Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT
STREAMING EDITION

ASTREA Advanced Security, Training Research, Events Agency

Sessione
Oltre il Siem: come modernizzare il rilevamento e la risposta alle minacce

Alessio Pennasilico, Comitato Scientifico, Clusit
Fabrizio Cassoni, Senior Systems Engineer, Secureworks
Alessandro Stobbia, Pre Sales SMB - Enterprise, Sababa Security

9 novembre 2022 orario 15:00-16:00

Alessio L.R. Pennasilico aka -=mayhem=-

Partner, Practice Leader Information & Cyber Security Advisory Team P4I
Security Evangelist & Ethical Hacker

Membro del Comitato Scientifico Clusit Associazione Italiana per la Sicurezza Informatica

Membro del Comitato Direttivo di Informatici Professionisti AIP Associazione Informatici Professionisti ITCS Italian Computer Society

Vice Presidente del Comitato di Salvaguardia per l'Imparzialità Lloyd's Register LRQA

Membro del Comitato di schema kiwa intertek Total Quality. Assured.

Direttore Scientifico della testata CYBERSECURITY360

Senior Advisor dell'Osservatorio Cyber Security & Data Protection del Politecnico di Milano osservatori.net digital innovation

Fabrizio Cassoni

SENIOR SYSTEMS ENGINEER

Secureworks®

Alessandro Stobbia

PRINCIPAL PRESALES CONSULTANT

Sababa Security

Il problema del Mid-Market

Una tendenza osservata negli ultimi mesi:

- Le attenzioni degli attaccanti sembrano concentrate sulle aziende di medie dimensioni.
- Le richieste economiche di riscatto sono relativamente modeste, ma compensate dalla quantità di attacchi.
- Se un bersaglio si rivela più difficile del previsto, gli attaccanti ne scelgono un altro.
- Fattore economico: volatilità delle Criptovalute?

Il problema del Mid-Market

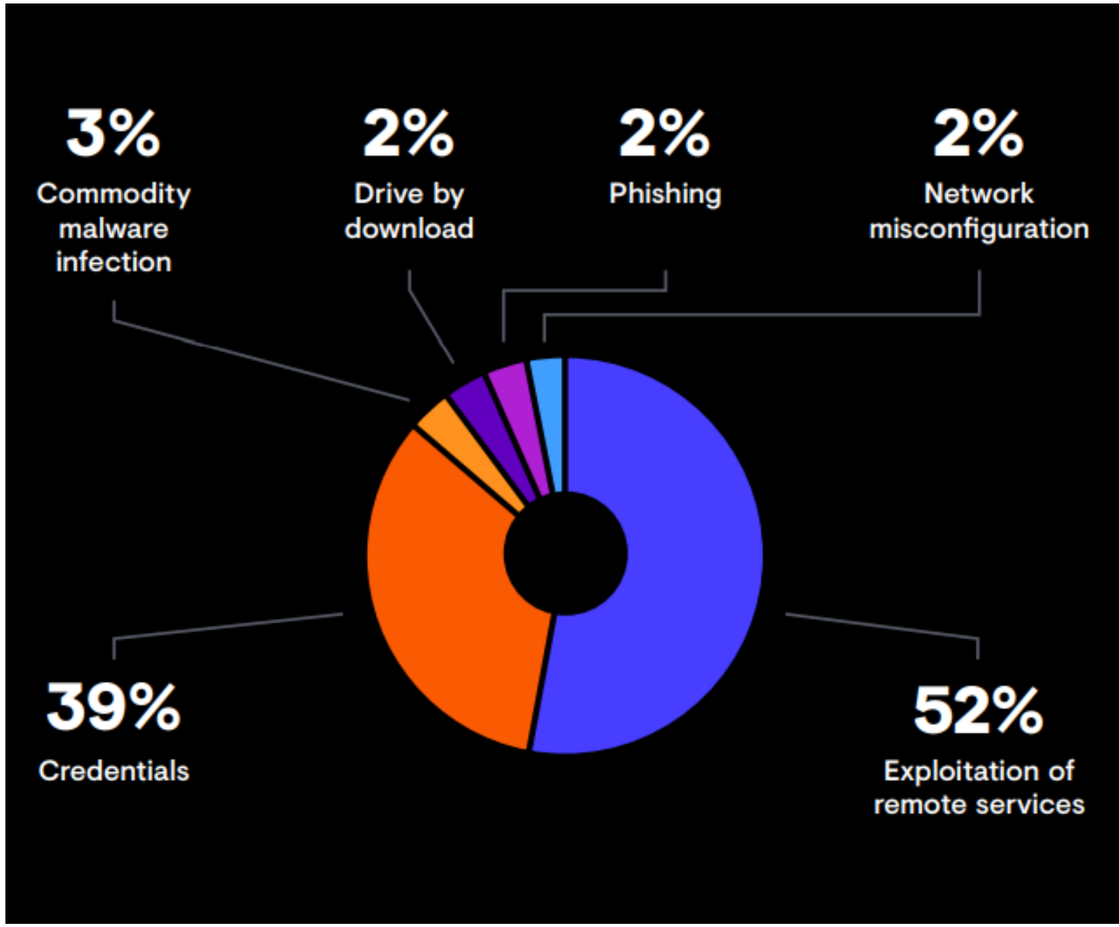
Aziende Mid-Market vs. grandi corporates:

- Non altrettanto sorvegliate
- Spesso mancano profili specializzati nella Cybersecurity
- Maggiormente motivate al pagamento di un riscatto non troppo gravoso
- Molti breach non vengono resi pubblici
- La “barriera linguistica”

Initial Access Vectors: (ossia “come ci riescono?”)

L’importanza dei “Fondamentali”:

- Identificate i vostri asset
- In fase di Remediation, assegnate le priorità in base al profilo di rischio per la vostra attività
- Prevenite tutto il possible, monitorate tutto e rilevate quello che non può essere prevenuto
- Diventate un “bersaglio difficile”



Initial access vectors for ransomware incidents, June 2021 - June 2022.
(Source: Secureworks)

Parliamo di SIEM

Le sfide del SIEM (secondo chi si occupa di SIEM):

- Il Costo – iniziale e di esercizio.
- Necessità di fine-tuning – oppure Alert Fatigue.
- “Per operare un SIEM, occorre essere esperti di SIEM” (M. De Lapalisse, apocrifo) - complessità.
- Eccellente in specifici casi d’utilizzo (es. Compliance), ma difficile da far scalare verso l’alto quando il volume dei dati aumenta.

Secureworks®

Leader nei servizi di Cybersecurity da 22 Anni

5,300

Clienti in
57 Paesi

1,400+

Incarichi di Incident Response all’anno

246

Threat groups monitorati

Forrester
Leader,
Wave 2021 Managed Detection and Response

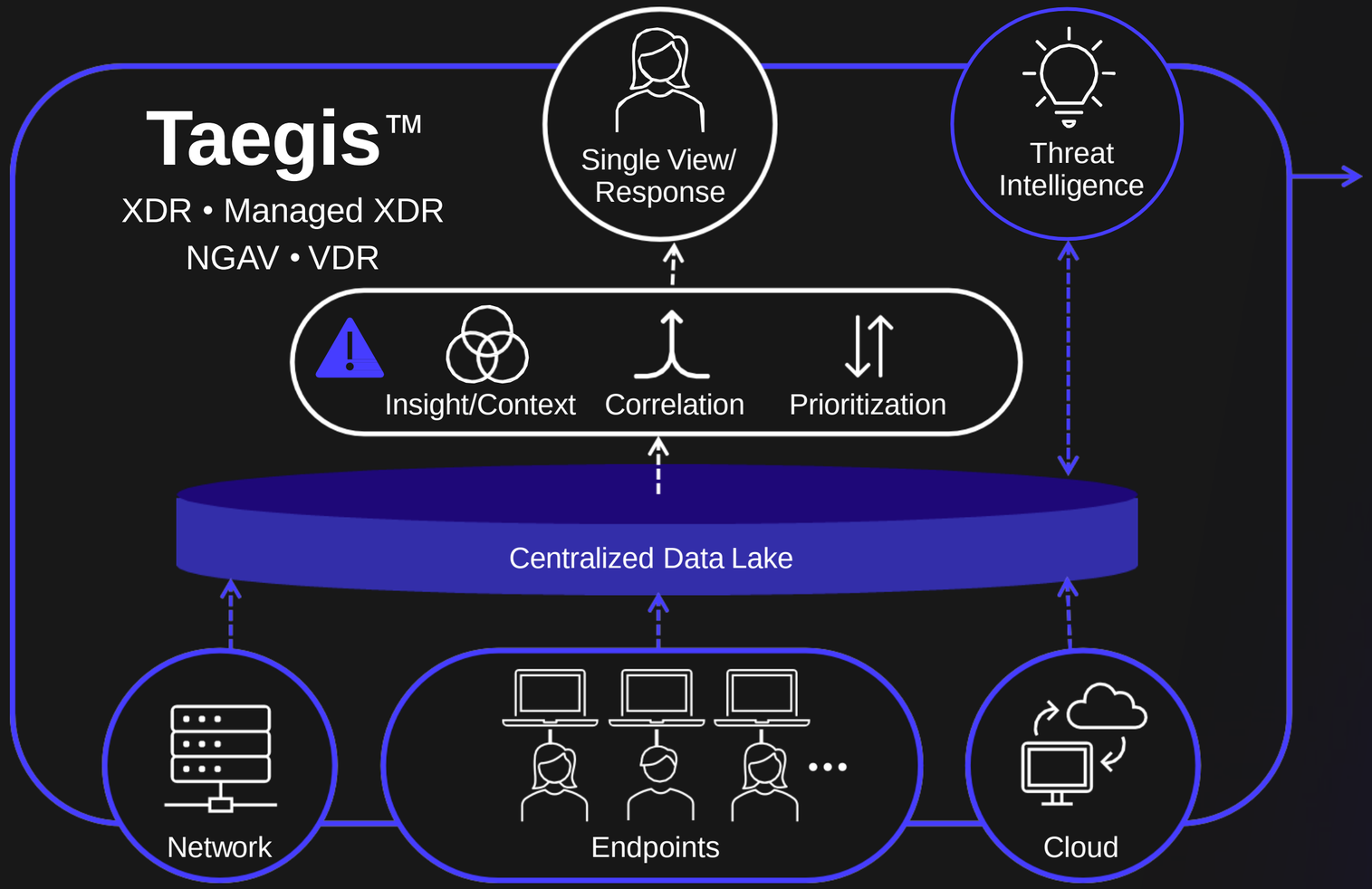
Gartner
11-times Leader,
Magic Quadrant for Managed Security Services, Worldwide

IDC
Leader
- MarketScape: Worldwide MSS ‘20
- MarketScape: U.S. MDR ‘21

Secureworks®

Secureworks Taegis XDR

A constantly evolving, cloud-native, security operations and analytics platform



Full cloud, network and endpoint coverage

- ✓ Breadth and depth of analytics
- ✓ Automated response and remediation
- ✓ Orchestration
- ✓ APIs for easy integration
- ✓ Collaborative platform
- ✓ Real-time access to experts
- ✓ Native telemetry Windows, Mac and Linux
- ✓ Significant ROI

Secureworks®

EXPLORE NEW CORPORATE PERIMETER

Digital transformation and cloud migration

Remote work styles increased the number of cyberattacks

More complex cyberattacks featuring new vectors, e.g. supply chains

Targets are getting smaller

ENDPOINTS
workstations, servers, mobile devices

NETWORK
Firewall, proxy, AD, databases

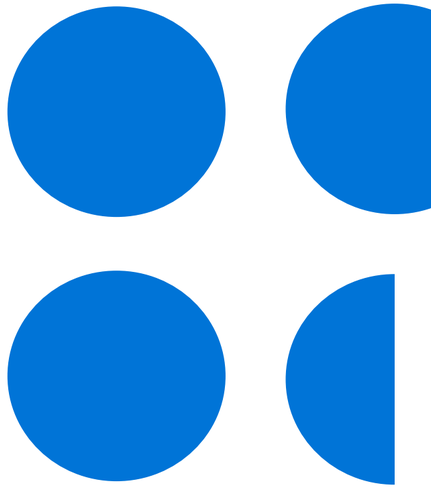
NETWORK
Firewall, proxy, AD, databases

ATTACKS ARE GETTING FASTER

Killchain remains the same, though some alerts cannot wait till Monday, while the others would remain silent for years

Complex cyber-attacks require time-effective detection and accurate response

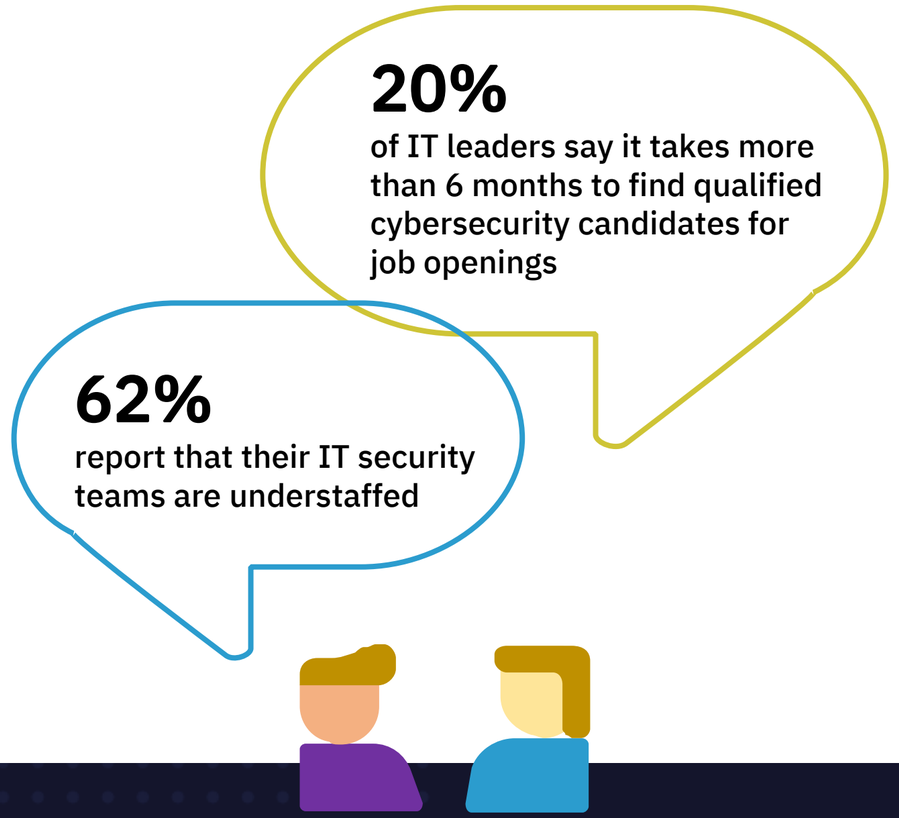
SIEM-based vs. SIEM-free



4.5 DAYS

Is an average dwell time for ransomware actors

CYBERSECURITY RESOURCE AND SKILL SHORTAGE



Cybersecurity professionals are difficult to recruit and even harder to retain

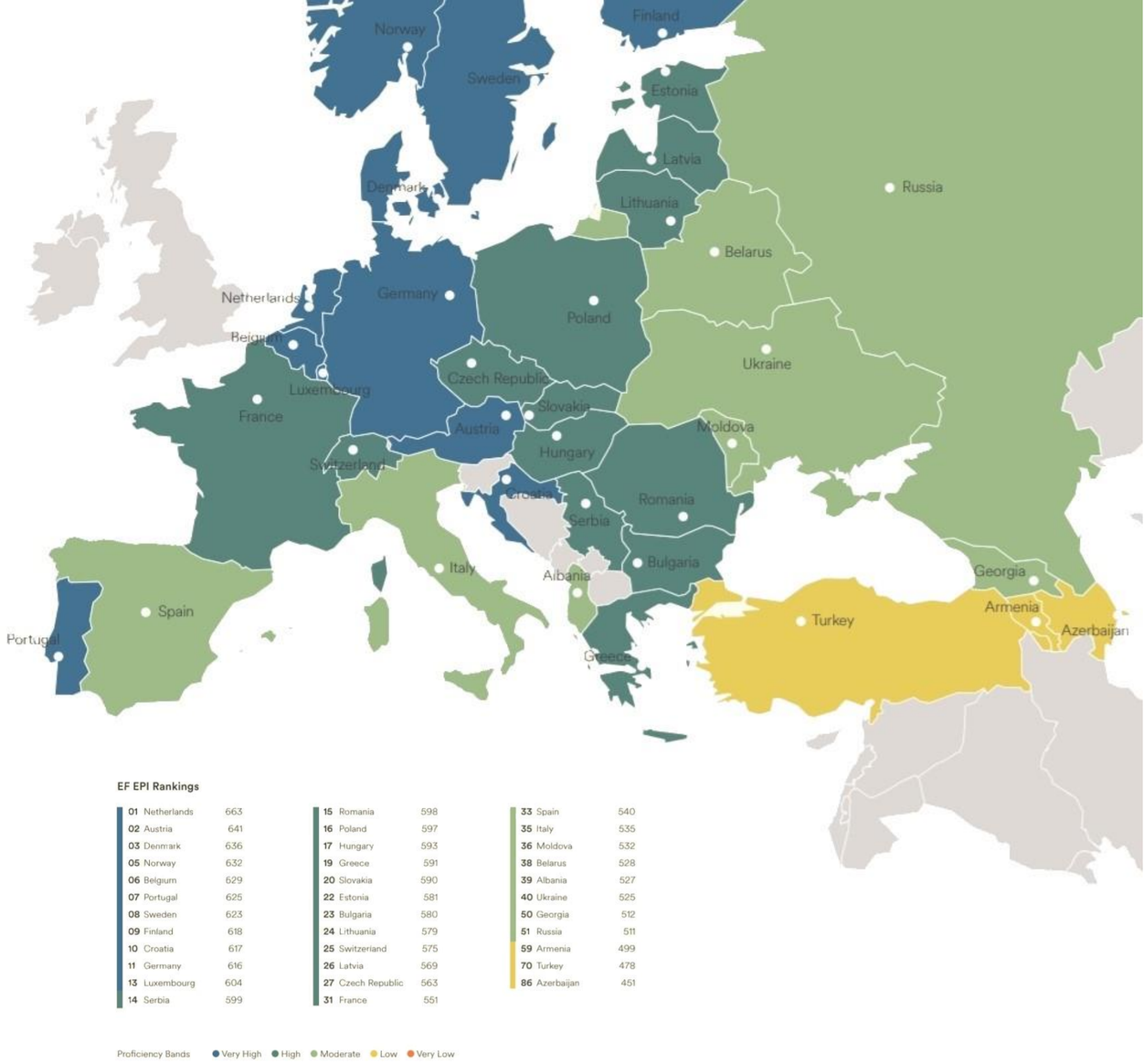
Role diversity when it comes to attack detection, prioritization, response, and investigation

Expectations from IT security teams are changing alongside the transformation of the cybersecurity role for business

WHO MANAGES SECURITY FOR YOU?

You work 8x5, while cyber criminals are ready 24x7

Only 34% of Italians speak English – less than average among the other Europeans

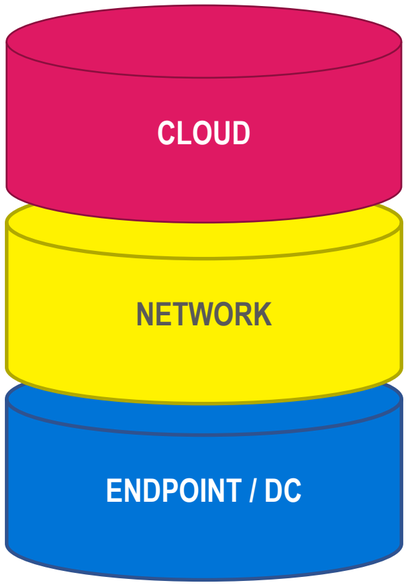


EF EPI Rankings

01	Netherlands	663	15 Romania	598	33 Spain 540
02	Austria	641	16 Poland	597	35 Italy 535
03	Denmark	636	17 Hungary	593	36 Moldova 532
05	Norway	632	19 Greece	591	38 Belarus 528
06	Belgium	629	20 Slovakia	590	39 Albania 527
07	Portugal	625	22 Estonia	581	40 Ukraine 525
08	Sweden	623	23 Bulgaria	580	50 Georgia 512
09	Finland	618	24 Lithuania	579	51 Russia 511
10	Croatia	617	25 Switzerland	575	59 Armenia 499
11	Germany	616	26 Latvia	569	70 Turkey 478
13	Luxembourg	604	27 Czech Republic	563	86 Azerbaijan 451
14	Serbia	599	31 France	551	

Proficiency Bands ● Very High ● High ● Moderate ● Low ● Very Low

THREAT DETECTION: NORTH-SOUTH



Data is analyzed to detect threats across your environment and prioritize alerts

Endpoint Network Cloud Apps Data Email

Vuln. Data Threat Intelligence

THREAT DETECTION: EAST-WEST

* Average for a network of ~1500 nodes

HOW MANAGED XDR WORKS

Info

Less than 20%
likelihood of malicious or suspect activity

Low

20% to 40%
likelihood of malicious or suspect activity

Medium

40% to 60%
likelihood of malicious or suspect activity

Available for review during investigations

High

60% to 80%
likelihood of malicious or suspect activity

Sababa Security

Critical

Greater than 80%
likelihood of malicious or suspect activity

Sababa Security

XDR Service Investigations
Focus on **High** and **Critical** alerts

SOC LEVELS AND ROLES

TIER 1
Monitora l'infrastruttura del cliente

REAL-TIME MONITORING & TRIAGE

VULNERABILITY SCANNING

NETWORK MAPPING

TIER 2
Risponde agli eventi di sicurezza

INCIDENT ANALYSIS

INCIDENT COORDINATION & RESPONSE

COUNTERMEASURE IMPLEMENTATION

FORENSIC ANALYSIS

COMPETENCE CENTER
Ricerca sulle minacce e gestione del SOC

THREAT INTELLIGENCE

TOOL ENGINEERING & DEPLOYMENT

SENSOR & TUNING MAINTENANCE

VULNERABILITY ASSESSMENT & PENETRATION TESTING

SABABA XDR – POWERED BY SECUREWORKS TAEGIS

Licensing

- XDR platform with managed cyber triage for corporate endpoints, IT network and cloud assets
- Security Monitoring 24x7 
- Direct contact for security emergences and 24x7 automated critical event notification
- 1- and 3-years licenses
- Constant update and finetuning of the montiored assets
- Adjustable RBAC for MSSP and end-customers
- Data is hosted in the EU or US with the respect to GDPR
- Monthly reports on security events, performance and recommendastions

Add-Ons

- Incident Response packages with various SLAs
- Tailored Threat Intelligence
- NGAV – VDR for antimalware capabilities
- Virtual CISO to drive cybersecurity projects

Taegis™ Powered by Secureworks | Sababa Security

Take no time to detect even complex cyber-attacks across corporate endpoints, network and cloud assets with a recognized and rewarded technology

Onboard a multi-level SOC team with a wide range of security skills – supporting you 24x7 in Italian

Scale security with the changing objectives of your business, integrating modular technologies with no additional agents, introducing Virtual CISO or preparing an Incident Response plan

Q&A