spritzmatter

your cybersecurity partner for innovation

OUR IDENTITY

CyberSecurity

We offer a range of services for improving cybersecurity for businesses.

Artificial Intelligence

Incorporate the power of Artificial Intelligence securely within your business assets.

Our mission

We are a spin-off of the University of Padua, specializing in advanced cybersecurity solutions.

Our mission is to ensure a secure digital environment for companies, protecting data and ensuring operational continuity.

We use innovative technologies like artificial intelligence and are constantly updated on the latest trends to develop cutting-edge solutions.

Università degli Studi di Padova

Spritz Matter è uno SPIN-OFF dell'Università di Padova

Scan for more information

www.spritzmatter.com

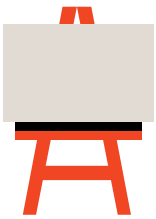
info@spritzmatter.com

Enhance your cyber posture

OUR OFFER

Vulnerability Assessment
A targeted activity designed to highlight the cyber threats affecting corporate assets (IT infrastructure, web applications) and to identify a list of corrective remediations.

Penetration Test
A team of experts simulating a cyberattack on corporate assets to identify potential vulnerabilities and exploit them, conducting attacks that assess system resilience.



Phishing Laboratory
An interactive workshop designed to better prepare your employees to recognize spam and phishing threats.

AntiPhishing Defense System
An anti-phishing system to integrate within your corporate assets. Thanks to the integration of advanced Artificial Intelligence technologies, our solution can detect even the most dangerous phishing emails.

Secure AI Fast Prototyping
A dedicated team of experts to integrate Artificial Intelligence solutions into your business processes.

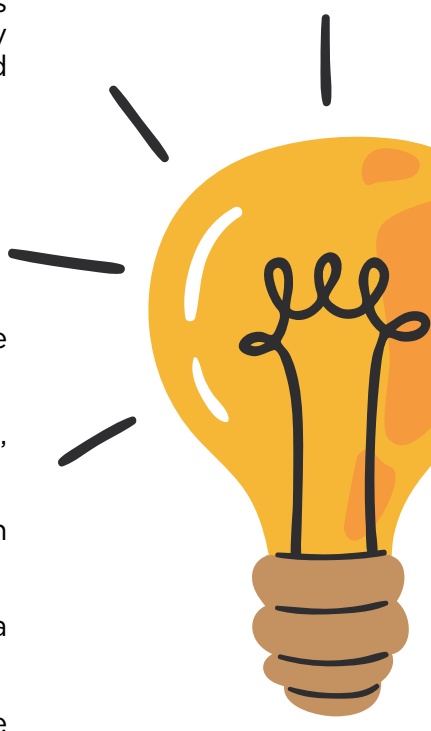
spritzmatter
your cybersecurity partner for innovation

Università degli Studi di Padova

Spritz Matter è uno SPIN-OFF dell'Università di Padova

Vulnerability Assessment

Overview. A Vulnerability Assessment (VA) is a non-intrusive analysis designed to identify and evaluate the vulnerabilities of an IT system, such as networks, applications, or business devices. Essentially, it is a security "check-up" that helps uncover weaknesses that hackers or malware could exploit to attack the company.



Why is it useful?
Investing in a Vulnerability Assessment means:

- Preventing attacks: Identifying vulnerabilities before they can be exploited.
- Saving time and resources: An attack can cause economic, reputational, and legal damage. Prevention is always less costly than repair.
- Ensuring compliance: Helps to meet security and data protection regulations.
- Strengthening trust: With customers and partners, demonstrating a concrete commitment to security.

A secure company is a stronger company. A Vulnerability Assessment is the first step to protecting your business!

Which companies should invest in a Vulnerability Assessment?

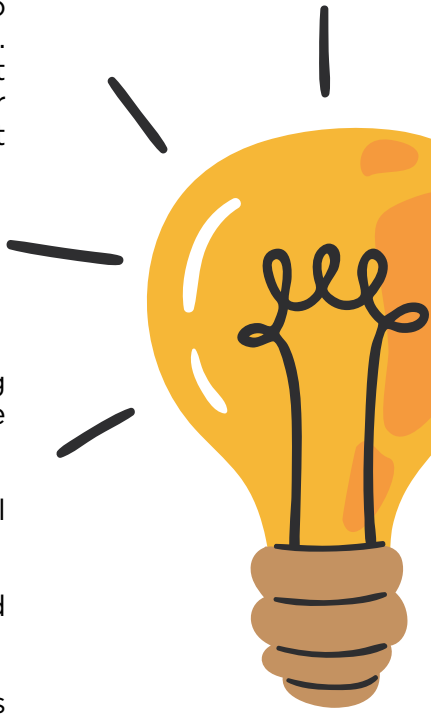
A Vulnerability Assessment is essential for all companies, but it is particularly crucial for those that:

- Handle sensitive data: Companies dealing with personal, financial, or health data, such as banks, hospitals, legal firms, and e-commerce companies.
- Have complex digital infrastructures: Organizations with extensive corporate networks, cloud, or IoT systems, often found in the tech, manufacturing, or logistics sectors.
- Are subject to strict regulations: Regulated sectors, like finance, insurance, or energy, which must comply with specific security standards (GDPR, ISO 27001, NIS2, etc.).
- Operate in strategic sectors: Companies providing essential services, such as utilities, telecommunications, or public administration suppliers, often targeted by cyberattacks.
- Innovative start-ups and SMEs: Growing businesses focusing on digital and innovation, which cannot afford economic or reputational losses due to an attack.

In summary: If your company uses IT systems, collects data, or relies on digital processes, a Vulnerability Assessment is a fundamental step to protect your business.

Penetration Test

Overview. The Penetration Test (PT) is an advanced cybersecurity activity that simulates a hacker attack on company systems to test their resilience. In other words, security experts (known as ethical hackers) act as real cybercriminals to discover and exploit vulnerabilities, allowing them to identify and resolve weaknesses before they can be used by real attackers. The Penetration Test is more advanced than the Vulnerability Assessment because, in addition to identifying vulnerabilities, it simulates real hacker attacks to test the actual resilience of systems, assessing the practical impact of security flaws.



Why is it useful?
Investing in a Penetration Test means:

- Identifying and understanding the impact of vulnerabilities: By simulating real attacks, you discover which weaknesses and critical points can be exploited and with what repercussions.
- Quantifying the risks: Understand the impact and scope of the potential consequences of a successful attack.
- Strengthening compliance and increasing trust among clients and partners by demonstrating a concrete commitment to security.

A Penetration Test is not just a test, but a true strategy to anticipate threats and protect your business.

Which companies should invest in a Penetration Test?

A Penetration Test is essential for all companies, but it is particularly crucial for those that:

- Handle sensitive data: Companies that deal with personal, financial, or health data, such as banks, hospitals, law firms, and e-commerce companies.
- Have complex digital infrastructures: Organizations with extensive corporate networks, cloud or IoT systems, often found in the technology, manufacturing, or logistics sectors.
- Are subject to stringent regulations: Regulated sectors like finance, insurance, or energy, which must comply with specific security standards (GDPR, ISO 27001, NIS2, etc.).
- Operate in strategic sectors: Companies providing essential services, such as utilities, telecommunications, or public administration suppliers, often targeted by cyberattacks.
- Innovative start-ups and SMEs: Growing entities focusing on digital and innovation, which cannot afford to suffer economic or reputational losses due to an attack.

In summary: If your company uses IT systems, collects data, relies on digital processes, or develops software or hardware, a Penetration Test is a valuable tool to identify and mitigate threats before they can cause damage.

Phishing Laboratory

Overview. The phishing workshop is a 3-hour session designed to educate employees on recognizing and defending against phishing attacks, one of the most widespread cyber threats.

Workshop Structure

- **Theoretical Part (1 hour):**
  - Introduction to phishing: What it is, how it works, and the main techniques used by cybercriminals.
  - Warning signs: Analysis of real cases to identify typical clues of a phishing email (language, suspicious links, urgent requests).
  - Best practices: Practical advice to avoid falling into the trap and behaviors to adopt in case of suspicion.
- **Practical Part and Gamification (2 hours):**
  - Participants access an interactive platform designed to simulate real scenarios.
  - Through a gamified mode, employees must analyze and classify a series of emails as phishing or legitimate, earning points for each correct answer.

Realistic simulations with increasing difficulty levels, testing the skills learned.

Why choose it?

Phishing is currently one of the main threats to corporate security, with a potentially devastating impact on business. Our lab provides your employees with the tools and skills necessary to recognize and correctly respond to phishing attempts, thereby strengthening the first line of defense for your organization: the human factor.

- A practical approach that combines theory and real simulations, allowing employees to develop the skills to identify phishing attempts and increase their awareness.
- A solid theoretical foundation and the use of gamification to make phishing training an interactive experience, ensuring greater engagement and better learning.
- A structured workshop with realistic simulations of increasing complexity, allowing participants to test their skills in a safe and controlled environment.

Investing in strengthening your employees' skills reduces risks and protects the company from threats, potential financial losses, and reputational damage.

Antiphishing System

Overview. Our on-demand anti-phishing system is a flexible and advanced solution that easily integrates into your corporate assets, offering immediate and personalized protection against phishing threats. Thanks to the use of sophisticated Artificial Intelligence algorithms, this solution not only identifies harmful emails but also provides direct and continuous support to your employees.

How does it work?

- On-demand analysis: When an employee has doubts about a suspicious email, they can forward it to our dedicated service.
- Personalized feedback: Our system analyzes the email and provides a quick response, indicating whether it is phishing or a legitimate communication.

Continuous education: In addition to feedback, the service provides a detailed explanation of why the email is considered safe or dangerous, helping employees improve their ability to recognize potential scams.

Why choose it?

Our on-demand anti-phishing service is the perfect combination of advanced technology and human support. It drastically reduces the risk of cyber attacks, educates your employees in real-time, and strengthens your company's resilience against one of the most common cyber threats.

What does the subscription include?

- On-Demand Analysis: Whenever an employee is unsure about a suspicious email, they can forward it for a thorough analysis by our AI system, which will provide immediate feedback, explaining whether the email is legitimate or phishing.
- Flexibility: You can use the analysis package for any suspicious email and customize it according to your needs.
- Continuous Support: Each analysis is accompanied by clear explanations and instructions to improve employee awareness and prevent future attacks.
- Regular Updates: Regular maintenance and updates to ensure that the system is always capable of detecting the latest and most sophisticated threats.

Secure AI Fast Prototyping

Overview

Our Fast AI Prototyping service is designed to help companies develop custom Artificial Intelligence solutions, optimized for their specific needs. From creating personalized algorithms to integrating them into existing business systems, we handle every aspect, ensuring high performance and maximum security. Our philosophy is based on adopting the "AI on-premise" model, which allows companies to maintain full control over their sensitive data without compromising privacy or regulatory compliance.

How it works

- Initial analysis: We start with a dedicated workshop to understand business needs, define requirements, and identify specific challenges.
- Solution design: We craft a personalized AI strategy that leverages the most innovative technologies while ensuring compliance with security and regulatory standards.
- Development of PoC (Proof of Concept): We create a functional prototype that demonstrates the technical feasibility and added value of the solution. This includes training AI models, data collection and processing, and preliminary validation.
- Iteration towards the MVP (Minimum Viable Product): Once the PoC is validated, we expand the solution towards an MVP, integrating it into business workflows and optimizing it for scalability and operational performance.

Why Choose it

- Total Customization: Every solution is tailor-made to perfectly fit your operational needs.
- Security: Our on-premise approach allows you to maintain complete control over your data, eliminating risks associated with third-party management.
- Speed and Efficiency: From the initial concept to the prototype, we work to minimize development time without sacrificing quality or security.
- Continuous Innovation: We leverage the latest AI technologies to offer cutting-edge, competitive, and future-oriented solutions.

Why Choose Us.

We are the ideal partner for companies looking for custom AI solutions, combining innovation, security, and speed. Thanks to our Fast AI Prototyping approach, we quickly develop customized prototypes while maintaining a strict focus on compliance and the protection of sensitive data, thanks to the on-premise AI model. With an expert and multidisciplinary team, we offer cutting-edge technologies, ensuring high performance and solutions designed to meet your unique needs. We collaborate transparently, involving your team at every stage to build a safe and innovative digital future together.