Day 8 – Sysmon

MONITORAGGIO DEGLI EVENTI DI WINDOWS

Cos'è Sysmon?

Sysmon (System Monitor) è uno strumento di monitoraggio di Microsoft che fa parte della suite Sysinternals. Viene eseguito come servizio di sistema su Windows e consente di raccogliere dettagliati log di sistema su eventi come creazione di processi, connessioni di rete, ecc.

Inoltre:
- E' personalizzabile
- Offre visibilità dettagliata sulle attività del sistema operativo

Capacità di Logging di Sysmon

1. Registra la creazione di processi e altri eventi di sistema

•Sysmon monitora la creazione di processi e altri eventi critici (modifiche a file, servizi, registro), fornendo dettagli come nome del processo e timestamp. Utile per rilevare attività sospette o malevole.

2. Registra hash dei file per OSINT

•Calcola e registra gli hash dei file eseguibili, permettendo di confrontarli con database pubblici (es. VirusTotal) per identificare potenziali malware.

3. GUID del processo per correlare eventi

•Ogni processo ha un identificatore unico (GUID), permettendo di collegare eventi diversi (es. modifiche file o connessioni di rete) allo stesso processo, essenziale per le indagini di sicurezza.

Insight: GUID del Processo

Perché il GUID è utile per correlare eventi in Sysmon?
Quando si analizza un incidente di sicurezza o si monitora il comportamento del sistema, il GUID (Globally Unique Identifier , relativo a un processo) consente di collegare facilmente i vari eventi associati a un singolo processo. Ad esempio, puoi usare il GUID per:

1. **Collegare la creazione di un processo ad altre attività**, come le connessioni di rete o modifiche ai file.
2. **Tracciare il comportamento del processo nel tempo**, anche se il nome del processo può essere comune o se ci sono più istanze dello stesso processo in esecuzione (ad esempio, "notepad.exe").
3. **Rilevare attività sospette**: Se un processo crea connessioni di rete verso server esterni o modifica file di sistema, puoi usare il GUID per verificare **se lo stesso** processo ha avviato **altre azioni malevole**.

Capacità di Logging di Sysmon

4. Monitora le connessioni di rete

•Registra connessioni di rete effettuate da processi, includendo indirizzi IP e porte, aiutando a rilevare comunicazioni sospette o malevoli come connessioni verso server C2.

5. Logging di rete disabilitato di default

•Il monitoraggio delle connessioni di rete è disabilitato per impostazione predefinita. Deve essere attivato manualmente per evitare un eccessivo accumulo di dati.

ID Evento in Sysmon

Cosa sono gli ID Evento in Sysmon?
Gli **ID Evento** sono identificatori numerici assegnati agli eventi che Sysmon monitora. Ogni ID rappresenta un **tipo specifico di attività che avviene sul sistema**, come la creazione di un processo, una connessione di rete, o un tentativo di evasione. Monitorare questi eventi con Sysmon aiuta a identificare e analizzare comportamenti sospetti o dannosi sul sistema, offrendo visibilità su diversi aspetti delle attività di sistema.

ID Evento in Sysmon

1. ID Evento 1: Creazione di processi

•**Cosa monitora:** Traccia quando un processo viene avviato. Questo include informazioni come il nome del processo, il percorso del file eseguibile, gli argomenti della riga di comando utilizzati, e l'hash del file eseguibile.

•**Perché è importante:** Fornisce una visione dettagliata delle applicazioni che vengono eseguite sul sistema. Gli hash dei file possono essere usati per confrontare i processi con database di malware conosciuti, identificando software potenzialmente pericoloso.

2. ID Evento 3: Connessioni di rete originate dai processi

•**Cosa monitora:** Registra ogni connessione di rete che parte da un processo specifico. Le informazioni includono l'indirizzo IP e la porta locale, l'indirizzo IP e la porta remota, il protocollo utilizzato (TCP/UDP), e il processo che ha generato la connessione.

•**Perché è importante:** È fondamentale per rilevare traffico di rete sospetto, come connessioni verso server malevoli (es. Command and Control) o connessioni attraverso porte non standard. Aiuta a individuare quali processi stanno comunicando su reti esterne.

ID Evento in Sysmon

3. ID Evento 6-8: Tentativi di evasione

•**Cosa monitora:**

- **ID Evento 6**: Traccia le modifiche ai permessi sui file, che possono essere un tentativo di compromettere la sicurezza.
- **ID Evento 7**: Monitora tentativi di **code injection**, dove un processo inietta codice malevolo in un altro processo legittimo.
- **ID Evento 8**: Traccia la creazione di **file remoti**, spesso utilizzata in tecniche di evasione per eseguire codice esternamente.

•**Perché è importante:** Questi eventi aiutano a rilevare tentativi di evasione dei controlli di sicurezza, come attacchi che mirano a nascondere il codice malevolo all'interno di processi legittimi. Anche se possono generare falsi positivi, sono essenziali per identificare tentativi di attacco più sofisticati.

ID Evento in Sysmon

4. ID Evento 10: Accesso alle credenziali (attacchi lsass.exe)
•**Cosa monitora:** Registra quando un processo tenta di accedere alla memoria di un altro processo, come l'acquisizione di credenziali. Questo include attacchi diretti a **lsass.exe**, che è il processo responsabile della gestione delle credenziali di Windows.
•**Perché è importante:** Attacchi come **Mimikatz** tentano di estrarre credenziali sensibili dalla memoria del processo **lsass.exe**. Monitorare questo evento è cruciale per identificare tentativi di furto di credenziali e accessi non autorizzati.

5. ID Evento 22: Query DNS
•**Cosa monitora:** Registra ogni query DNS fatta da un processo. Questo include il dominio richiesto e il processo che ha generato la richiesta.
•**Perché è importante:** È utile per rilevare comportamenti sospetti legati a domini pericolosi. Alcuni malware usano **DGA (Domain Generation Algorithms)** per generare automaticamente e dinamicamente nomi di dominio, rendendo difficile il rilevamento. Questo evento aiuta a tracciare quali domini sono stati richiesti, permettendo di individuare attività potenzialmente malevole.