SECURITY SUMMIT

Security Summit

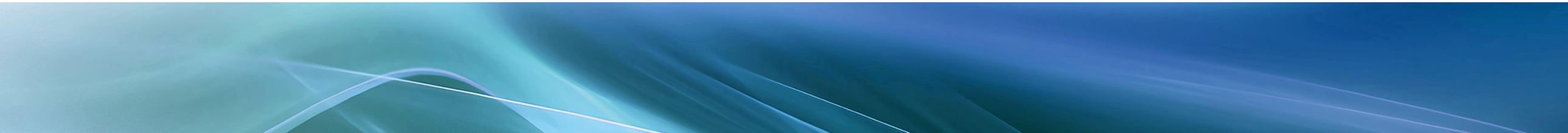
Napoli 23 settembre 2025

Clusit 25th 2000-2025

ASTREA

Cybersicurezza 2025: tra complessità digitale, intelligenza artificiale e resilienza aziendale

Relatore | Alessio Pennasilico – Comitato Scientifico Clusit
Relatore | Leonardo Tonelli – Senior Enterprise Account Executive - Sophos
Relatore | Giovanni Giovannelli – Senior Sales Engineer - Sophos



Alessio Pennasilico

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

Membro del Comitato Scientifico Clusit

Membro del Comitato Direttivo di Informatici Professionisti AIP ITCS

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

Membro del Comitato di schema kiwa intertek

Direttore Scientifico della testata CYBERSECURITY360

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

Leonardo Tonelli
Senior Enterprise Account Executive **- Sophos**

Quasi 40 anni di esperienza in aziende multinazionali operando nei settori ICT, Networking e Security (Honeywell/Bull, Compuware, Cisco, Checkpoint, Sophos).

Ho sviluppato un approccio consulenziale per supportare i Clienti nella scelta di servizi e soluzioni di Cybersecurity in grado di sviluppare e proteggere in maniera innovativa il Business Aziendale.

Giovanni Giovannelli
Senior Sales Engineer **- Sophos**

Professionista con 20 anni di esperienza nel settore della Sicurezza delle Informazioni e delle Reti, con competenze sia tecniche che commerciali. Da sempre appassionato di cybersecurity, mi dedico allo studio continuo delle evoluzioni tecnologiche e delle tendenze di mercato.

Il mio obiettivo è essere un **Trusted Advisor** per clienti, prospect e partner, comprendendo a fondo le loro esigenze per proporre soluzioni efficaci e personalizzate. Ho una forte attitudine alla presentazione e alla formazione, e riesco a instaurare e mantenere **relazioni solide e durature** con i clienti.

Mi piace anticipare i bisogni del mercato e mi impegno costantemente per rimanere aggiornato sulle nuove tecnologie, con un approccio proattivo e orientato al valore.

Causa Tecnica Principale degli Attacchi

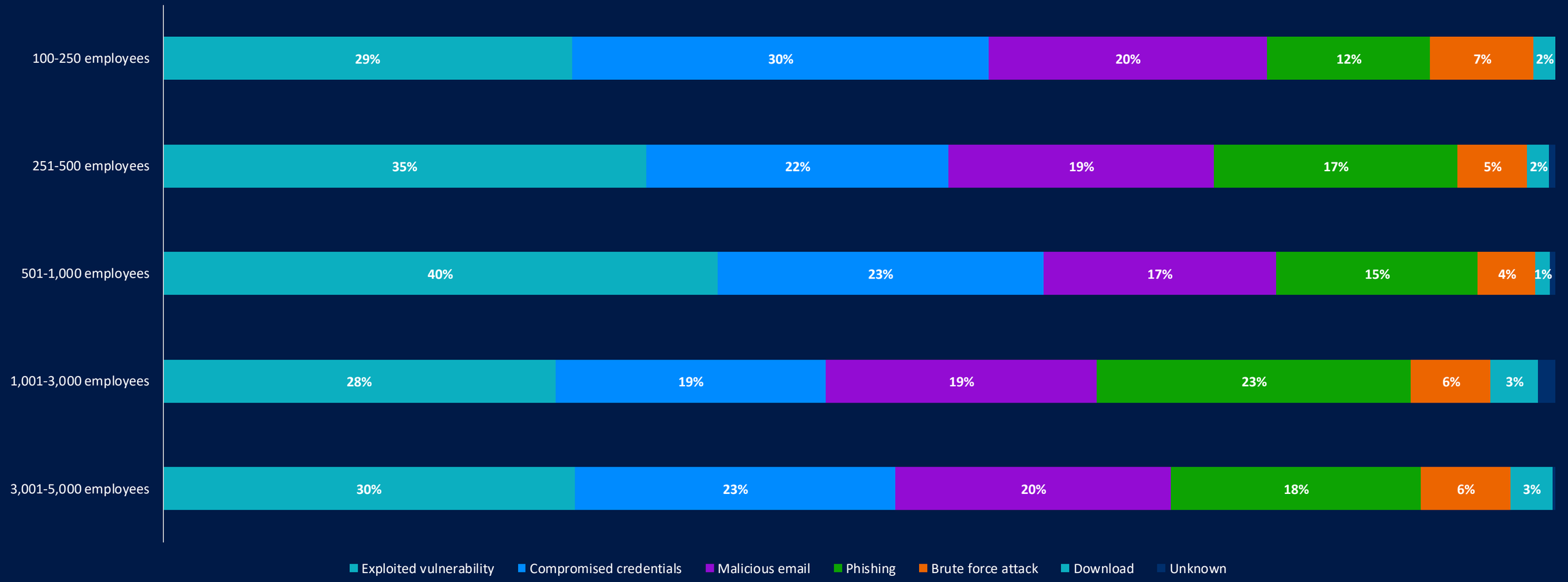
Per il terzo anno consecutivo, le vulnerabilità sfruttate sono la causa principale degli attacchi ransomware

Conosci la causa principale dell'attacco ransomware che la tua organizzazione ha subito nell'ultimo anno? Sì. n=3.400 (2025), 2.974 (2024), 1974 (2023).

SOPHOS

Causa Tecnica degli Attacchi | Dimensioni dell’Azienda

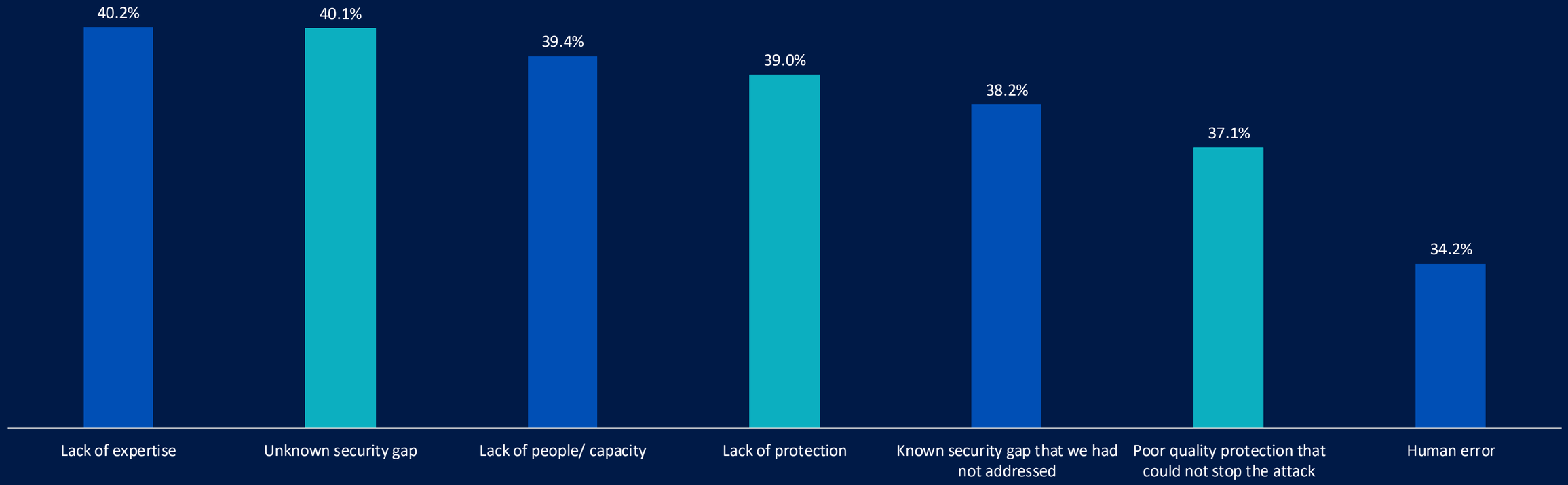
La causa principale percepita varia in base alle dimensioni dell'organizzazione, anche se le vulnerabilità sfruttate sono la causa più comune per tutti i segmenti, ad eccezione dei 100-250 dipendenti, dove le credenziali compromesse sono in cima alla lista.



Conosci la causa principale dell'attacco ransomware che la tua organizzazione ha subito nell'ultimo anno? Sì. n=3.400 (2025)

Causa Principale Operativa degli Attacchi

La mancanza di competenze (ovvero non possedere le capacità o le conoscenze per rilevare e fermare un attacco) è il motivo più comune per cui le organizzazioni ne sono state vittime, seguito da vicino da un gap di sicurezza di cui l'organizzazione non era a conoscenza.

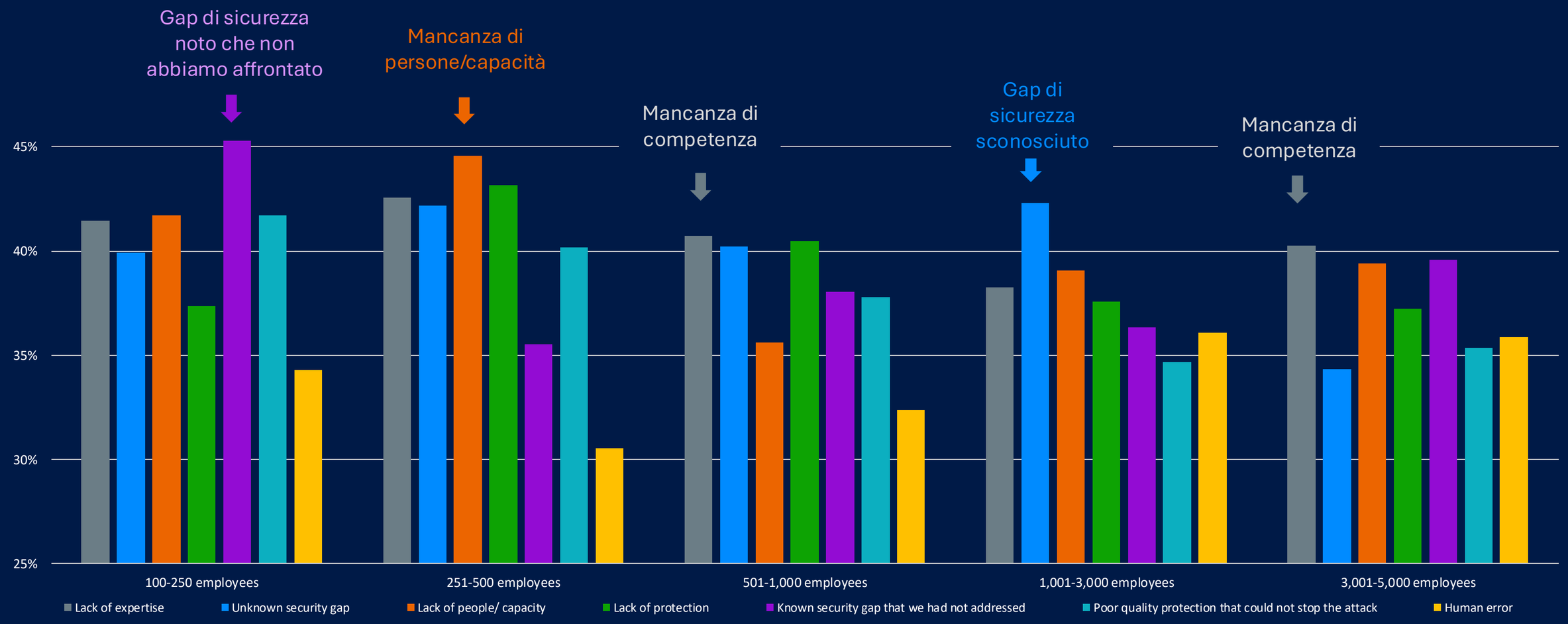


Perché pensi che la tua organizzazione sia stata vittima dell'attacco ransomware? n=3.400

SOPHOS

Causa Operativa degli Attacchi | Dimensioni dell’Azienda

Il motivo organizzativo più comune per cui le aziende sono state vittime di ransomware varia in base alle dimensioni dell'organizzazione.



Perché pensi che la tua organizzazione sia stata vittima dell'attacco ransomware? n=3.400. Suddivisi per dimensione organizzativa (numero di dipendenti)

SOPHOS

Evoluzione normativa

- Queste normative e standard presentano dei fattori comuni come la conduzione di valutazioni del rischio, la formazione interna in materia di cybersecurity, la gestione degli incidenti, la business continuity e la supervisione dei fornitori.

MDR basato sulla più grande piattaforma aperta AI-native

La potenza della piattaforma su larga scala

Il nostro esclusivo approccio **incentrato sulla prevenzione** riduce le violazioni e migliora i risultati di rilevamento e risposta

Gli insegnamenti tratti dalle indagini e dagli attacchi bloccati da Sophos MDR **apportano miglioramenti** alla protezione proattiva

SOPHOS

VISIONE AI

L’AI sfruttata per l'intero ciclo di vita della prevenzione, del rilevamento e della risposta alle minacce per garantire l'efficienza, insieme all'esperienza umana per fronteggiare gli attaccanti.

Il social engineering potenziato dall'IA

DEEP FAKE

- Creazione di deepfake audio e video per truffe, ricatti o disinformazione.

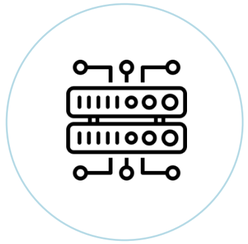
PHISHING

- Generazione di e-mail di phishing altamente credibili e personalizzate grazie all'analisi di dati e testi.

SOCIAL ENGINEERING

- Raccolta e analisi di informazioni dai social network per costruire attacchi mirati (es. spear phishing, social engineering).

L’IA al servizio dei cyber criminali

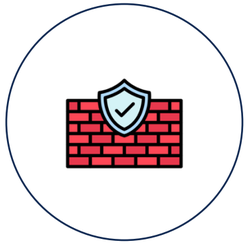


IDENTIFICAZIONE VULNERABILUTA’

- Sfruttamento dell’IA per identificare sistemi vulnerabili e punti deboli nelle infrastrutture informatiche.

GENERAZIONE MALWARE

- Generazione e perfezionamento di malware tramite algoritmi di apprendimento automatico.



ELUSIONE

- Automatizzazione delle tecniche di evasione delle misure di sicurezza (es. elusione di antivirus e firewall).

RICERCA & SVILUPPO

- Ricerca e sviluppo di nuovi metodi d’attacco per compromettere sistemi e reti.

Modelli Comuni di AI

TIPOLOGIA

Deep Learning AI

Utilizza reti neurali artificiali per riconoscere modelli e prendere decisioni in un modo che imita il cervello umano.

Generative AI

Crea (genera) contenuti nuovi in base alla struttura e al modello dei dati esistenti.

DIMENSIONE

Massive AI Models

Assiste gli utenti nell'esecuzione di un'ampia gamma di attività. Vengono addestrati su grandi quantità di dati disponibili pubblicamente.

Small AI Models

Progettati e realizzati per casi d'uso specifici e mirati. In genere vengono addestrati su set di dati proprietari

Gartner®

By 2028, multiagent AI in threat detection and incident response will rise from 5% to 70% of AI implementations **to primarily augment, not replace staff.**

—Gartner, "How to Evaluate Cybersecurity AI Assistants," October 2024

L'evoluzione degli Agenti AI

AIUTANTI CONTESTUALI

Utilizzano alberi decisionali rudimentali e un semplice riconoscimento delle parole chiave per generare script

AGENTI BASATI SULL'APPRENDIMENTO

Sono in grado di comprendere il linguaggio umano naturale e di elaborare script

AGENTI CONVERSAZIONALI

Utilizzano tecniche avanzate di natural language processing (NLP) e machine learning (ML); sanno imparare dalle interazioni passate

AGENTI DI AI GENERATIVA

Utilizzano i trasformatori per combinare set di dati complessi, consentendo di comprendere il contesto e generare contenuti complessi

AGENTI AUTONOMI E ORIENTATI ALL'OBIETTIVO ("AGENTIC")

Modelli di ML multipli che lavorano insieme, per risolvere problemi in tempo reale; è in grado di anticipare i bisogni, ricercare soluzioni ed eseguire azioni prima che gli venga chiesto

#1 vantaggio ricercato nella GenAI, per dimensione dell'azienda

NUMERO DI DIPENDENTI

50-99	100-249	249-499	500-999	1.000-1.999	2.000-3.000
Riduzione del **burnout** dei dipendenti	Migliore ritorno sulla spesa per la cybersecurity (**ROI**)	Maggiore **protezione** dalle minacce informatiche	Maggiore **efficienza** e impatto dell'analista IT	Maggiore **protezione** dalle minacce informatiche	Maggiore **protezione** dalle minacce informatiche
28%	**30%**	**23%**	**30%**	**30%**	**24%**

—Sophos, "Beyond the hype: The business reality of AI for cybersecurity," January 2025

Difesa Basata su AI

Mitigare il rischio

Esempio:
Sophos Managed Risk sfrutta un modello di intelligenza artificiale VPR (Vulnerability Priority Rating) che predice la probabilità di sfruttamento di CVE entro 28 giorni

Bloccare le minacce

Esempio:
I modelli di protezione web in Sophos Endpoint e Sophos Firewall rilevano URL dannosi, siti Web di phishing e altre minacce basate sul Web

Indagare le minacce

Esempio:
Gli LLM Explainer, gli incident summaries in Taegis XDR e Taegis MDR aiutano gli analisti a interpretare più rapidamente le informazioni complesse

Rispondere agli attacchi

Esempio:
AI Case Summary in Sophos XDR fornisce una panoramica di facile comprensione dei rilevamenti e dei passaggi successivi consigliati, accelerando la risposta

SOPHOS

Difesa Basata su AI

Mitigare il rischio

Esempio:
Sophos Managed Risk sfrutta un modello di intelligenza artificiale VPR (Vulnerability Priority Rating) che predice la probabilità di sfruttamento di CVE entro 28 giorni

Bloccare le minacce

Esempio:
I modelli di protezione web in Sophos Endpoint e Sophos Firewall rilevano URL dannosi, siti Web di phishing e altre minacce basate sul Web

Indagare le minacce

Esempio:
Gli LLM Explainer, gli incident summaries in Taegis XDR e Taegis MDR aiutano gli analisti a interpretare più rapidamente le informazioni complesse

Rispondere agli attacchi

Esempio:
AI Case Summary in Sophos XDR fornisce una panoramica di facile comprensione dei rilevamenti e dei passaggi successivi consigliati, accelerando la risposta

Difesa Basata su AI

Mitigare il rischio

Esempio:
Sophos Managed Risk sfrutta un modello di intelligenza artificiale VPR (Vulnerability Priority Rating) che predice la probabilità di sfruttamento di CVE entro 28 giorni

Bloccare le minacce

Esempio:
I modelli di protezione web in Sophos Endpoint e Sophos Firewall rilevano URL dannosi, siti Web di phishing e altre minacce basate sul Web

Indagare le minacce

Esempio:
Gli LLM Explainer, gli incident summaries in Taegis XDR e Taegis MDR aiutano gli analisti a interpretare più rapidamente le informazioni complesse

Rispondere agli attacchi

Esempio:
AI Case Summary in Sophos XDR fornisce una panoramica di facile comprensione dei rilevamenti e dei passaggi successivi consigliati, accelerando la risposta

SOPHOS

Difesa Basata su AI

Mitigare il rischio

Esempio:
Sophos Managed Risk sfrutta un modello di intelligenza artificiale VPR (Vulnerability Priority Rating) che predice la probabilità di sfruttamento di CVE entro 28 giorni

Bloccare le minacce

Esempio:
I modelli di protezione web in Sophos Endpoint e Sophos Firewall rilevano URL dannosi, siti Web di phishing e altre minacce basate sul Web

Indagare le minacce

Esempio:
Gli LLM Explainer, gli incident summaries in Taegis XDR e Taegis MDR aiutano gli analisti a interpretare più rapidamente le informazioni complesse

Rispondere agli attacchi

Esempio:
AI Case Summary in Sophos XDR fornisce una panoramica di facile comprensione dei rilevamenti e dei passaggi successivi consigliati, accelerando la risposta

SOPHOS

Difesa Basata su AI

Mitigare il rischio

Esempio:
Sophos Managed Risk sfrutta un modello di intelligenza artificiale VPR (Vulnerability Priority Rating) che predice la probabilità di sfruttamento di CVE entro 28 giorni

Bloccare le minacce

Esempio:
I modelli di protezione web in Sophos Endpoint e Sophos Firewall rilevano URL dannosi, siti Web di phishing e altre minacce basate sul Web

Indagare le minacce

Esempio:
Gli LLM Explainer, gli incident summaries in Taegis XDR e Taegis MDR aiutano gli analisti a interpretare più rapidamente le informazioni complesse

Rispondere agli attacchi

Esempio:
AI Case Summary in Sophos XDR fornisce una panoramica di facile comprensione dei rilevamenti e dei passaggi successivi consigliati, accelerando la risposta

L’AI in Ogni Punto della Difesa

MITIGARE IL RISCHIO
Ridurre l'esposizione

TAEGIS XDR, TAEGIS MDR
Il motore di definizione delle priorità in attesa di brevetto fornisce agli analisti un elenco di avvisi con priorità per elevare visivamente le minacce

SOPHOS MANAGED RISK
Sfrutta il modello di intelligenza artificiale VPR (Tenable Vulnerability Priority Rating) per predire la probabilità di sfruttamento CVE entro 28 giorni

BLOCCARE LE MINACCE
Impedire l'esecuzione degli attacchi

SOPHOS ENDPOINT
Modelli AI multipli proteggono da attacchi noti e nuovi, comprese le minacce nelle soluzioni MS Office e nei PDF

SOPHOS FIREWALL
Protezione dalle minacce zero-day basata sull’AI tramite SophosLabs Intelix

SOPHOS ENDPOINT & FIREWALL
I modelli di protezione Web rilevano URL dannosi, siti Web di phishing e altre minacce basate sul Web

SOPHOS EMAIL
I modelli NLP basati sul deep learning identificano i tentativi di impersonificazione

SOPHOS MOBILE
Il modello Android DL viene addestrato su dati Android proprietari per rilevare malware specifici di Android

INDAGARE SULLE MINACCE
Identificare le attività dannose

SOPHOS XDR, SOPHOS MDR
AI Assistant guida i professionisti della sicurezza di tutti i livelli di competenza in ogni fase dell’indagine

TAEGIS XDR, TAEGIS MDR
GenAI viene utilizzato per i riepiloghi delle indagini di sicurezza, inclusi i dettagli relativi al contesto e agli avvisi

SOPHOS MDR
Il triage dei casi basato sull’AI accelera le indagini MDR ed elimina i casi duplicati

TAEGIS XDR, TAEGIS MDR
I riepiloghi degli incidenti spiegano le complesse attività command-line, la logica di rilevamento e le suddivisioni dettagliate degli avvisi

SOPHOS XDR, SOPHOS MDR
AI Search consente agli analisti di utilizzare il linguaggio naturale per la ricerca dei dati

RISPONDERE AGLI ATTACCHI
Neutralizzare le minacce

TAEGIS XDR, TAEGIS MDR
Le azioni di risposta automatizzate e i flussi di lavoro con funzionalità SOAR integrate accelerano la mitigazione

SOPHOS XDR, SOPHOS MDR
AI Assistant fornisce consigli su come rispondere agli attacchi, espellendo gli avversari

SOPHOS ENDPOINT
Pulisce automaticamente i dispositivi infetti

SOPHOS FIREWALL
Isola automaticamente gli endpoint infetti, anche da altri dispositivi sullo stesso switch

ACTIVE THREAT RESPONSE
Risponde istantaneamente alle nuove informazioni sulle minacce, provenienti da analisti e altre fonti

Esempi di AI nei prodotti e nei servizi Sophos

SOPHOS

Consigli

Prevenzione

Affrontare le cause tecniche e operative:

- **La Gestione del Rischio a**iuta a ridurre l'esposizione alle vulnerabilità.
- **MFA e ZTNA** aiutano a mitigare l'impatto del furto di credenziali.
- Investire in **soluzioni di sicurezza e-mail basate sull'AI.**
- **MSP e provider MDR** possono aggiungere competenze e capacità in materia di minacce.
- Continuare a fornire **corsi di formazione sulla sicurezza** agli utenti.

Protezione

Gli endpoint (inclusi i server) sono gli obiettivi principali degli attacchi ransomware.

Assicurarsi che siano ben difesi, includendo una **protezione anti-ransomware dedicata** per bloccare e ripristinare le attività di crittografia dannosa.

Rilevamento e Risposta

Il rilevamento e la risposta alle minacce 24 ore su 24 sono ora un livello di difesa essenziale.

Se non si hanno le risorse o le competenze per fornire tutto questo internamente,o se si vuole avere un supporto complementare e specialistico per il proprio team, lavorare con un **fornitore di servizi di Managed Detection and Response (MDR) affidabile.**

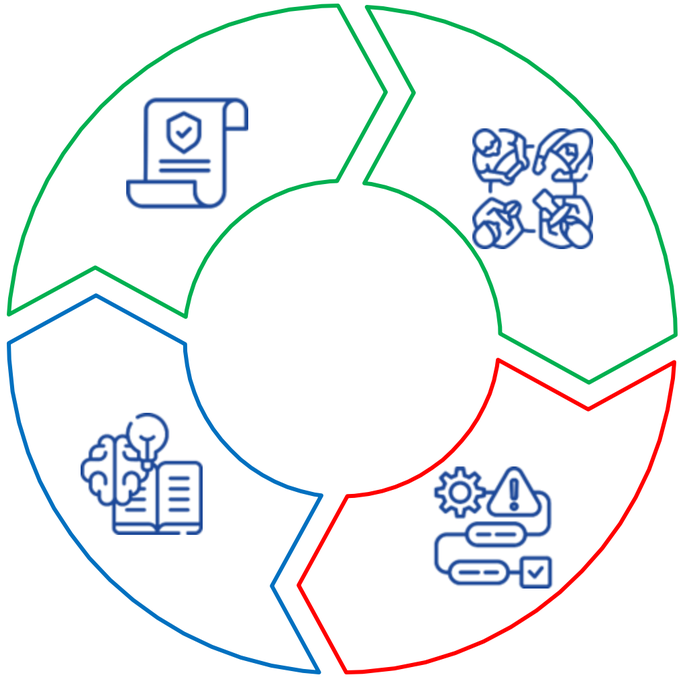
Le fasi di una corretta gestione di una crisi

Preparazione

Fase in cui si prepara l'Azienda per una eventuale gestione futura di una crisi, grazie alla scrittura/affinamento di policy, procedure, processi, playbook e template

Follow up

Fase in cui si effettuano eventuali altre comunicazioni necessarie una volta che la crisi si è conclusa e si gestiscono le «lesson learned», imparando il più possibile da ciò che è successo



Misurazione

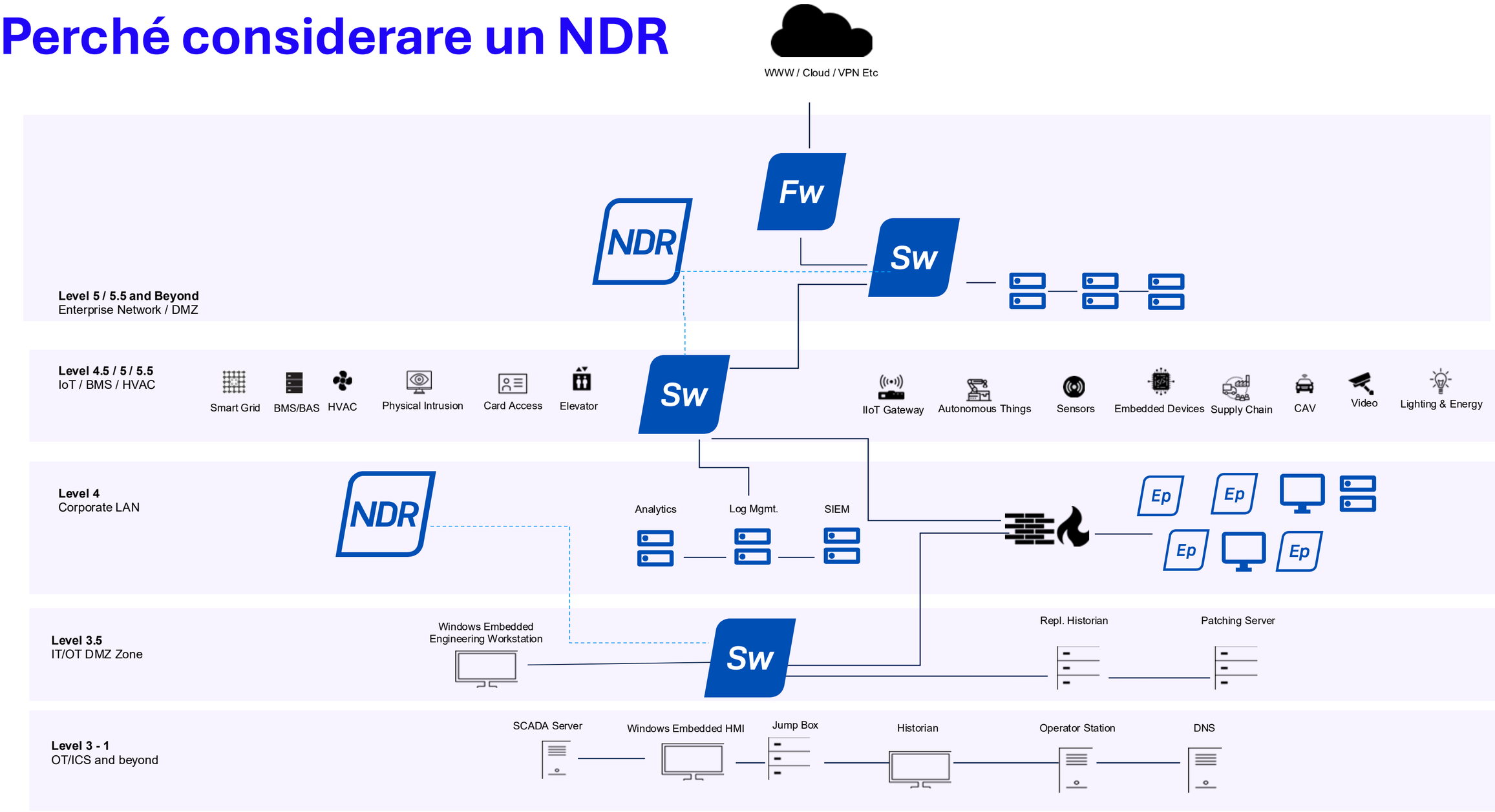
Fase in cui si testa la preparazione dell'azienda, grazie ad alcune attività come simulazioni tecniche di crisi, simulazioni C-Level e Table-Top Exercise
Questa fase può essere utilizzata anche come «Assessment», prima della fase di Preparazione, oppure come formazione al personale, per spiegare i documenti scritti o rivisti nella fase precedente

Gestione

Fase che comprende la gestione di una crisi nel momento in cui avviene. Si divide in:

- *Technical management* → trattamento della crisi dalla sua identificazione alla risoluzione
- *Communication management* → effettuazione delle comunicazioni necessarie nei momenti di crisi

Perché considerare un NDR



Principali casi d’uso di Sophos NDR

Dispositivi non Protetti

Dispositivi non autorizzati

Minacce IoT / OT

Attacchi Zero-Day

Minacce Interne

Advisory Services

Tipologia	Focus	A cosa è utile	Scenari di esempio
External Penetration Testing	Sistemi accessibili da Internet: siti web, VPN e servizi rivolti al pubblico	Cosa può vedere e accedere un attaccante da Internet? Ci sono servizi esposti non conosciuti?	Test di siti Web e servizi rivolti al pubblico; Identificazione delle vulnerabilità prive di patch
Internal Penetration Testing	Sistemi, applicazioni e dati presenti nella rete interna	Cosa potrebbe fare un attaccante se riuscisse ad accedere alla nostra rete? Potremmo rilevarlo?	Testare la facilità con cui una minaccia interna può aumentare i privilegi ed esfiltrare i dati
Wireless Network Penetration Testing	Infrastruttura Wi-Fi, protocolli di crittografia, autenticazione e controlli di accesso	La nostra rete wireless è sicura? Ci sono dispositivi non autorizzati o rogue?	Testare la sicurezza della rete Wi-Fi; identificare i punti di accesso non autorizzati; tentare connessioni non autorizzate
Web Application Security Assessment	Difetti di programmazione, autenticazione e gestione delle sessioni, controllo degli accessi	Le nostre app sono sicure? I dati sensibili sono esposti? Come possiamo correggere le vulnerabilità?	Test di portali clienti, siti di e-commerce, web app interne; identificazione di SQL injection, XSS o difetti di autenticazione

Q&A

Contatti:

Vieni a trovarci al nostro stand!