CYBER SECURITY

CONFERENCE 2025

MILANO - 13 FEBBRAIO

Dall'ingegno di Leonardo alla Sicurezza Digitale:
un viaggio nel futuro della Cyber Security

OTS

MBARO SIANA
Veneranda Biblioteca Ambrosiana

Lenovo

cynet

proofpoint.

NOZOMI NETWORKS

Inquadra il QR Code per scaricare il materiale dell'evento

Il Gruppo OTS - Uniti nell'Innovazione

athon

www.athon.eu

- ERP (MS365 Business Central)
- Business Intelligence
- Data Analytics
- Document System

OTS

www.ots-web.com

- Cloud
- CyberSecurity
- Managed Services
- Professional Services
- Projects

ITB Salesforce inside

www.itb-web.com

- CRM
- Sales
- Digital Marketing
- Service
- Field Service

OTS - CyberSecurity Services

Defensive Security (Blue Team)

- Security Operations Center (SOC) 24/7
- **Managed Detection & Response (MDR) 24/7**
- Threat Intelligence
- ContinuousVA
- Compromise Credential Monitoring

Offensive Security (Red Team)

- Vulnerability Assessment & Penetration Test (VA/PT)
- **RedTeaming & Gap Analysis**
- Social Engineering & Phishing Simulation

Compliance & Governance (Consulting Team)

- **Security Risk Assessment** & Posture
- **Incident Response Planning**
- **NIS2**
- Security **Hardening** (on-prem & cloud)
- **Security Awareness**

CyberSecurity Conference | 13 febbraio 2025

OTS CyberSecurity Outlook 2025

Autori:

Marco Stefanini
Sales Engineer & Cyber Security Enthusiast

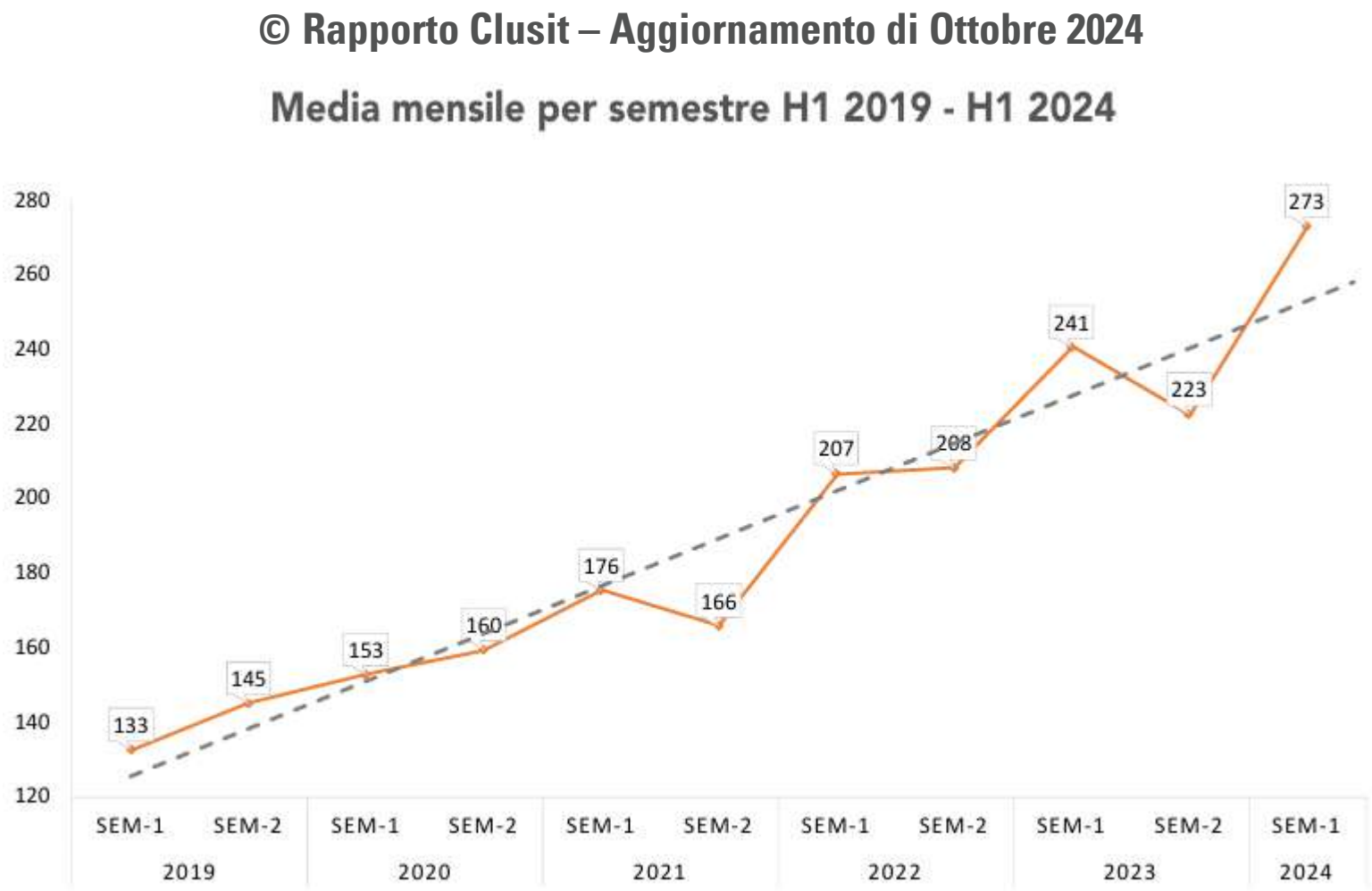
Massimo Montedoro
Head of IT Services & Innovation

OTS

MBARO SIANA
Veneranda Biblioteca Ambrosiana

Trend di Crescita degli Attacchi

© Rapporto Clusit – Aggiornamento di Ottobre 2024



Identity Theft

Nel I sem. 2024 sono avvenuti nel mondo più incidenti di questa categoria che negli anni precedenti

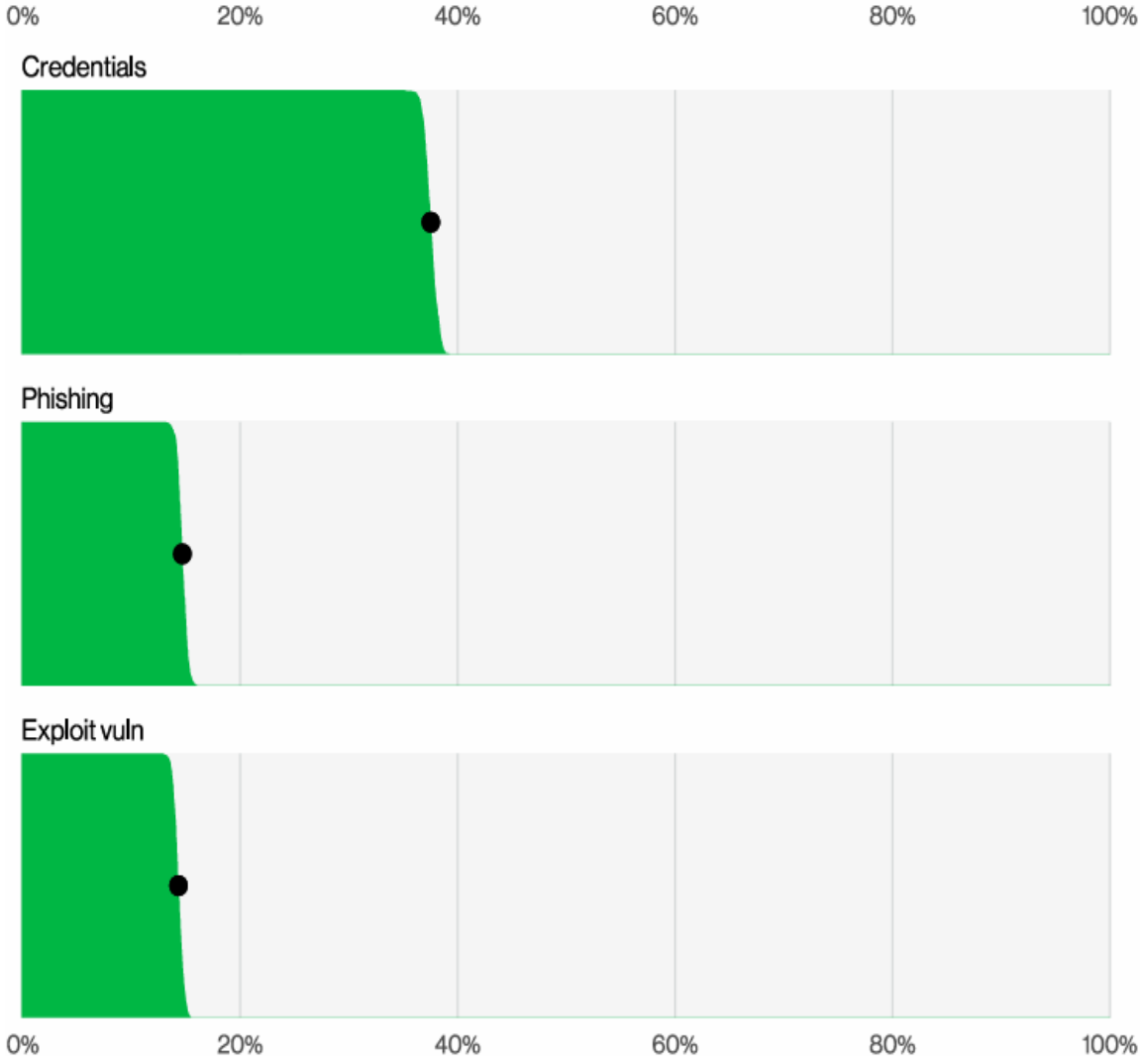
1/3

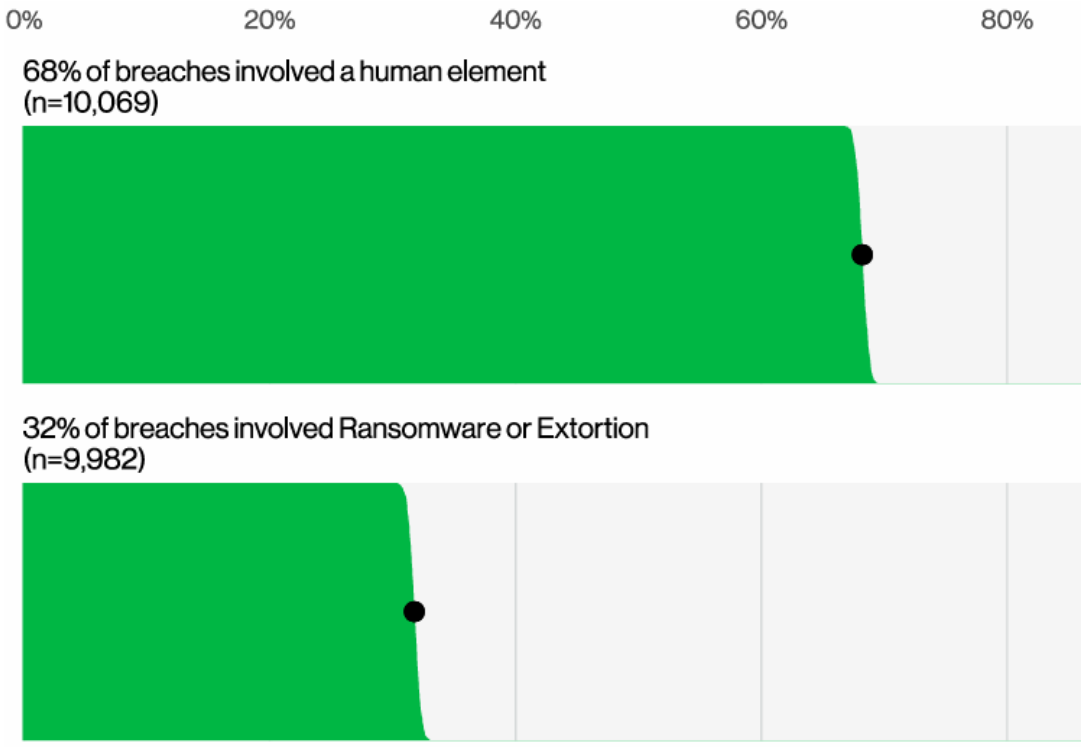
degli incidenti a livello mondiale colpisce il continente europeo

1° Manifacturing

il settore più colpito da incidenti cyber in Italia nel I semestre 2024

Principali Vettori di Attacco



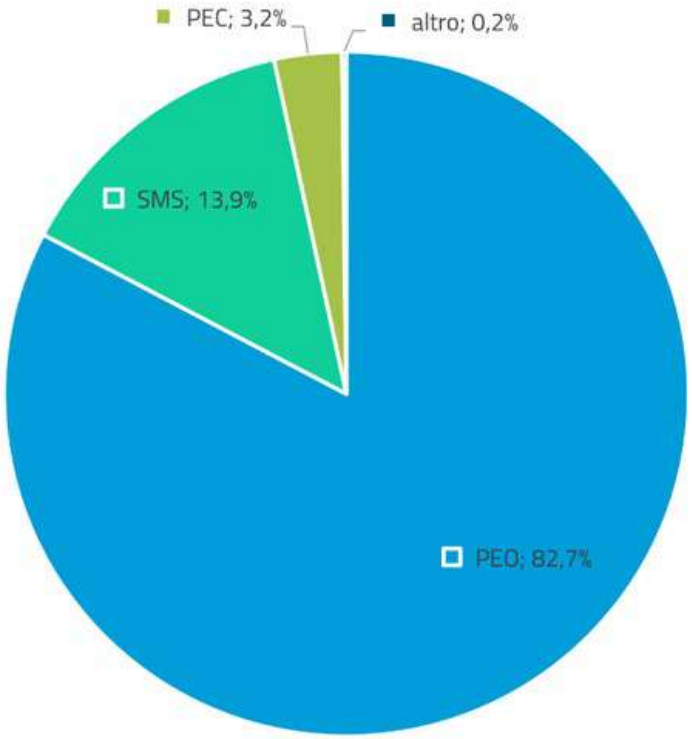


Data Breach Investigations Report 2024

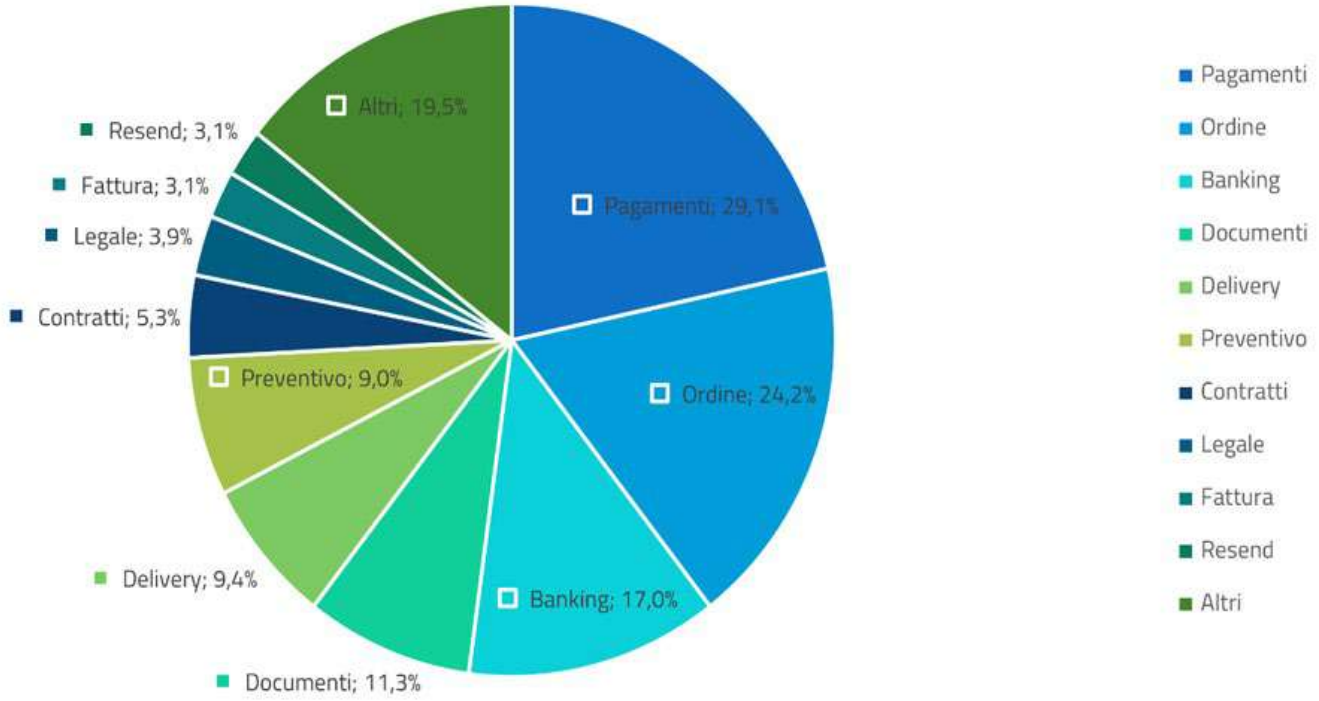
© Verizon

Cyber Threat Landscape Italia - Cert-AgID 2024

Canali di diffusione delle campagne malevole nel 2024



"Temi" più sfruttati per veicolare malware nel 2024



Email

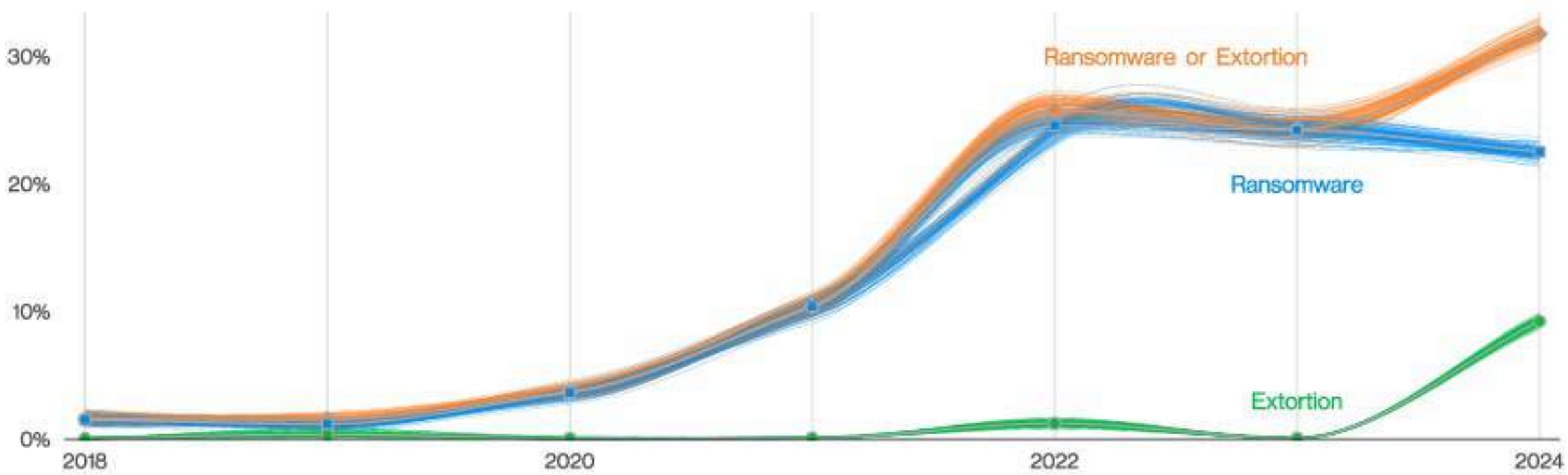
Principale canale per phishing/malware.

PEC compromesse usate per attacchi credibili

Tema "Pagamenti"

141 campagne legate a transazioni finanziarie

Ransomware and Extortion Breaches over Time



+95% Ransomware nel settore manifatturiero

Diminuzione attacchi Ransomware «puri»

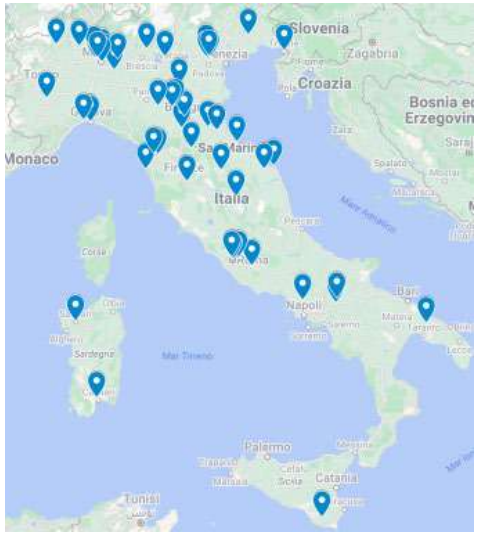
Aumento attacchi con sola esfiltrazione dati

Data Breach Investigations Report 2024

© Verizon

Ransomware – Focus Italia

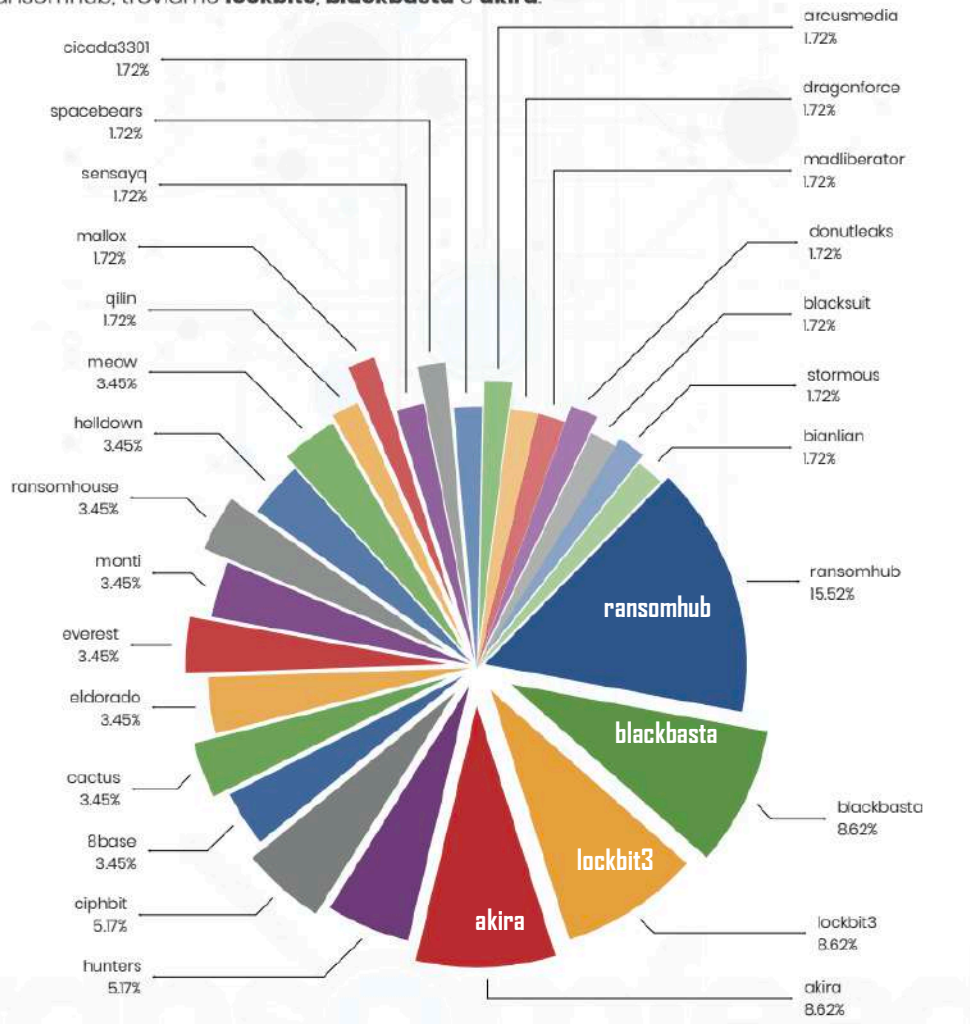
- **industria**, 41.0%
- **commercio**, 28.2%
- **tecnologia**, 23.1%
- **consulenza**, 12.8%
- **istruzione**, 12.8%
- **servizi**, 10.3%
- **salute**, 7.7%
- **logistica**, 7.7%
- **pubblica amministrazione**, 5.1%



© Ransomfeed.it - DRM

Gruppi Criminali più attivi in Italia (2024)

Diventano così **quattro i grandi player** criminali del quadrimestre in Italia: oltre a ransomhub, troviamo **lockbit3**, **blackbasta** e **akira**.



Gruppo	Vettori di Attacco	Tecniche/Tattiche (TTP)
Ransomhub 15,52%	Phishing, accesso remoto (RDP/VPN), *exploit di vulnerabilità*	Sfruttamento di credenziali compromesse, cifratura dei dati, *doppia estorsione*
BlackBasta 8,62%	Phishing mirato, accesso remoto (RDP), *exploit di vulnerabilità*	Accesso iniziale via phishing, movimento laterale rapido, esfiltrazione dati, *doppia estorsione*
LockBit3 8,62%	RDP/VPN, phishing, *exploit di vulnerabilità*	Automazione (Cobalt Strike), brute force o credenziali compromesse, movimento laterale, *doppia estorsione*
Akira 8,62%	Phishing, accesso remoto (RDP/VPN) e *sfruttamento di vulnerabilità*	Combinazione di phishing e exploit, movimento laterale, esfiltrazione e cifratura, *doppia estorsione*

© Ransomfeed.it **DRM-Report-Q2-2024.**

Impatti di un attacco

Data rilevamento	Vittima
2025-02-11 07:56:55	I.B.G SPA
2025-02-06 07:59:31	DIEM
2025-02-03 17:58:28	gruppozaccaria.it
2025-02-01 00:56:11	GATTELLI SpA
2025-01-31 02:00:56	akran
2025-01-29 08:42:44	BENASSI IMMOBILIARE SAS DI BENASSI ROBERTO E C.
2025-01-24 14:53:02	ELTEK Group (eltekgroup.com)
2025-01-17 16:43:01	Divimast
2025-01-17 09:18:52	LYNXSPA
2025-01-16 16:50:59	Volt Infrastructure
2025-01-16 06:51:17	bsegroup.it
2025-01-14 16:43:17	Boart & Wire
2025-01-13 20:42:04	Conad (conad.lan)

© Ransomfeed.it **DRM-Report-Q2-2024.**

Costi Diretti

15%

Il **pagamento del riscatto** rappresenta solo una piccola parte, a volte pari ad **appena il 15% dei costi complessivi** associati a un attacco ransomware

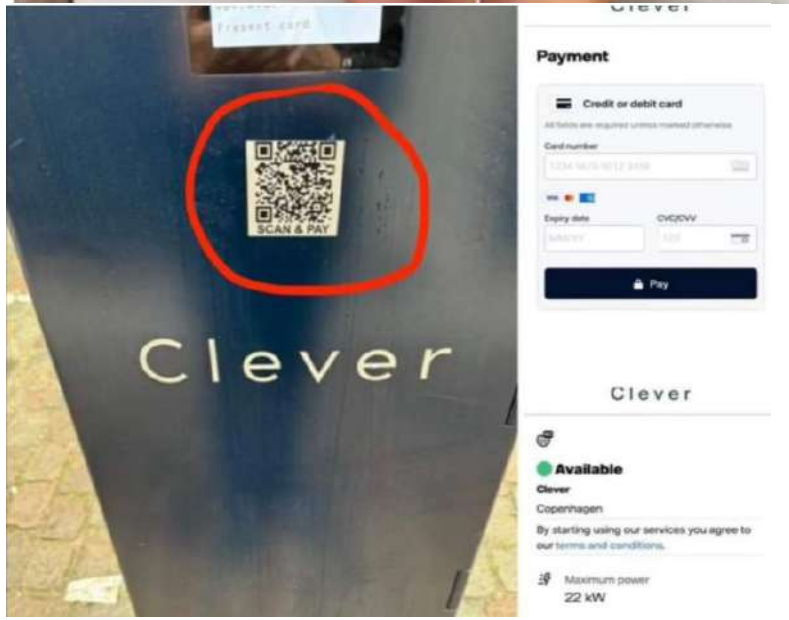
Costi Indiretti

x50

L'azienda media sperimenta un **periodo di interruzione operativa di 22 giorni**. Aggiungendo gli extra costi per l'IR e il ripristino, si arriva ad un **costo medio di cinquanta volte superiore a quello del riscatto**

Fonte: Akamai Ransomware Report EMEA et al.

Il Fenomeno del Quishing



Social Engineering e AI

I criminali hanno utilizzato i messaggi di chat di Microsoft Teams per comunicare con gli utenti, aggiungendoli alle chat con utenti esterni che operano da tenant ID Entra fraudolenti.

Questi utenti esterni, **mascherandosi da personale di supporto, amministratori o help-desk**, utilizzano nomi progettati per ingannare gli utenti, facendoli credere di comunicare con account di help-desk autentici.

Meta multata per 91 milioni di euro! Password in chiaro per uno scandalo globale

La **Commissione irlandese per la protezione dei dati (DPC)** ha multato Meta Platforms Ireland Limited (MPIL) di 91 milioni di euro per aver archiviato le password di centinaia di milioni di utenti in chiaro. Il DPC sta indagando su questo incidente dal 2019.

Social Engineering e AI

Servizio | Ad Hong Kong

Video fake del direttore finanziario: dipendenti spostano 25 milioni ma è una truffa

Un contenuto creato grazie all'intelligenza artificiale trae in inganno alcuni impiegati, così la multinazionale è stata truffata

di Biagio Simonetta

7 febbraio 2024

INTERVISTA

Lucia Aleotti sulla truffa del finto Crosetto: «Nessuno è al sicuro. Brava la mia assistente, ha fiutato subito la frode»

di **Giuliano Ferraino**

CYBERSECURITYITALIA

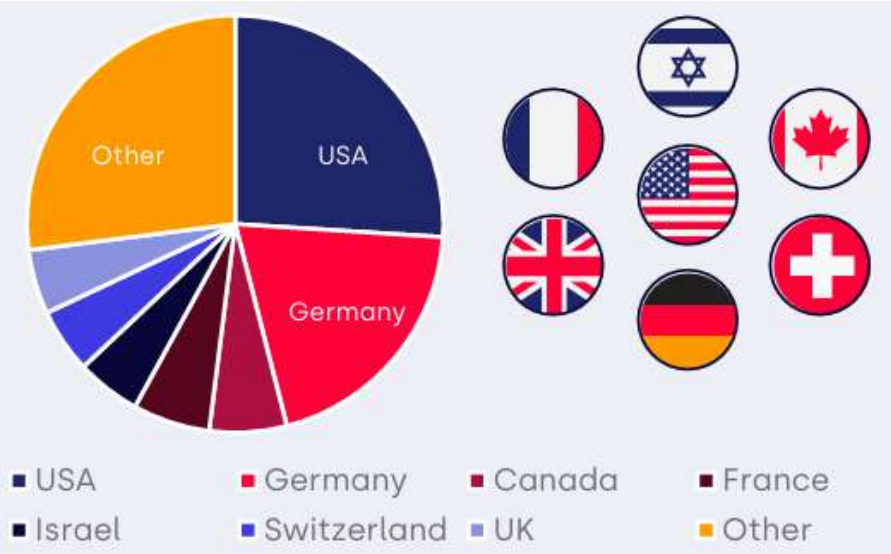
Deepfake del CEO di Ferrari cerca di truffare un manager sfruttando l'intelligenza artificiale

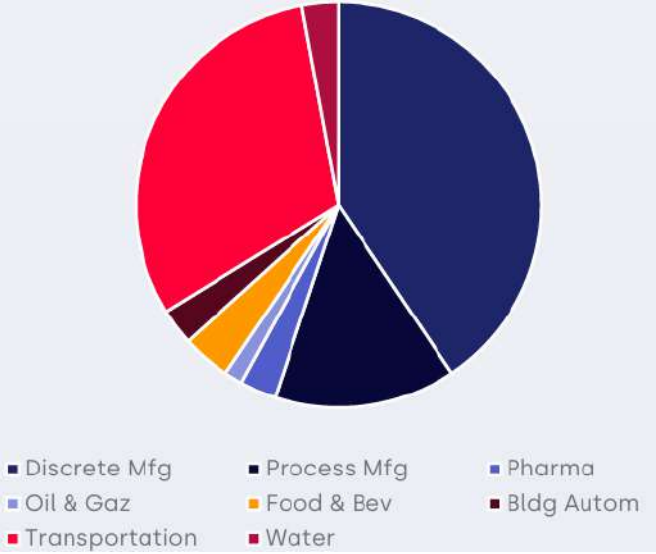
MASSIMO CANORRO — 29 LUGLIO 2024 —

ITALIA, NEWS

2024 - OT Cyberattacks with Physical Consequences

- Sono di natura deliberata, non sono errori o omissioni, non sono guasti di apparecchiature o software
- Portano a conseguenze fisiche, tra cui interruzioni della produzione, danni alle attrezzature, disastri ambientali e lesioni o vittime.
- Hanno avuto luogo nella produzione, nell'automazione degli edifici, nell'industria pesante e nelle infrastrutture industriali critiche, compreso il trasporto di persone e merci





Fonte: Waterfall Security Solutions Ltd
2024 Threat Report

Supply Chain Attack

98% Le società in Europa che hanno avuto un incidente di sicurezza nella loro catena di fornitura nell'ultimo anno

31% La media per le società in UK, Francia, Germania, Italia e Scandinavia

Fonte: SecurityScorecard - Europe's Top 100 Companies Cybersecurity Threat Report 2024

POLITICO

CYBERSECURITY

Middle East pager attacks ignite fear of supply chain warfare

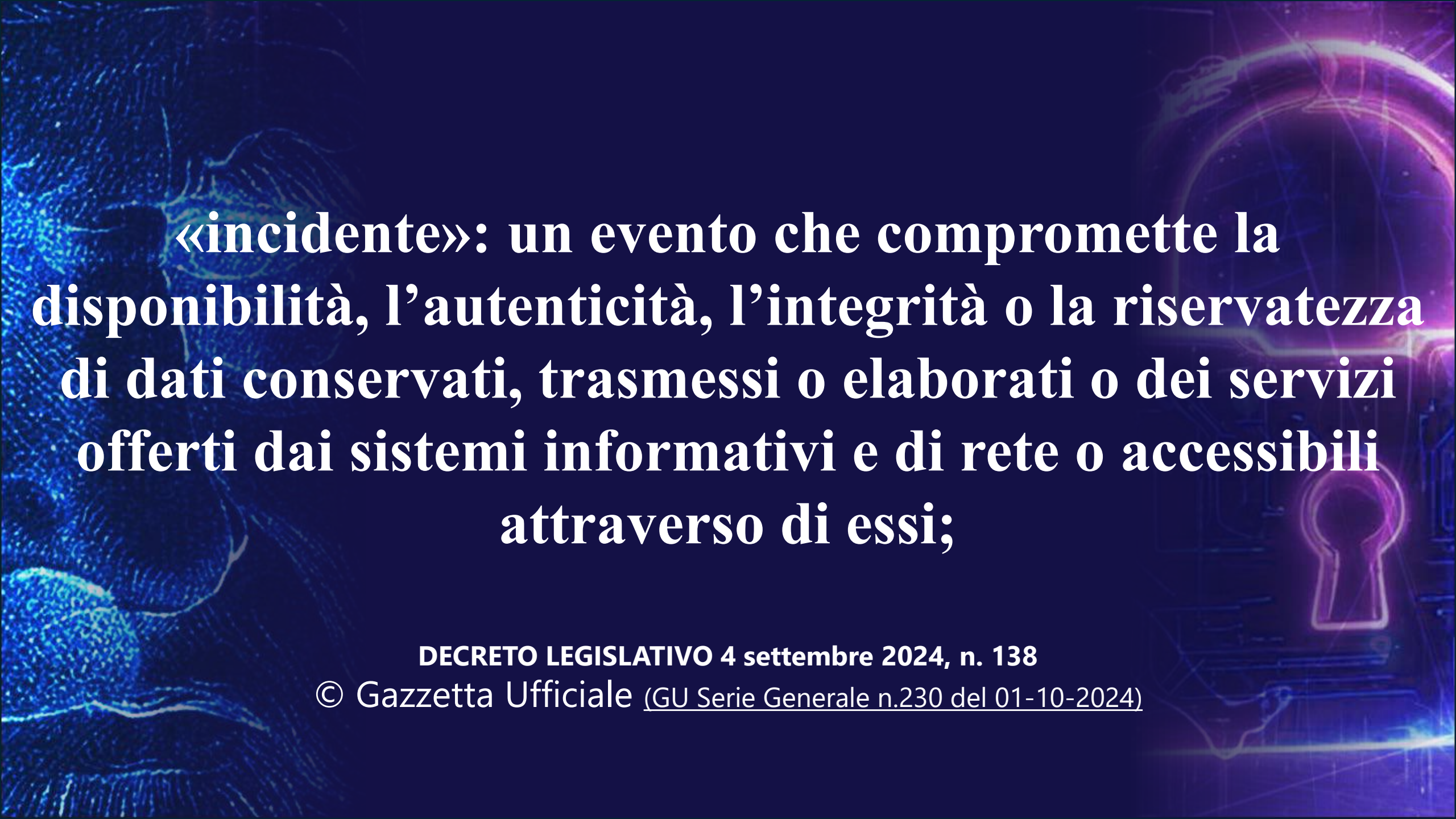
The operations in Lebanon and Syria could spark a global reckoning over vulnerabilities faced by tech companies with global manufacturing operations.

Servizio | Cybersicurezza

Hacker contro fornitore esterno Infocert: rubati dati personali degli utenti. La società: «Dati di Spid, firma e Pec non compromessi»

La società ammette una violazione ai propri database, ma rassicura: nessuna informazione sensibile è messa a rischio

29 dicembre 2024 • articolo aggiornato il 30 dicembre 2024 alle ore 16,30



«incidente»: un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi;

DECRETO LEGISLATIVO 4 settembre 2024, n. 138

© Gazzetta Ufficiale (GU Serie Generale n.230 del 01-10-2024)

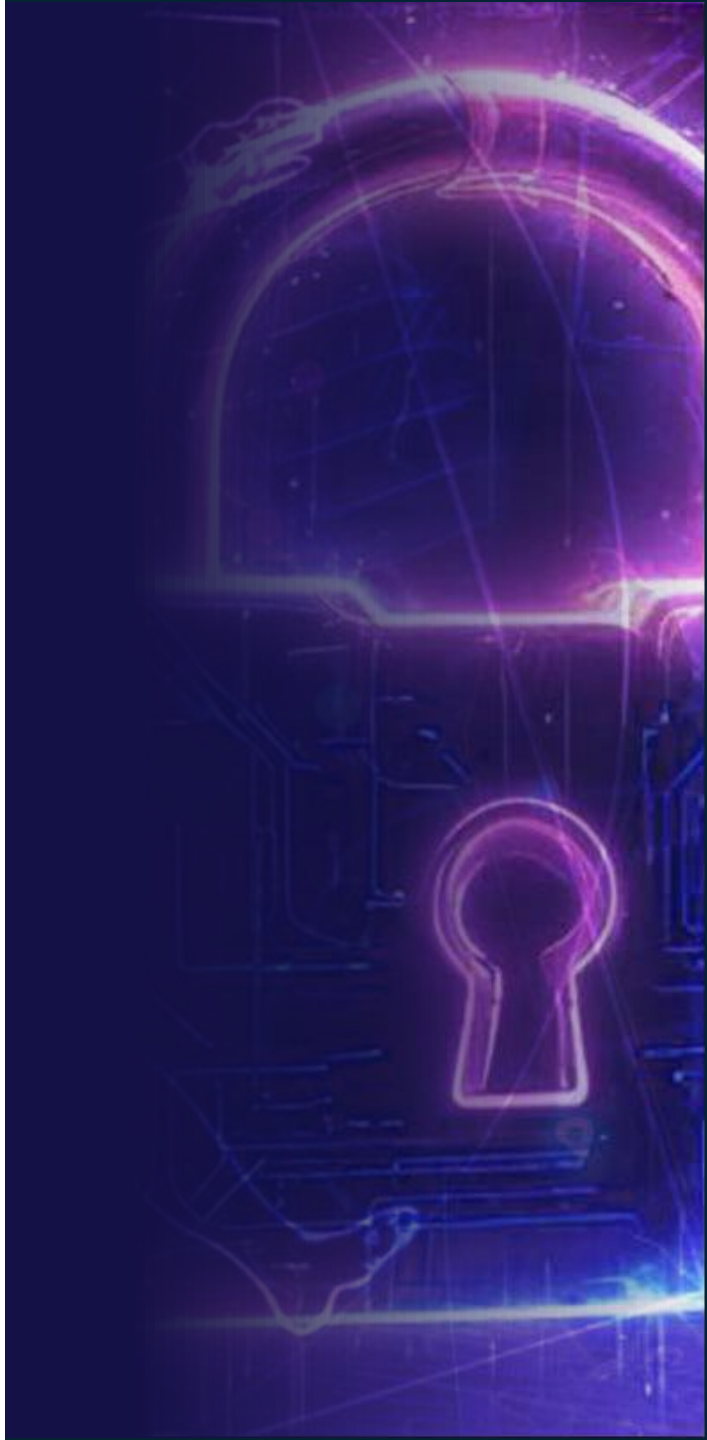

Costo Medio di un Data Breach (Italia)
Cost of a Data Breach Report 2024
© Copyright IBM Corporation
€ 4,58 Milioni

Cost of a data breach by country or region

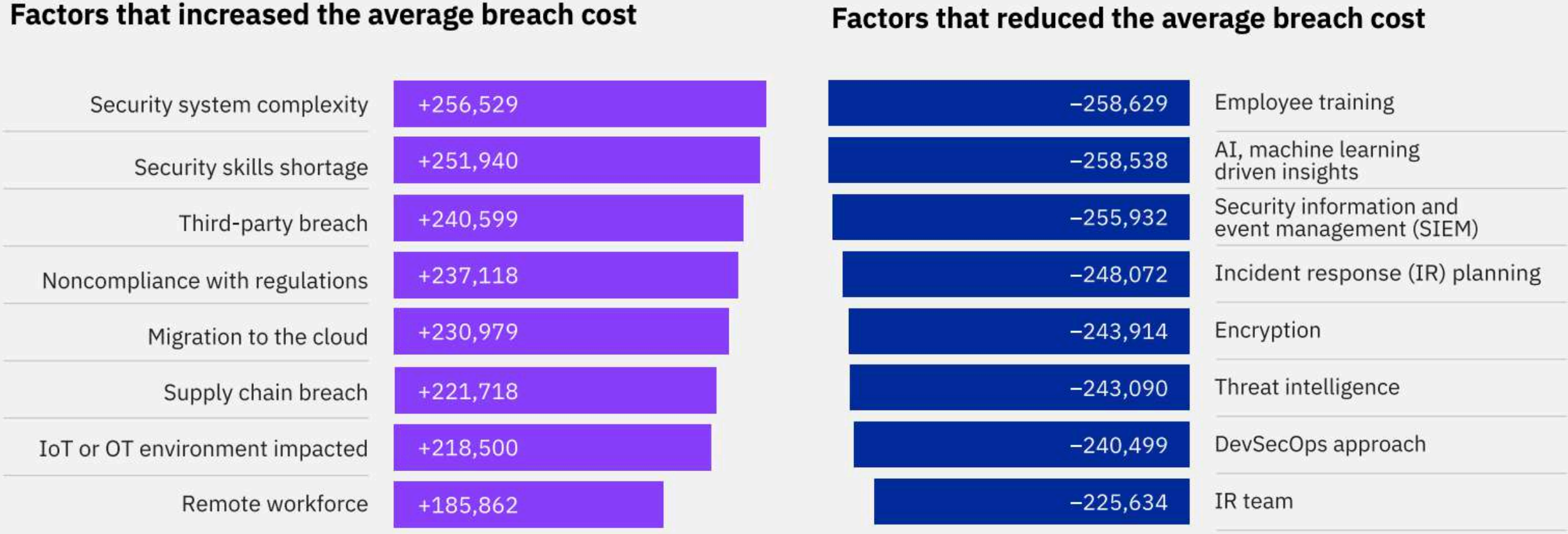
#	Country	2024	2023
1	United States	$9.36	$9.48
2	Middle East	$8.75	$8.07
3	Benelux	$5.90	—
4	Germany	$5.31	$4.67
5	Italy	$4.73	$3.86
6	Canada	$4.66	$5.13
7	United Kingdom	$4.53	$4.21
8	Japan	$4.19	$4.52
9	France	$4.17	$4.08
10	Latin America	$4.16	$3.69
11	South Korea	$3.62	$3.48
12	ASEAN	$3.23	$3.05
13	Australia	$2.78	$2.70
14	South Africa	$2.78	$2.79
15	India	$2.35	$2.18
16	Brazil	$1.36	$1.22

Figure 2A. Measured in USD millions

© Copyright IBM Corporation



Fattori che influenzano il costo di un Data Breach



@IBM Cost of a Data Breach Report 2024

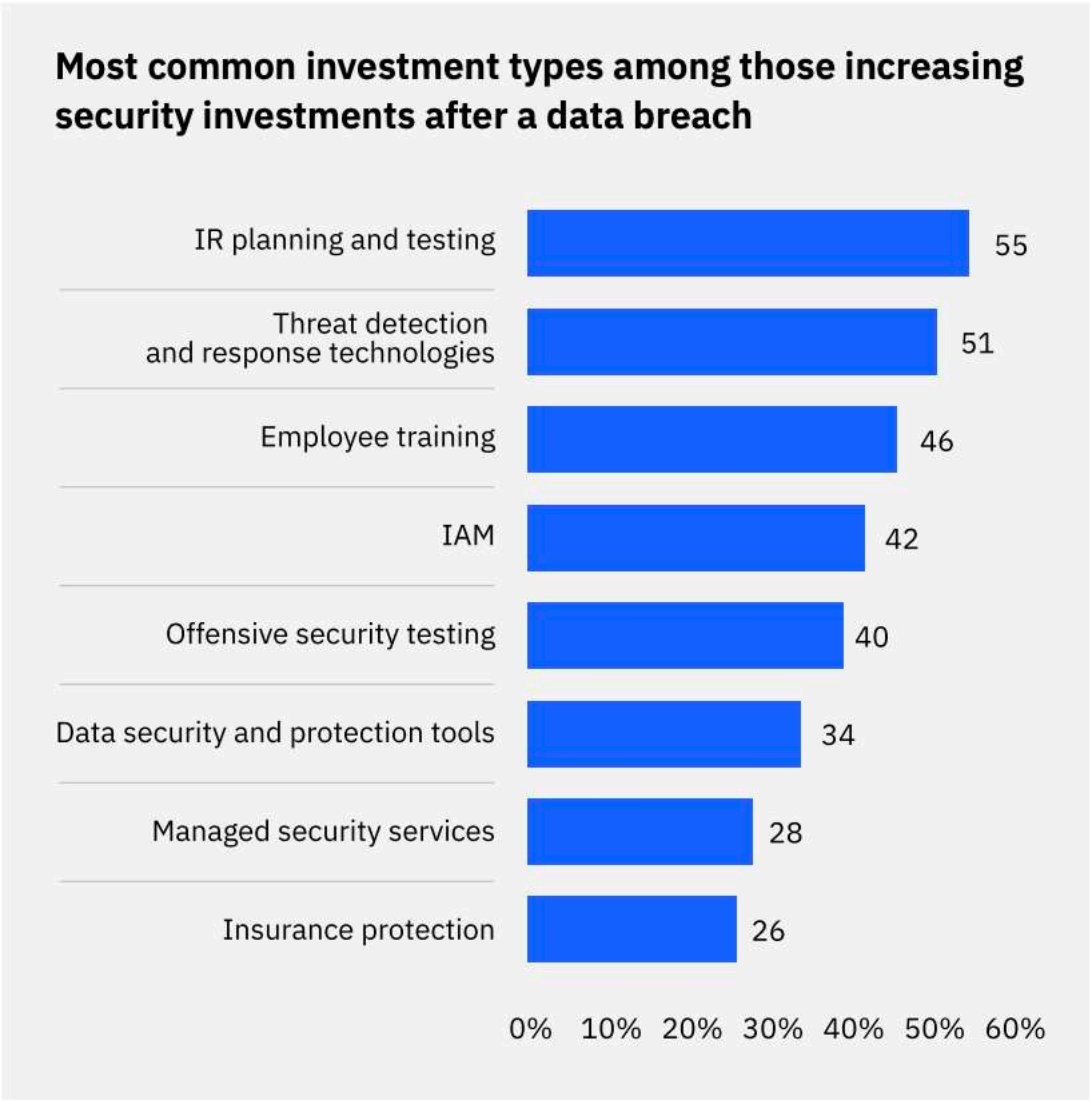


Figure 45. Share among organizations that are increasing security investment; more than 1 response permitted

Figure 25. Cost difference from USD 4.88M breach average; measured in USD

© Copyright IBM Corporation

Fattori che influiranno sulle strategie di CyberResilienza

Geopolitical tensions

Geopolitical tensions are an influence on cyber strategy in nearly 60% of organizations, with one in three CEOs citing cyber espionage and loss of sensitive information/IP as top concerns.

Cybercrime sophistication

72% of respondents say cyber risks have risen in the past year, with cyber-enabled fraud on the rise, an increase in phishing and social engineering attacks and identify theft becoming the top personal cyber risks.

Supply chain interdependencies

With 54% of large organizations citing third-party risk management as a major challenge, supply chain challenges remain a top concern for achieving cyber resilience.

Regulatory requirements

78% of leaders from private organizations feel that cyber and privacy regulations effectively reduce risk in their organization's ecosystems. However, two-thirds of respondents cited the complexity and proliferation of regulatory requirements as a challenge.

AI and emerging tech

66% of respondents believe that AI will affect cybersecurity in the next 12 months, but only 37% have processes in place for safe AI deployment.

Cyber skills gap

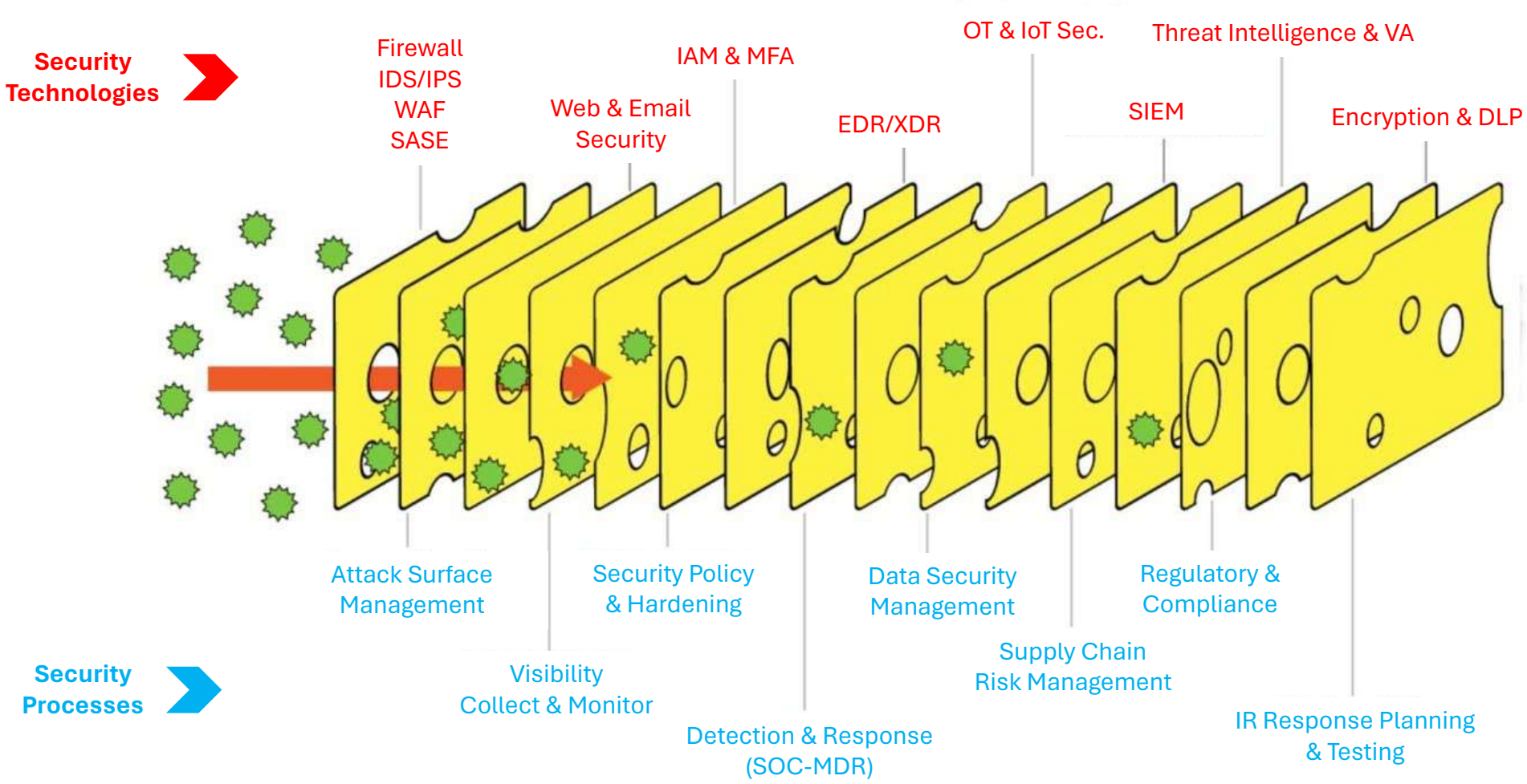
The cyber skills gap has widened since 2024, with two in three organizations reporting moderate-to-critical skills gaps. Only 14% of organizations are confident that they have the people and skills required.

© World Economic Forum **Global Cybersecurity Outlook 2025**

The Swiss Cheese Model

James T. Reason CBE (1 May 1938 – 5 Feb 2025)
professore di psicologia all'Università di Manchester

Swiss Cheese Model in CyberSecurity



HARDENING

Fare Hardening con il CIS

CIS Center for Internet Security | 25 YEARS

CIS is an independent, nonprofit organization with a mission to create confidence in the connected world.

https://www.cisecurity.org/

Secure Specific Platforms

CIS Benchmarks™
100+ vendor-neutral configuration guides

CIS Benchmarks Community
Develop & update secure configuration guides

CIS-CAT®Pro
Assess system conformance to CIS Benchmarks

CIS Hardened Images®
Virtual images hardened to CIS Benchmarks on cloud service provider marketplaces

OTS

CyberSecurity Conference | 13 febbraio 2025

Next Generation SOC-MDR

Augmented SOC-MDR

Endpoint Telemetry (EDR)
(security, ueba, changes)

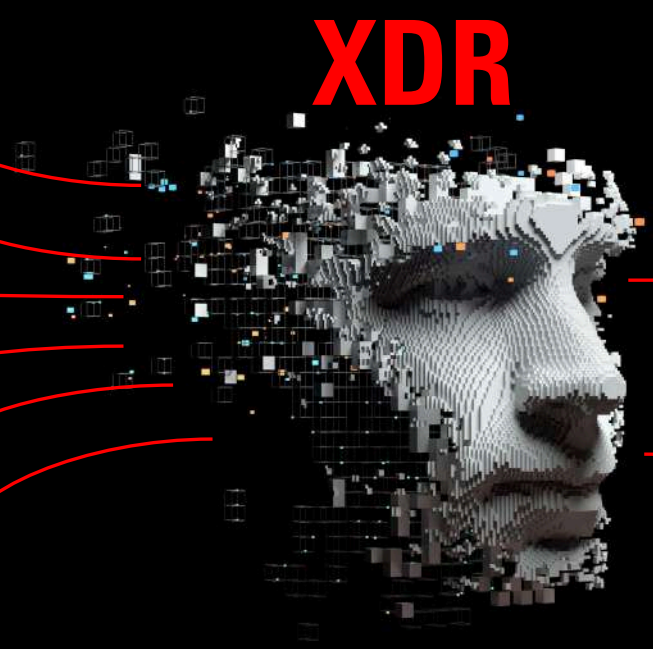
Network Traffic Logs (NDR)
(geoip, threat, DDoS, log)

Threat Intelligence
(news & darkweb info)

Cloud Security Log (CASB)
(security, ueba, changes)

Business Application Log
(security, changes)

Thrird-party Log
(security, changes)



24x7x365 Alert Monitoring

Fast-Triage
(direct contact)

Automated Playbook
(threat containment)

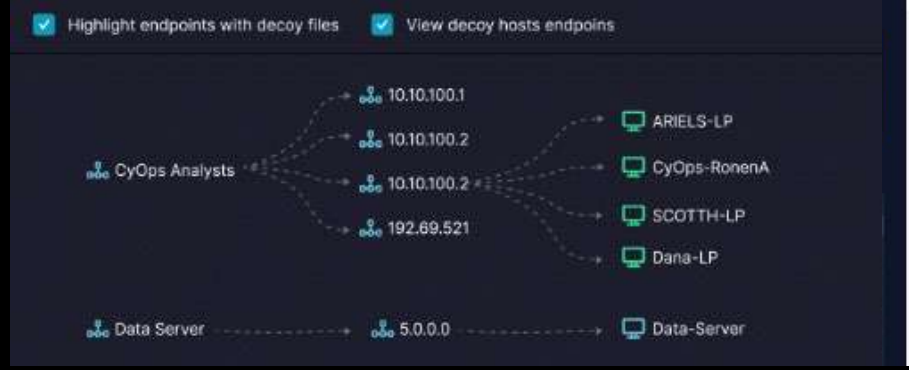
Fast-Response
(threat containment)

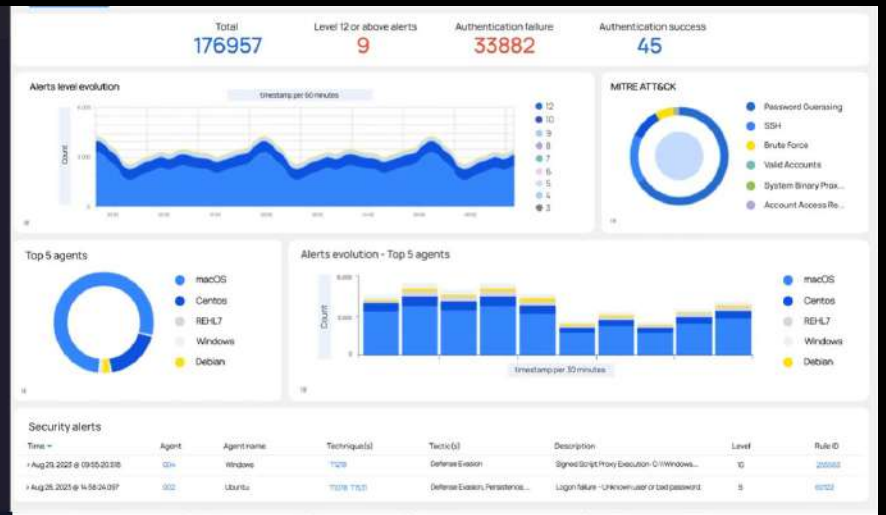
Remediation & Recovery

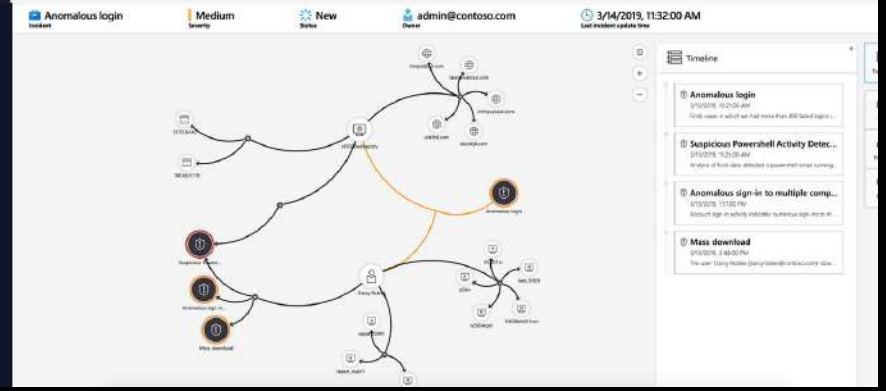
Incident Response
(digital forensic)

Log Feed (input) ----------> Detection & Response (Output)

SOC-MDR as a Service







Vantaggi:

- **Migliore Visibilità**
- **Riduzione dei tempi di Risposta**
- **Elevata Automazione**
- **Migliore Protezione da Attacchi Avanzati e Persistenti**
- **Diminuzione dei carichi di lavoro per il cliente**

CyberSecurity Conference | 13 febbraio 2025

Grazie!!

Uniti per migliorare la CyberSecurity ;)

OTS