# RAPORT Z ANALIZY LOGÓW W SIEM

Analiza podejrzanego połączenia sieciowego i mechanizmu persistence w SIEM

Celem analizy było:

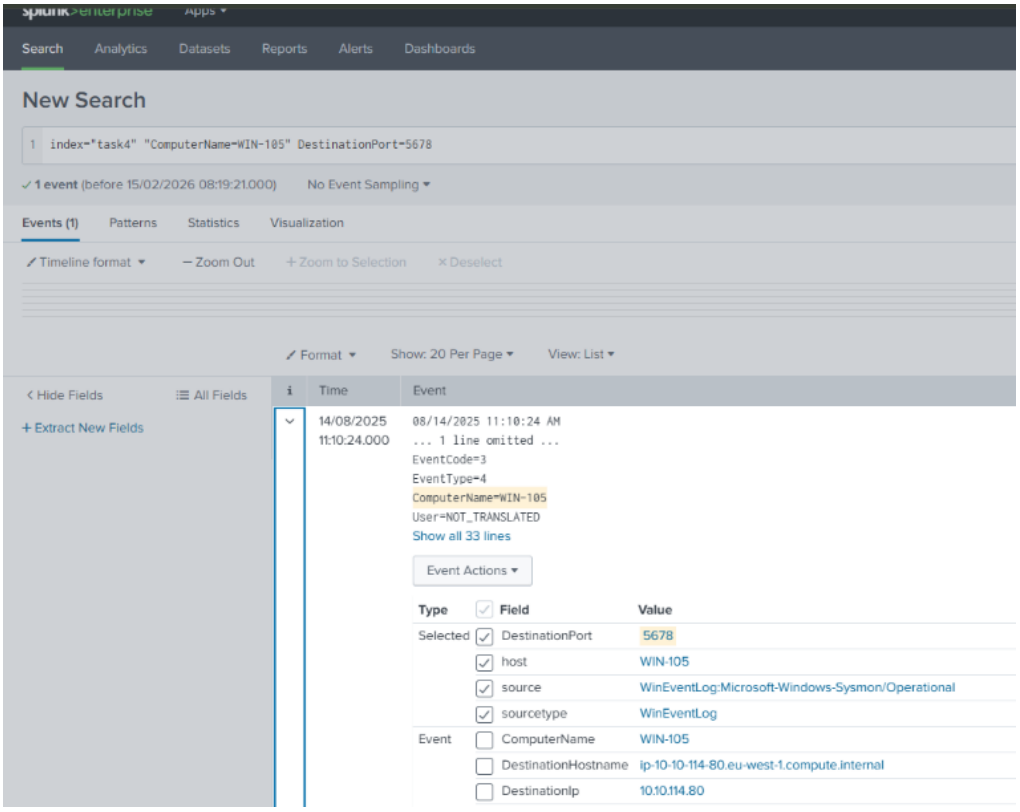
- zidentyfikowanie źródła i charakteru połączenia,
- ustalenie procesu odpowiedzialnego za ruch sieciowy,
- sprawdzenie potencjalnych mechanizmów persistence,
- ocena ryzyka i wpływu na środowisko.

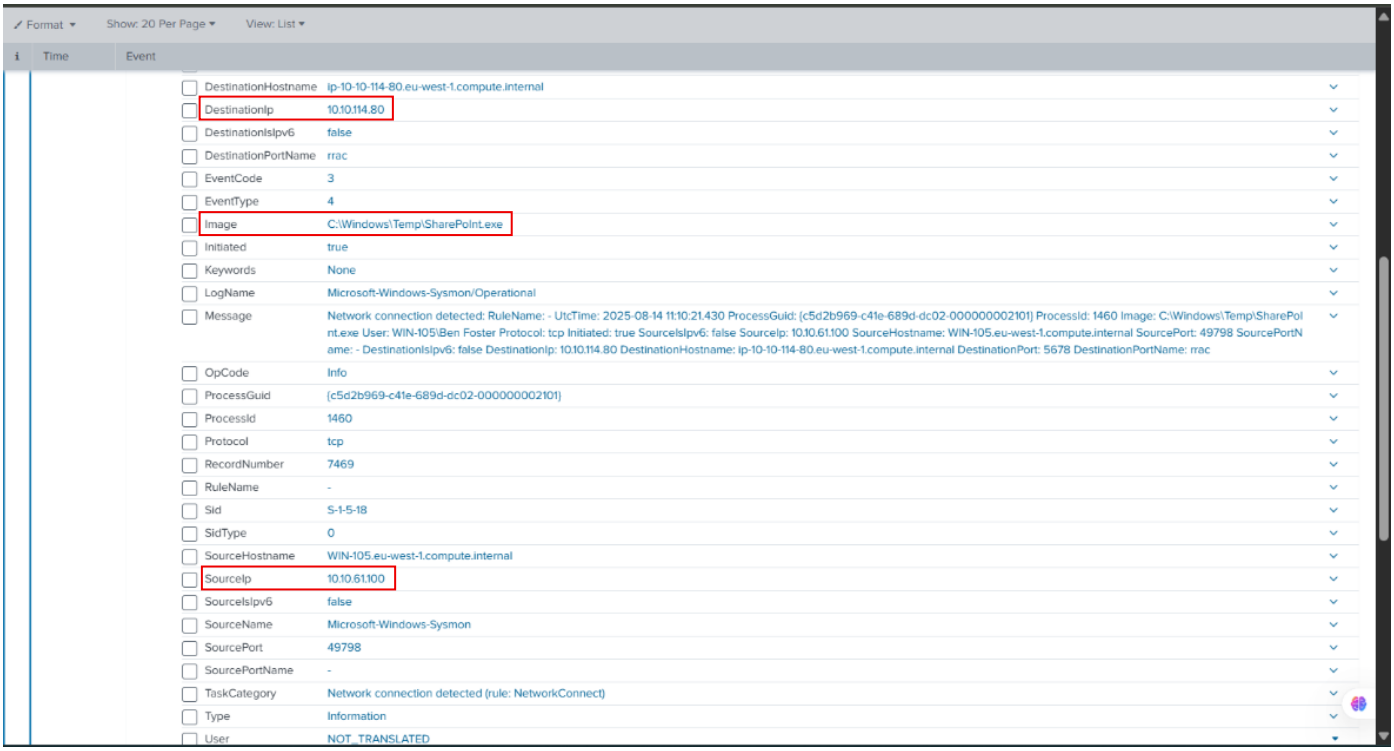
**Practice Scenario**

> You are an SOC Level 1 Analyst on shift and have received an alert indicating a suspicious network connection using port 5678 on the WIN-105 host. Your task is to conduct an investigation and determine whether this activity is suspicious.

The logs for this task are located in the Splunk index task4. Use the following query:

```
index=task4
```






Alert został wygenerowany na podstawie logów sieciowych pochodzących z Sysmon (zdarzenia Network Connection). Nietypowy był zarówno **port docelowy**, jak i fakt, że połączenie odbywało się **wewnątrz sieci LAN**.

Odnaleziony adres IP jest z grupy prywatnych. Oznacza to że połączenie zostało nawiązane m.in. poprzez: VPN, proxy lub z endpointu w tej samej sieci.

## Analiza połączenia sieciowego

Zawężono zakres wyszukiwania do konkretnego hosta oraz portu docelowego.

**Wynik analizy:**

- Host źródłowy: 10.10.61.100
- Host docelowy: 10.10.114.80
- Połączenie: internal → internal (ta sama sieć)

Fakt, że komunikacja odbywała się pomiędzy dwoma hostami w tej samej sieci, **znacząco podnosi poziom ryzyka**, ponieważ może oznaczać, że atakujący:

- posiada już dostęp do środowiska,
- próbuje rozszerzyć kontrolę na kolejne endpointy. (tzw. Lateral Movement – ruch boczny)

**Identyfikacja procesu inicjującego połączenie**

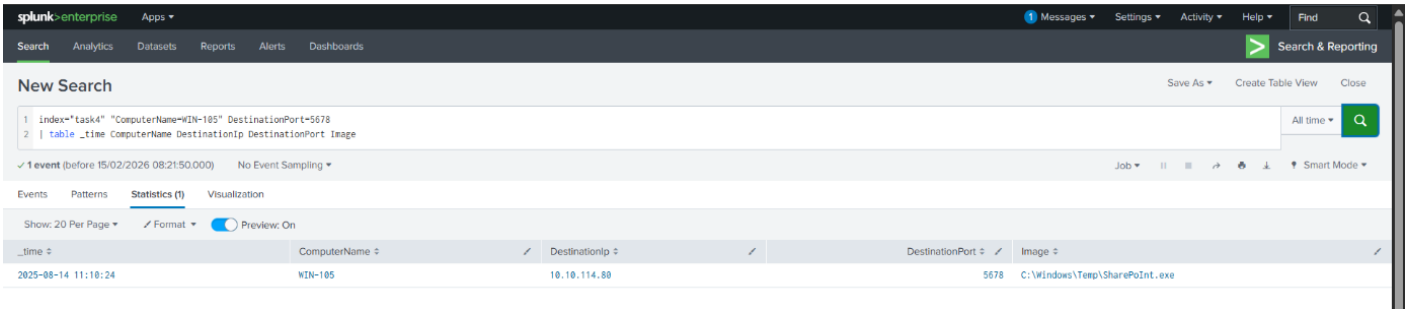
Analiza **procesu, który zainicjował ruch sieciowy** wykazała, że połączenie zostało nawiązane przez plik:

C:\Windows\Temp\SharePoInt.exe

**Obserwacje:**

- Nietypowa lokalizacja (folder Temp).
- Nazwa sugerująca legalną aplikację Microsoft SharePoint, jednak zawierająca **literówkę**.
- Brak zgodności z typowymi ścieżkami instalacyjnymi legalnych komponentów systemowych.

Na tej podstawie proces został zaklasyfikowany jako **wysoko podejrzany.**

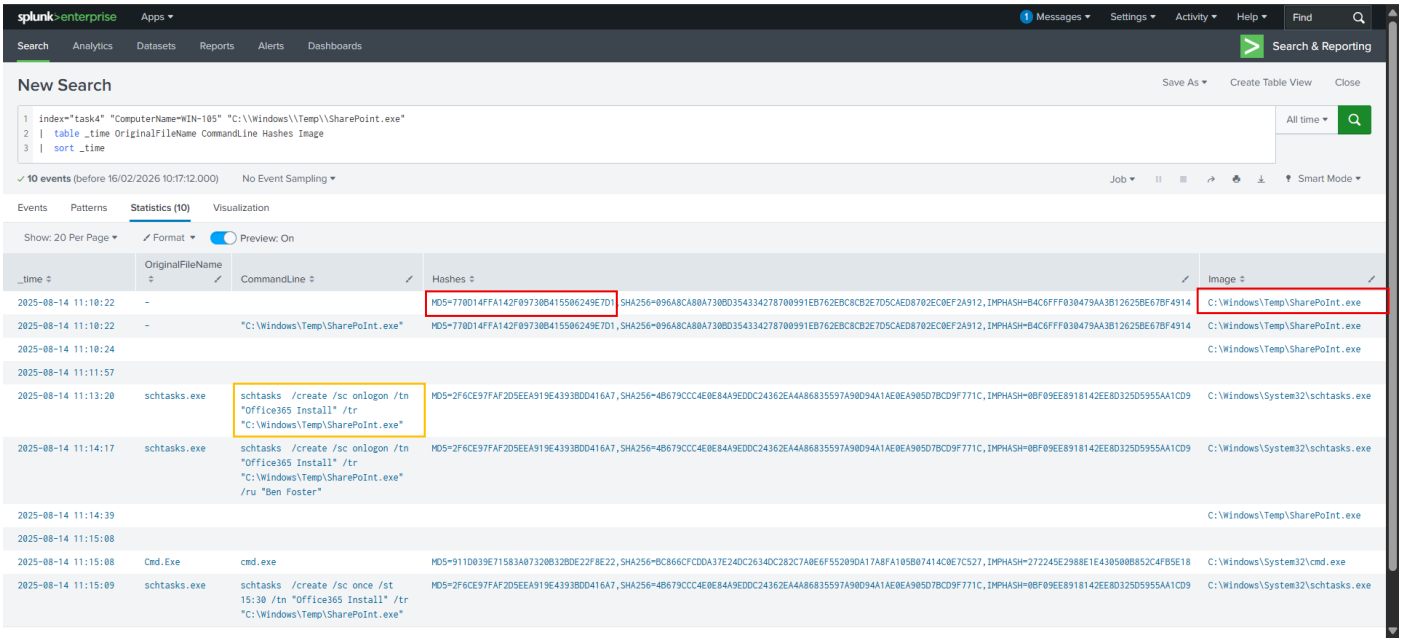



# Analiza pliku i reputacji

*Znajomość hashu wywołanego procesu jest kluczowa w dziedzinie cyberbezpieczeństwa. Działa on jak unikalny cyfrowy odcisk palca konkretnej wersji pliku.*

- *Na przykład: Pozwala natychmiast sprawdzić, czy działający proces jest znanym wirusem, trojanem lub innym zagrożeniem. Bazy danych takie jak VirusTotal przechowują hashe milionów szkodliwych plików, umożliwiając ich błyskawiczne wykrycie. Antywirusy porównują hashe, dzięki czemu są w stanie zapobiec kompromitacji systemu.*
- *Dzięki hashowi można także potwierdzić, że uruchomiony program jest oryginalny i nie został zmodyfikowany przez napastnika (np. wstrzyknięcie kodu do legalnego pliku system32).*

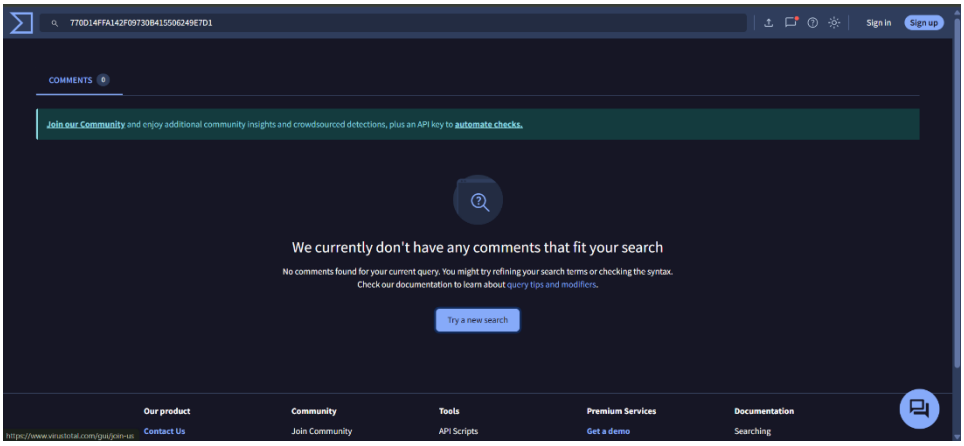
Dla zidentyfikowanego procesu pozyskano metadane oraz skróty kryptograficzne (w tym MD5).




Hash pliku został wykorzystany do weryfikacji reputacji w publicznych bazach zagrożeń (m.in. VirusTotal).

Nie został on dopasowany do znanych próbek.

**Nie wyklucza to złośliwego charakteru pliku.**




**Wnioski:**

- Brak detekcji **nie oznacza bezpieczeństwa**.
- Plik może być:
    - malware typu **FUD (Fully Undetectable)**,
    - narzędziem stworzonym specjalnie pod dany atak (custom payload).

W połączeniu z nietypową lokalizacją i zachowaniem sieciowym, plik należy traktować jako **złośliwy.**

---

# Analiza persistence

Dalsza analiza logów wykazała utworzenie **zaplanowanego zadania systemowego** o nazwie:

*Office365 Install*

**Znaczenie:**

- Zaplanowanie zadania systemowego sugeruje legalne działanie administracyjne.
- Zadanie zostało powiązane czasowo z uruchomieniem podejrzanego procesu.
- Jest to klasyczny mechanizm **utrzymania dostępu (persistence)**

---

# Ocena incydentu

**Klasyfikacja:** High Severity
**Uzasadnienie:**

- Podejrzany proces imitujący legalne oprogramowanie,
- Nawiązanie połączenia sieciowego wewnątrz LAN,
- Wykryty mechanizm persistence,
- Ryzyko lateral movement.

**Rekomendowane działania (Response)**

1. Natychmiastowa izolacja hosta 10.10.61.100.
2. Usunięcie zaplanowanego zadania i podejrzanego pliku.
3. Reset poświadczeń użytkownika powiązanego z hostem.
4. Przeskanowanie środowiska pod kątem:
    - podobnych nazw plików,
    - analogicznych zaplanowanych zadań,
    - komunikacji na port 5678.
5. Utworzenie reguły detekcyjnej w SIEM dla:
    - procesów uruchamianych z katalogu Temp,
    - nazw imitujących produkty Microsoft.

# Podsumowanie

Analiza wykazała, że pojedynczy alert sieciowy może prowadzić do wykrycia **pełnego łańcucha ataku**, obejmującego:

- uruchomienie złośliwego procesu,
- komunikację sieciową,
- mechanizm persistence.

Case potwierdza znaczenie korelacji logów sieciowych i procesowych oraz pokazuje praktyczne podejście do analizy incydentów w środowisku SIEM.

# Refleksja

W trakcie analizy:

- przećwiczyłam identyfikację **procesów podszywających się pod legalne oprogramowanie (masquerading)** na podstawie nazwy pliku, jego lokalizacji oraz obserwowanego zachowania,
- potwierdziłam, że **brak detekcji hasha w bazach reputacyjnych nie oznacza braku zagrożenia**, a ocena pliku musi uwzględniać kontekst jego działania oraz powiązania z innymi zdarzeniami,
- przeanalizowałam na rzeczywistych logach **typowe mechanizmy utrzymania dostępu (persistence)**, w szczególności wykorzystanie zaplanowanych zadań systemowych jako metody zapewnienia ponownego dostępu do systemu.

---

ŹRÓDŁO: https://tryhackme.com/room/loganalysiswithsiem [sekcja: Windows Logs]