THE GLOBAL CHALLENGE OF SUPPLY CHAIN CYBERSECURITY

Addressing threats, vulnerabilities, and solutions

Zadagerey Zhanarys

Matricola: 702814

INTRODUCTION

Context: Digital interconnectivity of global supply chains.

Significance: Increasing reliance on technology and third-party vendors.

Main Focus: Challenges, examples, and solutions in supply chain cybersecurity.

IMPORTANCE OF SUPPLY CHAIN CYBERSECURITY

- **Dependency:** Organizations rely on a network of third-party vendors and tools.
- **Impact of breaches:** Disruptions can ripple across industries and nations.
- **National Security:** Critical infrastructure is vulnerable to sophisticated attacks.

WHAT IS IT ?

Definition of Supply Chain Attacks

Attackers exploit vulnerabilities in third-party vendors to infiltrate targets.

Techniques: Malware injection, phishing, exploiting software vulnerabilities.

A supply chain attack is a combination of at least two attacks. Attack on supplier, then on target

PROMINENT EXAMPLES OF SUPPLY CHAIN ATTACKS

SolarWinds Hack (2020)

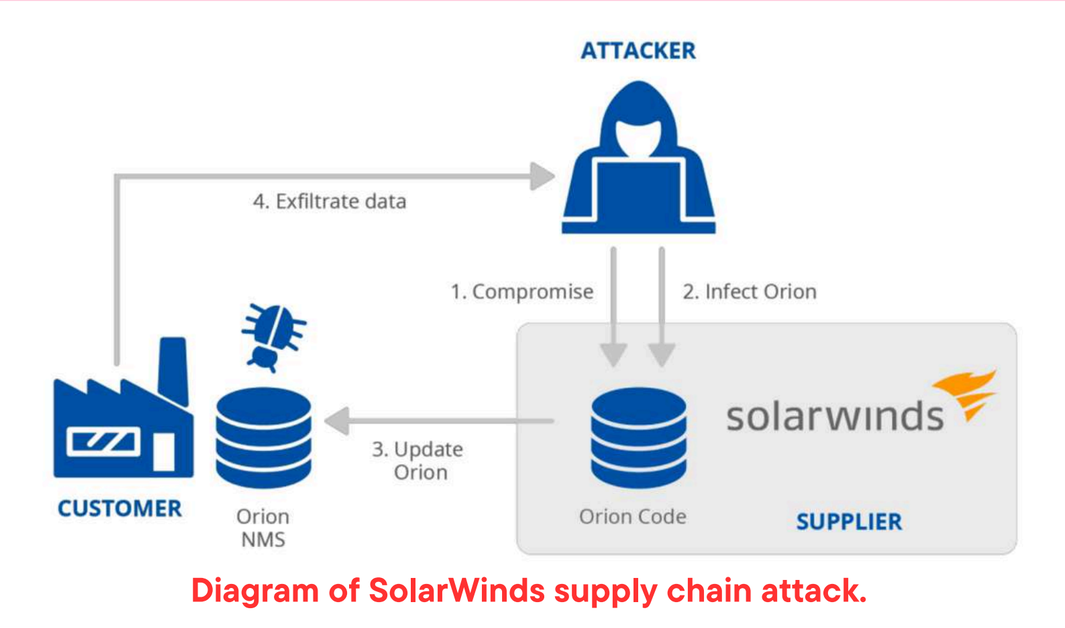


Diagram of SolarWinds supply chain attack.

The attackers compromised SolarWinds and modified the code of ORION software. The ORION instances in the customers were updated with malware, which allowed the attackers to access the data of customers.

Attack method: Backdoor in software updates.

Scale: Affected U.S. government agencies and corporations

.

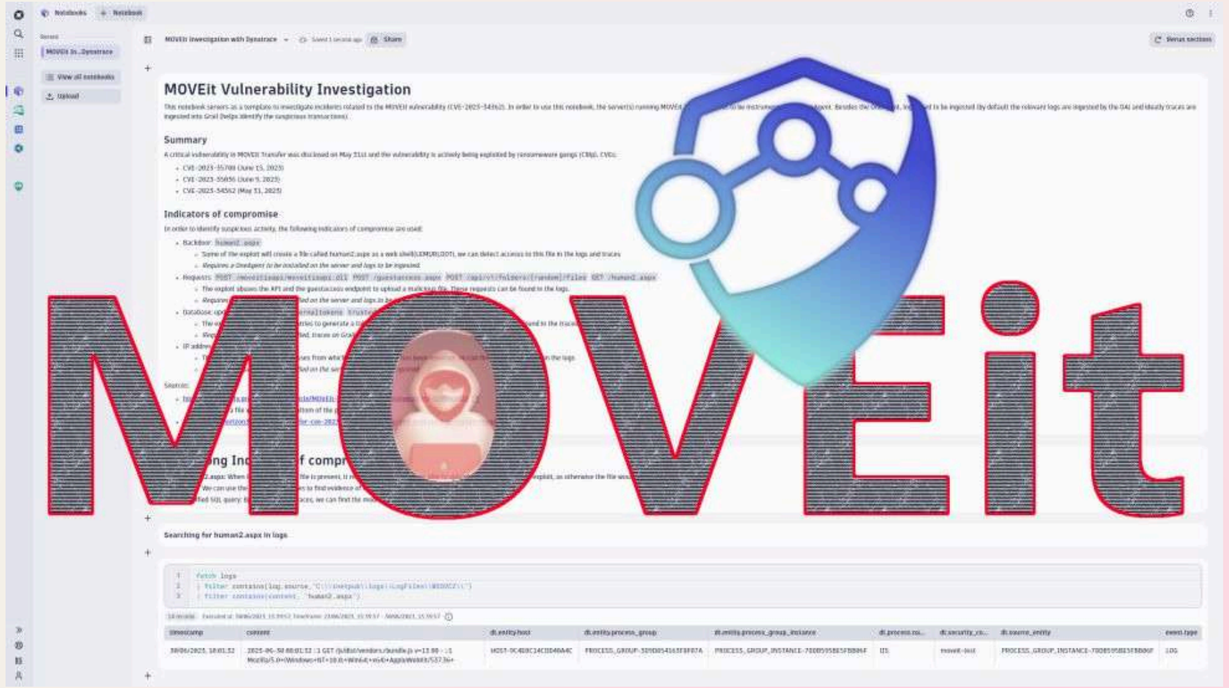
Impacts: Espionage, data theft, and network compromise.

MOVEIT BREACH (2023)

Attacks on Progress Software's MOVEit managed file transfer application. The MOVEit attacks, carried out by the **Clop** cybercriminal group.

Exploited vulnerabilities in file transfer software.

Consequences: Stolen healthcare data of 62 million people globally.



COMMON THREATS IN SUPPLY CHAIN CYBERSECURITY

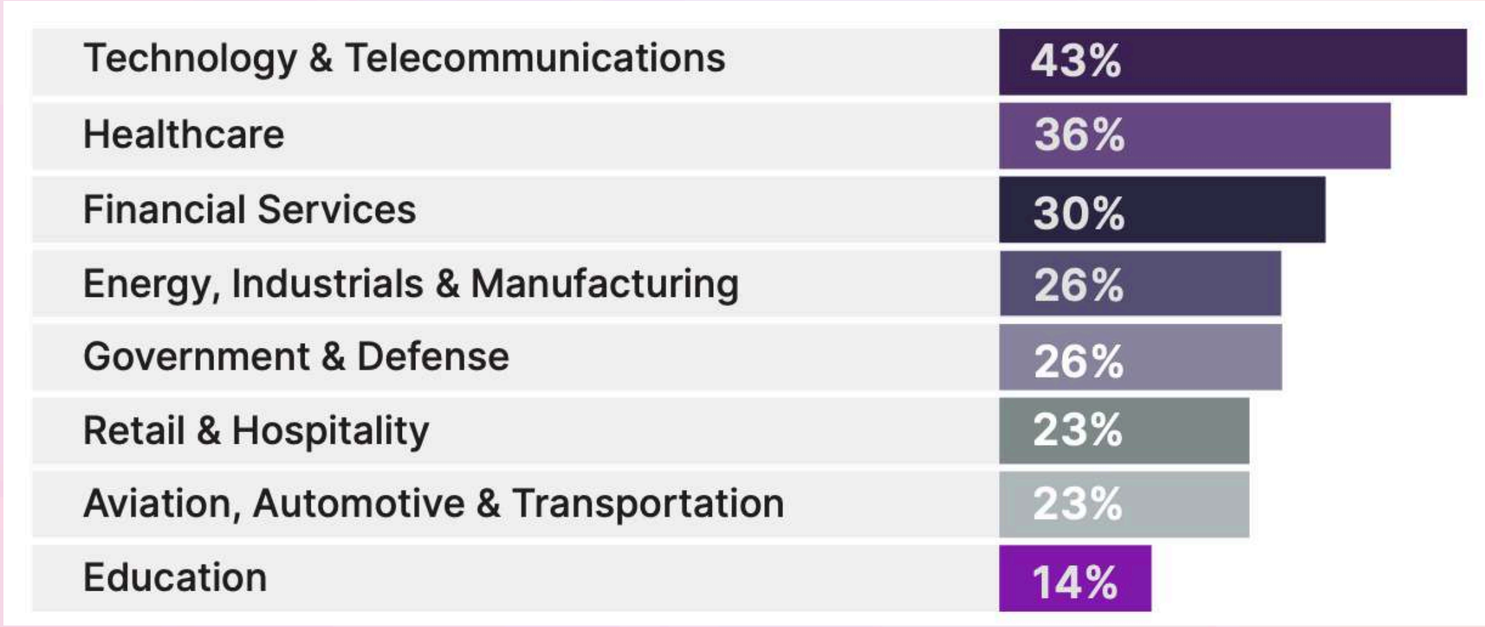
1. **Third-Party Vendor Risks:** Weak cybersecurity practices
2. **Ransomware Attacks:** Critical operations held hostage.
3. **Data Exfiltration:** Theft of sensitive intellectual property.
4. **Hardware & Software Vulnerabilities:** Outdated tools increase risks.

IMPACTS OF SUPPLY CHAIN ATTACKS

- Economic Costs: Recovery, ransom payments, lawsuits.
- Reputation Damage: Customer trust erosion, market value losses.
- National Security Threats: Disruption to critical sectors like healthcare and energy.

IMPACTS OF SUPPLY CHAIN ATTACKS

PERCENTAGE OF THIRD-PARTY BREACHES IN EACH INDUSTRY



The industry with the highest internal rate of third-party breaches was technology & telecommunications at a whopping 43%, exceeding the cross-industry rate of 29% by a wide margin.

WHY ARE SUPPLY CHAINS SO VULNERABLE?

Complexity of supply chains.

Limited visibility into third-party security practices.

Lack of standardized cybersecurity protocols.

Difficulty detecting sophisticated, multi-layered attacks.

PROPOSED SOLUTIONS

Solution 1:
Strengthening Third-Party Risk Management

Real-World Example: Cisco’s Security Assurance Program.

59%

of organizations experienced vendor-related security incidents in 2022.

What are the key steps to effective third party risk management?

The first requirement is that your company is familiar with the nature of risk management plans. The main objective here is not to reduce the use of third parties, but to effectively use third parties to your company’s advantage by identifying, assessing and managing the risks associated with third party relationships.

Strengthening Third-Party Risk Management

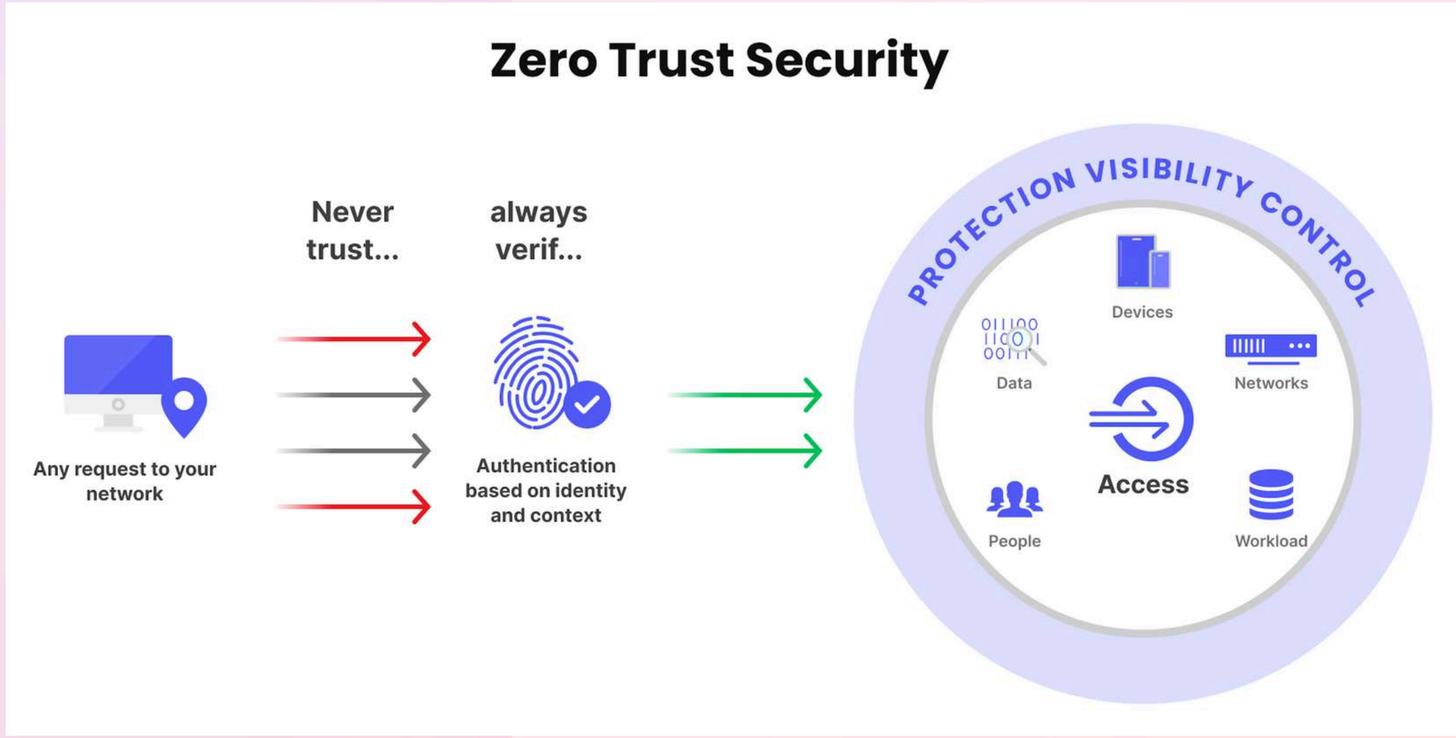
Risk assessment is the cornerstone of an effective risk management program, which should include the following steps:

1.	Deciding whether to engage a third party for a specific purpose, identifying the business case.
2.	Identifying and assessing the potential risks and vulnerabilities associated with engaging third parties
3.	Comparing potential third parties and assessing their qualifications
4.	Identifying the risks associated with the third party in question.

SOLUTION 2: ZERO TRUST ARCHITECTURE

The National Institute of Standards and Technology (NIST) introduced Zero Trust Architecture (ZTA) in Special Publication SP 800-207, defining it as a key cybersecurity concept for today's enterprise infrastructure.

Continuous verification of identity and access.



Real-World Example: Google's BeyondCorp model.

- Impact: 80-90% breach risk reduction with Zero Trust models.

ZERO TRUST ARCHITECTURE

Zero Trust architecture is based on several key principles:

1.	All data and computing resources are considered assets	This means that every device, system, and user should be treated with strong authentication, without any assumptions about “security by default”
2.	Trust is location independent	Even devices connected to the corporate network should be verified in the same way as external ones
3.	Dynamic authentication and authorization	Access rights are granted at the level of an individual session, with the minimum privileges necessary to perform a specific task
4.	Access policies are formed based on many attributes	Both internal (user role, device) and external (location, time, and behavioral data)
5.	The integrity of all assets is checked regularly	The organization must have mechanisms for continuous monitoring and remediation of vulnerabilities on devices
6.	Control at all levels	Access to resources is controlled at the authentication and authorization level, which includes the use of multi-factor authentication (MFA) and other control methods

REAL DATA PROVIDING IMPACT OF ZERO TRUST

A 2023 Forrester Research report found that **62%** of organizations implementing Zero Trust reported a reduction in data breaches, with many also seeing improvements in their ability to detect and respond to incidents.

Zscaler, a leader in Zero Trust security, reported that their customers saw an average of **90%** fewer security incidents after migrating to a Zero Trust framework.

Solution 3:

COLLABORATIVE THREAT INTELLIGENCE SHARING

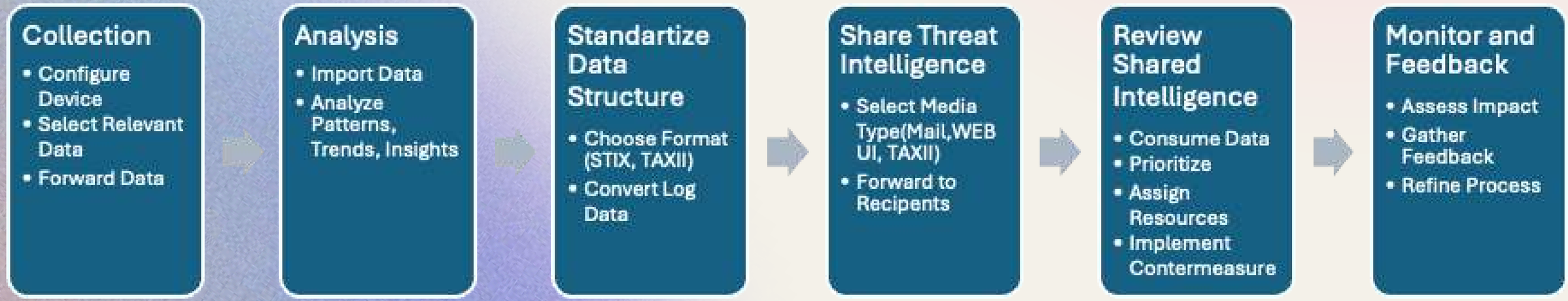
Platforms like ENISA’s ECSP enable real-time data sharing

To maintain privacy and foster collaboration, organizations should establish clear guidelines and use standardized protocols like Structured Threat Information Expression (STIX) or Trusted Automated eXchange of Indicator Information (TAXII) when sharing threat intelligence outside the company

Benefits: 30% faster response to threats, reduced impact of attacks.

THREAT INTELIGENCE SHARING PROCESS:

STIX or TAXII, are used to structure the data, ensuring consistency, readability, and easy processing by different tools and systems. Organizations share this threat intelligence through various channels, including email, file transfers, web platforms, or automated protocols like STIX and TAXII



IMPACT OF COLLABORATIVE THREAT INTELLIGENCE SHARING

ENISA is a prime example of how collaborative threat intelligence sharing can help mitigate supply chain risks. ENISA's platform has been instrumental in helping EU members prevent coordinated cyberattacks targeting their supply chains, such as those in the **2017 NotPetya** campaign, which disrupted companies globally.

Effectiveness of Threat Intelligence Sharing, according to a 2021 Cybersecurity Collaborative survey, **72%** of organizations that engaged in threat intelligence sharing reported a significant reduction in the number of security incidents.

A study by IBM found that organizations that actively share cybersecurity intelligence with their peers experienced **30%** fewer data breaches than those that do not participate in such collaborations.

INDUSTRY-SPECIFIC VULNERABILITIES

Healthcare: High volume of sensitive data and complex ecosystems.

Finance: Regular target for ransomware and data theft.

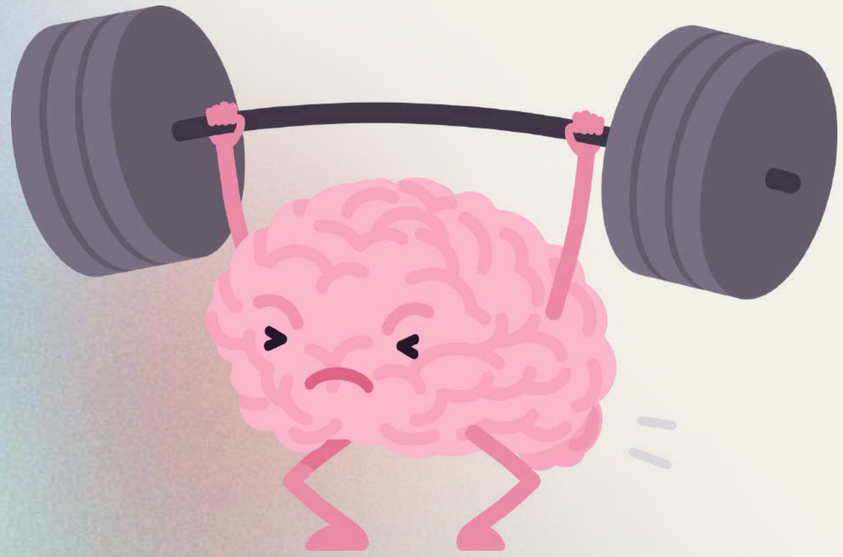
Technology: High dependency on third-party software and open-source tools.

FUTURE TRENDS

- Increased use of malicious open-source packages (e.g., npm, PyPI).
- Regulatory focus on incident reporting and risk management.
- Rise in AI-related vulnerabilities due to insufficient safeguards.

Source: The State of Software Supply Chain Security 2024, pg. 6-9

STEPS TO ENHANCE RESILIENCE



- Implement robust supply chain monitoring tools.
- Increase investment in cybersecurity audits.
- Foster collaboration with industry partners.
- Emphasize Secure-by-Design development principles.

CALL TO ACTION

Encouragement: Adopt proactive cybersecurity practices.

Invest: In advanced technologies and Zero Trust frameworks.

Collaborate: Across industries and nations for shared intelligence.

CONCLUSION

Challenges, impacts, and solutions in supply chain cybersecurity.

Takeaway: Collective action is crucial to building resilience.

REFERENCES:

	LINKS
ENISA Threat Landscape for Supply Chain Attacks	https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
Global Third-Party Cybersecurity Breaches Report	https://securityscorecard.com/wp-content/uploads/2024/02/Global-Third-Party-Cybersecurity-Breaches-Final-1.pdf
The State of Software Supply Chain Security 2024	https://3375217.fs1.hubspotusercontent-na1.net/hubfs/3375217/Documents/The-State-of-Software-Supply-Chain-Security-2024.pdf
And my own report that I wrote to understand deeply the problem	Contact me if you want to get my report, since I didnt upload it one the internet

ICT Risk
Assesment Course
24/25

THANKS FOR YOUR ATTENTION AND TIME

If you will have any further question, feel free to contact me:

zadagerei0405@gmail.com
z.zadagerey@unipi.studenti.it