SECURITY SUMMIT

Security Summit

Streaming Edition 5 novembre 2025

Clusit 25th 2000-2025

ASTREA

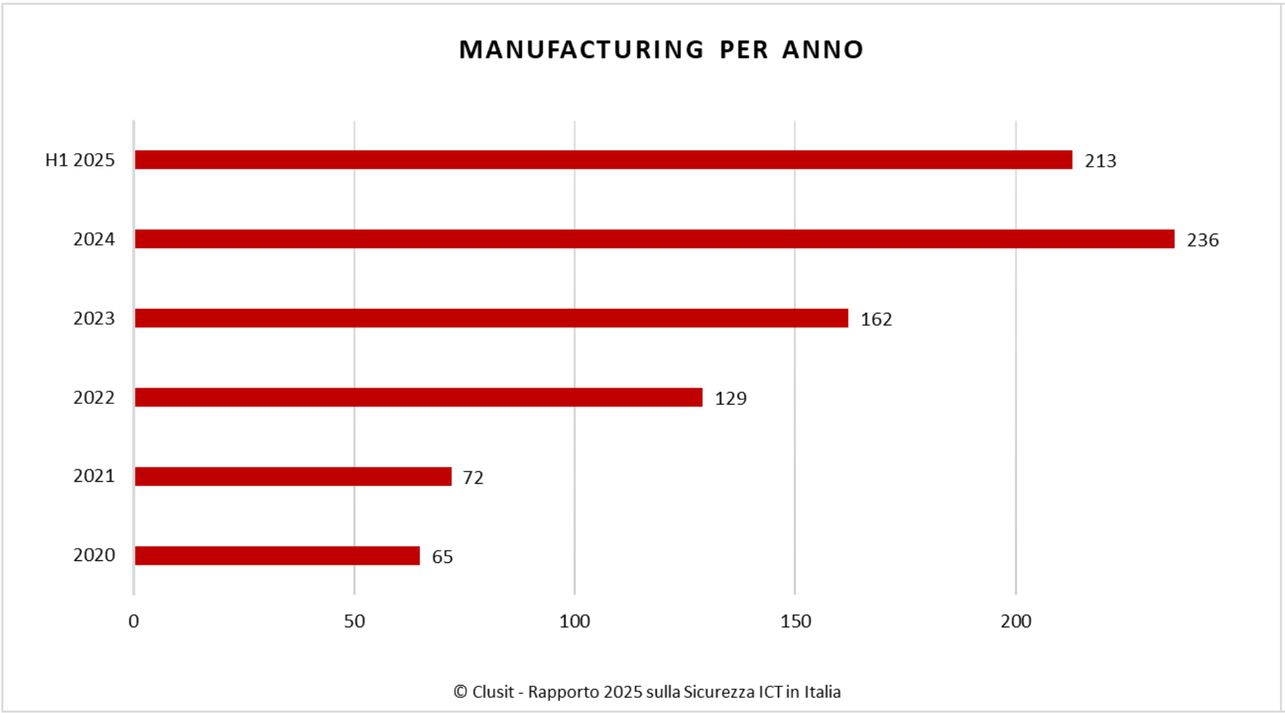
Sessione Manufacturing

Sicurezza della Supply Chain Manifatturiera: l'impatto della NIS2

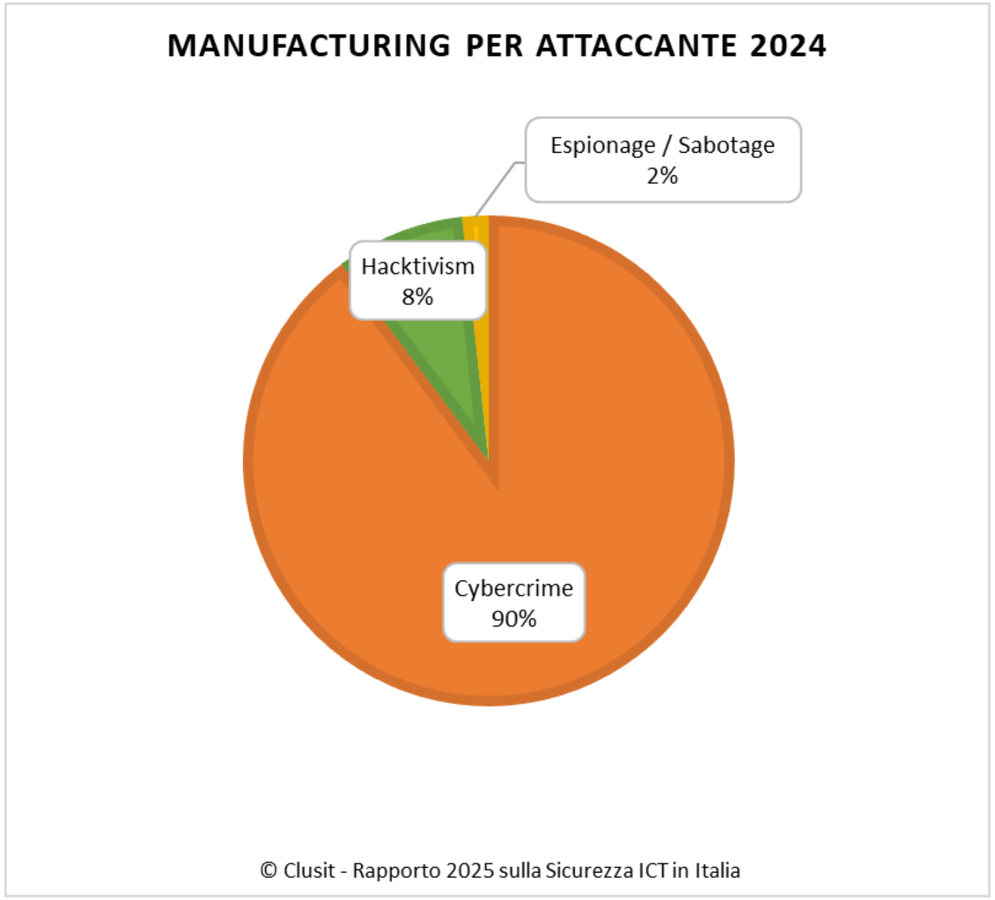
Modera **Paola Girdinio**, CD Clusit
Intervento di **Milena Antonella Rizzi -** Capo Servizio Regolazione dell'**Agenzia per la Cybersicurezza Nazionale**
Partecipano:
- **Lorenzo Ivaldi,** UNIGE
- **Andrea Monteleone**, Presidente di ANIE Sicurezza
- **Ivan Monti**, CISO, Ansaldo Energia
- **Alessio Pennasilico**, CS Clusit
- **Valeria Prosser**, Head of Governance, Risk & Compliance, E-phors S.p.a.

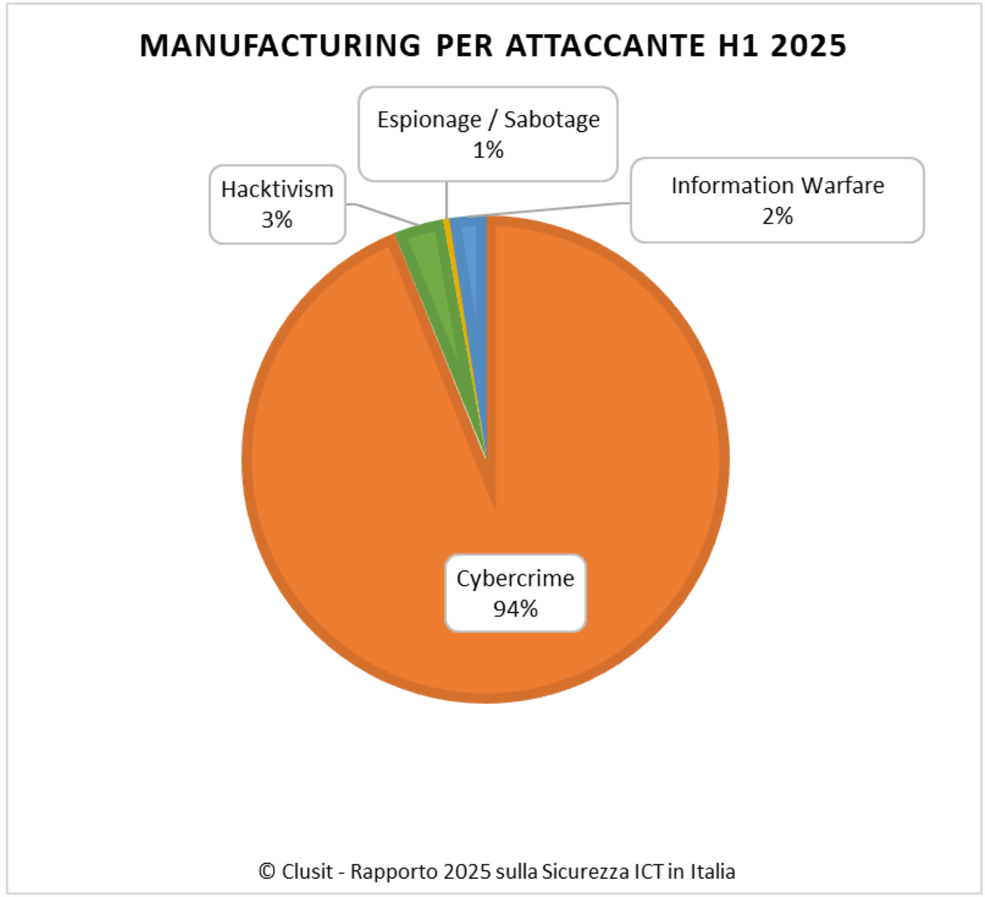
Orario 16.30 – 18.00

Dati dal Rapporto Clusit sulla sicurezza ICT in Italia
(Ed. Novembre 2025, con i dati da 1.1 al 30.6.2025)

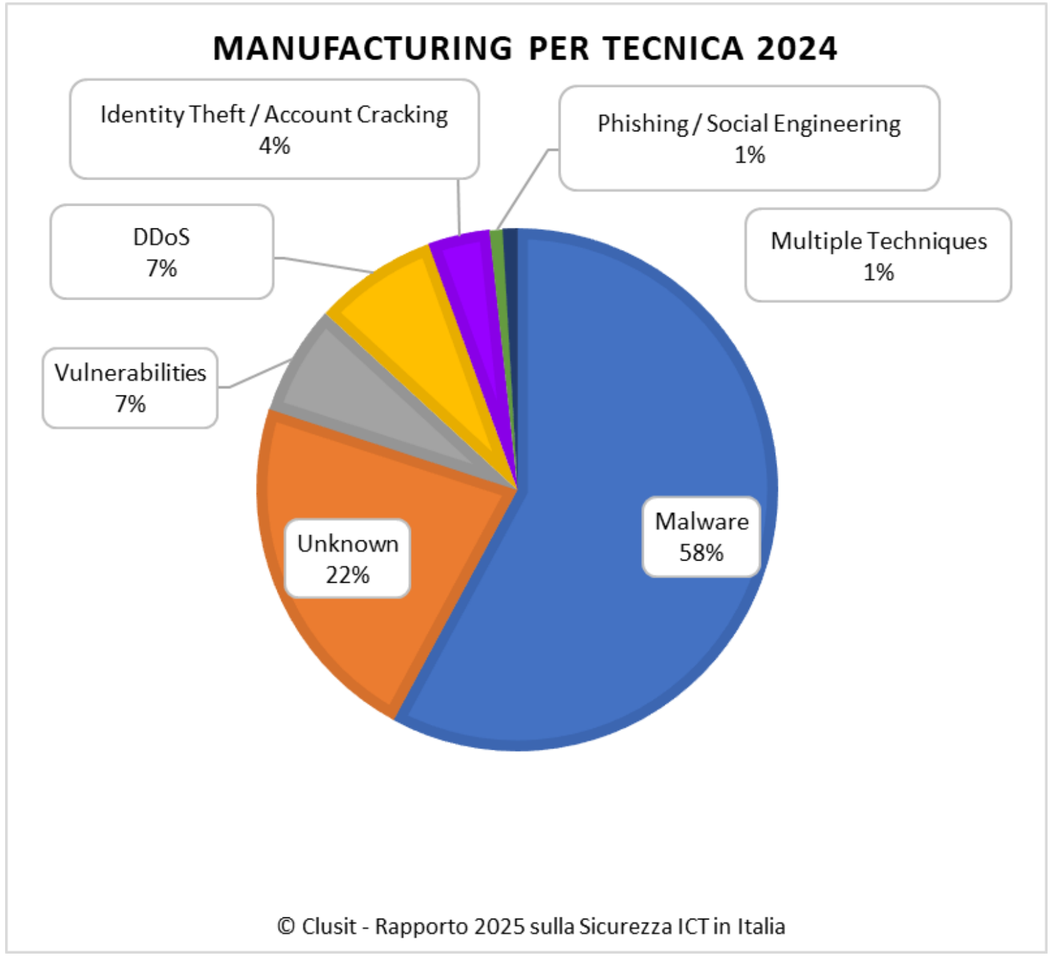


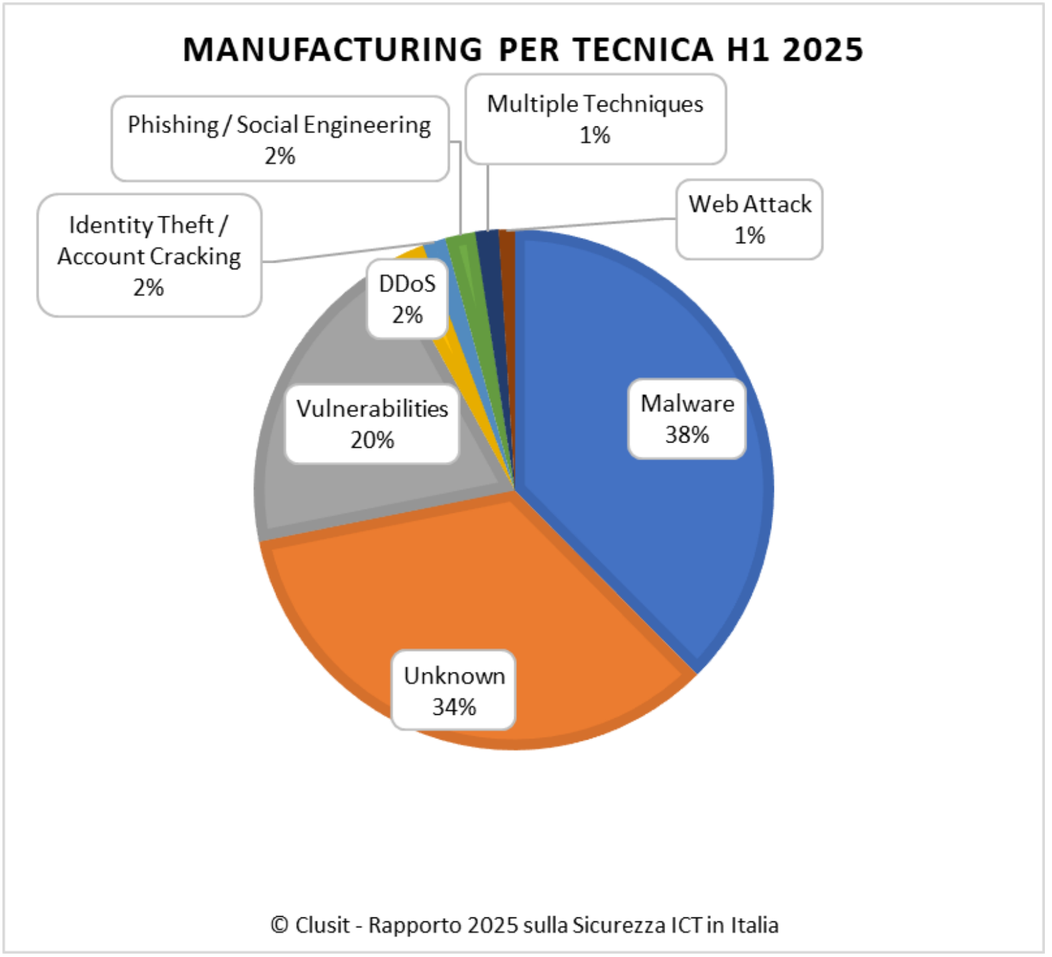
- H1 2025 trend sul 45% (stima dei 213 attacchi rispetto ai 236 del 2024)
- Settore manifatturiero al centro del mirino degli attaccanti



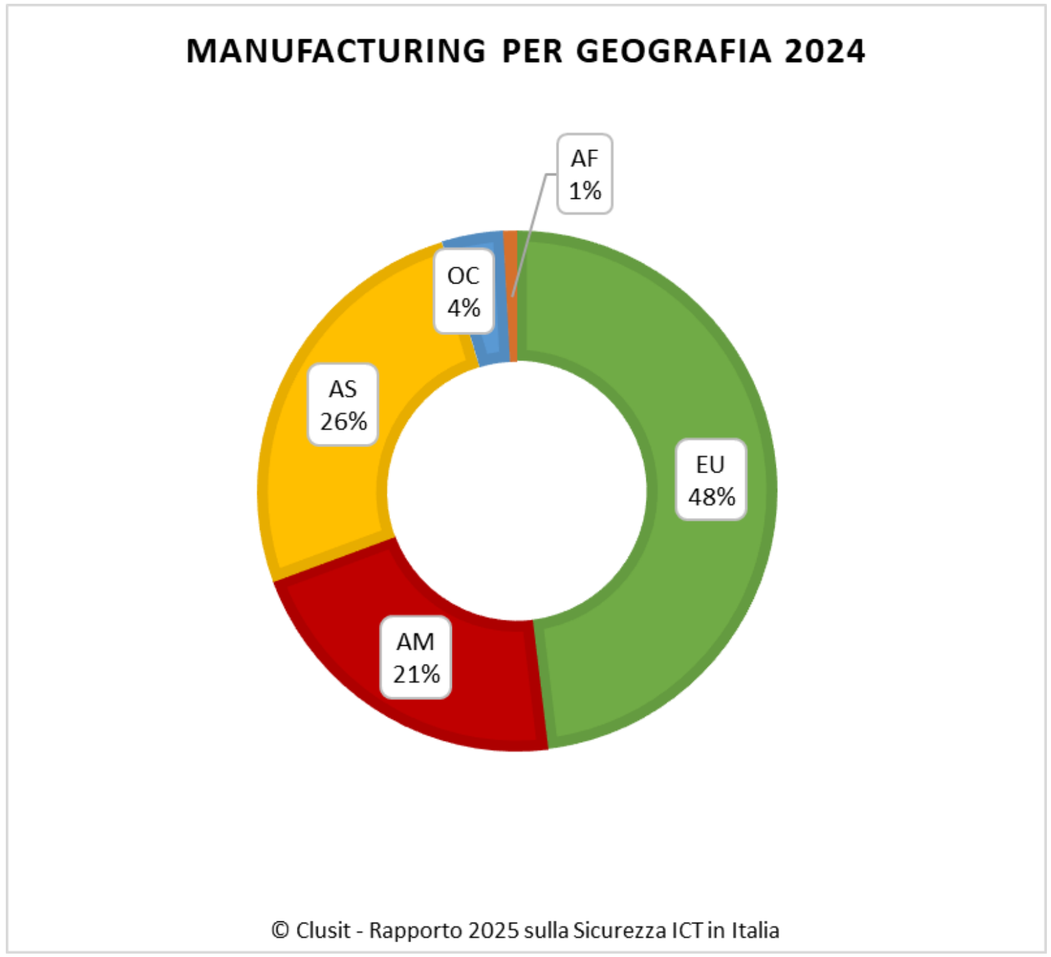


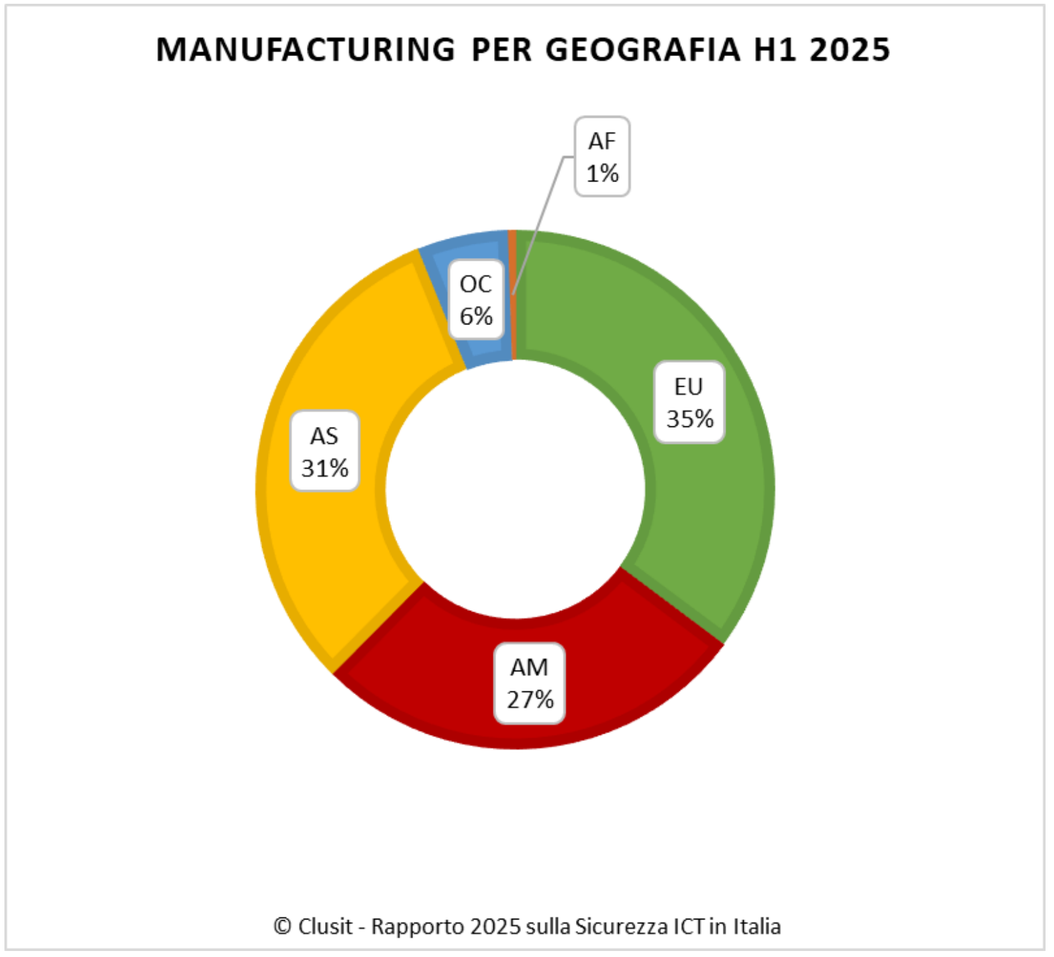
- Cresce ancora la minaccia del cybercrime"



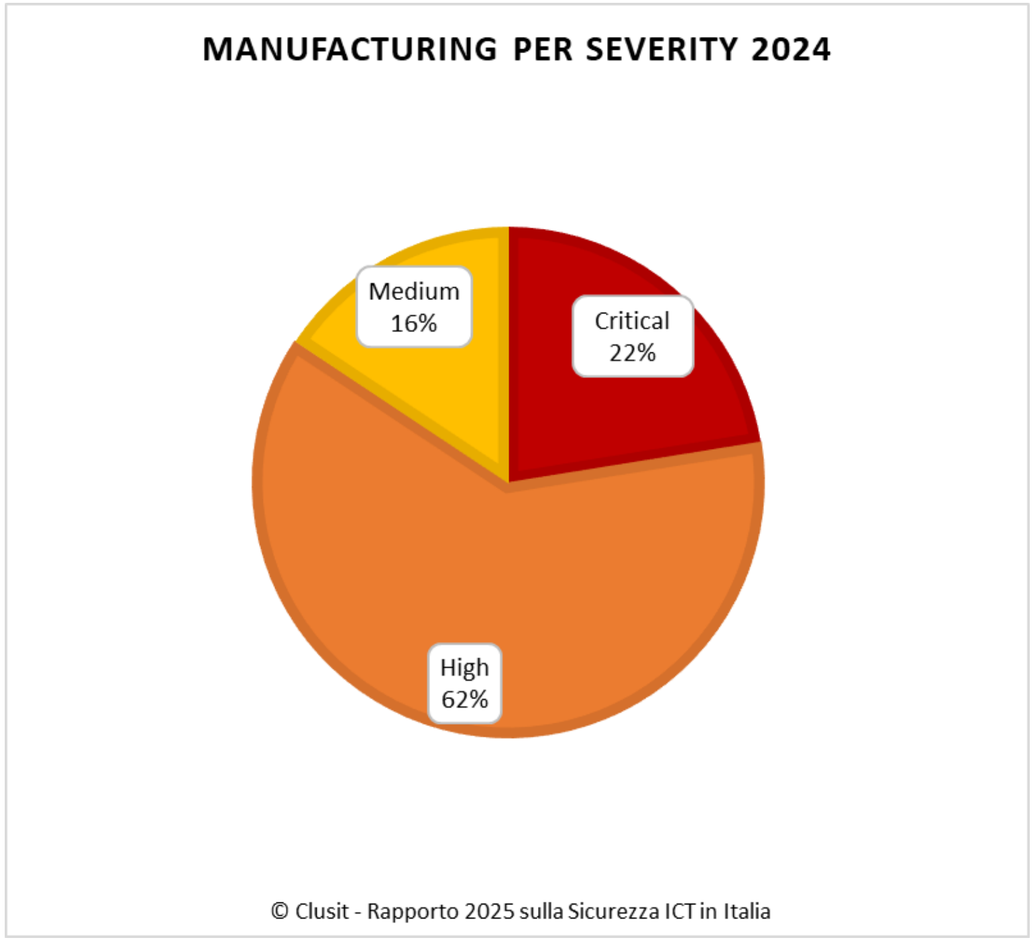


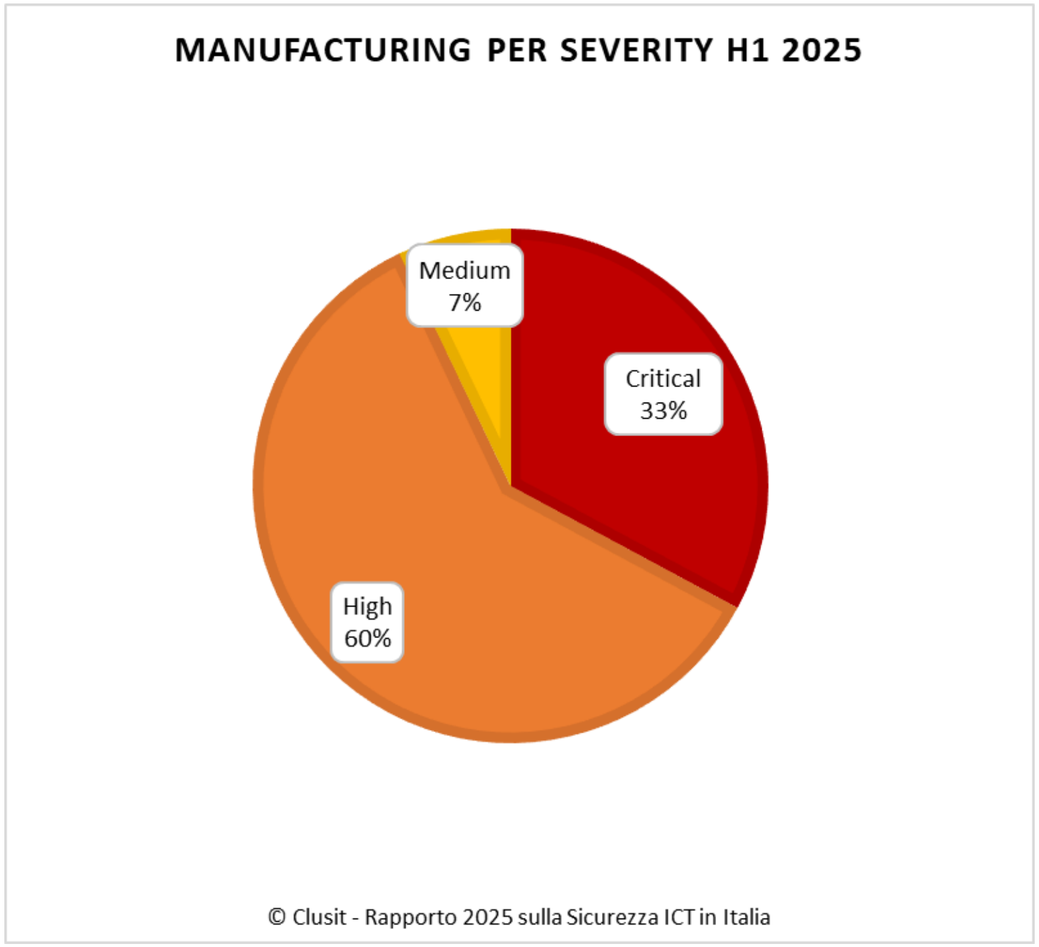
- Il Malware scende, ma gli 0-Day salgono
- Le vulnerabilità note e non patchate arrivano al 20%



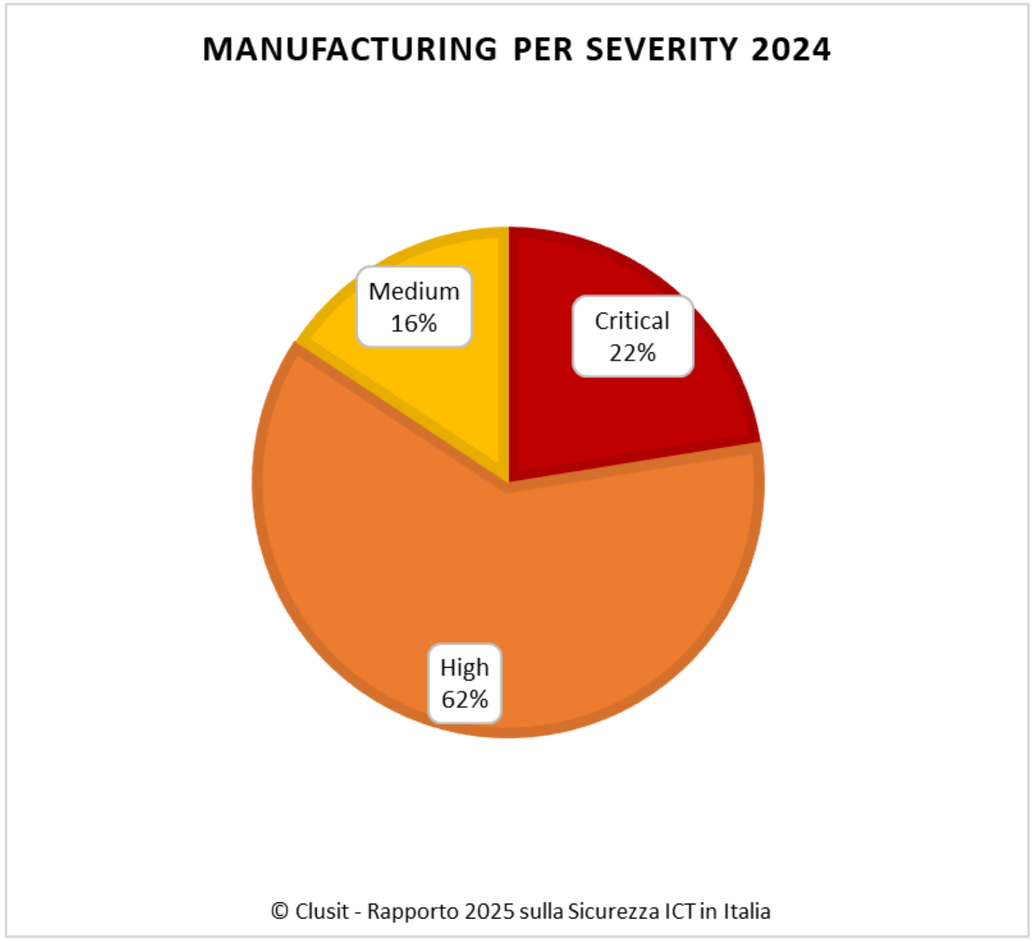


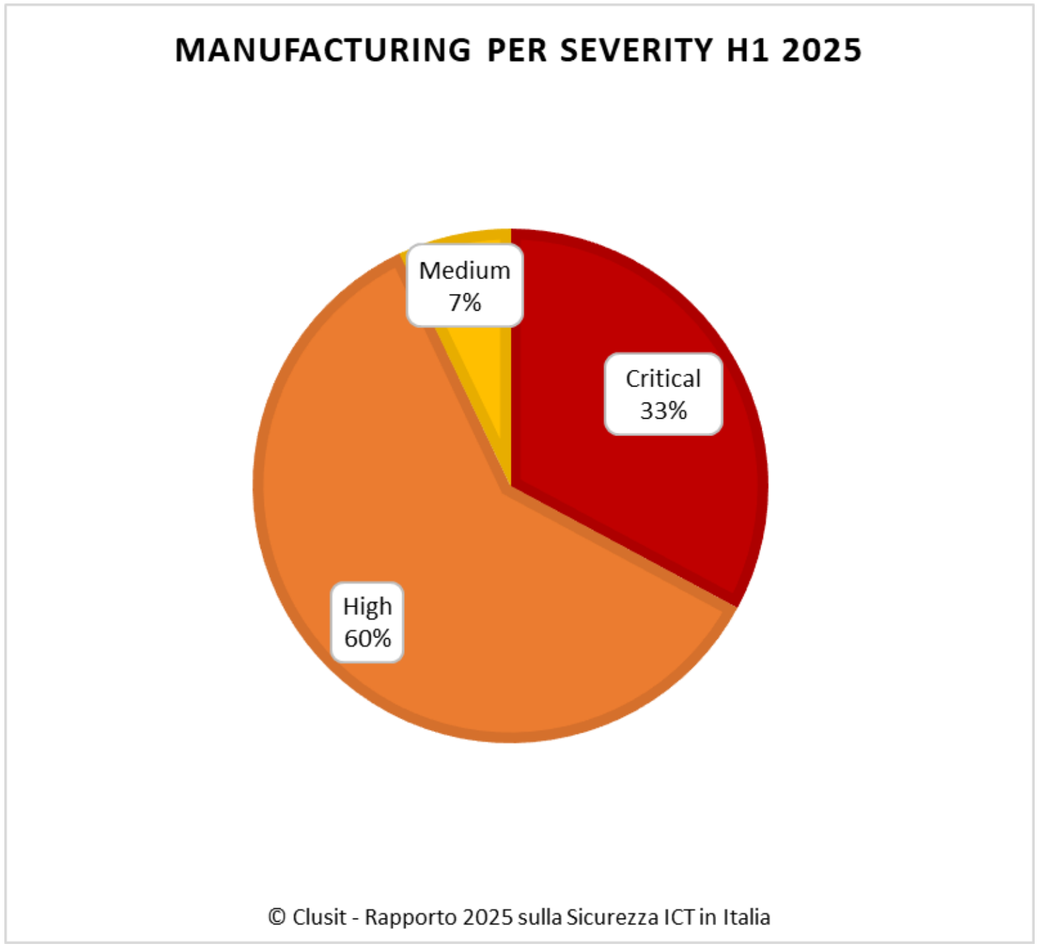
- L’Europa è sempre il bersaglio preferito
- L’Asia dichiara qualche attacco in più, così come le Americhe





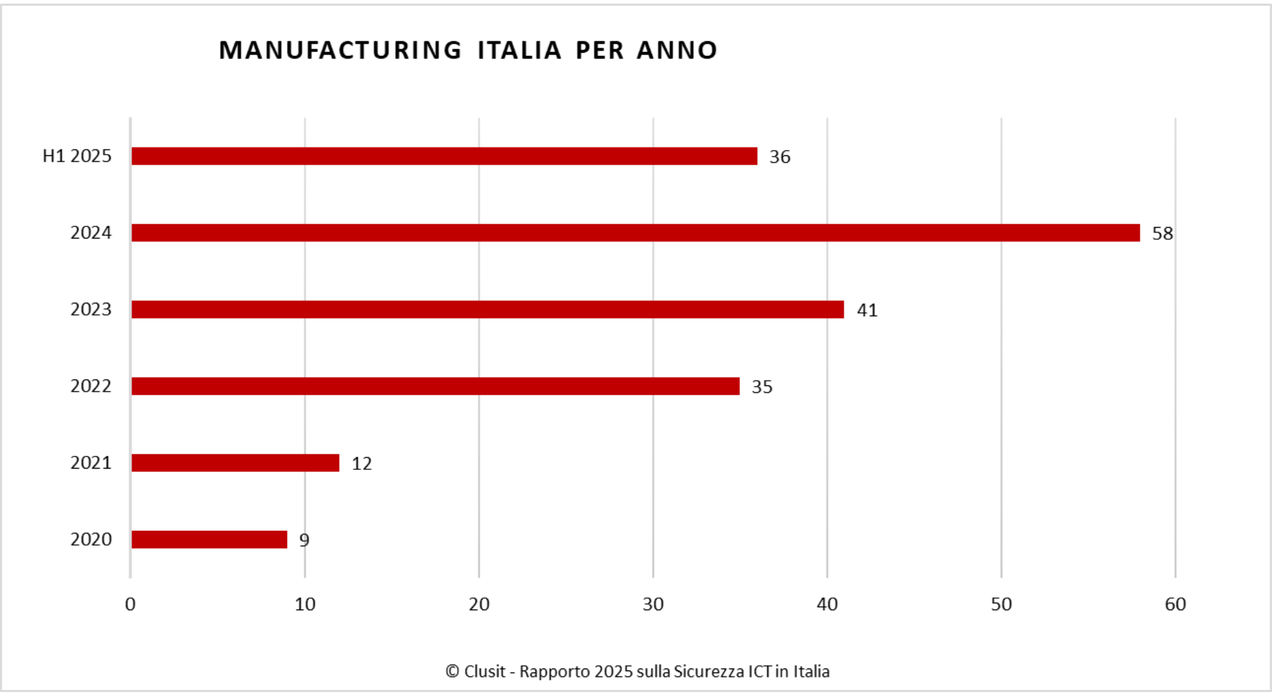
Attacchi con impatti critici al 22% nel 2024, saliti al 33% nell’ H1-2025

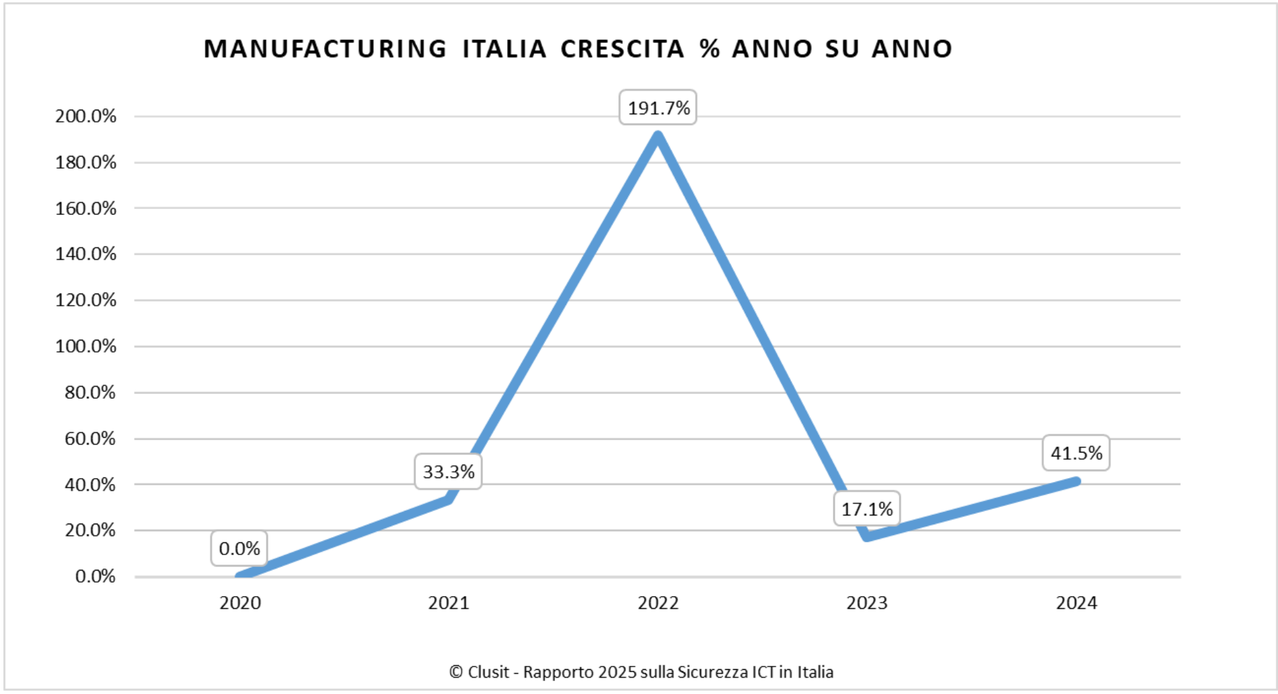




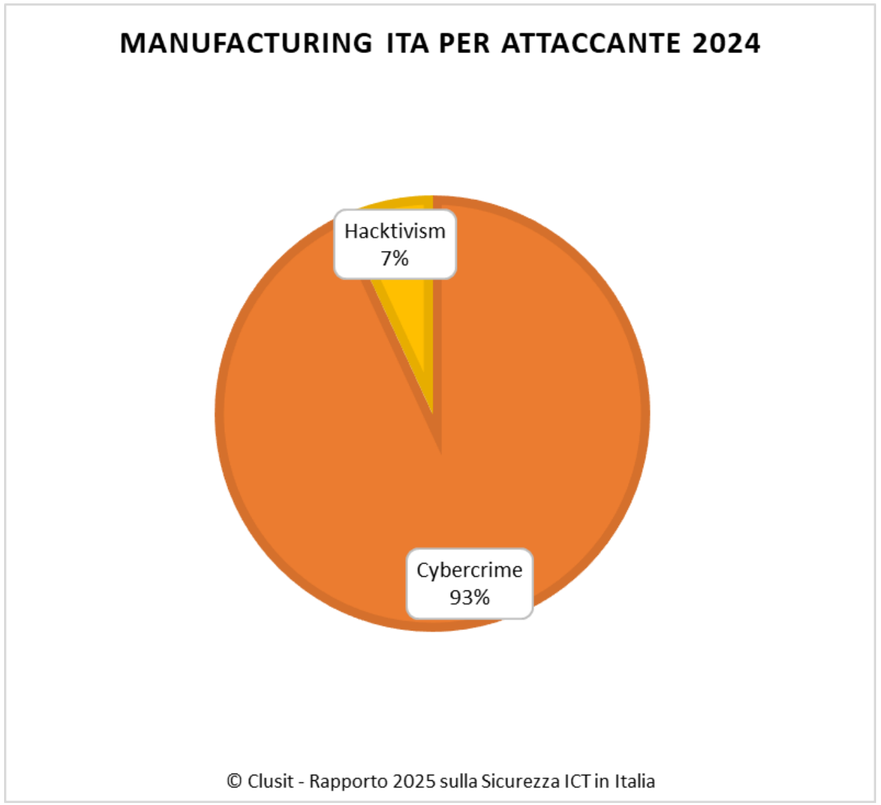
Gravità degli attacchi in crescita:
meno attacchi di media gravità e in crescita attacchi di gravità alta o critica"

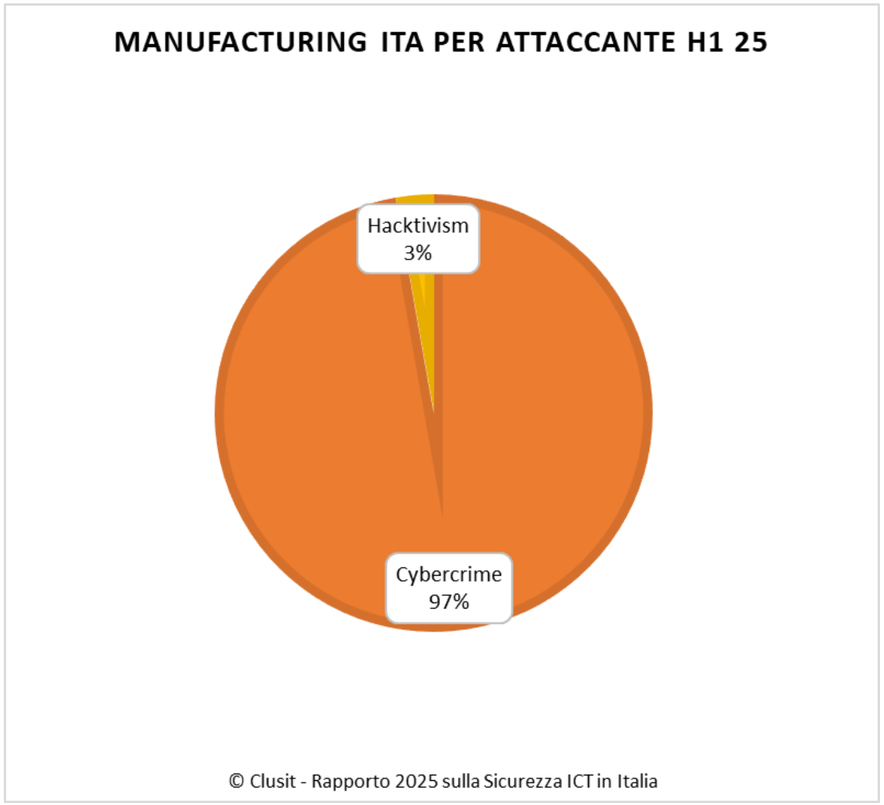
La situazione nazionale



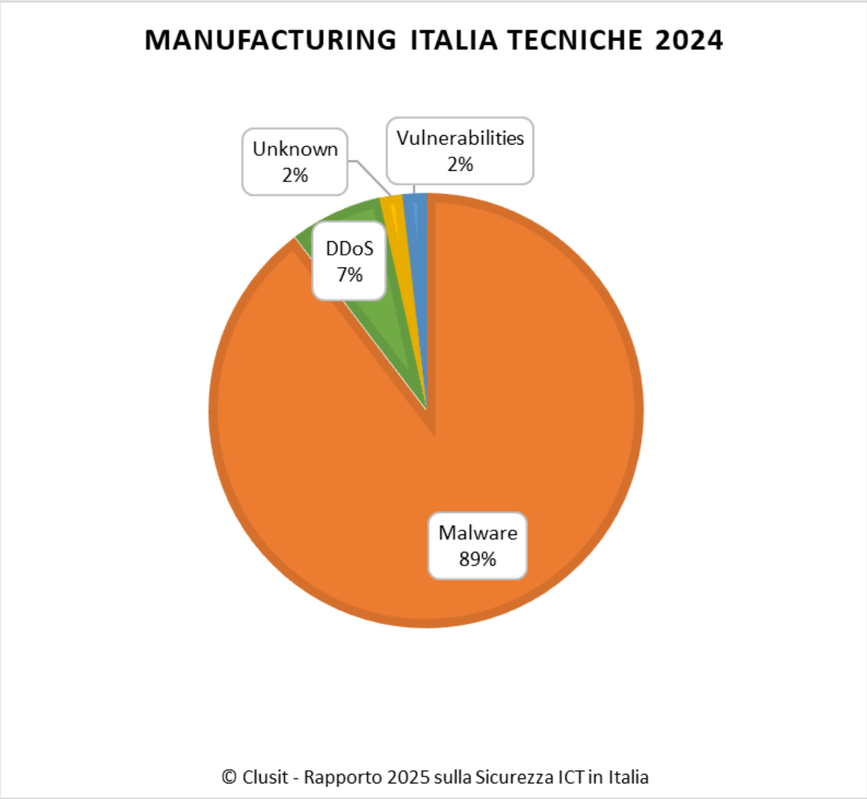


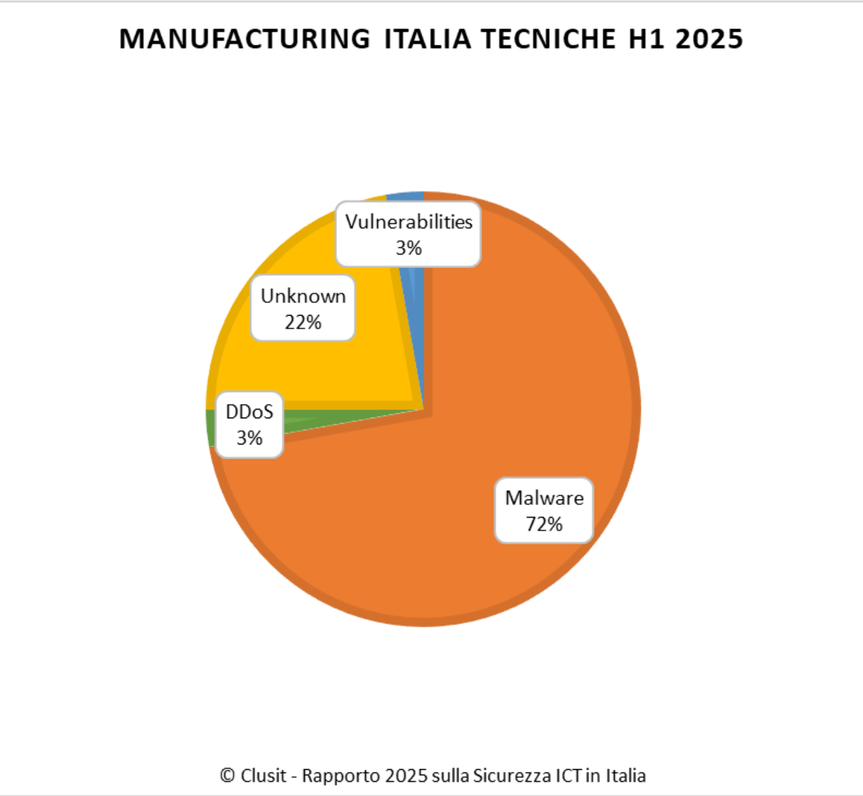
- H1 2025 trend sul 41%, lievemente meglio del Worldwide
- Il manifatturiero nazionale rimane nodo critico della filiera europea da proteggere



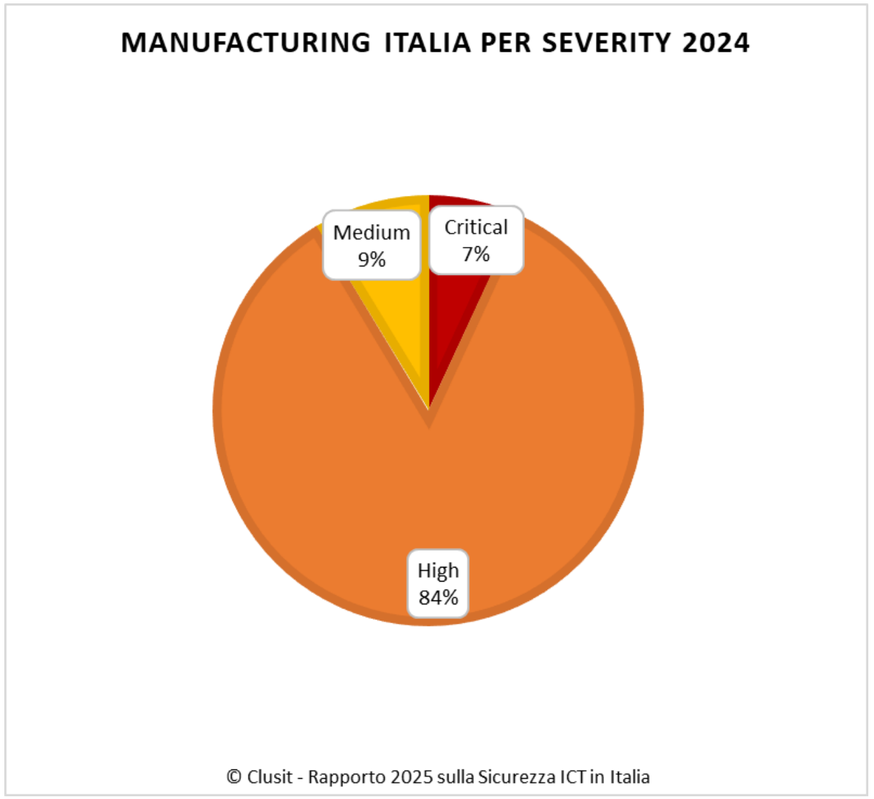


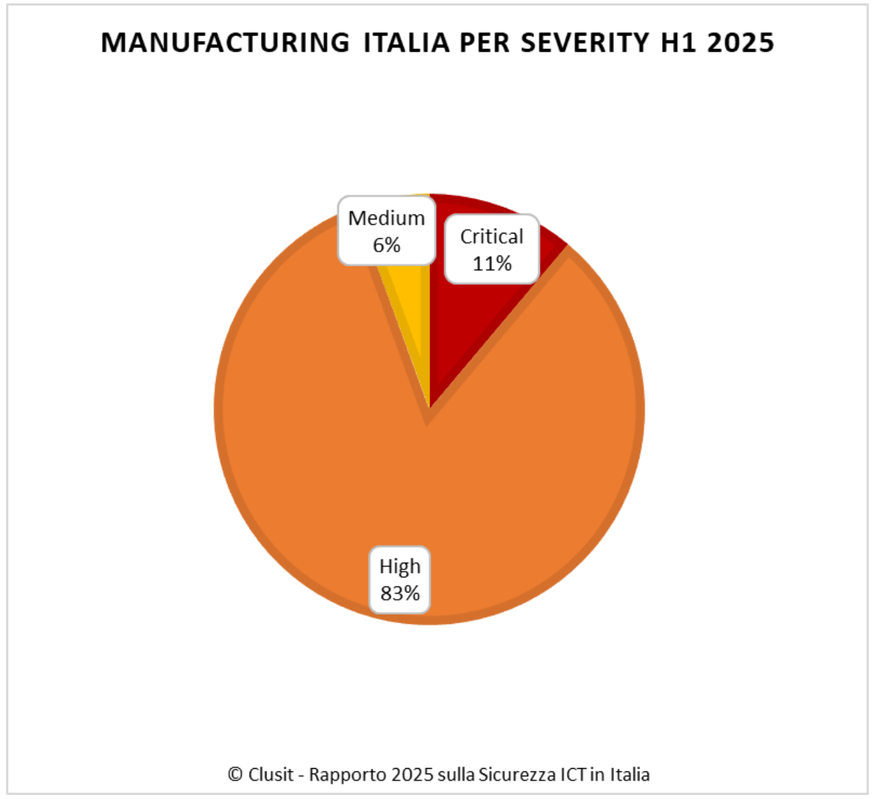
- Gli attacchi sono quasi tutti Cybercrime anche in Italia





- Scende il malware, ma crescono gli 0-Day
- Vulnerabilità non patchate sempre basse





- Meno attacchi critici
- Comunque troppi High

Due ulteriori punti di vista: Report Dagos 2025

Key Ransomware Findings

87%

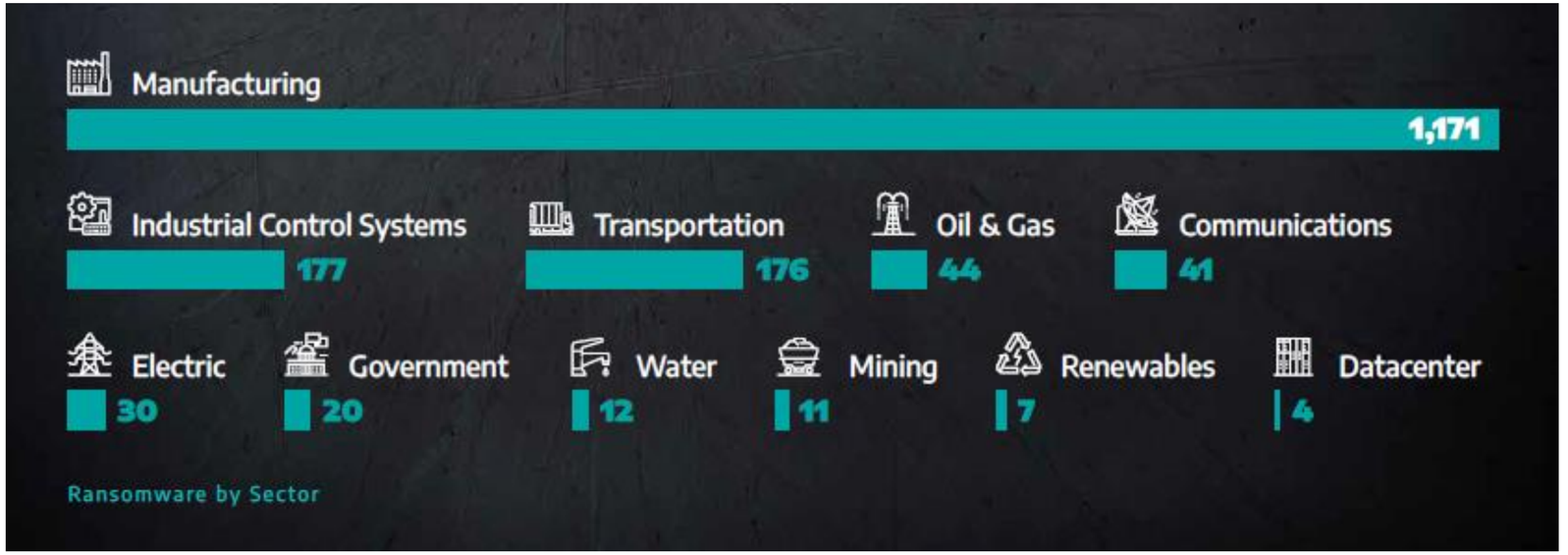
Ransomware attacks against industrial organizations **increased 87 percent** over the previous year.

60%

Dragos tracked **60 percent more ransomware groups** impacting OT/ICS in 2024.

69%

of all ransomware attacks targeted **1,171 manufacturing entities** in **26 unique manufacturing subsectors**.



MDDR 2025

Top 10 recommendations from this report

1. Manage cyber risk at the boardroom level

Treat cybersecurity as a business risk on par with financial or legal challenges. It is important that corporate boards and CEOs understand the security weaknesses of their organization. Track and report metrics like multifactor authentication (MFA) coverage, patch latency, incident counts, and incident response time to develop a comprehensive understanding of both your organization's potential vulnerabilities and its preparedness in the event of a cybersecurity incident.

2. Prioritize protecting identities

Since identity is the top attack vector, enforce phishing-resistant multifactor authentication across all accounts, including administrative accounts.

3. Invest in people, not just tools

Cybersecurity is a whole-of-organization effort. Find ways to upskill your workforce and consider making security part of performance reviews. Culture and readiness—not just technology—are primary factors in both an organization's defenses and its resilience.

4. Defend your perimeter

A third of attackers use crude tactics as the easy path into an organization's exposed footprint, often looking beyond what you deploy to the vendors and supply chain you trust, including perimeter web-facing assets (18%), external remote services (12%), and supply chains (3%). Knowing the full scope of your perimeter, auditing the accesses you grant to trusted partners, and patching any exposed attack surface forces attackers to work harder to be successful.

5. Know your weaknesses and pre-plan for breach

Combine knowledge of the organization's exposure footprint with organizational risk awareness to develop a proactive plan for responding to future breach. Tie security controls to business risks in terms the board can understand. Since a breach is a matter of when, not if, develop, test, and practice your incident response (IR) plan—including specific scenarios for ransomware attacks, which remain one of the most disruptive and costly threats to operations. How fast can you isolate a system or revoke credentials?

6. Map and monitor cloud assets

Since the cloud is now a primary target for adversaries, conduct an inventory on every cloud workload, application programming interface (API), and identity within the organization, and monitor for rogue virtual machines, misconfigurations, and unauthorized access. At the same time, work proactively to enforce app governance, conditional access policies, and continuous token monitoring.

7. Build and train for resiliency

If breaches are all but inevitable, resilience and recovery become key. Backups must be tested, isolated, and restorable, and organizations should have clean rebuild procedures for identity systems and cloud environments.

8. Participate in intelligence sharing

Cyber defense is a team, not individual, sport. By sharing and receiving real-time threat data with peers, industry groups, and government, we can make it harder for cyber adversaries to achieve their goals.

9. Prepare for regulatory changes

It's more important than ever for organizations to align with emerging laws like the European Union (EU) Cyber Resilience Act or United States (US) critical infrastructure mandates, which may require reporting cyber incidents within a certain timeframe or Secure by Design practices. These regulations reinforce the importance of timely incident reporting and stronger internal oversight of an organization's cybersecurity practices.

10. Start AI and quantum risk planning now

Stay ahead of emerging technologies. Understand both the benefits and risks of AI use within an organization and adjust your risk planning, attack surface exposure, and threat models appropriately. Prepare for a post-quantum cryptography (PQC) world by taking the time to inventory where encryption is used and create a plan to upgrade to modern standards as they evolve.