

IL NUOVO SECURITY COMPETENCE CENTER A PALERMO



Il nuovo centro operativo H24 7 giorni su 7

Com'è strutturato il nostro centro operativo

Il nostro security competence center, con sede a Palermo, è concepito come un punto di riferimento strategico per le aziende che desiderano garantire la massima protezione dei propri sistemi informatici e dei dati sensibili. Dotato di personale altamente qualificato, il nuovo centro è in grado di monitorare costantemente le minacce informatiche e di intervenire tempestivamente in caso di incidenti.



Le strutture specialistiche



Security Operation Center

Il nostro centro operativo è dotato di una **Control Room** dedicata al monitoraggio, triage e gestione degli eventi di sicurezza H24/7.



Network Operation Center

Il NOC è un centro operativo che si occupa specificamente della gestione e del monitoraggio della rete.



MDR

La gestione remota dell'infrastruttura si riferisce alla possibilità di monitorare, configurare e controllare a distanza tutti i componenti che compongono l'IT di un'azienda.



I servizi erogati

- **Security Operation Center**
- **Network Operation Center**
- **Managed Services**

Security Operation Center (SOC)

Il Security Operation Center è un centro operativo 24 ore al giorno, 7 giorni su 7, composto da specialisti in Cyber Security, dedicato al monitoraggio costante degli eventi di Cyber Security che possono impattare l'infrastruttura aziendale.

Le attività principali del SOC prevedono:

- Monitoraggio, identificazione, segnalazione e blocco delle minacce informatiche in real-time 24H 7 giorni su 7.
- Threat Hunting preventivo e real-time per identificare proattivamente le minacce più evolute.
- Malware Analysis, al fine di comprendere l'impatto di una minaccia all'interno di una infrastruttura aziendale.
- Incident Response, che consiste in processi ed attività volti a mitigare e rispondere ad un incidente informatico.
- Early Warning, un servizio erogato sotto forma di "bollettini" che avvisano il cliente circa nuove ed emergenti minacce.
- DarkWeb Analysis, al fine di evidenziare l'esposizione sul darkweb o identificare azioni fraudolente che possano minare la sicurezza informatica dei nostri clienti.
- Vulnerability Assessment, per identificare le vulnerabilità e ridurre la superficie di attacco.

Network Operations Center (NOC)

Il NOC è un centro operativo che si occupa specificamente della gestione e del monitoraggio della rete. Le sue principali funzioni sono:

1. Monitoraggio continuo dello stato di salute della rete 24 ore su 24, 7 giorni su 7.
2. Rilevamento degli alert al fine di identificare tempestivamente eventuali problemi o anomalie nella rete, come interruzioni, rallentamenti o altre anomalie.
3. Risoluzione delle problematiche, ripristinando il servizio nel minor tempo possibile.
4. Ottimizzazione delle prestazioni resolvendo i "bottleneck" e ottimizzando le prestazioni della rete.

Managed Services

La gestione remota dell'infrastruttura si riferisce alla possibilità di monitorare, configurare e controllare a distanza tutti i componenti che compongono l'IT di un'azienda. Ciò include:

- Server: Fisici o virtuali, che ospitano le applicazioni e i dati dell'azienda.
- Reti: Cablate e wireless, che connettono tutti i dispositivi all'interno dell'infrastruttura.
- Dispositivi di rete: Router, switch, firewall, che gestiscono il traffico di rete.
- Applicazioni: Software utilizzati dall'azienda per svolgere le proprie attività.



Una risposta efficace agli incidenti informatici

ELMI ha recentemente realizzato un investimento in un nuovo centro di elevata competenza. Abbiamo aggiunto un tassello fondamentale all'interno della nostra realtà aziendale, offrendo un significativo potenziamento della nostra capacità di erogare servizi avanzati di cybersecurity. L'obiettivo della squadra è quello di migliorare e ampliare la nostra offerta di servizi sia in ambito security-oriented che network-oriented, rispondendo proattivamente alle minacce e agli incidenti di sicurezza con un team dedicato di esperti IT e di cyber security. Questo ci permette di fornire una risposta immediata, efficace e coordinata a qualsiasi incidente, giorno e notte, rappresentando, altresì, un valore aggiunto significativo per la nostra azienda, attraverso:

- +** Accrescimento della nostra capacità di erogazione dei servizi
- +** Ampliamento dei Servizi di cyber security e network center
- +** Control room operativa e presidiata 24H 7 giorni su 7
- +** Rafforzamento/valorizzazione delle risorse umane e della capacità di erogazione di servizi di incident response



Operativi su tutto il territorio

Vantaggi strategici per le organizzazioni

Il nuovo centro operativo è un ambiente moderno, progettato per affrontare le sfide di cyber sicurezza con un approccio integrato e proattivo.

La nostra forza risiede nella multidisciplinarietà del nostro team e nell'esperienza maturata in progetti per aziende di diversi settori, distribuite su tutto il territorio nazionale.

- Approccio integrato che ci consente di rispondere tempestivamente alle esigenze dei clienti;
- Offriamo un servizio personalizzato e su misura a 360 gradi in ambito cyber;
- Competenze trasversali del nostro team, composto da esperti di cyber security, system & network administrator, esperti in ambito normativo e consulenti;
- La nostra attenzione è rivolta alla tecnologia: crediamo fermamente nelle nostre soluzioni, sviluppate per soddisfare le sfide più complesse.

Soluzioni e partner tecnologici

Il nostro centro si avvale di soluzioni di elevata competenza per la corretta erogazione del servizio.

Alle tecnologie pre-esistenti verranno affiancati altri prodotti necessari al funzionamento del processo di analisi, ingaggio, segnalazione degli incidenti di sicurezza.



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.

Pertanto, 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.





Security
Services
Partner

Contatti

security@elmisoftware.com

www.elmisoftware.com