
NETGROUP
CYBERSECURITY
CYBERSECURITY
CYBERSECURITY
CYBERSECURITY

HUMANS FOR CYBERSECURITY

humans for
CYBERSECURITY
DIGITAL TRANSFORMATION

Quando ci approcciamo alla cybersecurity non interveniamo solamente sulle minacce riguardanti la tecnologia ma anche su quelle che prendono di mira le persone. La principale vulnerabilità, infatti, è rappresentata dal fattore umano che è sempre più l'oggetto degli attacchi cyber.

Sempre più spesso si investe in tecnologia senza considerare le necessità dei singoli, gli obiettivi delle aziende, le strategie del Paese.

Il viaggio verso la Cybersecurity non ha come destinazione la tecnologia: quello è soltanto il punto di partenza. Alla meta si giunge con l'allineamento fra strategia d'impresa e strategia per la sicurezza IT.

METODOLOGIA

Progettiamo e realizziamo servizi e soluzioni di sicurezza informatica, turn-key oppure ritagliate sulle specifiche esigenze del cliente.

Rispondiamo ai requisiti più sfidanti, impiegando soluzioni tecniche all'avanguardia ritagliate sullo specifico cliente e contesto, che prendono forma sugli obiettivi e sulle priorità delle persone.

Integriamo i paradigmi della Security by Design e della Defense in Depth in ogni fase del progetto, dall'identificazione dei requisiti alla gestione delle soluzioni. Tale approccio viene impiegato per tutti gli ambiti di intervento, inclusa l'erogazione di servizi in ambienti Cloud e Multi-cloud.

SERVIZI

Eroghiamo servizi di sicurezza in ambito Enterprise/IT e Industrial/OT, centralizzando il monitoraggio delle infrastrutture mediante SIEM best in class e tecnologie di Anomaly Detection, assicurando un supporto continuo lungo tutte le fasi della gestione degli Incidenti di Sicurezza.
Operiamo un assessment dei processi rispetto ai requisiti di protezione, siano essi definiti dai regolamenti cogenti o da policy interne.
Eseguiamo valutazioni della sicurezza di infrastrutture e applicazioni web, operando in conformità alle buone pratiche OWASP e OSSTMM per il security testing.

Ricerche mirate e continue dal Surface, Deep e Dark web: combinando diverse tecniche e approcci, forniamo soluzioni modellate su specifici scenari quali violazione e furto dei dati, prevenzione delle frodi, protezione del brand e della reputazione delle figure aziendali chiave.

Facciamo parte del RTI che si è aggiudicato la gara CONSIP di cybersecurity «Servizi di sicurezza da remoto, di compliance e controllo» e che erogherà per le Pubbliche Amministrazioni Centrali servizi quali: SOC, NGFW, WAF, Gestione Vulnerabilità, Threat Intelligence & Vulnerability Data Feed, Protezione Internet e Posta Elettronica, EPP, Certificati, Gestione Identità, Firma Digitale, Sigillo Elettronico, Timbro Elettronico, Servizi Specialistici e Formazione.

OLTRE I CONFINI

CYBERSECURITY™
MADE IN EUROPE

ECS

La nostra mission va oltre i confini nazionali, puntando al rafforzamento della sovranità digitale e al consolidamento della resilienza informatica dell'Europa. Il conseguimento da parte di Netgroup della Label Cybersecurity Made in Europe di ECSO certifica l'adesione a tali obiettivi, oltre a fornire ai clienti che ci scelgono la garanzia che i nostri prodotti e servizi siano stati sviluppati nel rispetto delle linee guida europee di Security Awareness.

La Label è un'iniziativa di ECSO (European Cyber Security Organisation) che ha l'obiettivo di contribuire alla costruzione di un ecosistema europeo per la cybersecurity sempre più solido, consentendo di identificare gli attori del settore che, attraverso i propri investimenti in ricerca e sviluppo, si fanno promotori dei criteri fondamentali di cyber-resilienza, coerenti con le linee guida emanate dall'Agenzia Europea per la Cybersicurezza.

OSSERVATORIO

ONC

OSSERVATORIO NETGROUP CYBERSECURITY

Osservatorio Netgroup si sostanzia nel lavoro di un team di analisti e ricercatori che svolgono un'azione di monitoraggio, analisi e divulgazione delle tendenze del CyberCrime osservabili in Surface, Deep e Dark Web.

L'ONC, grazie all'ausilio di tool sviluppati e brevettati ad hoc da Netgroup e, in particolare, di Horus®, è in grado di rintracciare in tempo reale informazioni sul gruppo hacker responsabile dell'attacco, sulle tipologie di malware impiegate, sul target e sull'entità dell'eventuale compromissione in modo da rispondere alle minacce e perfino predire eventuali nuovi scenari d'azione.

Horus® è il nostro software di cybersecurity che monitora le attività online dei gruppi criminali e consente di prevenire i loro attacchi. Il sistema, grazie all'uso di IA e Machine Learning, è in grado di analizzare le interazioni sul web per individuare attività insolite che potrebbero indicare un imminente attacco e, una volta isolate, inviare in tempo reale messaggi e notifiche, in modo da adottare le contromisure opportune.

FORMAZIONE & CONSULENZA

Humans for Cyberscurity significa anche costruire conoscenza, consapevolezza e competenze nelle persone per prevenire e riconoscere minacce cyber.

Grazie a MyForge, l'Academy di Netgroup, e alla partnership con la Fondazione YMCA e con l'ICT — International Institute for Counter-Terrorism presso Tel Aviv — eroghiamo percorsi di alta specializzazione sui temi della Cybersecurity e della Critical Assets Defense.

ENERGIA & UTILITIES

GOVERNO & DIFESA

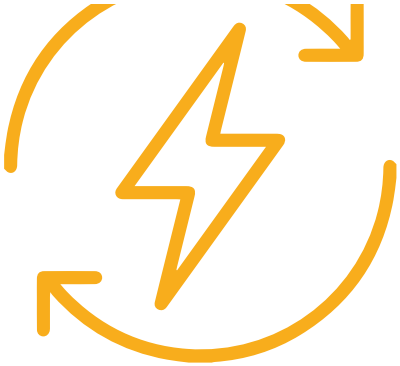
INDUSTRIA & LOGISTICA

MEDICINA & SANITÀ

TRASPORTI & MOBILITÀ

TELCO & MEDIA

ENERGIA & UTILITIES



Obiettivo per hacktivisti, cyberterroristi e cyber-gang con azioni a fini estorsivi.

La diffusione delle utenze rende poi le utilities maschera ideale per campagne di phishing e veicolo formidabile per la distribuzione di malware. Le reti di distribuzione presentano dispositivi vulnerabili fisicamente e logicamente con conseguenze sulla continuità delle forniture e sulla salute dei cittadini.

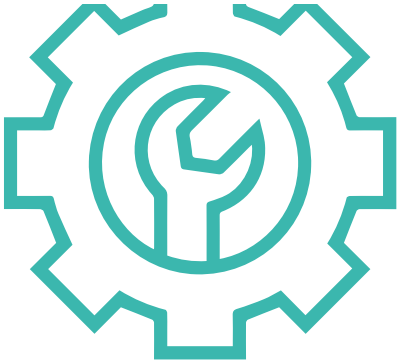
Per contrastare queste minacce forniamo servizi e tecnologie per l'anomaly detection basata su IA, anche in ambito Operational Technology.

GOVERNO & DIFESA

Tentativi di violazione tipicamente di alto profilo, mirati a spionaggio e influenza politica o dell'opinione pubblica e capitalizzazione dell'elevato valore dei dati. Quello Cibernetico rappresenta oggi un nuovo dominio di guerra, come dimostra la costituzione del Perimetro di Sicurezza Nazionale Cibernetico e lo sviluppo di un Framework Nazionale per la Cybersecurity.

Assicuriamo la resilienza di infrastrutture critiche e fornitori di servizi essenziali con attività di assessment delle pratiche, dei processi e dei sistemi IT secondo i control framework più appropriati.

INDUSTRIA & LOGISTICA



È il settore maggiormente colpito. Si pensi all'esposizione generata dall'accesso multicanale, interconnessioni alla supply chain, e ampia gestione di dati industriali e finanziari. Anche le piccole imprese sono esposte, ma spesso non hanno risorse necessarie per un piano efficace di cybersecurity: la conseguenza è che, anche per il loro numero, rappresentano la categoria più colpita.

Grazie ad un team di specialisti forniamo servizi di sicurezza anche in ambito SOC OT, per la detection degli incidenti di sicurezza in contesti industriali.

MEDICINA & SANITÀ

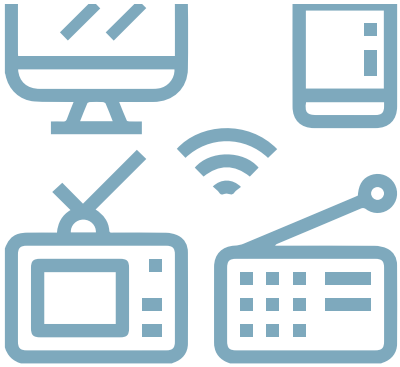
Elevata concentrazione di dati personali e impatto, in caso di violazione, che può portale a perdita di vite umane.
Le organizzazioni medico-sanitarie trattano i dati con procedure spesso più focalizzate sull'efficienza operativa che non sulla resilienza ai cyberattacchi.

Nonostante rigorosi obblighi di conformità, la cybersecurity sta muovendo i primi passi esponendo le attività a un rischio troppo elevato, mitigabile grazie alle nostre attività di valutazione e certificazione dei livelli di sicurezza, in conformità con i più recenti indirizzi in ambito europeo.

TRASPORTI & MOBILITÀ

Incidenti di sicurezza possono avere implicazioni sull'incolumità dei cittadini e causare danni economici. La crescente interconnessione delle auto e delle stesse infrastrutture viarie ne aumenta la vulnerabilità.
I sistemi di gestione sono inoltre soggetti ad attacchi che possono paralizzare le piattaforme per l'emissione di titoli di viaggio.

Forniamo servizi di weakness & vulnerability assessment e penetration test volti a verificare l'effettiva resilienza di sistemi e infrastrutture anche secondo le buone pratiche OWASP e OSSTMM.



TELCO & MEDIA

Il settore è esposto a tangibili rischi di cyber sicurezza, con attacchi indirizzati alla compagnia o ai suoi clienti. Il costante aumento dei servizi, soprattutto in cloud, estende poi la superficie d'attacco e i rischi connessi agli incidenti di sicurezza.
Il mondo dei Media inoltre fa sempre più ricorso a tecniche di OSINT per la ricerca di informazioni sul web.

Contrastiamo le intrusioni di sicurezza e mitighiamo gli effetti di un data breach intercettando con tempestività la diffusione non autorizzata di dati, con ricerche mirate e continue dal Surface, Deep e Dark web.

Gli attacchi Cyber sono continui
e possono provocare danni.
A chiunque.

www.netgroup.it
info@netgroup.it