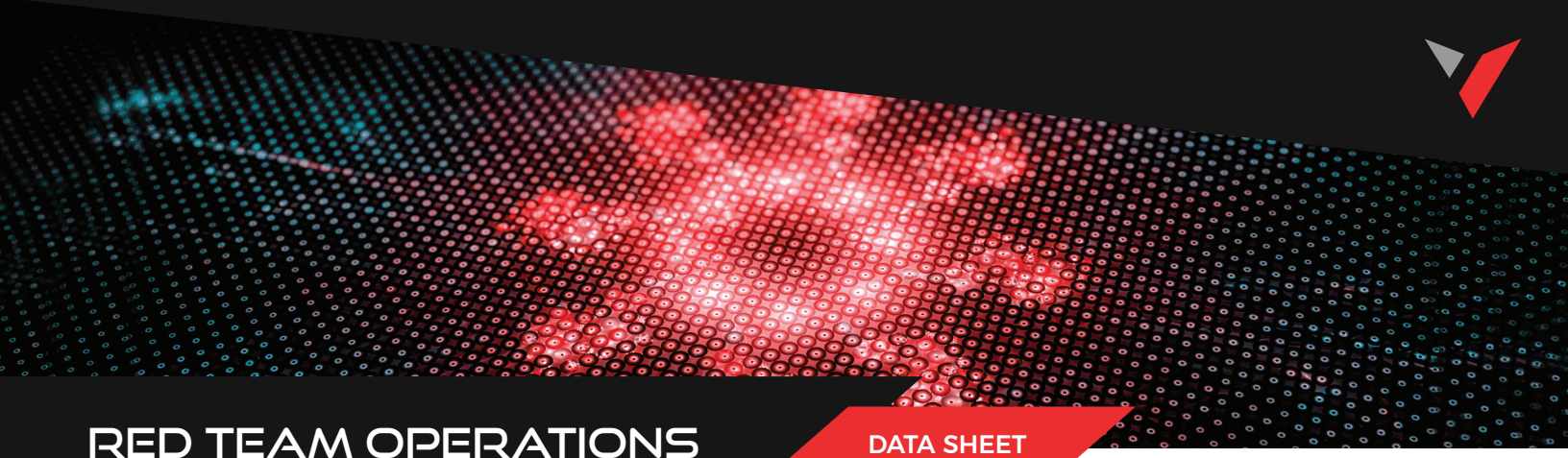

RED TEAM OPERATIONS

DATA SHEET

What is Red Team Operations?

A red team assessment is similar to a penetration test in many ways. During a penetration test, the assessor attempts to identify as many security vulnerabilities as possible and perform exploitation to demonstrate potential impact. However, a red team assessment is different in that it is much more focused and goal-oriented. A red team assessment consists of an assessor establishing goals and objectives with an organization and attempting to accomplish those goals through any way possible. In many cases, a red team assessment can include performing a variety of attacks, including wireless, social engineering, internal, and external penetration testing attacks.

Organizations that have a mature security program can gain a lot of value in red team assessments as these assessments are the closest to a realistic attack scenario. Attackers seeking to gain access to sensitive information and systems are not restricted to rules of engagements.

By performing a red team assessment, an organization can gain an understanding of the following:

- Incident response and detection procedures
- Configuration strengths and weaknesses of technical security controls
- Effectiveness of user awareness training program
- Security vulnerabilities that expose the organization's assets and data

Vonahi Security offers a comprehensive red team engagement that challenges the security of your organization. After concluding the assessment, our consultants work with your network security staff to review the results and identify areas of improvement within the environment.

SIMULATE MALICIOUS ATTACKERS

We simulate the activities of a motivated attacker attempting to gain access to your sensitive data and/or information systems. These activities are scoped with limited rules of engagement to ensure a realistic simulation of real-world scenarios.

ASSESSMENT OF YOUR INFRASTRUCTURE

Combining all of our attacks, our consultants will assess your infrastructure for security weaknesses to launch an attack. This assessment will identify areas of interest that an attacker may target when performing reconnaissance against your environment.

VARIETY OF ATTACK METHODS

To accomplish the end-goal of gaining access to sensitive data and/or systems, our red team operations may consist of a variety of attack methods. These attack methods could leverage social engineering, network, and even physical security attacks.

Our Red Team Operations Methodology

Based on our professional experience, research, and the activities performed by modern-day attackers, Vonahi Security consultants follow a red team methodology that combines both traditional and new attack techniques to assist us in becoming successful with identifying your security flaws and areas for improvement.

INTELLIGENCE GATHERING

Information about your organization is gathered to map out the environment. Information such as domains, IP addresses and ranges, compromised email addresses, and employee information is discovered. This information allows us to determine the initial scope of the assessment.

THREAT MODELING

Based on the attack vectors exposed during the vulnerability analysis phase, we perform threat modeling to understand the business and analyze the best plan for attack. Using this information, we map out the attacks as well as potential results to ensure maximum effectiveness of our attack.

VULNERABILITY ANALYSIS

After mapping out the available environments for the attack, we analyze the targets for potential vulnerabilities that may lead to a successful access of data or systems within the environment.

PERFORM EXPLOITATION

After identifying potential vulnerabilities and understanding the method of attacks, we attempt exploitation of our vulnerability targets. This could include network systems as well as user.

POST-EXPLOITATION

Once we gain access into your environment, we will attempt to locate the objectives set during the project scoping while maintaining stealth within the environment.

TIMELY REPORTING

Documentation is collected during the entire process to ensure your organization understands how, when, and why our attacks were executed within your environment. These reports will also demonstrate the attacks through screenshots and a variety of supporting evidence.

What You Get

At Vonahi Security, we understand the demands and expectations for quality information security services. As part of our red team operations, your organization can expect the following:

- **Project Management & Planning**
- **Daily Status / Progress Reports**
- **Quality Deliverables & Presentations**
- **Experienced & Certified Security Experts**

VONAHI SECURITY

ABOUT US

Vonahi Security is a cybersecurity consulting firm that offers comprehensive information security services. Our team is comprised of security experts experienced in offensive and defensive operations, allowing us to provide quality information security services. We ensure your organization is successful with achieving its security goals and remaining one step ahead of malicious adversaries.

HELLO WORLD. MEET MODERN SECURITY.

www.vonahi.io

info@vonahi.io

1.844.VONASEC (866-2732)

@vonahisec