SERVIZI DI OT SECURITY

PROTEZIONE CONTINUA E SMART PER AMBIENTI INDUSTRIALI CRITICI

BV·TECH

SERVIZI DI OT SECURITY

Attività Annuale

OT Visibility

Asset Discovery
Identificazione automatica dispositivi sulla rete (PLC, SCADA, HMI, DCS) effettuata in modo passivo, non intrusivo, tramite l'analisi del traffico e la ricerca dei fingerprint all'interno di database di firme di dispositivi industriali.
Associazione di metadati (versione firmware, vendor) ai dispositivi identificati.

Network Topology Mapping
Generazione di una mappa visiva della rete OT con interconnessioni, protocolli, flusso dati.

SERVIZI DI OT SECURITY

Attività Annuale

OT Security Assessment

Vulnerability Assessment dei dispositivi OT

Partendo dalla conoscenza dei dispositivi presenti sulla rete (PLC, SCADA, HMI, DCS), comprensiva di marca, modello e versione del firmware, l'attività consiste nella valutazione delle vulnerabilità note e nella prioritizzazione degli interventi in base alla probabilità che una vulnerabilità venga effettivamente sfruttata, in base ai seguenti fattori chiave:

- **Network Location & Accessibility**: La misura in cui un asset è esposto a potenziali attori minacci, inclusa la sua collocazione all'interno delle zone di rete.
- **Active Exploitation Data (KEV/EPSS)**: Le sonde di rete OT integrano il catalogo delle Known Exploited Vulnerabilities (KEV) e il Sistema Exploit Prediction Scoring System (EPSS) per dare priorità alle vulnerabilità attualmente prese di mira dai Threat Actor, migliorando l'efficienza nella valutazione del rischio.
- **Communication Patterns**: Analisi delle interazioni con altri asset (capacità di movimento laterale).
- **Protocol & Port Exposure**: Il numero di porte aperte e i protocolli industriali specifici in uso.
- **Compensating Controls**: Valutazione delle misure di sicurezza esistenti che riducono la probabilità di un incidente

Vulnerability Assessment dell'infrastruttura di rete OT

Viene svolta un'attività di assessment dell'infrastruttura di rete rilevata, effettuando una gap analisys rispetto alle best practice di riferimento quali **Purdue Model** e **IEC 62443**

SERVIZI DI OT SECURITY

Attività continuativa a canone

OT Network Detection and Response (NDR)

Acquisizione Traffico
Osservazione del traffico, avendo cura di mantenere un impatto zero sull'operatività OT.

Creazione di un modello di dati di campo
IP, MAC, protocolli industriali (Modbus, OPC UA), connessioni, comportamenti dei dispositivi.

Deep packet inspection (DPI)
Analisi delle comunicazioni, riconoscimento dei principali protocolli industriali e analisi dei dati scambiati.

Invio di Alert
Avviso in tempo reale in caso di rilevazione di attività sospette e/o incidenti di sicurezza.
Suggerimento di azioni di mitigazione e ripristino.

SERVIZI DI OT SECURITY

Servizio a canone

Remote Port Architecture

Il servizio utilizza una famiglia di appliance sviluppate da BV TECH, chiamata **Remote Port Architecture (RPA)**.

Essa consente di acquisire il traffico di rete da infrastrutture ICT con estesa distribuzione geografica e numero considerevole di asset, su più siti remoti, mediante una appliance chiamata **Remote Filter & Forwarder (RFF)**.

Il traffico viene filtrato, compresso e criptato e solo i flussi di interesse sono inviati centralmente ad una seconda appliance chiamata **Traffic Collector (TC)**, che decripta il traffico e lo rende disponibile ad un servizio di packet inspection effettuato mediante sonda OT.

Se la connessione tra i siti non è stabile, il traffico di interesse è registrato localmente su RFF e inoltrato a TC quando possibile.

Nel caso di **siti completamente isolati**, durante gli interventi di manutenzione, il traffico registrato su RFF può essere analizzato.

Le appliance RFF e TC non hanno funzionalità di packet inspection, il che le rende ideali per le situazioni in cui il traffico di interesse è limitato ed è richiesta una soluzione conveniente.