Deception Technology: come ottenere la resilienza informatica attraverso l'inganno

metodologie e tecnologie di threat intelligence al fine di ingannare l'avversario

Francesco Arruzzoli

Sr. Cyber Security Threat Intelligence Architect

- Resp. Centro Studi Cyber Defence Cerbeyra
- Membro commissione Cyberwarfare SOCINT

Cyber Crime Conference, Roma, 11-12 maggio 2023

«Sollecitatelo e imparate i principi che regolano la sua attività o inattività. Costringetelo a rivelarsi, a scoprire i suoi punti vulnerabili..»

Inganno (Deception): tremila anni di storia

L'inganno in guerra è probabilmente antico quanto il conflitto armato stesso. La logica di confondere l'avversario è ovvia ed i vantaggi sono molteplici.

«Sollecitatelo e imparate i principi che regolano la sua attività o inattività. Costringetelo a rivelarsi, a scoprire i suoi punti vulnerabili»

Sun Tzu, L'arte della Guerra

VI secolo a.C.

«…se il nimico ti mettesse innanzi una preda, dèi credere che in quella sia l'amo e che vi sia dentro nascoso lo inganno.»

«..il nimico le assalta da quella parte donde essi non credono essere assaltati ….. e questo inganno nasce da due cagioni: o per essere che sia inaccessibile, o per essere usata arte dal nimico di assaltargli da uno lato, con romori finti e, dall'altro, taciti e con assalti veri.»

Niccolò Machiavelli, Dell'arte della guerra

1520 a.D.

Con l'aumento della tecnologia nelle organizzazioni **aumenta la superficie di attacco** e la complessità degli attacchi.

L'idea che un'organizzazione con una **rigida difesa perimetrale**, sia più sicura ha dimostrato più volte di essere **errata**.

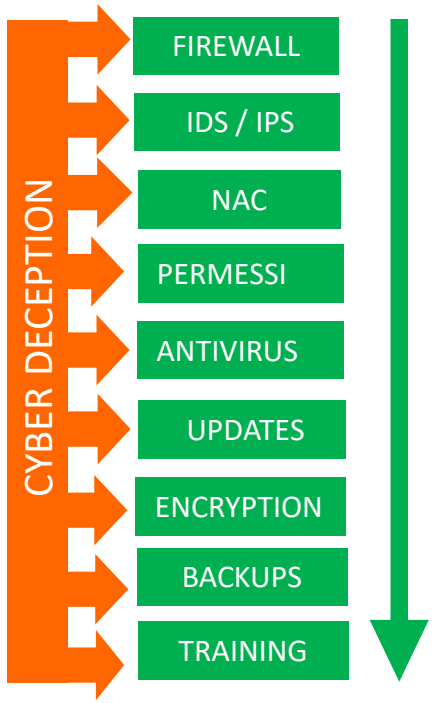
I **team di sicurezza** sono spesso **limitati** al solo constatare il corretto funzionamento o meno dei sistemi di difesa (ad es. firewall, antivirus, etc..).

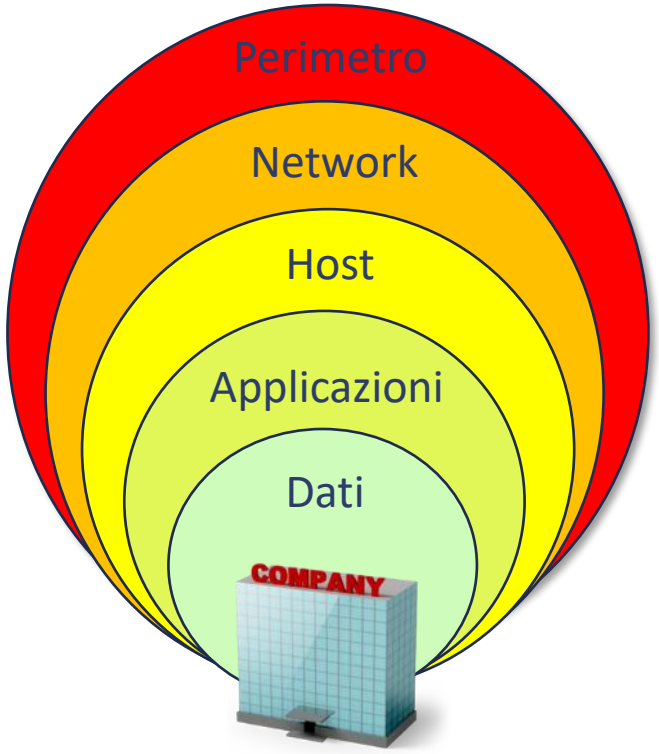
Attacchi sofisticati richiedono difese sofisticate:

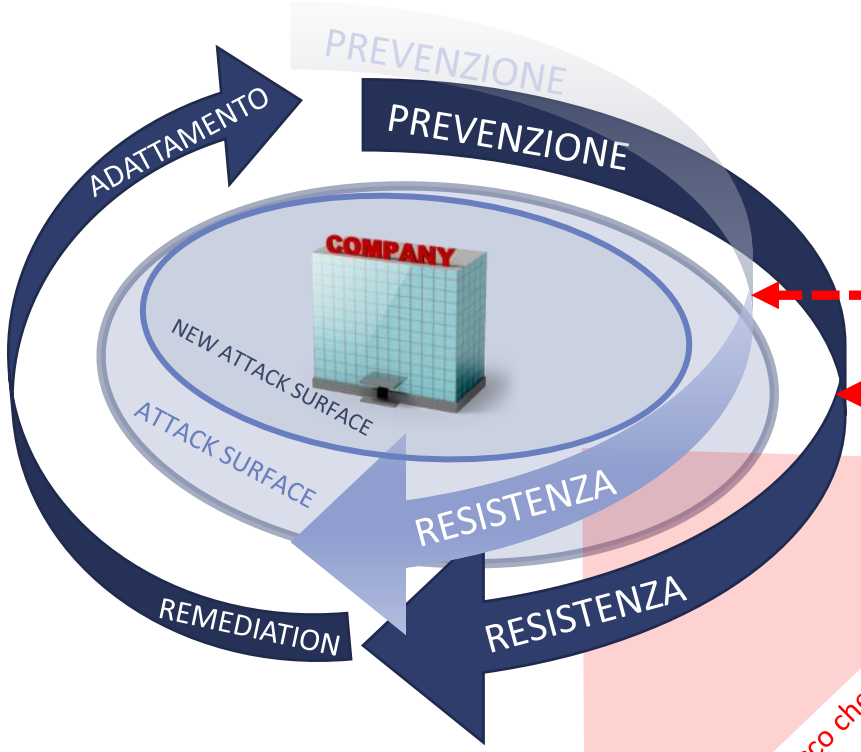
- Predittiva piuttosto che Preventiva
- Proattiva piuttosto che Reattiva
- Agile piuttosto che Rigida
- Dinamica piuttosto che Statica

Il quotidiano conflitto con le cyber minacce e la necessità di garantire la resilienza delle organizzazioni, impone ai resp. della sicurezza la necessità di integrare nuove metodologie e strategie di difesa.

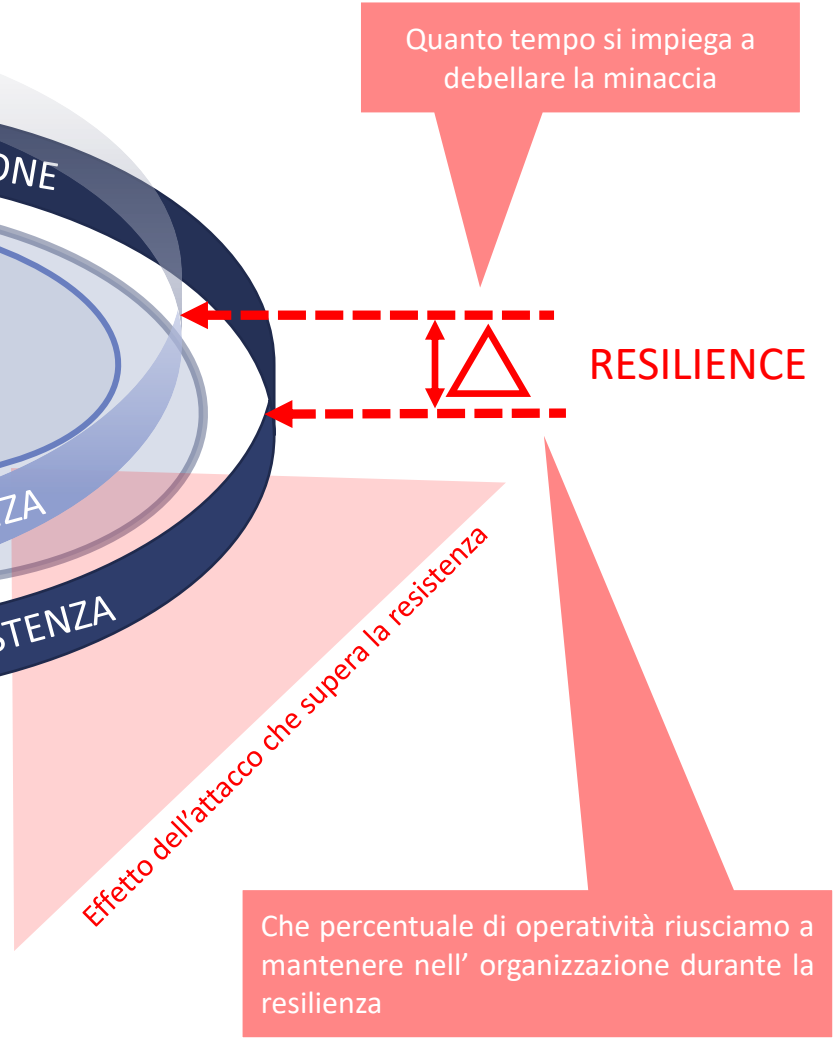
LA CYBER RESILIENCE DELLE AZIENDE VIENE CONTINUAMENTE MESSA ALLA PROVA







Persone, HW, SW, Informazioni, Processi, Regole



Le tecnologie dell'inganno migliorano il rilevamento e rallentano l'attaccante.

La principale caratteristica della difesa basata sull'inganno è il vantaggio che si crea nei confronti dell'attaccante.

OSSERVARE E RILEVARE

La tecnologia dell' inganno crea un ambiente ostile per gli aggressori riducendo la superficie di attacco e implementando un rilevamento basato sull'inganno. L'inganno aumenta drasticamente lo sforzo e i costi per l'attaccante.

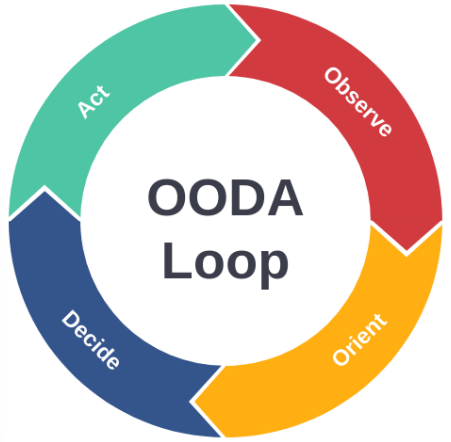
INFLUENZARE E MANIPOLARE

Essere ingannevoli nei confronti degli hacker vuol dire passare attivamente informazioni ingannevoli che influenzano le fasi di osservazione, orientamento, decisione e azione dell'avversario.

VANIFICARE E RELEGARE

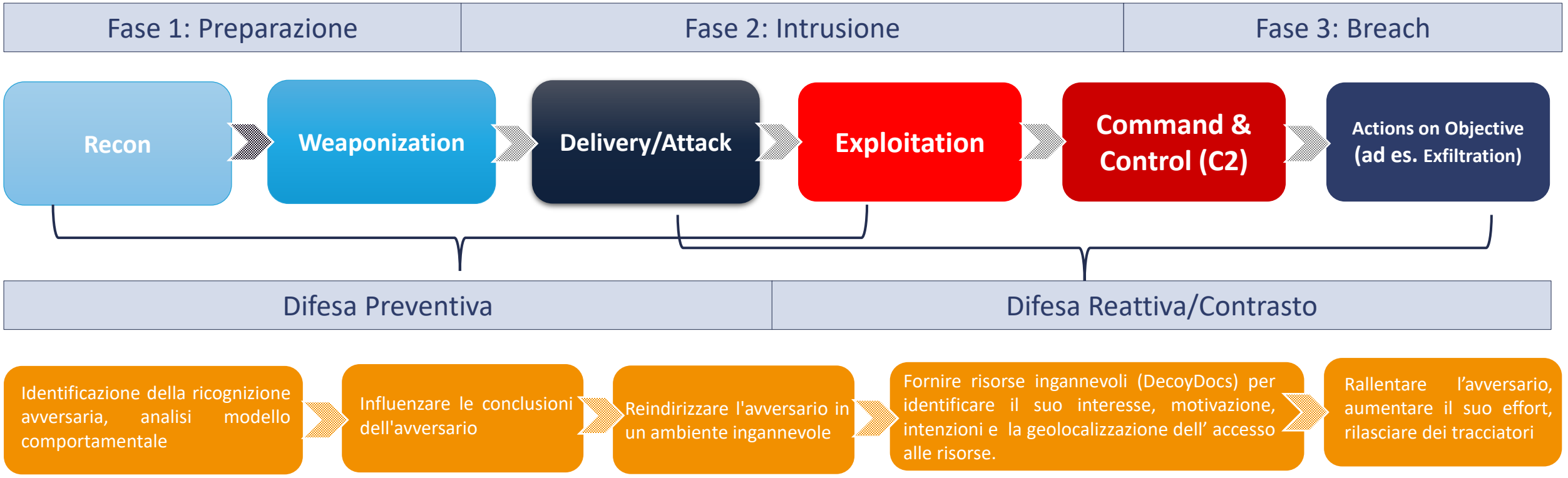
Per essere uno strumento di rilevamento efficace, gli inganni devono essere inevitabili, non rilevabili e ineludibili.

Il loop OODA (Observe, Orient, Decide, and Act) è un modello di processo ciclico proposto da John Boyd. Descrive come un'entità reagisce ad un evento. Per vincere è necessario eseguire questo ciclo più velocemente dell'avversario. Il vantaggio è che, utilizzando il loop OODA, **IL DIFENSORE RALLENTA IL PROCESSO DELL'AVVERSARIO E CONCEDE AI DIFENSORI PIÙ TEMPO PER DECIDERE E AGIRE.**



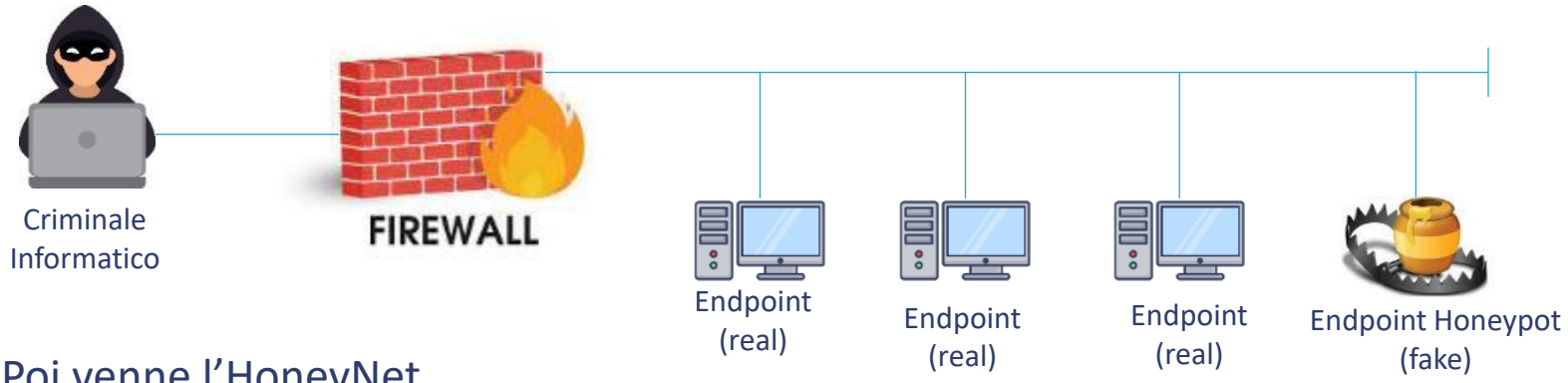
Cyber Kill Chain e Cyber Deception Chain

Nella strategia militare, "**Kill Chain**" è un modello che descrive la fase dell'attacco. Una **Cyber Kill Chain** contiene una serie di step che un criminale informatico deve completare al fine di compromettere un'infrastruttura target e raggiungere gli obiettivi. La **Cyber Deception Chain** è stata creata per identificare e mappare le fasi e le procedure necessarie per implementare con successo l'inganno informatico.

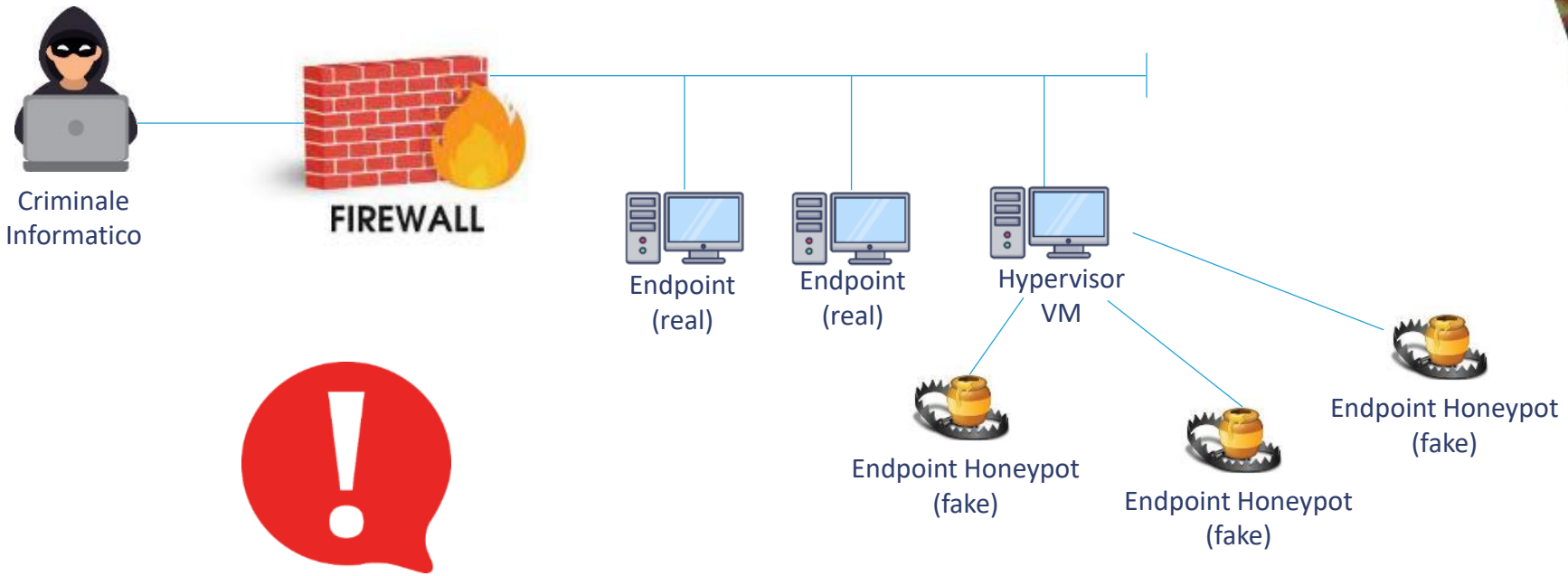


Cyber Deception Chain

All’inizio c’era l’HoneyPot.. correva l’anno 1990



Poi venne l’HoneyNet..



Sistemi che richiedono molto lavoro per essere «credibili»

I criminali informatici si sono abituati a «sniffare» le Honeypots

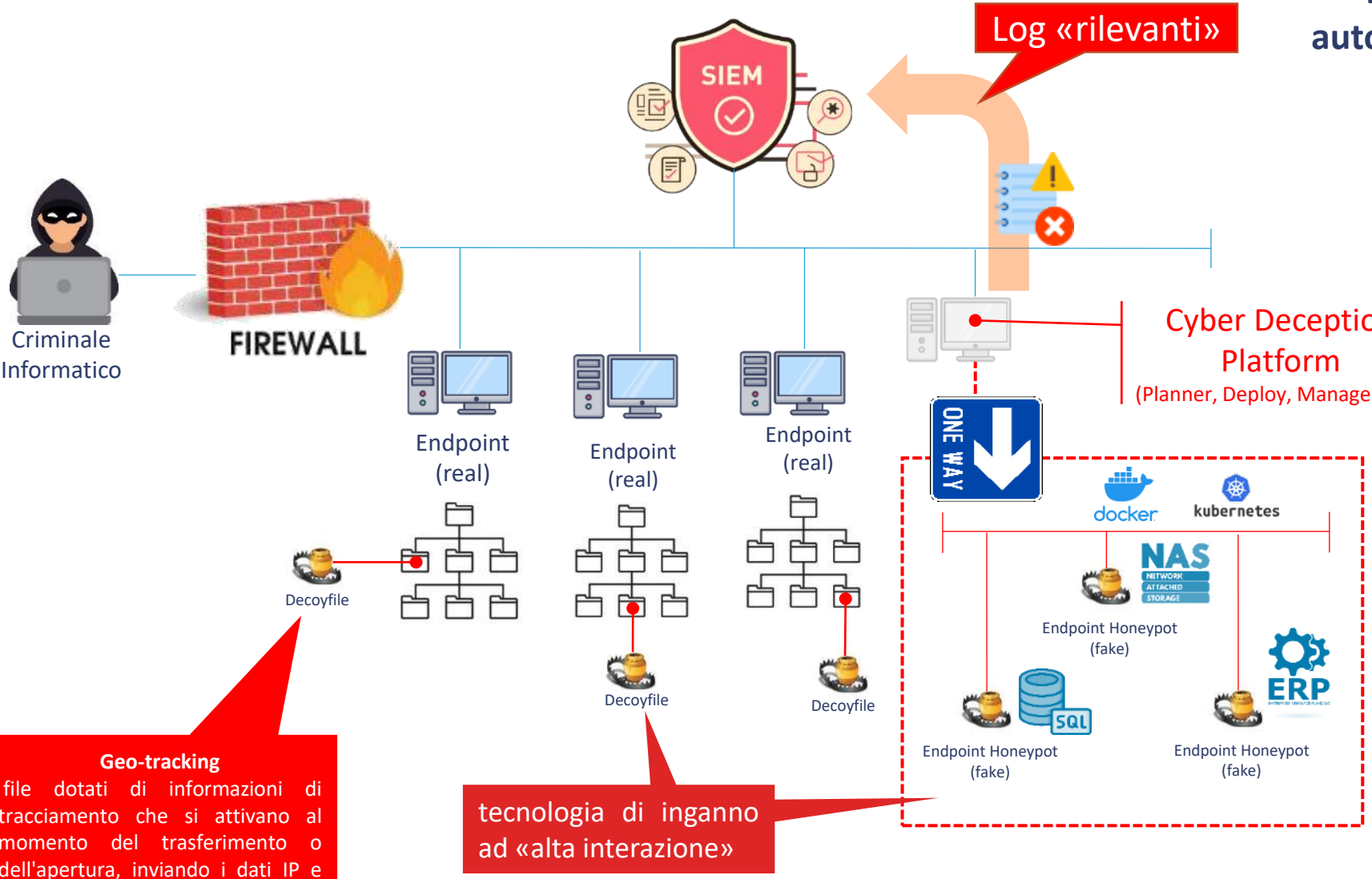
Il framework **«Mitre Engage»** lo descrive come un vero e proprio processo e non come uno stack di tecnologico.

Cognitive Deception Model (CDM)

L' A.I. per un nuovo approccio alla gestione della cyber deception «one click»
Manipolare gli avversari e generare intelligence utilizzabile

ICT Security MAGAZINE

CYBER CRIME CONFERENCE



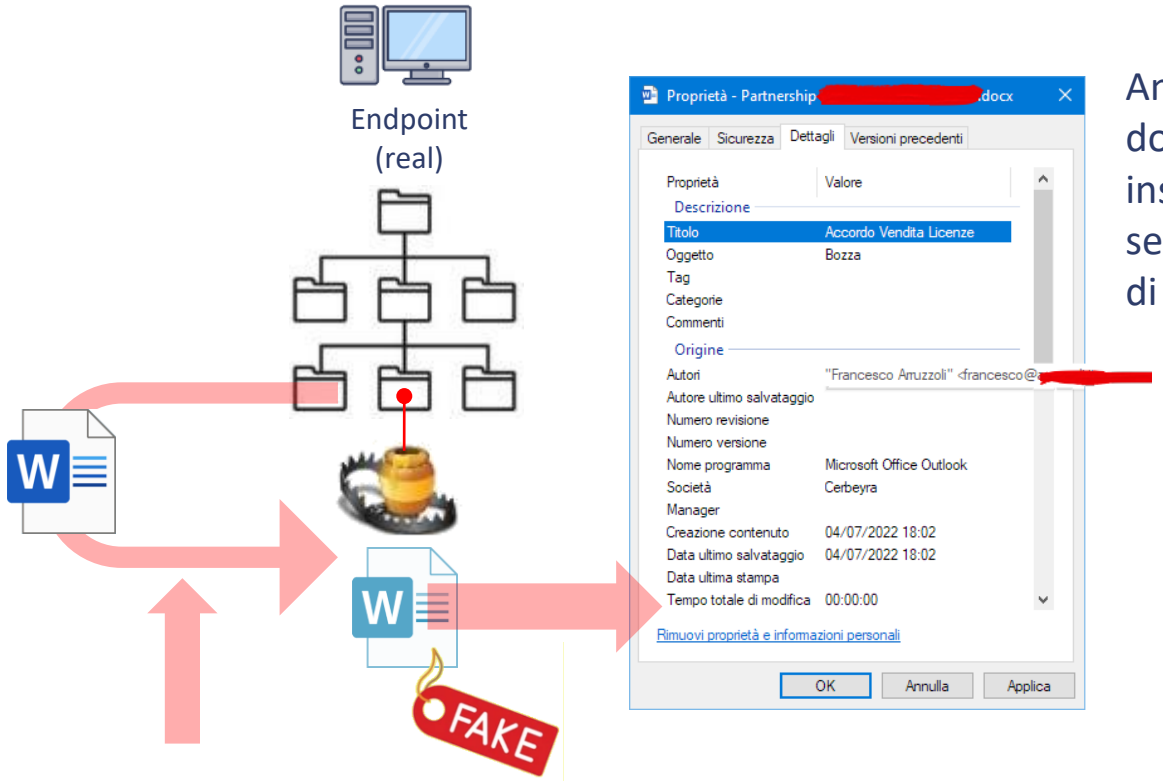
L' A.I. per la creazione e la gestione automatica di servizi e risorse «plausibili»

I sistemi di inganno intelligenti sono in grado di creare inganni personalizzati per reti, sistemi, applicazioni, server e dati che appaiono nativi dell'ambiente.

ATTIVAZIONE CON UN CLICK

Cognitive Deception Model (CDM)

L' A.I. per la creazione di file «esca» realisticamente «attraenti»



I documenti vengono generati da una rete neurale che prende un documento in ingresso e genera un documento sintatticamente coerente, dall'aspetto plausibile e convincente, cognitivamente in grado ingannare gli avversari.

Interessante studio :

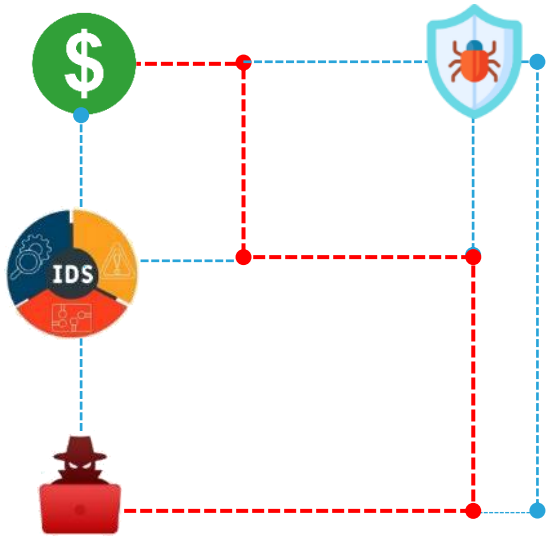
IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

DOI: 10.1109/ACCESS.2022.3166628

Anche i metadati contenuti nel documento vengono modificati inserendo informazioni esca che se utilizzate attivano segnalazioni di allarme (ad es. email fake)

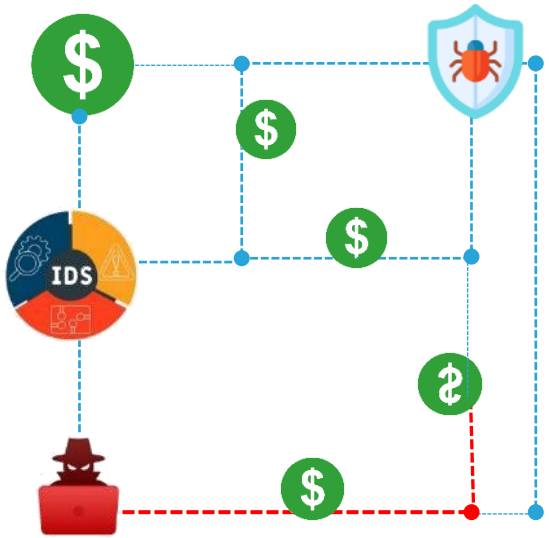
ChatGPT

«addestrata al fake»



Difesa tradizionale

L'attaccante conosce le strategie e cerca di anticiparle.



Tecnologia dell'inganno

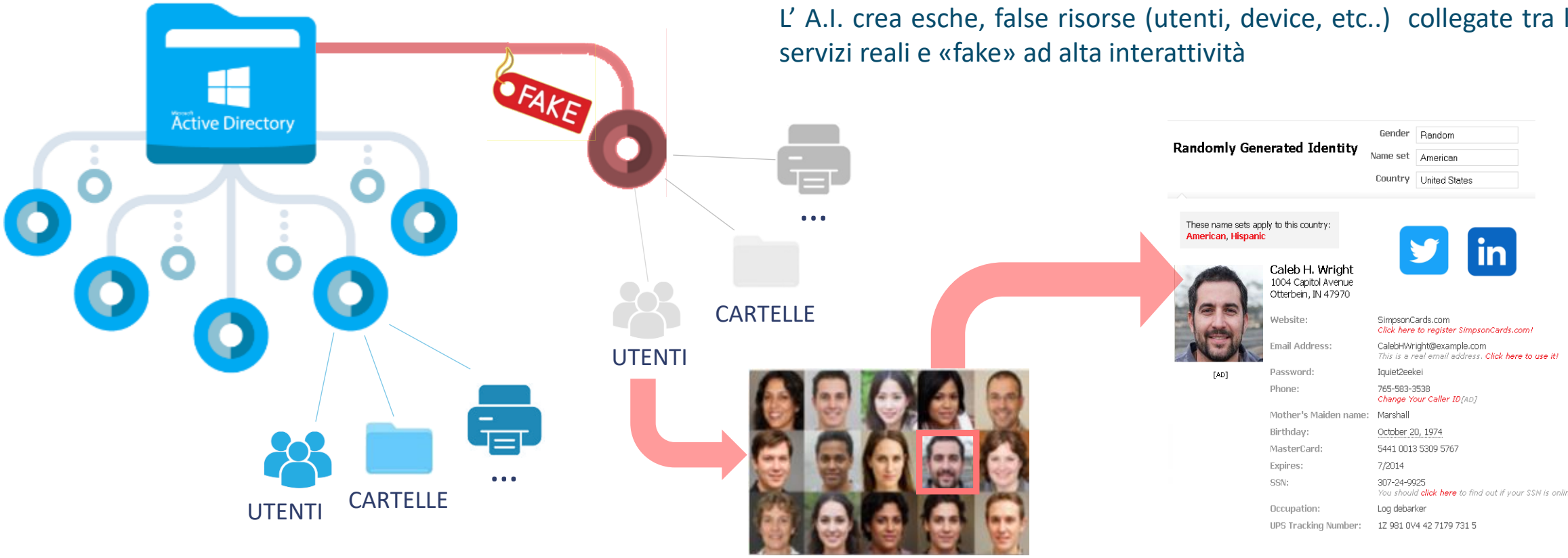
L'attaccante si ritrova in un ambiente imprevisto che non conosce e che deve studiare.

Cognitive Deception Model (CDM)

Active Directory (AD) è il principale servizio che controlla l'accesso alla rete aziendale e viene utilizzato da oltre il 90% delle organizzazioni. Questo lo rende un obiettivo chiave per gli aggressori «la chiave d'oro» per cercare di ottenere privilegi aggiuntivi ed intensificare i loro attacchi

Active Directory Deception protegge AD restituendo informazioni false in risposta a tentativi di accesso ed utilizzo da parte di aggressori. Quando gli aggressori utilizzano i dati falsi restituiti da AD, il sistema li isola in un ambiente sicuro in cui è possibile raccogliere informazioni preziose come TTP e IOC.

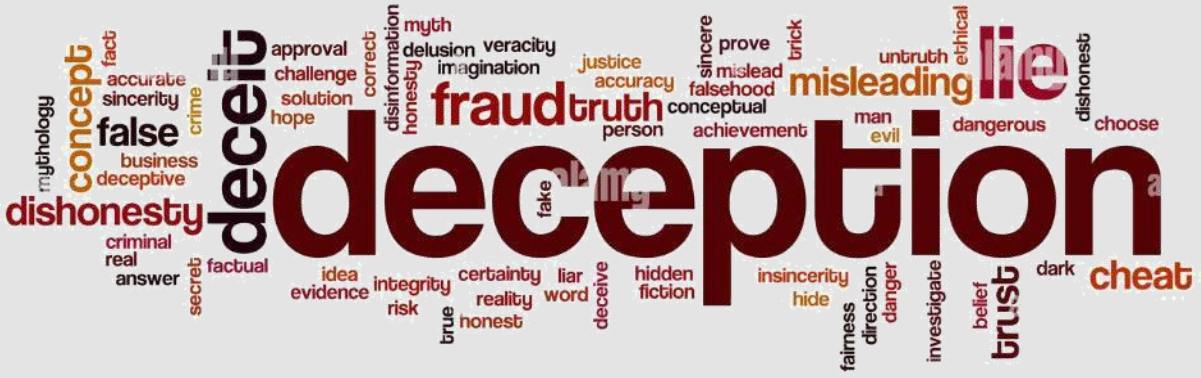
L' A.I. crea esche, false risorse (utenti, device, etc..) collegate tra loro a servizi reali e «fake» ad alta interattività



Rileva, inganna, difendi..

Un nuovo livello di difesa per tutte le organizzazioni

La cyber deception può portare organizzazioni, con diversi livelli di maturità, a disporre di informazioni reali e tempestive, diminuendo drasticamente i falsi positivi, e contenendo esfiltrazioni ed accessi non autorizzati, il che significa resilienza, risparmio di risorse critiche, ed ottimizzazione dell'effort nei team di sicurezza e SOC soprattutto se di piccole dimensioni.



E’ necessario cambiare il paradigma classico della cyber security difensiva, perché se la miglior difesa è l’attacco, la cyber deception rappresenta un nuovo modello integrativo e proattivo per la resilienza delle organizzazioni alle cyber minacce.

«Chi inganna l'ingannatore, non merita pena, ma onore»
(anonimo)

Francesco Arruzzoli

francesco.arruzzoli@cerbeyra.com

Grazie per l’attenzione