMULATION

RED TEAM SERVICES

Arancia specializes in Red Team Exercises, advanced simulations that go beyond traditional security assessments. Our team of elite cybersecurity professionals replicates real-world attacks to uncover vulnerabilities that might evade detection through regular testing.

WHAT IS ARANCIA'S RED-TEAMING?

"Red Teaming" is a term that's used frequently within the cybersecurity space. Its meaning and purpose have evolved, often being misunderstood due to vendor marketing and compliance requirement confusion. Red Teaming is the process of using tactics, techniques, and procedures (TTPs) to emulate a real-world threat, aiming to measure the effectiveness of the people, processes, and technologies used to defend an environment. Red teams provide an adversarial perspective, challenging organizational assumptions about security, such as "we're secure because we patch" or "technology Y would stop that." By doing so, red teams identify areas for improvement in an organization's operational defense.

WHY CHOOSE US?

Expertise & Experience

Our experienced cybersecurity team specializes in simulating real-world attacks and identifying vulnerabilities missed by traditional assessments.

Comprehensive Methodology

We follow industry standards aligned with the MITRE ATT&CK framework for comprehensive security assessments, including threat hunting, social engineering, and Dark Web evaluations.

Validation of Blue Team Readiness

Our exercises not only assess technical vulnerabilities but also validate the readiness of your IT and security operations team (Blue Team) to detect and respond to sophisticated threats.

Realistic Simulations

We simulate cyber-attacks to test vulnerabilities thoroughly, covering reconnaissance, planning, and execution phases for external breaches and insider threats.

Actionable Insights & Reporting

You get detailed reports with prioritized recommendations to enhance security defenses. Reports focus on critical vulnerabilities and offer a roadmap for mitigation.

Proven Track Record

Arancia offers tailored Red Team Exercises to enhance cybersecurity resilience for organizations, with a refined methodology from years of experience.

RED TEAM GOALS

ACCESS TO COMPANY SYSTEMS:
Simulate breaches to gain access to critical systems and data.

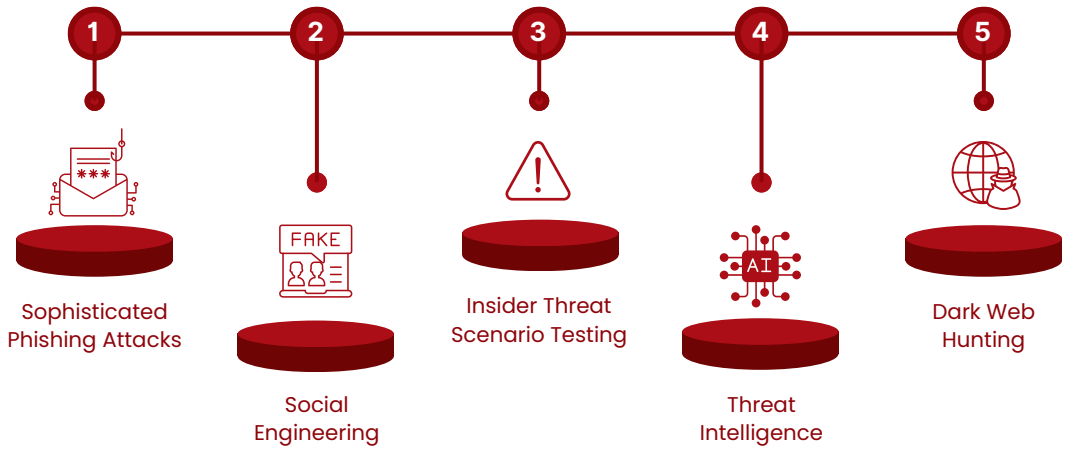
COMPROMISE HIGH-VALUE TARGETS
Target and attempt to compromise crucial assets within the organization.

COMPREHENSIVE ASSESSMENT
Test the entire infrastructure, including physical and digital components, to identify vulnerabilities.

RED TEAM EXERCISE APPROACH & METHODOLOGY

Arancia's Red Team Exercise approach aims to gain access to systems using any means necessary. This validates Blue Team readiness and involves real-life exercises by our elite cyber professionals.

Security Tests offered include:



Our Approach

- **Reconnaissance:** Impartial assessment to identify access points and vulnerabilities.
- **Planning and Preparation:** Thorough vulnerability scans and data gathering.
- **Execution:** Realistic attack simulations across networks and applications.
- **Reporting:** Detailed reports with prioritized vulnerabilities and mitigation strategies.

Arancia's Red Team employs a robust methodology involving:

1	2	3	4	5
INITIAL COMPROMISE	**ESTABLISH FOOTHOLD**	**ESCALATE PRIVILEGES**	**PERFORMANCE AND CONTROL**	**MISSION COMPLETION**
Gaining access to target systems.	Ensuring persistent access for further exploration.	Acquiring higher-level permissions to penetrate deeper.	Moving horizontally across the network to expand influence.	Achieving objectives without damaging assets.

ARANCIA

Arancia's Red Team Exercise Services are tailored to fortify organizational resilience against cyber threats through rigorous testing and strategic insights. Contact us today to safeguard your digital assets with confidence.