BLUE TEAM

DEFENSIVE SECURITY

I servizi **BLUE TEAM** di IMQ Intuity permettono ai clienti di aumentare la propria sicurezza e di essere compliant a standard internazionali, regolamenti interni o normativi.

Consentono di acquisire la piena consapevolezza del problema e di capire come questo impatta nella propria realtà, di gestire tutti gli aspetti di sicurezza con approccio moderno e proattivo e di implementare una strategia di protezione efficace.

OBIETTIVI E BENEFICI DEI SERVIZI DI BLUE TEAM

PROTECTION

Garantire la sicurezza aziendale: correggere le vulnerabilità più critiche, rafforzare i presidi tecnologici, monitorare e rispondere a situazioni di rischio.

COMPLIANCE

Aderire correttamente a normative e standard richiesti: *ISO27001, PCI-DSS, AgID*, internal compliance.

AWARENESS

Aumentare la consapevolezza interna sul problema: rendere il fattore umano un elemento chiave per la sicurezza del business.

Sede Operativa: Via Brunello Rutoli, 6 35129 | Padova
Sede Operativa: Via Nazionale, 230 CAP 00184 | Roma
Sede Legale: Via M. F. Quintiliano, 45 - 20138 | Milano

Tel: 049 817 0850
E-mail: info@intuity.it

SERVIZI DI BLUE TEAM

INCIDENT DETECTION & RESPONSE

Il servizio è rivolto alle aziende che vogliono dotarsi di un servizio per la rilevazione e la gestione di incidenti informatici o che desiderino estendere la copertura di servizi esistenti includendo visibilità su quanto accade a livello di Endpoint, sui dispositivi mobili o sui sistemi Cloud. Il servizio consente di reagire tempestivamente, prevenire un danno e rispettare la compliance agli standard di sicurezza più comuni quali: *ISO27001, GDPR, PCI DSS*.

EMERGENCY RESPONSE

IMQ Intuity assisterà il cliente durante un attacco informatico per bloccare l'aggressore, trovare il vettore di attacco e inibirlo per evitare che il criminale entri di nuovo in azienda. Il cliente viene inoltre supportato nel percorso di *Data Recovery*.

THREAT INTELLIGENCE

Spesso gli aggressori utilizzano le informazioni che possono recuperare da Internet con lo scopo di preparare ed eseguire un attacco. Queste informazioni possono essere trovate sul Web, ma molto spesso anche nelle aree più inaccessibili di Internet conosciute come *Deep e Dark Web*. Il servizio di *Threat Intelligence di* IMQ Intuity utilizza le stesse fonti di informazioni per tenere i clienti lontani dalle minacce.

VULNERABILITY HUNTING

Un bug di sistema, una configurazione errata, un documento sensibile inavvertitamente divulgato o un utente con privilegi troppo elevati, sono solo alcuni esempi di situazioni che possono esporre l'azienda a gravi conseguenze. I servizi IMQ Intuity di *Vulnerability Assessment* e *Penetration Test* si basano su analisi più tradizionali, integrando azioni di *Intelligence* come la ricerca *OSINT*, analisi dei risultati nel contesto del business e la determinazione dell'effettivo profilo di rischio dell'azienda.

DIGITAL FOOTPRINTING

Attività che ha la finalità di mappare in modo dettagliato ed esaustivo quanto un'azienda espone su Internet: indirizzi IP, servizi, domini e sotto domini. L'obiettivo è mantenere aggiornata la mappa dell'infrastruttura aziendale, in modo da ottenere il controllo sulle risorse digitali e controllarne il livello di sicurezza.

Sede Operativa: Via Brunello Rutoli, 6 35129 | Padova
Sede Operativa: Via Nazionale, 230 CAP 00184 | Roma
Sede Legale: Via M. F. Quintiliano, 45 - 20138 | Milano

Tel: 049 817 0850
E-mail: info@intuity.it

CONSULTING & AWARENESS

INCIDENT RESPONSE PLAN

Le organizzazioni devono fare del loro meglio per prevenire attacchi informatici e avere successo, allo stesso tempo hanno bisogno di essere preparati allo scenario peggiore: un hacker può violare le difese. In questo caso, una risposta rapida ed efficiente può salvare l'azienda da un potenziale disastro.

SECURITY AWARENESS

Le persone sono una risorsa fondamentale per ogni azienda: gestiscono il business, accedono ai dati, usano dispositivi tecnologici ogni giorno e ovunque. Per questi motivi, sono l'obiettivo principale per la maggior parte degli attacchi informatici. Le statistiche dicono che il 90% degli attacchi inizia con una e-mail di phishing. L'unico modo per mitigare questo problema è rafforzare la capacità delle persone di riconoscere una minaccia ed evitarla, qualunque sia il loro ruolo all'interno dell'organizzazione.

ADVISORING/CONSULTANCY

Aiutiamo le aziende ad approcciare alla cybersecurity in modo corretto, indirizzando il cliente verso il percorso ottimale e specifico per le proprie esigenze.

SECURITY ASSESSMENT

L'obiettivo del servizio è quello di analizzare lo stato della postura di sicurezza aziendale contro le pratiche comuni di attacco e di suggerire azioni correttive. Il servizio, sviluppato secondo il modello proposto dal *CIS (Center for Internet Security)*, ci consente di ottenere una valutazione del livello di maturità della sicurezza IT della società e di evidenziare eventuali carenze nella protezione dei dati aziendali e personali.

Sede Operativa: Via Brunello Rutoli, 6 35129 | Padova
Sede Operativa: Via Nazionale, 230 CAP 00184 | Roma
Sede Legale: Via M. F. Quintiliano, 45 - 20138 | Milano

Tel: 049 817 0850
E-mail: info@intuity.it

PARTNER TECNOLOGICI

Selezioniamo le migliori e più innovative tecnologie da integrare ai nostri servizi di *Defensive Security*, con l'obiettivo di offrire ai clienti le soluzioni più efficaci e appropriate per le loro esigenze aziendali. Collaboriamo con i leader del mercato per affrontare insieme questa sfida.

RAPID7

Le soluzioni Rapid7 aiutano le aziende nell'identificare i rischi alle quali sono esposte e a definire un *remediation-plan* focalizzato sul reale livello di *severity*.

SPEARTIP
CYBER COUNTERINTELLIGENCE

Società di *cyber counter-intelligence* che protegge i clienti dalle minacce informatiche attraverso servizi sia proattivi che reattivi. Aiuta le organizzazioni a identificare il rischio informatico e le vulnerabilità e garantisce una protezione completa, continua e end-to-end.

_IntelligenceX

Protegge la tua azienda dalle minacce più attuali con la tecnologia più avanzata sul mercato.

LastPass

È la soluzione di *LogMeIn* che permette di memorizzare e gestire le proprie password in modo semplice e sicuro. Si tratta di un gestore di password in cui i propri dati vengono crittografati e decrittografati a livello di dispositivo e memorizzati nella propria cassaforte.

CROWDSTRIKE

Protegge le aziende dalle minacce più avanzate con la tecnologia più avanzata sul mercato.

Invicti

Le soluzioni *Invicti* offrono la soluzione DAST più accurata ed efficiente per i team DevOps/DevSecOps, per scoprire e proteggere tutte le applicazioni che gestiscono le loro organizzazioni.

KnowBe4
Human error. Conquered.

È il leader di riferimento per la sua offerta di servizi di *Security Awareness* e si prefigge di migliorare la linea di difesa più importante del contesto aziendale: i propri dipendenti.

SpyCloud

Monitora costantemente la presenza di informazioni sensibili sul web e sul *Dark Web*, per agire prima che possano essere utilizzate contro una data organizzazione.

FUDO SECURITY

I prodotti *Fudo Security* consentono di monitorare l'attività degli utenti con accesso a risorse critiche, aiutano le aziende a gestire la politica sulla password e avvisano in caso di comportamenti sospetti.