ENGINEERING
INFOGRAPHICS

Garantire la continuità energetica attraverso la sicurezza

Cyber Resilience per proteggere la nostra infrastruttura energetica

L'energia è il motore invisibile e indispensabile della nostra società. Un attacco informatico al settore energetico potrebbe causare blackout su vasta scala, con gravi conseguenze economiche, sociali e per la sicurezza nazionale.

Gli attacchi di ransomware e quelli alla catena di approvvigionamento rappresentano gravi minacce per il settore energetico, mentre la gestione delle identità e degli accessi è cruciale per mitigare rischi di sicurezza.

4 Key Pillars

- **Definire una strategia** per migliorare la security posture
- **Implementare una logica "Zero Trust"** per gestire dinamicamente gli accessi a dati e applicazioni cruciali
- **Adottare SOC con analisi dati avanzate e automazione** per neutralizzare minacce avanzate, persistenti (Advanced Persistent Threats, APTs) e interne (Insider Threats)
- **Prevenire proattivamente gli attacchi**, per riprendere in modo rapido e sicuro l'operatività.

Per affrontare le sfide della Cybersecurity, è essenziale adottare **un approccio olistico** e una difesa **multilivello "in-depth"**. Integriamo soluzioni verticali e trasversali per proteggere dispositivi, identità, dati, infrastrutture tecnologiche, carichi di lavoro e servizi applicativi distribuiti nel cloud. **Combiniamo tecnologie, processi e competenze** secondo gli standard di settore e le moderne metodologie e **best practices** per garantire la sicurezza e la **resilienza** delle operazioni energetiche.

The Value of Technology's Impact

AI-Driven Value

Utilizziamo l'AI per rilevare e prevenire attacchi in tempo reale, analizzare grandi quantità di dati per identificare pattern anomali o comportamenti sospetti, e automatizzare processi di sicurezza come la risposta agli incidenti. Un approccio efficace alla cybersecurity basato sull'AI richiede l'implementazione di **sistemi di difesa avanzati**, la formazione continua del personale per comprendere e utilizzare queste tecnologie in modo appropriato, e la costante evoluzione delle **strategie di sicurezza** per affrontare le minacce sempre più sofisticate del panorama digitale.

Cybersecurity Awareness

Implementiamo una Gestione dell'Accesso e delle Identità (IAM) robusta per controllare l'accesso agli ambienti critici e per garantire la conformità normativa, ottimizzando i costi operativi e promuovendo una cultura della sicurezza informatica fondamentale per la crescita aziendale sostenibile. Questo approccio non solo **rafforza la sicurezza interna**, ma anche **la consapevolezza dei consumatori** di energia riguardo alle **migliori pratiche di sicurezza informatica**, contribuendo così a consolidare l'intera catena di sicurezza del settore.

Composable Business Models

La cybersecurity componibile applicata nell'energia implica la creazione di **framework di sicurezza modulari** che possono essere adattati e integrati nell'infrastruttura esistente. L'obiettivo è migliorare la protezione contro le minacce informatiche in evoluzione, mantenendo al contempo l'efficienza operativa e l'affidabilità dei sistemi energetici. Il **Composable Mesh** nel nostro framework SOC rivoluziona l'approccio tradizionale, avvicinando i punti di controllo e le misure di sicurezza direttamente agli asset critici attraverso una **piattaforma centralizzata multistrato**.

Our Toolbox

Our Impact

SCOPRI DI PIÙ →