infonet solutions

Security Room
infonet solutions

AI Cyber Defence Service
di Infonet Solutions

L'applicazione dell'Intelligenza Artificiale ai servizi SIEM

L'applicazione dell'Intelligenza Artificiale ai servizi SIEM

La tecnologia dei sistemi SIEM (Security Information and Event Management) ha come **obiettivo la raccolta centralizzata in tempo reale degli eventi e dei LOG di sicurezza**, generati da strumenti di sicurezza (es. sistemi di antivirus, antimalware, Intrusion Detection Systems, Web filters, etc.), dispositivi di rete (es. routers, switch, etc.), apparati (es. mobile device, ...) e applicazioni.

Uno strumento di SIEM consente agli analisti di sicurezza di **risalire all'origine degli allarmi**, utile per la risoluzione delle criticità.

Come è avvenuto in molti settori, l'**Intelligenza Artificiale** rappresenta un'arma fondamentale anche per la **Cyber Security**, dove gli scenari di applicazione sono di natura molto differente: vanno dai flussi di rete, ai LOG dei server, fino alle informazioni più destrutturate, come quelle relative ai comportamenti delle persone.

Le reti neurali profonde riescono a unire insieme queste informazioni di natura ben diversa, dandone una rappresentazione omogenea e mantenendo gli elementi essenziali **per rilevare vulnerabilità o comportamenti anomali**.

SIEM: AI Cyber Defence Service di Infonet Solutions

"La potenza è nulla senza controllo"

"*Power is nothing without control*": così recitava lo slogan di un noto spot pubblicitario di un importante brand di pneumatici, per evidenziare quanto fosse essenziale associare alla potenza tecnologica un adeguato controllo.

Allo stesso modo Infonet Solutions approccia alla soluzione tecnologica utilizzata per erogare i propri servizi di Security Information and Event Management: un prodotto di **Cyber Defence, applicato all'Intelligenza artificiale**, molto funzionale e potente, specialmente per la gestione e la correlazione di grandi volumi di dati.

Perché lo strumento sia utilizzato correttamente e perché tutte le sue potenzialità vengano sfruttate, è essenziale però **affiancare alla soluzione un team di Security** dedicato alla sua corretta configurazione e gestione.

In questo, i servizi della **Security Room di Infonet Solutions** garantiscono di poter usufruire, in completa sicurezza, dei vantaggi della tecnologia e delle sue funzionalità.

Nello specifico, le attività previste dal servizio di Security Information and Event Management, erogato dalla Security Room di Infonet Solutions sono le seguenti:

- **Configurare** correttamente la soluzione.
- **Definizione e revisione periodica delle regole di correlazione.**
- Fornire il **monitoraggio** sullo stato di salute della sicurezza.
- **Identificare e notificare al cliente gli incidenti** o i potenziali incidenti di sicurezza.
- Dare **priorità** agli incidenti ritenuti più pericolosi e d'impatto sul business del cliente.
- **Tracciare** gli incidenti fintanto non siano stati presi in carico e chiusi dalla Security Room.
- Analisi e definizione delle **Remediation**.
- **Mantenimento del sistema aggiornato** in base alle nuove feature di analisi dello strumento.
- Prevedere eventuali **Service Review**.

Perché adottare una soluzione di SIEM?

- **Aumentare visibilità, flessibilità e velocità** necessarie per gestire le minacce avanzate.
- **Visione consolidata di tutti gli eventi di sicurezza** che accadono nella propria rete.
- **Integrazione** con gli strumenti di help desk aziendali per velocizzare le richieste IT e la risoluzione degli incidenti.

La Security Room
di Infonet Solution

La **Security Room** di Infonet Solutions ha come focus quello di aiutare le aziende a gestire con efficacia la propria sicurezza informatica con l'obiettivo di:

- Garantire l'integrità, la disponibilità e la fruibilità dei sistemi IT.
- Proteggere il business aziendale.
- Adeguarsi a standard e regolamenti.

I servizi di cybersecurity erogati dalla Security Room di Infonet Solutions:

- Servizio di gestione degli **Incident di Sicurezza**.
- Attività periodica di **Vulnerability Assessment & Penetration Test.**
- Remediation Planning & **IT Security Review**.
- **Firewall Management**.
- **Security Information and Event Management.**
- **Active Directory Audit** & FileServer.
- Gestione accessi privilegiati e **Multi-Factor Authentication**.
- **Patch Management**.
- **IT Audit e Risk Assessment**.

infonet solutions

Sede Legale
Via Einaudi 23
ZI Pieve di Curtarolo (PD)
info@infonetsolutions.it

Headquarters
Via Garibaldi 3
35010 Curtarolo, Padova
tel +39 049 9620572

Cybersecurity is never a destination.
It's a **journey** we're on together!