Swascan
TINEXTA GROUP

SWASCAN

The
CYBER
SECURITY
PARTNER

The Threat Intelligence
Platform

Cyber Security
Competence Services

The First Cyber Security
Testing Platform

Cyber Risk Indicators di:
nomeazienda.it

Cyber Security ACTION PLAN
ROAD MAP

info@swascan.com
swascan.com
In collaboration with **CISCO**

MISURA Il tuo RISCHIO CYBER!

Il servizio di **Domain Threat Intelligence** permette di valutare ed identificare il rischio di **CYBER ATTACK e RANSOMWARE ATTACK** di una azienda in base alle informazioni che sono già disponibili nel Web, Dark Web e Deep Web. Informazioni che terzi hanno pubblicato e di conseguenza accessibili e disponibili a tutti.

Si tratta di un servizio di "security intelligence" che effettua una ricerca delle informazioni pubbliche e semipubbliche relative alle vulnerabilità del dominio, sottodomini ed e-mail compromesse. Il servizio non effettua alcun test diretto sul target, opera unicamente sulle informazioni disponibili a livello OSINT e CLOSINT.

L'attività di Domain Threat Intelligence viene effettuata su target e identificavi digitali relativi agli asset ed alle e-mail compromesse. L'attività è condotta attraverso la ricerca, individuazione e selezione delle informazioni disponibili pubblicamente relative al dominio, sottodomini ed e-mail compromesse.

Il servizio non effettua alcun test di sicurezza sul target, opera unicamente sulle informazioni raccolte a livello OSINT e CLOSINT e disponibili sul Dark Web.

OSINT: acronimo di Open Source Intelligence, si fa riferimento al processo di raccolta d'informazioni attraverso la consultazione di fonti di pubblico dominio definite anche «fonti aperte» impatti.

CLOSINT: Close Source Intelligence, processo di raccolta d'informazioni attraverso consultazione di «fonti chiuse», non accessibili al pubblico o aree «riservate».

Swascan
TINEXTA GROUP

Lo stato dell'arte del RISCHIO CYBER di

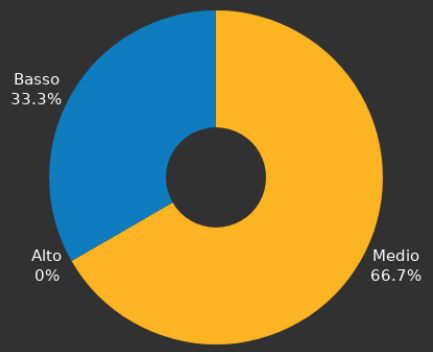
nomeazienda.it

IL RISCHIO CYBER di *nomeazienda.it*

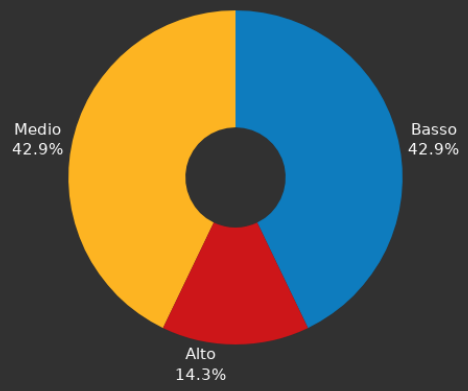
Vulnerabilità potenziali totali	Alta Severità	Media Severità	Bassa Severità
12	2	8	2

IP Totali trovati	Sottodomini Totali trovati	Emails compromesse	Fonti delle Breach
3	4	7	7

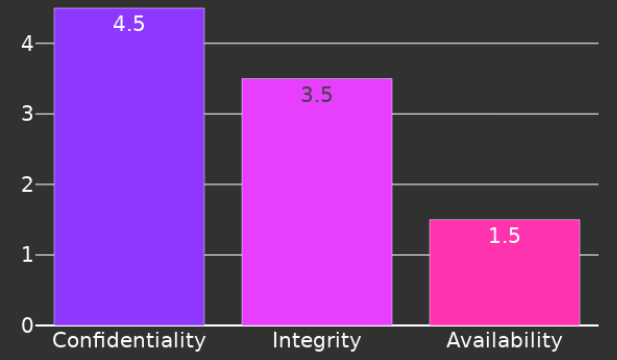
Rischio Tecnologico (Potenziali vulnerabilità per rischio)



Human Risk (Breaches per rischio)



GDPR Risk (Impatto su Confidentiality, Availability e Integrity)



Cyber Risk Indicators: Technology Risk

Vulnerabilità potenziali totali	Alta Severità	Media Severità	Bassa Severità
12	2	8	2

Terze parti hanno indicato pubblicamente la presenza di **12 potenziali vulnerabilità** presenti sul perimetro esposto su internet a livello di dominio e sottodominio. Vulnerabilità che se sfruttate e sfruttabili potrebbero compromettere i servizi e permettere a terzi di accedere direttamente all'interno dell'infrastruttura aziendale per:

- Un attacco ransomware
- Esfiltrare i dati
- Interrompere l'operabilità dei sistemi

ACTION PLAN

- Attività di Penetration Test a livello infrastrutturale e applicativo
- Attività di Network Scan della rete interna
- Attività di Active Directory Assessment
- ISO27001 Assessment
- Web Application Firewall
- Security Operation Center

Cyber Risk Indicators: Social Engineering

E-mail compromesse

7

Sono state identificate 7 e-mail compromesse. Parliamo di e-mail e password che i dipendenti hanno usato per registrarsi su siti terzi, siti che hanno subito un data breach e di conseguenza le credenziali (e-mail/password) sono diventate pubbliche.

I rischi sono:

- **Phishing e Spear Phishing**: le mail possono essere usate per campagne mirate di Phishing. Campagne customizzate utilizzando anche dalle ulteriori informazioni rilasciate sui siti terzi (data di nascita, cellulari, indirizzi fisici…)
- **Account Take Over:** furto dell'identità, in particolare gli account social. In questo modo è possibile inviare messaggi con link malevoli ai propri contatti
- **Credential Stuffing**: utilizzo delle credenziali per accedere ai servizi esposti su internet (VPN, webmail, gestionali,…)

ACTION PLAN

- Attività di Phishing Simulation
- Attività di Formazione e Awareness dei dipendenti
- GDPR Assessment
- Security Operation Center

Cyber Risk Indicators: Superficie di Attacco

IP totali trovati

3

L'attività di Domain Threat Intelligence ha evidenziato che terze parti hanno identificato e mappato:

- 3 IP assegnati all'azienda
- 4 domini e sottodomini aziendali

Sottodomini totali

4

L'attività di Information Gathering permette di determinare la superficie di attacco e rappresenta il primo step del Ransomware Cyber Kill Chain.

ACTION PLAN

- Domain Threat Intelligence
- Cyber Threat Intelligence
- Early warning Giornaliero
- Technology Monitoring

Swascan
TINEXTA GROUP

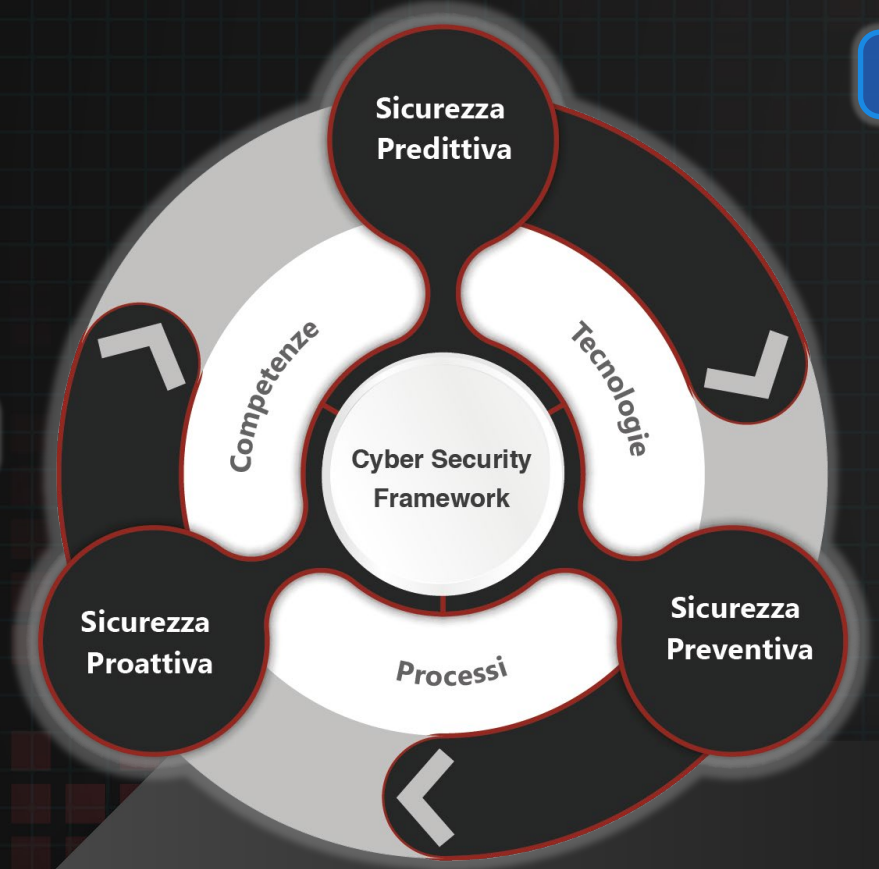
Proposta Progettuale

Cyber Risk Framework

Proposta Progettuale

Sicurezza Predittiva

- Domain Threat Intelligence
- Threat Intelligence
- Early warning Giornaliero



Sicurezza Preventiva

Rischio Tecnologico

- Attività di Penetration Test del perimetro esposto
- Attività di Penetration Test degli applicativi esposti su Internet
- Attività di Network Scan della rete interna
- Attività di Active Directory Assessment
- Technology Monitoring

Human Risk

- Attività di Phishing Simulation
- Attività di Formazione e Awareness dei dipendenti

Organizational Risk

- GDPR Assessment
- ISO27001 Assessment

Sicurezza Proattiva

- SOC as a Service
- Incident Response Team

Swascan
TINEXTA GROUP

SWASCAN

The
CYBER
SECURITY
PARTNER

The Threat Intelligence
Platform

Cyber Security
Competence Services

The First Cyber Security
Testing Platform

Cyber Risk Indicators di:
nomeazienda.it

Cyber Security ACTION PLAN
ROAD MAP

info@swascan.com
swascan.com
In collaboration with **CISCO**