

Day 9 – Sysmon Setup

Obiettivi

- **Installare Sysmon su Windows Server**
- **Confermare della raccolta dei dati**

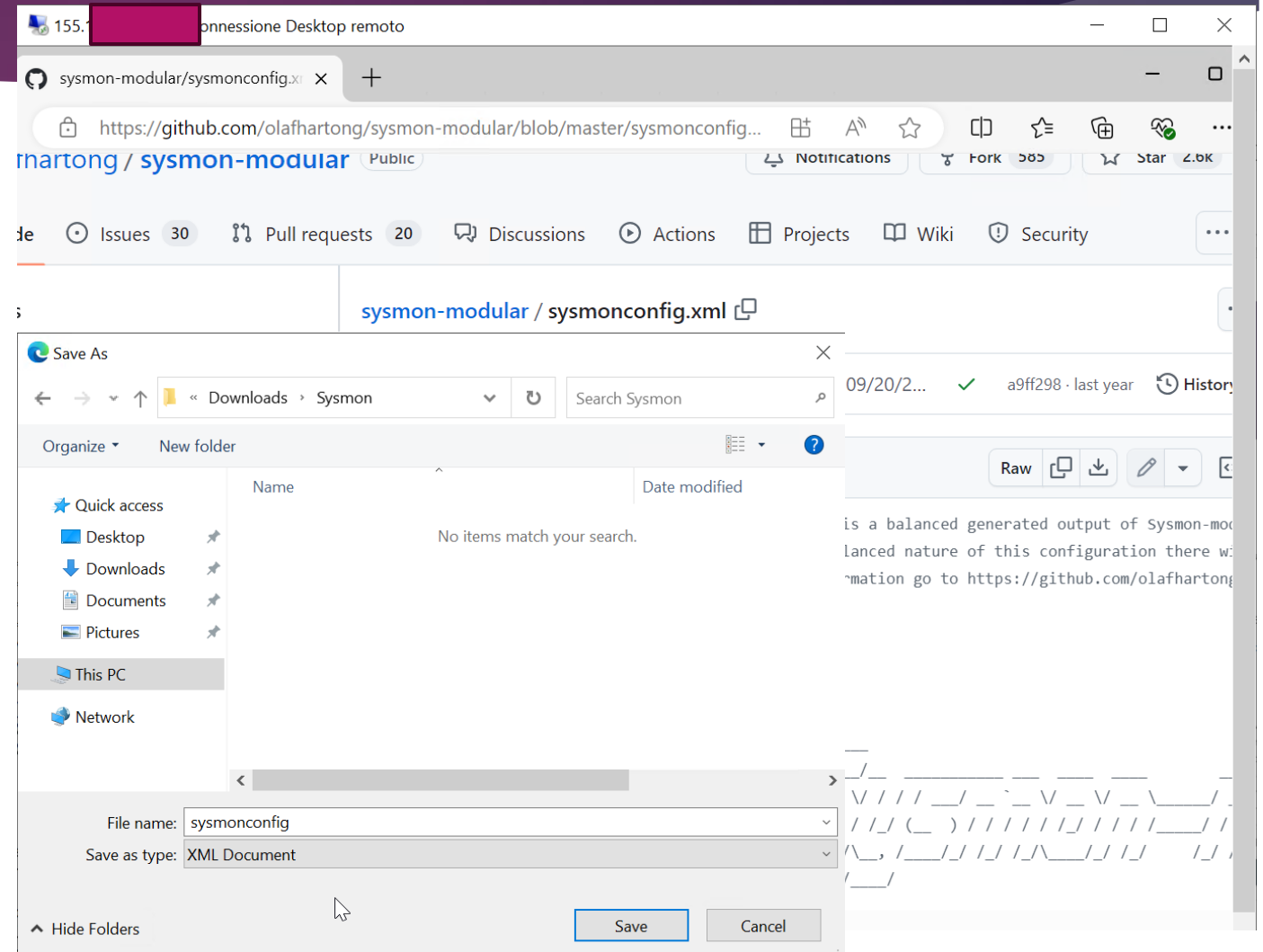
Sysmon Setup

Ci connettiamo da remoto al **Windows Server**, scarichiamo l'ultima versione di **Sysmon** ed estraiamo il contenuto del file scaricato.

The screenshot shows a remote desktop connection window titled "155. [redacted] Connessione Desktop remoto". The main content area displays the Sysmon website. On the left is a navigation menu with a search bar "Filter by title" and a list of items: Security Utilities, Autologon, LogonSessions, NewSID, PsLoggedOn, PsLogList, RootkitRevealer, Sysmon (highlighted), System Information, Miscellaneous, Sysinternals Suite, Microsoft Store, Community, Resources, Software License Terms, Licensing FAQ, and a "Download PDF" link at the bottom. The main content area on the right includes links for "Overview of Sysmon Capabilities", "Screenshots", "Usage", and "Show 5 more". Below these, it lists the authors "By Mark Russinovich and Thomas Garnier" and the publication date "Published: July 23, 2024". There are two download links: "Download Sysmon (4.6 MB)" with a download icon, and "Download Sysmon for Linux (GitHub)". The "Introduction" section begins with the text: "System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network. The service runs as a protected process, thus disallowing a wide range of user mode". In the top right corner, a "Downloads" window shows the file "Sysmon.zip" being downloaded at 0 B/s, with a progress bar indicating 4.6 MB of 4.6 MB. The Windows taskbar at the bottom shows the Start button, a search bar with the text "Type here to search", and several application icons including Edge, File Explorer, and a terminal.

Sysmon Setup

Ora scarichiamo il file di configurazione 'sysmon configuration olaf', uno dei più utilizzati. Clicchiamo su 'Raw' e lo salviamo nella cartella di **Sysmon**.



Sysmon Setup

Apriamo **Powershell** come Administrator, effettuiamo un 'cd' nel path della cartella **Sysmon**.

```
Administrator: Windows PowerShell
PS C:\Users\Administrator\elastic-agent-8.15.1-windows-x86_64> cd C:\Users\Administrator\Downloads\Sysmon
PS C:\Users\Administrator\Downloads\Sysmon> dir

Directory: C:\Users\Administrator\Downloads\Sysmon

Mode                LastWriteTime         Length Name
----                -
-a----          9/21/2024   3:19 PM             7490 Eula.txt
-a----          9/21/2024   3:19 PM        8480560 Sysmon.exe
-a----          9/21/2024   3:19 PM        4563248 Sysmon64.exe
-a----          9/21/2024   3:19 PM        4993440 Sysmon64a.exe
-a----          9/21/2024   3:25 PM        253169 sysmonconfig.xml

PS C:\Users\Administrator\Downloads\Sysmon> _
```

Sysmon Setup

Procediamo con
l'installazione di **Sysmon**
da **Powershell**.

```
Administrator: Windows PowerShell
PS C:\Users\Administrator\elastic-agent-8.15.1-windows-x86_64> cd C:\Users\Administrator\Downloads\Sysmon
PS C:\Users\Administrator\Downloads\Sysmon> dir

Directory: C:\Users\Administrator\Downloads\Sysmon
Mode                LastWriteTime         Length
----                -
-a----            9/21/2024 3:15:11 PM           1024
-a----            9/21/2024 3:15:11 PM           1024
-a----            9/21/2024 3:15:11 PM           1024
-a----            9/21/2024 3:15:11 PM           1024
-a----            9/21/2024 3:15:11 PM           1024

PS C:\Users\Administrator\Downloads\Sysmon> .\Sysmon.exe

System Monitor v15.15 - System Monitor
By Mark Russinovich and Thomas Esch
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2009 Thai Open Source Software Center
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.90
Configuration file validated.
```

System Monitor License Agreement

You can also use the /accepteula command-line switch to accept the EULA.

SYSINTERNALS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Sysinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

- updates,
- supplements,
- Internet-based services, and

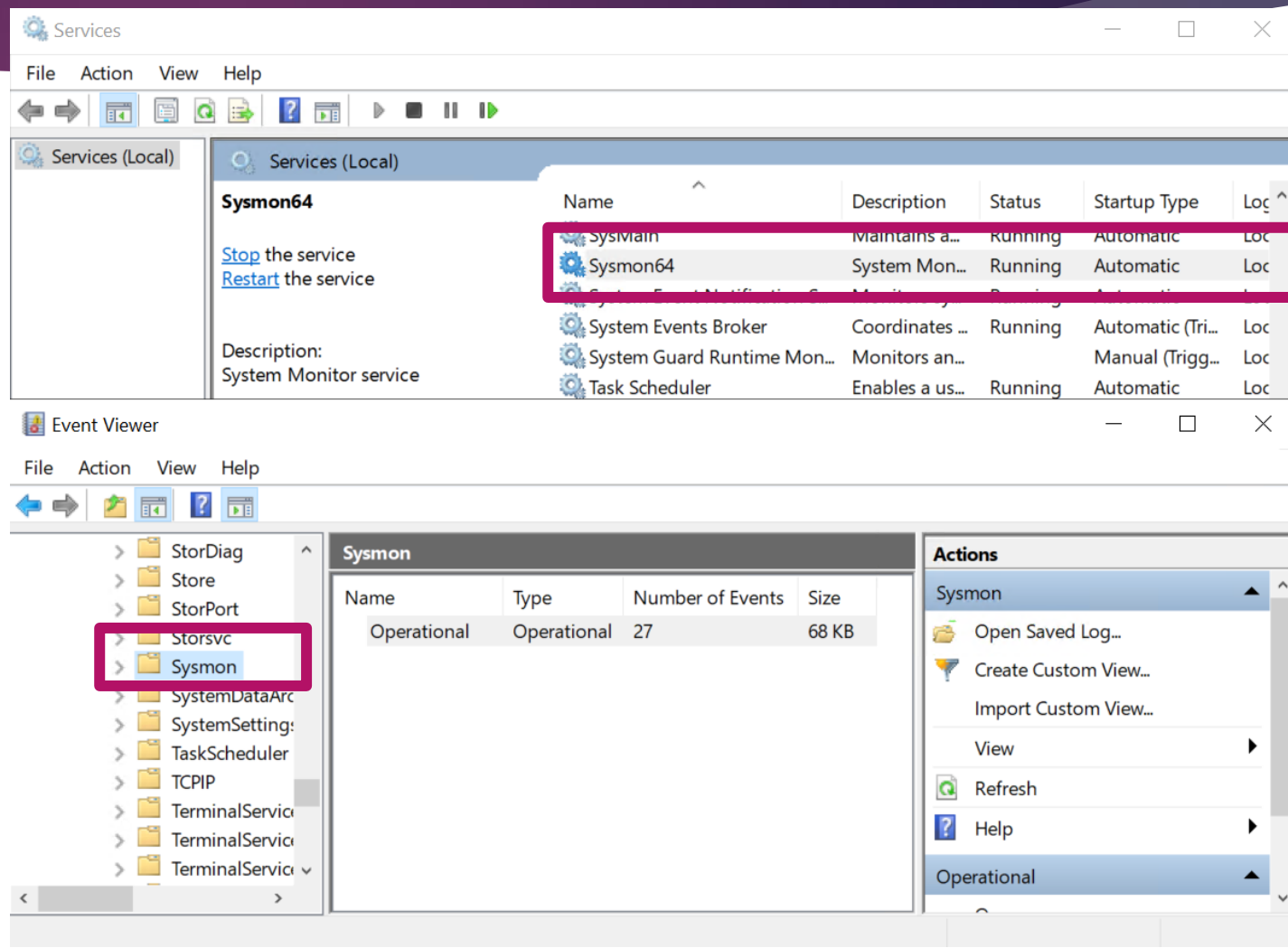
Print

Agree

Decline

Sysmon Setup

Una volta installato **Sysmon**, vedremo il servizio attivato tra quelli di Windows, e i log generati saranno visibili su 'Event Viewer' in Application and Services Logs/Microsoft/Windows.



Dal file Operational possiamo visualizzare i primi eventi e, consultando la documentazione di **Sysmon**, comprenderne il significato. Qui possiamo confermare che gli eventi vengono generati.

Event Viewer

File Action View Help

StorDiag

Store

StorPort

Storsvc

Sysmon

SystemDataArc

SystemSetting:

TaskScheduler

TCPIP

TerminalServic

TerminalServic

TerminalServic

TerminalServic

TerminalServic

TerminalServic

TerminalServic

Time-Service

Time-Service-F

TZSync

TZUtil

UAC

UAC-FileVirtua

UI-Search

UniversalTele

User Control P

User Device Re

User Profile Ser

User-Loader

UserPnp

Operational

Number of events: 37 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	9/21/2024 3:41:57 PM	Sysmon	13	Registry value set (rule...
Information	9/21/2024 3:41:08 PM	Sysmon	11	File created (rule: FileC...
Information	9/21/2024 3:40:08 PM	Sysmon	11	File created (rule: FileC...
Information	9/21/2024 3:39:48 PM	Sysmon	3	Network connection d...
Information	9/21/2024 3:39:08 PM	Sysmon	11	File created (rule: FileC...
Information	9/21/2024 3:38:46 PM	Sysmon	3	Network connection d...
Information	9/21/2024 3:38:44 PM	Sysmon	3	Network connection d...
Information	9/21/2024 3:38:42 PM	Sysmon	3	Network connection d...
Information	9/21/2024 3:38:41 PM	Sysmon	3	Network connection d...
Information	9/21/2024 3:38:08 PM	Sysmon	11	File created (rule: FileC...
Information	9/21/2024 3:37:22 PM	Sysmon	7	Image loaded (rule: Im...
Information	9/21/2024 3:37:19 PM	Sysmon	7	Image loaded (rule: Im...
Information	9/21/2024 3:37:19 PM	Sysmon	7	Image loaded (rule: Im...
Information	9/21/2024 3:37:19 PM	Sysmon	7	Image loaded (rule: Im...
Information	9/21/2024 3:37:19 PM	Sysmon	7	Image loaded (rule: Im...
Information	9/21/2024 3:37:19 PM	Sysmon	7	Image loaded (rule: Im...
Information	9/21/2024 3:37:16 PM	Sysmon	7	Image loaded (rule: Im...

Event 13, Sysmon

General

Details

Registry value set:
RuleName: -
EventTvpne: SetValue

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Event ID: 13
Level: Information

Logged: 9/21/2024 3:41:57 PM
Task Category: Registry value set (rule: RegistryEvent)
Keywords:

Actions

Operational

Open Saved Log...

Create Custom View...

Import Custom View...

Clear Log...

Filter Current Log...

Properties

Disable Log

Find...

Save All Events As...

Attach a Task To this Log...

View

Refresh

Help

Event 13, Sysmon

Event Properties

Attach Task To This Event...

Copy

Save Selected Events...

Refresh

Help