



HACKING E PRIVACY: MINACCE INVISIBILI E DIFESE CONSAPEVOLI

MASSIMO CHIRIVÌ – 23/10/2025 – FIRENZE

- 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.

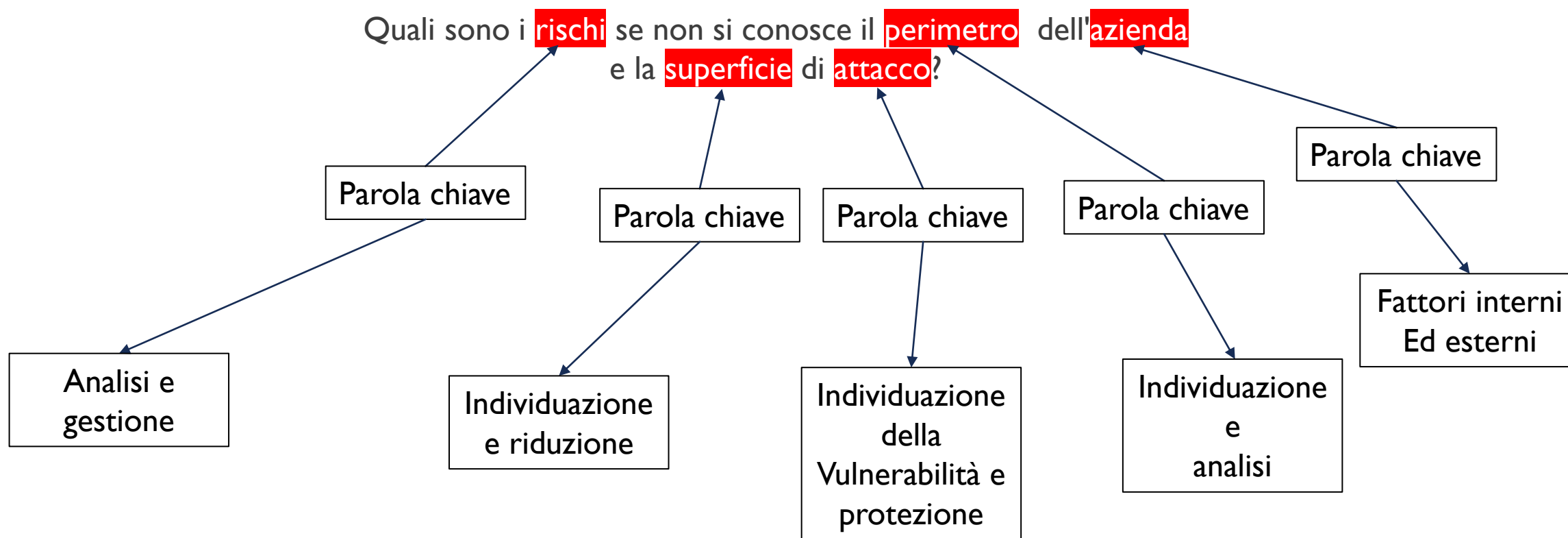
Ethical Hacking (White Hat) ≠ Hacking (Black Hat)

FOCUS sul MODUS OPERANDI!



ABOUT ME (SINTETICA)

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

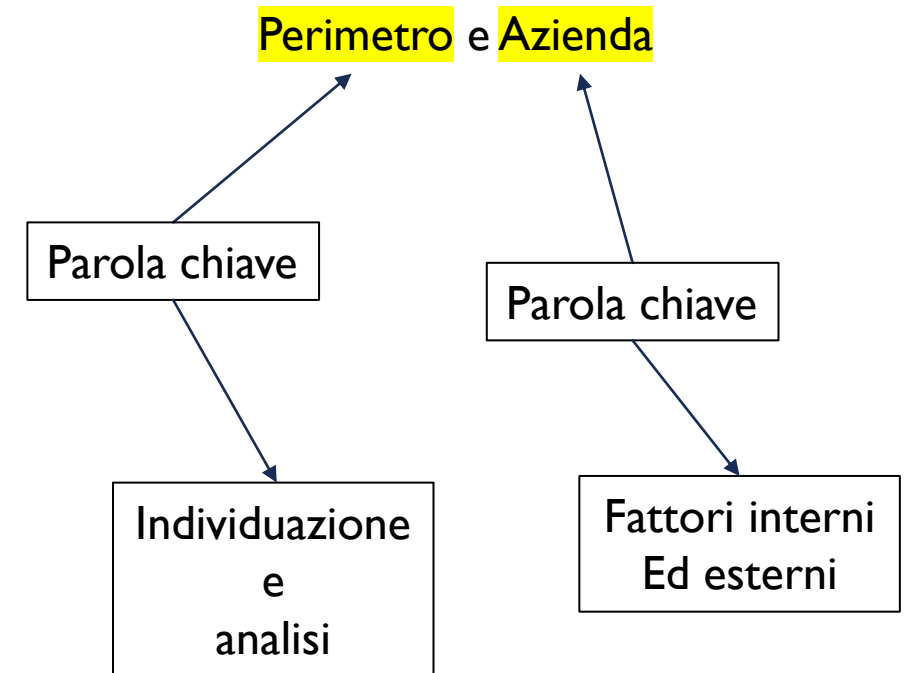
Numero dipendenti: 50 in ufficio + 250 in produzione

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**

catena di approvvigionamento di
prodotto o servizio

Si apre uno scenario incredibile...

Abbiamo introdotto solo un altro termine: **superficie**

ANALISI DELLA SUPERFICIE (DI ATTACCO)



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?

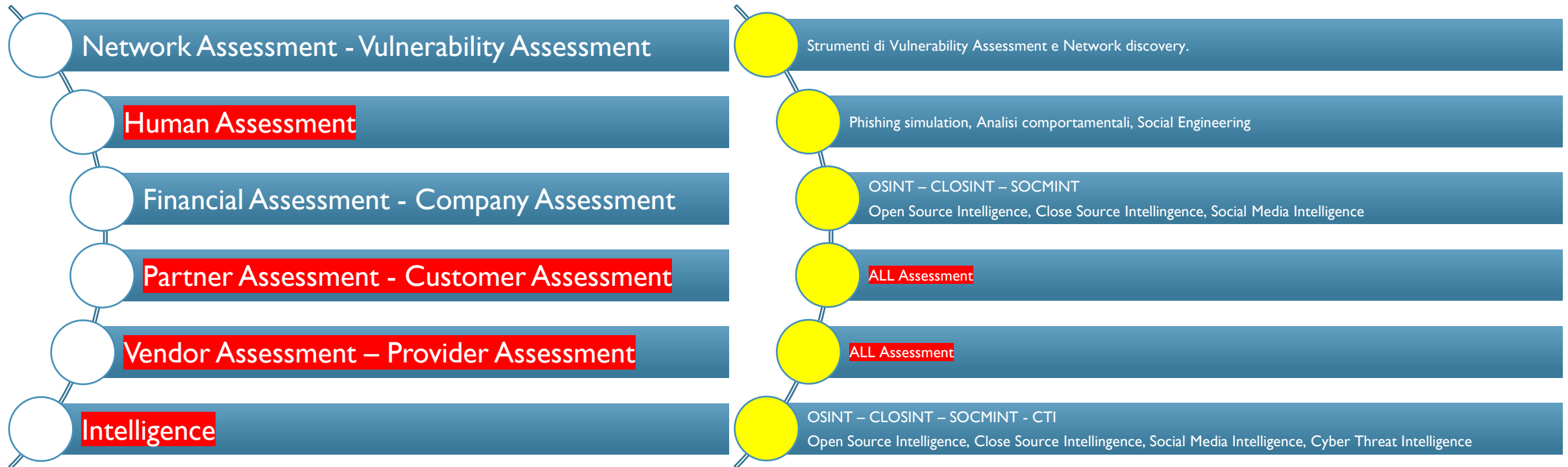
Qui il «gioco» diventa complesso!

E bisogna avere obbligatoriamente una

«mentalità hacker, bisogna vedere oltre...»

per andare a fondo e fare le analisi correttamente.

COSA BISOGNA FARE?



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

DEHASHED

massimochirivi.net

Search

Pricing

Data Wells

Blog

Support

FAQ

API

WHOIS

Monitoring

My Account

- Payments
- Settings
- Sign Out

17
RESULT(S) FOUND

3.349MS
SEARCH ELAPSED TIME

14,453,524,343
ASSETS SEARCHED

48,796
AGGREGATED DATA WELLS

Results:

Because of the nature of the displayed data, no guarantee can be and/or is made regarding its accuracy.

info@massimochirivi.net

Sourced from Zoosk data

Request entry removal

→

info@massimochirivi.net

Sourced from Exploit.in data

Request entry removal

→

info@massimochirivi.net

Sourced from Collections data

Request entry removal

→

info@massimochirivi.net

What's DeHashed and those results?

DeHashed is a public data search-engine created for Security Analysts, Journalists, Security Companies, and everyday people to help secure accounts and provide insight on breaches and account leaks. DeHashed can also be used for investigations & fraud prevention.

Result #181838361

Email

info@massimochirivi.net

Password

STRUMENTI DI CYBER THREAT INTELLIGENCE

THREATfox
by ABUSE[.]ch

[Browse IOC](#) [IOC Requests](#) [Share IOC](#) [Request IOC](#) [Data](#) [FAQ](#) [About](#) [Login](#)

ThreatFox IOC Database

You are browsing the Indicator Of Compromise (IOC) database of ThreatFox. If you would like to contribute IOCs to the corpuse, you can do so through either the [web form](#) or the [API](#).



667

IOCs shared (past 24 hours)



Agent Tesla

Most seen malware family (past 24 hours)



1'221'953

IOCs in corpus

Using the form below, you can search for malware samples by a hash (MD5, SHA256, SHA1), imphash, tlsh hash, ClamAV signature, tag or malware family.

Browse Database

See search syntax see below, example: malware:ZLoader

Search

Search Syntax ?

Show 1 entries

Search:

Date (UTC)	IOC	Malware	Tags	Reporter
2024-05-08 16:50	cnc.nperm.net	Mirai	botnetdomain Mirai	abus3reports
2024-05-08 16:50	poor-indians-tax-me.icu	Mirai	botnetdomain Mirai	abus3reports
2024-05-08 16:50	scan.nperm.net	Mirai	botnetdomain Mirai	abus3reports
2024-05-08 15:54	193.222.96.124:7287	Venom RAT		NDA0E
2024-05-08 15:54	http://193.222.96.124:7287/2.hta	Venom RAT		NDA0E
2024-05-08 15:54	http://193.222.96.124:7287/1.hta	Venom RAT		NDA0E
2024-05-08 15:54	http://193.222.96.124:7287/3.hta	Venom RAT		NDA0E
2024-05-08 15:54	http://193.222.96.124:7287/5.hta	Venom RAT		NDA0E
2024-05-08 15:54	http://193.222.96.124:7287/4.hta	Venom RAT		NDA0E

URLhaus
by ABUSE[.]ch

[Browse](#) [API](#) [Feeds](#) [Statistics](#) [About](#)

URLhaus Database

Here you can propose new malware urls or just browse the URLhaus database. If you are looking for a parsable list of the dataset, you might want to check out [the URLhaus API](#).

There are **2'804'768** malicious URLs tracked on URLhaus. The queue size is **10**.

Submit a URL

In order to submit a URL to URLhaus, you need to login with [your abuse.ch account](#)

Browse Database

domain, url, md5, sha256, tag:SocGholish, filetype:doc or url_status:online

Search

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2024-05-08 16:50:13	http://61.2.81.96:48707/Mozi.m	Online	elf Mozi	lrz_urlhaus
2024-05-08 16:50:12	http://59.96.132.125:56713/Mozi.m	Online	elf Mozi	lrz_urlhaus
2024-05-08 16:49:11	http://59.88.222.30:41821/Mozi.m	Online	elf Mozi	lrz_urlhaus
2024-05-08 16:49:07	http://39.90.185.161:40424/Mozi.m	Online	elf Mozi	lrz_urlhaus
2024-05-08 16:49:06	http://182.117.25.179:38198/Mozi.m	Online	elf Mozi	lrz_urlhaus
2024-05-08 16:49:06	http://164.163.25.146:49039/Mozi.m	Online	elf Mozi	lrz_urlhaus
2024-05-08 16:47:09	http://94.232.45.38/eee01.exe	Online	dropped-by-PrivateLoader	Bitsight
2024-05-08 16:47:09	http://182.121.170.42:47597/bin.sh	Online	32-bit elf mips Mozi	geenensp
2024-05-08 16:47:08	http://scan.nperm.net/thinkphp	Online	botnetdomain elf shellscript	abus3reports
2024-05-08 16:47:08	http://scan.nperm.net/zyxel	Online	botnetdomain elf shellscript	abus3reports
2024-05-08 16:47:08	http://cnc.nperm.net/realtek	Online	botnetdomain elf shellscript	abus3reports

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 $\neq$ 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

Metadati in una foto

Mostra EXIF con GPS e modello del telefono.

“Anche se l’immagine è innocua, i dati raccontano dove e quando.”

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.

Tracker e profilazione

Ogni sito carica decine di script.

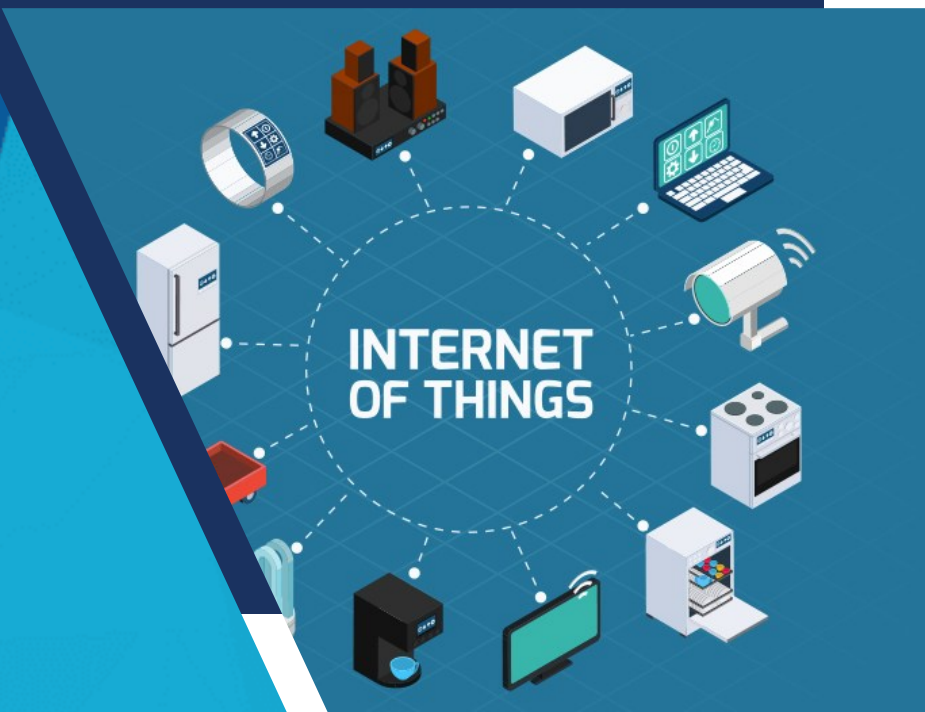
Identificano browser, device, abitudini.

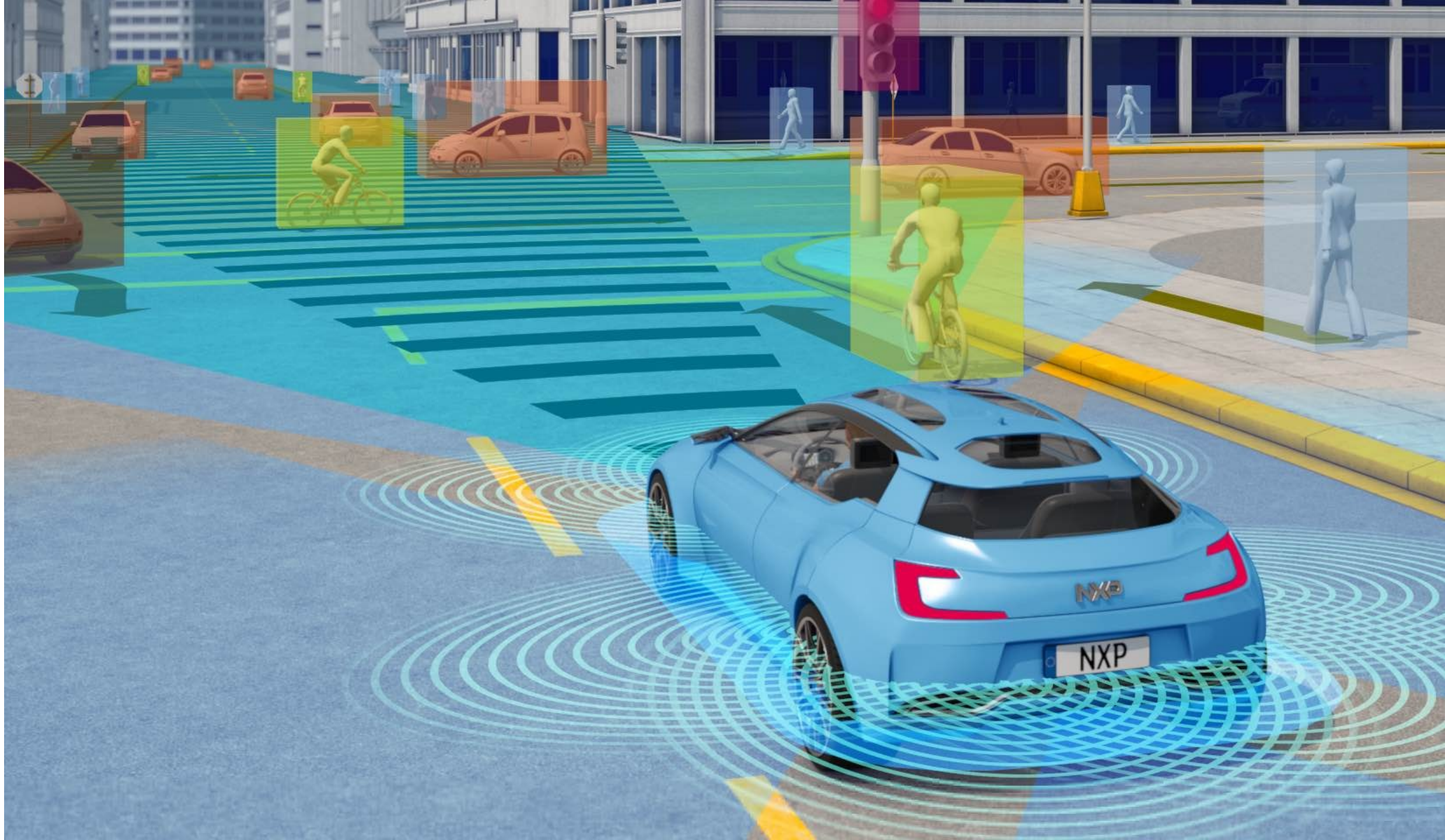
... nessuna domanda ma tanti spunti di riflessione e tanto lavoro da fare in azienda

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?







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!

