NodeRisk

DATASHEET

Red Team Operations

Why NodeRisk

NodeRisk brings cutting-edge cybersecurity expertise, grounded in experience with advanced threat landscapes and evolving tactics, techniques, and procedures (TTPs). With NodeRisk's experts simulating a full-spectrum adversary, you receive a unique, insight-driven assessment that reflects current attacker behaviors and methods.

Service Overview

The **Red Team Assessment** offers a realistic, boundary-pushing evaluation within your operational environment. Our team aligns with your organizational priorities to define strategic objectives and employ stealthy, active threat techniques to emulate real-world threat actors. This approach enables a rigorous evaluation of your internal team's detection and response capabilities.

Objectives

- Exfiltrate sensitive emails from high-profile accounts.
- Infiltrate isolated network segments with critical or sensitive data.
- Compromise key operational technology like IoT, medical, or industrial devices.

Deliverables

- **Executive Summary:** High-level insights for leadership with strategic findings.
- **Technical Report:** Step-by-step methodology and detailed findings for your technical teams.
- **Risk Analysis:** Context-driven analysis of vulnerabilities with actionable, priority-based recommendations.
- **Improvement Recommendations:** Tactical (immediate) and strategic (long-term) recommendations for enhancing security posture.

Methodology

The assessment begins by aligning on objectives and selecting knowledge constraints (limited or complete environmental familiarity). Leveraging extensive industry experience, NodeRisk structures each engagement to address significant risks, simulating adversary tactics to drive meaningful insights.

Phases of Engagement

1. **Reconnaissance:** Conduct comprehensive intelligence gathering using proprietary sources and open-source techniques.
2. **Initial Compromise:** Gain access via targeted vulnerabilities or social engineering, applying realistic attack scenarios.
3. **Privilege Escalation and Persistence:** Establish command and control structures to mirror real-world persistence techniques.
4. **Objective Execution:** Achieve objectives with minimal disruption, preserving business operations while delivering actionable findings.