

# BLUE TEAM

## HACKING PEOPLE

### SECURITY ASSESSMENT

Le eccezionali opportunità derivanti dall'evoluzione tecnologica e dalla conseguente trasformazione digitale portano con sé anche molteplici rischi legati alla sicurezza informatica.

Un'adeguata consapevolezza di questi rischi ed una presa di coscienza di quanto l'azienda è preparata ad affrontarli sono i precetti da cui partire per contrastare efficacemente eventuali incidenti di sicurezza.

**Obiettivo del servizio è di analizzare lo stato dell'azienda rispetto alla sicurezza del suo business nei confronti delle minacce informatiche e suggerire le corrette azioni di miglioramento.**

Il servizio **INTUITY Security Assessment** si sviluppa secondo il modello proposto dalla ISO 27001, consentendo quindi di ottenere un'iniziale valutazione sul livello di maturità dell'azienda nei confronti della sicurezza informatica e di evidenziare le principali carenze nella protezione dei dati personali rispetto a quanto prescritto dalla normativa UE 2016/679 (GDPR).



Il servizio INTUITY Security Assessment mira ad evidenziare le carenze aziendali della sicurezza informatica riconducibili ad una sua inadeguata gestione, a problemi di natura tecnologica o causate dalla mancanza di una condivisa cultura della sicurezza aziendale.

IL SERVIZIO INTUITY SECURITY ASSESSMENT PERMETTE DI OTTENERE, DA PARTE DI SPECIALISTI, UNA VISIONE E VALUTAZIONE SUPER-PARTES SULLA GESTIONE DELLA SICUREZZA INFORMATICA AZIENDALE ED UNA SERIE DI REMEDIATION COMMISURATE AI RISCHI REALI PER IL BUSINESS.

## LE ATTIVITA' PREVISTE DAL SERVIZIO SONO:



### SECURITY POSTURE ASSESSMENT

Intervista al management, ai responsabili IT ed al personale per raccogliere informazioni sull'organizzazione generale dell'azienda da un punto di vista tecnico e di gestione della sicurezza informatica.



### SECURITY AWARENESS ASSESSMENT

Valutare la consapevolezza del personale aziendale nei confronti di una delle minacce più comuni, sottoponendo un panel di dipendenti ad una campagna di Phishing simulata. L'attività è completata da un questionario anonimo da sottoporre a tutta l'azienda su temi generali legati alla sicurezza informatica.



### VULNERABILITY ASSESSMENT

Attività volta a identificare, analizzare e classificare eventuali vulnerabilità presenti nei sistemi e nelle applicazioni aziendali. Questa attività permette di rilevare il livello della sicurezza dell'intera infrastruttura aziendale.



### ACTIVE DIRECTORY ANALYSIS

Analisi di eventuali criticità legate ad Active Directory ed alla gestione degli account aziendali.



### REPORT & REMEDIATIONS

In base ai risultati della fase di analisi, si propone un piano di azioni volte al raggiungimento di un livello di sicurezza ottimale, oltre che una maggiore aderenza a quanto richiesto dall'attuale regolamento generale europeo sulla protezione dei dati, UE 2016/679 (GDPR).

## A CHI CONSIGLIAMO DI EFFETTUARE UN SECURITY ASSESSMENT?

- Alle aziende che vogliono avere una prima analisi sullo stato della propria sicurezza informatica.
- Alle aziende che vogliono orientarsi nell'ottimizzazione della sicurezza informatica interna, ma non sanno da dove iniziare. In questo, il servizio INTUITY Security Assessment, abbinato al servizio HACK IN A DAY (<https://www.intuity.it/red-team/#hack-in-a-day>), rappresenta uno "starter kit" per muovere i primi passi consapevolmente e con metodo in questo percorso.
- Alle aziende che intendono verificare la propria ottemperanza agli standard normativi e migliorarla dove necessario.
- Alle aziende che intendono valutare il proprio livello di awareness sulla sicurezza informatica, con l'intento di intraprendere successivamente un'attività di formazione su questo tema.

### Chi è INTUITY?

INTUITY è un'azienda specializzata in Cybersecurity. I suoi servizi consentono di elevare la sicurezza delle aziende in modo efficace e durevole nel tempo, consentendo di ottimizzare gli investimenti già fatti e quelli futuri.

INTUITY approccia il problema della Cybersecurity attraverso un cambio di prospettiva: guardare le aziende con gli occhi di un "hacker". Nello specifico, l'azienda ha realizzato un servizio di Offensive Security chiamato INTUITY Red Team, il quale simula un vero e proprio attacco informatico, con l'obiettivo di capire se le strategie di sicurezza implementate da un'azienda siano davvero efficaci o meno per contrastare un eventuale attacco.