S|3 SPECIALIZED SECURITY SERVICES

PENETRATION TESTING FOR THE NEXT GENERATION OF CYBER ATTACKS

CYBER SECURITY MUST EVOLVE TO ADDRESS NEW AI, OT AND HUMAN-CENTRIC THREATS

CONTENT OVERVIEW

OVERVIEW

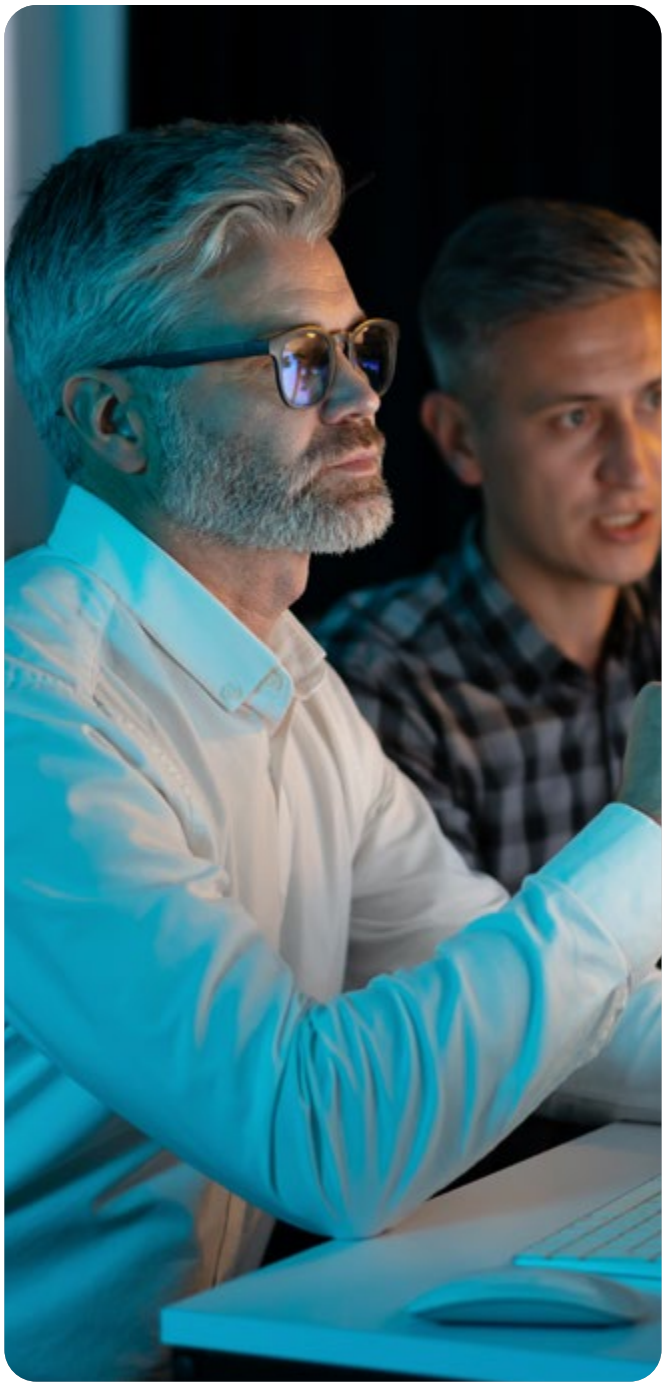
Many organizations rely on penetration testing approaches designed for environments that no longer reflect how their systems operate today. Traditional penetration testing focused primarily on corporate networks, internal systems, and web applications. But while these areas remain critical, enterprise environments have evolved significantly.

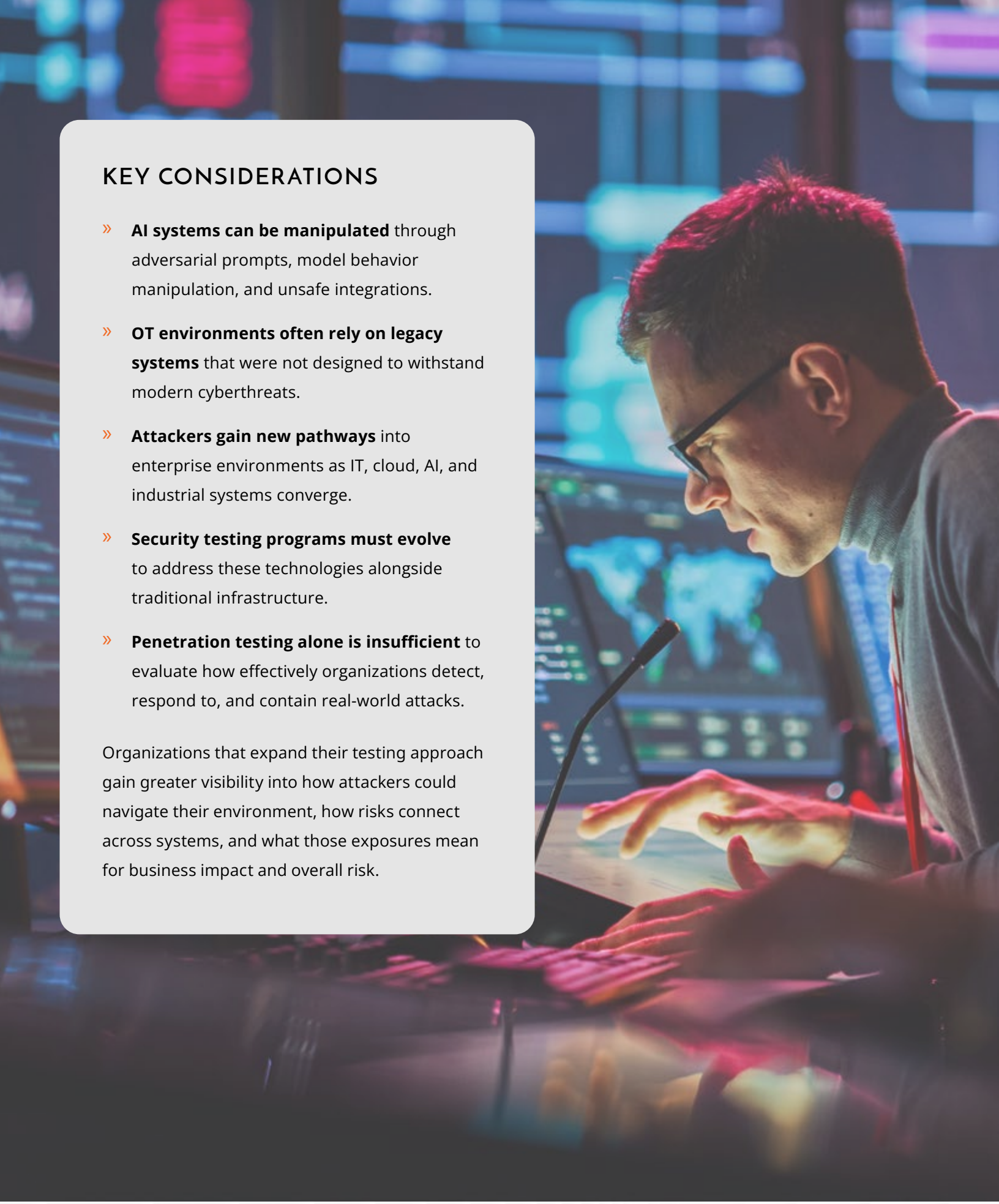
Today's modern environments are more interconnected, dynamic, and difficult to evaluate using traditional testing alone.

As a result, organizations are being forced to expand and evolve their penetration testing strategies to address three key developments:

1. Artificial Intelligence (AI) systems, particularly large language models (LLMs).
2. Operational Technology (OT) environments controlling physical infrastructure.
3. Expanded offensive security activities that evaluate detection, response, and human risks.

These changes introduce new attack paths and behaviors that traditional penetration testing approaches were not designed to fully address. Understanding how an attacker could move through these environments, and what that means for business risk, is becoming increasingly important.





KEY CONSIDERATIONS

- **AI systems can be manipulated** through adversarial prompts, model behavior manipulation, and unsafe integrations.
- **OT environments often rely on legacy systems** that were not designed to withstand modern cyberthreats.
- **Attackers gain new pathways** into enterprise environments as IT, cloud, AI, and industrial systems converge.
- **Security testing programs must evolve** to address these technologies alongside traditional infrastructure.
- **Penetration testing alone is insufficient** to evaluate how effectively organizations detect, respond to, and contain real-world attacks.

Organizations that expand their testing approach gain greater visibility into how attackers could navigate their environment, how risks connect across systems, and what those exposures mean for business impact and overall risk.

THE EVOLUTION OF PENETRATION TESTING

Penetration testing has long been a core component of cybersecurity programs. Historically, these assessments focused on identifying vulnerabilities within traditional enterprise infrastructure.

TRADITIONAL PENETRATION TESTING FOCUS AREAS

Most programs evaluated security across three primary domains:

1. EXTERNAL NETWORK TESTING

Internet-facing systems such as web servers, VPNs, firewalls, and remote access services.

2. INTERNAL NETWORK TESTING

Simulated attacker movement within corporate environments after gaining an initial foothold.

3. WEB APPLICATION TESTING

Vulnerabilities such as authentication flaws, injection attacks, and insecure session management.

These assessments remain important today; however, enterprise environments have evolved significantly.

THE MODERN ENTERPRISE TECHNOLOGY ENVIRONMENT

Organizations now operate within complex, interconnected ecosystems that include:

- Cloud infrastructure and SaaS platforms
- Microservices and API architectures
- Third-party integrations and partner systems
- AI tools embedded in workflows
- OT connected to corporate networks

Each of these systems introduces potential entry points for attackers. More importantly, they create opportunities for attackers to move between systems, turning isolated weaknesses into connected attack paths that can increase business impact across the organization.

THE EXPANDING ATTACK LANDSCAPE

Modern organizations rely on technologies that were not designed to withstand today's threat landscape, creating new and often unintended security exposure. There are three areas of expansion that are reshaping how organizations evaluate security risk.

1. ARTIFICIAL INTELLIGENCE (AI) SYSTEMS

AI technologies are being deployed to support:

- Internal productivity tools
- AI copilots and assistants
- Customer service automation
- Software development workflows
- Data analysis and decision support

These systems often connect to internal applications, APIs, and proprietary data sources, introducing new and often unpredictable attack paths that increase exposure across the business.

2. OPERATIONAL TECHNOLOGY (OT) ENVIRONMENTS

OT refers to systems that control physical processes, including:

- Manufacturing control systems
- Industrial Control Systems (ICS)
- Building automation systems
- Energy and utilities infrastructure
- Transportation systems

Historically isolated from corporate networks, many of these environments are now connected to enterprise infrastructure. This convergence introduces new pathways between IT and operational systems, increasing the potential for cross-environment compromise.

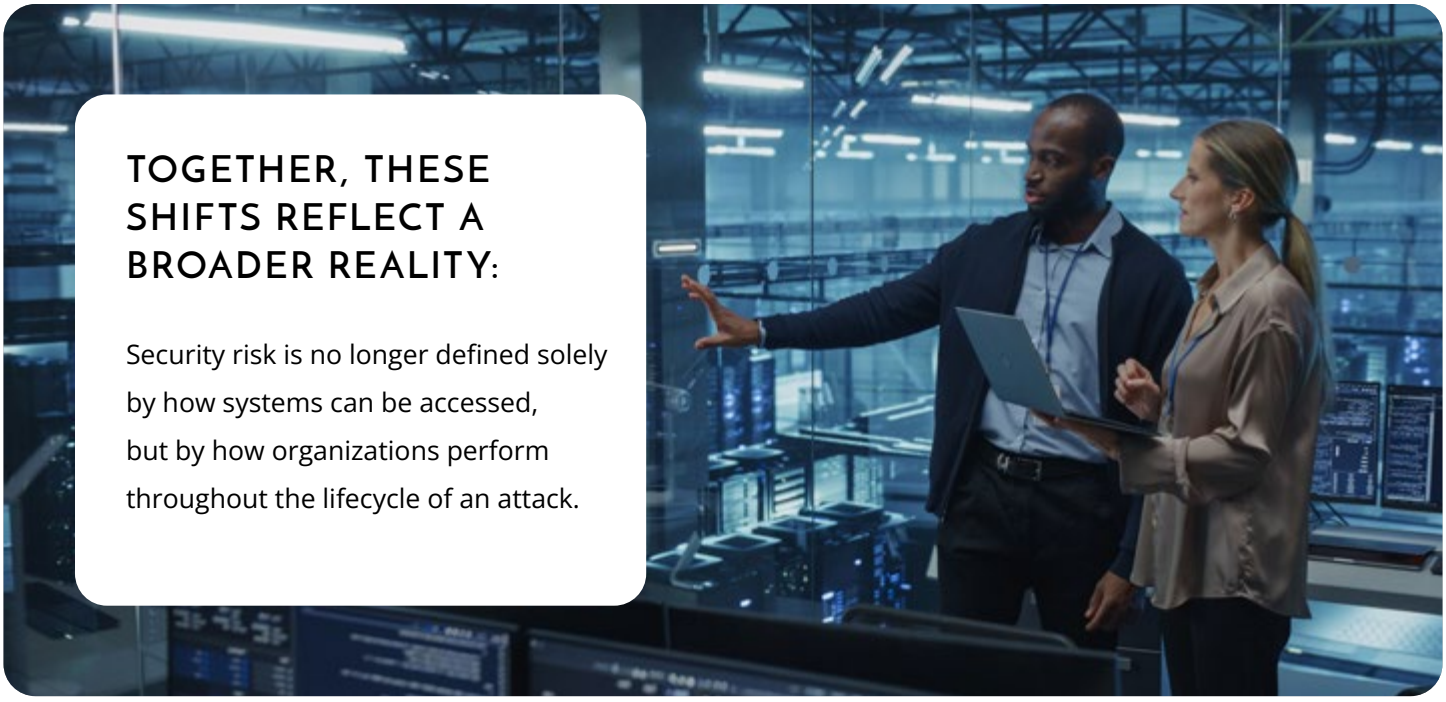
3. EXPANDING OFFENSIVE SECURITY STRATEGIES

Organizations are increasingly recognizing that identifying how an attacker gains access is only part of the risk. Traditional penetration testing focuses on initial compromise, but real-world incidents are often defined by what happens next.

As a result, security programs are expanding to evaluate:

- How quickly threats are detected.
- How effectively teams respond.
- How well attacker activity is contained.
- How employees behave under real-world attack scenarios.

This shift reflects a broader understanding that security is not only about preventing access, but also about resilience during an active attack.



TOGETHER, THESE SHIFTS REFLECT A BROADER REALITY:

Security risk is no longer defined solely by how systems can be accessed, but by how organizations perform throughout the lifecycle of an attack.

ARTIFICIAL INTELLIGENCE (AI) SYSTEMS AND LARGE LANGUAGE MODEL (LLM) SECURITY RISKS

AI technologies, particularly large language models (LLMs), are rapidly being integrated into enterprise environments; however, these systems behave very differently from traditional software.

Unlike deterministic applications that follow fixed logic, AI systems generate outputs dynamically based on model training and user input. **This creates new opportunities for manipulation, misuse, and unintended outcomes.**

COMMON AI SECURITY RISKS

1. PROMPT INJECTION

Attackers craft inputs designed to manipulate a model's instructions – a risk that's particularly relevant in LLM implementations.

Potential outcomes may include:

- Bypassing safety guardrails
- Altering model behavior
- Influencing automated decisions

2. SENSITIVE DATA EXPOSURE

AI systems may inadvertently reveal confidential information if:

- Training data contains sensitive content.
- The model is connected to internal knowledge sources.
- Integrations expose proprietary data.

3. MODEL MANIPULATION

Adversarial inputs may cause models to generate inaccurate or harmful outputs.

This can impact:

- Automated decision-making systems
- Customer-facing AI tools
- Data analysis processes

4. UNSAFE INTEGRATIONS

Many AI systems connect to:

- APIs
- Internal databases
- Automation tools

If these integrations are not properly secured, attackers may gain access to unintended capabilities or sensitive functions.

5. KNOWLEDGE SOURCE MANIPULATION

Architectures such as Retrieval-Augmented Generation (RAG), commonly used in LLMs, rely on external data sources. If these sources are compromised, attackers may influence or poison the responses generated by the system.

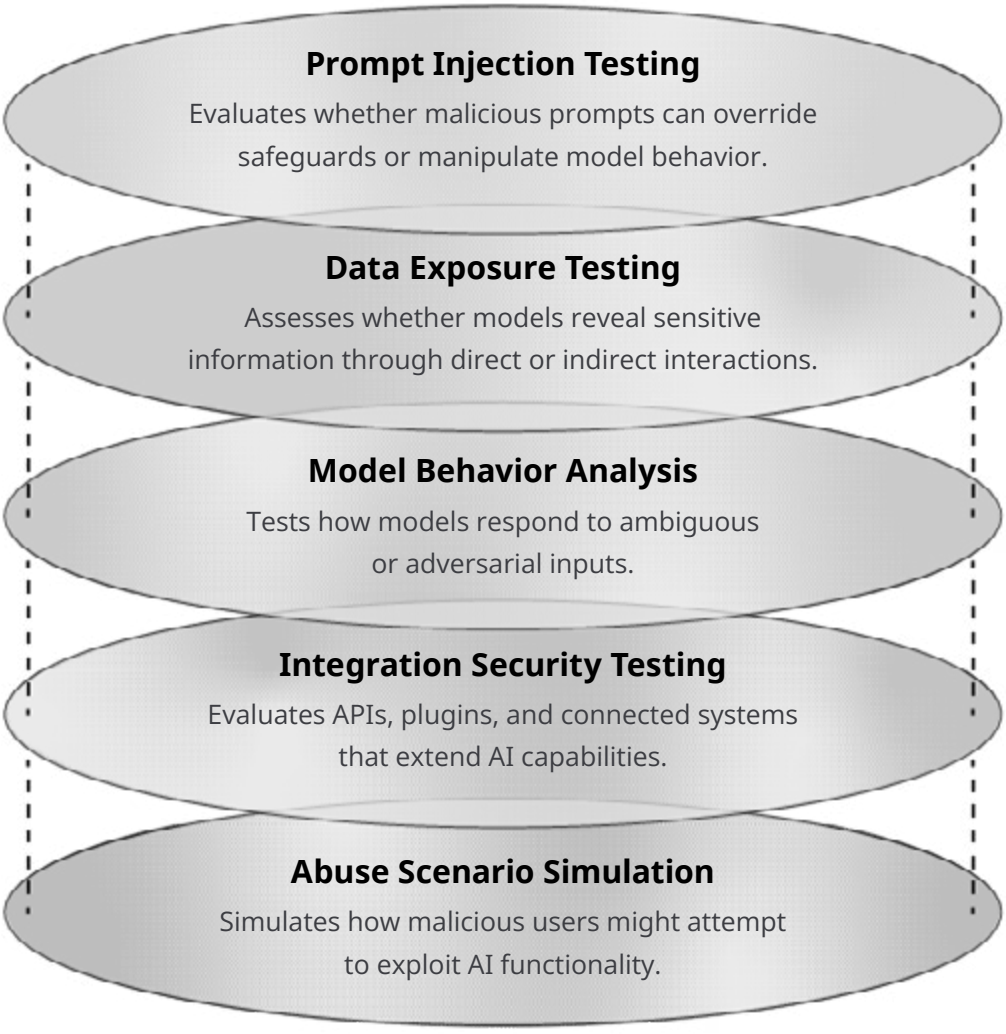
AI PENETRATION TESTING METHODOLOGIES

As organizations rapidly deploy AI capabilities, many are doing so without fully understanding how these systems can be manipulated or abused.

Testing AI systems requires specialized techniques designed to evaluate how models behave under adversarial conditions. Unlike traditional application testing, these assessments focus on model behavior, system interactions, and how outputs can be influenced by malicious inputs.

CORE COMPONENTS OF AI SECURITY TESTING

These assessments help organizations understand how their AI systems may be manipulated, misused, or exploited in real-world scenarios.



OT AND THE CONVERGENCE OF IT AND PHYSICAL SYSTEMS

As organizations modernize industrial environments, many are introducing connectivity without fully understanding the resulting security implications or exposure.

OT environments monitor and control physical processes across industries such as manufacturing, energy, transportation, and utilities.

Historically, these systems operated in isolated environments with limited connectivity to corporate networks. However, modernization initiatives have increasingly connected OT environments to enterprise IT systems.

EXAMPLES OF OT COMPONENTS

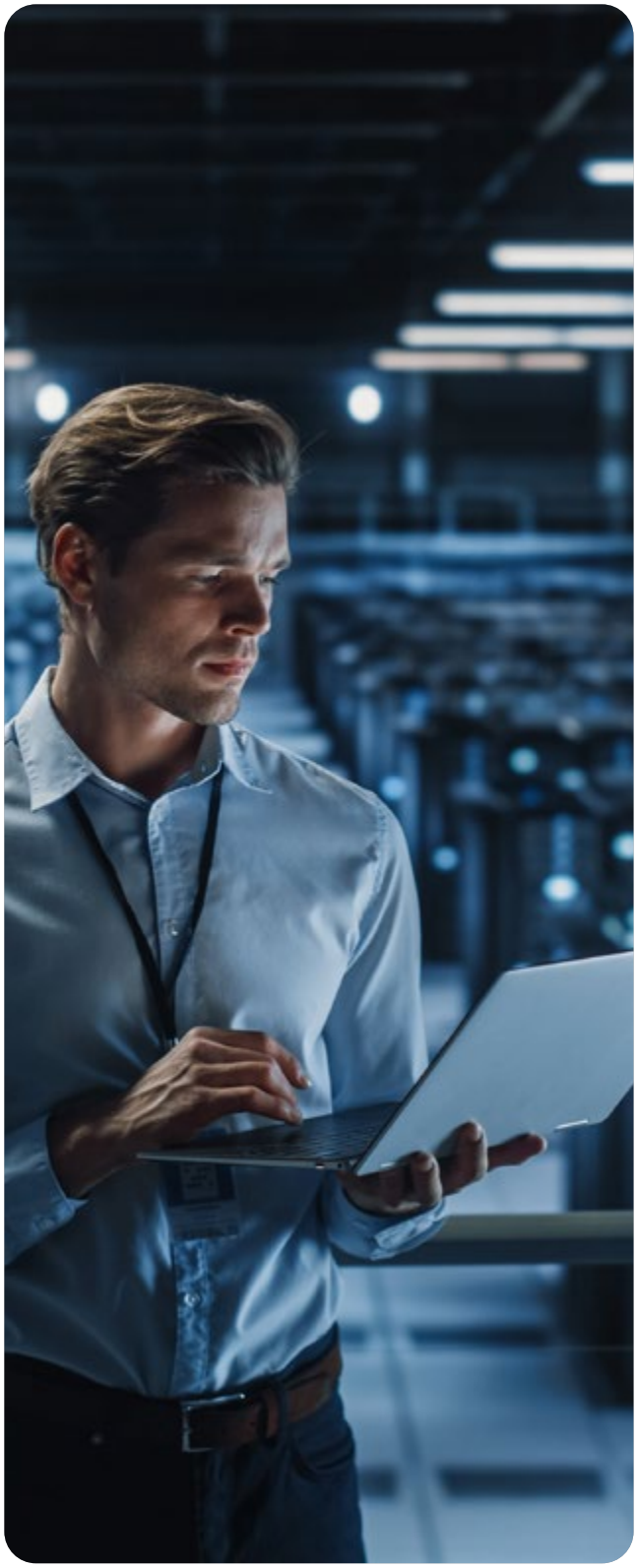
- Programmable Logic Controllers (PLCs)
- Industrial Control Systems (ICS)
- Supervisory Control Systems (SCADA)
- Building Management Systems
- Industrial Sensors and Connected Devices

DRIVERS OF IT/OT CONVERGENCE

Organizations are integrating OT systems with enterprise infrastructure to support:

- Remote monitoring and maintenance
- Centralized operational analytics
- Cloud-based management tools
- Vendor support access

While these changes improve visibility and efficiency, they also introduce new pathways between IT and operational environments.



UNIQUE OT SECURITY CHALLENGES

Operational environments often include:

- Legacy hardware with long lifecycles
- Unsupported operating systems
- Proprietary industrial protocols
- Limited patching capabilities

In addition, cyber incidents in OT environments may have physical consequences, including:

- Operational disruption
- Equipment damage
- Safety risks to personnel and infrastructure

These factors make OT environments fundamentally different from traditional IT systems and require specialized approaches to security testing.

OT PENETRATION TESTING APPROACHES

Security testing within operational environments must be carefully designed to avoid disrupting critical processes.

OT penetration testing typically includes:

» ARCHITECTURE REVIEW

Evaluates how OT systems connect to corporate IT networks and external environments.

» NETWORK SEGMENTATION TESTING

Determines whether segmentation controls effectively isolate industrial systems.

» INDUSTRIAL PROTOCOL ANALYSIS

Examines specialized communication protocols used within OT environments.

» DEVICE SECURITY ASSESSMENT

Evaluates controllers, sensors, and connected devices for vulnerabilities.

» CONTROLLED EXPLOITATION TECHNIQUES

Employs safe testing methods designed to prevent operational disruption.

The overall objective is to identify vulnerabilities and potential attack paths while maintaining operational continuity.

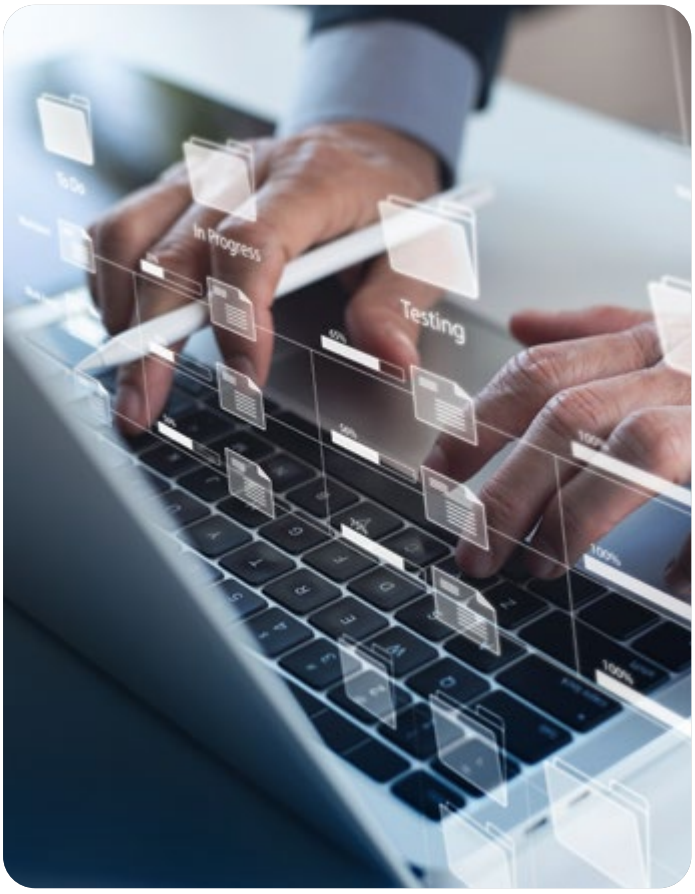
EXPANDING BEYOND INITIAL ACCESS: EVALUATING DETECTION, RESPONSE, AND HUMAN RISK

As emerging technologies introduce new attack surfaces, many organizations are discovering that traditional penetration testing does not fully evaluate what happens after access is gained. This gap between initial compromise and incident response is where many organizations experience the greatest risk.

Initial access remains an important measure of exposure. However, in actual attack scenarios, the overall business impact of an incident is often determined by how quickly threats are detected, how effectively teams respond, and how far an attacker can move within the environment.

Many organizations also find that while penetration testing identifies how access is gained, it does not fully evaluate how their teams perform once an attack is underway.

As a result, security leaders are expanding their offensive security strategies to assess resilience across people, processes, and technology.



EXPANDING THE SCOPE OF OFFENSIVE SECURITY

Modern security programs are incorporating additional assessments that provide visibility into areas not typically addressed through standard penetration testing.

These approaches focus on:

- How quickly threats are detected.
- How effectively teams respond.
- How well systems and processes contain attacker activity.
- How employees behave under real-world attack conditions.

KEY AREAS OF EXPANSION

1. INCIDENT RESPONSE TABLETOP EXERCISES

Facilitated simulations that **guide executive leadership and technical teams** through realistic cyber incident scenarios.

These exercises evaluate:

- Decision-making under pressure
- Communication workflows across teams
- Clarity of roles and responsibilities

Key Benefit: Strengthens leadership confidence and ensures teams are prepared before a real incident occurs.

2. RANSOMWARE SIMULATION AND RED TEAM EXERCISES

Advanced adversary simulations designed to **emulate real-world attack behavior across multiple stages** of an attack lifecycle.

These engagements evaluate:

- Detection capabilities
- Response timing and coordination
- Ability to contain stealthy attacker activity

Key Benefit: Validates not just whether an attacker can gain access, but whether the organization can detect and stop them.

3. SOCIAL ENGINEERING ASSESSMENTS

Simulated attempts to manipulate employees into providing sensitive information or granting unauthorized access.

These assessments **evaluate how individuals respond to a range of real-world attack techniques**, including:

- Phishing/Smishing campaigns (email, SMS, and voice-based attacks)
- Phone-based social engineering (vishing)
- Pretexting and impersonation techniques
- In-person interaction scenarios

As a result, these engagements help organizations:

- Identify high-risk user groups.
- Measure the effectiveness of security awareness programs.
- Evaluate how human behavior contributes to overall risk.

Key Benefit: Assesses the human element of security, one of the most frequently targeted and exploited attack vectors.

BUILDING A MODERN PENETRATION TESTING PROGRAM

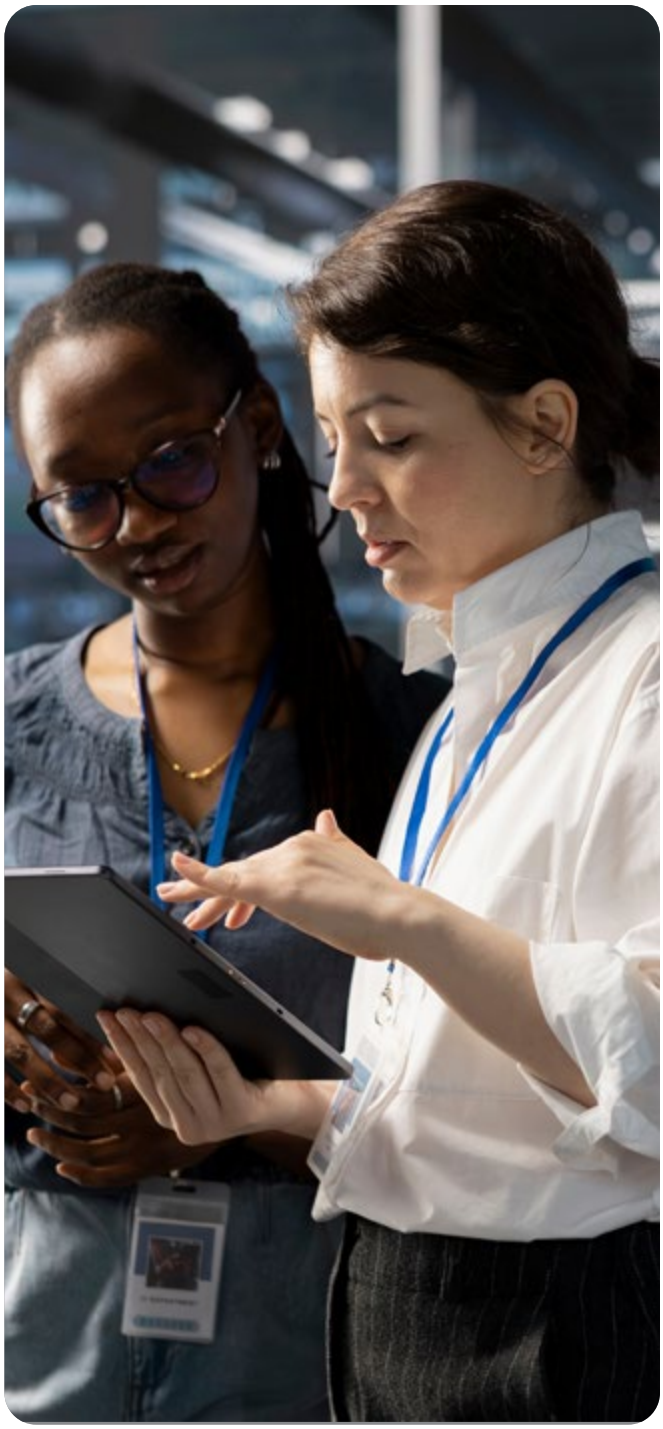
As enterprise technology environments evolve, penetration testing programs must expand to address new attack surfaces and evolving security expectations. A modern testing strategy should evaluate security across multiple domains and how those risks interact across the environment.

Attackers do not limit themselves to a single vulnerability or environment. They chain weaknesses together to move through systems and increase impact. Effective penetration testing should reflect that same reality.

KEY AREAS OF SECURITY EVALUATION

- Corporate network infrastructure
- Web applications and APIs
- Cloud environments
- AI and LLM systems
- OT environments
- Human errors and risks

Many organizations find that their current testing programs do not fully reflect how their environments operate or how attackers behave in practice.



CRITICAL QUESTIONS FOR SECURITY LEADERS

Security leaders evaluating their testing strategy should ask themselves:

ARE EMERGING TECHNOLOGIES SUCH AS AI AND OT INCLUDED IN CURRENT TESTING EFFORTS?

Many penetration testing programs were designed for traditional IT environments and do not adequately assess AI systems or OT environments. This creates blind spots as these technologies introduce new, interconnected, and often unpredictable attack paths.

Without specialized testing, organizations may underestimate how AI integrations or IT/OT convergence can be exploited. Proactively evaluating these environments provides a clearer view of risk and helps organizations identify exposures before attackers do.

DOES TESTING EVALUATE HOW ATTACKS PROGRESS BEYOND INITIAL ACCESS?

Gaining initial access is only the beginning of a real-world attack. The greatest business impact often occurs after an attacker is inside the environment and able to move laterally, escalating privileges, or accessing sensitive systems.

Testing that evaluates how attacks progress beyond initial access reveals how weaknesses can be chained together. Without simulations that reflect this behavior, organizations may overlook the paths attackers are most likely to use to cause real damage.

HOW EFFECTIVELY CAN TEAMS DETECT, RESPOND TO, AND CONTAIN REAL-WORLD THREATS?

Many organizations regularly identify vulnerabilities but rarely test how effectively their teams detect and respond to an active attack. As a result, leadership often lacks visibility into response speed, coordination, and containment capabilities.

Simulating real-world attack scenarios helps surface gaps that vulnerability testing alone cannot reveal. This is frequently where organizations uncover their most meaningful opportunities to improve resilience and reduce impact during an actual incident.

CRITICAL QUESTIONS FOR SECURITY LEADERS

ARE HUMAN-FOCUSED RISKS BEING ASSESSED ALONGSIDE TECHNICAL VULNERABILITIES?

Attackers consistently target people as a primary entry point, yet human risk is often underrepresented in traditional penetration testing. Social engineering and behavioral assessments demonstrate how employees respond under realistic attack conditions.

Evaluating human-focused risk alongside technical vulnerabilities provides a more accurate view of organizational exposure and highlights where awareness, process, or control improvements can significantly reduce risk.

DO TESTING ACTIVITIES REFLECT HOW REAL ATTACKERS BEHAVE IN TODAY'S ENVIRONMENTS?

Modern attackers do not rely on a single vulnerability or system. They combine technical exploits, user manipulation, and environmental awareness to achieve their objectives. Testing that mirrors this behavior delivers a far more accurate understanding of risk than isolated vulnerability checks.

Organizations that adopt attacker-informed testing gain clearer insight into how risks connect across systems and are better positioned to prioritize remediation where it matters most.

IN SUMMARY

Penetration testing remains a foundational component of security programs. Organizations that expand their approach gain deeper visibility into how risk manifests across technology, operations, and human behavior. This broader perspective enables more informed decisions, stronger resilience, and security strategies that better reflect today's threat landscape.

PREPARING FOR THE NEXT GENERATION OF CYBER RISK

The enterprise attack surface is evolving rapidly as organizations adopt new technologies to drive innovation and operational efficiency. AI systems, OT environments, and the growing need to evaluate detection and response capabilities are reshaping how security risk is understood and managed. Traditional penetration testing approaches were not designed to address how these environments behave today.

Organizations that expand their testing strategies gain clearer visibility into how attacks originate, how they progress across systems, and where controls are most likely to fail. More importantly, they gain insight into how those weaknesses could impact business operations and where to take action before they are exploited.

Proactive security testing remains one of the most effective ways to strengthen resilience in an increasingly complex environment. For organizations evaluating whether their current approach reflects today's threat landscape, expanding beyond traditional testing provides a more practical and complete view of risk and helps prioritize what to fix first.

In today's environment, understanding how an attacker gets in is no longer enough. The organizations that are best prepared understand how attacks unfold, how they are detected, and how effectively they are contained, so they can identify and address weaknesses in advance before they become real business problems.

HOW S3 SECURITY CAN HELP

As organizations expand beyond traditional penetration testing, many find they need more than a point-in-time assessment. They need a partner who can help them understand how their environment would perform under real-world conditions and where to focus next.

S3 Security works alongside your teams to evaluate risk across modern environments and provide clear, practical guidance on how to strengthen detection, response, and overall resilience. Our approach is designed to simulate real attacker behavior and uncover the attack paths that matter most.

Every engagement is led by senior-level testers with deep, real-world experience. There are no junior resources and no unnecessary complexity.

Most importantly, we focus on helping your team understand not just where vulnerabilities exist, but how attackers move through your environment, how risks connect across systems, and which actions will have the greatest impact in reducing exposure.

FOR ORGANIZATIONS EVALUATING WHETHER THEIR CURRENT APPROACH REFLECTS TODAY'S THREAT LANDSCAPE,

S3 SECURITY PROVIDES A CLEARER PATH FORWARD.

S|3 SPECIALIZED SECURITY SERVICES

STRENGTHEN YOUR CYBERSECURITY STRATEGY

Contact Us Today.

INFO@S3SECURITY.COM