CyberSIGMA
By Sigma Consulting

CyberSIGMA

SERVIZI

- **IT GOVERNANCE E COMPLIANCE** — PER SAPERNE DI PIÙ
- **SERVIZI GDPR** — PER SAPERNE DI PIÙ
- **FORMAZIONE** — PER SAPERNE DI PIÙ
- **VULNERABILITY ASSESSMENT E PENETRATION TEST** — PER SAPERNE DI PIÙ
- **SOC** — PER SAPERNE DI PIÙ
- **INTELLIGENCE** — PER SAPERNE DI PIÙ
- **SICUREZZA INFORMATICA 360°** — PER SAPERNE DI PIÙ
- **ALTRI SERVIZI DI SICUREZZA AZIENDALE** — PER SAPERNE DI PIÙ

CyberSIGMA è la nuova **Business Unit** di Sigma Consulting che si occupa di **soluzioni** avanzate di **cyber security**: **FORMAZIONE** E **SERVIZI**, personalizzati per la tua azienda.

SIGMA CONSULTING SRL - P.IVA 056780951002

Sede legale: Via Cavareno 13 - 00124 Roma - **Sede operativa**: Via Adriano Olivetti 24/26 - 00131 Roma

+390687725590 +39068772559 info@sigmaconsulting.it www.sigmaconsulting.it / www.cybersigma.it/

CyberSIGMA
By Sigma Consulting

FORMAZIONE

I Corsi saranno erogati in modalità on line o in presenza. Alla fine del corso verranno forniti materiali didattici e Attestato di partecipazione.

La maggior parte delle violazioni dei dati sono dovute a negligenza e comportamento errato da parte di datori di lavoro / dipendenti. Questo fenomeno può essere ridotto attraverso **Corsi di formazione che Cyber Sigma ha pensato per le aziende e per gli imprenditori. Corsi personalizzati di livello base e di livello avanzato.**

CORSO SECURITY AWARENESS (BASE)

Il corso include:

- Sicurezza informatica: una questione di mentalità
- Gestione del personale
- Attacchi social engineering
- Sicurezza fisica aziendale
- Sicurezza delle operazioni informatiche
- Gestione delle policy
- Business Continuity e al Disaster Recovery

CYBERSECURITY E PROTEZIONE DEI DATI: AWARENESS DIPENDENTI→ FORMAZIONE DI BASE PER ACQUISIRE CONSAPEVOLEZZA E INFORMARE TUTTI I **DIPENDENTI** DELL'ORGANIZZAZIONE.

Il corso include:

- Introduzione alla Cybersecurity
- Minacce e contromisure
- Best practice per l'utilizzo delle risorse IT
- Introduzione al GDPR

CYBERSECURITY E PROTEZIONE DEI DATI: AWARENESS GESTIONE MANAGEMENT→ FORMAZIONE MIRATA PER IL **MANAGEMENT**.

Il corso include:

- Introduzione alla Cybersecurity
- Minacce e contromisure
- Linee guida per la governance IT
- Introduzione al GDPR

CORSO OFFENSIVE (AVANZATO).

Il corso include:

- Foot printing and Reconnaissance
- Scanning Networks

- Enumeration
- Vulnerability Analysis
- System Hacking
- Hacking Web Servers

SERVIZI e SOLUZIONI DI CYBERSECURITY

■ IT GOVERNANCE E COMPLIANCE:

ISO / IEC 27001 è uno standard internazionale che definisce i requisiti per un corretto **Sistema di Gestione per la Sicurezza delle Informazioni.** Implementare un Sistema di Gestione per la Sicurezza delle Informazioni aiuta a ridurre rischi e perdite di entrate causati dalla tecnologia, migliorando al tempo stesso l'immagine del tuo business.

ISO 27001: ANALISI GAP 2013

- Analisi del GAP e verifica della compliance rispetto allo standard ISO/IEC 27001:2013
- Intervista dei responsabili del settore
- Identificazione dei requisiti
- Report di analisi del GAP (processo che aiuta a determinare la differenza nel loro attuale stato di sicurezza delle informazioni rispetto a requisiti specifici)
- Piano di rimedio

SECURITY ASSESSMENT

- Valutazione della sicurezza IT con focus sui principali processi aziendali
- Intervista dei responsabili del settore
- Vulnerability assessment
- Identificazione e valutazione dei rischi in termini di priorità e criticità degli impatti.

■ **GDPR:** Il **Regolamento Generale Sulla Protezione Dei Dati** (Reg UE n. 2016/679) è operativo dal 25 maggio 2018. Ogni azienda deve **valutare** la propria **conformità** rispetto al regolamento.

GDPR ASSESSMENT E PIANO DI RIMEDIO

- GDPR Analisi del GAP
- Registro dei trattamenti
- Gestione dei Consensi ed Informative
- Piano di rimedio

GDPR IMPLEMENTAZIONE

- Assessment & Piano di rimedio
- Data Protection Impact Assessment (DPIA)
- Policy Review ed Imolementazione dell'adeguament

DPO COME SERVIZIO. Il DPO (**Data Protection Officer**) è una figura che si occupa della continua verifica dei requisiti GDPR. I nostri professionisti sono a disposizione per il **servizio DPO in outsourcing.**

CORSI DI FORMAZIONE GDPR

- La protezione dei dati personali.
- introduzione al nuovo Regolamento UE 679/16: definizioni, novità ed obblighi.
- Gli aspetti chiave di un percorso di adeguamenti: censimento dei trattamenti, la gestione dei consensi, il sito aziendale, il trasferimento dei dati, la nomina del responsabile del trattamento, la DPIA, il registro dei trattamenti.
- L'importanza delle misure di sicurezza e della revisione continua dei processi che trattano dati personali.

■ VULNERABILITY ASSESSMENT E PENETRATION TEST

Un test di sistema per la valutazione delle vulnerabilità è una delle attività più richieste per questo deve essere eseguita per testare l'affidabilità del sistema e la sua conformità al GDPR.

- **L'identificazione degli asset e dei rischi** è un compito fondamentale: esso deve essere eseguito regolarmente per scoprire il sistema vulnerabilità prima di qualcun'altro (malintenzionato).
- **Risorse critiche** e **errori** di **configurazione** della sicurezza.
- **Sicurezza** del **sistema** VA / PT eseguita secondo le metodologie standard

VULNERABILITY ASSESSMENT (VA)

- Information gathering
- Individuazione ed elenco puntuale delle vulnerabilità scoperte
- Piano di rimedio: valutazione dell'impatto sul business aziendale

PENETRATION TEST

- Information gathering
- Individuazione ed elenco puntuale delle vulnerabilità scoperte
- Exploit e simulazione di attacco
- Piano di rimedio: valutazione dell'impatto sul business aziendale e proposte per la mitigazione del rischio

■ SECURITY OPERATION CENTER

Un Security Operation Center rappresenta un'unità centralizzata in cui le informazioni possono essere monitorate e analizzate.

ATTIVITÀ:

- Gestione degli eventi
- I log vengono raccolti e archiviati centralmente all'interno del perimetro o direttamente nel nostro Data Center SOC (a seconda della disponibilità della larghezza di banda)

Piattaforme SIEM (Security Information & Event Management)

Il servizio analizza gli eventi acquisiti e li compara rispetto a un insieme di regole di correlazione creando fornendo supporto all' analista della sicurezza

Gestione dei dispositivi di sicurezza

Questo servizio include la gestione IDS/IPS sia a livello di rete che a livello di host fornendo report periodici su qualsiasi attività sospetta (intrusione non riuscita, tentativi di hacking malevoli) mediante azioni supervisionate su regole di routing e policy.

Monitoraggio di eventi e eventi

Questo servizio aiuta nella tempestiva identificazione e correlazione delle anomalie di sicurezza attraversa il rilevamento in tempo reale di errori e allarmi da fonti multiple ed eterogenee.

Prevenzione delle minacce

Prevenzione di eventi di sicurezza informatica mediante analisi e manipolazione in tempo reale (normalizzazione, aggregazione e correlazione) del traffico di rete.

■ INTELLIGENCE

I servizi di intelligence sono progettati per **raccogliere dati da diverse fonti correlando** tra loro i **dati grezzi** raccolti e **convertendo queste** informazioni in **informazioni fruibili** (ad esempio per i processi decisionali).
La Security Intelligence consente di supportare un'organizzazione nella propria strategia di sicurezza.
*La Security Intelligence può essere fornita a distanza sia in outsourcing che in locale o in un modello di servizio ibrido.

Cyber Threat Intelligence

- Early warning
- Prevenzione delle violazioni
- Protezione da attacchi hacker

Open Source INTelligence (OSINT)

- Analisi dei dati multimediale
- Costruzione di modelli predittivi
- Analisi dei big data

■ SERVIZIO SICUREZZA INFORMATICA 360°

- Valutazione di sicurezza aziendale
- Formazione sicurezza del personale
- Interventi di Business continuity e Disaster Recovery
- Vulnerability Assessment e Penetration Test
- Report finale e soluzioni di remediation

■ ALTRI SERVIZI DI SICUREZZA AZIENDALE

REVISIONE DELLE POLICY DI SICUREZZA DEI DISPOSITIVI: Garantire che le regole e la configurazione dei dispositivi di sicurezza soddisfino le best practice è un'attività fondamentale per la protezione delle informazioni.

PREVENZIONE DEGLI INCIDENTI: Questo servizio si basa sulla gestione e l'ottimizzazione dei processi di rilascio di patch al fine di ridurre le perdite sulle risorse aziendali. Include una valutazione del rischio che mette in correlazione le informazioni con le vulnerabilità, le probabilità e gli impatti.

PREVISIONE DI POLICY DI SICUREZZA: Valutazione dello stato attuale dell'organizzazione a più livelli (rete, sistemi e applicativo). Il servizio comprende una fase preliminare di analisi delle lacune rispetto agli standard di riferimento e alle principali best practice del settore, seguita da una valutazione del rischio e da attività tecniche di monitoraggio e vulnerabilità alla scoperta.

BUSINESS CONTINUITY MANAGEMENT: È importante identificare le risorse e i servizi fondamentali per garantire la continua di servizio e un rapido recupero a seguito di un'interruzione. Viene valutato ogni servizio necessario per il business e vengono pianificate eventuali possibili minacce attraverso un'analisi del rischio adeguata. Il servizio si conclude con la definizione di un piano di continuità aziendale.