

CANALE A: Informatica Classica



CANALE B: Machine Learning



2h00

SUPERVISIONATO

Classificazione
Malware

Riconosce minacce note
tramite esempi storici
etichettati.

NON SUPERVISIONATO

Rilevamento
Anomalie

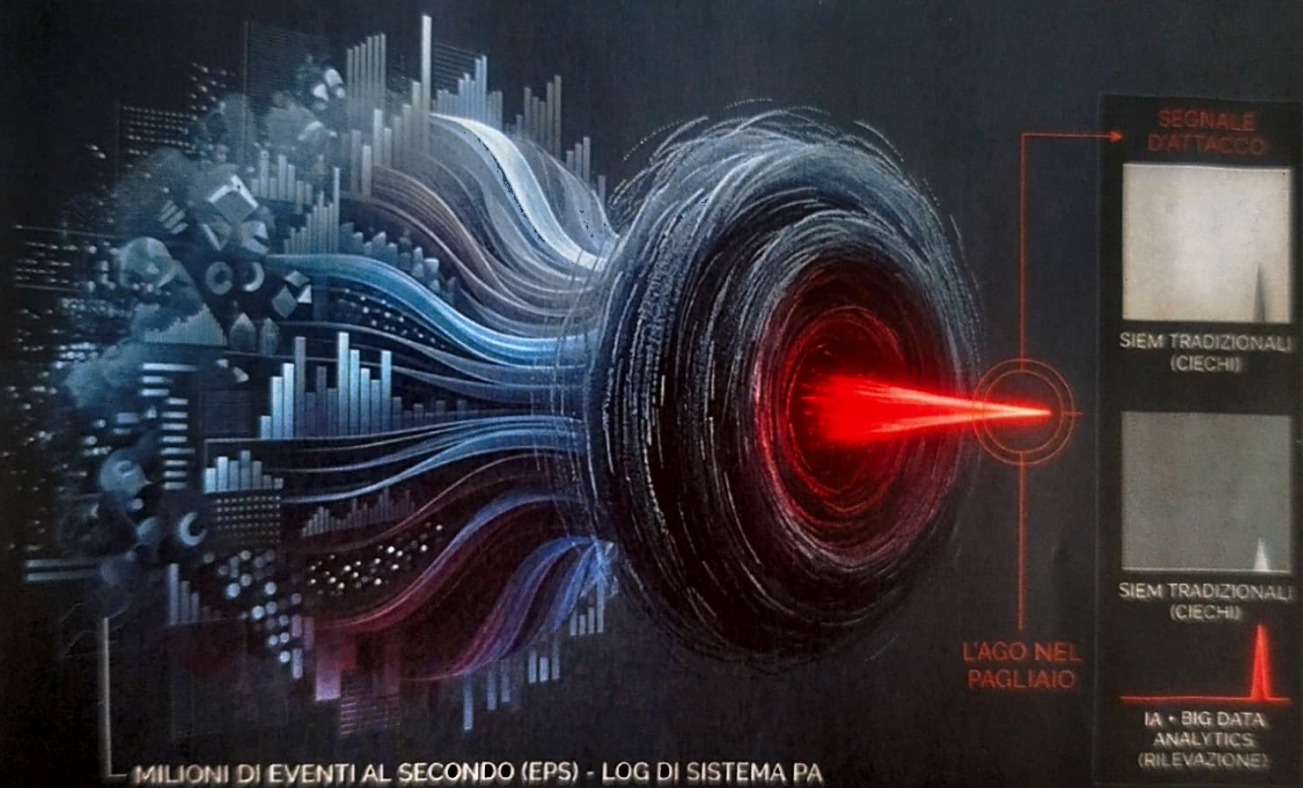
Identifica deviazioni
e comportamenti insoliti
rispetto alla norma.

DEEP LEARNING

Analisi dei flussi
di rete grezzi

Analizza pattern complessi
nei dati grezzi e traffico
senza filtri manuali.

MILIONI DI EVENTI AL SECONDO (EPS) - LOG DI SISTEMA PA



LA SCALA DEI BIG DATA NELLA PA RICHIEDE IA
PER SUPERARE LA CECITÀ DEI SISTEMI TRADIZIONALI

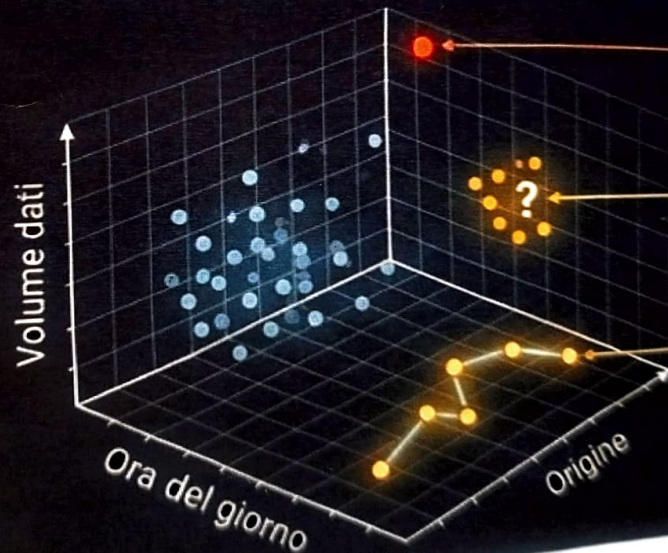
Slide 4: Che cos'è l'Anomaly Detection?

Tassonomia delle deviazioni

- 1. **Anomalie Puntuali** (es. picchi di traffico).
- 2. **Anomalie Contestuali** (es. accessi in orari non lavorativi).
- 3. **Anomalie Collettive** (es. scansioni di rete distribuite nel tempo).

Elementi visivi: Mappatura tridimensionale dei comportamenti di rete

1. **Anomalie Puntuali**
Puntuali (es. picchi di traffico).
2. **Anomalie Contestuali** (es. accessi in orari non lavorativi).
3. **Anomalie Collettive** (es. scansioni di rete distribuite nel tempo).



Punto isolato
(Anomalia Puntuale,
es. Picco traffico)

Punto normale ma
fuori orario
(Anomalia Contestuale)

Catena di punti
apparentemente innocui
(Anomalia Collettiva,
es. Scansione)

UEBA Control Dashboard

Analisi del Comportamento Utenti ed Entità - Scenario Fittizio

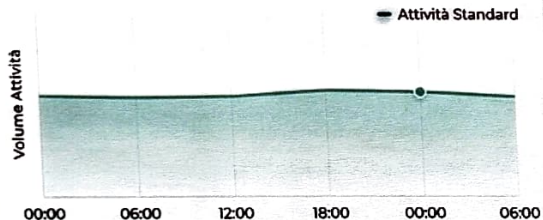
Profilo Utente Fittizio: 'Mario Rossi'



Ruolo: Amministratore

Identità: ID_7849_PA

Baseline Comportamentale (Ultime 48 Ore)



Punteggio di Rischio Dinamico (Risk Score)

ALTO RISCHIO - Rilevata Deviazione



Fattori di Deviazione: Download massivo notturno (ore 02-30),
Accesso a cartelle non autorizzate.

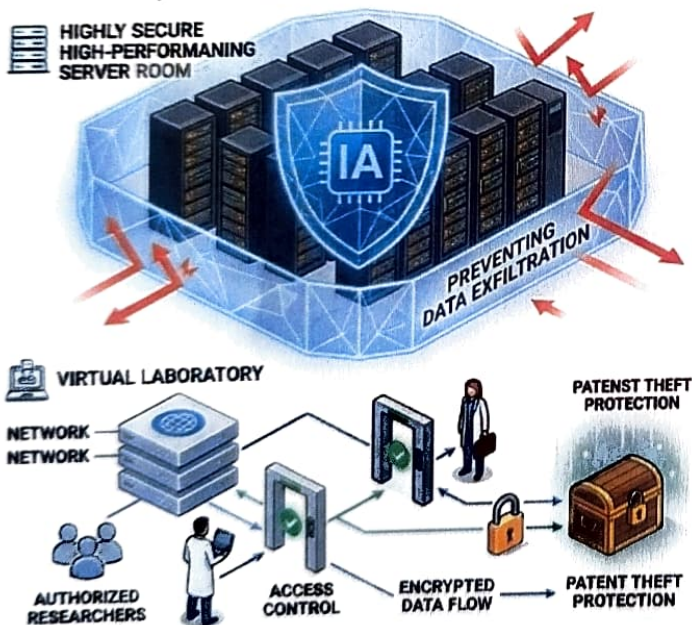
Baseline aggiornata: Deviazione significativa.

SLIDE 7: CASI D'USO PRATICI IN ENTI SCIENTIFICI E DI MONITORAGGIO AMBIENTALE



1. CNR

'Supercomputing & Data Protection'



ARPAC

2. ARPAC

'Environmental Network & Data Integrity'



ARPAC NETWORK

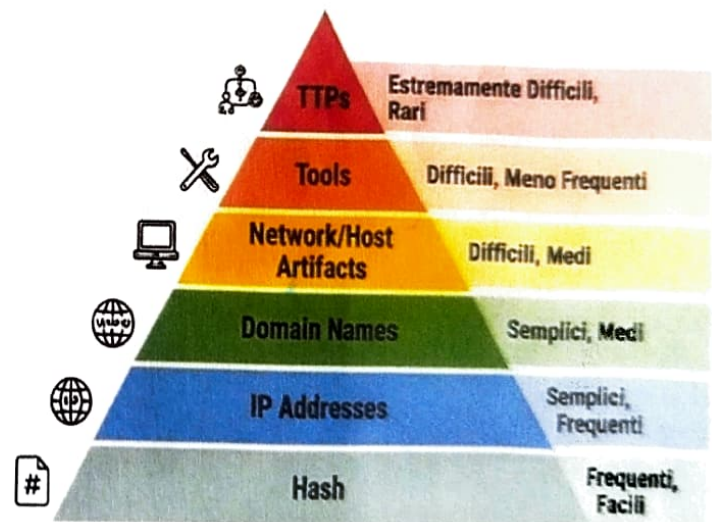


Cyber Threat Intelligence: Modulo 3

Il Ciclo CTI



Piramide del Dolore



I 3 Livelli CTI nella PA

1		STRATEGICA (Dirigenza)	Decisioni a lungo termine, trend globale
2		TATTICA (IT Manager)	TTPs degli attaccanti, pianificazione difese
3		OPERATIVA/TECNICA (Sistemi)	IoC specifici, blocco in tempo reale

SLIDE 9: IL RUOLO DELL'IA NELLA THREAT INTELLIGENCE

Velocizzare la conoscenza e governare la complessità cyber

A. LA PIPELINE DI INGESTIONE DATI (Flusso Orizzontale)

1. INGESTIONE FONTI

Fonti Eterogenee:

- Social Media & Blog Tecnici
- Deep & Dark Web
- Chat Multilingua (Cinfilico, Cinese)



2. MOTORE NLP + IA

Elaborazione Centrale:

- Estrazione automatica IoC
- Traduzione cross-lingua
- Correlazione automatica dati



3. OUTPUT FINALE

Risultato per la PA:

- Report e dati strutturati
- Indicatori (IoC) pronti all'uso
- [■] Presidio Sicurezza

B. ANALISI DEL VALORE (Paragrafo 9)

■ LA SFIDA ATTUALE (Il Problema)

- **Vastità delle Fonti:** Mole enorme di dati non strutturati provenienti da ambienti sommersi.
- **Il Fattore Tempo:** Finestra temporale ridotta per agire tempestivamente prima dell'attacco.

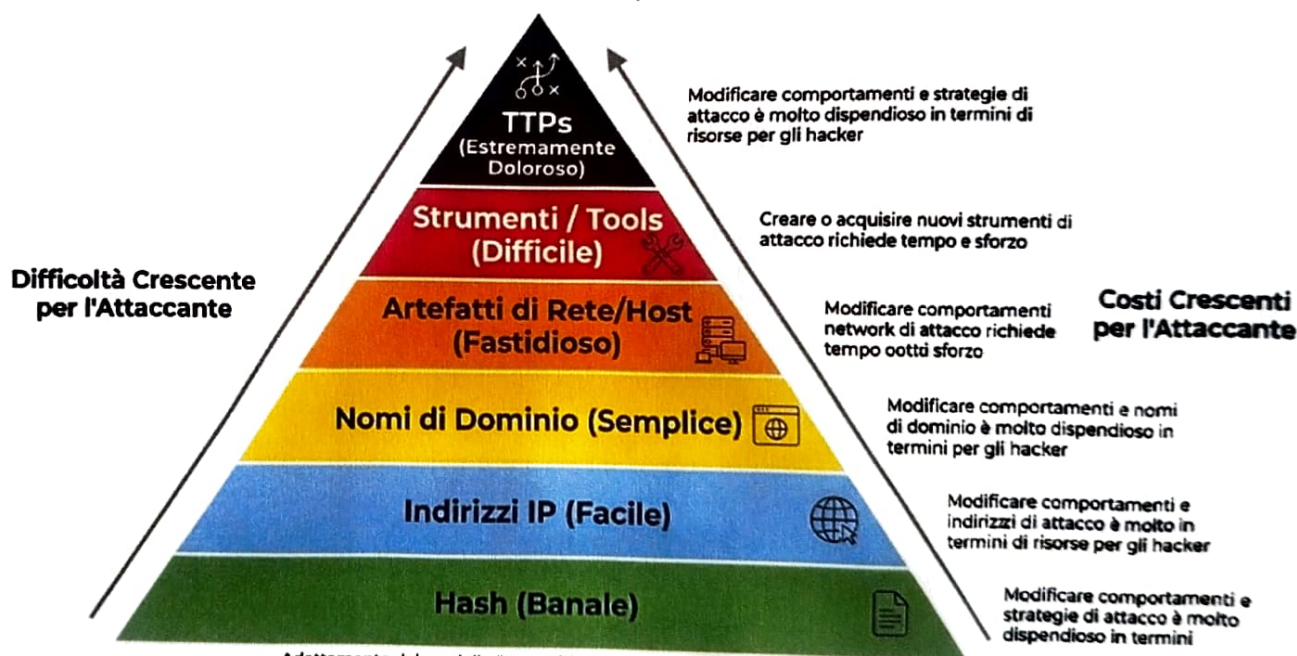
■ **Limite Umano:** Sovraccarico informativo (Information Overload).

■ LA SOLUZIONE CON IA (L'Impatto)

- **Accelerazione Totale:** Forte incremento della velocità di elaborazione della conoscenza cyber.
 - **Correlazione Trans-Nazionale:** Capacità di unire i puntini analizzando fonti in più lingue simultaneamente.
- **Vantaggio:** Intelligence preventiva e strutturata.

LA PIRAMIDE DEL DOLORE NELLA CYBERSECURITY

Incrementare la Difficoltà per l'Attaccante



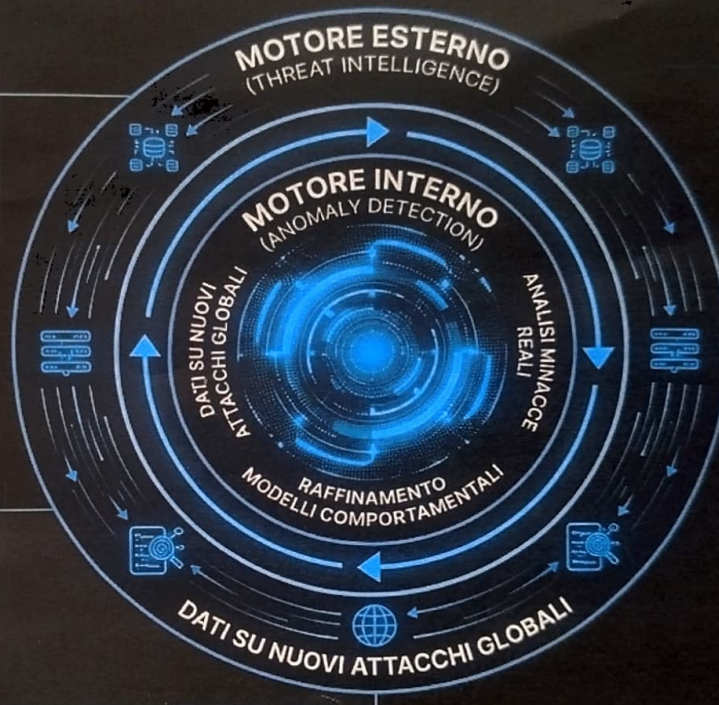
Adattamento del modello "Pyramid of Pain" di David J. Bianco
Illustrazione concettuale per la difesa informatica

SCHEDA ELEMENTI VISIVI - SLIDE 11

L'ecosistema di difesa predittiva – La convergenza dei pilastri

ELEMENTI VISIVI:

Schema circolare
dinamico a due
motori
interconnessi



CONCETTI CHIAVE:

Cyber
Cyber Resilienza e
Difesa Predittiva

OBIETTIVO COMUNICATIVO:

Passaggio dal
rilevamento
passivo
all'intercettazione
proattiva della
catena d'attacco
(Cyber Kill Chain)



PARAGRAFO 11: La sinergia operativa - Dal dato locale alla reazione globale

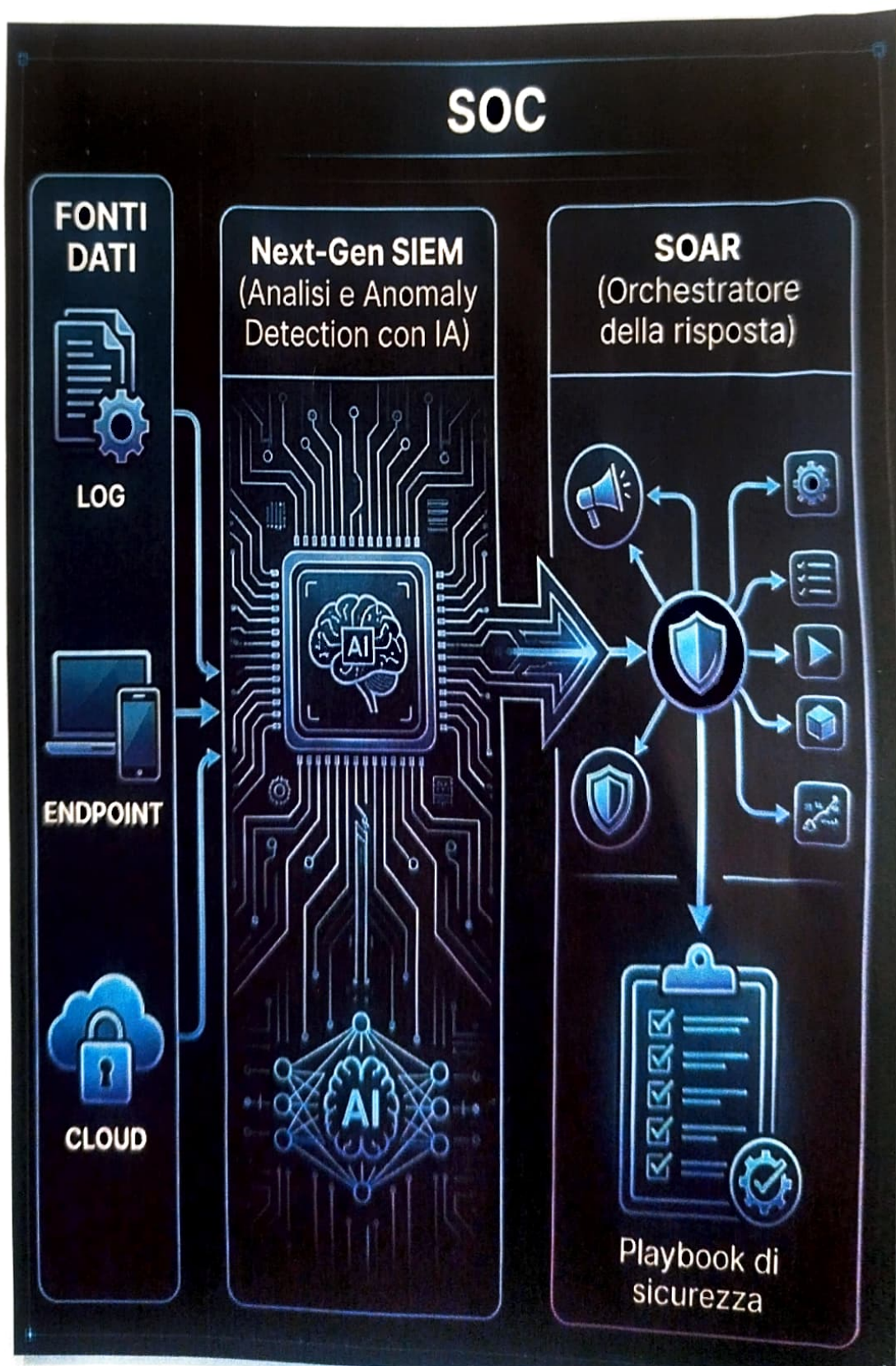
SCHEDA GRAFICA: Slide 12 - I sistemi SIEM e SOAR di nuova generazione

CONCETTI CHIAVE 1

Evoluzione tecnologica: dai SIEM tradizionali basati su regole ai SIEM cognitivi.

CONCETTI CHIAVE 2

Cos'è il SOAR e come automatizza risposta agli incidenti.





**Governance,
Aspetti Giuridici ed Etici
ed Etici per i Dirigenti PA**

Il quadro normativo europeo e nazionale - NIS 2, GDPR e AI Act

**DIRETTIVA
NIS 2**
(Gestione del
rischio PA)

GDPR
(Tutela della privacy
dei dati e dei lavoratori)

AI ACT
(Regolamentazione
del rischio dei sistemi di
Intelligenza Artificiale)

QUADRO REGOLATORIO COGENTE

Il quadro regolatorio cogente
per il dirigente pubblico

OBBLIGHI DI CONFORMITÀ

Obblighi di conformità
e adempimenti



Scheda grafica per Slide 15 - Il problema dei falsi positivi ed il fattore umano - L'approccio Human-in-the-loop

1

**I limiti intrinseci dell'IA nella PA:
Falsi Positivi e Falsi Negativi**



**ANALISTA
UMANO**



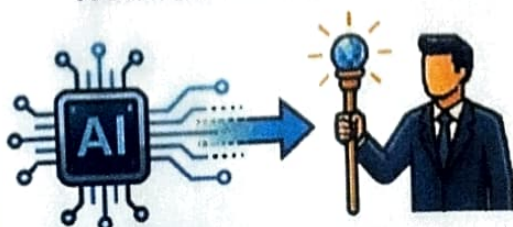
**CERTEZZA
INVESTIGATIVA**



**RUMORE
ALGORITMICO**
(Migliaia di falsi allarmi)

2

**FILOSOFIA
"HUMAN-IN-THE-LOOP"**



L'IA propone → L'uomo decide e governa

3

**IMPORTANZA
DELLA FORMAZIONE
DELL'ANALISTA
UMANO**



SLIDE 16: L'USO DELL'IA DA PARTE DEI CYBER-CRIMINALI - LA MINACCIA ASIMMETRICA

DIFENSORE DELLA PA



Iconografia "Dual-Use" dell'IA - Protezione e Sicurezza

IA OFFENSIVA: L'OMBRA OSCURA



L'altra faccia dell'IA - Minaccia Cyber Asimmetrica



Evoluzione della minaccia:
Spear Phishing iper-personalizzato con IA generativa

**E-mail di phishing generate sinteticamente
senza difetti grammaticali**



Rilevamento phishing avanzato (Esempio)

✉ e-mail

**OGGETTO: Aggiornamento urgente sulle
credenziali del portale dei dipendenti PA**

E-mail di phishing generate senza la
perfectly written without notatato without a single
grammatical mistake, in pre esentivo sche-
iperpersonalizzata un specifico (fictional)
dipartimento (fictional) dipartimento.
Demando un click auniti su un **glowang link!**



I LIMITI DELL'ALGORITMO E LA CENTRALITÀ DELL'UOMO

POTENZA E VELOCITÀ
DI CALCOLO DELL'IA

ETICA, CONTESTO E
GIUDIZIO CRITICO
DELL'UOMO



FILOSOFIA "HUMAN-IN-THE-LOOP"

L'IA ACCELERA,
CORRELA E PROPONE



L'ANALISTA UMANO
CONVALIDA LA DECISIONE
E GESTISCE LA COMPLESSITÀ