Elementi essenziali e gestione della sicurezza informatica (settore energetico)

CSP001

Argomento 5/7: Progettazione e implementazione di architetture sicure per i sistemi energetici

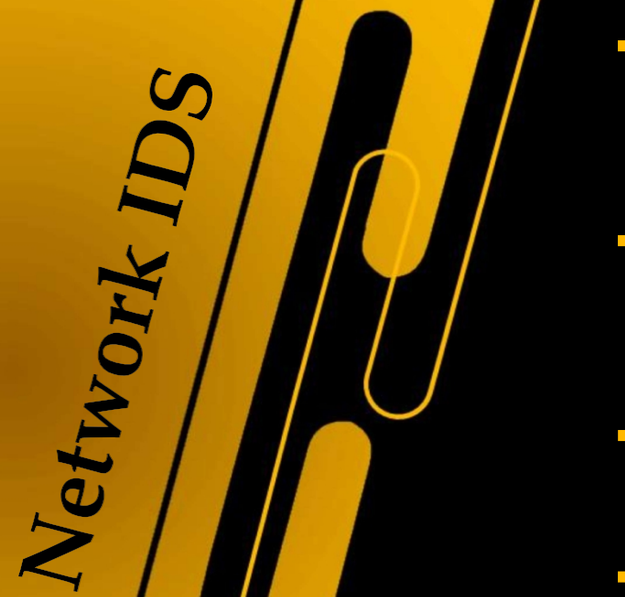
PRESENTAZIONE DI: STYLIANOS KARAGIANNIS (PDMFC, PORTOGALLO)

Host IDS - SIEM

Host IDS - SIEM

Protezione del settore energetico con Host IDS - SIEM

- I sistemi di rilevamento delle intrusioni basati su host (IDS) e le piattaforme di gestione delle informazioni e degli eventi di sicurezza (SIEM) svolgono un ruolo cruciale nella protezione del settore energetico.
- Host IDS monitora i singoli dispositivi o host all'interno del infrastruttura
  per attività sospette o tentativi di accesso non autorizzati.
- Fornisce funzionalità di rilevamento e risposta in tempo reale per mitigare potenziali minacce alla sicurezza.
- Le piattaforme SIEM aggregano dati provenienti da varie fonti, tra cui avvisi Host IDS, traffico di rete e registri di sistema, per fornire una visibilità completa sugli incidenti di sicurezza.
- Vantaggi: a) Rilevamento tempestivo delle violazioni della sicurezza e delle minacce interne, b) Miglioramento delle capacità di risposta agli incidenti attraverso avvisi in tempo reale e azioni di risposta automatizzate, c) Maggiore visibilità e analisi forense degli eventi di sicurezza per una gestione proattiva dei rischi.



IDS di rete

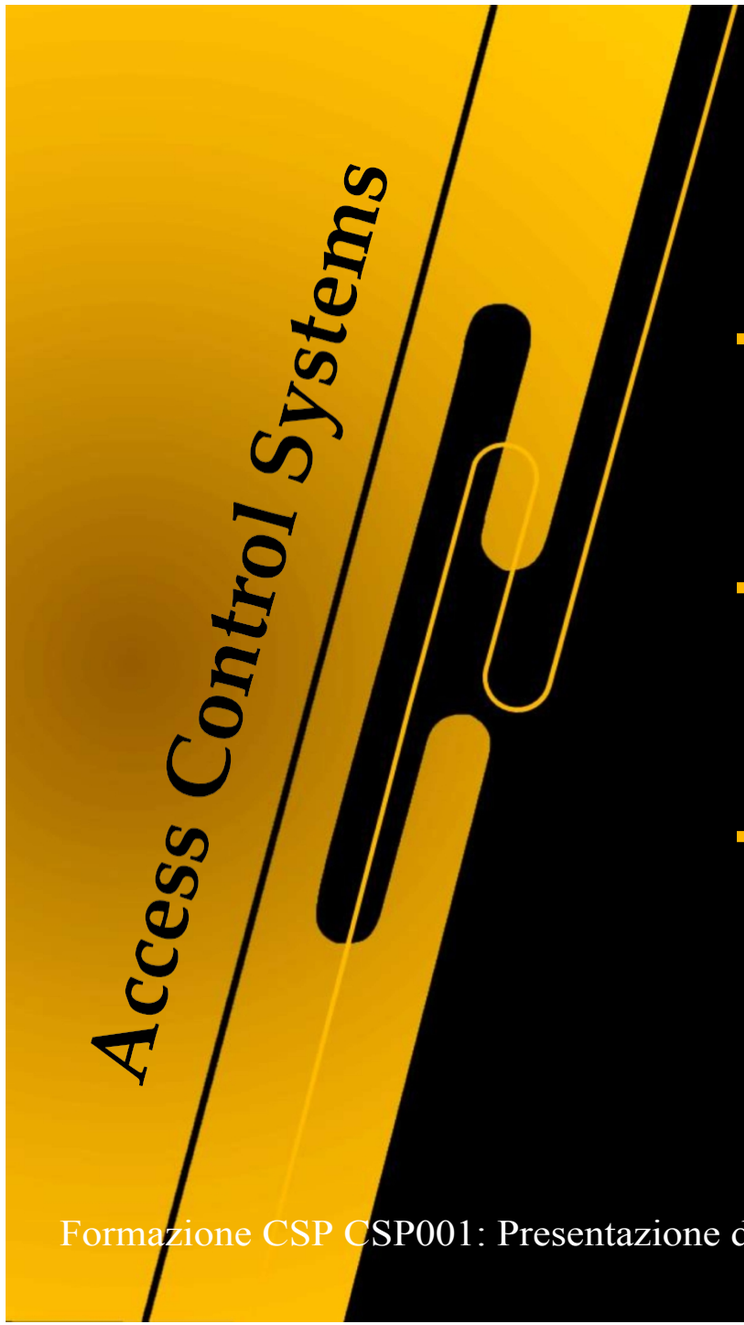
Protezione del settore energetico con Network IDS

- I sistemi di rilevamento delle intrusioni basati sulla rete (IDS) svolgono un ruolo fondamentale nella protezione del settore energetico monitorando il traffico di rete alla ricerca di segni di attività dannose.
- Gli IDS di rete analizzano passivamente i pacchetti di rete per rilevare e segnalare comportamenti sospetti, come tentativi di accesso non autorizzati o modelli di traffico anomali.
- Operano al perimetro della rete o all'interno dei segmenti interni per fornire visibilità sulle potenziali minacce alla sicurezza.
- Vantaggi: a) Rilevamento tempestivo delle minacce esterne, inclusi malware, tentativi di phishing e accessi non autorizzati, b) Identificazione delle minacce interne e dei comportamenti anomali all'interno della rete energetica,
  c) Maggiore visibilità della rete per una migliore intelligence sulle minacce e risposta agli incidenti.

Protezione e risposta degli endpoint (EDR)

Protezione del settore energetico

- Le soluzioni di rilevamento e risposta degli endpoint (EDR) forniscono funzionalità avanzate di rilevamento e risposta alle minacce per i singoli dispositivi e endpoint all'interno dell'infrastruttura energetica, compresi quelli che utilizzano Modbus e DNP3.
- Le soluzioni EDR monitorano continuamente le attività degli endpoint, analizzano i modelli di comportamento e rilevano attività sospette indicative di minacce informatiche.
- In caso di incidente di sicurezza, l'EDR consente di intraprendere azioni di risposta rapide, come mettere in quarantena gli endpoint interessati, contenere la minaccia e avviare misure correttive per ridurre al minimo l'impatto sui sistemi critici.



Sistemi di controllo degli accessi

Protezione del settore energetico

- I sistemi di controllo degli accessi applicano politiche di autenticazione e autorizzazione granulari per regolare l'accesso a sistemi, applicazioni e risorse sensibili all'interno dell'infrastruttura energetica, compresi quelli che utilizzano Modbus e DNP3.
- Questi sistemi utilizzano tecniche quali il controllo degli accessi basato sui ruoli (RBAC), l'autenticazione a più fattori (MFA) e l'accesso con privilegi minimi per limitare i tentativi di accesso non autorizzati e mitigare il rischio di minacce interne.
- I sistemi di controllo degli accessi forniscono anche audit trail e funzionalità di registrazione per tracciare le attività degli utenti e garantire la conformità alle politiche di sicurezza e ai requisiti normativi.

Data Encryption - Modbus

Modbus - Crittografia dei dati

Modbus

- Le tecnologie di crittografia dei dati svolgono un ruolo fondamentale nella protezione dei dati sensibili in transito e inattivi all'interno delle infrastrutture energetiche, compresi i dati trasmessi tramite i protocolli Modbus e DNP3.
- Modbus è un protocollo ampiamente utilizzato nei sistemi di controllo industriale (ICS) nel settore energetico per la comunicazione tra dispositivi quali controllori logici programmabili (PLC) e sistemi di supervisione, controllo e acquisizione dati (SCADA).
- L'implementazione di meccanismi di crittografia dei dati, come TLS (Transport Layer Security), per le comunicazioni Modbus garantisce che i dati scambiati tra i dispositivi siano crittografati, proteggendoli dall'intercettazione e dall'accesso non autorizzato.
- Ad esempio, l'implementazione della crittografia Modbus tramite TLS garantisce che i comandi, i dati dei sensori e i segnali di controllo trasmessi tra PLC e sistemi SCADA siano crittografati, proteggendo le operazioni critiche dalle minacce informatiche.

DNP3 - Crittografia dei dati

Protocollo di rete non attendibile 3

- Il DNP3 (Distributed Network Protocol) è un protocollo di comunicazione ampiamente utilizzato nel settore energetico, in particolare nei sistemi di automazione delle utility e delle sottostazioni, per lo scambio di dati in tempo reale.
- L'implementazione della crittografia dei dati per i canali di comunicazione DNP3 è fondamentale per proteggere i dati operativi sensibili trasmessi tra dispositivi come le unità terminali remote (RTU) e i centri di controllo.
- Per migliorare la sicurezza dei canali di comunicazione DNP3, l'azienda di servizi pubblici decide di implementare la crittografia AES (Advanced Encryption Standard) per i dati scambiati tra le RTU e il centro di controllo.
- La crittografia AES encryption prevede l'uso di un algoritmo di crittografi per crittografare i dati data packets inviati tramite DNP3 canali di comunicazione utilizzando un algoritmo di crittografia simmetrica.
- La crittografia garantisce la sicurezza dei dati operativi critici, prevenendo interruzioni dei processi essenziali e mantenendo l'affidabilità dei sistemi di distribuzione dell'energia.

Secure Architecture Pt.1

Architettura sicura Pt.1

Mettere tutto insieme?

- Definire i requisiti di sicurezza: identificare e documentare i requisiti e gli obiettivi di sicurezza specifici per i sistemi energetici.
- Gestione dell'inventario e delle risorse: creare un inventario di tutti i dispositivi, endpoint e sistemi all'interno dell'infrastruttura energetica, compresi quelli che utilizzano protocolli come Modbus e DNP3.
- Implementare sistemi di rilevamento delle intrusioni basati su host (IDS) su dispositivi e host critici all'interno dell'infrastruttura energetica per monitorare attività sospette, inclusi tentativi di accesso non autorizzati e comportamenti anomali. Integrare gli avvisi IDS host con una piattaforma SIEM (Security Information and Event Management) per consentire la registrazione, la correlazione e l'analisi centralizzate degli eventi di sicurezza nella rete energetica.
- Installare sistemi di rilevamento delle intrusioni basati su rete (IDS) in punti strategici all'interno dell'infrastruttura di rete per analizzare passivamente il traffico di rete alla ricerca di segni di attività dannose, compresi quelli che interessano i sistemi che utilizzano Modbus e DNP3. Configurare i sensori IDS di rete per monitorare i punti di ingresso/uscita e i segmenti di rete critici che gestiscono il traffico relativo ai sistemi energetici.

Architettura sicura Pt.2

Mettere tutto insieme?

- Implementare soluzioni di rilevamento e risposta degli endpoint (EDR) sui dispositivi endpoint che comunicano tramite i protocolli Modbus e DNP3 per fornire funzionalità avanzate di rilevamento e risposta alle minacce. Configurare le soluzioni EDR per monitorare le attività degli endpoint, analizzare i modelli di comportamento e rilevare attività sospette indicative di minacce informatiche.
- Applicare le politiche di controllo degli accessi: implementare sistemi di controllo degli accessi per applicare le politiche di autenticazione e autorizzazione per l'accesso a sistemi, applicazioni e risorse sensibili all'interno dell'infrastruttura energetica. Configurare i sistemi di controllo degli accessi per applicare l'accesso con privilegi minimi e l'autenticazione a più fattori (MFA) per i sistemi che utilizzano Modbus e DNP3.
- Implementare la crittografia dei dati: implementare meccanismi di crittografia dei dati, come TLS per Modbus e AES per DNP3, per garantire la riservatezza e l'integrità dei dati trasmessi tra dispositivi e sistemi. Configurare i protocolli di crittografia per crittografare i canali di comunicazione per i protocolli Modbus e DNP3 al fine di proteggere da intercettazioni e manomissioni dei dati.

Secure Architecture Pt.3

Architettura sicura Pt.3

Mettere tutto insieme?

- Monitoraggio del traffico di rete: implementare soluzioni di monitoraggio del traffico di rete per acquisire e analizzare il traffico di rete relativo ai sistemi energetici, compresi quelli che utilizzano Modbus e DNP3. Configurare strumenti di monitoraggio del traffico di rete per raccogliere i registri e analizzare i modelli di traffico alla ricerca di segni di comportamenti anomali o potenziali minacce alla sicurezza.
- Monitoraggio e aggiornamenti continui: monitorare continuamente le misure e i sistemi di sicurezza per rilevare e rispondere agli incidenti di sicurezza in tempo reale. Aggiornare regolarmente le misure di sicurezza, comprese le regole IDS, le configurazioni SIEM e i protocolli di crittografia, per affrontare le minacce e le vulnerabilità emergenti.
- Risposta e gestione degli incidenti: sviluppare e documentare piani e procedure di risposta agli incidenti per rispondere in modo efficace e mitigare gli incidenti di sicurezza che interessano l'infrastruttura energetica. Stabilire canali di comunicazione e procedure di escalation per coordinare gli sforzi di risposta agli incidenti con i team interni e le parti interessate esterne.
- Conformità e audit: condurre audit e valutazioni periodici sulla sicurezza per garantire la conformità ai requisiti normativi, agli standard di settore e alle politiche di sicurezza dell'organizzazione. Conservare la documentazione e le prove dei controlli, delle configurazioni e delle attività di sicurezza per dimostrare la conformità durante gli audit e le ispezioni normative.

Grazie

Relatore: Stylianos Karagiannis (PDMFC, Portogallo) Si prega

di inviare tutte le domande a:
stylianos.karagiannis@pdmfc.com