Infrastrutture critiche e sicurezza per la salute

CSP008

PRESENTAZIONE DA PARTE DI: STYLIANOS KARAGIANNIS (PDMFC, PORTOGALLO)

Introduction

Settore sanitario

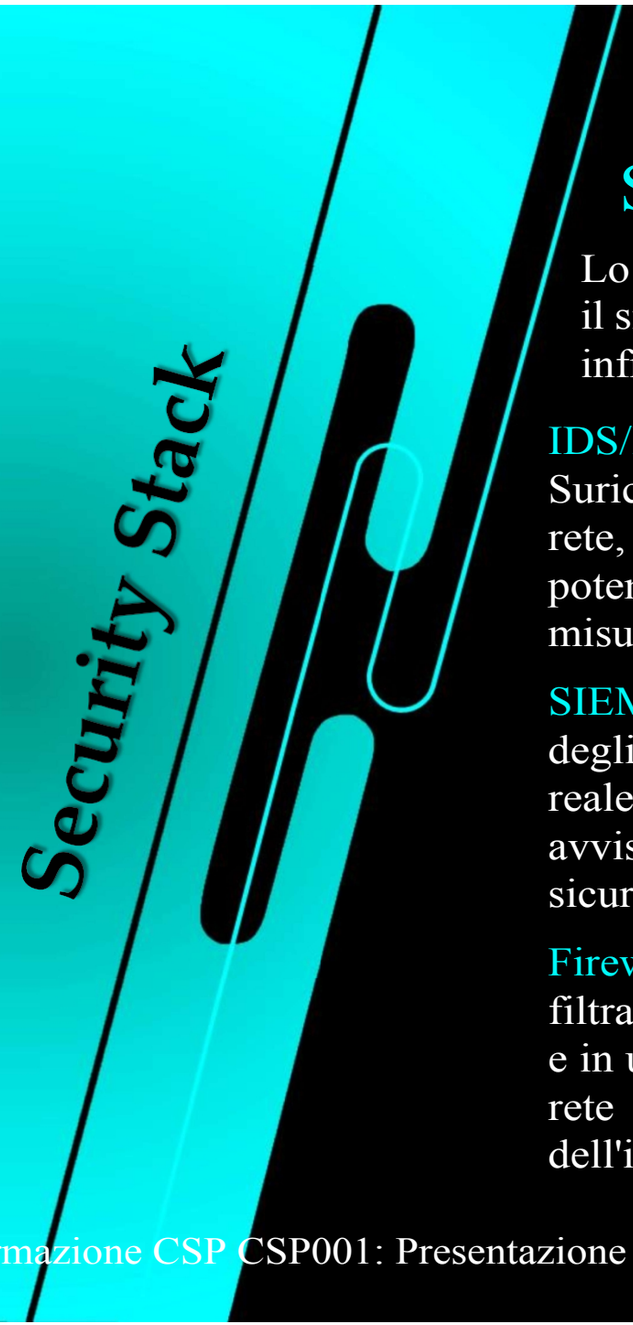
Nell'ambiente sanitario, risorse come Windows Domain Controller, Health Information System, Laboratory Information System, Picture Archiving and Communication System, DICOM-Enabled Modality e Windows Host sono interconnesse tramite VLAN Ethernet, facilitando lo scambio di dati senza soluzione di continuità e consentendo funzioni critiche come l'autenticazione, la gestione delle cartelle cliniche, la diagnostica per immagini e l'elaborazione generale dei dati.

Attività e protocolli in sanità

- DICOM (Digital Imaging and Communications in Medicine): DICOM è uno standard per la trasmissione, l'archiviazione e la condivisione di dati di imaging medico come radiografie, risonanze magnetiche e TAC. È ampiamente utilizzato in ambito sanitario per lo scambio di immagini mediche tra diversi sistemi e strutture.
- PACS (Picture Archiving and Communication System): Il PACS è un sistema utilizzato per archiviare, recuperare e distribuire immagini mediche. Si integra con DICOM e fornisce agli operatori sanitari l'accesso alle immagini dei pazienti e ai relativi dati.
- HL7 FHIR (Health Level Seven Fast Healthcare Interoperability Resources): HL7 FHIR è uno standard per lo scambio di informazioni sanitarie elettroniche. Consente l'interoperabilità tra diversi sistemi sanitari e facilita lo scambio di dati del paziente come cartelle cliniche, risultati di laboratorio e osservazioni cliniche.
- Controller di dominio - Active Directory: Active Directory è un servizio di directory sviluppato da Microsoft per gestire le identità degli utenti, le autorizzazioni e l'accesso alle risorse all'interno di una rete. Nelle organizzazioni sanitarie, Active Directory viene utilizzato per gestire gli account utente, i controlli di accesso e l'autenticazione.

Sicurezza sanitaria

Stack di sicurezza

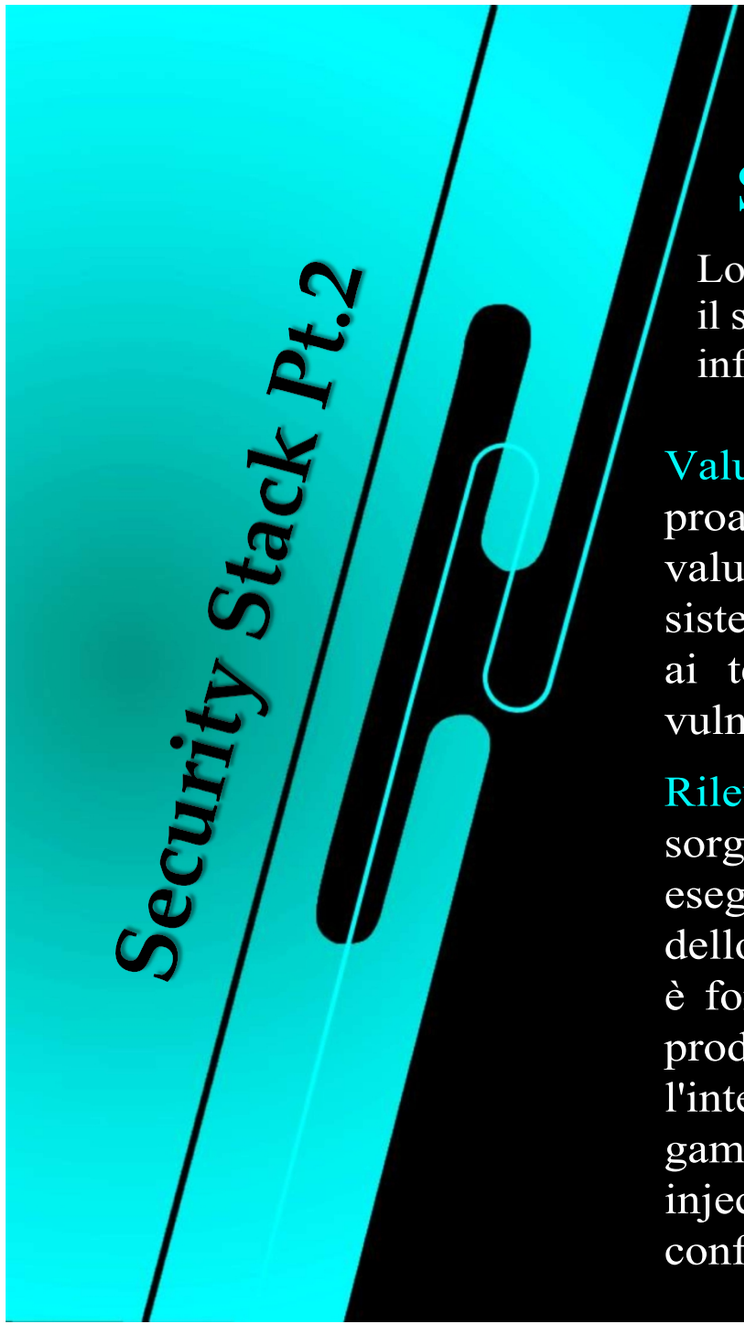


Lo stack di sicurezza in ambito sanitario comprende componenti essenziali volti a fortificare il sistema di sicurezza.
infrastruttura di rete e proteggere i dati sensibili dei pazienti.

IDS/IPS (Intrusion Detection System/Intrusion Prevention System): L'IDS/IPS, fornito da Suricata, funge da guardiano vigile della rete sanitaria. Monitora continuamente il traffico di rete, analizzandolo alla ricerca di schemi o anomalie sospette che possano indicare una potenziale minaccia alla sicurezza. In caso di minaccia rilevata, il sistema può adottare misure proattive per evitare che comprometta l'integrità o la riservatezza della rete.

SIEM (Security Information and Event Management): Aggrega e mette in relazione i dati degli eventi di sicurezza provenienti da varie fonti della rete, fornendo visibilità in tempo reale su potenziali minacce o attività sospette. Grazie a funzionalità avanzate di analisi e di avviso, il SIEM consente ai team di sicurezza di rispondere rapidamente agli incidenti di sicurezza, riducendo al minimo l'impatto potenziale.

Firewall: Rafforza le difese perimetrali della rete sanitaria. Grazie a solide funzionalità di filtraggio basate su regole, il firewall applica i criteri di sicurezza, regola il traffico in entrata e in uscita e vanifica i tentativi di accesso non autorizzato. Creando una barriera sicura tra la rete interna e le minacce esterne, il firewall aumenta la resilienza complessiva dell'infrastruttura sanitaria.



Sicurezza sanitaria

Stack di sicurezza Pt.2

Lo stack di sicurezza in ambito sanitario comprende componenti essenziali volti a fortificare il sistema di sicurezza.
infrastruttura di rete e proteggere i dati sensibili dei pazienti.

Valutazione delle vulnerabilità: Strumenti come Velociraptor consentono una gestione proattiva della postura di sicurezza nell'ambiente sanitario. Effettuando scansioni e valutazioni complete, Velociraptor identifica potenziali punti deboli o vulnerabilità nei sistemi, nelle applicazioni e nelle configurazioni. Questo approccio proattivo consente ai team di sicurezza di stabilire le priorità e di affrontare tempestivamente le vulnerabilità, riducendo al minimo il rischio di sfruttamento e di violazione dei dati.

Rilevamento precoce delle vulnerabilità: Gli strumenti SAST analizzano il codice sorgente delle applicazioni in modo statico, ovvero ispezionano il codice senza eseguirlo. Ciò consente di rilevare le vulnerabilità nelle prime fasi del ciclo di vita dello sviluppo, anche prima che l'applicazione venga distribuita. Il rilevamento precoce è fondamentale per evitare che le vulnerabilità vengano introdotte negli ambienti di produzione, dove possono rappresentare rischi significativi per i dati dei pazienti e l'integrità del sistema. Gli strumenti SAST sono progettati per rilevare un'ampia gamma di difetti di sicurezza comuni, come le vulnerabilità di iniezione (SQL injection, XSS), i problemi di autenticazione, l'archiviazione insicura dei dati e le configurazioni insicure.

Grazie

Presentatore: Stylianos Karagiannis (PDMFC, Portogallo)

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