HACKING E PRIVACY: MINACCE INVISIBILI E DIFESE CONSAPEVOLI

MASSIMO CHIRIVÌ – 23/10/2025 – FIRENZE

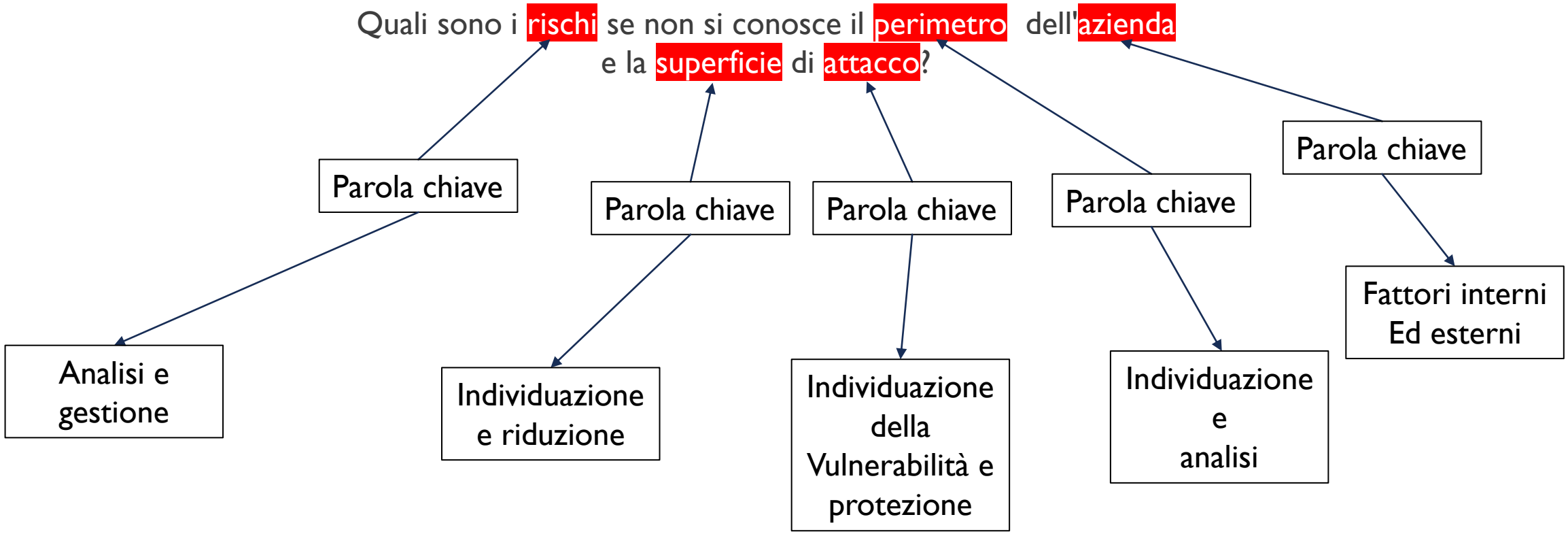
ABOUT ME (SINTETICA)

- **Tutte le info su Linkedin, esperienze, certificazioni, incarichi, collaborazioni, ecc.**
- **Oggi vi dico semplicemente che da 30 anni mi occupo d'informatica e da 20 di sicurezza informatica**
- **L'Ethical Hacking è la mia attività principale.**

Ethical Hacking (White Hat) ≠ Hacking (Black Hat)

FOCUS sul MODUS OPERANDI!

INIZIAMO CON UNA RIFLESSIONE



Attenzione! Sono cinque parole che sono tutte collegate tra di loro.
Non si devono mai dividere e/o trascurare.

PROVIAMO A RAGIONARE INSIEME SUL PERIMETRO?

PANORAMA COMPLESSO (EXAMPLE)

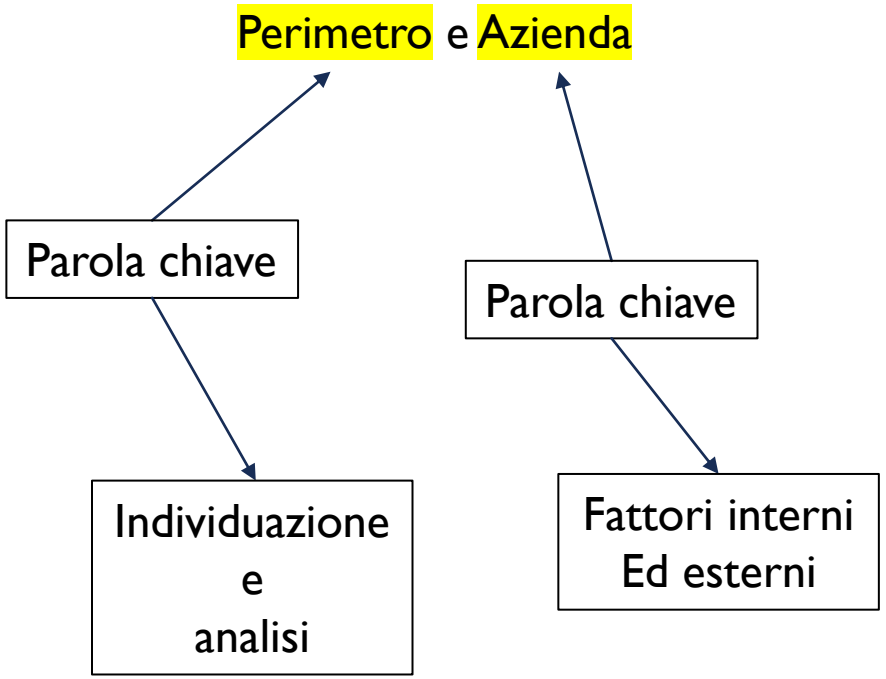
Ragione sociale: Contoso srl
Attività: Industria abbigliamento
Numero dipendenti: 50 in ufficio + 250 in produzione

Unità organizzative:

- Ufficio amministrazione
- Direzione generale
- Ufficio acquisti
- Ufficio vendite
- Ufficio campionario
- Ufficio produzione
- Ufficio modelli

Infrastruttura IT on premises
Infrastruttura IT on CLOUD
Infrastruttura IT del cliente
Infrastruttura IT del fornitore
Infrastruttura IT dei consulenti
…
Social Network, …

Stiamo solo analizzando e considerando 2 parole:



PROVIAMO A RAGIONARE INSIEME SUL PERIMETRO?

PANORAMA COMPLESSO (EXAMPLE)

Ragione sociale: Contoso srl
Attività: Industria abbigliamento
Numero dipendenti: 50 in ufficio + 250 in produzione

Unità organizzative:

- Ufficio amministrazione
- Direzione generale
- Ufficio acquisti
- Ufficio vendite
- Ufficio campionario
- Ufficio produzione
- Ufficio modelli

Infrastruttura IT on premises
Infrastruttura IT on CLOUD
Infrastruttura IT del cliente
Infrastruttura IT del fornitore
Infrastruttura IT dei consulenti
…
Social Network, …

Vulnerabilità dei sistemi
Problemi legati agli essere umani
Problemi legati alla supply chain

Si apre uno scenario incredibile…

Abbiamo introdotto solo un altro termine: superficie

ANALISI DELLA SUPERFICIE (DI ATTACCO)

- Network Assessment - Vulnerability Assessment
- Human Assessment
- Financial Assessment - Company Assessment
- Partner Assessment - Customer Assessment
- Vendor Assessment – Provider Assessment
- Intelligence

Se tutto questo non viene gestito correttamente il rischio collegato alla vulnerabilità non viene eliminato o mitigato e l'attacco prima o poi travolgerà il business aziendale.

La superficie di attacco di un sistema è quella parte del sistema stesso che può essere esposta ad accesso o a modifiche di utenti non autorizzati.

Tanto maggiore è la superficie, più alta è la probabilità che ci siano vulnerabilità

LE COMPLESSITÀ…

- Network Assessment - Vulnerability Assessment
- Human Assessment
- Financial Assessment - Company Assessment
- Partner Assessment - Customer Assessment
- Vendor Assessment – Provider Assessment
- Intelligence

E tutti gli oggetti connessi che abbiamo in tutto il perimetro? Quando li consideriamo?

Qui il «gioco» diventa complesso!

E bisogna avere obbligatoriamente una

«mentalità hacker, bisogna vedere oltre…»

per andare a fondo e fare le analisi correttamente.

COSA BISOGNA FARE?

Network Assessment - Vulnerability Assessment	Strumenti di Vulnerability Assessment e Network discovery.
Human Assessment	Phishing simulation, Analisi comportamentali, Social Engineering
Financial Assessment - Company Assessment	OSINT – CLOSINT – SOCMINT Open Source Intelligence, Close Source Intellingence, Social Media Intelligence
Partner Assessment - Customer Assessment	ALL Assessment
Vendor Assessment – Provider Assessment	ALL Assessment
Intelligence	OSINT – CLOSINT – SOCMINT - CTI Open Source Intelligence, Close Source Intellingence, Social Media Intelligence, Cyber Threat Intelligence

ALCUNI ESEMPI …

Phishing simulation, analisi comportamentali, social engineering

Si deve tendere alla Realtà

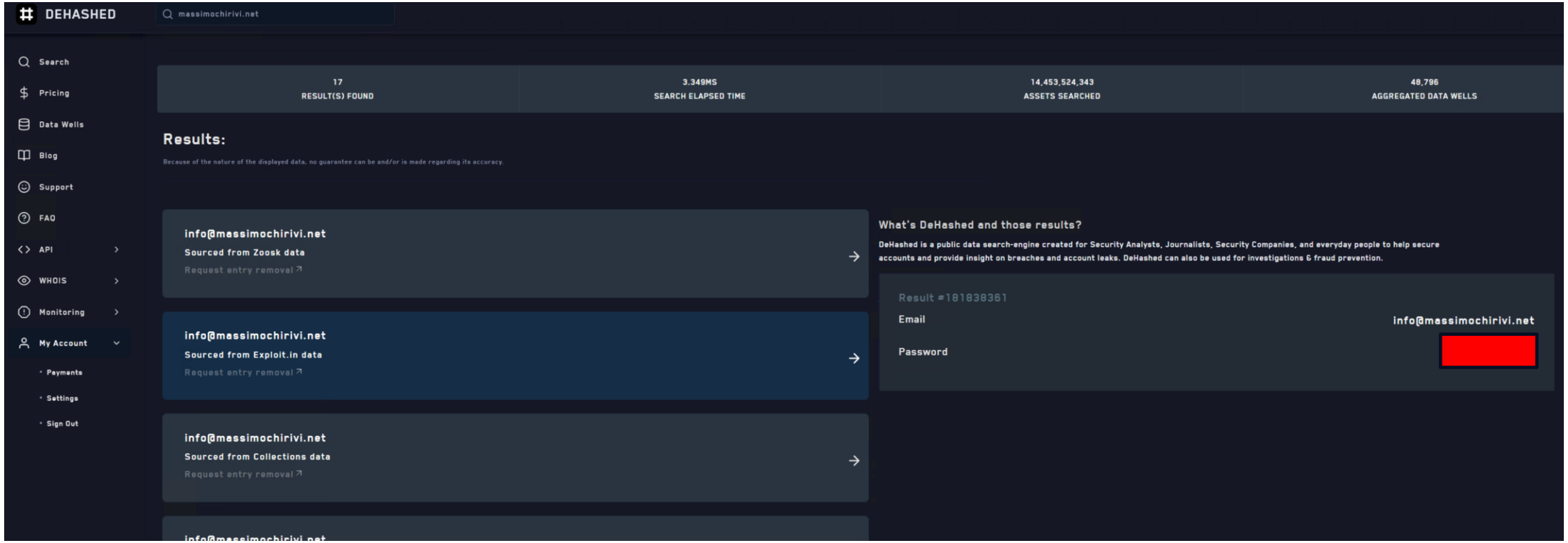
Per tendere alla realtà bisogna conoscere il contesto, il perimetro, la superficie

Una phishing simulation ha senso se viene fatta clonando una webapplication utilizzata dall'azienda e non inviando un phishing su Banca Intesa (ad esempio) se Banca Intesa non viene utilizzata dall'azienda.
Questo è solo un esempio!

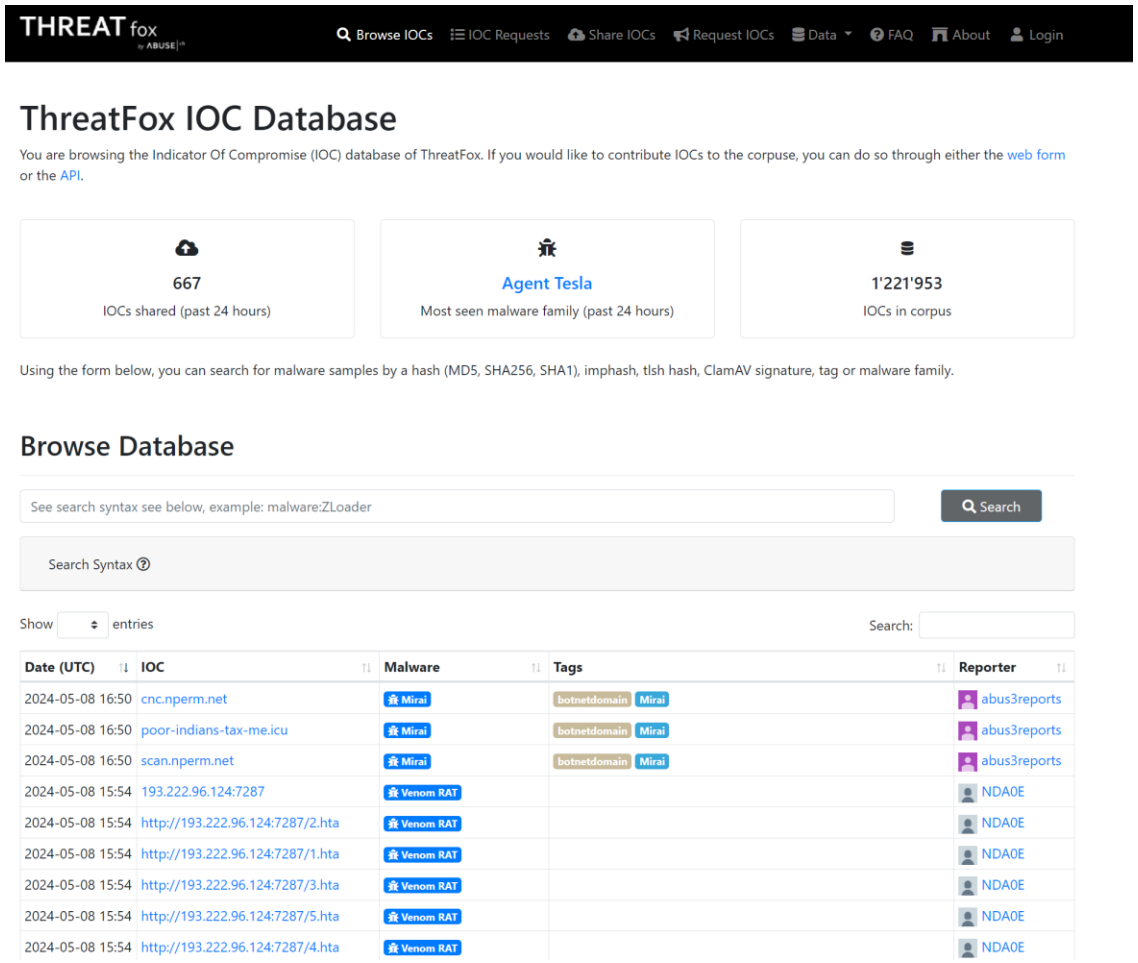
Se il dipendente Mario Rossi ogni sera va in palestra, conosciamo un abitudine e quindi un qualcosa legato a quell'abitudine potrebbe avere successo… e così via…

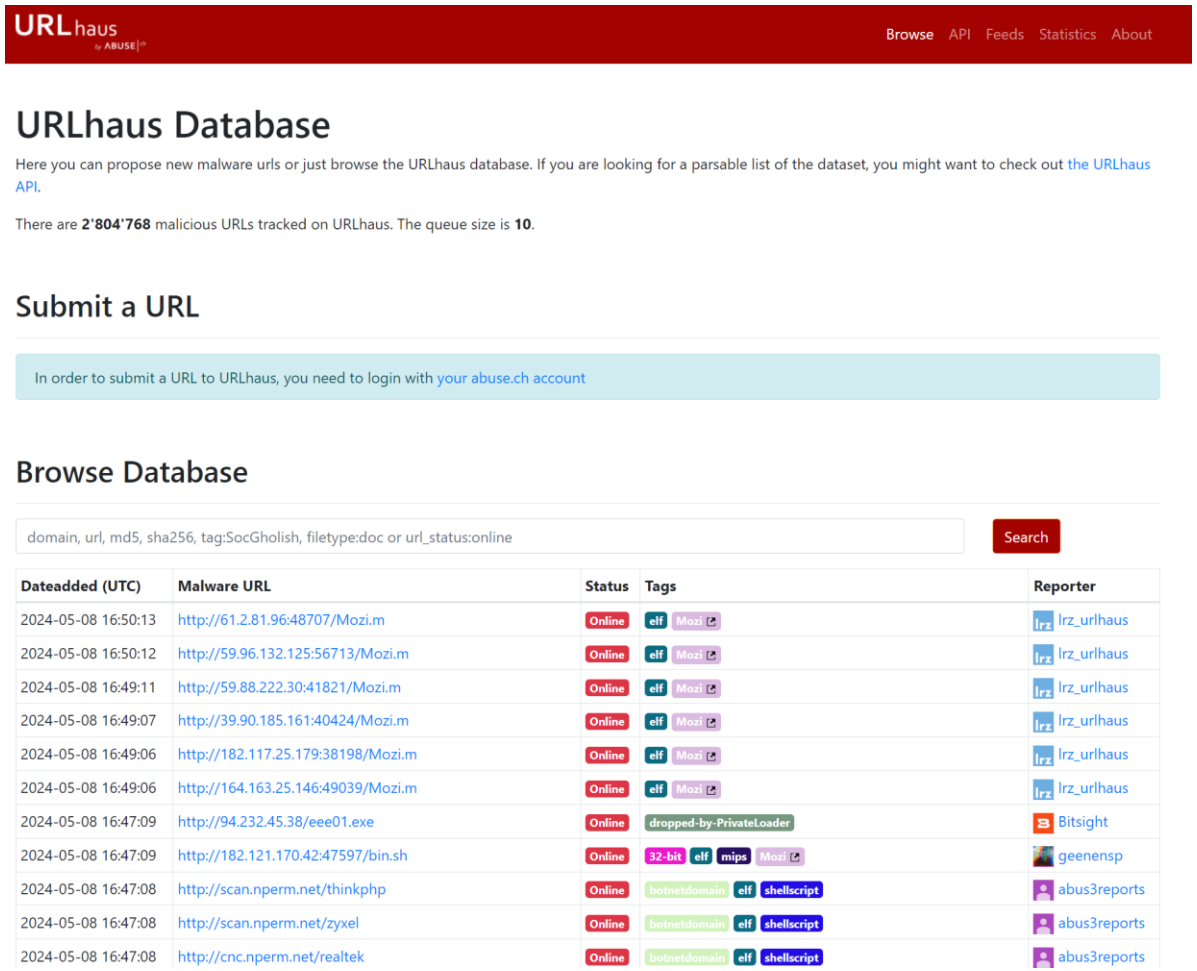
E' IMPORTANTE ANALIZZARE ED ADATTARSI BENE AL CONTESTO!

STRUMENTI DI LEAK ANALISYS



STRUMENTI DI CYBER THREAT INTELLIGENCE





RITORNIAMO AI PROCESSI AZIENDALI CHE NON GESTIAMO CORRETTAMENTE.

1. Dove ci siamo registrati?
2. Dove stiamo inserendo dati aziendali?
3. Chi effettua registrazioni?
4. Dove sono i nostri dati aziendali?
5. Possono essere cancellati? Ora ci sono tecnologie e sistemi che impediscono la cancellazione, a chiunque!
6. Chi sono gli utenti coinvolti?
7. Conosciamo veramente i dati che possediamo?
8. Conosciamo veramente chi possiede i nostri dati?
9. Conosciamo veramente con chi condividiamo i nostri dati?
10. Conosciamo gli strumenti e le tecnologie che utilizziamo in azienda?

Perché parlarne

Ogni giorno cediamo dati senza accorgercene.
Il confine tra "condividere" e "essere tracciati" è sempre più sottile.

… mi limito a 10 domande. Proviamo a darci una risposta?

LE DOMANDE CHE IN ALCUNI MOMENTI FANNO PAURA.

1. Sei sicuro di non essere mai stato attaccato?
2. Sei sicuro di non aver mai perso dei dati?
3. Sei sicuro di non aver mai subito un furto dei dati?
4. Sei sicuro di non essere mai stato intercettato?
5. Sei sicuro di essere l'unico al mondo con la tua identità digitale?

Privacy ≠ Sicurezza

Sicurezza: proteggere l'accesso.

Privacy: controllare chi sa cosa su di noi.

In comune: il perimetro dei nostri dati.

… questa volta mi limito a 5 domande. Proviamo a darci una risposta?

ATTENZIONE ALLE CONFIGURAZIONI SBAGLIATE

Nessuno ci attacca, ma da soli ci facciamo del male.

Alcuni esempi:

- Cancellazioni accidentali
- Sistemi RAID non gestiti
- Sistemi di Data Loss Prevention inesistenti
- Sistemi di virtualizzazione senza snapshot
- Aggiornamenti falliti
- Configurazioni backup errate
- Apparati non aggiornati
- Esposizioni pubbliche errate

Social engineering
Sim swap, finti SMS di banche, falsi aggiornamenti software.
"La vulnerabilità più grande è la fiducia umana."

Minacce invisibili
Tracker e fingerprinting.
Spyware e stalkerware.
Metadati "traditori".
Phishing e social engineering.

Metadati in una foto
Mostra EXIF con GPS e modello del telefono.

"Anche se l'immagine è innocua, i dati raccontano dove e quando."

Tracker e profilazione
Ogni sito carica decine di script.
Identificano browser, device, abitudini.

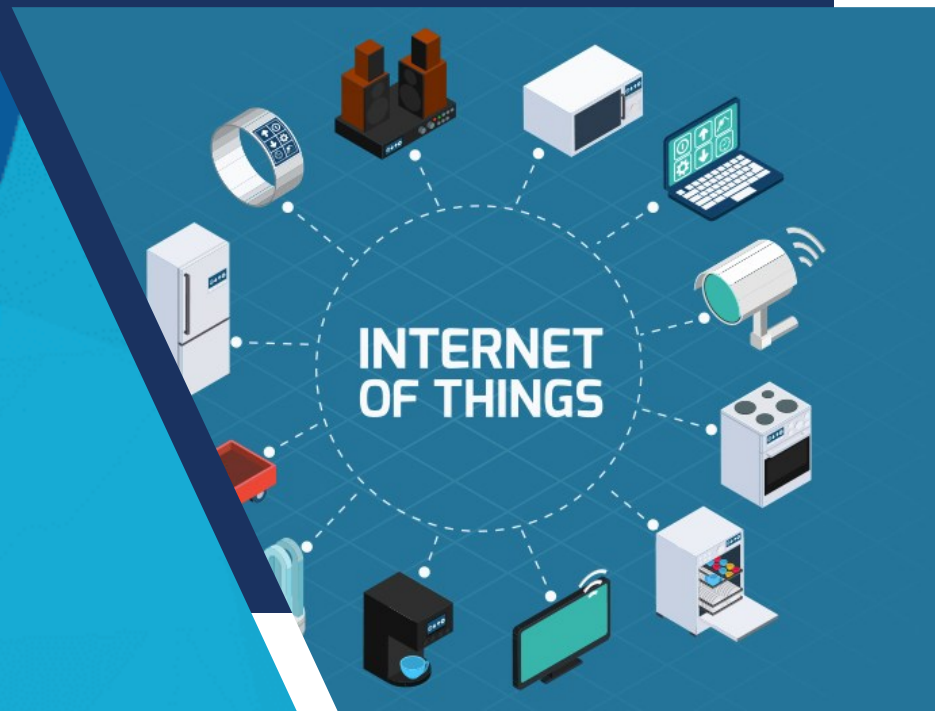
… nessuna domanda ma tanti spunti di riflessione e tanto lavoro da fare in azienda

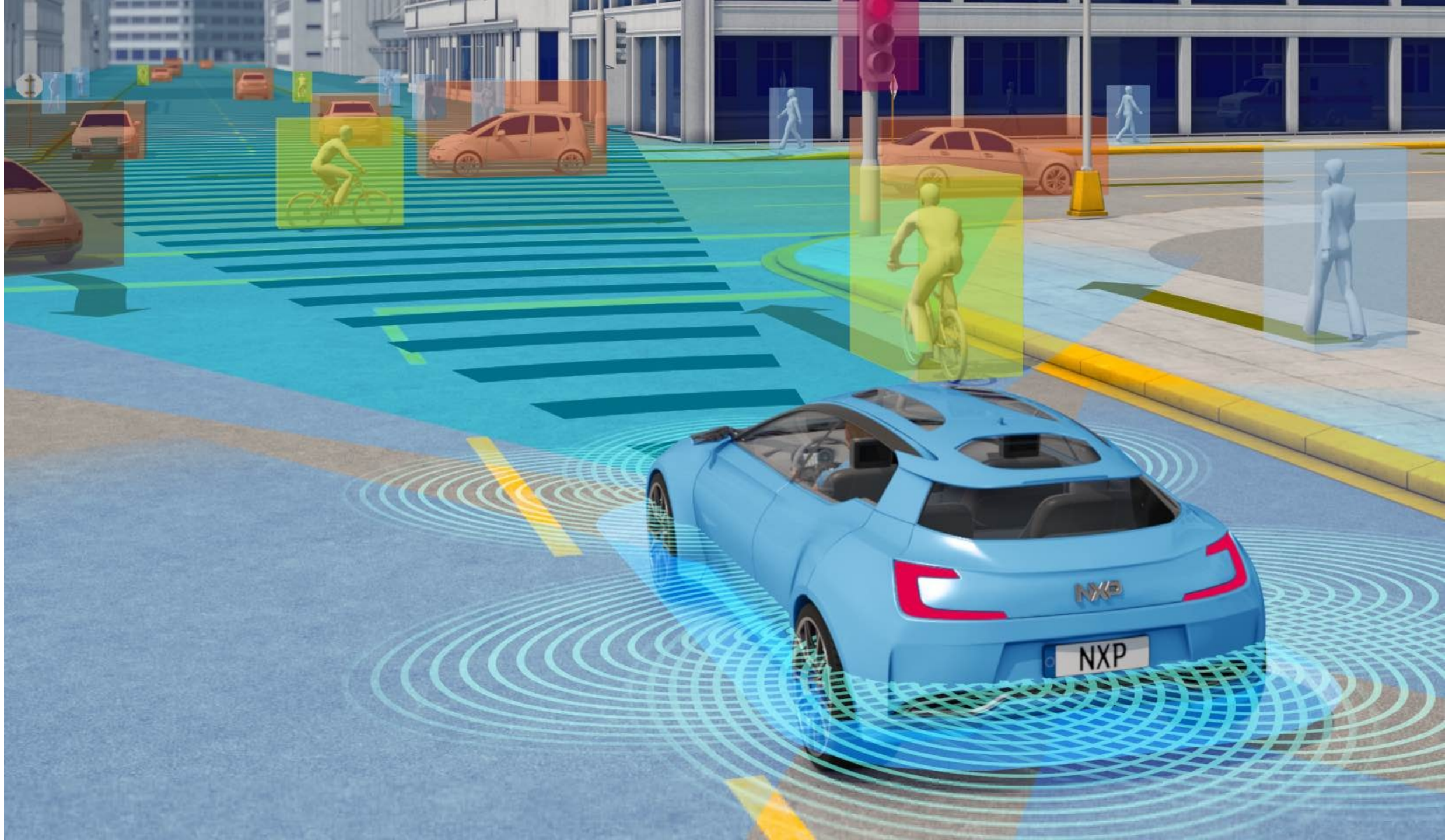
CONCLUSIONI

1. Sei sicuro di non essere mai stato attaccato?
2. Sei sicuro di non aver mai perso dei dati?
3. Sei sicuro di non aver mai subito un furto dei dati?
4. Sei sicuro di non essere mai stato intercettato?
5. Sei sicuro di essere l'unico al mondo con la tua identità digitale?

… questa volta mi limito a 5 domande. Proviamo a darci una risposta?


IOT
INTERNET OF THINGS


INTERNET
OF THINGS


NXP
NXP

IMPERSONATION AND TRUST

DUMPSTER DIVING

TAILGATING AND PIGGY BACKING

IDENTITY FRAUD AND INVOICE SCAMS

Frodi di identità:

- Database di credenziali (i dettagli degli account di attacchi precedenti sono ampiamente disponibili).

- Shoulder surfing (un attore della minaccia può imparare una password o un PIN (o altre informazioni sicure) osservando l'utente mentre li digita).

- Attacchi in pausa pranzo (la maggior parte dei metodi di autenticazione dipende dalla sicurezza fisica della postazione di lavoro).

Grazie!

Non serve essere hacker per difendere la propria privacy: serve solo imparare a vedere ciò che di solito è invisibile.

Vi aspetto in rete!