SECURITY SUMMIT

9 novembre 2023

Security Summit

Streaming Edition

Clusit Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

Security Summit Manufacturing

9 novembre orario 15.00-17.00

Modera: **Enzo Maria Tieghi,** CS Clusit

Partecipano:

•**Prof.ssa Paola Girdinio**, Presidente Centro di Competenza per la Sicurezza delle Infrastrutture Strategiche Digitali START 4.0

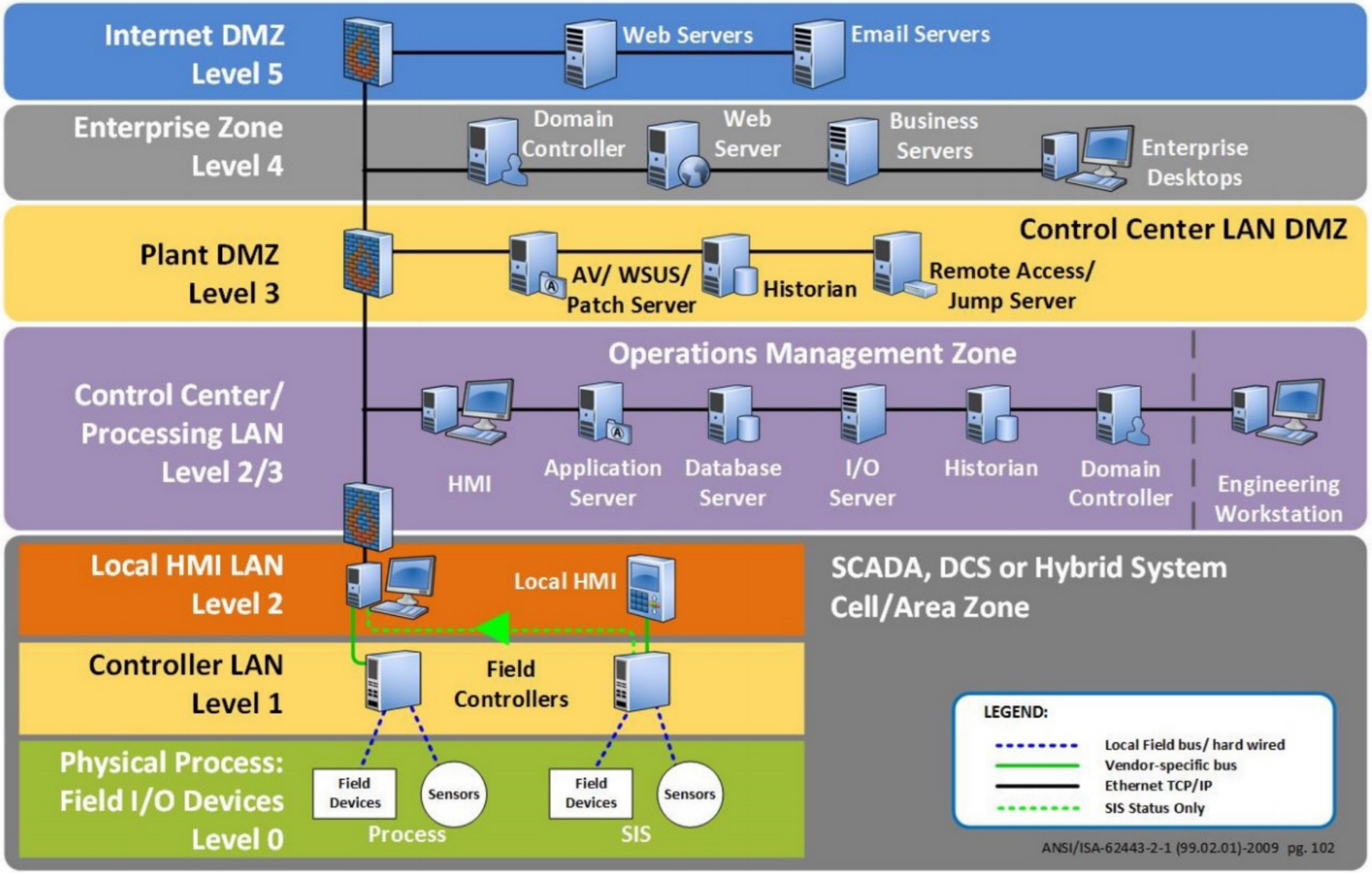
•**Ing. Lorenzo Ivaldi,** UNIGE Dipartimento di ingegneria navale, elettrica, elettronica e delle telecomunicazioni – DITEN

•**Giulio Iucci**, Presidente di ANIE Sicurezza

•**Alessandro Manfredini**, Presidente AIPSA e Direttore di Group Security e Cyber Defence del Gruppo A2A

•**Simone Peruzzi,** Enterprise Security Executive, Microsoft Italia

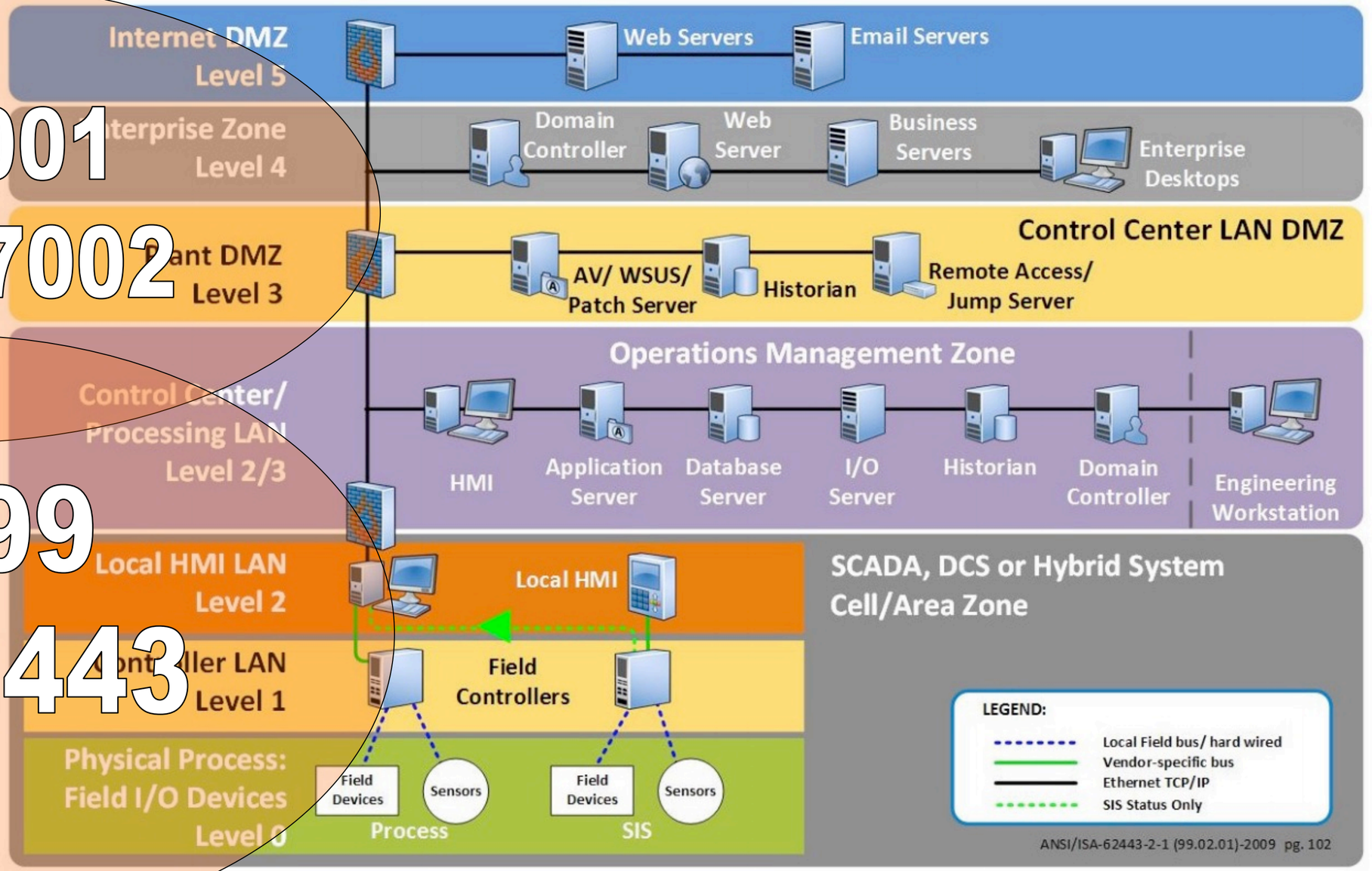
OT SECURITY: DI COSA PARLIAMO ? (ISA95 & PURDUE MODEL)



CONVERGENZA IT-OT, ISO-27K & IEC-62443

ISO27001
& ISO27002

ISA99
IEC62443



Transizione/Industria 4.0 e 5.0 : un mondo in trasformazione

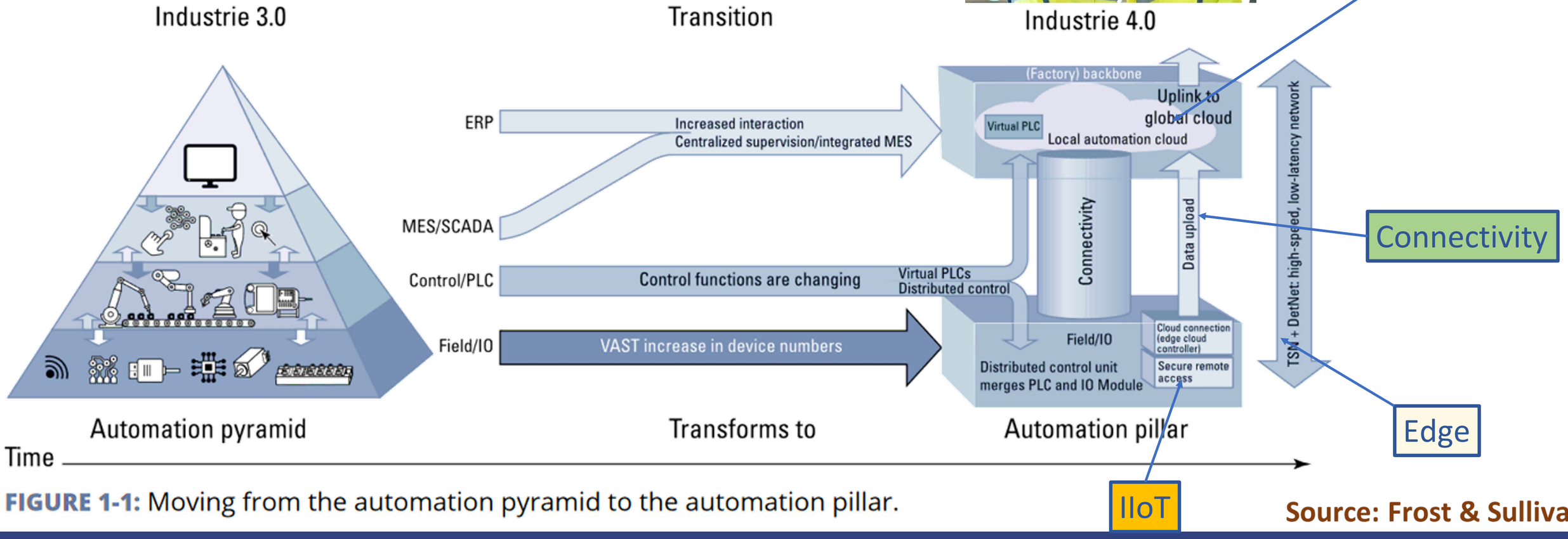
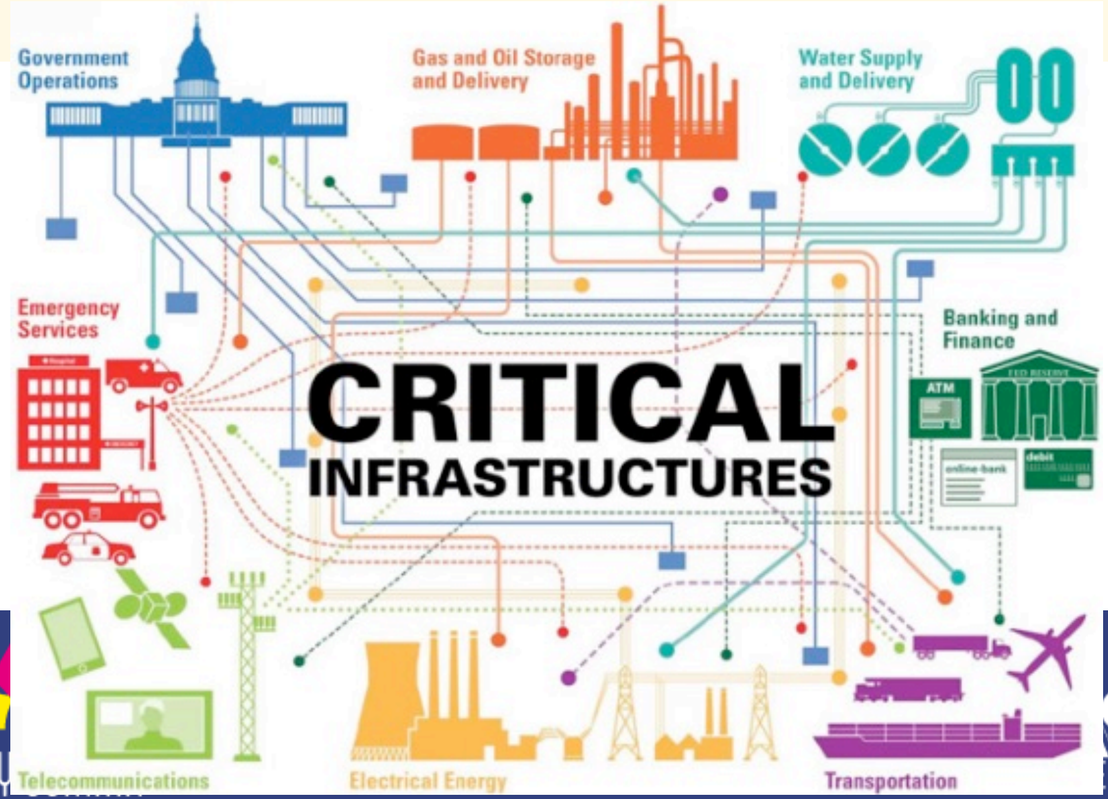


FIGURE 1-1: Moving from the automation pyramid to the automation pillar.

Source: Frost & Sullivan

“Le Infrastrutture Critiche e molti altri sistemi digitali, meno tutelati a livello normativo ma comunque essenziali per la collettività, saranno bersagli designati, costantemente al centro del mirino di numerosi attori, governativi e non.”

(cit. Andrea Zapparoli Manzoni).



I.C. ed Incidenti Cyber: Trend in Crescita

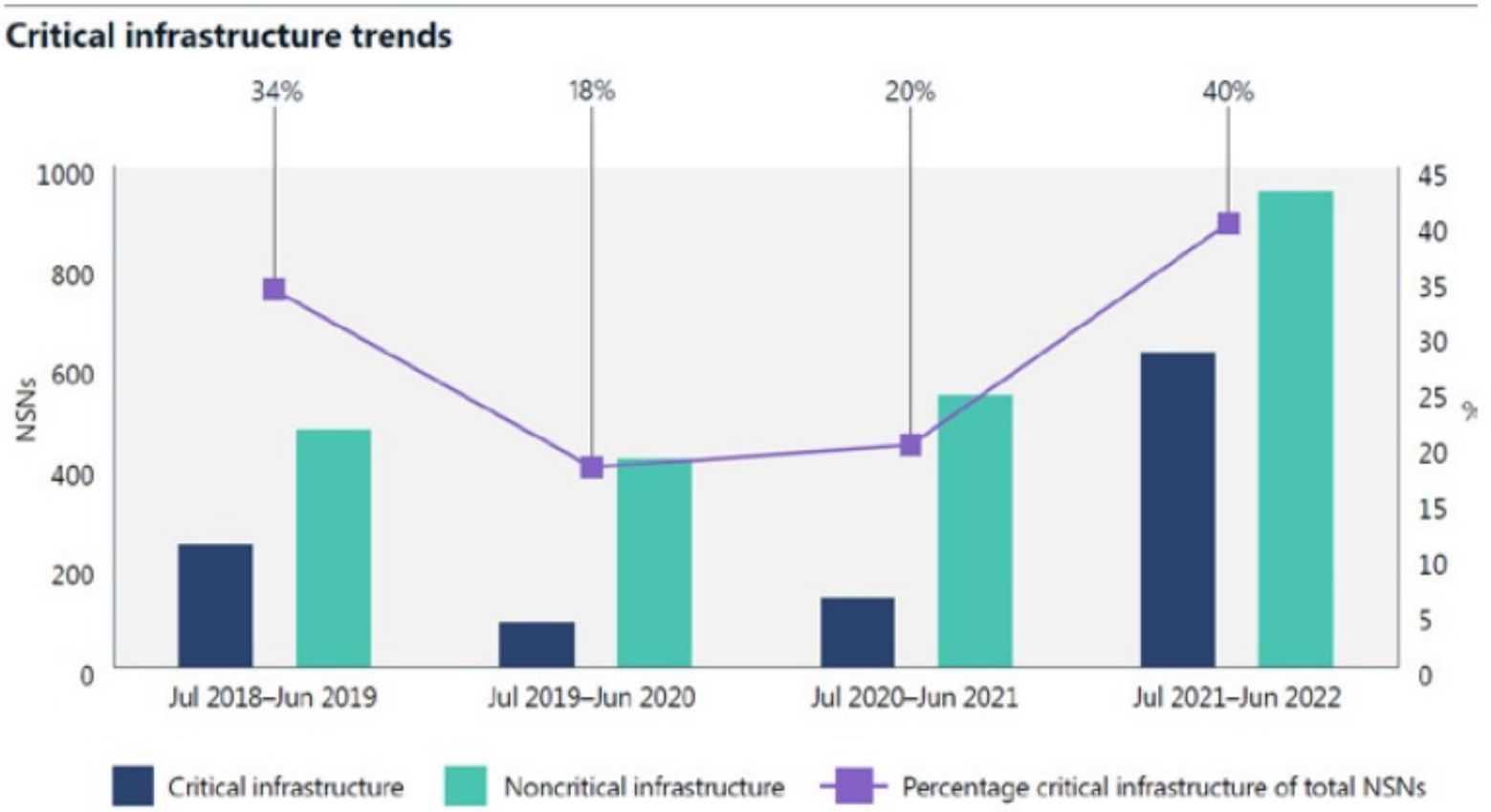
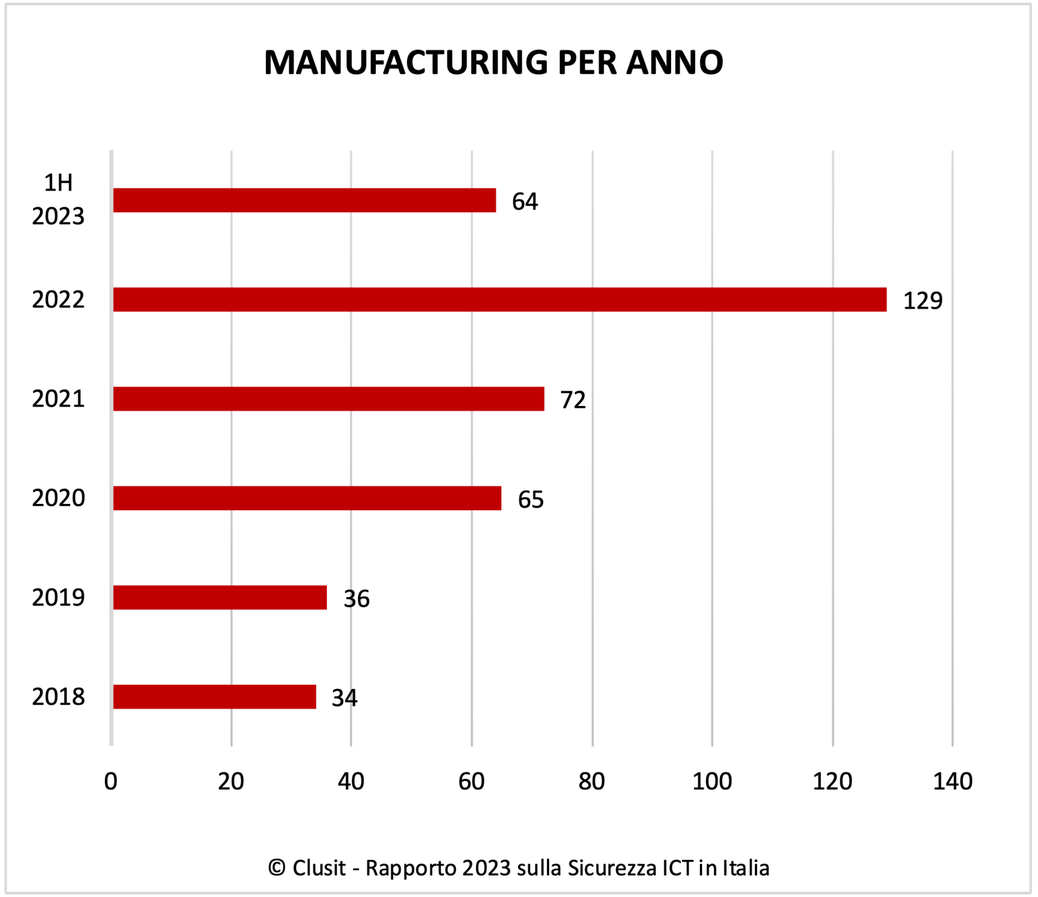
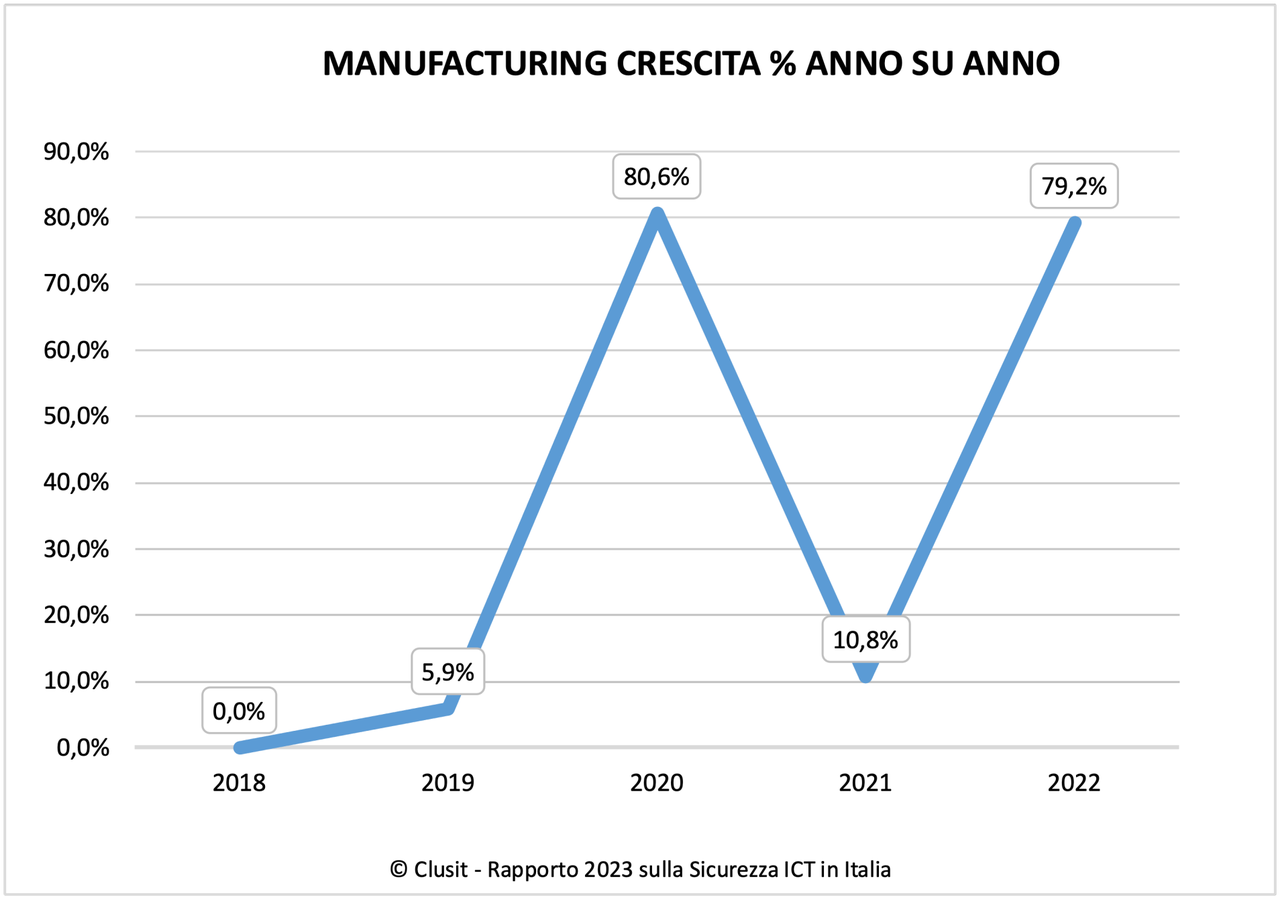


Figura 3 - *Trend degli attacchi alle Infrastrutture Critiche*

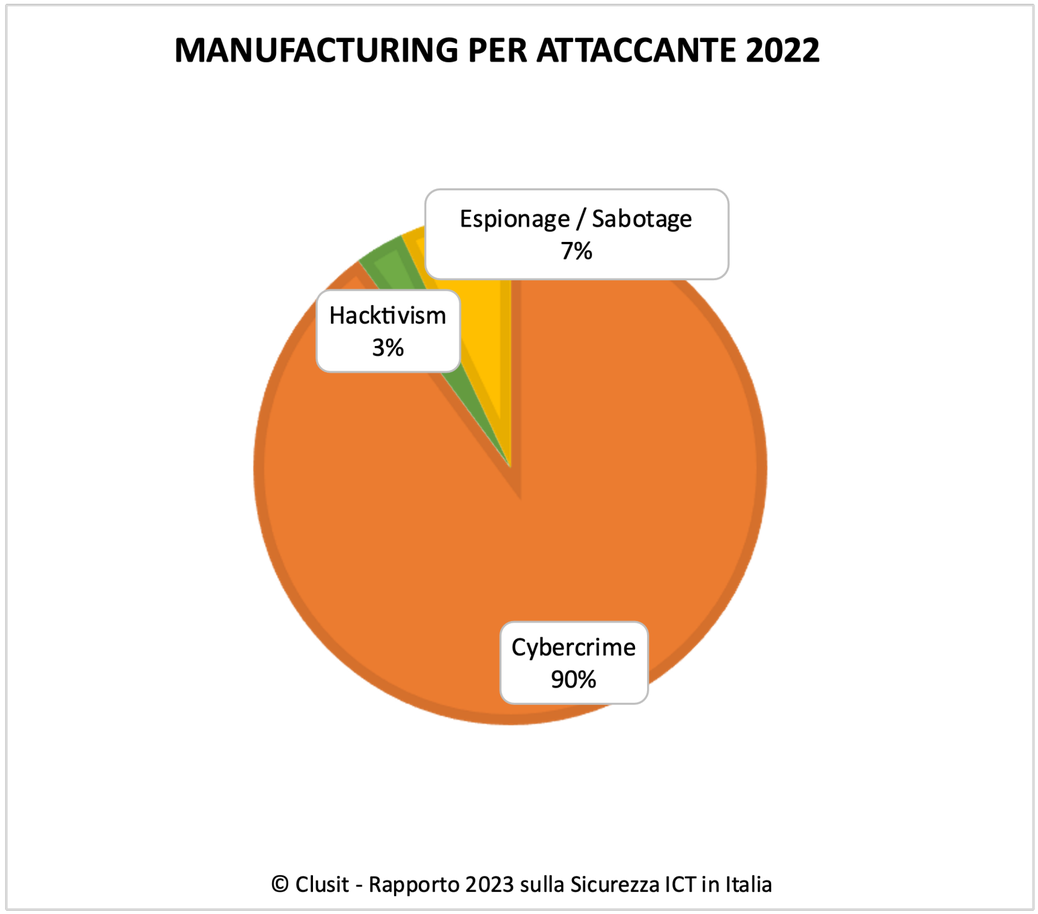
I.C., NIS e NIS2: si allarga il perimetro

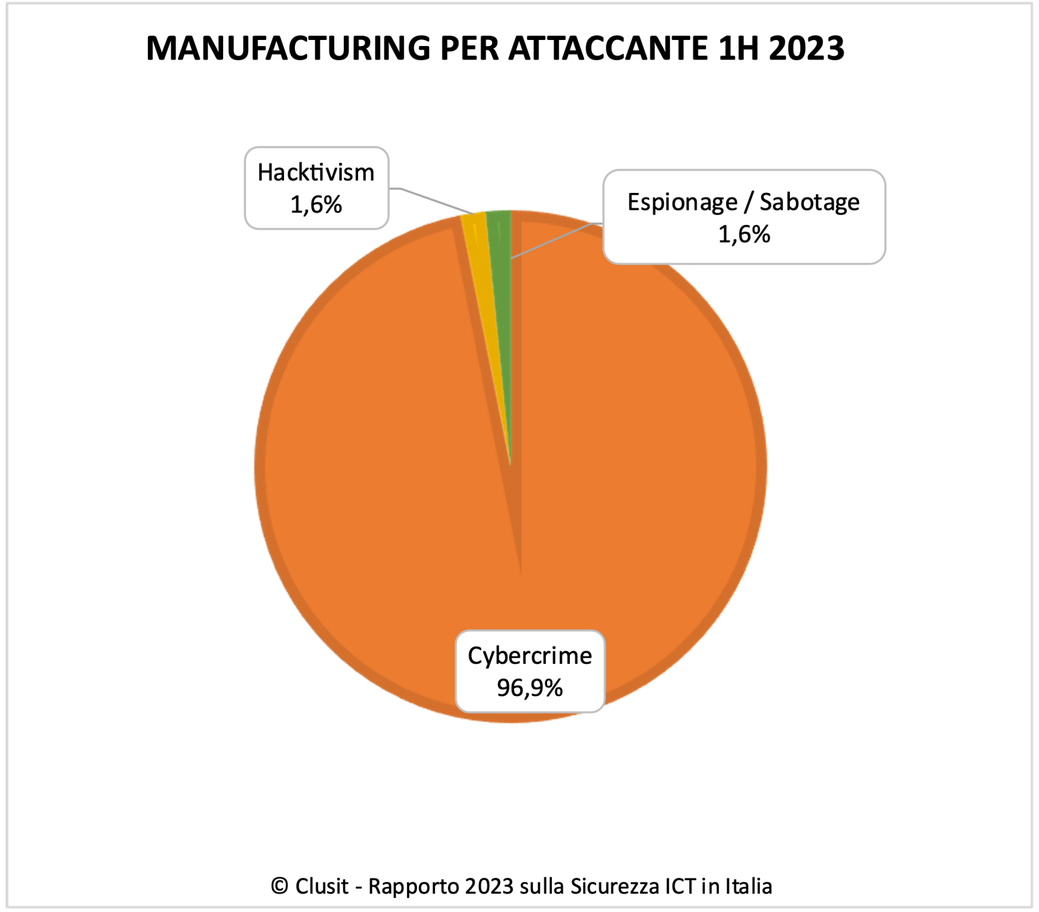
Dati dal Rapporto Clusit sulla sicurezza ICT in Italia
(Ed. ottobre 2023, con i dati da 1.1 al 30.6.2023)





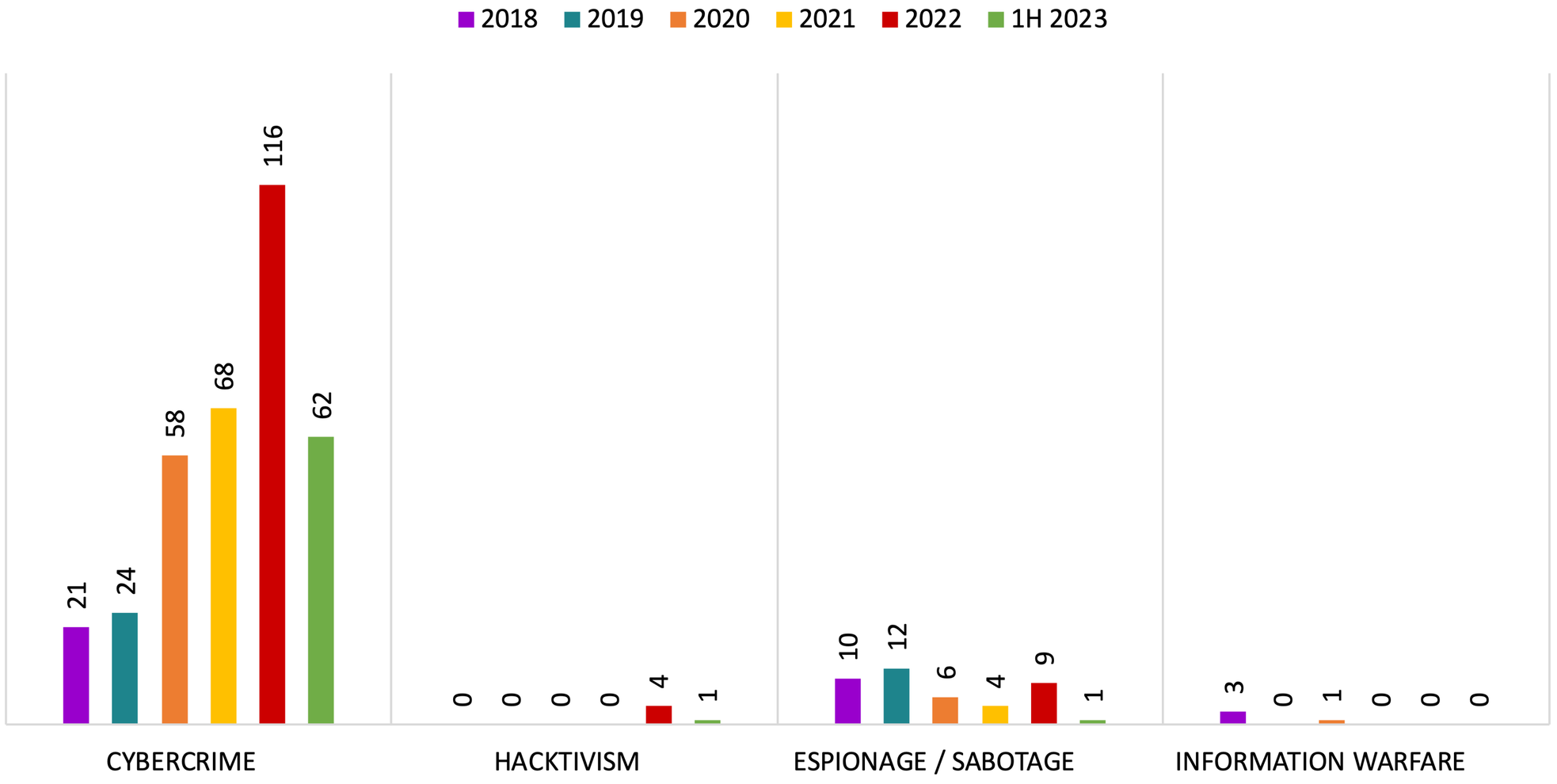
- Crescita costante con picchi nel 2020 (+80%) e 2022 (+79%)
- H1 2023 in linea con 2022, pari a tutto il 2021 e tutto il 2020

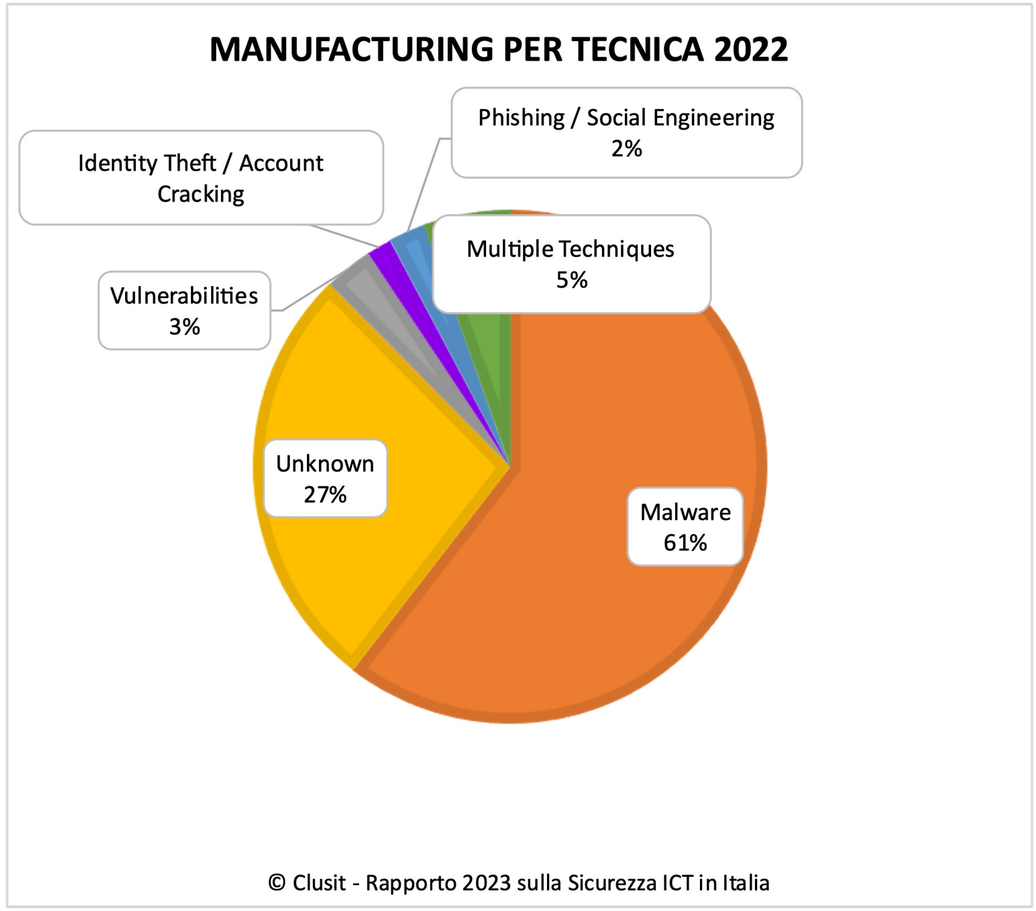


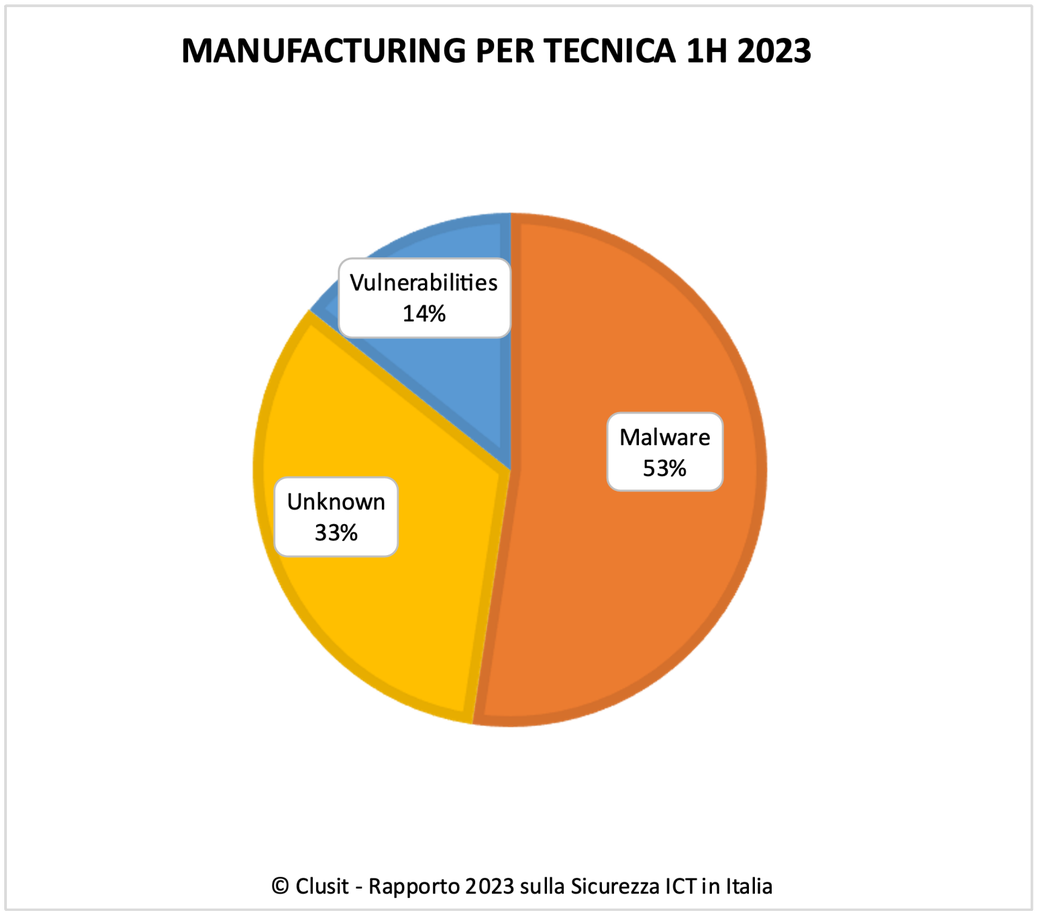


- Minaccia proviene dal Cybercrime quasi totalmente

MANUFACTURING PER ATTACCANTE 2018 - 1H 2023

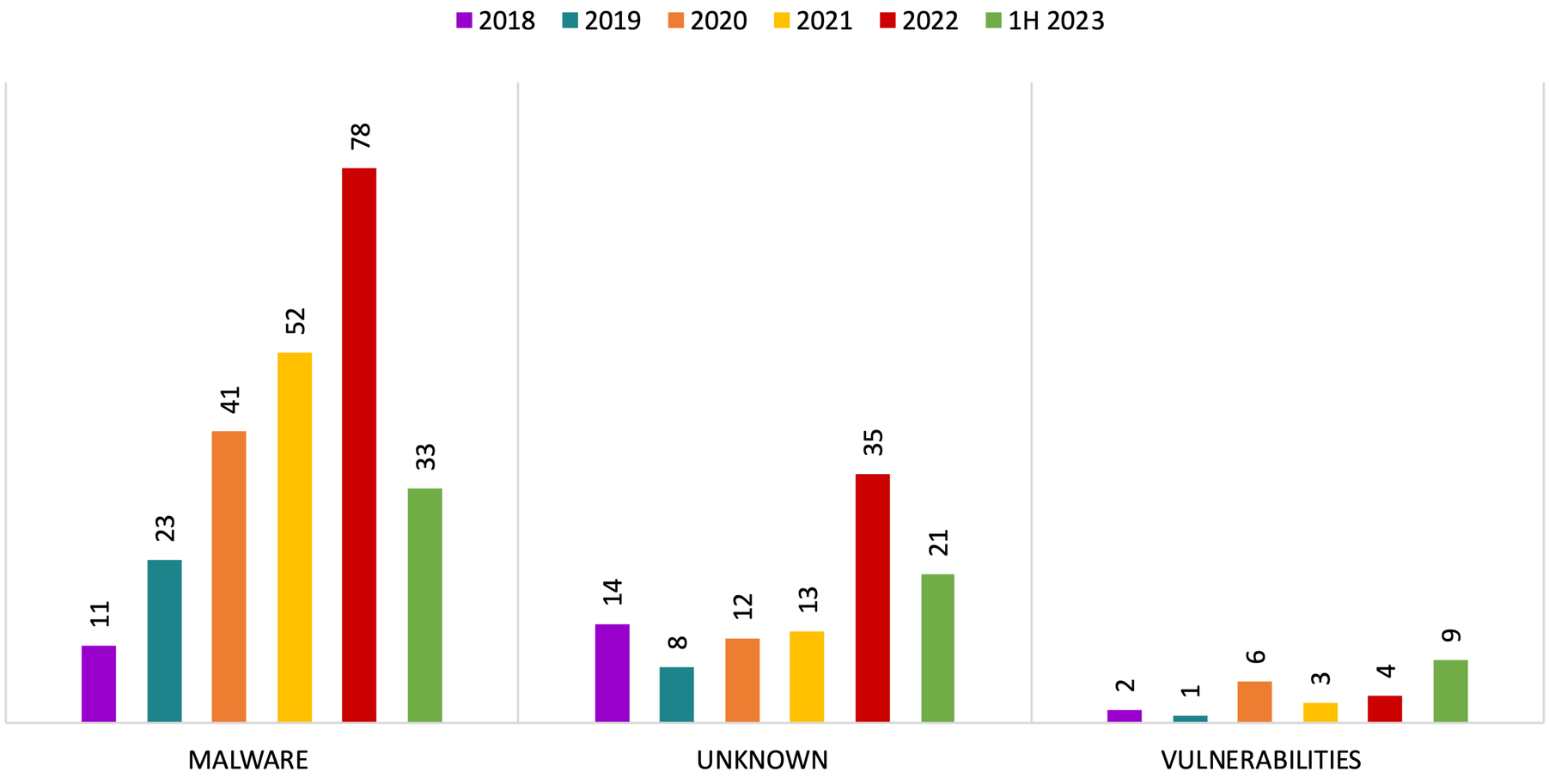




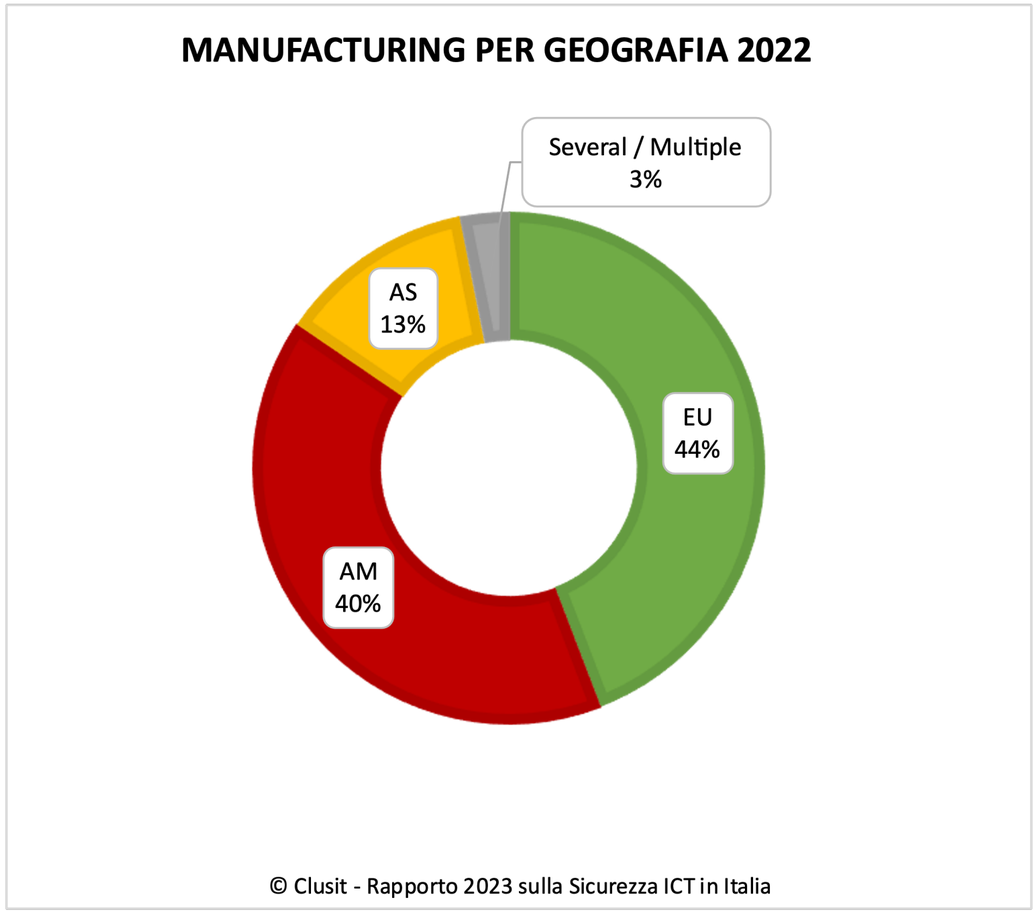


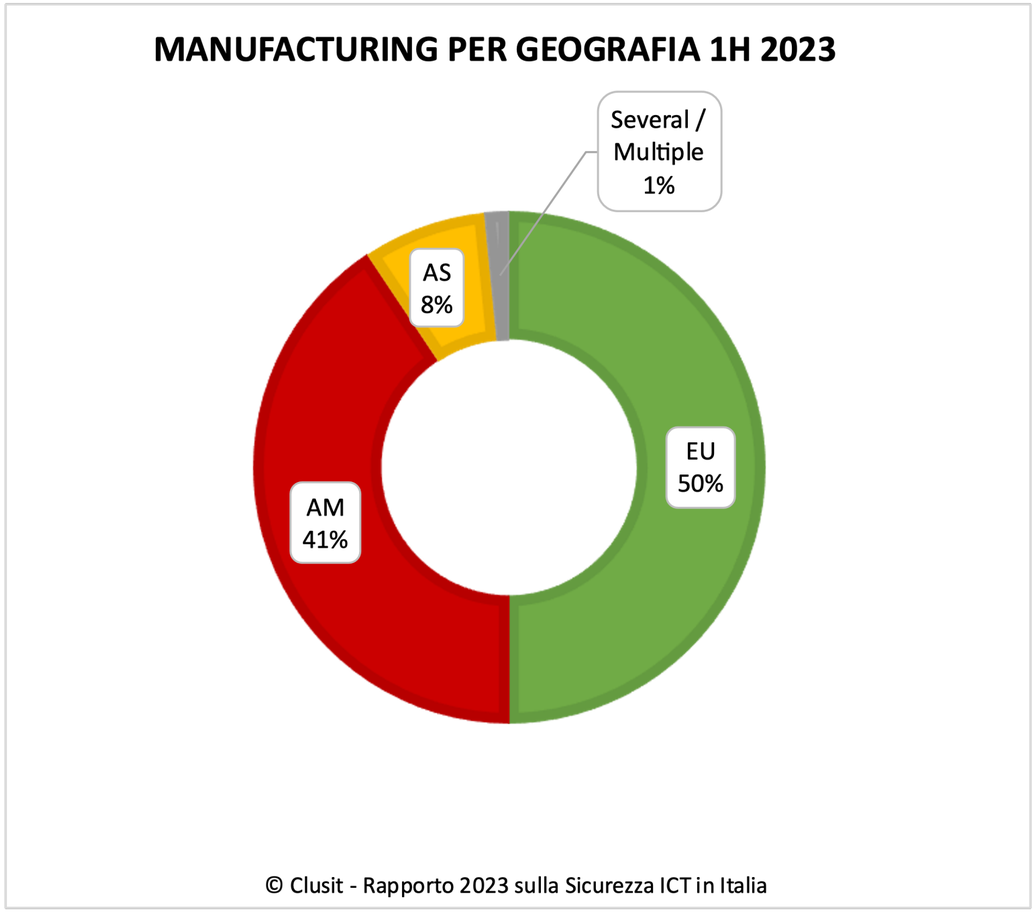
Tecnica principalmente utilizzata è Malware/Ransomware,
poi «Data Breach» (Unknown), a seguire Vulnerabilità (0-Days)

MANUFACTURING PER TECNICA DI ATTACCO 2018 - 1H 2023



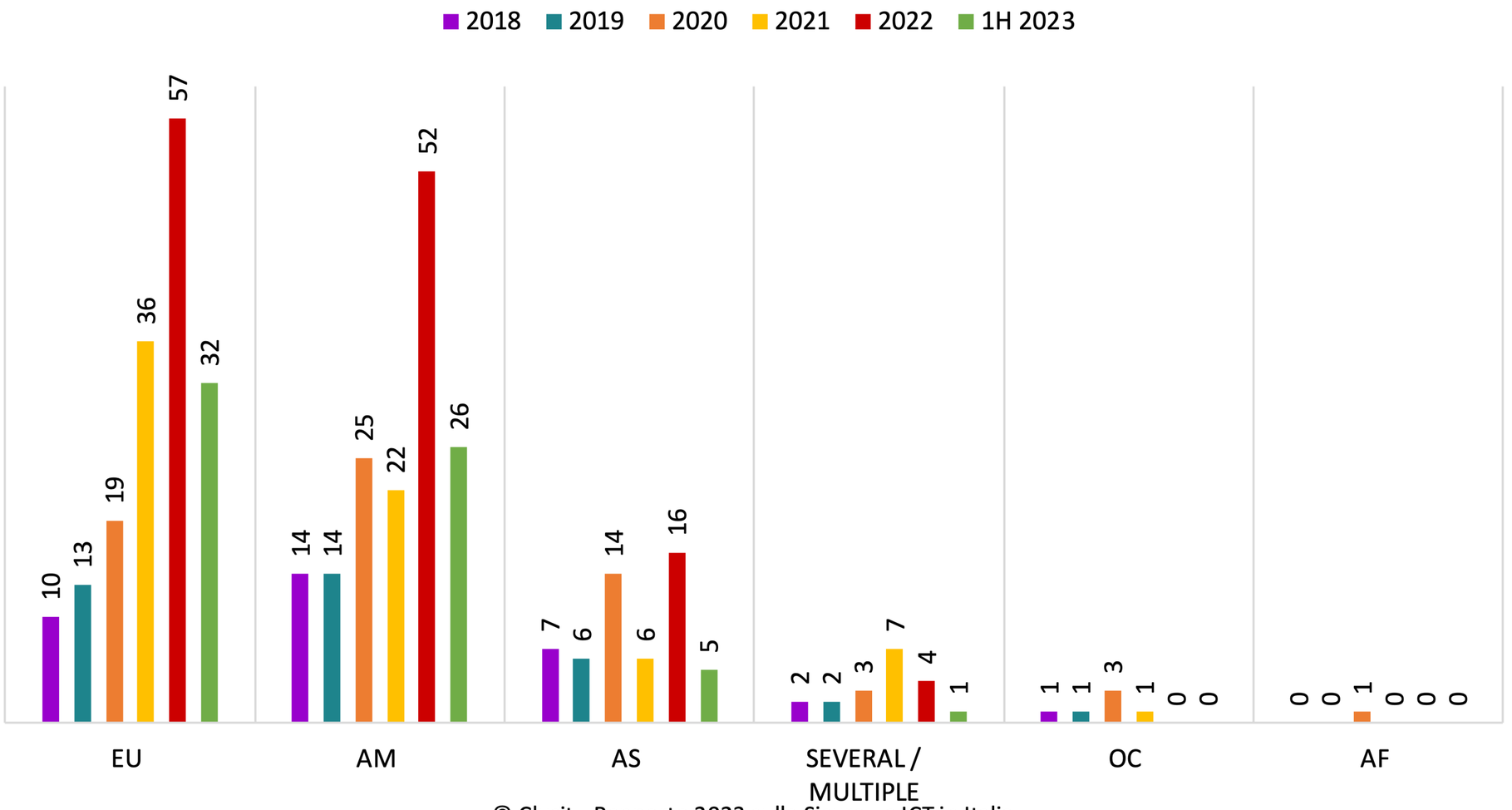
© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia



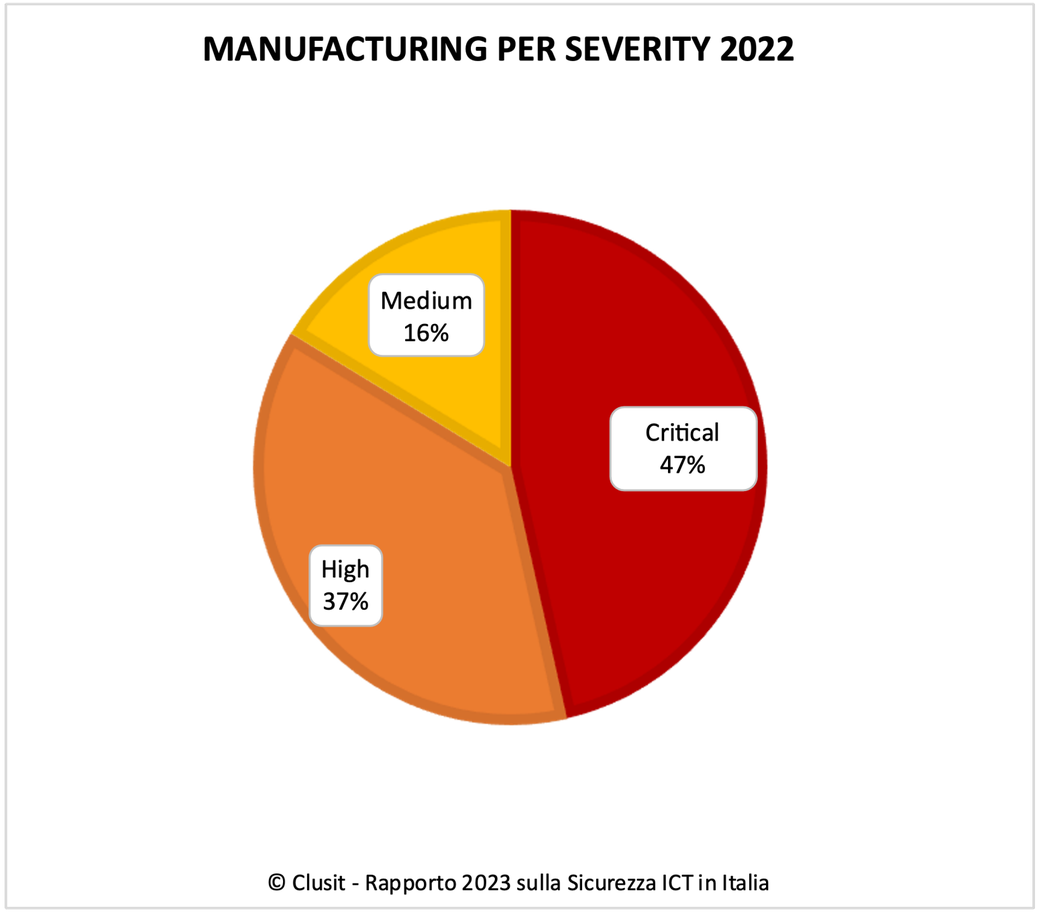


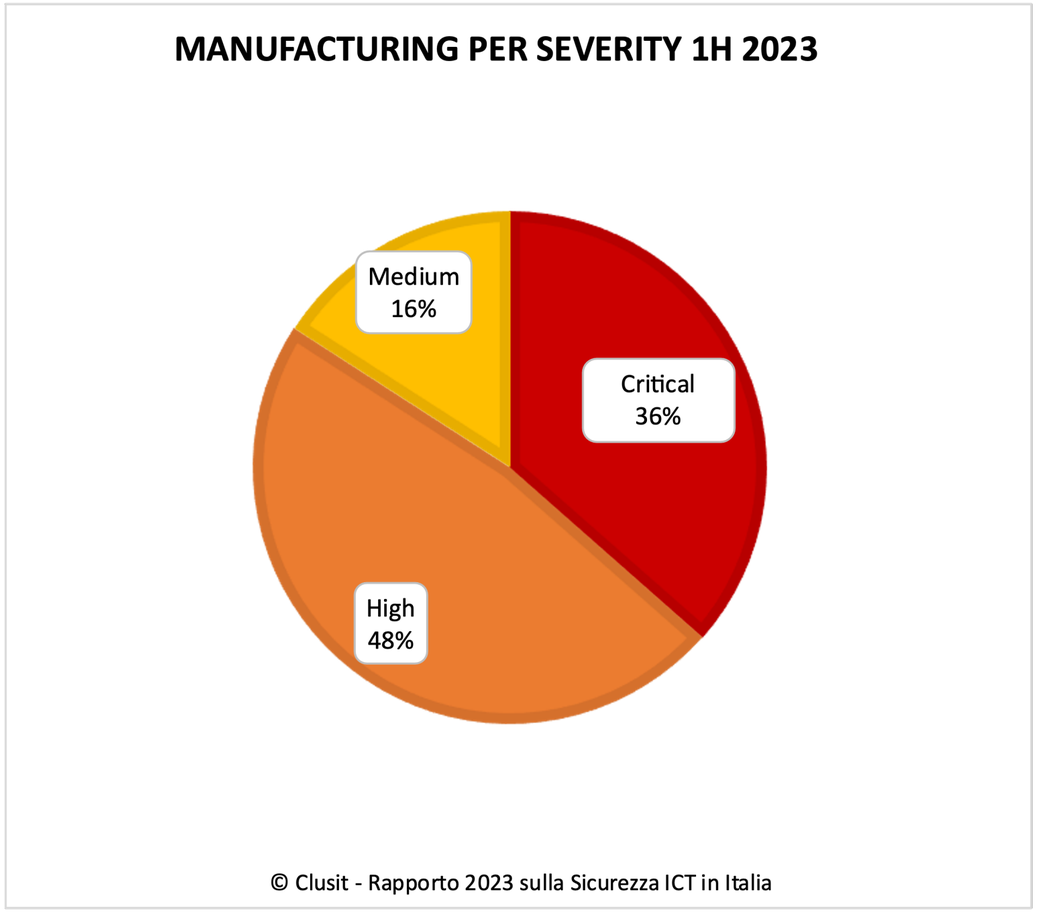
Target Europei i più colpiti (50% H1 2023), poi Americhe 41% resto è ROW (dati veritieri per il ROW?)

MANUFACTURING PER GEOGRAFIA DELLE VITTIME 2018 - 1H 2023

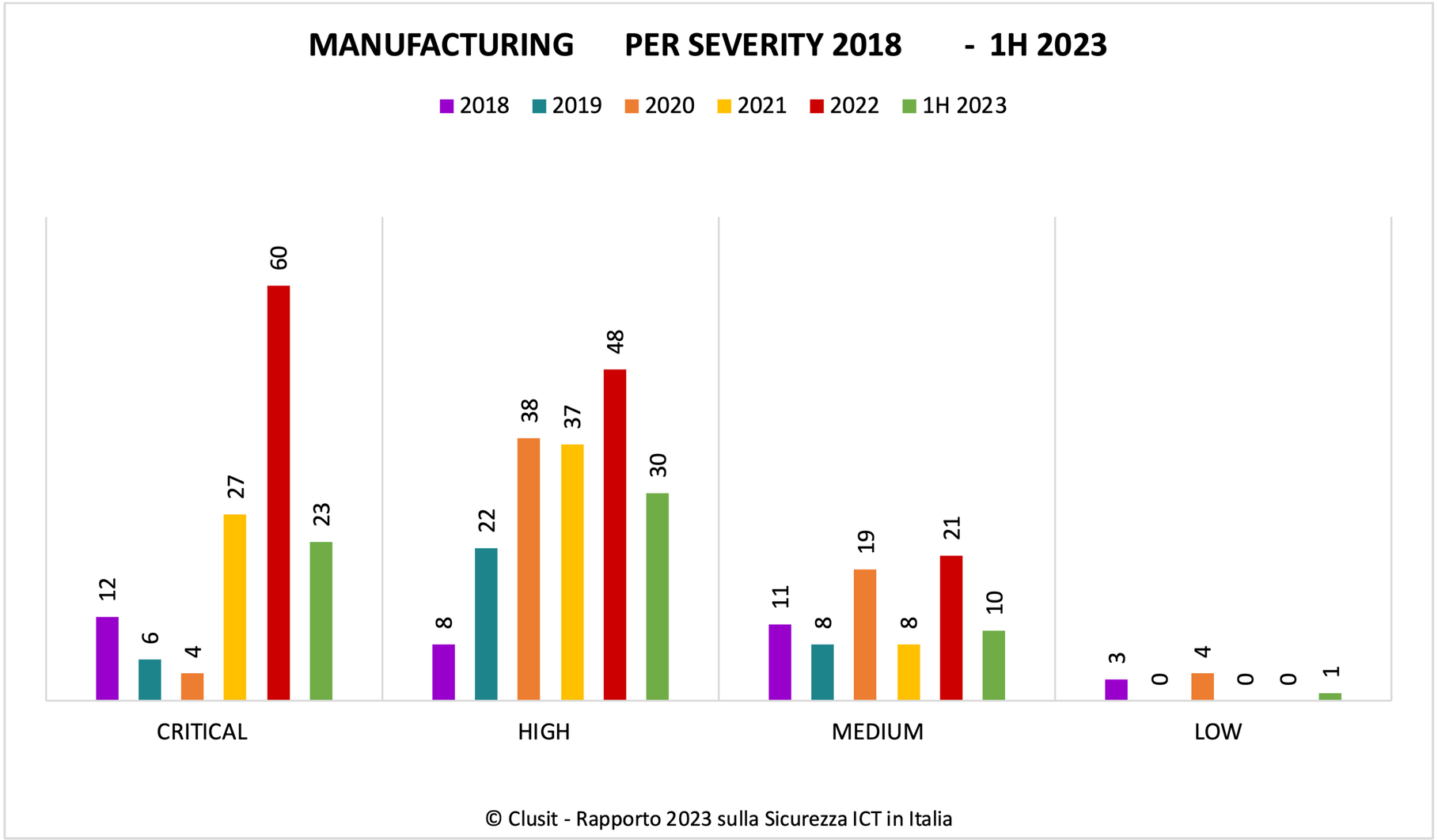


© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

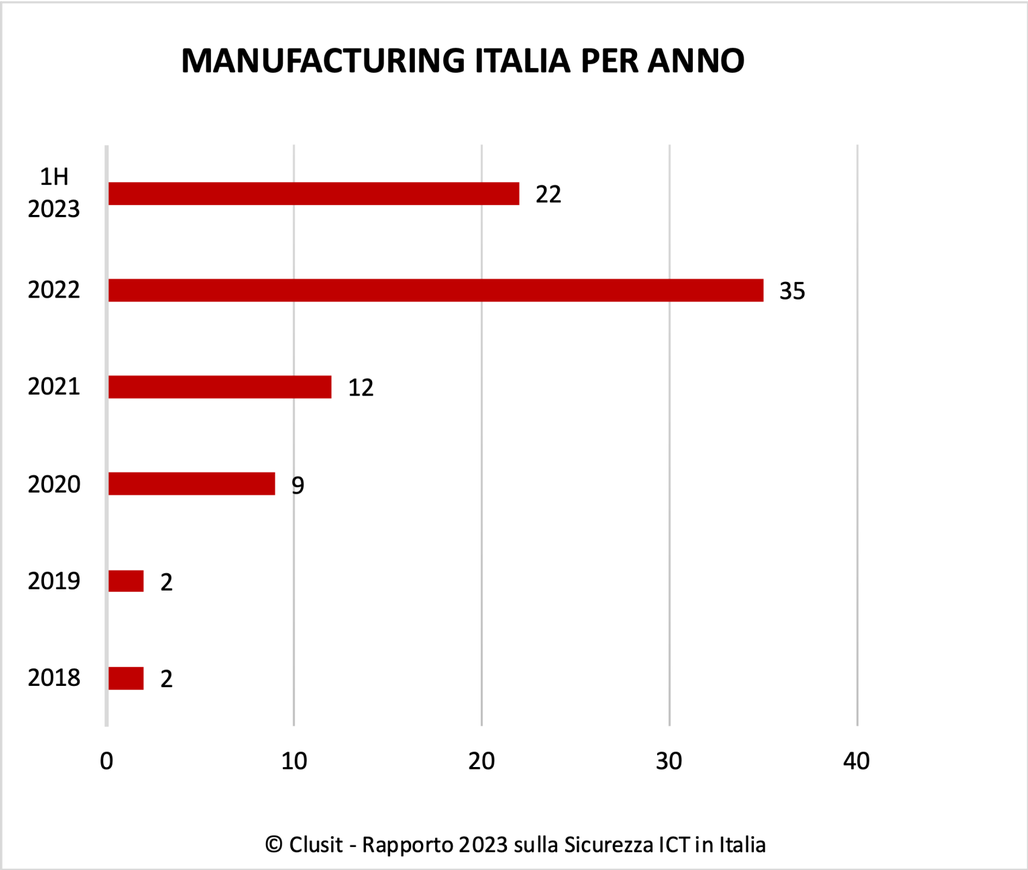


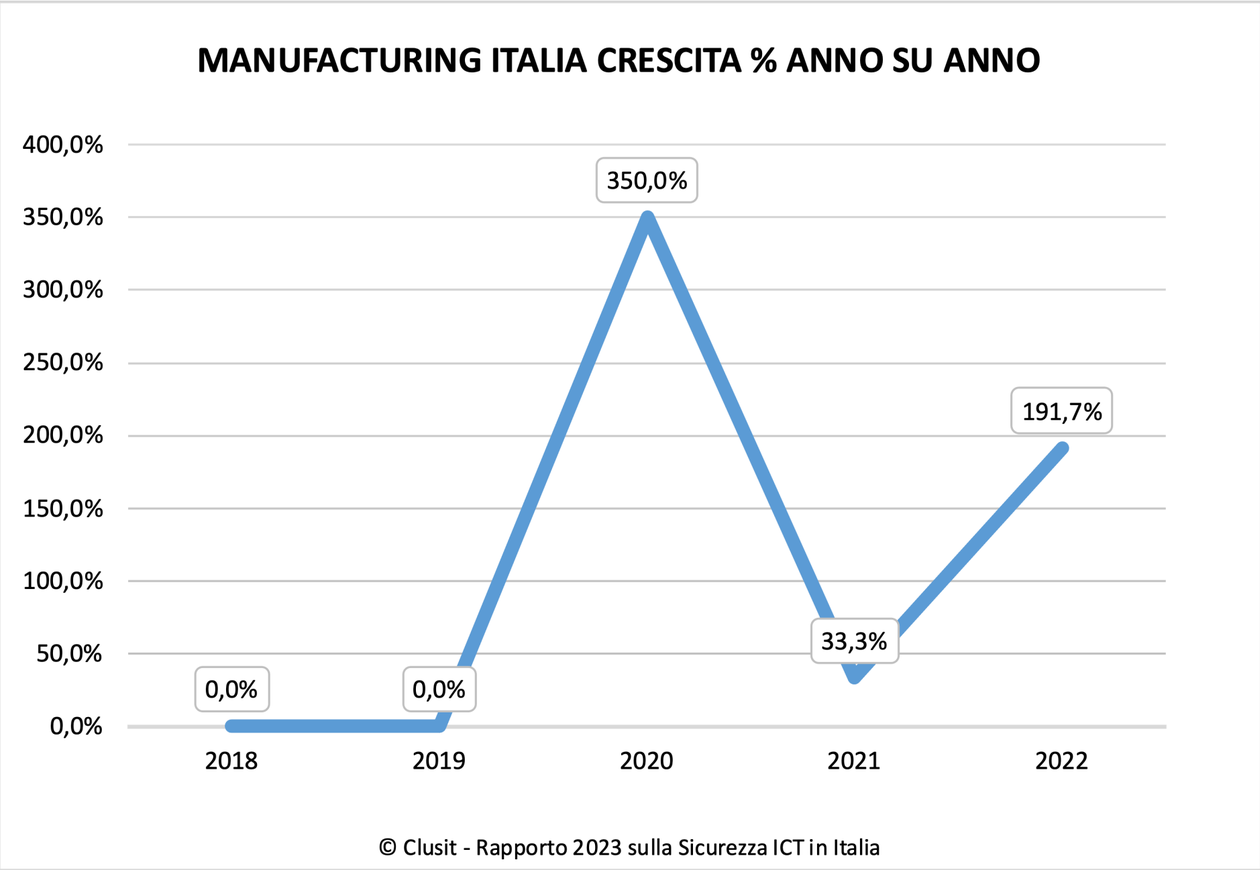


Attacchi con impatti critici vicini al 50% nel 2022, scende a 1/3 nel H1-2023



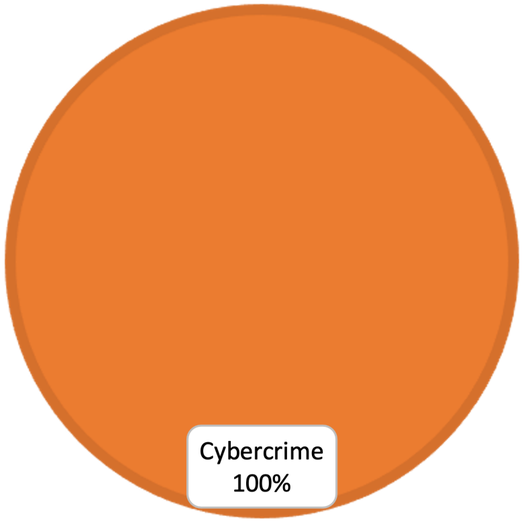
© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia





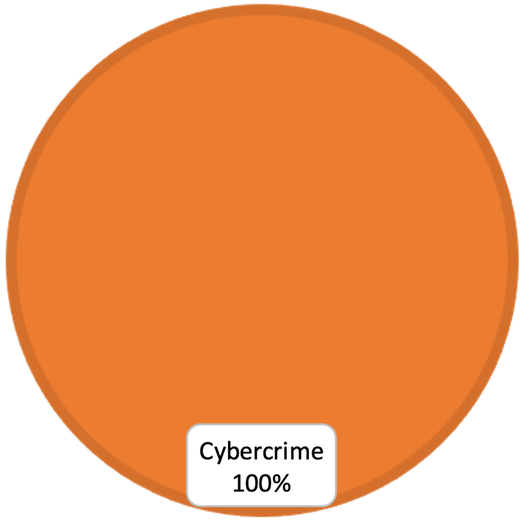
- Irrilevanti in passato, crescita con picchi nel 2020 (+350%) e 2022 (+191%)
- H1 2023 in linea con 2022, pari alla somma del periodo 2018-2021

MANUFACTURING ITALIA PER ATTACCANTE
2022



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

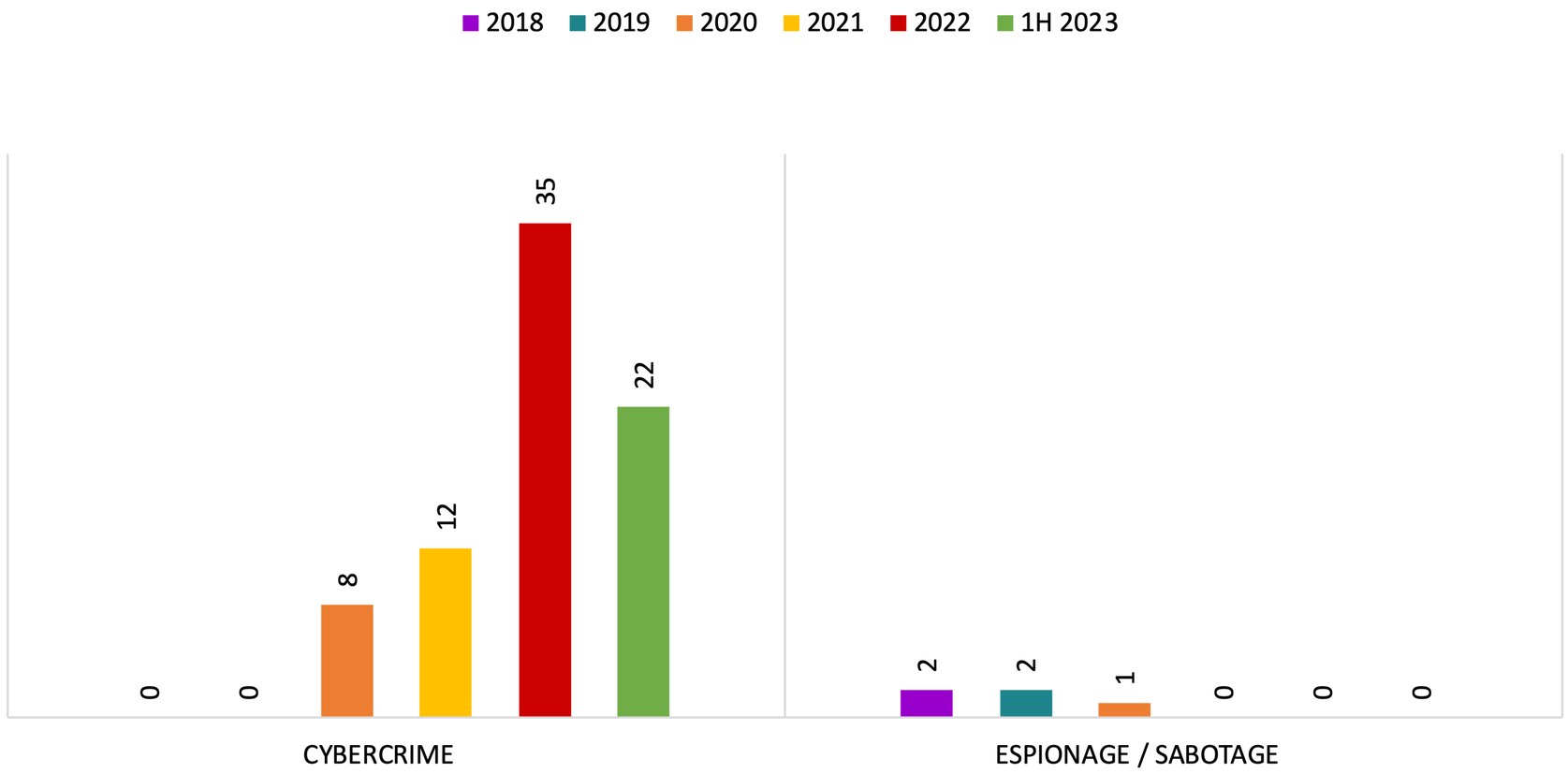
MANUFACTURING ITALIA PER ATTACCANTE 1H
23



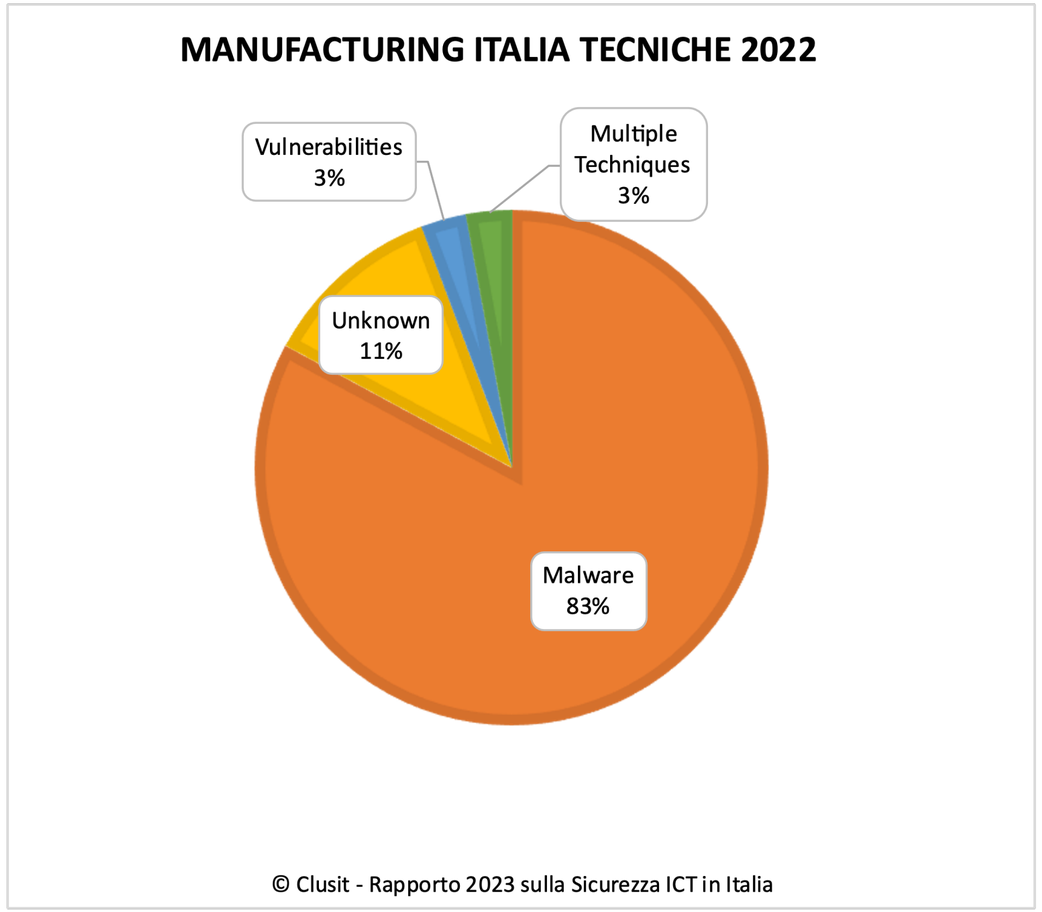
© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

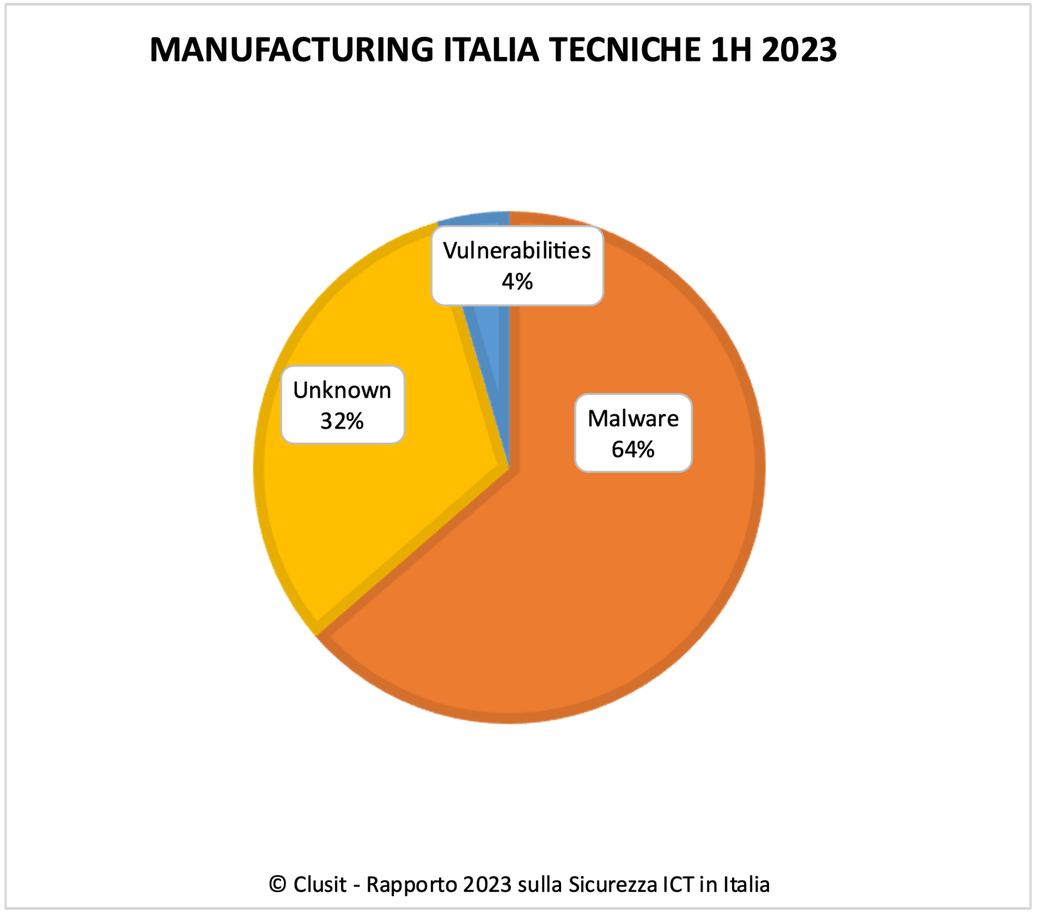
Senza commenti: 100% causato dal Cybercrime sia nel 2022 che H1-2023 !

MANUFACTURING ITALIA PER ATTACCANTE 2018 -1H 23

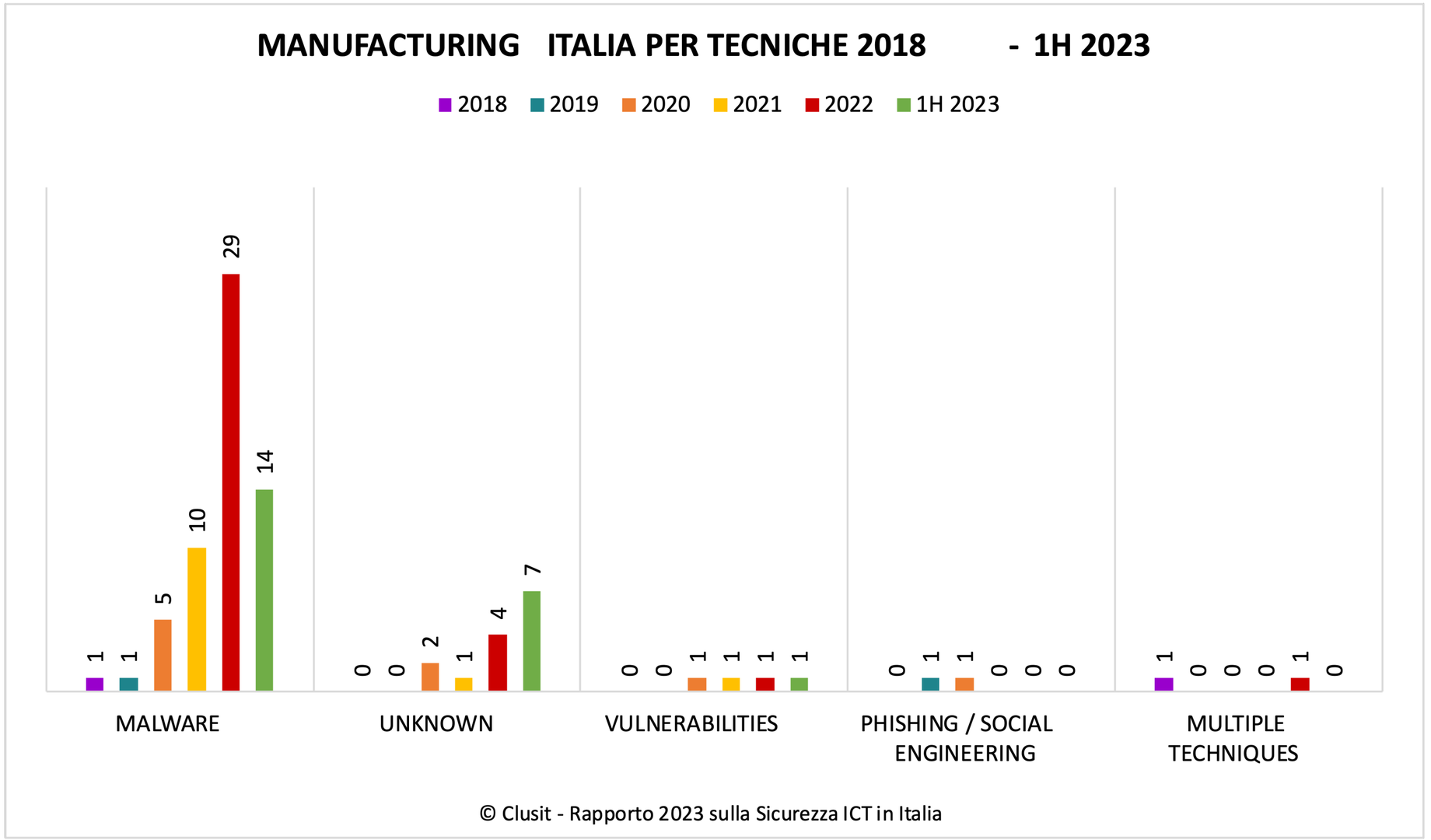


© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

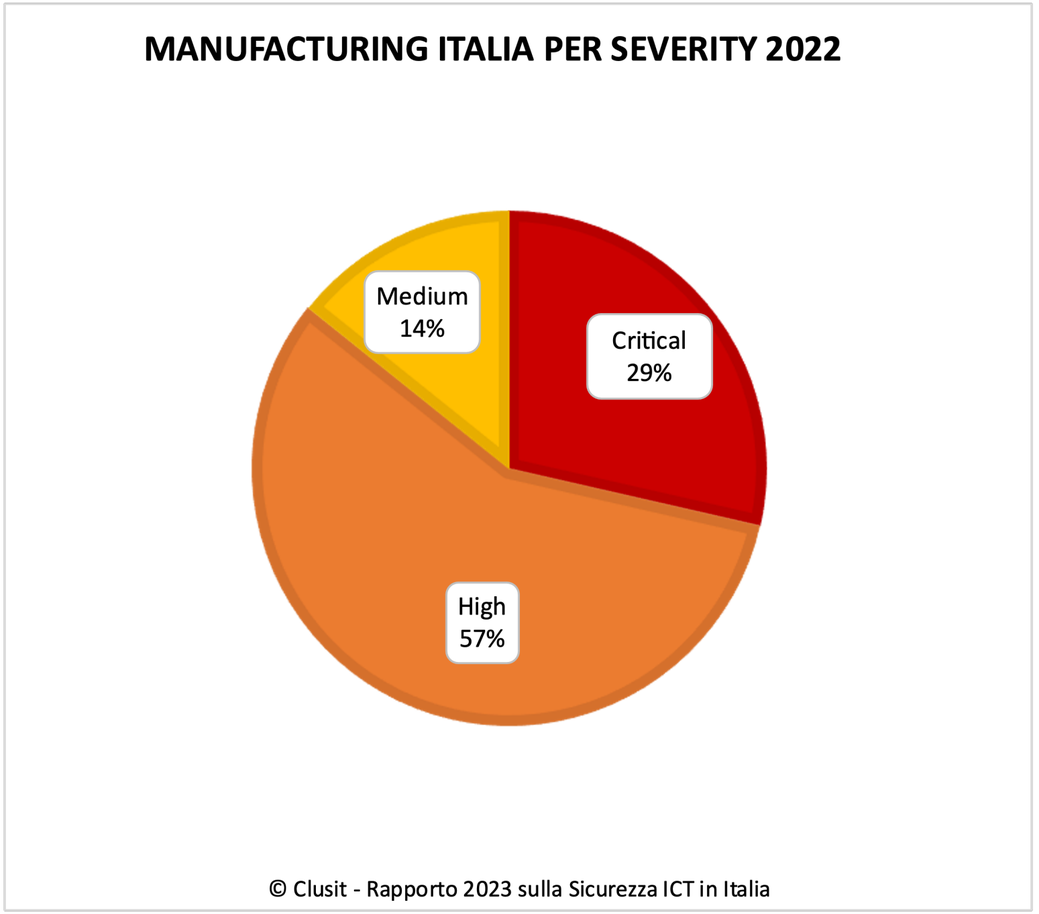


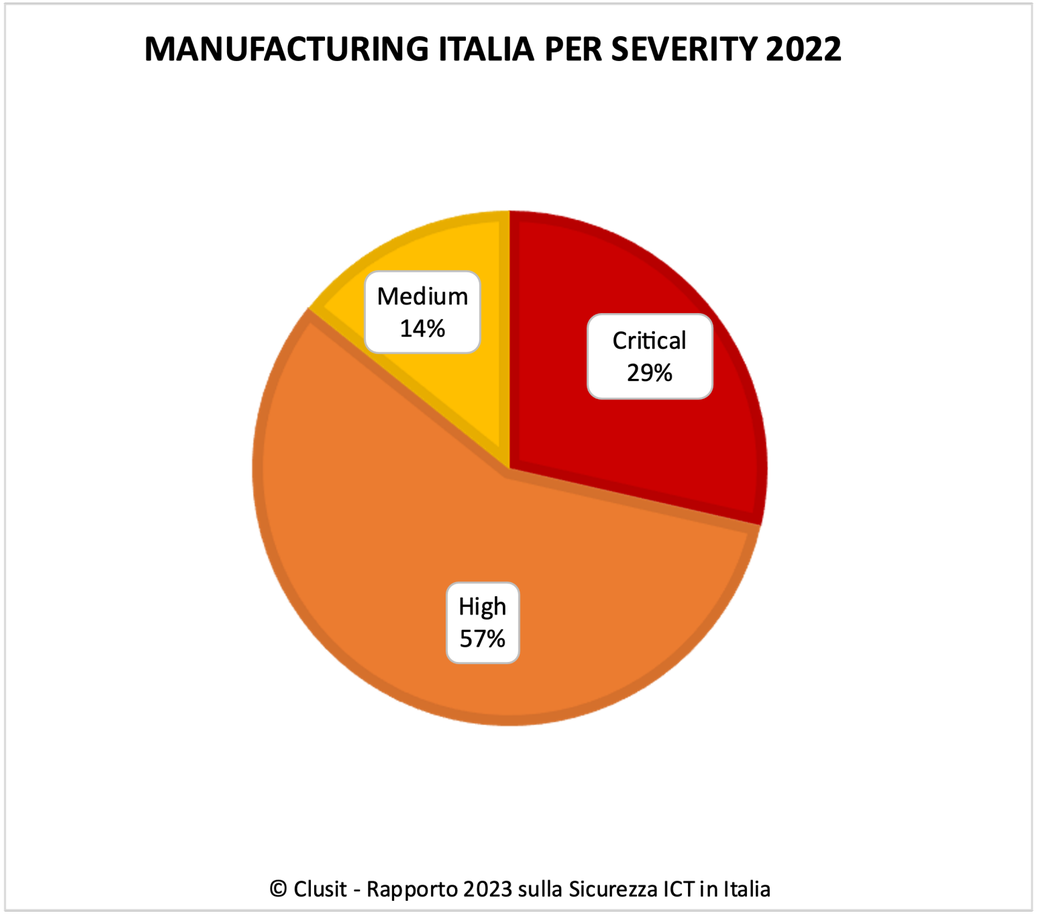


Come già visto a livello globale, Tecnica principalmente utilizzata (83%) è Malware/Ransomware, poi «Data Breach» (Unknown), a seguire poche Vulnerabilità (0-Days) sfruttate

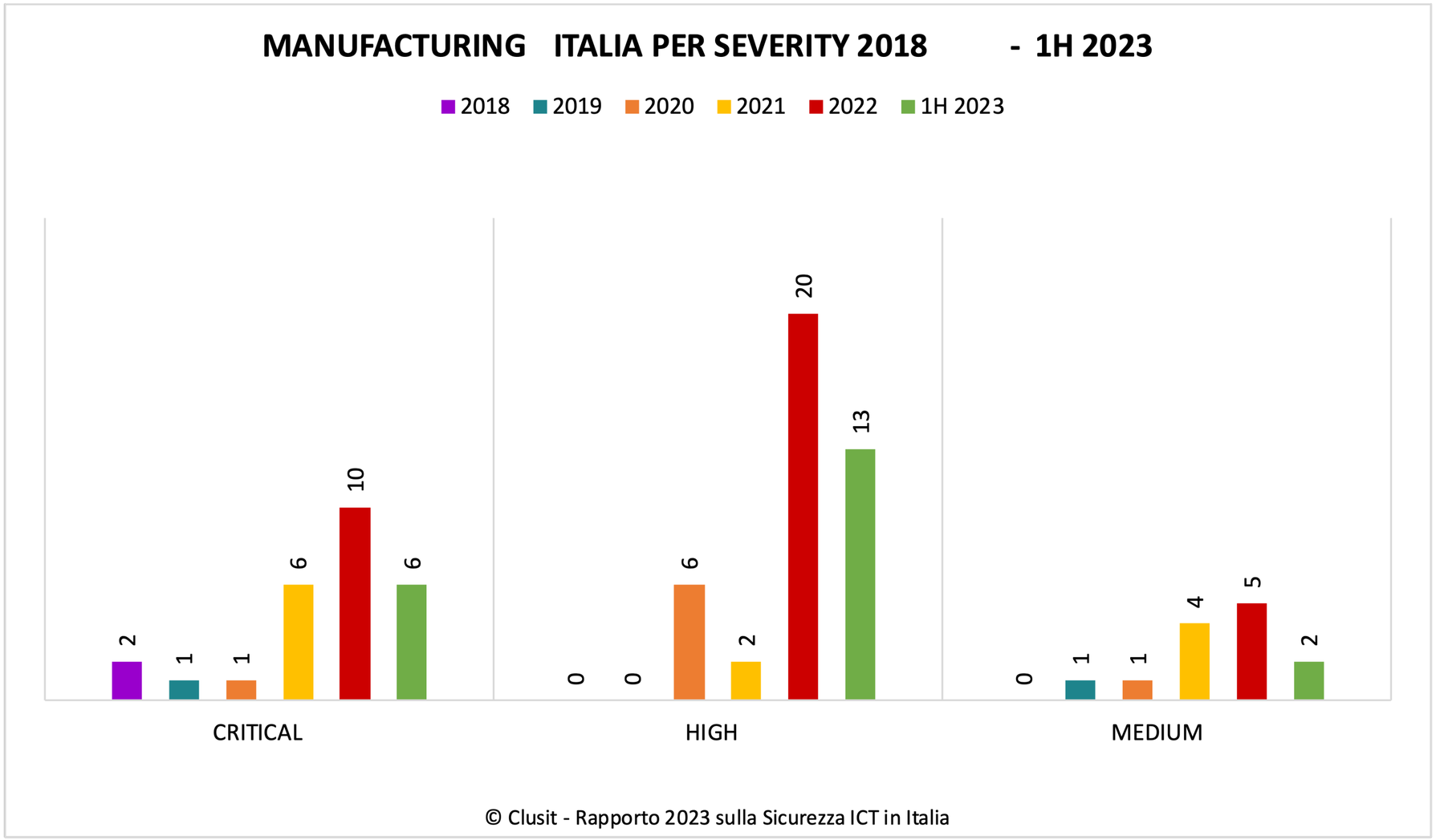


© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia





Anche da noi, attacchi con impatti critici vicini 1/3 sia nel 2022 e H1-2023



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

Ed alcuni dati dal Report
Dragos ICS/OT CyberSecurity
Year in Review 2022

(approfondimento Ransomware)

ICS/OT CYBERSECURITY
YEAR IN REVIEW 2022

A proposito di Ransomware con impatto ICS/OT

Key Ransomware Findings

↑ **87%**

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

+35%

Dragos tracked **35% more ransomware groups** impacting ICS/OT in 2022.

72%

of all ransomware attacks targeted **437 manufacturing entities** in **104 unique manufacturing subsectors**.

DRAGOS
SAFEGUARDING CIVILIZATION

Ransomware con impatto ICS/OT per settore

FIGURE 4: RANSOMWARE INCIDENTS BY SECTOR • 2022

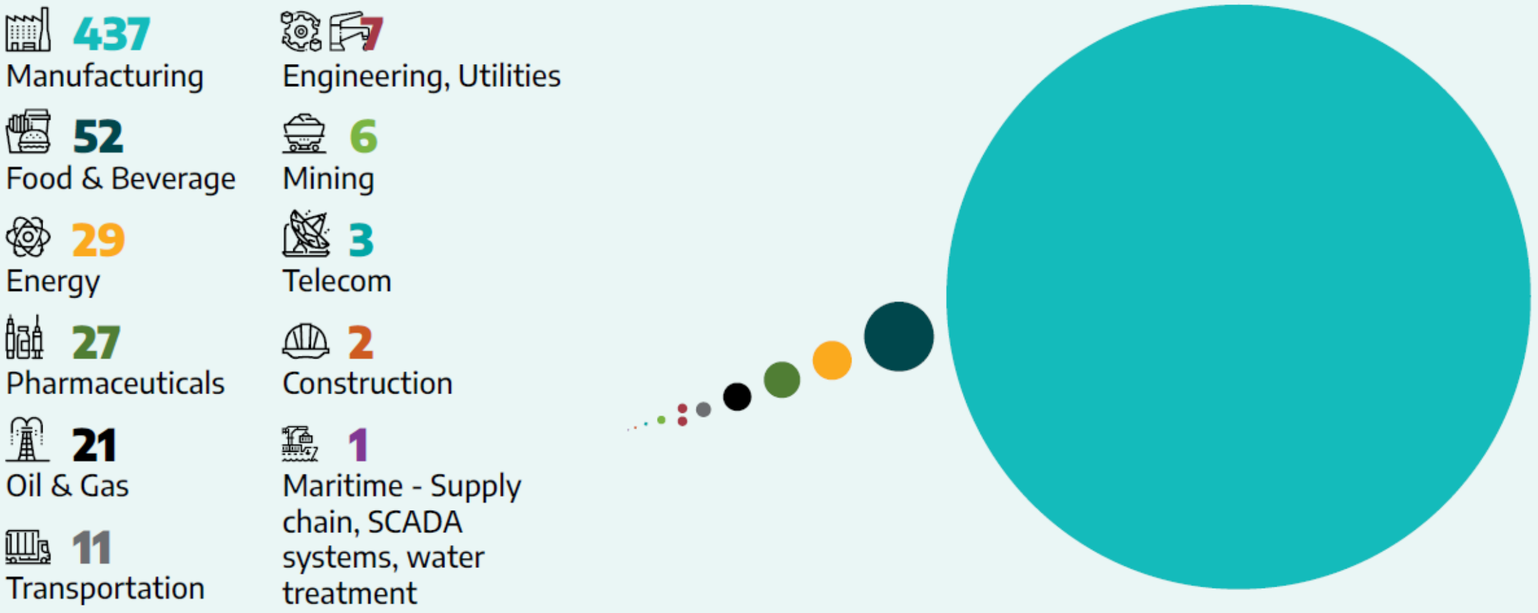


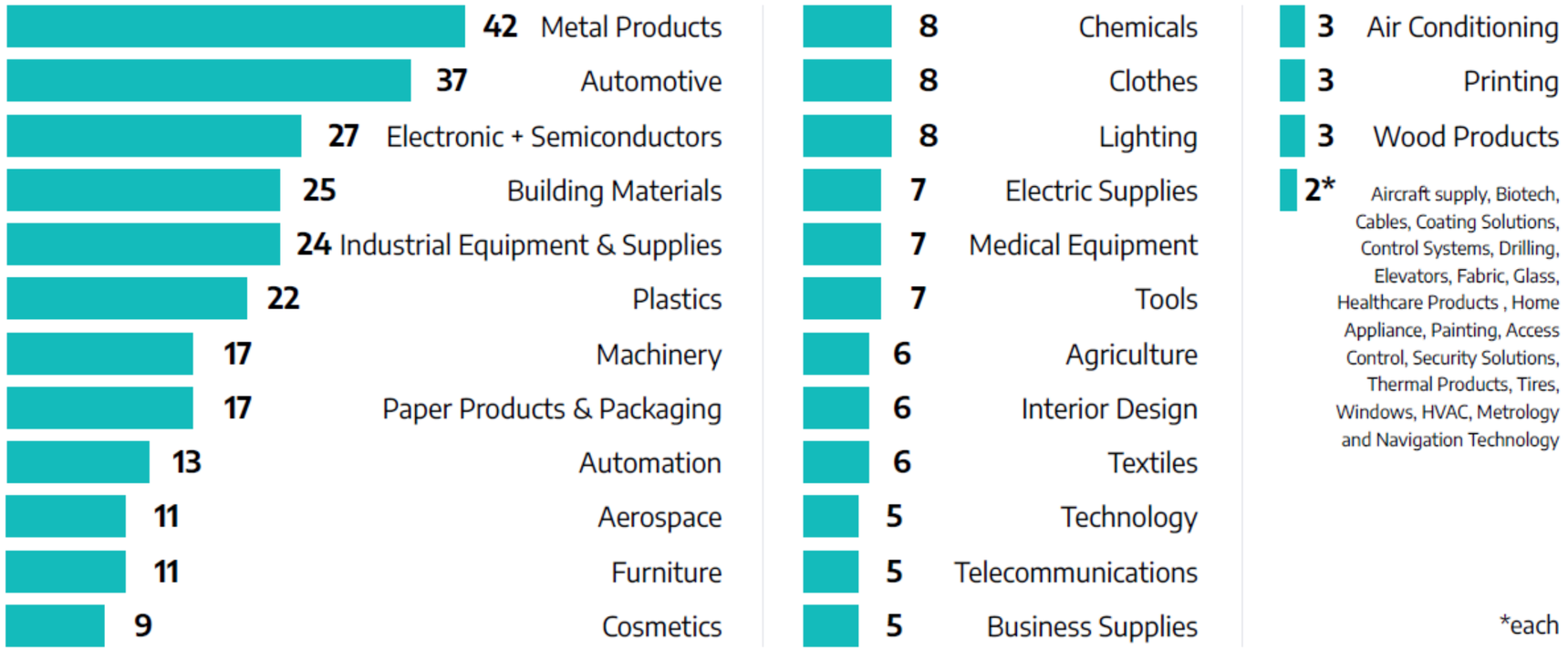
Figure 4 shows that 72 percent of all 2022 ransomware attacks Dragos tracked targeted 437 manufacturing entities in 104 unique manufacturing subsectors. Figure 4 also shows that nine percent of attacks targeted food and beverage; five percent targeted the energy sector; four percent targeted the pharmaceuticals; three percent targeted the oil and natural gas sector. Ten percent of victims were in metal products manufacturing, nine percent were in automotive, six percent were in electronic and semiconductor, 5.7 percent were in building materials, 5.5 percent were in industrial equipment and supplies manufacturing, and 5 percent were in plastics. See Figure 5.

72% attacchi con impatto MFG in 104 Settori industriali dei quali:

- 9% Alimentari
- 4% Farmaceutici
- 3% Oil & Gas
- 10% Metalli
- 9% Automotive
- 6% Elettronica e Semicond.
- 5% matriali edilizia
- 5% costruttori macchine
- 5% plastica

Ransomware con impatto ICS/OT per sotto-settore

FIGURE 5: RANSOMWARE BY MANUFACTURING SUBSECTOR



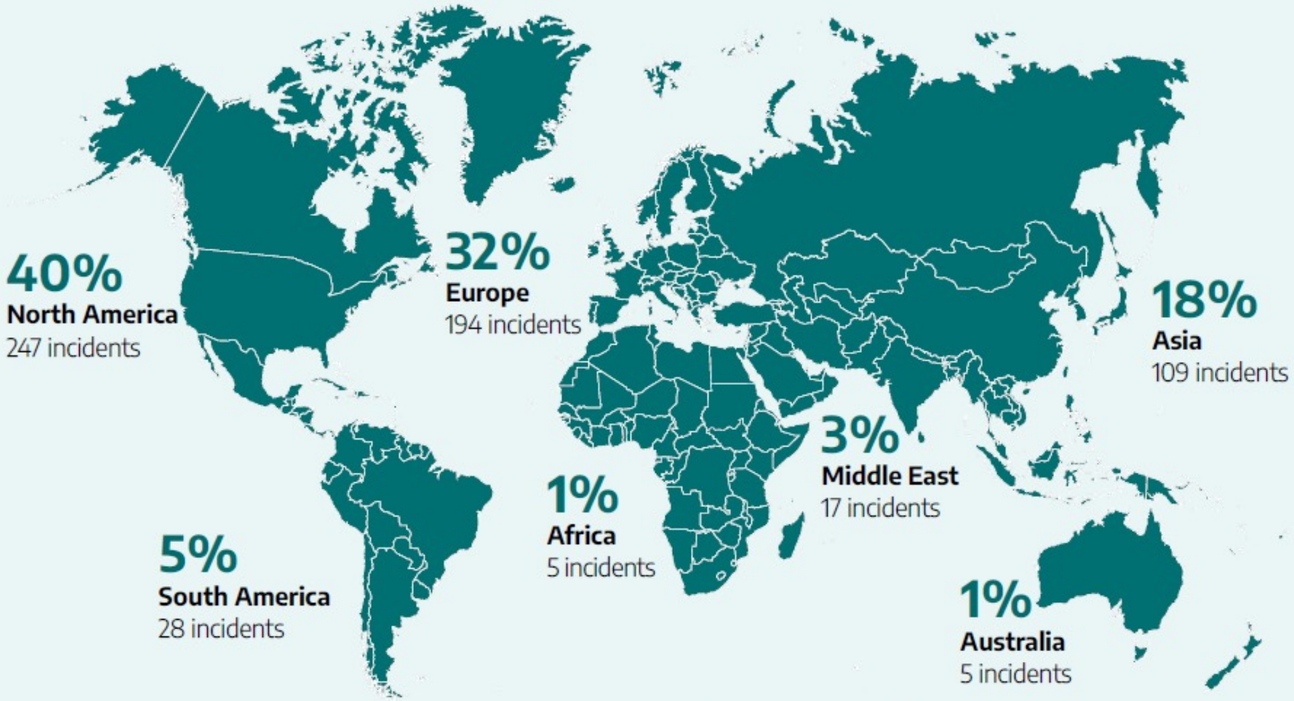
72% attacchi con impatto MFG in
104 Settori industriali dei quali:

- 10% Metalli
- 9% Automotive
- 9% Alimentari
- 6% Elettronica e Semicond.
- 5% materiali edilizia
- 5% costruttori macchine
- 5% plastica
- 4% Farmaceutici
- 3% Oil & Gas

DRAGOS
SAFEGUARDING CIVILIZATION

Ransomware con impatto ICS/OT per area geografica

FIGURE 3: RANSOMWARE INCIDENTS BY CONTINENT • 2022

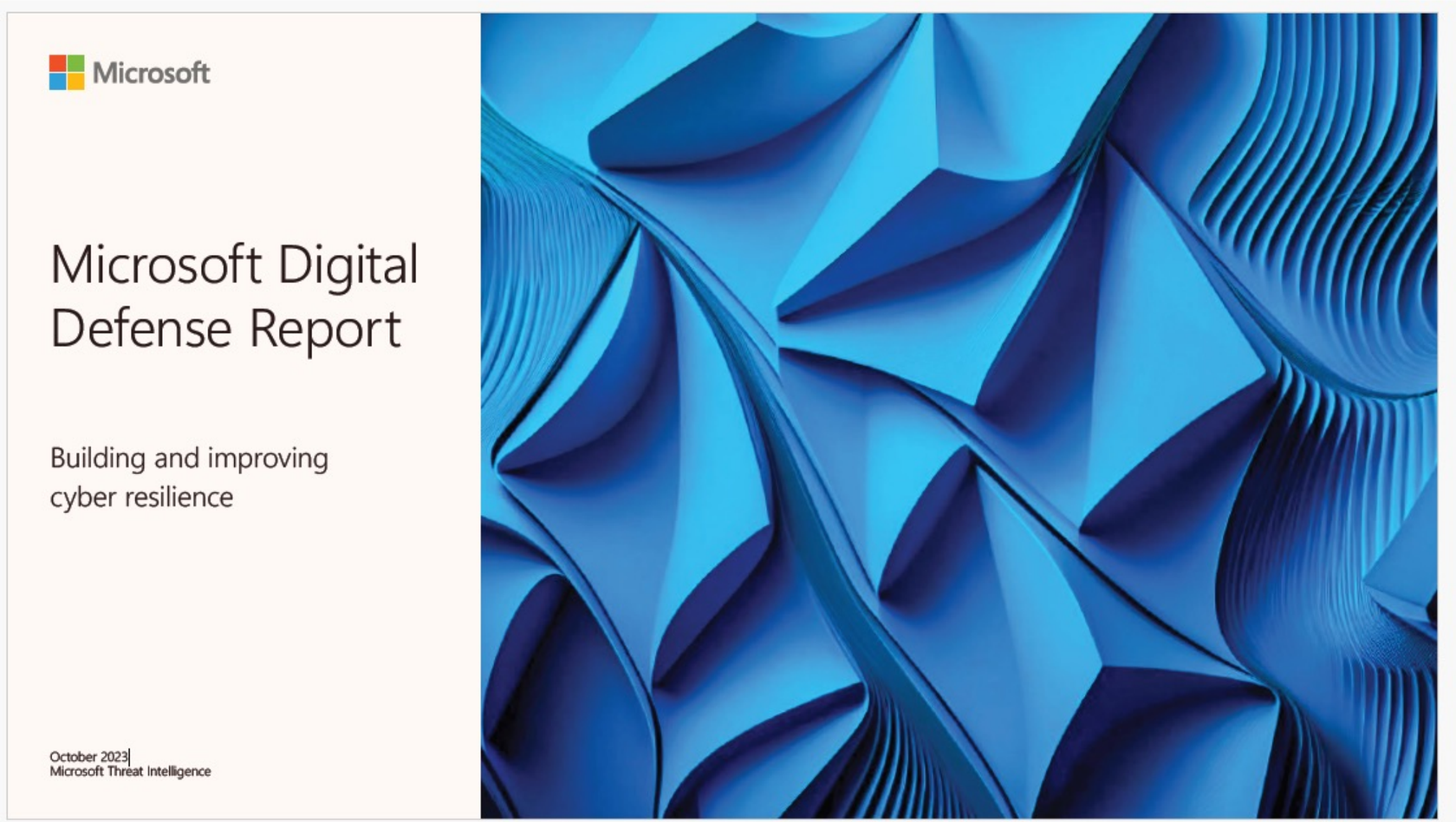


Globally, 40 percent of the ransomware attacks targeted industrial organizations and infrastructures in North America, for a total of 247 incidents; Europe is second with 32 percent or 194 incidents; Asia with 18 percent or 109 incidents; South America with 5 percent; the Middle East with 3 percent; Australia and Africa each had 1 percent. North America remains one of the most highly targeted regions by ransomware.

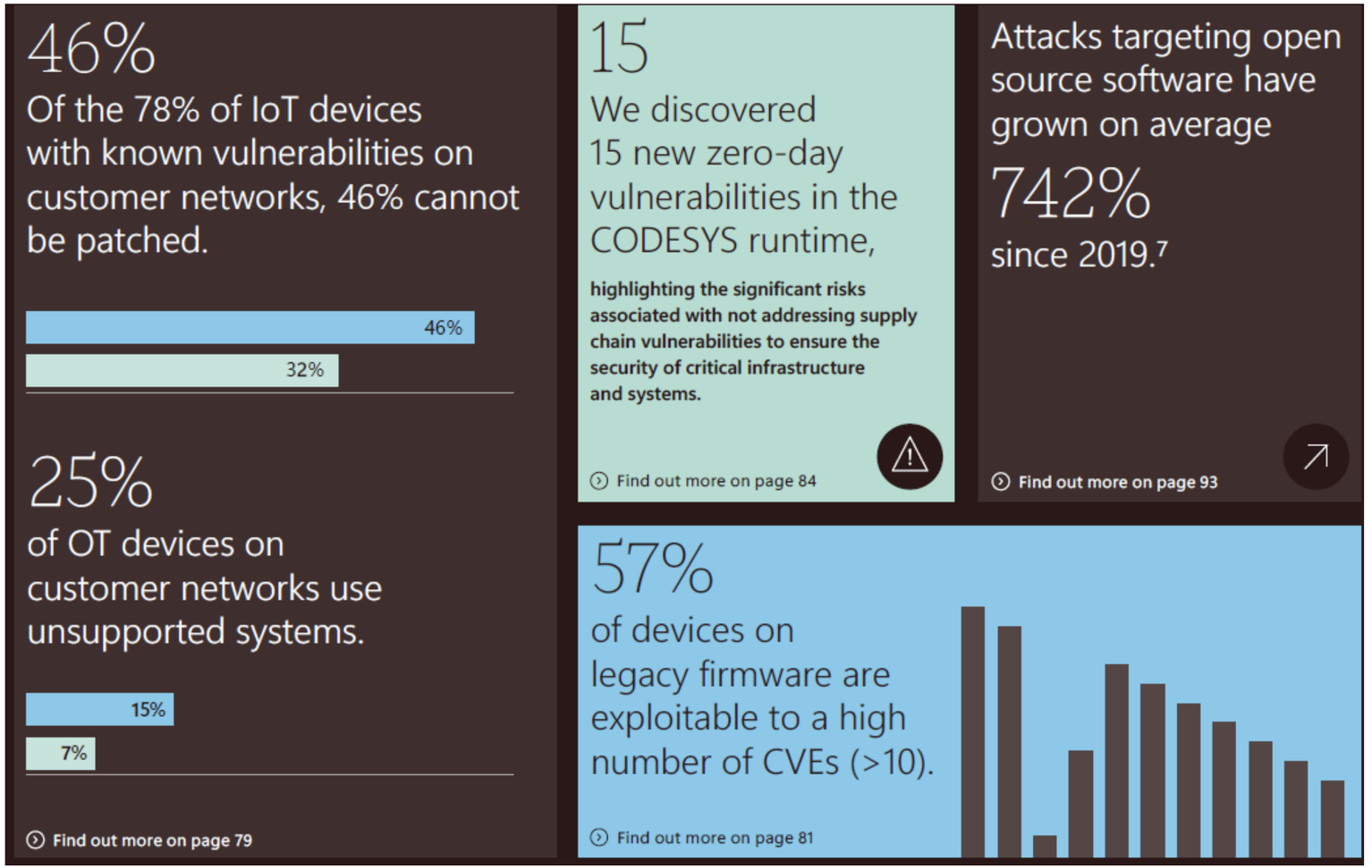
40+5=45% Americhe
32% Europa
(stimiamo 3-4% Italia)

18+3+1+1=23%
MEA/Asia/Oceania

Alcuni dati dal Microsoft Digital Defense Report (Oct.2023)



OT/IOT/IIoT esposti

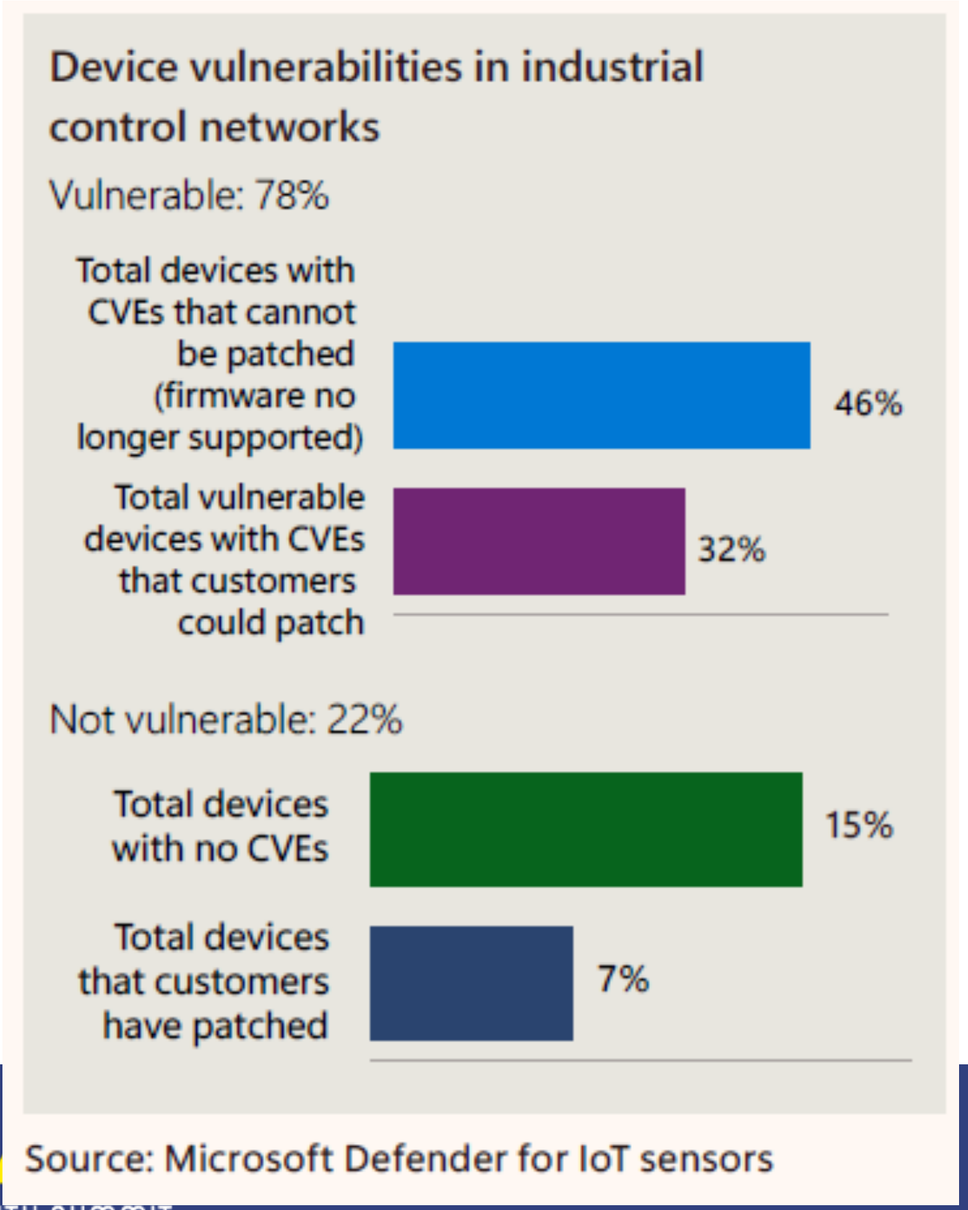


- 78% IoT con Vulnerabilità conosciute, con 46%, quasi la metà, senza possibilità di patch (ovvero il 36%)
- 25% dei dispositivi OT usa SW non supportato (senza possibilità di patch)
- 96% applicazioni usa SW componenti Open Source,
- +742% dal 2010 di attacchi su SW Open Source
- 57% firmare devce OT esposto a più di 10 CVE

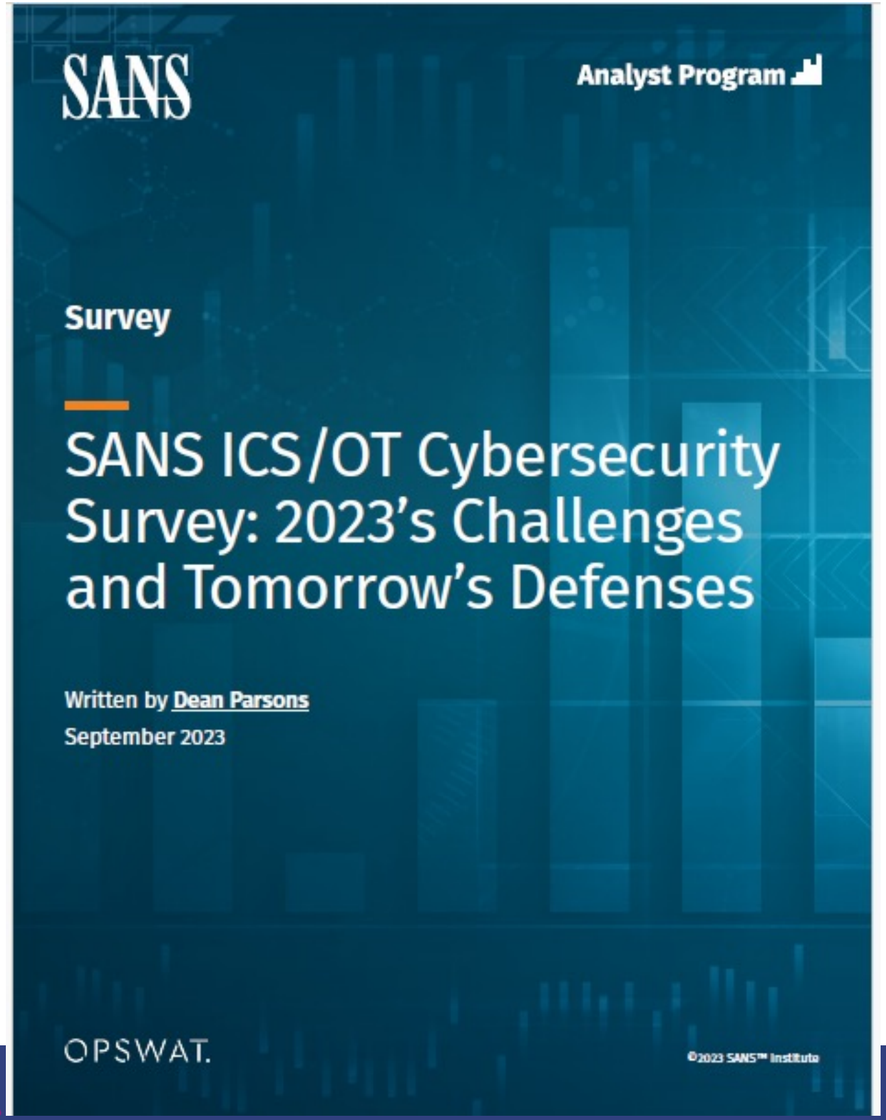
Device ICS/OT vulnerabili e non vulnerabili (PLC ecc.)

- 78% IoT con Vulnerabilità conosciute:
  46%, quasi la metà, senza possibilità di patch (ovvero il 36%)
  32% potrebbe avere patch (il 25%)

- 22% risulta non vulnerabile:
  15% senza CVE conosciute
  7% con patch applicate



Alcuni dati dal SANS ICS/OT CyberSec Survey (Sept.2023)



SANS ICS/OT CyberSec Survey - Demographics

Intervistati 701 CISO che gestiscono oltre 1760 Impianti industriali/Utility

70 CISO Europei (10%) con 245 Impianti (14%)

Oltre 60 categorie industriali

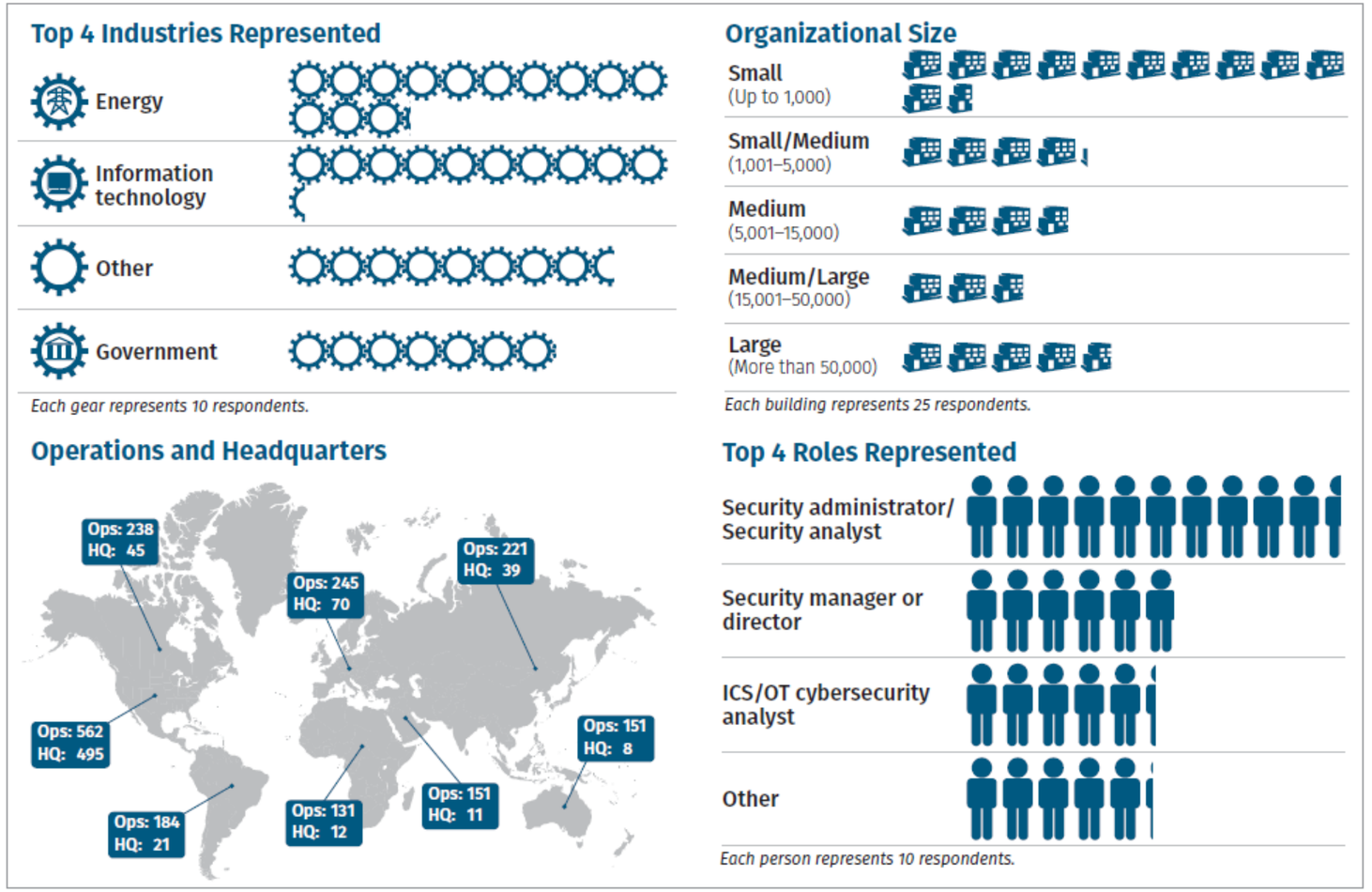


Figure 1. Survey Demographics

SANS ICS/OT CyberSec Survey – Gravità Minacce percepite

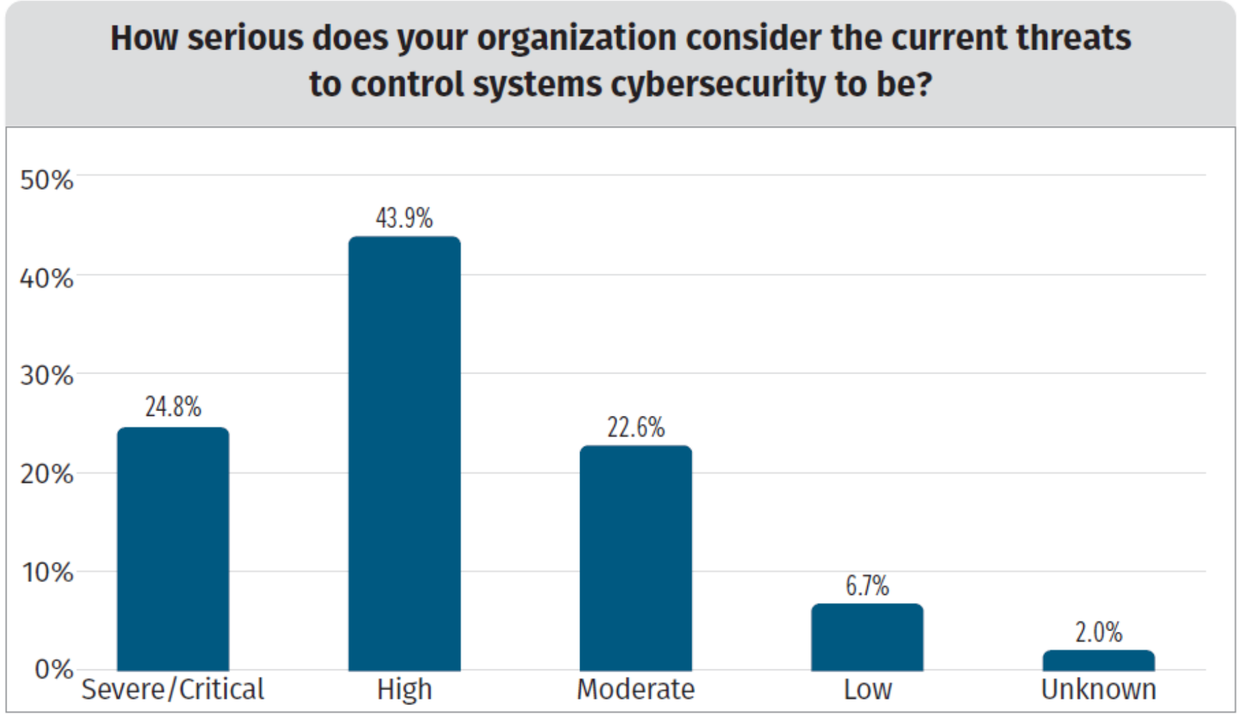


Figure 2. Current Threats to Control Systems

SANS ICS/OT CyberSec Survey – Da dove arriva attacco ?

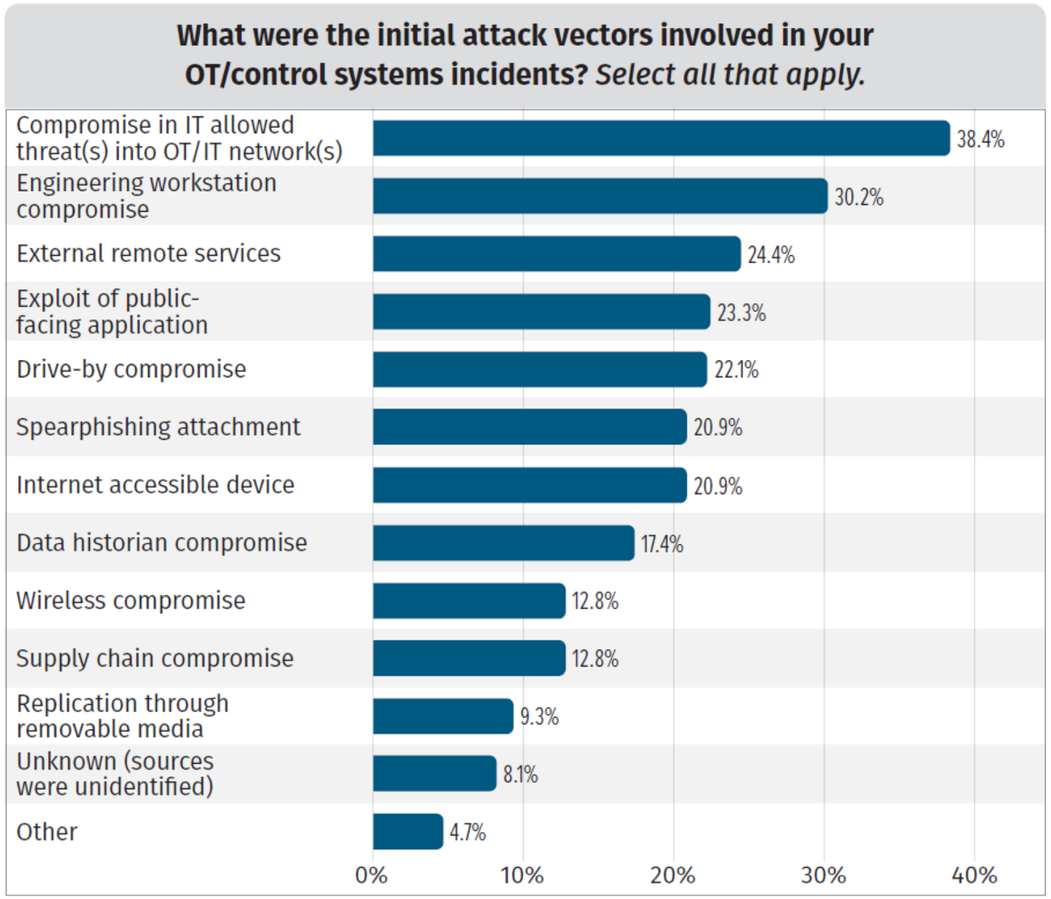


Figure 4. ICS Initial Attack Vectors

SANS ICS/OT CyberSec Survey – confronto budget 2021-23

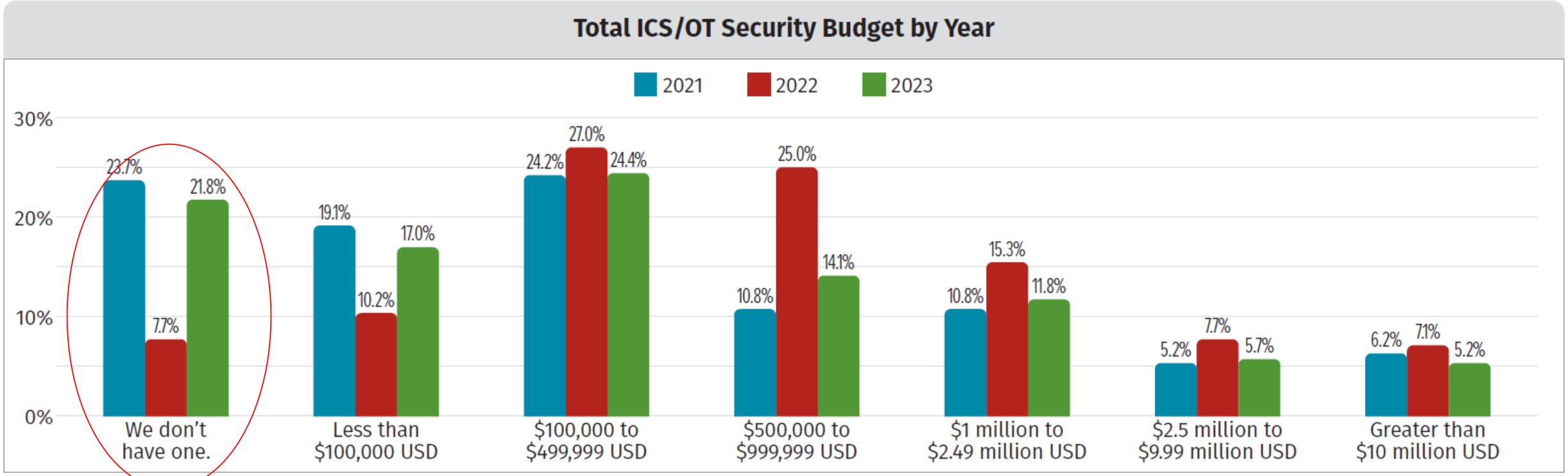


Figure 9. ICS/OT Cybersecurity Budget Comparisons 2021–2023

2022-23: contrazione dei budget per OT Security ed aumenta chi non ha budget ?!

SANS ICS/OT CyberSec Survey – Cosa nei prossimi 18 mesi?

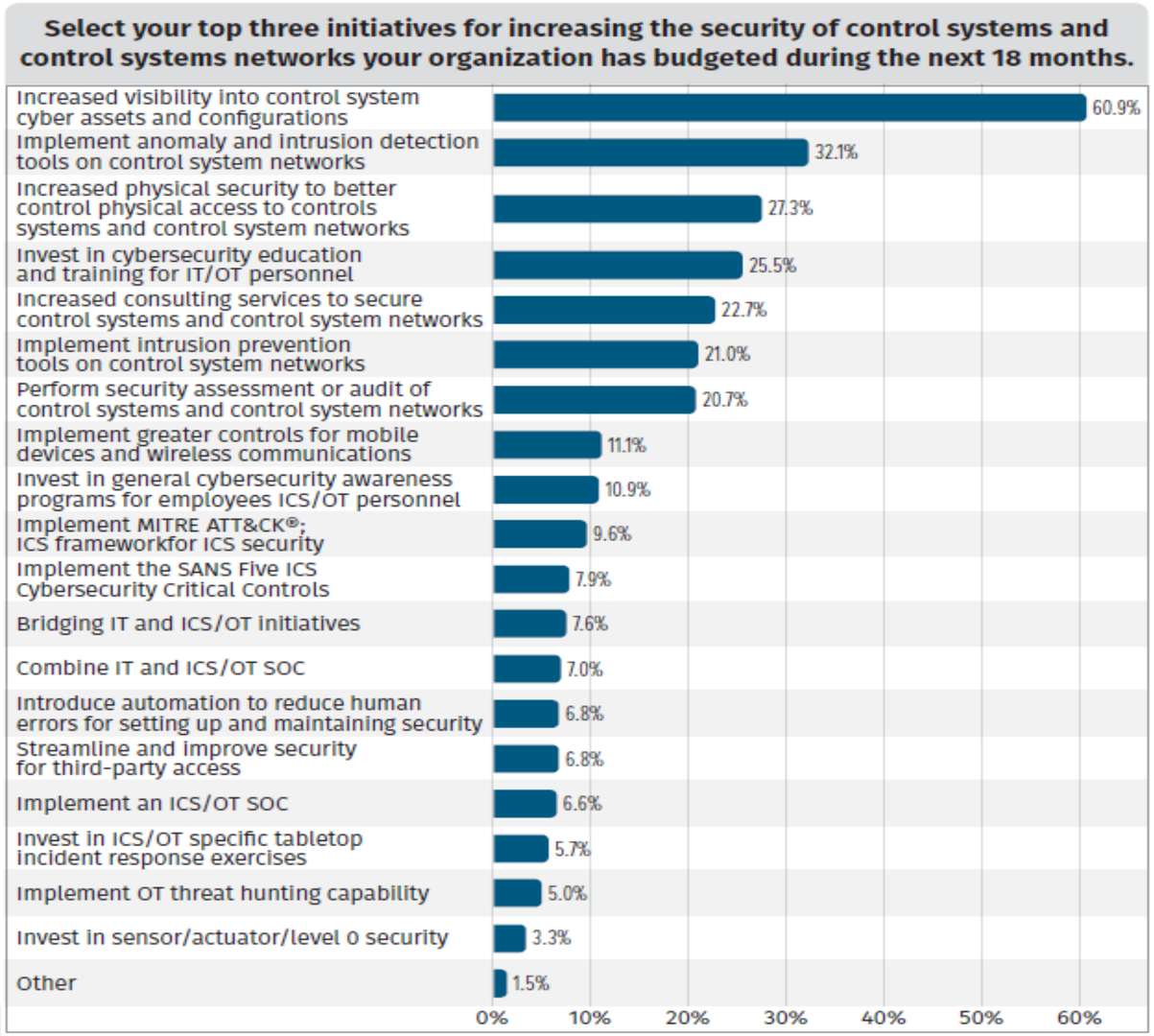


Figure 10. ICS Cybersecurity Investments in the Next 18 Months

SECURITY SUMMIT

9 novembre 2023

Security Summit

Streaming Edition

Security Summit Manufacturing

9 novembre orario 15.00-17.00

Modera: **Enzo Maria Tieghi,** CS Clusit

Partecipano:

•**Prof.ssa Paola Girdinio**, Presidente Centro di Competenza per la Sicurezza delle Infrastrutture Strategiche Digitali START 4.0

•**Ing. Lorenzo Ivaldi,** UNIGE Dipartimento di ingegneria navale, elettrica, elettronica e delle telecomunicazioni – DITEN

•**Giulio Iucci**, Presidente di ANIE Sicurezza

•**Alessandro Manfredini**, Presidente AIPSA e Direttore di Group Security e Cyber Defence del Gruppo A2A

•**Simone Peruzzi,** Enterprise Security Executive, Microsoft Italia

START4.0 – LINEA PNRR
Strumenti di finanziamento

SERVIZIO EROGATO IN AMBITO CYBERSECURITY	Micro e piccole imprese	Medie imprese	Grandi imprese
Audit tecnico, valutazione maturità tecnologica (assessment)	100%	90%	40%
Prova prima dell'investimento: assessment vulnerabilità	100%	80%	30%
Consulenza su protezione proprietà intellettuale	70%	60%	50%
Consulenza su accesso finanziamenti	70%	60%	50%
Consulenza di innovazione tecnologica di processo e di prodotto, networking e sensibilizzazione	80%	70%	50%
Progettazione dell'intervento di innovazione	50%	40%	30%

START4.0 – LINEA PNRR
Strumenti di finanziamento

SERVIZIO	STRUTTURA SERVIZIO	ESEMPI DI SERVIZI	MICRO E PICCOLE IMPRESE	MEDIE IMPRESE	GRANDI IMPRESE
FORMAZIONE	Fino a 24 ore	Formazione cybersecurity: concetti di base, awareness, gestione tavolo di crisi, normativa.	100 %	80%	50%
	Oltre 24 ore		70%	60%	40%