

Splunk è una potente piattaforma di analisi dati che ingloba, indicizza e correla enormi volumi di dati provenienti da diverse fonti all'interno di un'organizzazione. Pensala come un potente motore di ricerca per i tuoi dati, ma con la capacità di visualizzare, analizzare e correlare informazioni in modi che ti permettono di comprendere meglio ciò che sta accadendo nella tua infrastruttura IT.

Perché è importante nella Cyber Security? Nel panorama sempre più complesso delle minacce informatiche, la visibilità è fondamentale. Splunk offre questa visibilità, consentendo alle organizzazioni di:

- **Rilevare minacce in tempo reale:** Analizzando i log di sistema, di rete e di applicazioni, Splunk può identificare anomalie e attività sospette che potrebbero indicare un attacco in corso.
- **Investigare gli incidenti:** Quando si verifica un incidente di sicurezza, Splunk aiuta gli analisti a ricostruire la sequenza degli eventi, a identificare la causa principale e a valutare l'impatto.
- **Automatizzare le risposte:** Splunk può essere integrato con altri strumenti di sicurezza per automatizzare le risposte agli incidenti, come l'isolamento di sistemi compromessi o la generazione di ticket.
- **Conformità normativa:** Aiuta le organizzazioni a dimostrare la conformità ai requisiti normativi come GDPR e PCI DSS, fornendo un registro dettagliato delle attività di sistema.

Come funziona Splunk nella Cyber Security?

1. **Raccolta dati:** Splunk ingloba dati da una vasta gamma di fonti, tra cui firewall, sistemi operativi, applicazioni, dispositivi IoT e molto altro.
2. **Indicizzazione:** I dati vengono indicizzati per consentire ricerche rapide ed efficienti.
3. **Analisi:** Splunk offre un linguaggio di ricerca potente (SPL) che consente di eseguire query complesse e correlare dati da diverse fonti.
4. **Visualizzazione:** I risultati delle analisi possono essere visualizzati in dashboard personalizzati, grafici e tabelle per una facile comprensione.
5. **Alert:** Splunk può inviare avvisi quando vengono rilevate anomalie o violazioni delle politiche di sicurezza.

In sintesi Splunk è uno strumento indispensabile per qualsiasi organizzazione che prenda sul serio la sicurezza informatica. Fornisce una visione completa dell'infrastruttura IT, consentendo di rilevare e rispondere rapidamente alle minacce. La sua flessibilità e scalabilità lo rendono adatto a organizzazioni di qualsiasi dimensione.

Vantaggi chiave di Splunk nella Cyber Security:

- **Visibilità:** Fornisce una visione completa dell'infrastruttura IT.
- **Velocità:** Consente di analizzare grandi volumi di dati in tempo reale.
- **Flessibilità:** Può essere adattato a qualsiasi esigenza di sicurezza.
- **Scalabilità:** Può gestire ambienti di qualsiasi dimensione.
- **Community:** Una vasta community di utenti e sviluppatori offre supporto e risorse.

Conclusione Splunk è molto più di un semplice strumento di analisi dei log. È una piattaforma completa per la sicurezza informatica che può aiutare le organizzazioni a proteggere i loro asset più preziosi.

Di seguito gli screenshot dove vediamo che abbiamo monitorato la nostra Win10Pro con Splunk su WindowsServer2022

PostgreSQL Server	0%	1,0 MB	0 MB/s	0 Mbps
Processo host per attività di Win...	0%	1,6 MB	0,1 MB/s	0 Mbps
Runtime Broker	0%	6,0 MB	0 MB/s	0 Mbps
> Servizio SNMP	0%	0,6 MB	0 MB/s	0 Mbps
Sink to receive asynchronous ca...	0%	0,4 MB	0 MB/s	0 Mbps
> splunkd service	0%	65,1 MB	0,1 MB/s	0,5 Mbps
> TCP/IP Services Application	0%	0,2 MB	0 MB/s	0 Mbps
> VirtualBox Guest Additions Servi...	0%	0.7 MB	0 MB/s	0 Mbps

Elenco		Formato		20 per pagina		< Prec		1		2		3		4	
Tutti i campi		i		Ora		Evento									
		v		02/12/24 14:46:06,000		12/02/2024 02:46:06 PM ... 2 lines omitted ... EventType=0 ComputerName=DESKTOP-9K104BT SourceName=Microsoft-Windows-Security-SPP Type=Informazioni Mostra tutte le 12 righe									
						Azioni evento									
						Tipo		Campo		Valore					

System Information					
File Modifica Visualizza ?					
Risorse di sistema		Elemento		Valore	
Risorse hardware		Nome SO		Microsoft Windows 10 Pro	
Componenti		Versione		10.0.10240 build 10240	
Ambiente software		Descrizione altro SO		Non disponibile	
		Produttore SO		Microsoft Corporation	
		Nome sistema		DESKTOP-9K104BT	
		Produttore sistema		innotek GmbH	
		Modello sistema		VirtualBox	
		Tipo sistema		PC basato su x64	
		SKU sistema		Non supportato	
		Processore		11th Gen Intel(R) Core(TM) i7-11700F @ 2.50GHz,	
		Versione/data BIOS		innotek GmbH VirtualBox, 01/12/2006	
		Versione SMBIOS		2.5	
		Modalità BIOS		Legacy	
		Produttore scheda di base		Oracle Corporation	
		Modello scheda di base		Non disponibile	