ELMI Digital Innovation Partner

IT & Security Services

La BU IT & Security

La **business unit IT & Cyber Security**, ha l'obiettivo di proporre sul mercato soluzioni tecnologiche e servizi che soddisfino le richieste in termini di infrastrutture informatiche e protezione delle medesime.

La BU si è evoluta negli anni, portando in offering soluzioni infrastrutturali fisiche e virtuali complesse, progettando e realizzando infrastrutture di networking ed erogando servizi che vanno dall'help desk di primo livello fino al supporto sistemistico erogato da professionisti certificati.

Dal 2018 l'unità ha iniziato un processo di ampliamento dell'offering attraverso la vendita di prodotti e servizi in ambito Cyber Security.

Dapprima con specifiche verticalizzazioni basate sulle soluzioni IBM Security, successivamente, **strutturando un vero e proprio "framework" che consenta alle organizzazioni di affrontare il tema sicurezza informatica a 360 gradi**, portando sul mercato prodotti e soluzioni che coprono dalla difesa perimetrale, alla protezione degli endpoint fino a giungere all'erogazione in modalità SaaS dei servizi di Security Operation Center.

Le soluzioni ed i servizi che la business unit è in grado di erogare, perfettamente si sposano con la costante necessità delle aziende di supportare il business con infrastrutture tecnologiche resilienti e performanti e con la crescente necessità di proteggere le informazioni essenziali per il business dalle violazioni informatiche.

I nostri servizi

- Supporto Sistemistico
- Progettazione di infrastrutture
- Network Operation Center e "Total Care"
- Risk & Vulnerability Assessment
- Endpoint Protection
- SIEM & NTA
- Difesa perimetrale
- Backup & DR
- Security Awareness
- Security Operation Center

5 Business Unit

+ 70 dipendenti

+ 6 milioni di fatturato

+ 250 clienti in tutta Italia

Chi siamo

ELMI Digital Innovation Partner

ELMI è una PMI Innovativa e opera nel settore ICT come System Integrator con l'obiettivo di supportare le aziende private e pubbliche nello sviluppo di progetti innovativi e soluzioni tecnologicamente avanzate. Dal 1985 supportiamo e accompagniamo le aziende nel loro percorso di digital transformation. Oggi l'azienda è focalizzata sulle seguenti aree digitali:

- ✓ DPM - Digital Process Management
- ✓ Enterprise Asset Management
- ✓ Cyber Security & IT Infrastructure
- ✓ Data Strategy
- ✓ ERP e gestione aziendale

IBM Gold Partner

Data Center Partner Lenovo Gold

SAP

Infrastruttura IT

Servizi IT

Il nostro servizio di progettazione e realizzazione di **infrastrutture** complesse, sia **fisiche** che **virtuali**, è pensato per soddisfare le esigenze informatiche delle aziende moderne.

Il nostro team di esperti fornisce soluzioni su misura, valutando attentamente le necessità di ogni cliente e creando un'infrastruttura affidabile e scalabile. Grazie alla competenza maturata, siamo in grado di erogare servizi che vanno dall'implementazione di componenti fisici come server, cablaggi e dispositivi di rete, a soluzioni basate su ambienti virtuali e cloud computing **garantendo un ambiente tecnologico solido e performante.**

Supporto sistemistico di 1 e 2 Livello

Il servizio di supporto sistemistico di primo e secondo livello garantisce un funzionamento ottimale dell'ambiente informatico. **Il nostro team altamente qualificato, è specializzato nella risoluzione tempestiva dei problemi**, offrendo un supporto competente e affidabile.

Le nostre numerose certificazioni vendor neutral (**CompTIA A+, Security+, Network+**) e le certificazioni dei principali leader di settore (**Microsoft, Cisco, IBM, Lenovo, Palo Alto**), sono un chiaro segno della nostra competenza e della nostra dedizione alle migliori pratiche di settore.

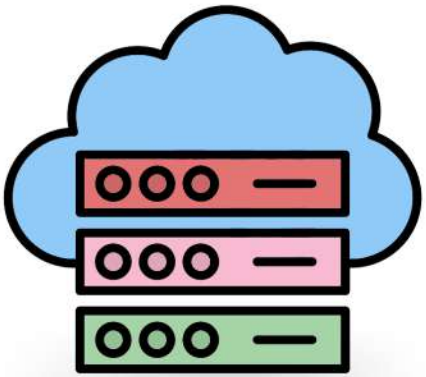
ELMI

Infrastruttura IT

Progettazione e realizzazione di infrastrutture complesse di networking

I nostri network engineer si avvalgono di professionalità ed esperienza per progettare ed implementare infrastrutture di rete, con un design solido e scalabile orientato a garantire elevati standard di sicurezza, avvalendosi di tecnologie consolidate unite a soluzioni e modelli NEXT-GEN.

Il nostro team è specializzato nell'implementazione reti SD-WAN, sistemi di controllo accessi (NAC) e soluzioni di micro-segmentazione orientati al paradigma Zero-trust.



NOC e Servizi TotalCare

Il servizio di monitoraggio NOC (Network Operations Center) e TotalCare **offre un controllo completo e continuo della tua infrastruttura informatica.** Il nostro team altamente specializzato monitora costantemente le prestazioni del tuo ambiente IT, identificando e risolvendo tempestivamente eventuali problematiche.

Grazie ad una combinazione di strumenti avanzati e competenze tecniche, siamo in grado di gestire attivamente gli aggiornamenti, l'installazione di software, le modifiche alle configurazioni e altre attività necessarie per mantenere l'infrastruttura al massimo delle prestazioni.

Cyber Security

Identificazione Security Needs

Il nostro servizio di cyber security è dedicato a garantire la sicurezza delle aziende. **Il nostro team di esperti analizza attentamente l'infrastruttura esistente e progetta soluzioni personalizzate basate sulle specifiche del settore**.

Utilizziamo le migliori pratiche e tecnologie avanzate per migliorare la postura di sicurezza, proteggendo i dati e mitigando i rischi cibernetici.

Risk & Vulnerability Assessment

Questo processo consiste nell'identificazione e valutazione dei rischi e delle vulnerabilità presenti nell'infrastruttura tecnologica. **Attraverso un'analisi approfondita, identifichiamo le potenziali minacce e le vulnerabilità che potrebbero compromettere la sicurezza dei tuoi dati e delle tue risorse**.

Questo ci consente di sviluppare e implementare strategie di mitigazione per ridurre al minimo i rischi. Il Risk e Vulnerability Assessment **è una pratica indispensabile per mantenere la sicurezza dei sistemi informativi** e proteggere la tua azienda da potenziali attacchi informatici.

Cyber Security

Endpoint Protection

Offriamo ai nostri clienti, **numerose soluzioni e servizi in ambito protezione degli endpoint** (pc client, server, dispositivi mobili) che consentano loro di proteggere i dispositivi aziendali e le informazioni in essi contenute. Le soluzioni consentono:

- ✓ Identificazione degli Asset
- ✓ Produzione di un vero e proprio inventario dei dispositivi informatici
- ✓ Gestione policy di sicurezza applicate
- ✓ Controllo applicativi on-board
- ✓ Massive software deployment e aggiornamenti di sicurezza
- ✓ Protezione anti malware, ransomware, trojan, infostealer
- ✓ Soluzioni best of breed per identificazione APT - Advanced Persistent Threat

SIEM – NTA

Con l'acronimo SIEM - si identificano quelle piattaforme di Security Intelligence, **capaci di acquisire i dati prodotti da tutti i dispositivi aziendali ed elaborarli in modo da determinare eventuali minacce alla sicurezza informatica**.

L'adozione di soluzioni di tipo SIEM in congiunzione con soluzioni di tipo NTA – Network Traffic Analyzer, **permette di ridurre i così detti "blind spot" delle infrastrutture informatiche** e di migliorare la postura in ambito cyber.

Inoltre, questo genere di soluzioni permettono di rispondere ai requisiti dei principali enti regolatori e normative, quali a titolo non esaustivo: GDPR, ISO, PCI-DSS. **Offriamo ai nostri clienti le migliori soluzioni in ambito SIEM – NTA**, corredate dai nostri servizi specialistici di progettazione, supporto tecnico verticale applicativo e MDR con l'ausilio del nostro Security Operation Center.

Difesa Perimetrale

Con il termine "difesa perimetrale" **si identificano tutte le soluzioni hardware e software poste a difesa dei "confini aziendali"**. Per quanto, nuovi scenari mutevoli e diversificati (es: cloud computing, smart working) abbiano ridisegnato il perimetro operativo, vi sono sistemi essenziali per una solida difesa aziendale, indipendente dalla loro collocazione geografica o dal loro "strato" applicativo. Tra le principali soluzioni e servizi che offriamo ai nostri clienti, possiamo citare:

- ✓ Next Generation Firewall
- ✓ Network Access Control
- ✓ IDS / IPS
- ✓ Antispam
- ✓ Policy

Ai prodotti hardware e software si aggiunge la capacità di progettazione di infrastrutture di reti complesse, volte ad ottimizzare la gestione e la sicurezza del network aziendale.

ELMI

Cyber Security

Backup & DR

Il Backup ed il DR - Disaster Recovery, rappresentano un **primo** ed importante **layer di protezione per i dati** e per la continuità dei processi aziendali. È necessario che **ogni fase**, dalla progettazione ed esecuzione, fino alle verifiche di funzionamento e revisione periodica, venga svolta con la **massima competenza ed attenzione**, rappresentando il backup, a tutti gli effetti un'ultima "ancora di salvezza" in presenza di un attacco informatico.

I nostri consulenti, guideranno il cliente, in tutte queste fasi, garantendo la sicurezza e disponibilità dei backup, il rispetto delle fasi di progetto e dei parametri stabiliti.
Ma come **agire** in presenza di **situazioni critiche** i cui tempi di soluzione si dilatano notevolmente? Un progetto di DR - Disaster Recovery, permette all'azienda, identificando le necessità di RPO e RTO di ripartire con i servizi essenziali al proprio business.

Security Awareness

Tra le principali cause di violazioni informatiche vi sono i comportamenti errati svolti dagli utenti. Abbiamo quindi inserito nella nostra value proposition delle soluzioni di Security Awareness che si dividono in due principali categorie: **training** & **simulation**.

Con il **training** si utilizzano piattaforme di **e-learning** nelle quali gli utenti possono **apprendere elementi chiave** volti a **migliorare** la loro **consapevolezza** in ambito cyber security. Con le attività di "**simulation**" invece, **mettiamo alla prova** la capacità degli utenti di **identificare tentativi di phishing** veicolati via email e la loro capacità di **identificare la minaccia e segnalarla** opportunamente.

Security Operation Center

Il Security Operation Center è un centro di controllo altamente specializzato e dedicato alla verifica degli eventi di sicurezza 24/7. Dotato di control room fisica, utilizza tecnologie best of breed quali SIEM, NDR-NTA, SOAR, XDR, CTI per l'erogazione dei servizi. ESOC – Elmi Security Operation Center è in grado di erogare servizi quali:

MONITORING E ANALISI
Servizio di analisi in tempo reale degli eventi per identificare i threat informatici in modo preventivo / proattivo.

MALWARE ANALYSIS
Studio che permette di comprendere e identificare il comportamento di file, processi sospetti.

PHISHING ANALYSIS
Servizio il cui obiettivo è di validare mail, url di dubbia natura.

DARK WEB ANALYSIS
Servizio di Threat Intelligence, svolto da specialisti di sicurezza che monitorano il darkweb, forum underground, gruppi Telegram o Discord ed altro ancora.

THREAT HUNTING
Attività svolte in modo preventivo e realtime con lo scopo di identificare specifici threat all'interno della infrastruttura aziendale.

INCIDENT RESPONSE
Processo strutturato di risposta agli incidenti informatici (NIST based) eseguito da team multidisciplinare che prevede la produzione di incident report al suo completamento.

VULNERABILITY ASSESSMENT
Servizio che permette l'identificazione delle vulnerabilità degli asset informatici e la riduzione della superficie di attacco.

Principali tecnologie utilizzate

Oltre alle competenze orizzontali sul team IT & Cyber Security, abbiamo maturato competenze specialistiche certificate sulle seguenti tecnologie / prodotti.

CATEGORIA TECNOLOGICA	PRODOTTO
SIEM	IBM Security QRadar SIEM
XDR	Cynet
Vulnerability Assessment	tenable
Endpoint Protection	ManageEngine
NTA-NDR	IBM Security
SOAR	FORTINET
Back & Dr	VEEAM
Next Gen Firewall	paloalto NETWORKS / FORTINET
Antispam	LIBRAESVA
Awareness /phishing Simulator	Cyber Guru

ELMI

Cyber Security

ELMI

Cyber Security

Certificazioni

In ambito Cyber Security, oltre alle certificazioni specialistiche inerenti prodotti e servizi, abbiamo strutturato piani formativi e di on-boarding per ogni figura del Security Operation Center, in modo da attestare e validare le competenze e la qualità del servizio reso ai nostri clienti.

Per tanto **i nostri analisti conseguono certificazioni "vendor neutral" in ambito Cyber Security**, di particolare rilievo è la certificazione Security Blue Team, che viene rilasciata dopo il superamento di uno specifico esame, costituito da un Incident Response della durata di 24h.

ELMI Digital Innovation Partner

Chiedici una consulenza

Riduciamo il rischio attraverso la consulenza e la nostra competenza sui prodotti di sicurezza. Scansiona il QR CODE e richiedi la consulenza di un esperto.

Contatti

www.elmisoftware.com

091-6704025

security@elmisoftware.com

Member of CISQ Federation

RINA IQNet

CERTIFIED MANAGEMENT SYSTEM

ISO 9001 - ISO/IEC 27001

RINA

SISTEMA DI GESTIONE

UNI PDR 125

Parità di Genere

IT & Security Services