FORES ENGINEERING

Profili ricercati

- Sistemista Telecom Networking
- Sistemista Telecom Radio
- Specialista di Infrastruttura
- Cyber Security Specialist
- Data Analyst
- Data Engineer

Attività (adatte prevalentemente a Tirocini, ma non escludono Tesi specifiche)

Adattamento di soluzioni tecnologiche di derivazione IT ad ambito specifico OT / ICS

- Syslog, Event Logs, SIEM, IoC, Security, Audit Reports.
- Integrazione Piattaforma Incident Management con SIEM interno / cliente, o MISP esterno.
- Virtualization Platforms, High Availability and Fault Tolerant computing platforms.
- Endpoint Security / Application Allowlisting – Denylisting.
- Vulnerability Scan Tools / Asset Inventory Scanning Tools.
- Network Traffic Analysis.
- Industrial Firewall, Deep Packet Inspection e mappatura flussi di comunicazione.
- SSL Inspection e in-transit encryption.
- Honeypot / Decoys.
- Authenticator / MFA / Centralized Authentication Systems.
- IDS / IPS, Deep Packet Inspection.
- Identity / Microsegmentation / ZTNA.
- Backup & Disaster Recovery Solutions.

Supporto per mantenimento e miglioramento del programma di sicurezza per IACS Service Provider (62443-2-4)

- Sviluppo / miglioramento / mantenimento dei processi aziendali IEC 62443-2-4.
- Sviluppo / miglioramento / mantenimento di meccanismi di Threat Intelligence e valutazione scenari di minaccia.
- Sviluppo / miglioramento / mantenimento di metodologie di Risk Assessment e integrazione con ciclo di vita Safety (61511).

- Sviluppo / miglioramento / mantenimento di processi di threat modeling su asset o architetture di riferimento.
- Sviluppo / miglioramento / mantenimento di configuration / security baselines per equipment / sistemi specifici.
- Sviluppo / miglioramento / mantenimento di verifiche dei controlli di sicurezza definiti per gli asset.
- Sviluppo / miglioramento / mantenimento di metodologie di Code Review e Software Bill of Material.
- Sviluppo / miglioramento / mantenimento di strategie e soluzioni di pen-testing specifiche per validazione.
- Sviluppo / miglioramento / mantenimento di Playbooks / Runbooks per azioni di intervento / manutenzione / risposta specifica incidents.
- Sviluppo / miglioramento / mantenimento delle metodologie di Network e Endpoint Security specifiche OT / ICS.
- Sviluppo / miglioramento / mantenimento di gestione di soluzioni di Remote Access e Privileged Access Management.

Supporto allo sviluppo di un Laboratorio di Cybersecurity OT / ICS (integrato con Laboratorio Idrogeno)

- A supporto dei processi aziendali IEC 62443-2-4 e sviluppo progetti interni.
- Modularità ed interfacciabilità con sistemi esterni o package aggiuntivi.
- Base per formazione interna ed esterna.
- Ambiente per product testing, demo.
- Showroom tecnologico per partnership, manufacturer e clienti.

Spunti per Tirocini e Tesi (ci possono essere tematiche complementari)

Cyber Security nelle Infrastrutture Critiche OT / ICS:

- Esamina la sicurezza delle infrastrutture critiche, come centrali elettriche, stazioni di trattamento delle acque o reti di trasporto, concentrandoti su come i sistemi IACS siano impattati da attuale stato di minacce.
- Risk Assessment (Qualitative, Quantitative) e valutazione dei rischi nelle differenti fasi di esecuzione di un progetto.
- Come selezionare la metodologie di Risk Assessment.
- Integrazione tra Safety e Security.
- Valutazione, priorità e benefici costi dei controlli di sicurezza e fattori di riduzione del rischio.

- Metodologie di valutazione e definizione dei Security Requirements.
- Governance e maturità tecnologica nel mantenimento e gestione di un piano di sicurezza informatica in ambito OT / ICS (62443-2-1 / NIST CSF / ISO 27001)

Sensibilizzazione alla Sicurezza nell'ambito OT / ICS:

- Studia come promuovere la consapevolezza e la formazione sulla sicurezza tra il personale coinvolto nell'implementazione e nell'uso di sistemi di controllo industriale.
- Requisiti legislativi e framework normativi a supporto.
- Tematiche ed approcci per aumentare sensibilità e comprensione sull'argomento.
- Simulazione Attacco di manipolazione Impianto Produzione Idrogeno.
- Analogie ed integrazioni tra HSE, Safety e Cybersecurity.
- Raccolta dati, presentazione scenari percorribili, case studies recenti o di comune riferimento nei segmenti industriali colpiti.

Third Party Risk Management OT / ICS:

- Condurre o integrare analisi del rischio per valutare le vulnerabilità e le minacce associate alle terze parti coinvolte.
- Stabilire standard di sicurezza chiari e requisiti minimi che le terze parti devono soddisfare.
- Implementare meccanismi di valutazione per le terze parti rispetto agli standard di sicurezza stabiliti.
- Garantire che le terze parti siano conformi alle normative di settore e che rispettino i requisiti contrattuali in materia di sicurezza.
- Collaborare con le terze parti per sviluppare piani di gestione degli incidenti.
- Audit sulle terze parti per verificare la conformità agli standard di sicurezza definiti.

Certificazione e Conformità dei Sistemi nell'ambito OT / ICS:

- Esaminare le regolamentazione, direttive e gli standard specifici che impattano infrastrutture critiche
- interazione tra IEC 61511, IEC 62443 e ISA TR84.00.09,
- Valutare come le organizzazioni possono ottemperare a tali requisiti, identificando sfide e soluzioni per la conformità.
- Valutare impiatti NIS2, DL 105/2019, Direttiva Macchine, e Safety.
- Requisiti assicurativi o sviluppo di un programma di Cybersecurity migliorativo a riduzione dei rischi di stop produttivo.

Analisi e Gestione delle Minacce e Vulnerabilità nell'ambito OT / ICS:

- Effettua un'analisi approfondita delle minacce e delle vulnerabilità specifiche per i sistemi di controllo industriale, identificando i punti critici di attacco e le misure preventive.
- Determinare metodologie di classificazione delle vulnerabilità.
- Metodi di prioritizzare azioni mitigative per mantenere una postura di sicurezza e superfici di attacco nel ciclo di vita di un progetto.
- Sviluppo, valutazione di piattaforme di Application Sandboxing per analisi malware o comportamenti applicazioni.

Gestione degli Incidenti di Sicurezza nell'ambito OT / ICS:

- Esaminare come le organizzazioni affrontano e gestiscono gli incidenti di sicurezza nei sistemi di controllo industriale.
- Proporre e sviluppare piani di risposta agli incidenti specifici per IACS e condurre esercitazioni di simulazione.
- Coordinamento tra staff Operation e IT e gestione delle responsabilità.
- Collegare piattaforma software di incident management con SIEM o da sorgenti esterne (clienti).
    - Blockchain per la Sicurezza degli IACS in Ambito Digital Forensic Preservation: Esplorare come la tecnologia blockchain può essere utilizzata per preservare la raccolta delle evidenze in caso di analisi di incidente.
    - Sviluppo e valutazione di piattaforme di Application Sandboxing per analisi malware o comportamenti applicazioni.

Sicurezza delle Reti Industriali OT / ICS:

- Progettazione, l'implementazione e la valutazione della sicurezza delle reti e dei sistemi di controllo industriali, inclusi i protocolli di comunicazione, le misure di isolamento e la protezione delle comunicazioni tra dispositivi OT.
- Physical Security.
- Segmentazione / Microsegmentazione / ZTNA in reti industriali. Test di tecnologie leader di mercato.
- Sicurezza dei principali protocolli di comunicazione e impatti della cifratura del traffico in transito.
- Impatti e strategie per impiego di reti wireless in ambiti industriali.
- Esaminare i rischi legati Industrial IoT e strategie per mitigarli, ad esempio segmentazione e hardening.

Monitoraggio Infrastruttura e Security in ambito OT / ICS:

- Criticità di monitoraggio di sistemi IT in ambito OT / ICS.

- Requisiti di legge NIS2 per gestione classificazione, monitoraggio, tracciatura e analisi degli incident.
- Definizione allarmi, inclusione di gestione allarmi e procedure di incident management.
- Trasportare visualizzazione stato di Security a pagine grafiche.
- Dimostrazione integrata e applicazione tramite piattaforma SIEM / Logging e Incident Management.
- Network Traffic Inspection e Meccaniche di IPS / IDS.

Analisi dei Log e SIEM nell'ambito OT / ICS:

- Approfondisci come i log dei sistemi IACS possano essere analizzati per rilevare e rispondere a minacce di sicurezza. Esamina come i sistemi SIEM (Security Information and Event Management) possano essere implementati e personalizzati per IACS per ottenere Indicatori di Compromissione.
- Dimostrazione e applicazione tramite piattaforma SIEM / Logging.
- Trasportare visualizzazione stato di Security a pagine grafiche.

Protezione dei Dati e Salvaguardia della Proprietà Intellettuale nei Sistemi di Controllo Industriale (IACS):

- Esamina le sfide legate alla protezione dei dati sensibili e alla proprietà intellettuale all'interno dei sistemi di controllo industriale.
- affrontare questioni come la crittografia dei dati, la gestione degli accessi e delle autorizzazioni, e la protezione dei segreti industriali nei contesti IACS.
- Protezione delle logiche PLC e di impianto.
- Code review e Software bill of Material.
- valutare come le organizzazioni possono bilanciare la necessità di condividere dati all'interno dell'azienda con la protezione delle informazioni riservate, sviluppando strategie per affrontare questo equilibrio delicato.

Autenticazione, Identity Management e Remote Access nei Sistemi di Controllo Industriale (IACS):

- Utilizzo di autenticazione e identity management nei contesti OT / ICS.
- Esamina come le organizzazioni possono garantire che solo utenti autorizzati possano accedere ai sistemi di controllo e come gestire le identità e le credenziali in modo sicuro.
- uso di autenticazione a più fattori (MFA), single sign-on (SSO), e la gestione delle identità privilegiate (PIM).
- Impatti dell’uso di tecnologie di autenticazione centralizzata nelle infrastrutture dei sistemi di controllo industriale.
- Gestione ed applicazione di sistemi di Accesso e Supervisione Remota agli impianti di controllo industriali.