

RAPORT Z ANALIZY LOGÓW W SIEM

Analiza podejrzaneego 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`

Splunk > enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards

New Search

```
1 index="task4" "ComputerName=WIN-105" DestinationPort=5678
```

✓ 1 event (before 15/02/2026 08:19:21.000) No Event Sampling ▾

Events (1) Patterns Statistics Visualization

✗ Timeline format ▾ - Zoom Out +Zoom to Selection × Deselect

✓ Format ▾ Show: 20 Per Page ▾ View: List ▾

| Time | Event |
|--|--|
| 14/08/2025 11:10:24 AM 11:10:24.000 | 08/14/2025 11:10:24 AM ... 1 line omitted ... EventCode=3 EventType=4 ComputerName=WIN-105 User=NOT_TRANSLATED Show all 33 lines |

Event Actions ▾

| Type | Field | Value |
|----------|---------------------|--|
| Selected | DestinationPort | 5678 |
| | host | WIN-105 |
| | source | WinEventLog:Microsoft-Windows-Sysmon/Operational |
| | sourcetype | WinEventLog |
| Event | ComputerName | WIN-105 |
| | DestinationHostname | ip-10-10-114-80.eu-west-1.compute.internal |
| | DestinationIp | 10.10.114.80 |

| | Time | Event | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------------|--|---|---------------------|--|---------------|--------------|-------------------|-------|---------------------|------|-----------|---|-----------|---|-------|--------------------------------|-----------|------|----------|------|---------|--------------------------------------|---------|--|--------|------|-------------|--|-----------|------|----------|-----|--------------|------|----------|---|-----|----------|---------|---|----------------|------------------------------------|----------|--------------|--------------|-------|------------|--------------------------|------------|-------|----------------|---|--------------|--|------|-------------|------|----------------|
| | | <table border="1"> <tr><td>DestinationHostname</td><td>ip-10-10-114-80.eu-west-1.compute.internal</td></tr> <tr><td>DestinationIp</td><td>10.10.114.80</td></tr> <tr><td>DestinationIsIPv6</td><td>false</td></tr> <tr><td>DestinationPortName</td><td>rrac</td></tr> <tr><td>EventCode</td><td>3</td></tr> <tr><td>EventType</td><td>4</td></tr> <tr><td>Image</td><td>C:\Windows\Temp\SharePolnt.exe</td></tr> <tr><td>Initiated</td><td>true</td></tr> <tr><td>Keywords</td><td>None</td></tr> <tr><td>LogName</td><td>Microsoft-Windows-Sysmon/Operational</td></tr> <tr><td>Message</td><td>Network connection detected: RuleName: - UtcTime: 2025-08-14 11:10:21.430 ProcessGuid: {c5d2b969-c41e-689d-dc02-000000002101} ProcessId: 1460 Image: C:\Windows\Temp\SharePolnt.exe User: WIN-105\Ben Foster Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 10.10.61.100 SourceHostname: WIN-105.eu-west-1.compute.internal SourcePort: 49798 DestinationIp: 10.10.114.80 DestinationHostname: ip-10-10-114-80.eu-west-1.compute.internal DestinationPort: 5678 DestinationPortName: rrac</td></tr> <tr><td>OpCode</td><td>Info</td></tr> <tr><td>ProcessGuid</td><td>{c5d2b969-c41e-689d-dc02-000000002101}</td></tr> <tr><td>ProcessId</td><td>1460</td></tr> <tr><td>Protocol</td><td>tcp</td></tr> <tr><td>RecordNumber</td><td>7469</td></tr> <tr><td>RuleName</td><td>-</td></tr> <tr><td>Sid</td><td>S-1-5-18</td></tr> <tr><td>SidType</td><td>0</td></tr> <tr><td>SourceHostname</td><td>WIN-105.eu-west-1.compute.internal</td></tr> <tr><td>SourceIp</td><td>10.10.61.100</td></tr> <tr><td>SourceIsIpv6</td><td>false</td></tr> <tr><td>SourceName</td><td>Microsoft-Windows-Sysmon</td></tr> <tr><td>SourcePort</td><td>49798</td></tr> <tr><td>SourcePortName</td><td>-</td></tr> <tr><td>TaskCategory</td><td>Network connection detected (rule: NetworkConnect)</td></tr> <tr><td>Type</td><td>Information</td></tr> <tr><td>User</td><td>NOT_TRANSLATED</td></tr> </table> | DestinationHostname | ip-10-10-114-80.eu-west-1.compute.internal | DestinationIp | 10.10.114.80 | DestinationIsIPv6 | false | DestinationPortName | rrac | EventCode | 3 | EventType | 4 | Image | C:\Windows\Temp\SharePolnt.exe | Initiated | true | Keywords | None | LogName | Microsoft-Windows-Sysmon/Operational | Message | Network connection detected: RuleName: - UtcTime: 2025-08-14 11:10:21.430 ProcessGuid: {c5d2b969-c41e-689d-dc02-000000002101} ProcessId: 1460 Image: C:\Windows\Temp\SharePolnt.exe User: WIN-105\Ben Foster Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 10.10.61.100 SourceHostname: WIN-105.eu-west-1.compute.internal SourcePort: 49798 DestinationIp: 10.10.114.80 DestinationHostname: ip-10-10-114-80.eu-west-1.compute.internal DestinationPort: 5678 DestinationPortName: rrac | OpCode | Info | ProcessGuid | {c5d2b969-c41e-689d-dc02-000000002101} | ProcessId | 1460 | Protocol | tcp | RecordNumber | 7469 | RuleName | - | Sid | S-1-5-18 | SidType | 0 | SourceHostname | WIN-105.eu-west-1.compute.internal | SourceIp | 10.10.61.100 | SourceIsIpv6 | false | SourceName | Microsoft-Windows-Sysmon | SourcePort | 49798 | SourcePortName | - | TaskCategory | Network connection detected (rule: NetworkConnect) | Type | Information | User | NOT_TRANSLATED |
| DestinationHostname | ip-10-10-114-80.eu-west-1.compute.internal | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DestinationIp | 10.10.114.80 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DestinationIsIPv6 | false | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DestinationPortName | rrac | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| EventCode | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| EventType | 4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Image | C:\Windows\Temp\SharePolnt.exe | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Initiated | true | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Keywords | None | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LogName | Microsoft-Windows-Sysmon/Operational | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Message | Network connection detected: RuleName: - UtcTime: 2025-08-14 11:10:21.430 ProcessGuid: {c5d2b969-c41e-689d-dc02-000000002101} ProcessId: 1460 Image: C:\Windows\Temp\SharePolnt.exe User: WIN-105\Ben Foster Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 10.10.61.100 SourceHostname: WIN-105.eu-west-1.compute.internal SourcePort: 49798 DestinationIp: 10.10.114.80 DestinationHostname: ip-10-10-114-80.eu-west-1.compute.internal DestinationPort: 5678 DestinationPortName: rrac | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OpCode | Info | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ProcessGuid | {c5d2b969-c41e-689d-dc02-000000002101} | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ProcessId | 1460 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Protocol | tcp | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecordNumber | 7469 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RuleName | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sid | S-1-5-18 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SidType | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SourceHostname | WIN-105.eu-west-1.compute.internal | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SourceIp | 10.10.61.100 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SourceIsIpv6 | false | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SourceName | Microsoft-Windows-Sysmon | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SourcePort | 49798 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SourcePortName | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TaskCategory | Network connection detected (rule: NetworkConnect) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Type | Information | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| User | NOT_TRANSLATED | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

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, **znaczaco 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\SharePolnt.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**.

```
index="task4" "ComputerName=WIN-105" DestinationPort=5678
2 | table _time ComputerName DestinationIp DestinationPort Image
✓ 1 event (before 15/02/2026 08:21:50.000) No Event Sampling

Events Patterns Statistics (1) Visualization
Show: 20 Per Page ▾ Format ▾ Preview: On
_time ▾ ComputerName ▾ DestinationIp ▾ DestinationPort ▾ Image ▾
2025-08-14 11:10:24 WIN-105 10.10.114.80 5678 C:\Windows\Temp\SharePoint.exe
```

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. wstrzygnięcie kodu do legalnego pliku system32).

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

```
index="task4" "ComputerName=WIN-105" "C:\Windows\Temp\SharePoint.exe"
2 | table _time OriginalFileName CommandLine Hashes Image
3 | sort _time
✓ 10 events (before 16/02/2026 10:17:12.000) No Event Sampling

Events Patterns Statistics (10) Visualization
Show: 20 Per Page ▾ Format ▾ Preview: On
_time ▾ OriginalFileName ▾ CommandLine ▾ Hashes ▾ Image ▾
2025-08-14 11:10:22 - MD5=770014FFA142F09730B415596249E7D1 SHA256=096A8CA80A730B035433427870991EB762EBC8CB2E705CAED8702EC0EF2A912,IMPHASH=B4C6FFF030479AA3B12625B6E7BF4914 C:\Windows\Temp\SharePoint.exe
2025-08-14 11:10:22 - "C:\Windows\Temp\SharePoint.exe" MD5=770014FFA142F09730B415596249E7D1,SHA256=096A8CA80A730B035433427870991EB762EBC8CB2E705CAED8702EC0EF2A912,IMPHASH=B4C6FFF030479AA3B12625B6E7BF4914 C:\Windows\Temp\SharePoint.exe
2025-08-14 11:10:24
2025-08-14 11:11:57
2025-08-14 11:13:20 schtasks.exe schtasks /create /sc onlogon /tn "Office365 Install" /tr "C:\Windows\Temp\SharePoint.exe" MD5=2F6CE97FAF205EEA919E4393B0D416A7,SHA256=4B679CCC4E0E84A9EDC24362EA4A8E835597A9094A1E0EA905D78C09F771C,IMPHASH=0BF09EE8918142E80325D955AA1CD9 C:\Windows\System32\schtasks.exe
2025-08-14 11:14:17 schtasks.exe schtasks /create /sc once /st 15:30 /tn "Office365 Install" /tr "C:\Windows\Temp\SharePoint.exe" /ru "Ben Foster" MD5=2F6CE97FAF205EEA919E4393B0D416A7,SHA256=4B679CCC4E0E84A9EDC24362EA4A8E835597A9094A1E0EA905D78C09F771C,IMPHASH=0BF09EE8918142E80325D955AA1CD9 C:\Windows\System32\schtasks.exe
2025-08-14 11:14:39
2025-08-14 11:15:08 Cmd.Exe cmd.exe MD5=911D0B39E71583A07320832BDE22F8E22,SHA256=BC866CCFDA37E24DC2634DC2827A0E6F55209DA17A8FA105B0741C0E7C527,IMPHASH=272245E2988E1E430500B852C4FB5E18 C:\Windows\System32\cmd.exe
2025-08-14 11:15:09 schtasks.exe schtasks /create /sc once /st 15:30 /tn "Office365 Install" /tr "C:\Windows\Temp\SharePoint.exe" MD5=2F6CE97FAF205EEA919E4393B0D416A7,SHA256=4B679CCC4E0E84A9EDC24362EA4A8E835597A9094A1E0EA905D78C09F771C,IMPHASH=0BF09EE8918142E80325D955AA1CD9 C:\Windows\System32\schtasks.exe
```

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.

The screenshot shows the VirusTotal interface with a search bar at the top containing the hash value: 770D14FFA142F09730B415506249ETD1. Below the search bar is a green banner with the text "Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks." The main content area has a heading "COMMENTS 0" and a message: "We currently don't have any comments that fit your search. No comments found for your current query. You might try refining your search terms or checking the syntax. Check our documentation to learn about query tips and modifiers." At the bottom of the page, there is a navigation bar with links: "Our product", "Contact Us", "Community", "Tools", "Premium Services", "Documentation", and "Get a demo".

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 wewnętrz LAN,
- Wykryty mechanizm persistence,
- Ryzyko lateral movement.

Rekomendowane działania (Response)

1. Natychmiastowa izolacja hosta 10.10.61.100.
2. Usunięcie zaplanowanego zadania i podejrzanej 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:

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