TESORION

Task Force Hybrid Shield

Hybride bescherming van kritieke infrastructuur

Kritieke infrastructuur gaat gebukt onder onder zware hybride dreigingen. Cyberaanvallen en fysieke sabotage, vaak tegelijk. Daarom gelden in 2026 twee nieuwe wetten: de Cyberveiligheidswet (Cbw, NIS2) en de Wet weerbaarheid kritieke entiteiten (Wwke). Bestuurders worden direct verantwoordelijk.

Niet voldoen kan leiden tot hoge boetes en persoonlijke aansprakelijkheid. De reden is helder. Europa ziet meer sabotage van onderzeese kabels, spoor, ziekenhuizen, water en energie, datacentra en meer. Vaak met simpele middelen. Moeilijk te zien. Moeilijk te stoppen. Daarom bundelen de Special Forces van Nassau420 en de cyberexperts van Tesorion hun kracht in Task Force Hybrid Shield.

Voordelen

Ons doel:
Jouw bestuur, crisisteam en beveiligers sterker maken in het herkennen, stoppen en herstellen van hybride aanvallen. In lijn met Cbw (NIS2) en Wwke.

Onze aanpak:
- Ondersteuning op 3 niveaus: Bestuur/Directie, Crisisorganisatie & Veiligheidsfunctionarissen
- Door (ex-)Special Forces, cyberspecialisten en experts E. de Jong en prof. dr. ir. D. Dohmen
- Scenario's direct inzetbaar in jouw bedrijf
- Actuele sabotagelessen uit Oekraïne verwerkt

Task Force Hybrid Shield:

Een unieke aanpak die organisaties snel weerbaar maakt. Hyper-realistisch.
'We Attack to Save You.'

Wat je krijgt:
- Heldere uitkomsten. Geen jargon
- Getraind crisisteam
- Overzicht kwetsbaarheden
- Concrete maatregelen
- Duidelijke stappen richting
- Cbw (NIS2) en Wwke

Ravenswade 2A, 3439 LD Nieuwegein, Nederland | 088 - 274 78 80 | info@tesorion.nl | www.tesorion.nl

TESORION

Eén aanpak voor zowel fysieke als digitale veiligheid

Task Force Hybrid Shield is de eerste samenwerking in Nederland die cyberveiligheid, fysieke beveiliging en menselijke weerbaarheid integraal combineert binnen één programma..

De aanpak van Task Force Hybrid Shield bestaat uit geïntegreerde trainingen, simulaties en realistische scenario's waarin fysieke, digitale en organisatorische kwetsbaarheden gelijktijdig worden getest.

Drie niveaus

	BESTUUR & DIRECTIE (strategisch)	CRISISTEAM (operationeel)	VEILIGHEIDSFUNCTIES (papieren aanval)
Duur	1 middag	1 dag	1 week
Doel	Inzicht in cyberen fysieke risico's	Een crisisteam dat samenwerkt en handelt onder druk	Snel beeld van risico's en verbeterpunten
Doelgroep	Bestuur en directie	Crisisteam en beveiligers	MT's en security officers
Inhoud	• Lezing Future-of-War • Workshop hybride dreiging (Cbw/Wwke) • Basis sabotageleer • CARVER risicomodel	• Workshop hybride aanval • Mini-missies Cyber + Fysiek • Eindmissie leiderschap onder druk in trainingscentrum • Team debrief Special Forces	• CARVER inschatting en Cyber quickscan op basis van interviews en OSINT • Aanbeveling Cbw/Wwke • Presentatie aan MTw
Locatie	Op locatie bij uw organisatie	Nassau420 Trainingscentrum	Op locatie bij uw organisatie
All Inclusive	Overzicht Cbw (NIS2) en Wwke op 1 pagina	Eten / drinken en alle oefenmaterialen	Actieplan op 1-2 pagina's
Optioneel	Full Mission Profile (FMP): een realistische aanval door ons red-team om uw processen te testen		