TAG

THE VALUE OF TRADITIONAL PENETRATION TESTING AND ASSESSMENT WITH NR LABS

DR. EDWARD AMOROSO,
CEO, TAG

NR LABS

THE VALUE OF TRADITIONAL PENETRATION TESTING AND ASSESSMENT WITH NR LABS

DR. EDWARD AMOROSO, CEO, TAG

This report provides guidance on the many advantages of traditional human expert-led penetration testing and security assessment with emphasis on the fine professional service offerings in these areas from commercial cybersecurity vendor NR Labs.[1]

INTRODUCTION:

The modern enterprise security manager has access to a variety of commercial options from vendors for reducing risk – and the majority of these security products leverage automation. Certainly, this is appropriate given the need for continuous monitoring – and automation does help vendors scale their solutions. But in this report, we celebrate a traditional approach to security that continues to provide value: *Human penetration testing*.

Penetration testing by human experts, often referred to as ethical hackers, is a proactive cybersecurity measure where simulated attacks are conducted on an organization's systems to identify vulnerabilities before malicious actors can exploit them. Engaging in regular penetration testing helps to maintain a robust security posture, as it uncovers weaknesses in networks, applications, and user behaviors.

[1] Detailed information on NR Labs and their various penetration testing and security assessment offerings can be obtained from their website (see https://nrlabs.com/).

Commercial vendor NR Labs offers a comprehensive, remediation-focused suite of penetration testing services tailored to the needs of each client based on decades of experience responding to active breaches. Their approach goes beyond traditional testing methodologies by emphasizing a deep understanding of the client's environment, industry-specific challenges, and business objectives. This perspective ensures that the security measures implemented are both effective and aligned with the organization's goals.

In the sections below, we outline the most important aspects of the NR Labs approach. Our purpose is not only to illustrate their commercial solutions, but also to highlight the importance of human penetration testing to complement more automated approaches. We believe this this confluence of human and machine-generated insight will create the best approach for security teams to manage and minimize cyber risk.

NR LABS PENETRATION TESTING PHILOSOPHY

The suite from NR Labs focuses primarily on penetration testing and security assessments. Their solutions start with what they refer to as *remediation-focused delivery*. Unlike approaches that solely highlight vulnerabilities, NR Labs centers on understanding and securing identified weaknesses. Their process is designed to not only detect vulnerabilities but also to provide strategies for remediation, ensuring that clients can address and mitigate risks; prioritizing risks most commonly seen in active breaches.

To do this, NR Labs offers *holistic recommendations*, which are tailored to address a client's specific environment and challenges. By adapting their guidance to the unique contexts of each organization, they ensure that the proposed security measures are practical, relevant, and implementable. If there has been a weakness in past penetration testing efforts, it has been ethical hackers who lack context about this business. NR Labs avoids this specifically.

The company also focuses on delivering *comprehensive reporting*. Recognizing the diverse stakeholders involved in cybersecurity, NR Labs develops reports that are accessible and informative to all parties, from board members to technical analysts. This inclusive reporting approach facilitates informed decision-making and fosters a culture of security awareness throughout the organization.

The team at NR Labs possesses deep expertise across various industries, allowing them to understand and anticipate sector-specific threats and implementation challenges. This specialized knowledge enables them to provide insights and solutions that are particularly relevant to the client's operational context, enhancing the effectiveness of their security strategies.

Beyond technical assessments, NR Labs also evaluates vulnerabilities concerning their potential impact on the client's business operations. This approach ensures that security efforts are aligned with business priorities, focusing on protecting critical assets and functions that are vital to the organization's success. Such assessment requires deep insight into the specific context of the client's business mission.

NR LABS SERVICE OFFERINGS

For external and internal penetration testing projects, NR Labs combines advanced threat simulation with comprehensive attack surface analysis to uncover and protect against hidden vulnerabilities. Their approach targets both external perimeters and key internal assets with realistic chained attacks, blending automated precision with expert human analysis to enhance security visibility and implement effective protection protocols.

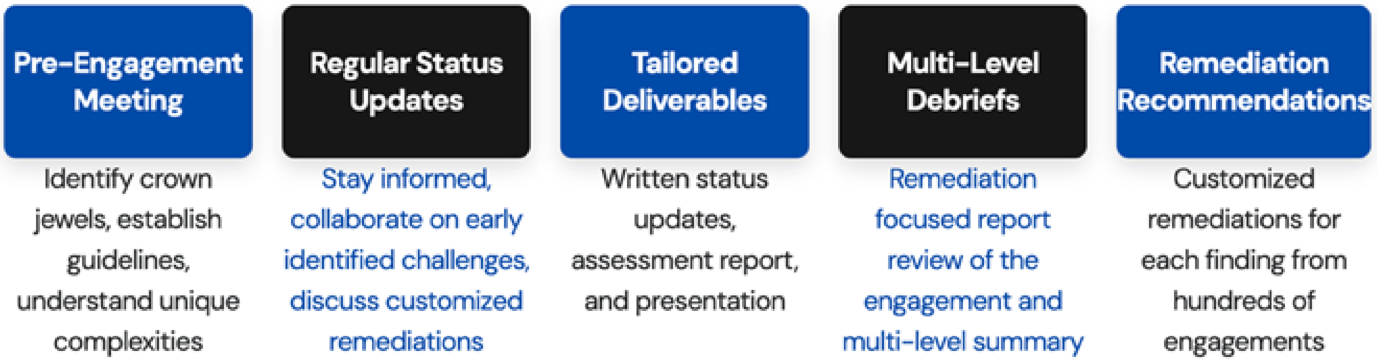
Pre-Engagement Meeting
Identify crown jewels, establish guidelines, understand unique complexities
Regular Status Updates
Stay informed, collaborate on early identified challenges, discuss customized remediations
Tailored Deliverables
Written status updates, assessment report, and presentation
Multi-Level Debriefs
Remediation focused report review of the engagement and multi-level summary
Remediation Recommendations
Customized remediations for each finding from hundreds of engagements

Figure 1. Stages Included in NR Labs Test and Assessment Engagements

Beyond traditional vulnerability scanning, NR Labs employs manual, in-depth testing methods to tackle complex security challenges, from supply chain integrity to application programming interface (API) robustness. Their approach to web application and API security ensures that web assets withstand sophisticated attacks, providing strategic guidance-led remediation to fortify digital infrastructures against emerging cyber threats.

NR Labs employs highly realistic, organization-specific scenarios to address social engineering and business email compromise (BEC) risk, elevating the standard of phishing simulation exercises. Drawing from an extensive repertoire of real breach campaigns, they provide immersive training experiences, enhancing employees' preparedness against sophisticated social engineering tactics, which is good for the local security culture.

Regarding support for ransomware prevention and avoidance, NR Labs leverages knowledge from numerous real-world breaches. The team specializes in simulating exact attacker tactics, techniques, and procedures. They offer industry-specific insights for tailored attacker missions and technically replicate attack chains to rigorously test detections and protections, enhancing incident response readiness.

Identity and authentication are also popular focus areas for security assessment: This work might, for example, validates that Conditional Access Policies within the Microsoft Entra ID environment are implemented and functioning as expected. By rigorously testing such policies, NR Labs ensures that only authorized users and devices can access corporate resources, safeguarding the organization against unauthorized access and potential breaches.

NR Labs can also support hardware and operational technology (OT) security assessment with will ensure that Internet of Things (IoT) and related devices are secure by leveraging hardware hacking methodologies such as firmware analysis, reverse engineering, and JTAG exploitation. This work helps to ensure that embedded devices are hardened against sophisticated adversaries, especially those targeting critical infrastructure.

As one might expect, artificial intelligence (AI) security assessments are essential, and NR Labs assists organizations in ensuring that services leveraging AI are secure and protected. They assess these services at every level of the technology stack, from performing adversarial attacks against foundational models to evaluating the infrastructure used to deploy and operate these services, as well as validating security controls used to sanitize AI input/output.

To complement their manual efforts, NR Labs can support continuous penetration testing with clients who request such on-going support. Consistent with the need to keep up with ever-changing threats, NR Labs offers continuous testing to provide ongoing security assurance. This service focuses on the most critical and current vulnerabilities, ensuring that defenses are robust and resilient against the latest threats.

ACTION PLAN

Our assessment at TAG is that NR Labs' penetration testing services provide good value by delivering tailored, comprehensive, and actionable insights into an organization's security posture. Their remediation-focused approach, combined with industry-specific expertise and a deep understanding of business impacts, ensures that clients are not only aware of potential vulnerabilities but are also equipped with the strategies needed to effectively address them.

Readers who need more information on how NR Labs approaches penetration testing and security assessment should contact the company directly. For readers who are TAG Research-as-a-Service (RaaS) customers, more information on this and any other topic related to cybersecurity and AI can be obtained from the TAG analyst team through the customer's RaaS portal account. We look forward to hearing from you.

ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity and artificial intelligence,.