ARANCIA

STRENGTHEN YOUR DEFENSES: PREPARE, PROTECT, PREVAIL

RANSOMWARE SIMULATIONS AND COMPROMISE ASSESSMENTS

In today's digital landscape, ransomware poses a significant threat, blocking access to critical systems and demanding hefty ransoms for decryption keys. These attacks can lead to severe financial losses, data breaches, and operational disruptions.

Arancia's Ransomware Simulation replicates key aspects of a ransomware attack to enhance your organization's preparedness and response without risking data loss. Our Compromise Assessments thoroughly examine your IT environment to uncover hidden threats and vulnerabilities by analyzing network traffic, system logs, and other indicators of compromise.

150% In 2023, ransomware attacks increased by 150%, with businesses losing an average of $133,000 per incident.

60% 60% of small businesses hit by ransomware close within six months.

70% 70% of ransomware attacks include threats of data leakage (double extortion).

ARANCIA'S RANSOMWARE SIMULATIONS AND COMPROMISE ASSESSMENTS

Arancia offers comprehensive Ransomware Simulations and Compromise Assessments designed to:

1. Simulate real-world ransomware infections.
2. Test your organization's defenses and response strategies.
3. Identify vulnerabilities and provide actionable recommendations.

WHY CHOOSE US?

Expertise

Our team comprises seasoned cybersecurity professionals with extensive experience in dealing with ransomware threats.

Realism

We replicate authentic ransomware tactics, techniques, and procedures (TTPs) to provide a realistic training environment.

Customization

Tailored simulations that align with your specific organizational needs and security posture.

Actionable Insights

Detailed reports with practical recommendations to enhance your cybersecurity defenses.

METHODOLOGY

Preparation

- Initial online meeting to outline objectives, rules, and use cases.
- Define requirements and schedule execution dates.

Execution

- Conducted via online meetings with shared screens.
- Client analysts execute simulated ransomware techniques under our guidance.
- Sessions may be split based on the number of selected targets.

Monitoring

- Real-time monitoring of defense solution dashboards during simulations.
- Check for alerts or logs triggered by simulated attacks.

Reporting

- A comprehensive report detailing outcomes for each use case.
- Recommendations based on test results, tailored to your company's needs.

ARANCIA

KEY STEPS IN THE SIMULATION:

Identify and Isolate:

Detect ransomware signs and isolate affected systems.

Observe SOC Detection:

Monitor Security Operations Center (SOC) responses.

Observe Endpoint Detection:

Evaluate endpoint security effectiveness.

Observe Incident Response:

Assess the incident response process.

SIMULATION USE CASES

Command and Control (C&C)

Demonstrates ransomware communication with attacker servers.

Encryption

Simulates file encryption without actual data risk.

Exfiltration

Shows potential data extraction and associated risks.

Keylogging

Tests for detection of keystroke recording software.

Persistence

We are committed to providing innovative solutions that will help create a better tomorrow for everyone.

ARANCIA

Strengthen your cybersecurity defenses today. Contact Arancia to schedule your Ransomware Simulation and Compromise Assessment. By choosing Arancia, you're not just preparing for an attack—you're fortifying your organization against one of the most pervasive threats in the cyber landscape. Let's make your defenses as dynamic and robust as the threats you face.