

# PROGETTO

**Installazione di Splunk  
M6W24-D1**

**25 / 02 / 2025**

**Cybersecurity Analyst**

Installazione di Splunk e Splunk Universal  
Forwarder

**Matteo Madonia**

## 1. Traccia progetto

### Traccia:

- Installazione di Splunk;
- Analisi dei log;
- Query, Query con AI
- Splunk Universal Forwarder (Facoltativo)

## 2. Svolgimento del progetto

### DEFINIZIONE: cos'è Splunk?

Splunk è una piattaforma di analisi dei dati che consente di raccogliere, indicizzare, monitorare e visualizzare dati provenienti da diverse fonti, come log di sistema, eventi di rete, metriche di sicurezza e dati machine-generated. È molto utilizzato in ambito **cybersecurity**, **IT operations** e **business analytics** per analizzare grandi volumi di dati in tempo reale.

### Funzionalità principali di Splunk:

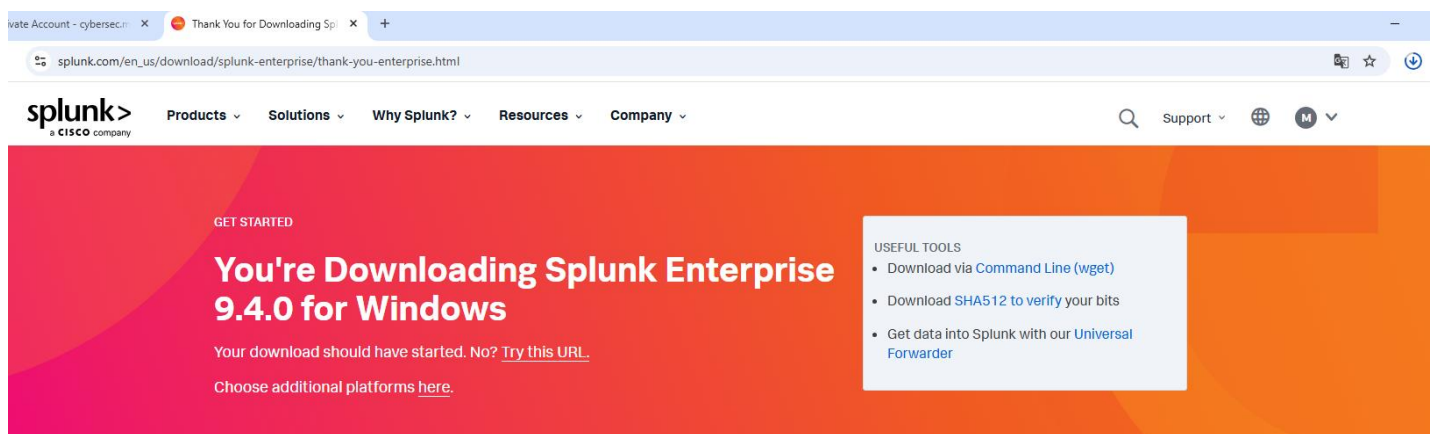
- **Raccolta e indicizzazione:** acquisisce dati da file di log, dispositivi di rete, sensori IoT, database e altre fonti.
- **Ricerca e analisi:** utilizza il **Splunk Search Processing Language (SPL)** per eseguire query avanzate sui dati raccolti.
- **Dashboard e report:** permette di creare visualizzazioni interattive, grafici e alert automatici.
- **Monitoraggio in tempo reale:** utile per rilevare anomalie, minacce informatiche e problemi operativi.
- **Automazione e risposta:** in combinazione con **Splunk SOAR**, può automatizzare azioni di risposta a eventi di sicurezza.

### Splunk e la Cybersecurity

Splunk è molto usato in ambito SOC (Security Operations Center) per il **monitoraggio delle minacce**, la **rilevazione di attacchi** e la **risposta agli incidenti**. Grazie a **Splunk Enterprise Security**, può analizzare eventi di sicurezza in tempo reale e migliorare la difesa contro malware, intrusioni e attività sospette.

### INSTALLAZIONE DI SPLUNK

Seguire attentamente in passaggi: registrarsi su splunk, selezionare prodotto splunk enterprise, versione trial, scegliere la versione per il sistema operativo sul quale verrà installato, download;



127.0.0.1:8000/it-IT/account/login?return\_to=%2Fit-IT%2F



←

→

↺

🔍 127.0.0.1:8000/it-IT/app/launcher/home

splunk>enterprise

App ▾

🟢

Administrator ▾

1 Messaggi ▾

Impostazioni ▾

Attività ▾

App

←

Cerca altre app 🔗

Gestisci ⚙️

Cerca app per nome...

🔍

➡️ Search & Reporting

🔍 AT Audit Trail

🔒 Splunk Secure Gateway

🔍 Upgrade Readiness App

Salve, Administrator

📖 Segnalibri

📊 Dashboard

📅 Cronologia delle ricerche

🕒 Visualizzati di recente

👤 Creato da te

👥 Condiviso con te

▼ I miei segnalibri (0)

Aggiungi segnalibro

▼ Condiviso con la mia organizzazione (0)

Aggiungi segnalibro

Condiviso da me

Condiviso dagli altri amministratori

▼ Consigliato da Splunk (13)

Attività comuni

Nascondi agli utenti

📄 Aggiungi dati

🔍 Cerca i tuoi dati

📊 Visualizza i tuoi dati

## ANALISI DEI LOG

Finalmente, dopo aver completato l'intera fase di installazione, possiamo esaminare in pratica come analizzare un file di log. Utilizzeremo un file di log fornito da Splunk come esercizio, chiamato "tutorialdata".

Questo file di log contiene dati dettagliati sulle richieste HTTP effettuate al server web, come richieste GET e POST, codici di stato HTTP, dimensioni delle risposte, e altri dettagli pertinenti per l'analisi del traffico web e del comportamento degli utenti sul sito del negozio online fittizio "Buttercup Games".

Riassunto dei Contenuti del Tutorial Data

- **access.log:** Contiene dati di accesso al server web Apache, utili per analizzare il traffico e le interazioni degli utenti con il sito.
- **secure.log:** Contiene eventi di sicurezza, come tentativi di accesso e altre attività rilevanti per la sicurezza del sistema.
- **vendor\_sales.log:** Contiene informazioni sulle vendite dei prodotti, utilizzato per analisi commerciali e di transazioni.

1. **File di Log:** ○ **access.log:** Contiene dati di accesso ai server web, utili per analizzare il traffico web e le richieste fatte ai server. ○ **secure.log:** Contiene dati relativi alla sicurezza, come i tentativi di accesso e altri eventi di sicurezza. ○ **vendor\_sales.log:** Contiene dati sulle vendite, utile per analisi di vendite e transazioni.

2. **Formato dei Dati:** ○ I log vengono generati quotidianamente e contengono eventi con timestamp degli ultimi sette giorni, rendendo i dati freschi e rilevanti per l'analisi. ○ I file di log sono in formati standard che Splunk può facilmente indicizzare e analizzare utilizzando i sourcetype appropriati.

Il tutorial di Splunk guida gli utenti attraverso una serie di passaggi per imparare a:

- **Caricare i dati:** Utilizzare l'assistente di caricamento dati per aggiungere il file tutorialdata.zip alla propria istanza di Splunk.
- **Ricerca dei Dati:** Eseguire ricerche di base e avanzate sui dati caricati, imparando a utilizzare il linguaggio di ricerca di Splunk (SPL).
- **Creazione di Report e Dashboard:** Salvare ricerche come report e creare dashboard per visualizzare i dati in modo interattivo e informativo.
- **Enrichment dei Dati:** Arricchire gli eventi con lookups per aggiungere ulteriori informazioni e migliorare le analisi.

## Esempio di Parsing

Quando carichi un file di log, Splunk applica il parsing per estrarre campi chiave dai dati grezzi.

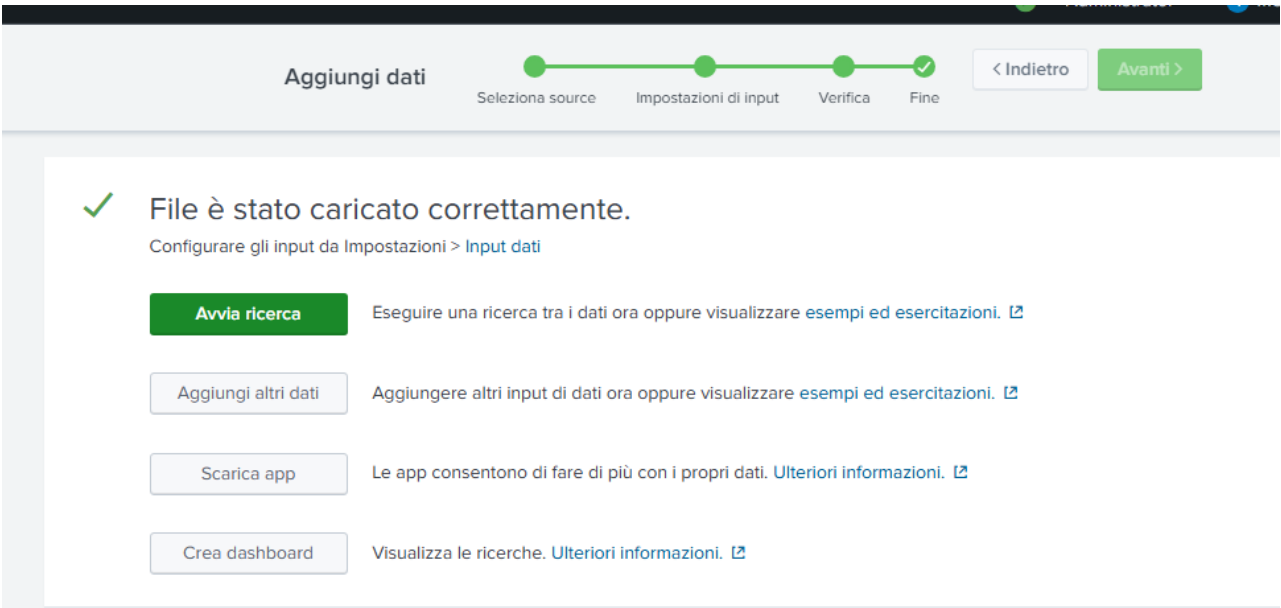
Ad esempio, un record nel access.log potrebbe essere: 175.44.24.82 - - 22/Feb/2021:18:44:40 +0000 "POST /product.screen?productId=WCCZSHZ1A01&JSESSIONID=SD7SL9FF5ADFF5066 HTTP/1.1" 200 3067 "http://www.buttercupgames.com/product.screen?productId=WCCZSHZ1A01" "Mozilla/5.0" Splunk scomporrà questo record per estrarre campi come indirizzo IP, timestamp, metodo HTTP, risorsa richiesta, codice di stato, e user agent.

Dove prendiamo il file di esempio: tutorialdata.zip

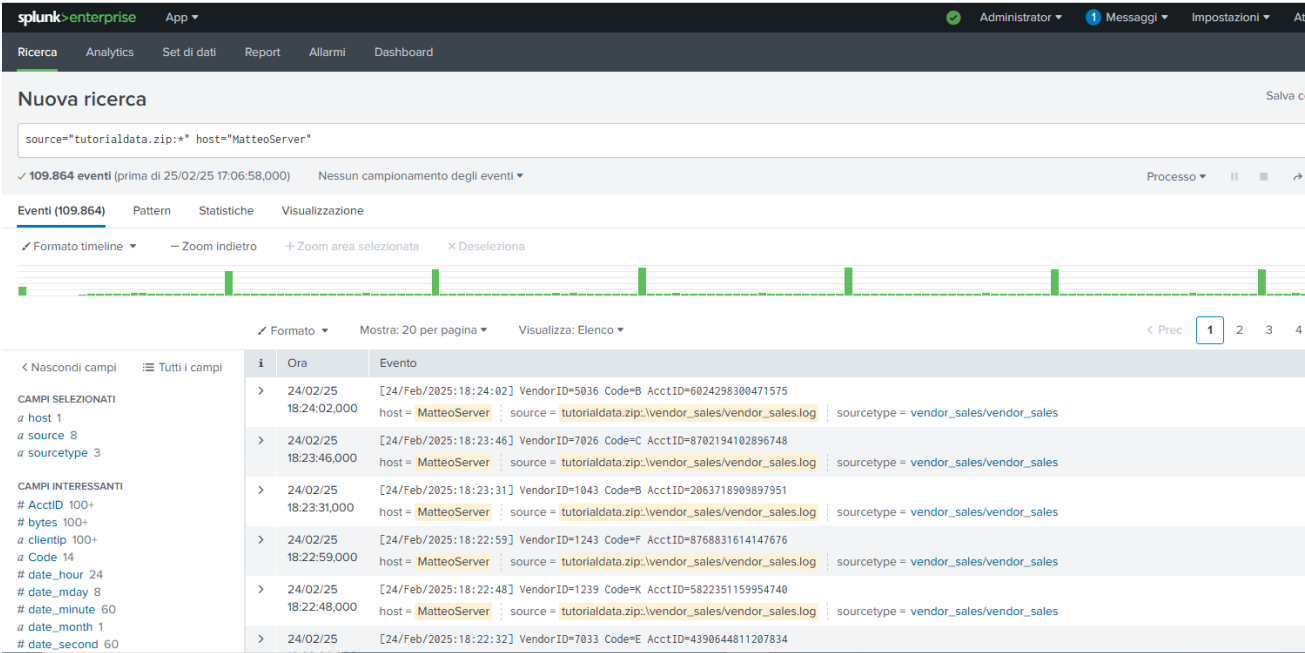
[https://docs.splunk.com/Documentation/Splunk/9.2.1/SearchTutorial/Systemrequirements#Download\\_the\\_tutorial\\_data\\_files](https://docs.splunk.com/Documentation/Splunk/9.2.1/SearchTutorial/Systemrequirements#Download_the_tutorial_data_files)

PROCEDURA

- Download del file tutorialdat.zip dal sito di Splunk (fornito dallo stesso per l’esercitazione)
- Importare il file zippato all’interno della piattaforma: aggiungi dati, carica, di nuovo carica, seleziona file, selezionare e caricare il file salvato in precedenza (ancora in formato .zip)
- Si avvia un menù di configurazione intuitivo dove daremo le impostazioni per la determinazione del sourcetype, host e indice (index)
- Procedere sempre cliccando con il tasto avanti e confermare il caricamento dei dati fino ad arrivare a questa schermata



- Cliccare su avvia ricerca: di seguito comparirà questa schermata



QUERY

Seguire attentamente le slide del corso e procedere con l’esercitazione. Si inizia dalla query base sotto riportata, per procedere alla richiesta di dati più precisi

**PRIMA QUERY:** source="tutorialdata.zip:\*" host="MatteoServer"

Questa query cerca tutti gli eventi nel file tutorialdata.zip provenienti dall'host MatteoServer.

Nuova ricerca

source="tutorialdata.zip:\*" host="MatteoServer"

✓ 109.864 eventi (prima di 25/02/25 17:13:06,000) Nessun campionamento degli eventi ▼

Eventi (109.864)

Pattern

Statistiche

Visualizzazione

✓ Formato timeline ▼

— Zoom indietro

+ Zoom area selezionata

× Deseleziona

✓ Formato ▼

Mostra: 20 per pagina ▼

Visualizza: Elenco ▼

< Nascondi campi

≡ Tutti i campi

CAMPI SELEZIONATI

a host 1

a source 8

a sourcetype 3

CAMPI INTERESSANTI

# AcctID 100+

# bytes 100+

a clientip 100+

a Code 14

# date\_hour 24

# date\_mday 8

# date\_minute 60

a date\_month 1

127.0.0.1:8000/it-IT/app/search/dashboa

i	Ora	Evento
>	24/02/25 18:24:02,000	[24/Feb/2025:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575 host = MatteoServer source = tutorialdata.zip:\vendor_sales\vendor_sales.log sourcetype = vendor_sales/vendor_sales
>	24/02/25 18:23:46,000	[24/Feb/2025:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748 host = MatteoServer source = tutorialdata.zip:\vendor_sales\vendor_sales.log sourcetype = vendor_sales/vendor_sales
>	24/02/25 18:23:31,000	[24/Feb/2025:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951 host = MatteoServer source = tutorialdata.zip:\vendor_sales\vendor_sales.log sourcetype = vendor_sales/vendor_sales
>	24/02/25 18:22:59,000	[24/Feb/2025:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676 host = MatteoServer source = tutorialdata.zip:\vendor_sales\vendor_sales.log sourcetype = vendor_sales/vendor_sales
>	24/02/25 18:22:48,000	[24/Feb/2025:18:22:48] VendorID=1239 Code=K AcctID=5822351159954740 host = MatteoServer source = tutorialdata.zip:\vendor_sales\vendor_sales.log sourcetype = vendor_sales/vendor_sales
>	24/02/25 18:22:32,000	[24/Feb/2025:18:22:32] VendorID=7033 Code=E AcctID=4390644811207834

**SECONDA QUERY:** source="tutorialdata.zip:\*" host="MatteoServer" | stats count as TotalEvents

Vogliamo sapere quanti eventi sono presenti nel file tutorialdata.zip per l'host MatteoServer.

splunk>enterprise

App ▼

Ricerca

Analytics

Set di dati

Report

Allarmi

Dashboard

Nuova ricerca

source="tutorialdata.zip:\*" host="MatteoServer" | stats count as TotalEvents

✓ 109.864 eventi (prima di 25/02/25 17:20:18,000) Nessun campionamento degli eventi ▼

Eventi

Pattern

Statistiche (1)

Visualizzazione

Mostra: 20 per pagina ▼

✓ Formato ▼

Anteprima: on

TotalEvents ↕

109864

**TERZA QUERY:** source="tutorialdata.zip:\*" host="MatteoServer" | stats count by source

Vogliamo vedere quanti eventi ci sono per ogni file specifico all'interno di tutorialdata.zip

Spiegazione

- source="tutorialdata.zip:\*": Cerca in tutti i file all'interno di tutorialdata.zip.
- host="MatteoServer": Filtra i risultati per l'host AX16Pro.
- stats count by source: Utilizza il comando stats per contare il numero di eventi, raggruppando per source

source="tutorialdata.zip:\*" host="MatteoServer" | stats count by source

219.728 eventi (prima di 25/02/25 20:36:33,000)

Nessun campionamento degli eventi

Processo

Modaltà intelligente

EventiPatternStatistiche (8)Visualizzazione

Mostra: 20 per paginaFormatoAnteprima: on

source	count
tutorialdata.zip:\mailsv\secure.log	19658
tutorialdata.zip:\vendor_sales\vendor_sales.log	60488
tutorialdata.zip:\www1\access.log	27256
tutorialdata.zip:\www1\secure.log	21186
tutorialdata.zip:\www2\access.log	25824
tutorialdata.zip:\www2\secure.log	19366
tutorialdata.zip:\www3\access.log	25984
tutorialdata.zip:\www3\secure.log	19966

**QUARTA QUERY:** source="tutorialdata.zip:\*" host="MatteoServer" | stats count by sourcetype

Eventi Raggruppati per Sourcetype

Vogliamo analizzare la distribuzione degli eventi per ciascun sourcetype.

splunk>enterprise

AdministratorMessaggiImpostazioniAttivitàGuidaTrova

RicercaAnalyticsSet di datiReportAllarmiDashboard

Search & Reporting

Nuova ricerca

Salva comeCrea vista tabellaChiudi

source="tutorialdata.zip:\*" host="MatteoServer" | stats count by sourcetype

219.728 eventi (prima di 25/02/25 20:48:28,000)

Nessun campionamento degli eventi

Processo

Modaltà intelligente

EventiPatternStatistiche (3)Visualizzazione

Mostra: 20 per paginaFormatoAnteprima: on

sourcetype	count
access_combined_wcookie	79064
vendor_sales/vendor_sales	60488
www1/secure	80176

**QUINTA QUERY:** sourcetype="vendor\_sales/vendor\_sales"  
ricerca dati e informazioni dei vendor\_sales tramite i sourcetype

**splink>enterprise**    App    ✔ Administrator ▼

---

Ricerca   Analytics   Set di dati   Report   Allarmi   Dashboard

---


## Nuova ricerca

sourceType="vendor\_sales/vendor\_sales"

✔ 60.488 eventi (prima di 25/02/25 20:53:12.000)
Nessun campionamento degli eventi ▼

**Eventi (60.488)**   Pattern   Statistiche   Visualizzazione

✔ Formato timeline ▼   
 — Zoom indietro   
 + Zoom area selezionata   
 × Deselezione



✔ Formato ▼   
 Mostra: 20 per pagina ▼   
 Visualizza: Elenco ▼

< Nascondi campi	☰ Tutti i campi	i	Ora	Evento
<b>CAMPI SELEZIONATI</b>				
a host 1		>	24/02/25 18:24:02.000	[24/Feb/2025:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575 host = MatteoServer   source = tutorialdata.zip:\vendor_sales\vendor_sales.log   sourceType = vendor_sales/vendor_sales
a source 1		>	24/02/25 18:24:02.000	[24/Feb/2025:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575 host = MatteoServer   source = tutorialdata.zip:\vendor_sales\vendor_sales.log   sourceType = vendor_sales/vendor_sales
a sourceType 1		>	24/02/25 18:24:02.000	[24/Feb/2025:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575 host = MatteoServer   source = tutorialdata.zip:\vendor_sales\vendor_sales.log   sourceType = vendor_sales/vendor_sales
<b>CAMPI INTERESSANTI</b>				
# AcctID 100+		>	24/02/25 18:23:46.000	[24/Feb/2025:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748 host = MatteoServer   source = tutorialdata.zip:\vendor_sales\vendor_sales.log   sourceType = vendor_sales/vendor_sales
# Code 14		>	24/02/25 18:23:46.000	[24/Feb/2025:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748 host = MatteoServer   source = tutorialdata.zip:\vendor_sales\vendor_sales.log   sourceType = vendor_sales/vendor_sales
# date_hour 24		>	24/02/25 18:23:46.000	[24/Feb/2025:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748 host = MatteoServer   source = tutorialdata.zip:\vendor_sales\vendor_sales.log   sourceType = vendor_sales/vendor_sales
# date_minute 60		>	24/02/25 18:23:46.000	[24/Feb/2025:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748 host = MatteoServer   source = tutorialdata.zip:\vendor_sales\vendor_sales.log   sourceType = vendor_sales/vendor_sales
# date_month 1		>	24/02/25 18:23:31.000	[24/Feb/2025:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951 host = MatteoServer   source = tutorialdata.zip:\vendor_sales\vendor_sales.log   sourceType = vendor_sales/vendor_sales
# date_second 60		>	24/02/25 18:23:31.000	[24/Feb/2025:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951 host = MatteoServer   source = tutorialdata.zip:\vendor_sales\vendor_sales.log   sourceType = vendor_sales/vendor_sales
# date_wday 7		>	24/02/25 18:23:31.000	[24/Feb/2025:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951 host = MatteoServer   source = tutorialdata.zip:\vendor_sales\vendor_sales.log   sourceType = vendor_sales/vendor_sales
# date_year 1		>	24/02/25 18:23:31.000	[24/Feb/2025:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951 host = MatteoServer   source = tutorialdata.zip:\vendor_sales\vendor_sales.log   sourceType = vendor_sales/vendor_sales



SPLUNK UNIVERSAL FORWARDER

Procedere all’installazione della sentinella/sonda Splunk Universal Forwarder, seguendo tutti i passaggi indicati nella slide; il download del tool è possibile dal sito ufficiale di Splunk.

Nell’immagini seguenti la prova dell’avvenuta installazione

Splunk Universal Forwarder è attivo come processo in background sul dispositivo Windows 10 Pro

> Servizio piattaforma protezione ...	1,6%	3,5 MB	0 MB/s	0 Mbps	Molto basso	Molto bass
▼ splunkd service	0%	61,2 MB	0,1 MB/s	0 Mbps	Molto basso	Molto bass
SplunkForwarder						
> Start	0,3%	16,9 MB	0 MB/s	0 Mbps	Molto basso	Molto bass

Lato server, osserviamo ora i dati sulla piattaforma web Splunk, ci aspettiamo che la nostra sentinella Splunk Forwarder, installata su windows 10, ci invii dati: ecco qui le prime informazioni che la nostra “sonda” ci invio dal dispositivo SuperHacker Windows 10 pro, sotto il dominio Matteo.local del server.

windows

✓ 413 eventi (27/02/25 11:00:00,000 - 28/02/25 11:35:04,000) Nessun campionamento degli eventi ▼

Processo ▼ ||

Eventi (413) Pattern Statistiche Visualizzazione

Formato timeline ▼ Zoom indietro Zoom area selezionata Deselezione

Formato ▼ Mostra: 20 per pagina Visualizza: Elenco ▼

< Nascondi campi Tutti i campi

CAMPI SELEZIONATI

a host 1

a source 3

a sourcetype 3

CAMPI INTERESSANTI

a ComputerName 1

a Dominio\_account 7

# EventCode 77

# EventType 4

a ID\_accesso 12

a ID\_processo 14

a ID\_sicurezza 10

a Index 1

a Keywords 7

# linecount 21

a LogName 3

a Message 100+

a Nome\_account 9

> 28/02/25 11:34:39,000

... 7 lines omitted ...

SidType=0

SourceName=Microsoft-Windows-Service Control Manager

Type=Informazioni

... 3 lines omitted ...

OpCode=Operazione completata.

Message=È stato modificato il tipo di avvio del servizio Programma di installazione dei moduli di Windows da Avvio su richiesta a Avvio automatico.

Mostra tutte le 15 righe

host = SUPERHACKER source = WinEventLog:System sourcetype = WinEventLog:System

> 28/02/25 11:34:30,000

... 2 lines omitted ...

EventType=0

ComputerName=SuperHacker.Matteo.local

SourceName=Microsoft-Windows-Security-SPP

Type=Informazioni

Mostra tutte le 12 righe

host = SUPERHACKER source = WinEventLog:Application sourcetype = WinEventLog:Application

> 28/02/25 02/28/2025 11:34:30 AM

▼ 28/02/25 11:34:30,000

... 2 lines omitted ...

EventType=0

ComputerName=SuperHacker.Matteo.local

SourceName=Microsoft-Windows-Security-SPP

Type=Informazioni

Mostra tutte le 12 righe

Azioni evento ▼

Tipo	Campo	Valore	Azioni
Selezionato	host ▼	SUPERHACKER	▼
	source ▼	WinEventLog:Application	▼
	sourcetype ▼	WinEventLog:Application	▼
Evento	ComputerName ▼	SuperHacker.Matteo.local	▼
	EventCode ▼	903	▼