CYBER SECURITY

Check your business

Namirial

DRCNETWORK.IT
by Namirial

CyberExpert

PERCHE'
CYBER THREAT ASSESSMENT (CTA)?

Namirial

DRCNETWORK.IT
by Namirial

Vantaggi del Servizio CyberExpert

CyberExpert

Nessun software da installare

CyberExpert è una piattaforma web pronta all'uso: nessun software da installare con notevole risparmio di tempo e di investimenti.

Semplicità di utilizzo

Attiva la piattaforma attraverso la tua identità digitale SPID, inserisci i dati richiesti

- indirizzo IP pubblico
- email
- dominio
- indirizzo web

e pianifica l'analisi.

Appena pronto, CyberExpert invierà il report direttamente al tuo indirizzo email.

Report intuitivi

I report generati da CyberExpert sono completi e di facile comprensione. Evidenziano le vulnerabilità della tua infrastruttura informativa, segnalano la presenza di tuoi dati nel deep web, di data breach, di malware e ti guidano nelle azioni di contrasto.

Namirial

DRCNETWORK.IT by Namirial

Caratteristiche del Servizio CTA CyberExpert

CyberExpert

PERCHE' UTILIZZARE CTA: →

- Rileva le minacce informatiche.
- Rileva gli incidenti occorsi all'interno dell'organizzazione.
- Rileva le vulnerabilità dei sistemi e dei servizi esposti sulla rete pubblica.

A COSA SERVE: →

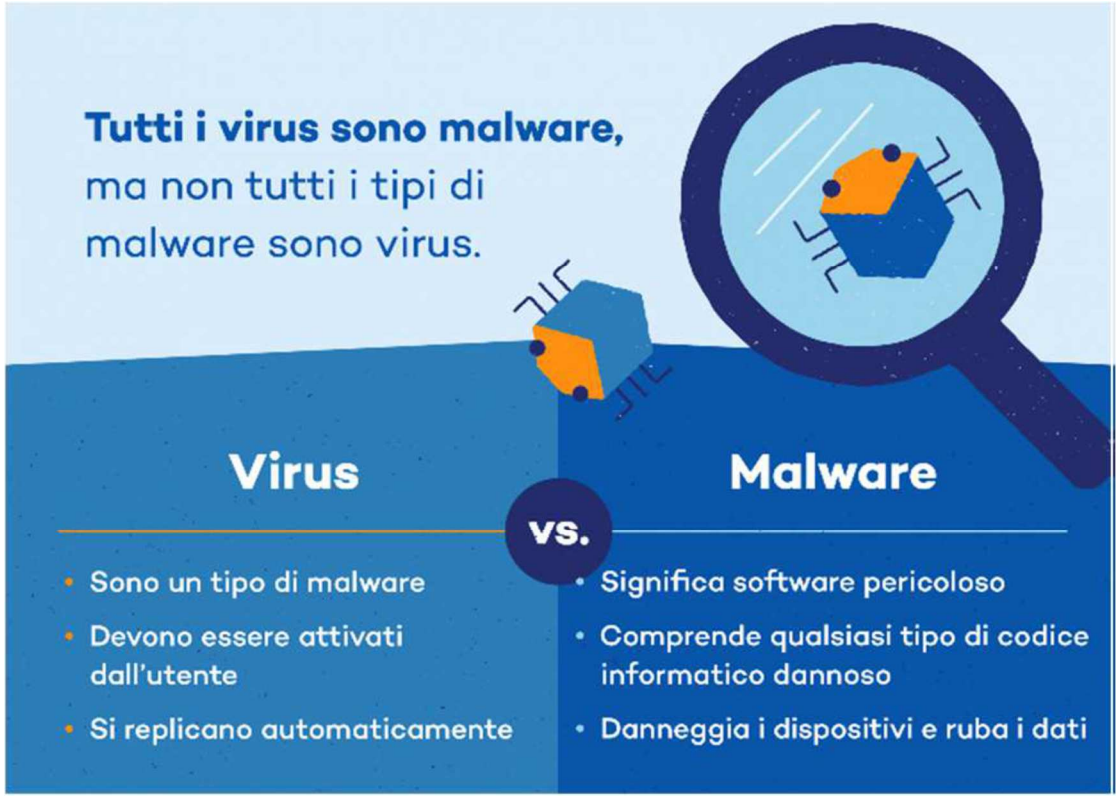
- Scoprire e porre rimedio alle minacce informatiche relative alle infezioni da malware.
- Identificare credenziali trapelate (data breach).
- Identificare violazioni di dati attraverso l'analisi del deep web.
- Identificare trasferimenti di dati pericolosi e/o che violano diritti d'autore su reti peer-to-peer.
- Identificare e dare priorità alla riparazione delle vulnerabilità.

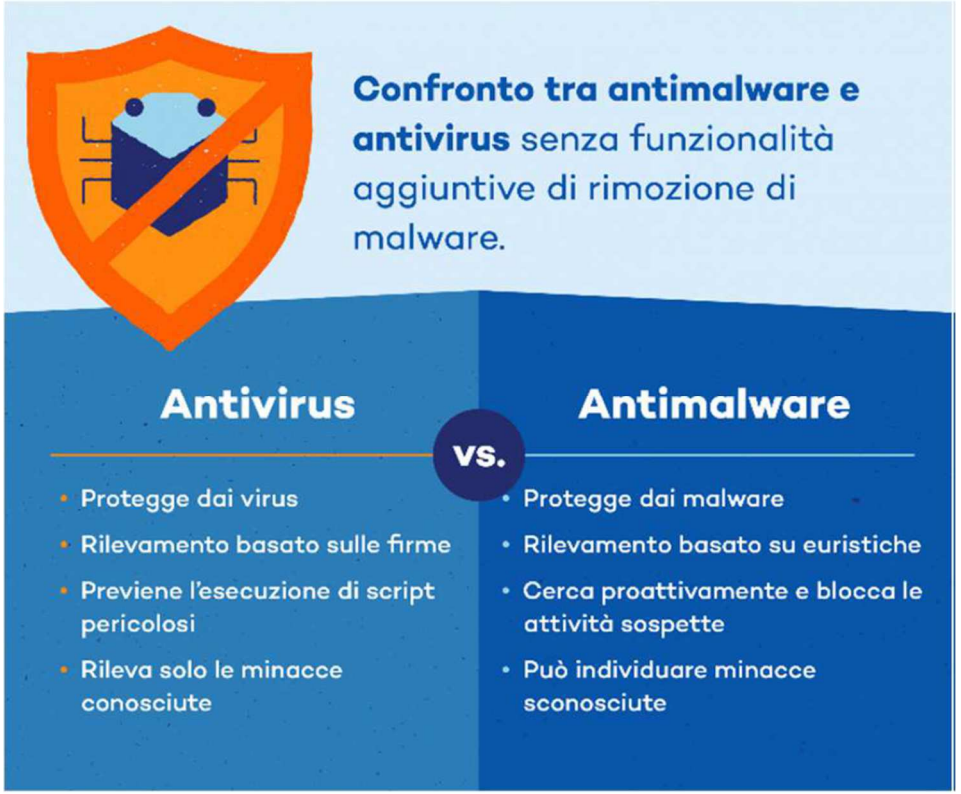
A CHI SI RIVOLGE: →

- Ai Professionisti ed alle Aziende per fare l'analisi delle minacce informatiche al fine di individuare e/o prevenire le violazioni dei dati (anche sensibili).
- A chi deve ottemperare agli obblighi dell'articolo 32, paragrafo 1, lettera d) del GDPR.

Antivirus ed Antimalware a Confronto

CyberExpert





Namirial

DRCNETWORK.IT by Namirial

Antivirus ed Antimalware a Confronto

CyberExpert

Antivirus e antimalware non sono la stessa cosa. Sono due componenti imprescindibili e complementari di un buon sistema di protezione da programmi dannosi, a cui dobbiamo aggiungere anche l'adozione di buone abitudini online. I software antimalware sono in grado di rilevare forme avanzate di malware e minacce informatiche, ad esempio gli **attacchi zero-day**, mentre l'efficacia degli antivirus dipende al 100% dalla qualità del database di riferimento.

Che cosa significa esattamente antivirus?

I programmi antivirus semplici eseguono una scansione del dispositivo alla ricerca di virus conosciuti. Di solito, gli **antivirus gratuiti** offrono un livello di protezione minimo contro i virus più noti come i **keylogger** e gli **worm**, mentre le **versioni premium** proteggono anche da minacce più avanzate e, come abbiamo visto, includono funzionalità antimalware.

Che cos'è un programma antimalware?

I programmi dannosi si evolvono continuamente, proprio come qualsiasi altro ambito del software. Gli antimalware vengono sviluppati pensando alle **nuove minacce e i nuovi meccanismi di infezione digitale**. In un certo senso, possiamo dire che **gli antimalware ci proteggono dal malware di seconda generazione**, che gli antivirus classici non sono in grado di individuare.

CyberExpert

DOMANDE FREQUENTI

Namirial

DRCNETWORK.IT by Namirial

CyberExpert

Che Report genera il CTA (Cyber Threat Assessment)?
Il CTA genera 3 report distinti:

Semafori (Traffic Light Report):
Il Report Semaforo riassume tutte le minacce informatiche in una pagina in modo visuale e intuitivo. Contiene tre semafori con i relativi colori, rosso, giallo o verde in base alla presenza e alla gravità delle minacce afferenti alle seguenti aree principali:

- sicurezza delle postazioni di lavoro,
- sicurezza della posta elettronica,
- sicurezza perimetrale Internet.

Tale report viene fornito per analisi fino a 20 indirizzi email.

Executive (Summary Cyber Threat Assessment Executive Report):
Da evidenza delle risultanze dell'assessment organizzate per macroaree:

- Infezioni Malware
- Data Breach
- File Sharing
- Vulnerabilità

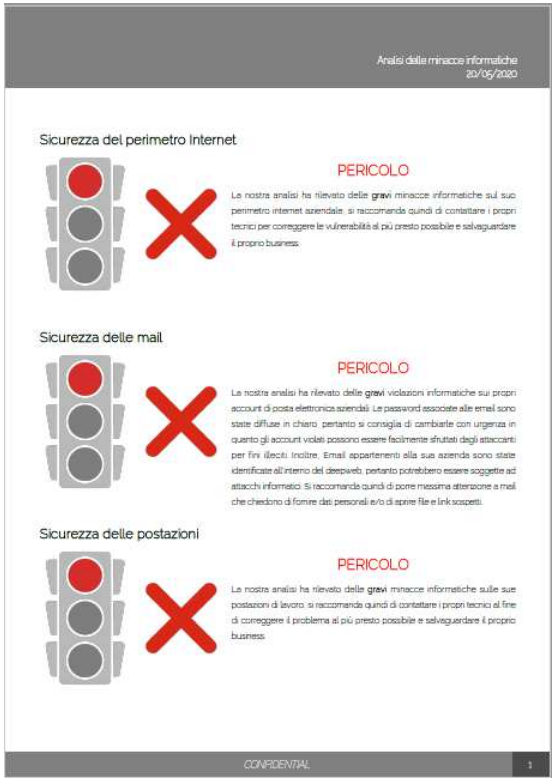
Report completo (Cyber Threat Assessment Report):
Questo report prende in esame la superficie di attacco, le vulnerabilità tecniche, l'esposizione di asset aziendali su deepweb, dati di account divulgati attraverso data breach di terze parti, infezioni da malware, utilizzo di protocolli insicuri.

Esempi di Report del Servizio CyberExpert

CyberExpert

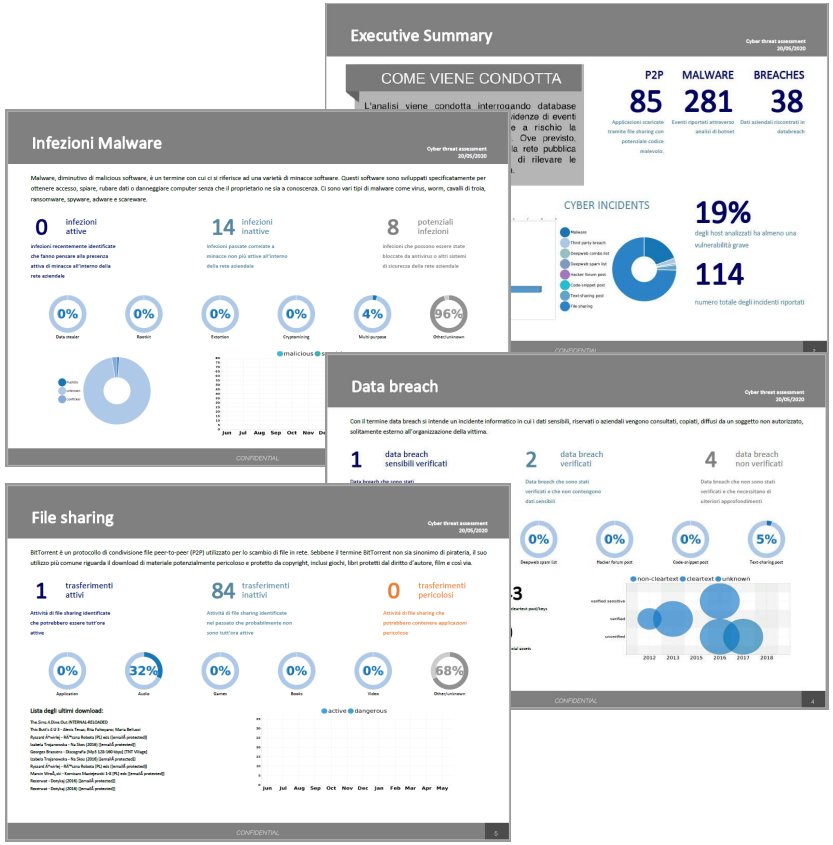
Traffic Light Report

Sintetizza tutti i risultati delle analisi tecniche in un'unica vista con 3 semafori che assumono colore rosso, giallo o verde in base alla presenza di minacce relative a tre aree fondamentali della sicurezza logica: sicurezza delle postazioni, sicurezza delle mail, sicurezza del perimetro internet.



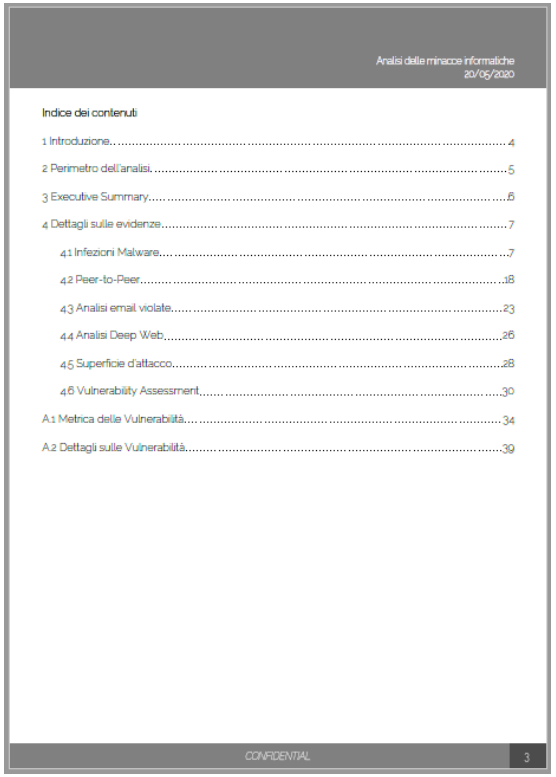
Cyber Threat Assessment Executive Report

Rappresenta in modo grafico la sintesi delle evidenze riscontrate dalle analisi tecniche.



Cyber Threat Assessment Report

Riporta analiticamente tutti i dettagli relativi alle evidenze riscontrate dalle analisi tecniche e permette all'utente di



Namirial

DRCNETWORK.IT by Namirial

Quali sono i parametri richiesti dalla piattaforma su cui è possibile eseguire un'analisi?

Si definiscono Assets:

- Indirizzi IP di rete
- Indirizzi Emails
- Domini
- Fully Qualified Domain Names

Come trovo il mio indirizzo IP?

Un metodo molto semplice per controllare: andate in http://www.mio-ip.it/

Come faccio a sapere se ho un indirizzo IP pubblico statico o dinamico?

Un metodo molto semplice per controllare: andate in http://www.mio-ip.it/ e verificate il vostro IP. Spegnete il modem/router ed aspettate circa un minuto. Riaccendete il router e ricontrollate l'IP: se è cambiato siete in presenza di un IP dinamico.

Esiste un modo per caricare in modo massivo indirizzi email?

Attualmente non è possibile caricare massivamente gli assets

È possibile analizzare un indirizzo email pec o Gmail, Yahoo etc?

Si è possibile.

Devo obbligatoriamente inserire tutti gli assets (Indirizzo IP, E-mail, Nome Dominio, Fully Qualified Domain Name) richiesti dalla piattaforma per poter effettuare l'assessment?

No non è necessario. Gli elementi necessari per per poter effettuare l'assessment CTA sono l'indicazione almeno di (1 indirizzo e-mail o 1 dominio) e (1 indirizzo IP o 1 Fully Qualified Domain Name). Gli elementi necessari per per poter effettuare l'assessment VA sono l'indicazione almeno di 1 indirizzo IP o 1 Fully Qualified Domain Name. Per l'esecuzione di un'analisi completa è comunque auspicabile che tutti gli assets siano

Quanto ci impiega la piattaforma ed effettuare l'assessment?

Non esiste una tempistica standard. Il tempo impiegato è legato al numero di assets inseriti e ai risultati che vengono raccolti nella fase iniziale della scansione.

La scansione non è terminata. Cosa è successo?

Se la piattaforma non riesce a terminare la scansione nell'intervallo temporale indicato, riprende le attività il giorno dopo nello stesso intervallo di tempo.

Che cos'è un Fully Qualified Domain Names?

Il termine "Fully Qualified Domain Name", in breve FQDN, indica l'indirizzo completo e univoco di un'entità Internet. È composto dal nome dell'host e dal dominio e viene utilizzato per localizzare specifici host su Internet e accedervi tramite la risoluzione del nome.

Devo obbligatoriamente inserire gli indirizzi e-mail?

Non è necessario inserire gli indirizzi e-mail. Se non vengono inseriti non si avrà evidenza di quale e-mail risulta coinvolta in breach/deepweb ma solo una mascheratura del tipo gpdr-masking@dominio.tld

Devo obbligatoriamente inserire un indirizzo IP per poter effettuare l'assessment?

No non è necessario ma per l'esecuzione di un'analisi completa è auspicabile che questo asset sia dichiarato.

Che cos'è il deep web?

Il web sommerso (in inglese deep web, web profondo") è l'insieme delle risorse informative del World Wide Web (www) non indicizzate dai normali motori di ricerca. Per spiegare la mole di dati presente nel deep web si utilizza la metafora dell'iceberg, dove la parte al di sopra dell'acqua corrisponde a tutte le pagine del web indicizzate dai motori di ricerca: il cosiddetto web accessibile; mentre la parte sostanziale dell'iceberg si trova sommersa e corrisponde al web sommerso.

Che cos'è il dark web?

Il dark web (in italiano: web oscuro o rete oscura) è la terminologia che si usa per definire i contenuti del World Wide Web nelle darknet (reti oscure) che si raggiungono via Internet attraverso specifici software, configurazioni e accessi autorizzativi.

Qual è la differenza tra deep web e dark web

I deep web è quella parte del World Wide Web non indicizzata dai comuni motori di ricerca. Di questa categoria fanno quindi parte nuovi siti non ancora indicizzati, pagine web a contenuto dinamico, web software e siti privati aziendali. Il dark web è un sottoinsieme del deep web, solitamente irraggiungibile attraverso una normale connessione Internet senza far uso di software particolari perché giacente su reti sovrapposte ad Internet chiamate genericamente darknet.

Cosa sono le reti Peer-to-Peer?

Le reti Peer-to-Peer (P2P) sono un tipo di reti decentralizzate e composte da centinaia e persino milioni di computer dislocati in tutto il mondo. Il protocollo di condivisione file Peer-to-Peer (P2P) utilizzato per lo scambio di file in rete è BitTorrent. Sebbene il termine BitTorrent non sia sinonimo di pirateria, il suo utilizzo più comune riguarda il download di materiale potenzialmente pericoloso e protetto da copyright, inclusi giochi, libri protetti dal diritto d'autore, film e così via.

Che cos’è un data breach?

Con il termine data breach si intende un incidente di sicurezza in cui dati sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato. Solitamente il data breach si realizza con una divulgazione di dati riservati o confidenziali all’interno di un ambiente privo di misure di sicurezze (da esempio, su web) in maniera involontaria o volontaria. Tale divulgazione può avvenire in seguito a:

- perdita accidentale: ad esempio, data breach causato da smarrimento di una chiavetta USB contenente dati riservati
- furto: ad esempio, data breach causato da furto di un notebook contenente dati confidenziali
- infedeltà aziendale: ad esempio, data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico
- accesso abusivo: ad esempio, data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite

Perché il mio indirizzo e-mail si trova nel deep web?

La presenza del tuo indirizzo e-mail significa che sei stato oggetto di attacco ed hai lasciato la tua email con le credenziali in qualche sito non sicuro.

Cosa significa che il mio indirizzo e-mail si trova nel deep web?

Essere presenti non vuol dire che ti accadrà inevitabilmente qualcosa di brutto ma potrebbe essere più difficile evitare email di spam. Inoltre, potresti essere inserito in campagne di phishing, in cui criminali informatici assumono l'identità di un'azienda o di un contatto fidato per indurti a divulgare informazioni di carattere personale. È meglio farsi trovare pronti nel caso in cui qualcuno tenti di truffarti o di accedere ai tuoi account.

Cosa devo fare se la mia e-mail si trova nel deep web?

Qualsiasi cosa succeda, la prima cosa da fare è rimanere calmi. Ci sono diversi accorgimenti che puoi adottare fin da subito per ridurre il rischio. Agendo rapidamente, puoi impedire che un ladro di identità abusi dei tuoi dati e attenuare eventuali danni in cui potresti incorrere:

- Cambia le password;
- Avvisa eventuali operatori finanziari che hanno questa casella nel tuo profilo
- Presenta le prove. Qualora ti venga richiesto presenta il report ottenuto con Namirial
- Aumenta la sicurezza informatica utilizzando dei software dedicati e/o attivando un doppio fattore di autenticazione qualora sia possibile