Clusit
Associazione Italiana per la Sicurezza Informatica

ASTREA

SECURITY SUMMIT

Security Summit

Verona, 24 ottobre 2024

Sessione Plenaria

2024: gestire le attuali minacce dalla NIS2 alla Threat Intelligence

Verona, 24 ottobre 2024

Clusit
Associazione Italiana per la Sicurezza Informatica

ASTREA

SECURITY SUMMIT

Security Summit

Verona, 24 ottobre 2024

Introduzione a cura di: **Gabriele Faggioli**, Presidente Clusit

Modera: **Alessio Pennasilico**, CS Clusit

Partecipano:
- **Dr. Letterio Saverio Costa**, Commissario capo tecnico (informatico) della Polizia di Stato, Compartimento Polizia Postale e delle Comunicazioni per il Veneto
- **Ettore Guarnaccia**, Cybersecurity manager, saggista e divulgatore
- **Claudio Telmon**, CD Clusit

I CONTENUTI DEL RAPPORTO

Analisi Clusit degli incidenti di sicurezza più significativi avvenuti a livello globale (Italia inclusa) nel 2023.

- Attacchi rilevati in Italia dal Security Operations Center (SOC) di FASTWEB.
- Rilevazioni e segnalazioni della Polizia Postale e delle Comunicazioni, rispetto ad attività ed operazioni svolte nel corso degli ultimi 12 mesi.
- **Settore FINANCE:** un'analisi sul Cyber-crime nel settore finanziario in Europa, a cura di IBM.
- **Cybersecurity in Sanità:** Tra Aumento degli Attacchi e Innovazioni Normative e Tecnologiche, realizzato dalle Women for Security.

Survey realizzata da Netwrix, che ha intervistato 1.610 professionisti IT provenienti da 106 paesi, sulle tendenze della Hybrid Security

I CONTENUTI DEL RAPPORTO: FOCUS ON

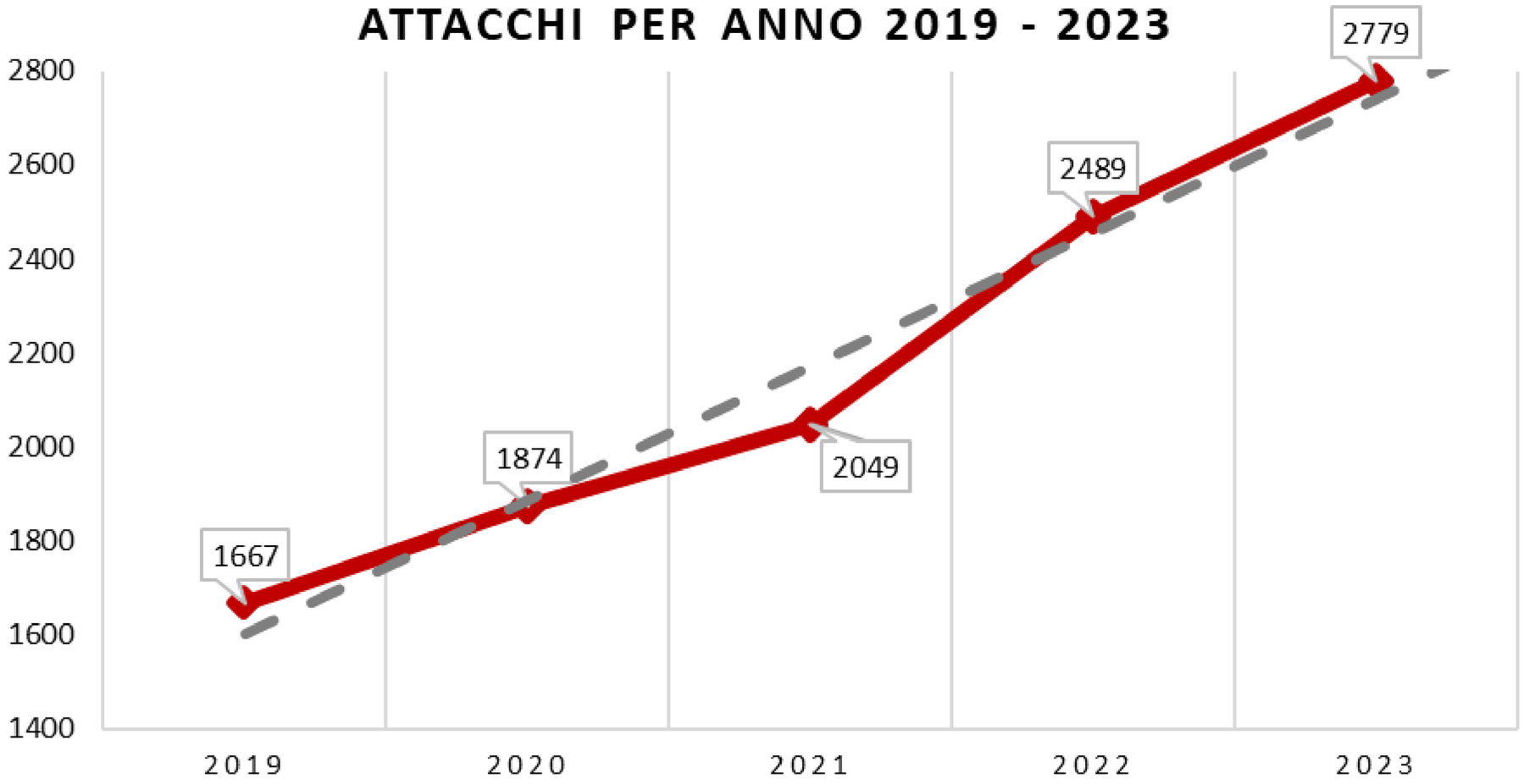
- Il mondo della **sicurezza delle Identità**, a cura di RSA Security Italia
- Attività della **Task Force** Cisco Talos in difesa dell'Ucraina, a cura di Cisco
- Secure Access Service Edge **(SASE),** a cura di Fortinet
- **Cloud adoption e superficie d'attacco:** aumentare la visibilità e la protezione contro gli attacchi nell'infrastruttura e nelle applicazioni Cloud adoption e superficie d'attacco cloud, a cura di Crowdstrike
- Costruire la **cyber resilience per la Space Economy**, a cura di Federica Maria Rita Livelli
- **CSIRT Network**: Incident Response per una Crisis Management di successo in un Contesto Internazionale, a cura di NTT Data
- **Intelligenza Artificiale e Automazione: le** chiavi per rivoluzionare il SOC, a cura di PaloAlto Networks
- La Sicurezza dei sistemi di acquisizione e stampa, a cura di ASSOIT
- Attraverso il tunnel del cambiamento: **l'evoluzione della connessione sicura da VPN a ZTNA**, a cura di HPE Aruba Networking
- Strategie di **data security nell'era dell'AI Generativa**, a cura di Microsoft
- Sviluppo sicuro del **codice software**, a cura di Roberto Obialero

+12%

È la crescita degli incidenti dal 2022 al 2023

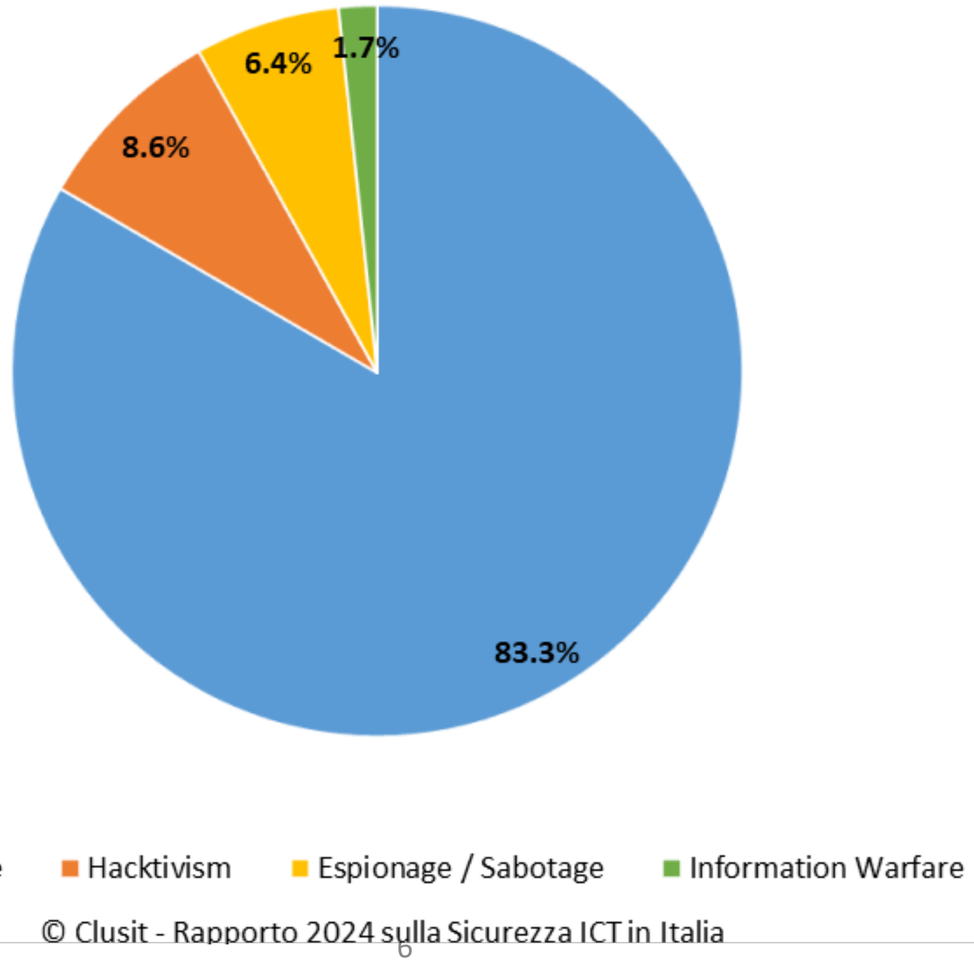
56%

Degli incidenti censiti dal 2011 sono avvenuti negli ultimi 5 anni



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

TIPOLOGIA E DISTRIBUZIONE ATTACCANTI 2023

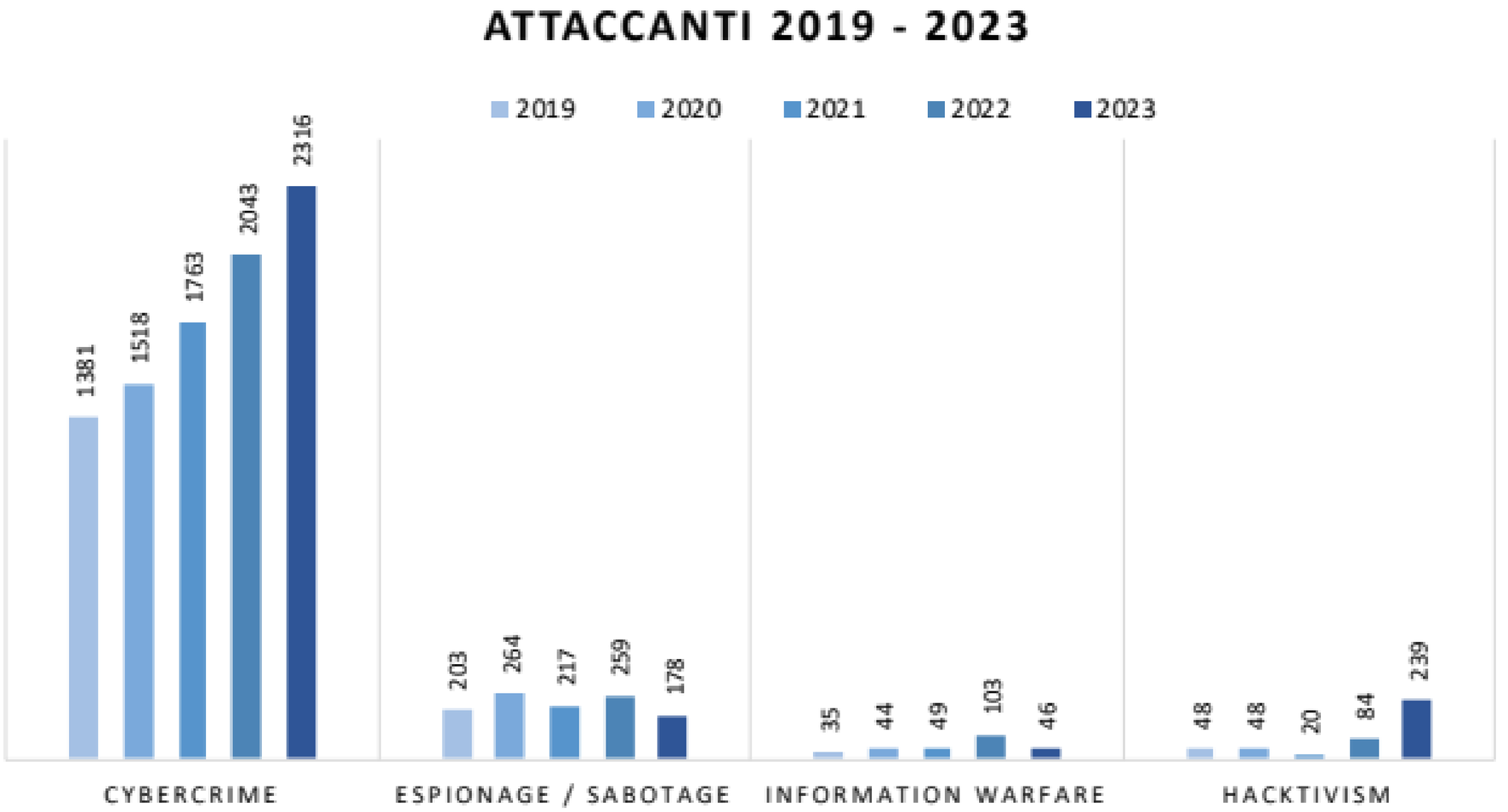


+13%

È la crescita degli incidenti causati dal Cybercrime nel 2023

1 su 10

è un incidente con matrice Warfare o Hacktivism



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

+30%

È la crescita del numero degli incidenti a danno del settore HealthCare

+50%

*gli incidenti al settore GOV negli ultimi **5 anni***

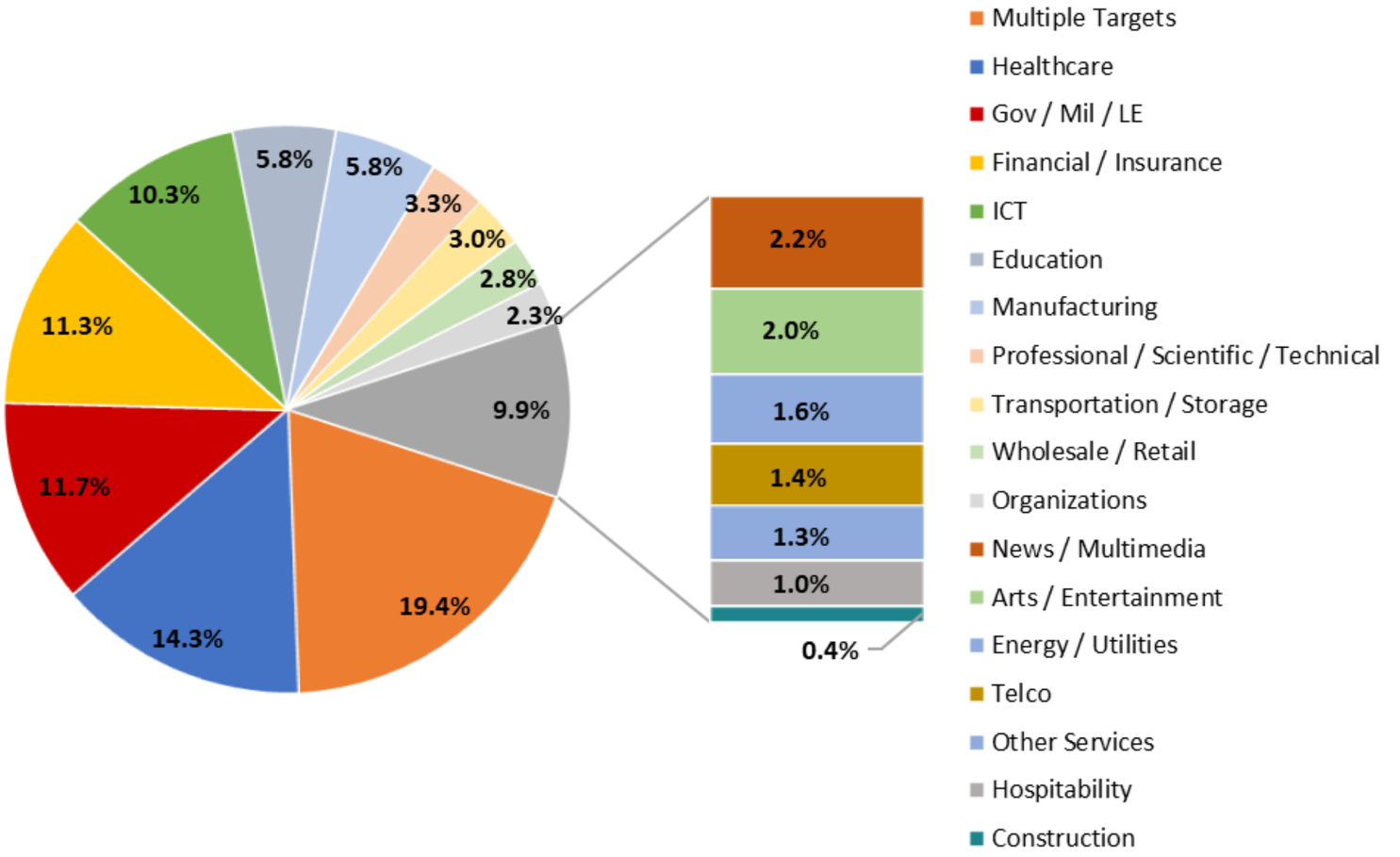
+62%

è la crescita degli incidenti a danno dei settori Financial/Insurance

+25%

è la crescita degli incidenti a danno del settore Manufacturing

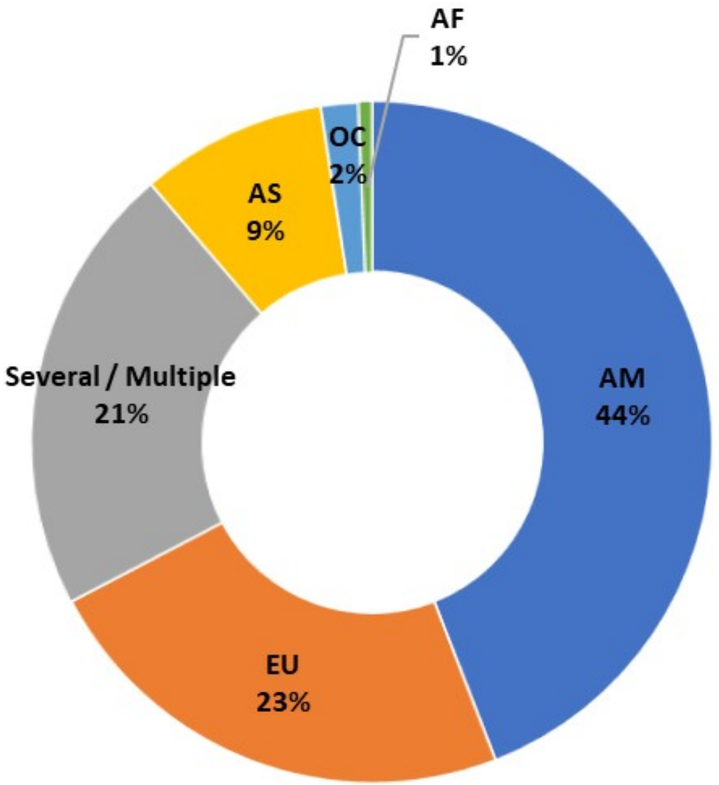
DISTRIBUZIONE DELLE VITTIME 2023



+7,5%

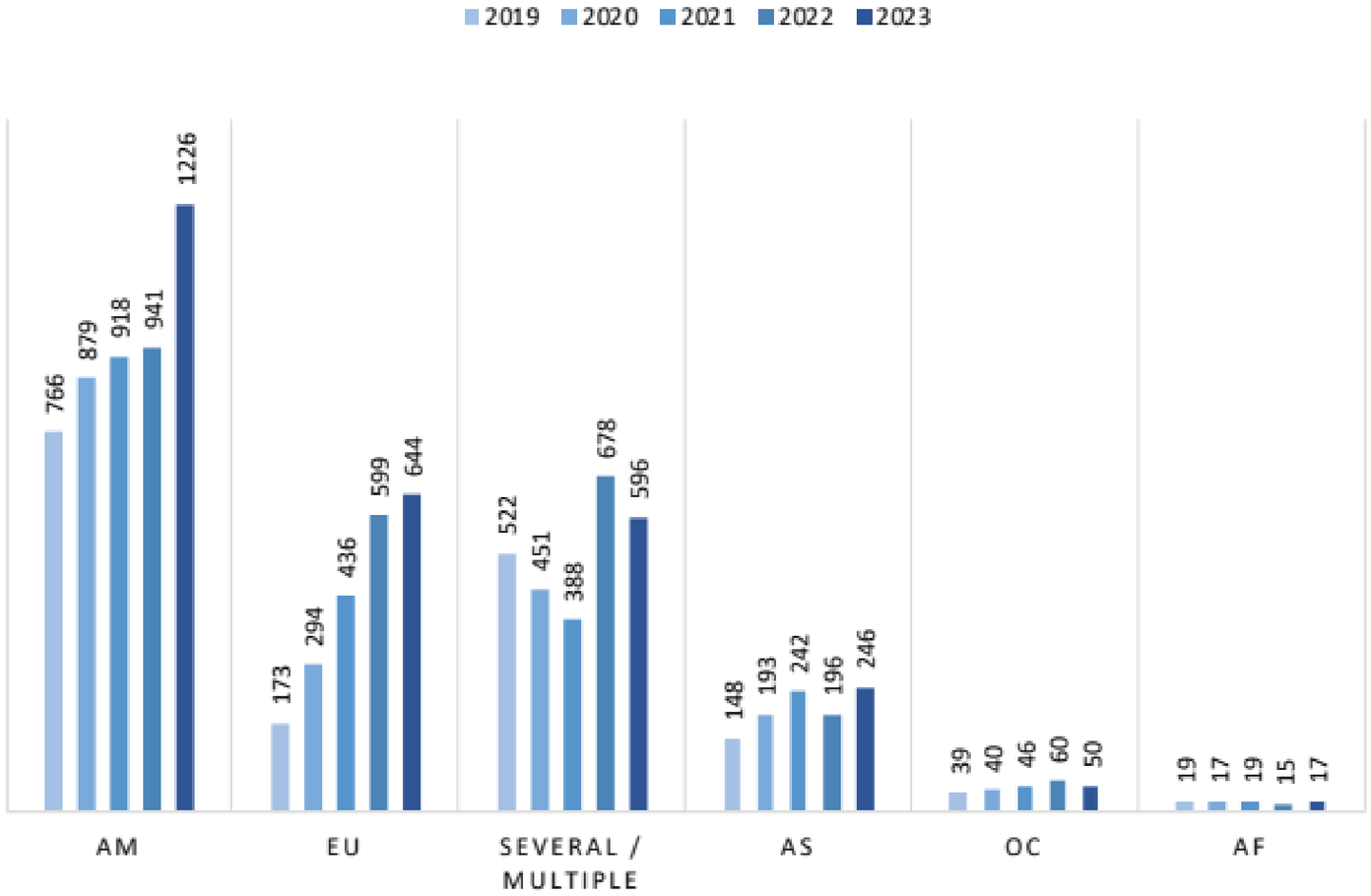
è la crescita degli incidenti avvenuti nel continente Europeo

GEOGRAFIA DELLE VITTIME 2023



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

GEOGRAFIA DELLE VITTIME 2019 - 2023



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

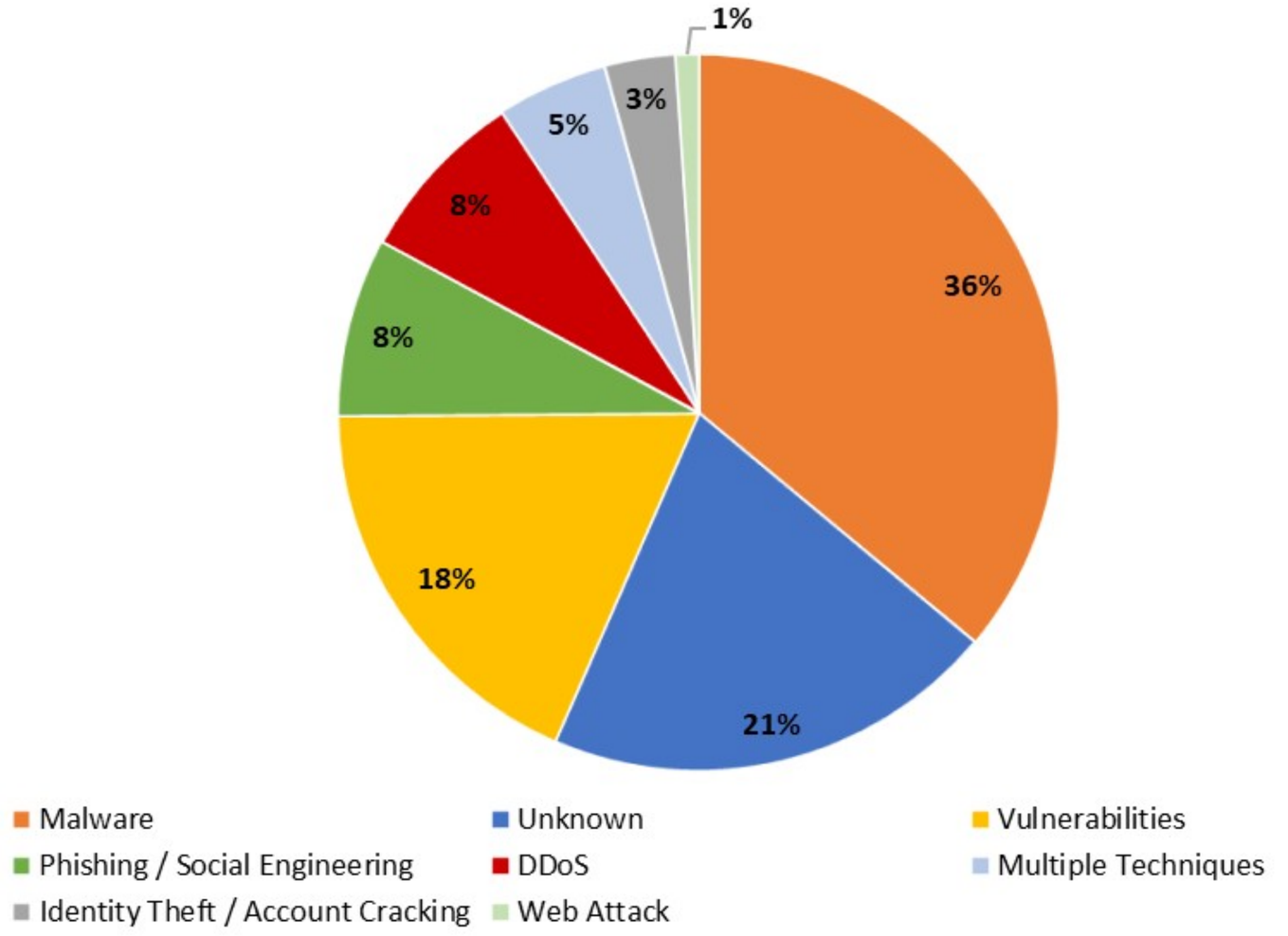
+75,9%

è la crescita degli attacchi basati su vulnerabilità note e 0-day

+98%

È la crescita del numero degli incidenti DDOS

DISTRIBUZIONE DELLE TECNICHE 2023

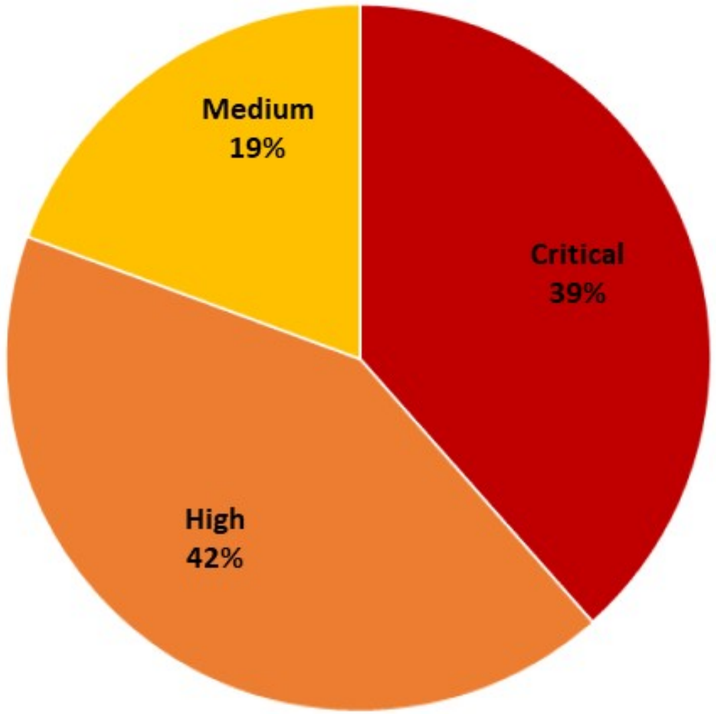


© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

4 su 5

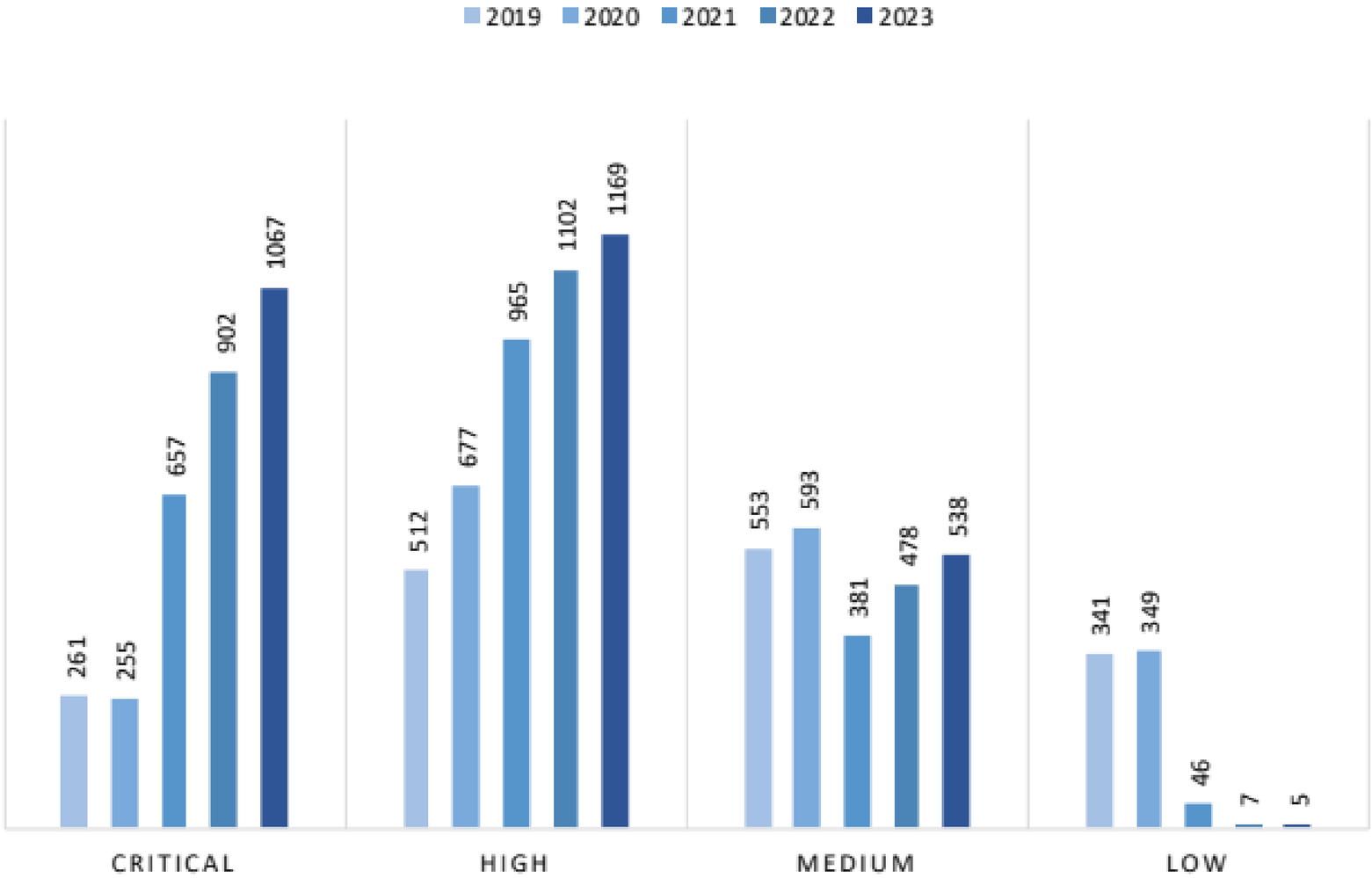
sono i casi in cui, quando avvengo, gli incidenti causano la massima Severity (Critical o High)

SEVERITY ATTACCHI 2023



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

SEVERITY 2019 - 2023

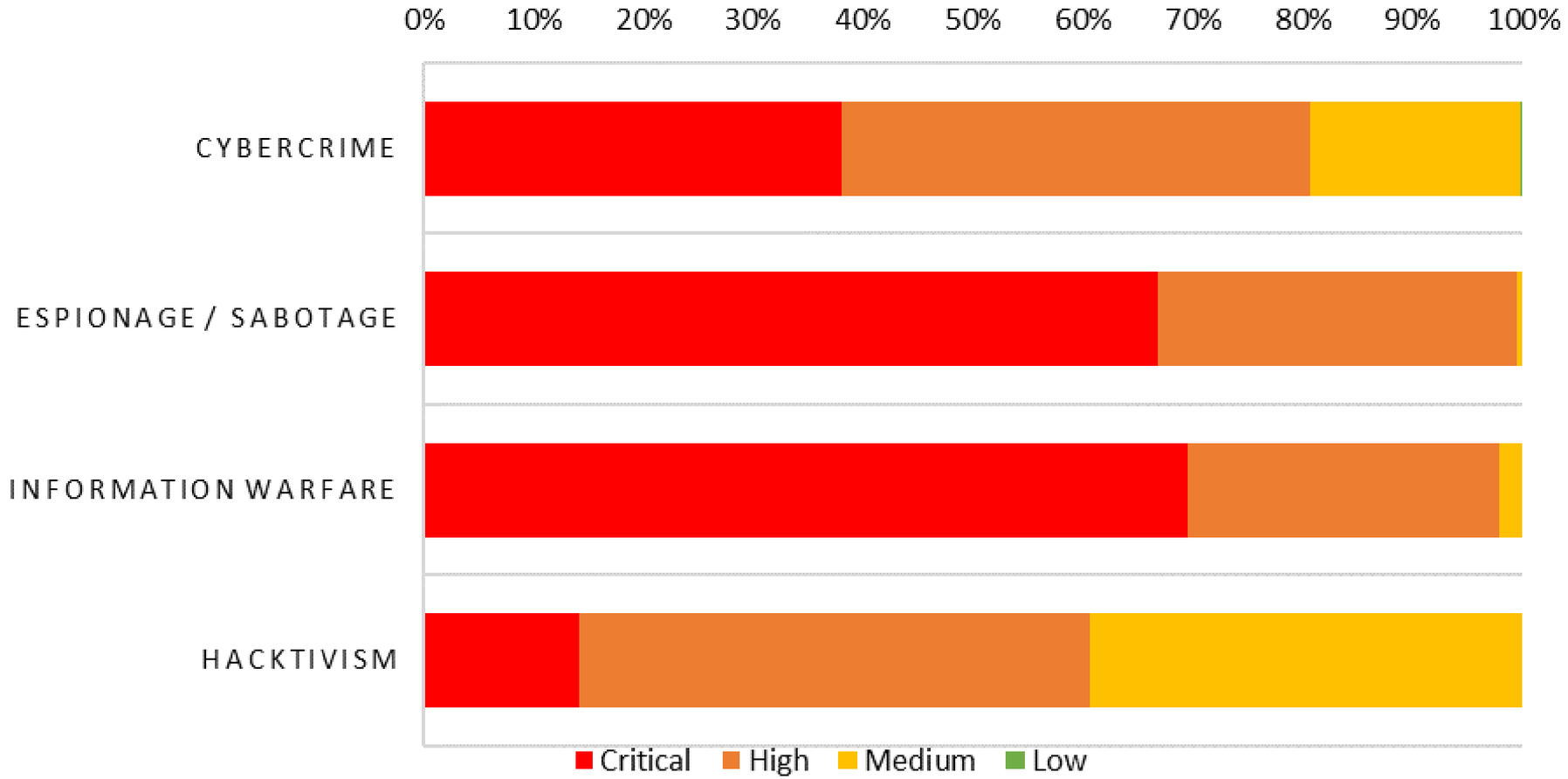


© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

-39,6%

è la riduzione degli incidenti di severità Critical per attacchi di Hacktivism

SEVERITY PER ATTACCANTI 2023



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

APPROFONDIMENTO **CLUSIT** SULLA SITUAZIONE **IN ITALIA**

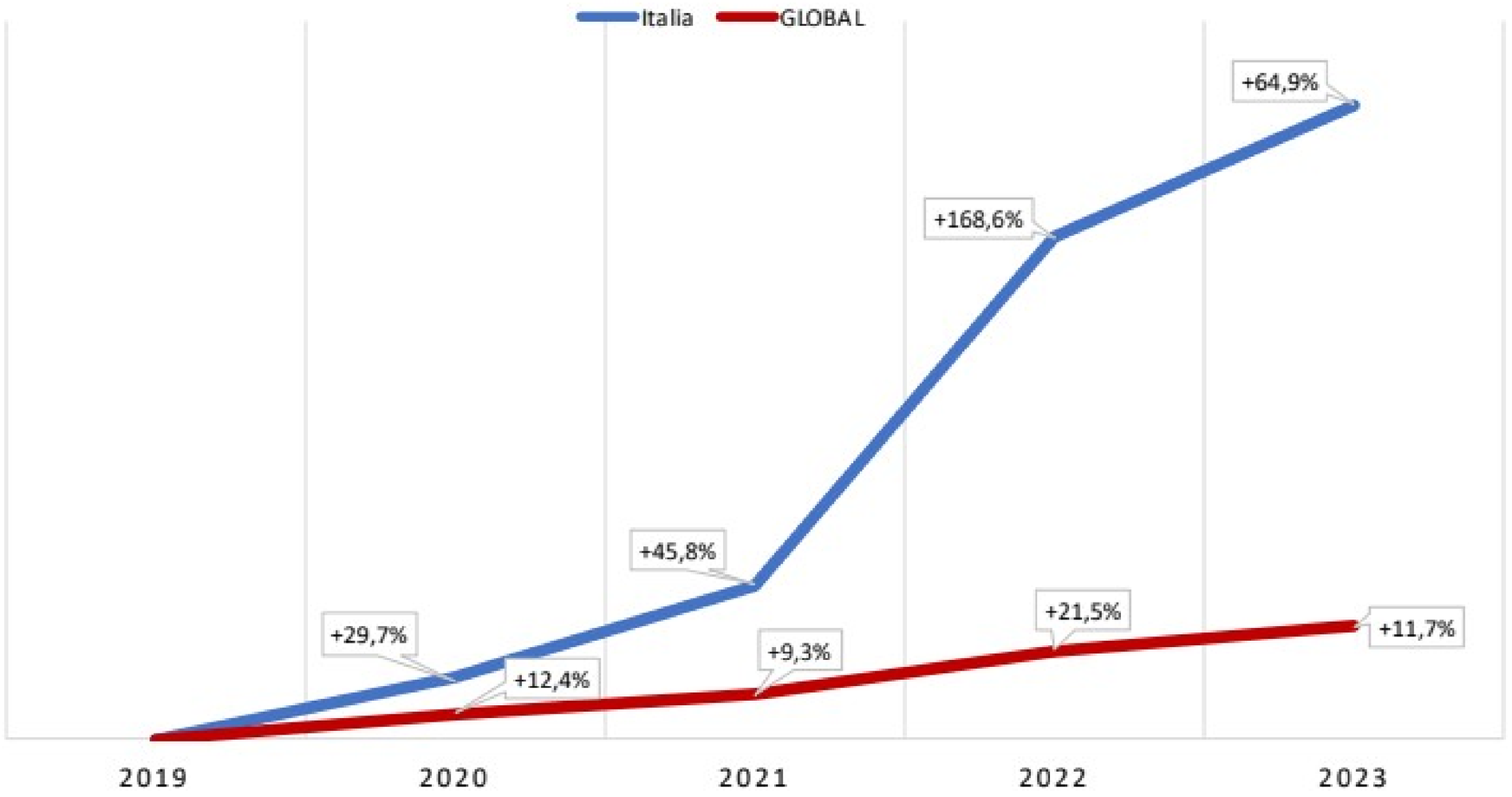
CONFRONTO CRESCITA % ITALIA VS GLOBAL

+65%

è la crescita degli incidenti informatici in Italia nel 2023

11,2%

è la quantità di incidenti censiti in Italia rispetto al resto del mondo

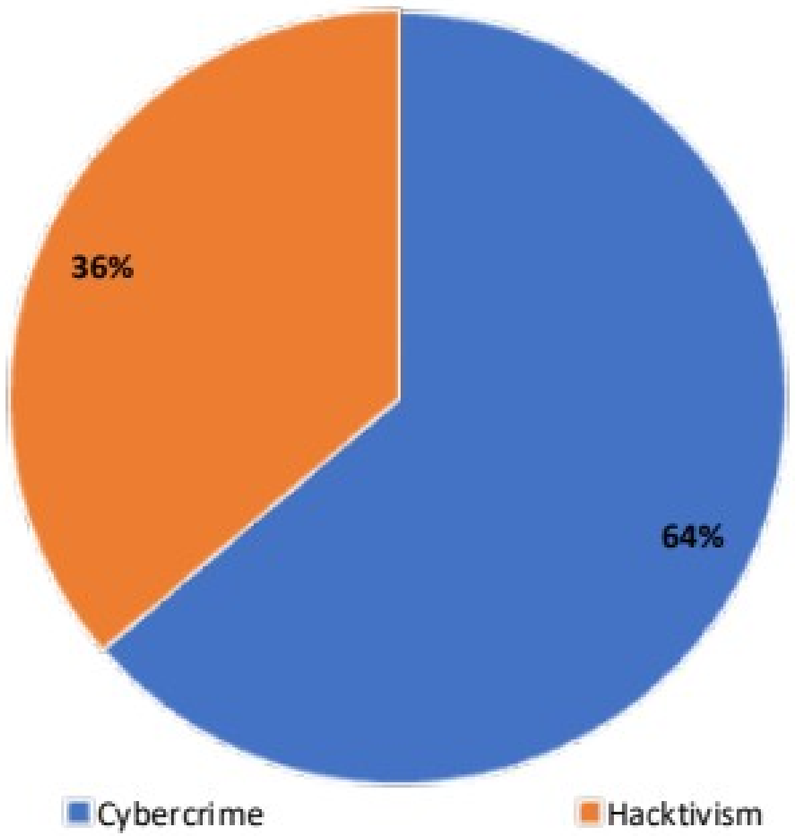


© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

47%

degli attacchi di Hacktivism a livello Global, è avvenuto a danni dell'Italia

ATTACCANTI IN ITALIA 2023



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

TECNICHE DI ATTACCO IN ITALIA 2023

DDOS

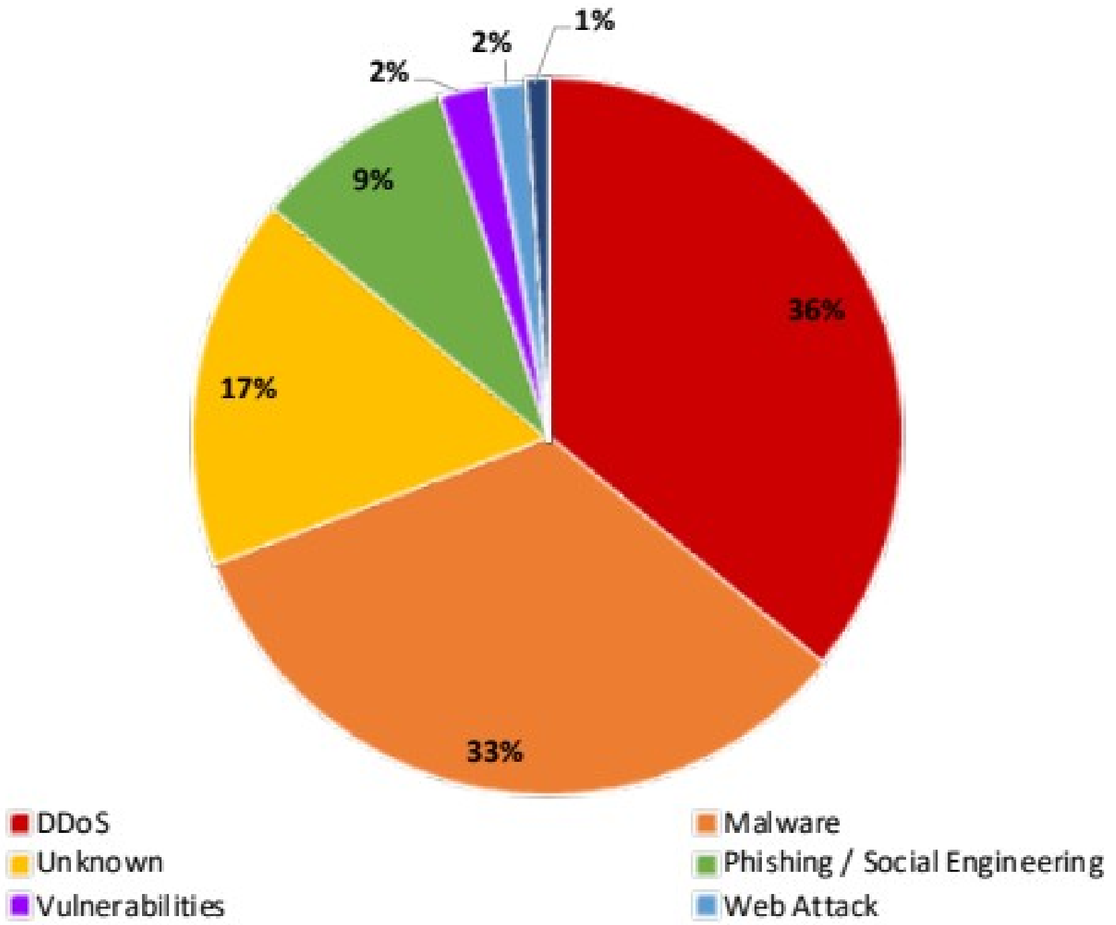
è la principale tecnica di attacco in Italia

+4%

è la crescita degli attacchi basati su Malware in Italia

+87%

è la crescita degli attacchi phishing e social engineering in Italia

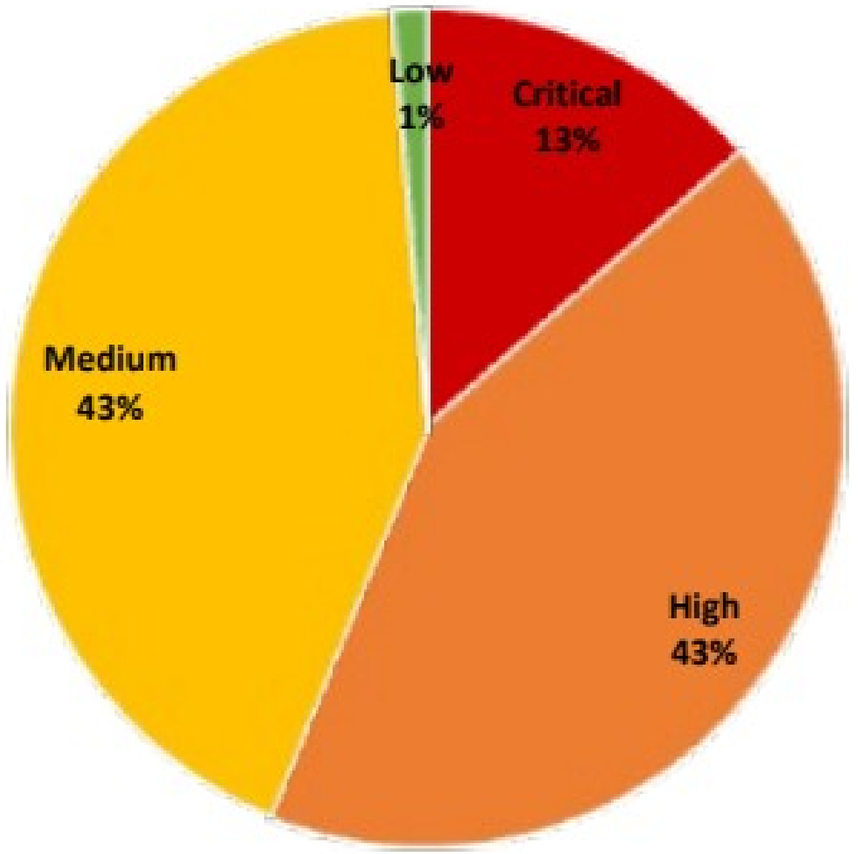


© Clusit - Rapporto 202 sulla Sicurezza ICT in Italia

SEVERITY IN ITALIA 2023

+53%

di attacchi con severity High in Italia, nel 2023



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

Take away

- Rafforzare la governance della sicurezza e la capacità di identificare, analizzare, valutare e gestire i rischi
- Sviluppare una cultura della sicurezza che sia parte del patrimonio di conoscenze di tutti i cittadini, a partire dalle nuove generazioni
- Governance dei processi di patch & vulnerability management
- Presidio continuo della sicurezza di prodotti e servizi lungo l'intero ciclo di vita (SSDLC - Secure Software Development LifeCycle)
- Gestione dei processi di sourcing e delle terze parti (anche in ottica ESG)
- Backup & Disaster Recovery & Continuità Operativa
- Rafforzamento della sicurezza del mondo OT
- Prepararsi alla gestione degli incidenti e delle crisi
- Utilizzo dell'AI per «contrastare» la AI
- Ridurre la frammentazione di infrastrutture e servizi

Clusit
Associazione Italiana per la Sicurezza Informatica

ASTREA

SECURITY SUMMIT

Security Summit

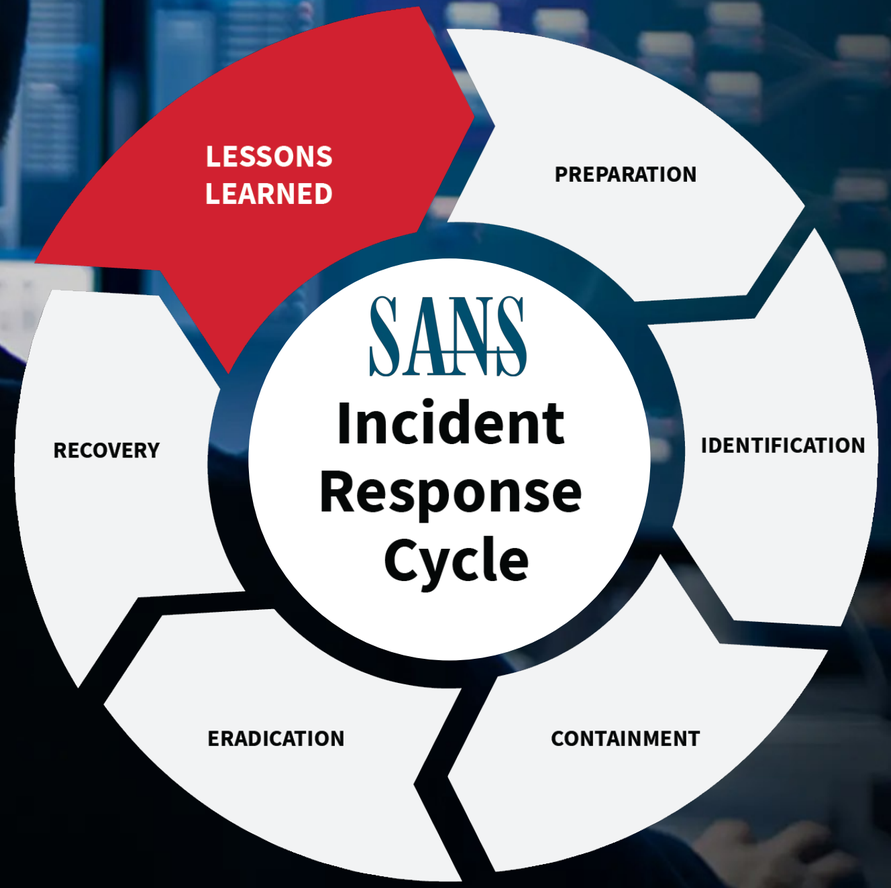
Verona, 24 ottobre 2024

Introduzione a cura di: **Gabriele Faggioli**, Presidente Clusit

Modera: **Alessio Pennasilico**, CS Clusit

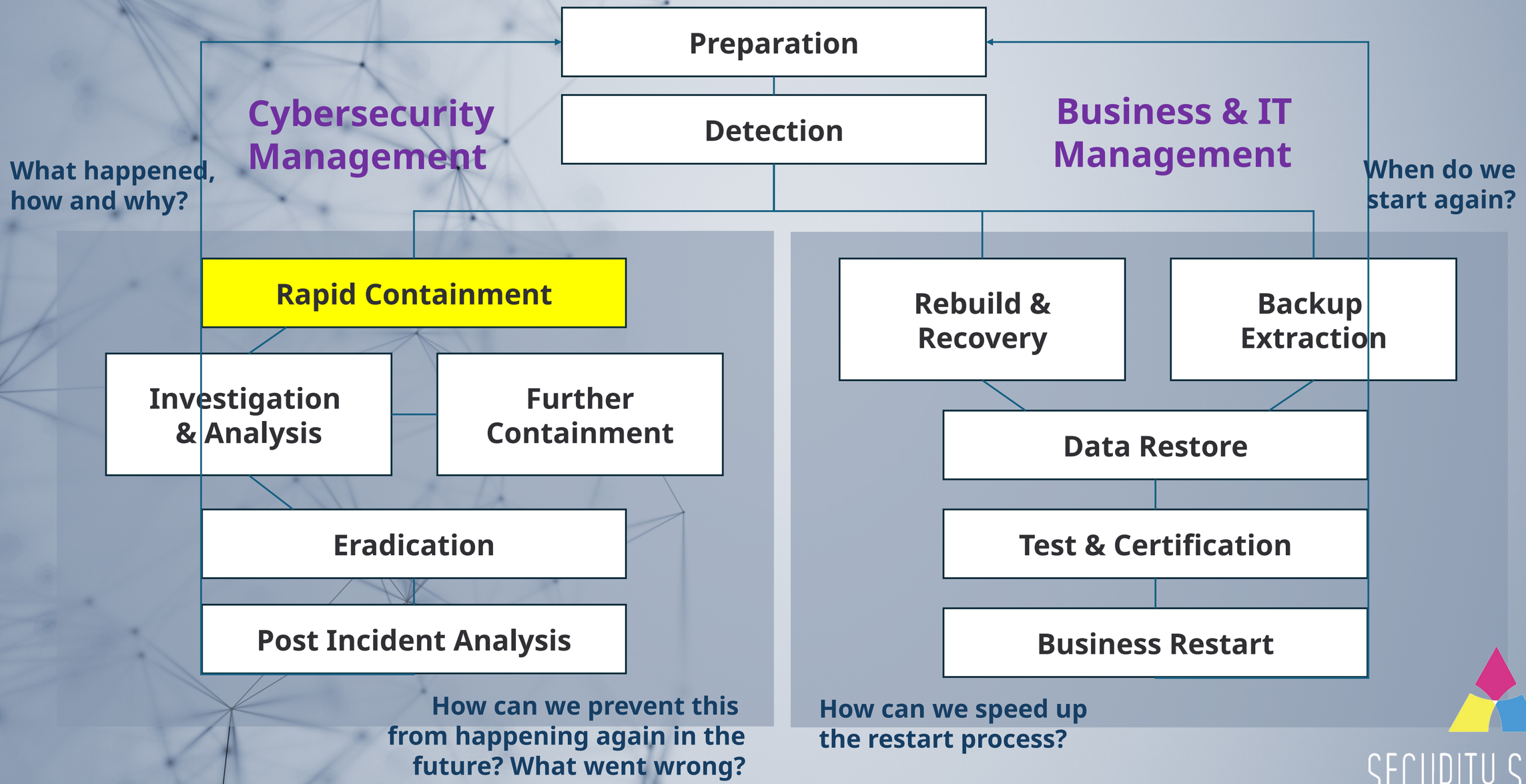
Partecipano:
- **Dr. Letterio Saverio Costa**, Commissario capo tecnico (informatico) della Polizia di Stato, Compartimento Polizia Postale e delle Comunicazioni per il Veneto
- **Ettore Guarnaccia**, Cybersecurity manager, saggista e divulgatore
- **Claudio Telmon**, CD Clusit

Traditional incident response frameworks are no longer suited to the modern context.



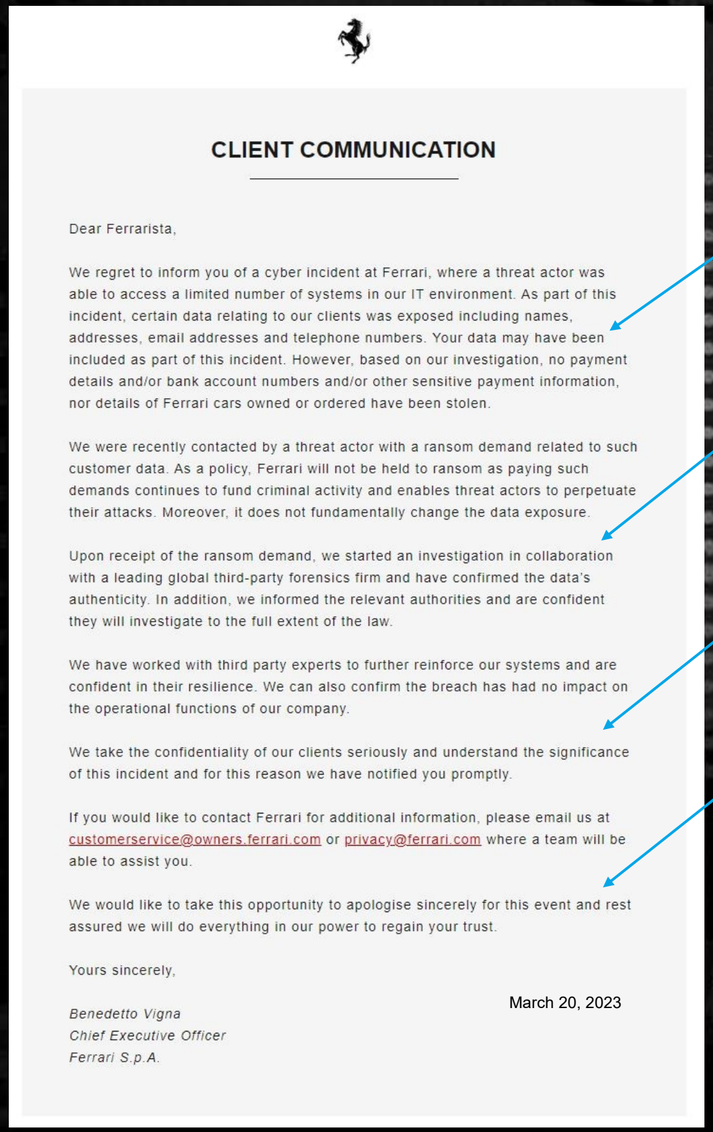
SECURITY SUMMIT

We no longer have the luxury of doing things one step at a time.



SECURITY SUMMIT

How to communicate properly



CLIENT COMMUNICATION

Dear Ferrarista,

We regret to inform you of a cyber incident at Ferrari, where a threat actor was able to access a limited number of systems in our IT environment. As part of this incident, certain data relating to our clients was exposed including names, addresses, email addresses and telephone numbers. Your data may have been included as part of this incident. However, based on our investigation, no payment details and/or bank account numbers and/or other sensitive payment information, nor details of Ferrari cars owned or ordered have been stolen.

We were recently contacted by a threat actor with a ransom demand related to such customer data. As a policy, Ferrari will not be held to ransom as paying such demands continues to fund criminal activity and enables threat actors to perpetuate their attacks. Moreover, it does not fundamentally change the data exposure.

Upon receipt of the ransom demand, we started an investigation in collaboration with a leading global third-party forensics firm and have confirmed the data's authenticity. In addition, we informed the relevant authorities and are confident they will investigate to the full extent of the law.

We have worked with third party experts to further reinforce our systems and are confident in their resilience. We can also confirm the breach has had no impact on the operational functions of our company.

We take the confidentiality of our clients seriously and understand the significance of this incident and for this reason we have notified you promptly.

If you would like to contact Ferrari for additional information, please email us at customerservice@owners.ferrari.com or privacy@ferrari.com where a team will be able to assist you.

We would like to take this opportunity to apologise sincerely for this event and rest assured we will do everything in our power to regain your trust.

Yours sincerely,

March 20, 2023

Benedetto Vigna
Chief Executive Officer
Ferrari S.p.A.

"We know" there has been a cyber incident

"We do" we are working hard on the solutions

"We care" we understand the gravity...

"We are sorry" we apologize...

"We will be back" and will keep you informed...

SECURITY SUMMIT

Clusit
Associazione Italiana per la Sicurezza Informatica

ASTREA

SECURITY SUMMIT

Security Summit

Verona, 24 ottobre 2024

Contatti

rapporti@clusit.it

info@astrea.pro