



# Zero Trust w środowiskach aplikacyjnych

Marcin Kornafel  
Sevenet S.A.

Tomasz Jedynak  
Cisco Systems





Zaufanie



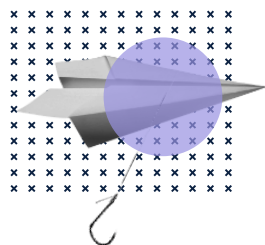
Wymuszenie



Ciągła weryfikacja



## Ograniczenie ryzyku



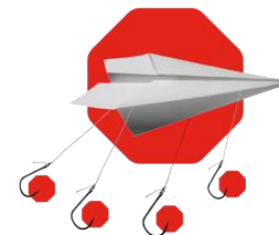
Zmniejszenie ryzyka  
naruszenia  
bezpieczeństwa

## Zyskaj widoczność



Identyfikacja ryzyka i  
symptomów  
naruszenia  
bezpieczeństwa

## Redukcja powierzchni ataku



Zatrzymanie włamania  
i ograniczenie lateral  
movement

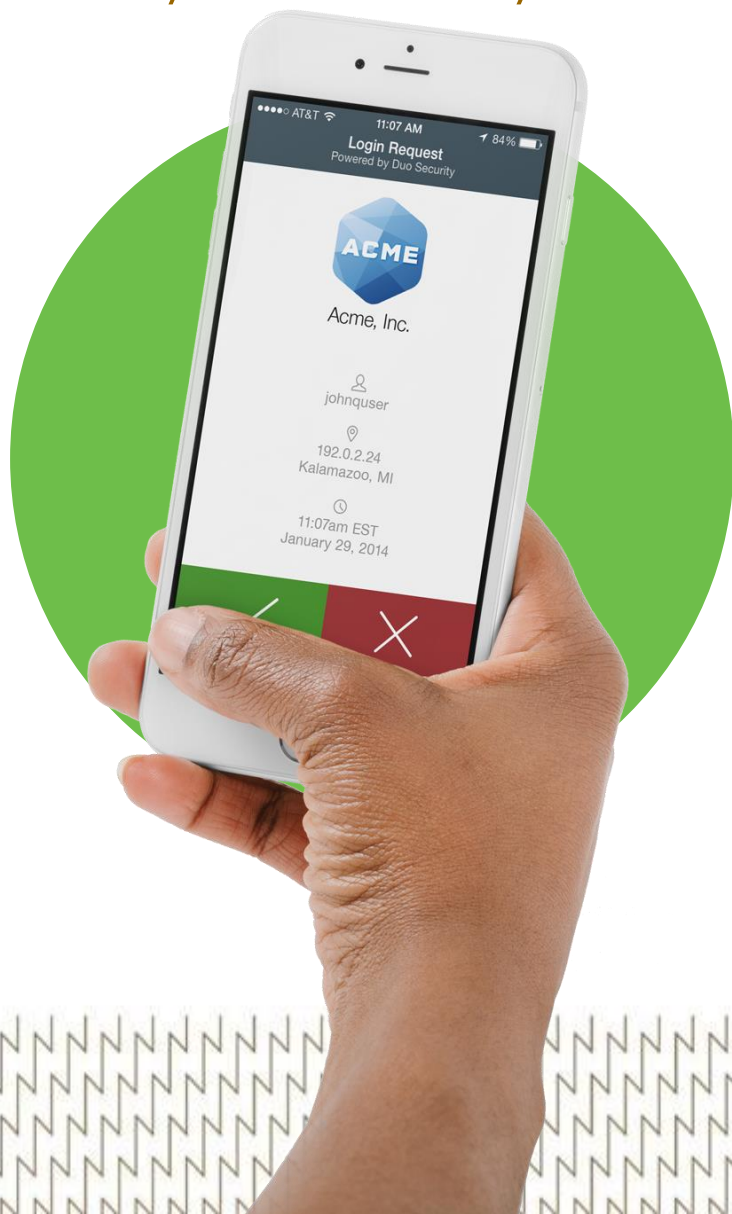
## Filozofia Zero Trust

Włącz kontrolę opartą na  
polityce  
dla każdego żądania dostępu w  
środowisku korporacyjnym

Sprawdź, kto i co  
uzyskuje dostęp do aplikacji,  
zasobów i sieci

Segmentacja sieci  
i zasobów roboczych poprzez  
egzekwowanie odpowiedniej  
polityki





99%

Eksploituowanych podatności jest znana przez organizacje przez przynajmniej rok

Source: Gartner, Dale Gardner, 2018 Security Summit

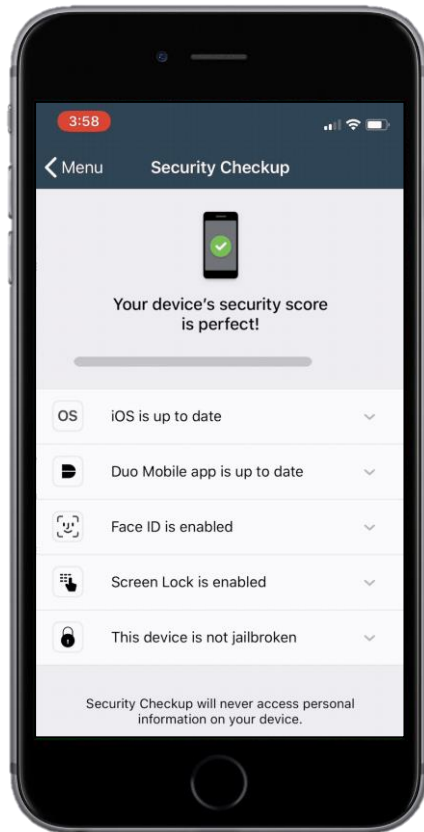
81%

Włamań wykorzystuje skradzione lub złamane hasła

Source: Verizon 2018 Data Breach Investigations Report



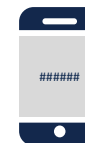




Wearables



Push

Phone  
Call

Soft Token



Biometrics



U2F

Hardware  
Tokens

SMS



Aplikacje  
własneŚrodowiska  
MicrosoftUsługi  
Chmurowe

Unix (SSH)



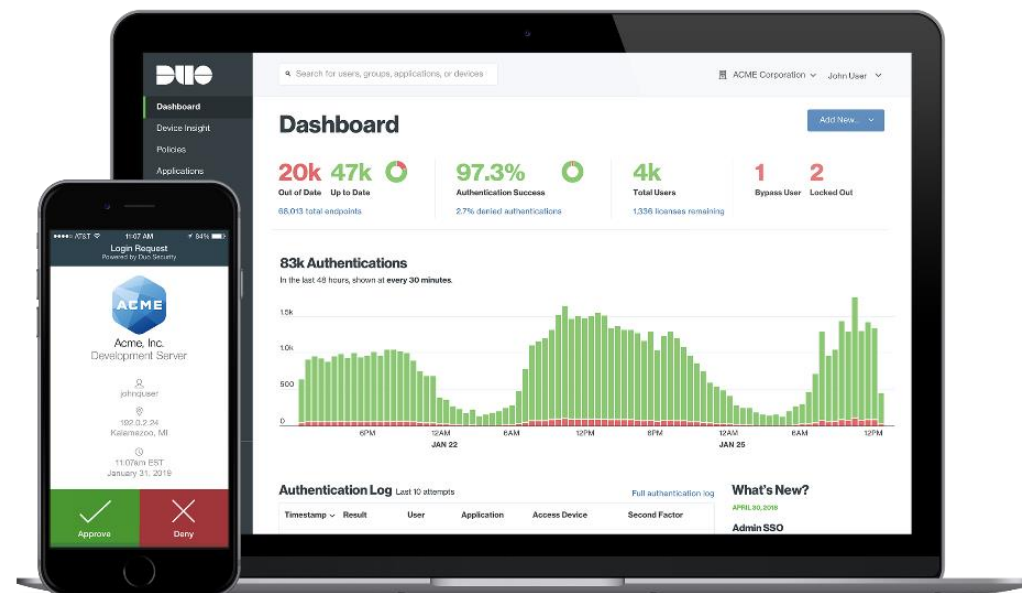
VPN

Aplikacje  
ChmuroweAplikacje  
WebAplikacje  
SAML 2.0

## Operating Systems by Platform



## Trusted Endpoints (58)

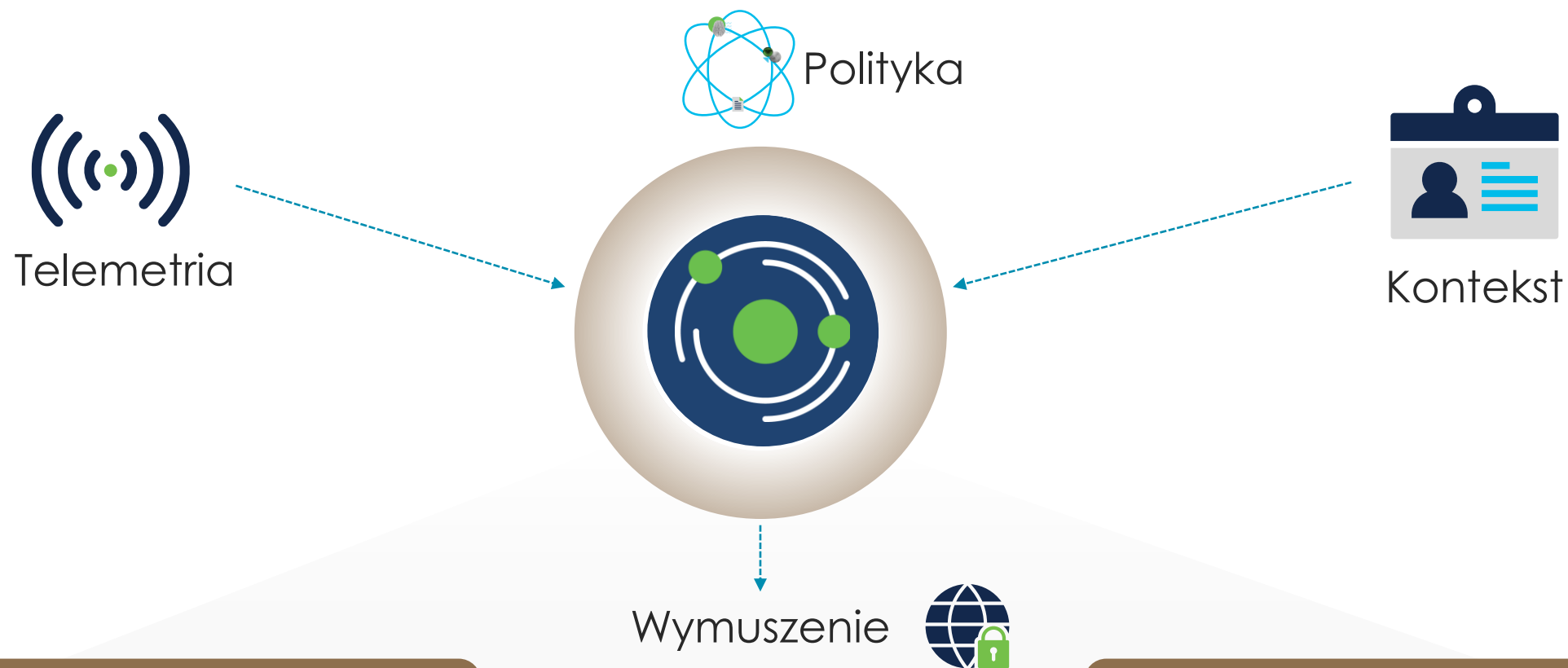




## Mikrosegmentacja + Dane “Big Data”







Host

Chmura

Sieć



Segmentation / Overview

Your browser is not fully supported. For best results, please use [Google Chrome](#).

Segmentation

Analyzed Applications4

Enforced Applications4

Pending Policy Connectors0

Workspaces

Draft Policies

Policy Requests

5 Workspaces

Q Filter all application workspaces

Sort

SharePoint

mslab : SharePoint

PRIMARY

ENFORCED

0 Conversations

5 Clusters

178 Policies

Last updated: SEP 20, 10:22 PM

Developer Workstations

mslab : DeveloperWorkstations

PRIMARY

0 Conversations

2 Clusters

13 Policies

Last updated: FEB 18, 10:10 PM

AppDev Servers

mslab : AppDev-Servers

PRIMARY

ENFORCED

163 Conversations

1 Cluster

52 Policies

Last updated: FEB 18, 10:09 PM

Reporting

mslab : Reporting

PRIMARY

ENFORCED

230 Conversations

2 Clusters

114 Policies

Last updated: FEB 18, 10:09 PM

Domain Controllers

mslab : DomainControllers

PRIMARY

ENFORCED

658 Conversations

1 Cluster

54 Policies

Last updated: FEB 18, 10:05 PM

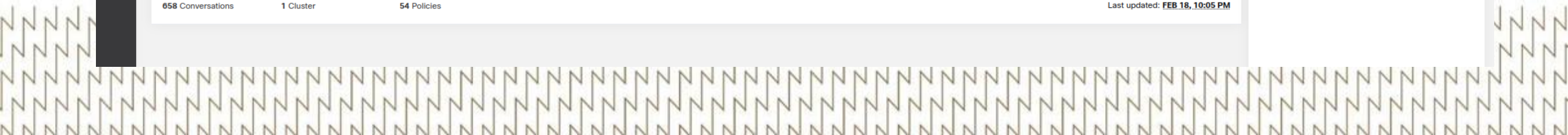
Get Started

1. Create Filter

2. Add Policy

3. Start Analysis

4. Enable Enforcement





# Polityki dla serwera



Cisco Secure Workload



Your browser is not fully supported. For best results, please use [Google Chrome](#).

## Reporting PRIMARY

[Switch Application](#)

mslab : Reporting Version: v4 Last Run: Oct 24, 5:45 AM

Activity Log Matching Inventories 13 Conversations 230 Filters 2 Policies 114 Provided Services App View 1

Policy Analysis Enforcement

Filter Policies ...

Absolute policies 0 Default policies 113 Catch All DENY

DENY and policies for ANY protocol have different behavior in Windows firewalls when compared to Linux. See [User Guide](#) for more details.

| ▼ | Priority ↑↓ | Action ↑↓ | Consumer ↑↓                   | Provider ↑↓               | Protocols And Ports ↑↓                     |
|---|-------------|-----------|-------------------------------|---------------------------|--------------------------------------------|
|   | 100         | ALLOW     | Reporting-DatabaseTier        | mslab                     | UDP : 53 (DNS) ...4 more                   |
|   | 100         | ALLOW     | Reporting-Web/AppTier         | mslab                     | UDP : 53 (DNS) ...4 more                   |
|   | 100         | ALLOW     | Reporting-DatabaseTier        | mslab : DomainControllers | ICMP : 0 ...8 more                         |
|   | 100         | ALLOW     | Reporting-Web/AppTier         | mslab : DomainControllers | ICMP : 0 ...9 more                         |
|   | 100         | ALLOW     | Reporting-DatabaseTier        | mslab : TetrationMS       | TCP : 443 (HTTPS) ...2 more                |
|   | 100         | ALLOW     | Reporting-Web/AppTier         | mslab : TetrationMS       | TCP : 443 (HTTPS) ...2 more                |
|   | 100         | ALLOW     | ApplicationDevelopmentServers | mslab : Reporting         | TCP : 80 (HTTP)                            |
|   | 100         | ALLOW     | DomainControllers             | mslab : Reporting         | UDP : 123 (NTP)                            |
|   | 100         | ALLOW     | mslab                         | Reporting-DatabaseTier    | UDP : 53797 ...1 more                      |
|   | 100         | ALLOW     | mslab : TetrationMS           | Reporting-DatabaseTier    | TCP : 49232 ...2 more                      |
|   | 100         | ALLOW     | Reporting-Web/AppTier         | Reporting-DatabaseTier    | UDP : 137 (NETBIOS Name Service) ...2 more |



Cisco Secure Workload



cisco SECURE

Your browser is not fully supported. For best results, please use [Google Chrome](#).

## Reporting PRIMARY

[Switch Application](#)

mslab : Reporting Version: v4 Last Run: Oct 24, 5:45 AM

Activity Log

Matching Inventories 13

Conversations 230

Filters 2

Policies 114

Provided Services

App View 1

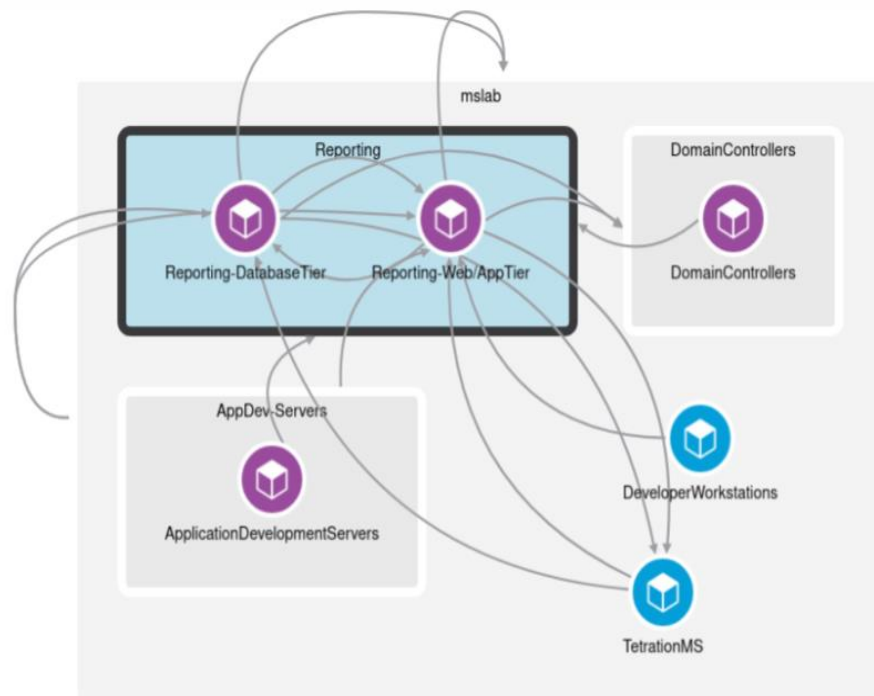
Policy Analysis

Enforcement



Quick Analysis

Filter Policies ...



Priority 100

Action ALLOW

Consumer mslab:TetrationMS

Provider Reporting-Web/AppTier

Flows View Conversations

Protocols and Ports 8

- TCP : 53629
- TCP : 53633
- TCP : 53642
- TCP : 62630
- TCP : 64791
- TCP : 64794
- TCP : 64800-64801
- TCP : 64804





# Test polityk



Cisco Secure Workload



Your browser is not fully supported. For best results, please use [Google Chrome](#).

## Reporting PRIMARY

[Switch Application](#)

[mslab : Reporting](#) Version: v4 Last Run: Oct 24, 5:45 AM

Activity Log Matching Inventories **13** Conversations **230** Filters **2** Policies **114** Provided Services App View **1**

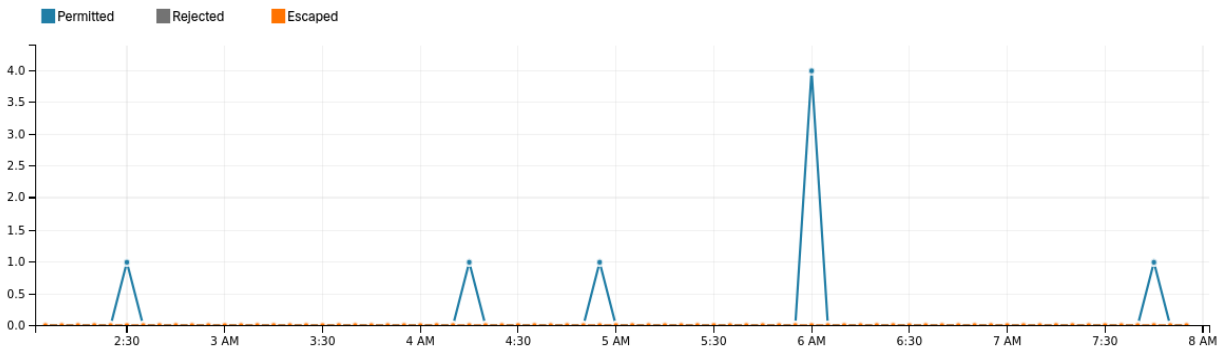
Policy Analysis Enforcement

**Consumer Address = 10.107.0.21** **Provider Address = 10.107.0.12** **Provider Port = 389** **Protocol = UDP**

[Filter Flows](#)

Filtered [Flow Observations](#)

[Permitted](#) [Rejected](#) [Escaped](#)



Found **8** Flow Observations [Show 20](#)

|  | Timestamp ↑↓     | Policy Categories ↑↓ | Consumer Name ↑↓ | Provider Name ↑↓ | Consumer Address ↑↓ | Provider Address ↑↓ | Consumer Port ↑↓ | Provider Port ↑↓ | Protocol ↑↓ | Service Name ↑↓ | Inbound Enforce |
|--|------------------|----------------------|------------------|------------------|---------------------|---------------------|------------------|------------------|-------------|-----------------|-----------------|
|  | Dec 12 2:32:00am | PERMITTED            | SQL01            | dc02             | 10.107.0.21         | 10.107.0.12         | 56588            | 389              | UDP         | LDAP            | Default         |
|  | Dec 12 4:18:00am | PERMITTED            | SQL01            | dc02             | 10.107.0.21         | 10.107.0.12         | 56956            | 389              | UDP         | LDAP            | Default         |
|  | Dec 12 4:56:00am | PERMITTED            | SQL01            | dc02             | 10.107.0.21         | 10.107.0.12         | 53406            | 389              | UDP         | LDAP            | Default         |
|  | Dec 12 6:04:00am | PERMITTED            | SQL01            | dc02             | 10.107.0.21         | 10.107.0.12         | 59554            | 389              | UDP         | LDAP            | Default         |

Top [Names](#) contributing to the selected Flow Observations.

Consumer Names

SQL01

Provider Names

dc02



# Wersje zmian



Cisco Secure Workload

SECURE

Your browser is not fully supported. For best results, please use [Google Chrome](#).

Reporting PRIMARY [Switch Application](#)

mslab : Reporting Version: v4 Last Run: Oct 24, 5:45 AM

Activity Log Matching Inventories 13 Conversations 230 Filters 2 Policies 114 Provided Services App View 1 Policy Analysis Enforcement

Application Activity Log Versions 5 Published Versions 4 [Compare Revisions](#)

v4 *untitled* [Switch to Version](#)

8 log events - Last Updated: **Feb 18, 10:09 PM**  
Created Oct 24, 5:43 AM by Vivek Dalvi <vivdalvi@cisco.com> via an ADM run.

v3 *untitled* [Switch to Version](#)

4 log events - Last Updated: **Oct 24, 5:35 AM**  
Created Oct 23, 5:18 PM by Vivek Dalvi <vivdalvi@cisco.com> via an ADM run.

v2 *untitled* [Switch to Version](#)

2 log events - Last Updated: **Oct 23, 4:49 PM**  
Created Oct 23, 4:38 PM by Vivek Dalvi <vivdalvi@cisco.com> via an ADM run.

v1 *untitled* [Switch to Version](#)

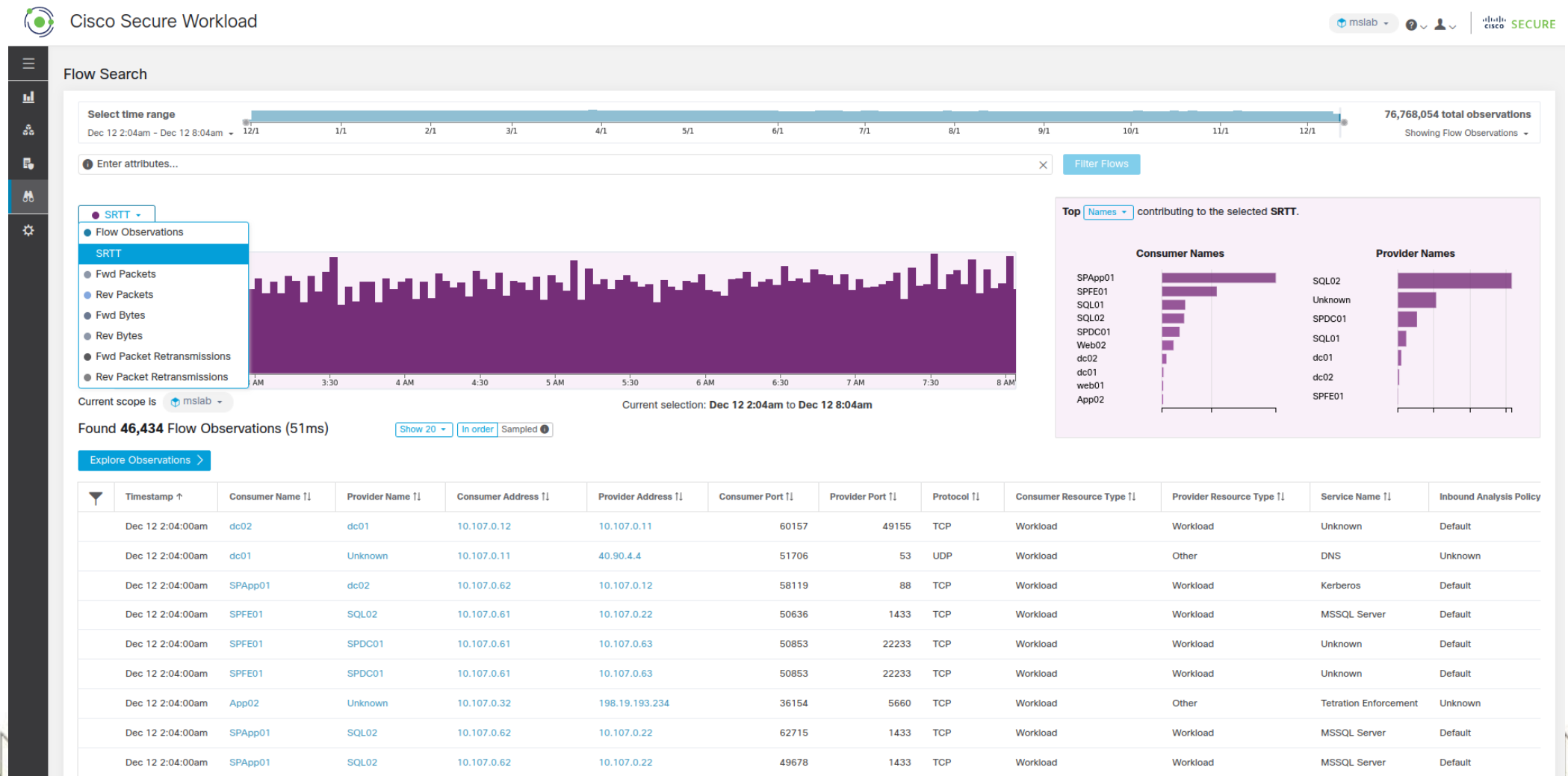
1 log event - Last Updated: **Oct 23, 4:37 PM**  
Created May 4, 1:10 AM

v0 *untitled* [Switch to Version](#)

0 log events  
Created May 4, 1:10 AM



# Dane „Big Data”



https://tetration.sund dc-03.com



Cisco Secure Workload

mslab



cisco SECURE

Dec 12 2:04:00am

SPFE01

SQL02

10.107.0.61

10.107.0.22

50636

1433

TCP

Workload

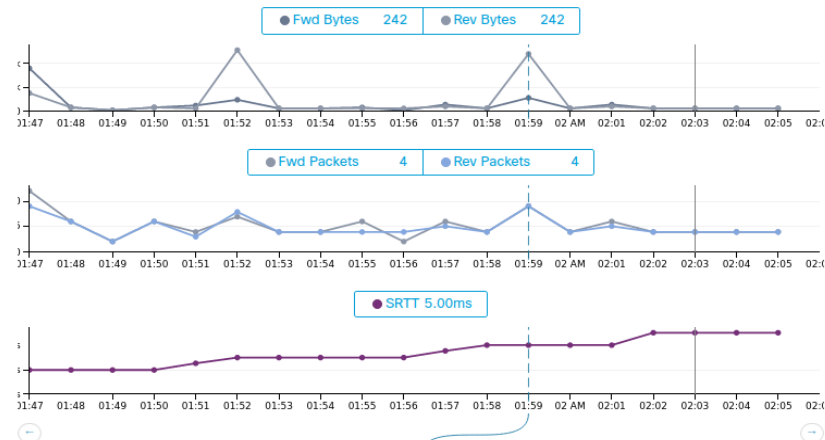
Workload

MSSQL Server

Default

## Flow Details

SPFE01 - 10.107.0.61 on port 50636 ↔ SQL02 - 10.107.0.22 on port 1433 (MSSQL Server) over TCP beginning on Dec 12 01:46:42 am (CET) lasting for 19 minutes.



Dec 12 01:59:00 am (CET)

|                    | Consumer ⓘ           | Provider ⓘ            |
|--------------------|----------------------|-----------------------|
| Flags              | PSH ACK              | PSH ACK               |
| ICMP Type and Code |                      |                       |
| Byte Count         | 1,100 (8,764 so far) | 4,829 (14,174 so far) |
| Packet Count       | 9 (72 so far)        | 9 (68 so far)         |
| SRTT               | 4.00ms               |                       |
| Drop Reason        | N/A                  | N/A                   |





# Opóźnienia w aplikacji



Cisco Secure Workload

mslab

SECURE

Your browser is not fully supported. For best results, please use [Google Chrome](#).

Flow Search

Select time range

Apr 26 3:42pm - Jun 5 9:52pm

12/1 1/1 2/1 3/1 4/1 5/1 6/1 7/1 8/1 9/1 10/1 11/1 12/1

76,752,177 total observations

Showing Flow Observations

( TCP Performance - App Limited )

Filter Flows

Flow Observations

Current scope is mslab

Current selection: Apr 26 3:42pm to Jun 5 9:52pm

Found 117 Flow Observations (75ms)

Show 20 In order Sampled

Explore Observations

|  | Timestamp ↑       | Consumer Name ↑ | Provider Name ↑ | Consumer Address ↑ | Provider Address ↑ | Consumer Port ↑ | Provider Port ↑ | Protocol ↑ | Consumer Resource Type ↑ | Provider Resource Type ↑ | Service Name ↑ | Inbound Analysis Policy Ran |
|--|-------------------|-----------------|-----------------|--------------------|--------------------|-----------------|-----------------|------------|--------------------------|--------------------------|----------------|-----------------------------|
|  | May 18 6:00:00am  | SQL02           | Unknown         | 10.107.0.22        | 65.55.44.109       | 51931           | 443             | TCP        | Workload                 | Other                    | HTTPS          | Unknown                     |
|  | May 18 7:10:00am  | SQL01           | Unknown         | 10.107.0.21        | 65.55.44.109       | 49331           | 443             | TCP        | Workload                 | Other                    | HTTPS          | Unknown                     |
|  | May 18 7:40:00am  | SQL01           | Unknown         | 10.107.0.21        | 65.55.44.109       | 49354           | 443             | TCP        | Workload                 | Other                    | HTTPS          | Unknown                     |
|  | May 18 7:55:00am  | SQL01           | Unknown         | 10.107.0.21        | 65.55.44.109       | 49360           | 443             | TCP        | Workload                 | Other                    | HTTPS          | Unknown                     |
|  | May 18 9:47:00am  | SQL02           | Unknown         | 10.107.0.22        | 65.55.44.109       | 52097           | 443             | TCP        | Workload                 | Other                    | HTTPS          | Unknown                     |
|  | May 18 12:12:00pm | SQL01           | Unknown         | 10.107.0.21        | 65.55.44.109       | 49458           | 443             | TCP        | Workload                 | Other                    | HTTPS          | Unknown                     |
|  | May 18 3:59:00pm  | SQL02           | Unknown         | 10.107.0.22        | 65.55.44.109       | 52360           | 443             | TCP        | Workload                 | Other                    | HTTPS          | Unknown                     |
|  | May 18 4:23:00pm  | SQL01           | Unknown         | 10.107.0.21        | 65.55.44.109       | 49573           | 443             | TCP        | Workload                 | Other                    | HTTPS          | Unknown                     |

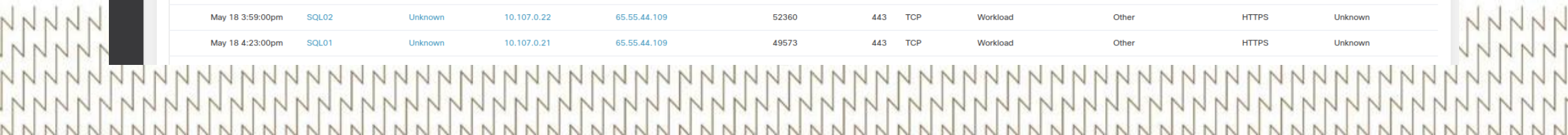
Top Names contributing to the selected Flow Observations.

Consumer Names

SQL01  
App02  
SPDC01  
SQL02  
web01  
SPFE01  
SPApp01  
App01  
dc02  
dc01

Provider Names

Unknown





# Opóźnienia na sieci



mslab

?

SECURE

Flow Search

Select time range

Apr 26 3:42pm - Sep 18 10:54pm

12/1 1/1 2/1 3/1 4/1 5/1 6/1 7/1 8/1 9/1 10/1 11/1 12/1

76,752,768 total observations

Showing Flow Observations

(

Fwd Packet Retransmissions > 0

and

Fwd Congestion Window Reduced = true

or

Rev Packet Retransmissions > 0

)

and

Rev Congestion Window Reduced = true

)

Filter Flows

Flow Observations

Current scope is mslab

Current selection: Apr 26 3:42pm to Sep 18 10:54pm

Found 19,880 Flow Observations (9984ms)

Show 20

In order

Sampled

Explore Observations

|  | Timestamp ↑      | Consumer Name ↑↓ | Provider Name ↑↓ | Consumer Address ↑↓ | Provider Address ↑↓ | Consumer Port ↑↓ | Provider Port ↑↓ | Protocol ↑↓ | Consumer Resource Type ↑↓ |
|--|------------------|------------------|------------------|---------------------|---------------------|------------------|------------------|-------------|---------------------------|
|  | Apr 26 3:44:00pm | SPApp01          | SQL02            | 10.107.0.62         | 10.107.0.22         | 63725            | 1433             | TCP         | Workload                  |
|  | Apr 26 3:52:00pm | SPDC01           | SQL02            | 10.107.0.63         | 10.107.0.22         | 53499            | 1433             | TCP         | Workload                  |
|  | Apr 26 3:57:00pm | SPDC01           | SQL02            | 10.107.0.63         | 10.107.0.22         | 53499            | 1433             | TCP         | Workload                  |

Top Names contributing to the selected Flow Observations.

Consumer Names

SPApp01

SPFE01

SPDC01

SQL02

SQL01

dc02

dc01

App01

App02

web01

Provider Names

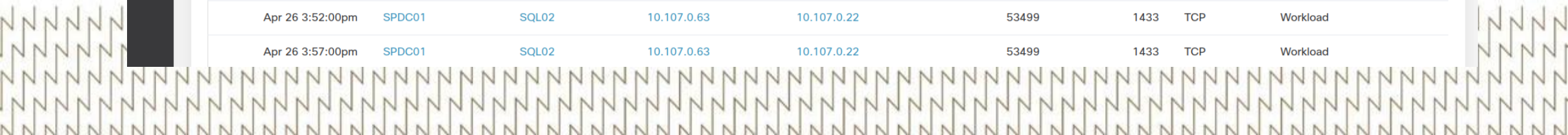
SQL02

Unknown

SPDC01

dc01

SPFE01





# Co jeszcze można ...



Cisco Secure Workload

mslab



SECURE

Your browser is not fully supported. For best results, please use [Google Chrome](#).

## Flow Search

Select time range

Dec 12 2:04am - Dec 12 8:04am



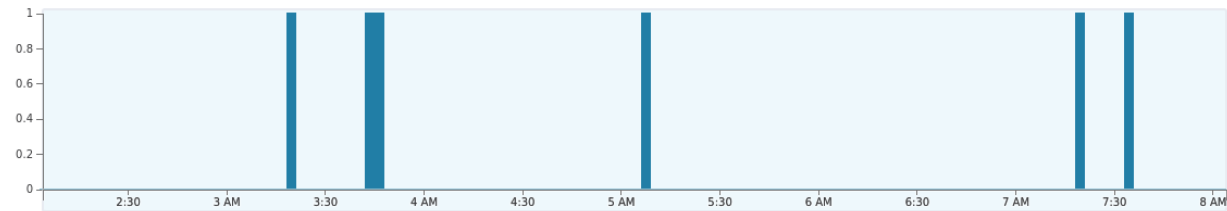
76,755,794 total observations

Showing Flow Observations

TCP Handshake (µs) > [200ms - 1.00s]

Filter Flows

Flow Observations



Current scope is mslab

Current selection: Dec 12 2:04am to Dec 12 8:04am

Found 6 Flow Observations (54ms)

Show 20

In order

Sampled

Explore Observations

Top Names contributing to the selected Flow Observations.

Consumer Names

Provider Names

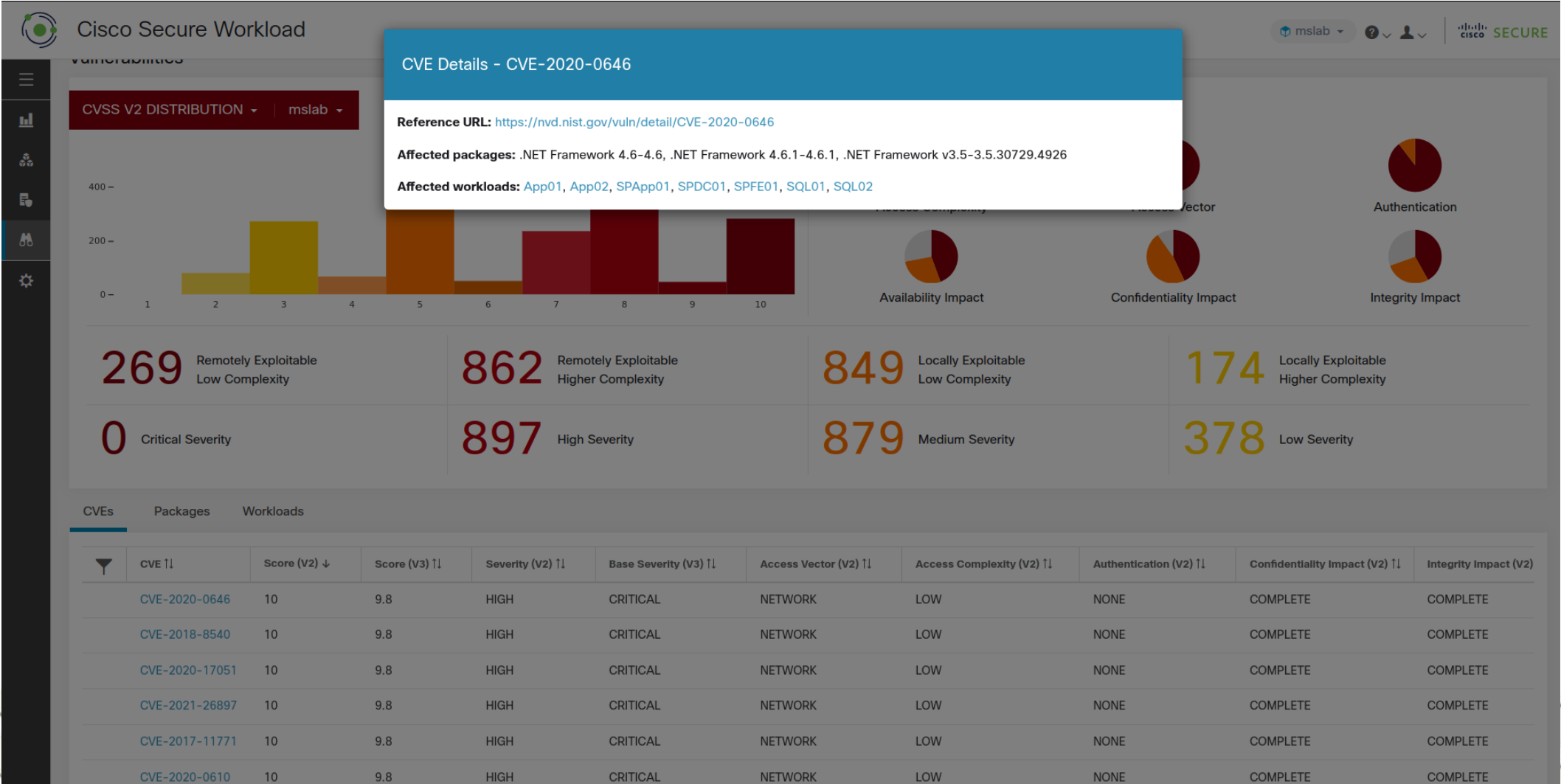
SPDC01

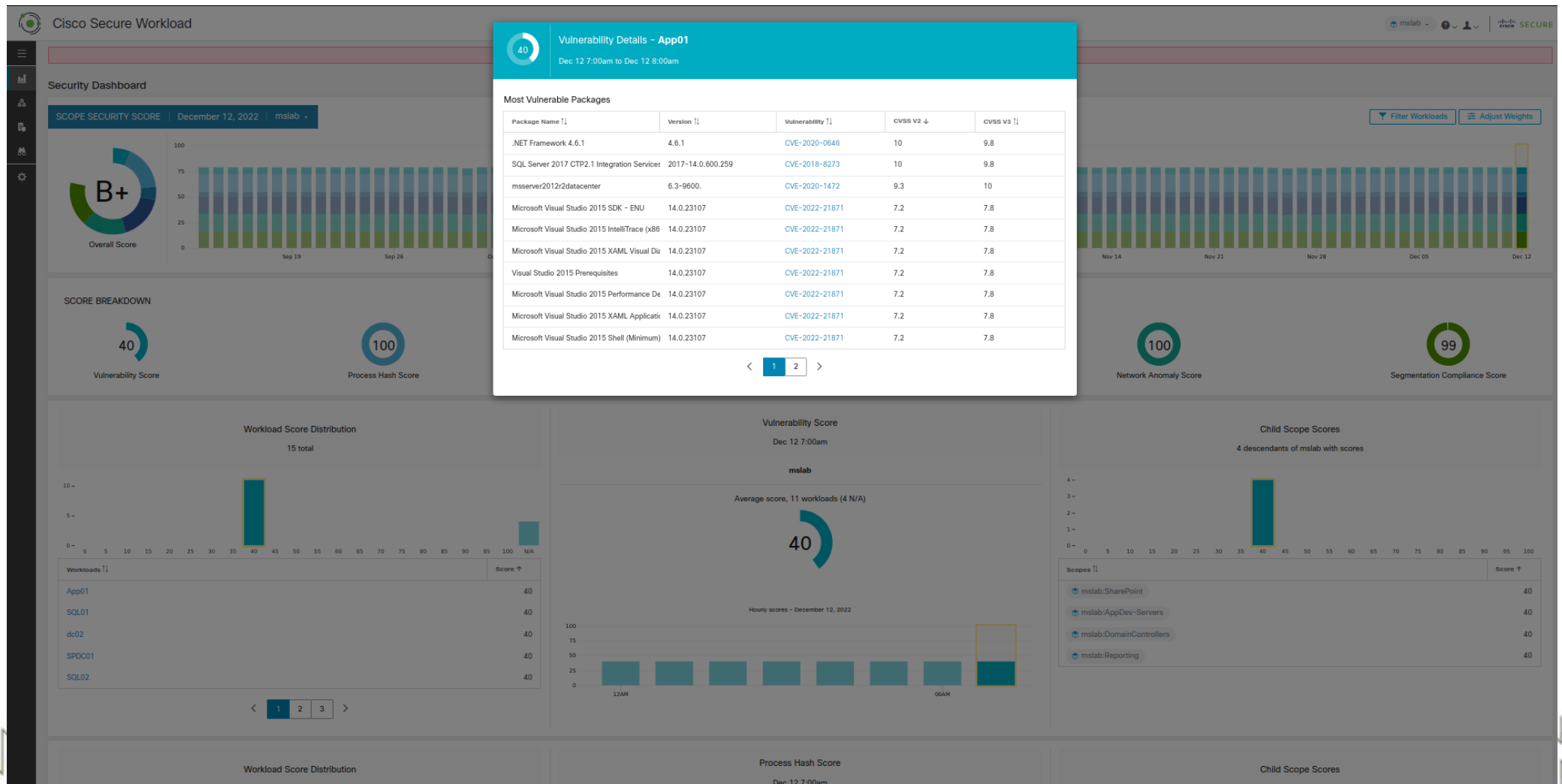
SPApp01

SPFE01

dc02

| Timestamp ↑      | Consumer Name ↑↓ | Provider Name ↑↓ | Consumer Address ↑↓ | Provider Address ↑↓ | Consumer Port ↑↓ | Provider Port ↑↓ | Protocol ↑↓ | Consumer Resource Type ↑↓ | Provider Resource Type ↑↓ | Service Name ↑↓ |
|------------------|------------------|------------------|---------------------|---------------------|------------------|------------------|-------------|---------------------------|---------------------------|-----------------|
| Dec 12 3:19:00am | SPApp01          | dc02             | 10.107.0.62         | 10.107.0.12         | 60149            | 88               | TCP         | Workload                  | Workload                  | Kerberos        |
| Dec 12 3:43:00am | SPDC01           | dc02             | 10.107.0.63         | 10.107.0.12         | 54138            | 88               | TCP         | Workload                  | Workload                  | Kerberos        |
| Dec 12 3:46:00am | SPFE01           | dc02             | 10.107.0.61         | 10.107.0.12         | 52225            | 88               | TCP         | Workload                  | Workload                  | Kerberos        |
| Dec 12 5:08:00am | SPDC01           | dc02             | 10.107.0.63         | 10.107.0.12         | 54735            | 88               | TCP         | Workload                  | Workload                  | Kerberos        |
| Dec 12 7:18:00am | SPDC01           | dc02             | 10.107.0.63         | 10.107.0.12         | 55671            | 88               | TCP         | Workload                  | Workload                  | Kerberos        |
| Dec 12 7:33:00am | SPApp01          | dc02             | 10.107.0.62         | 10.107.0.12         | 50070            | 88               | TCP         | Workload                  | Workload                  | Kerberos        |

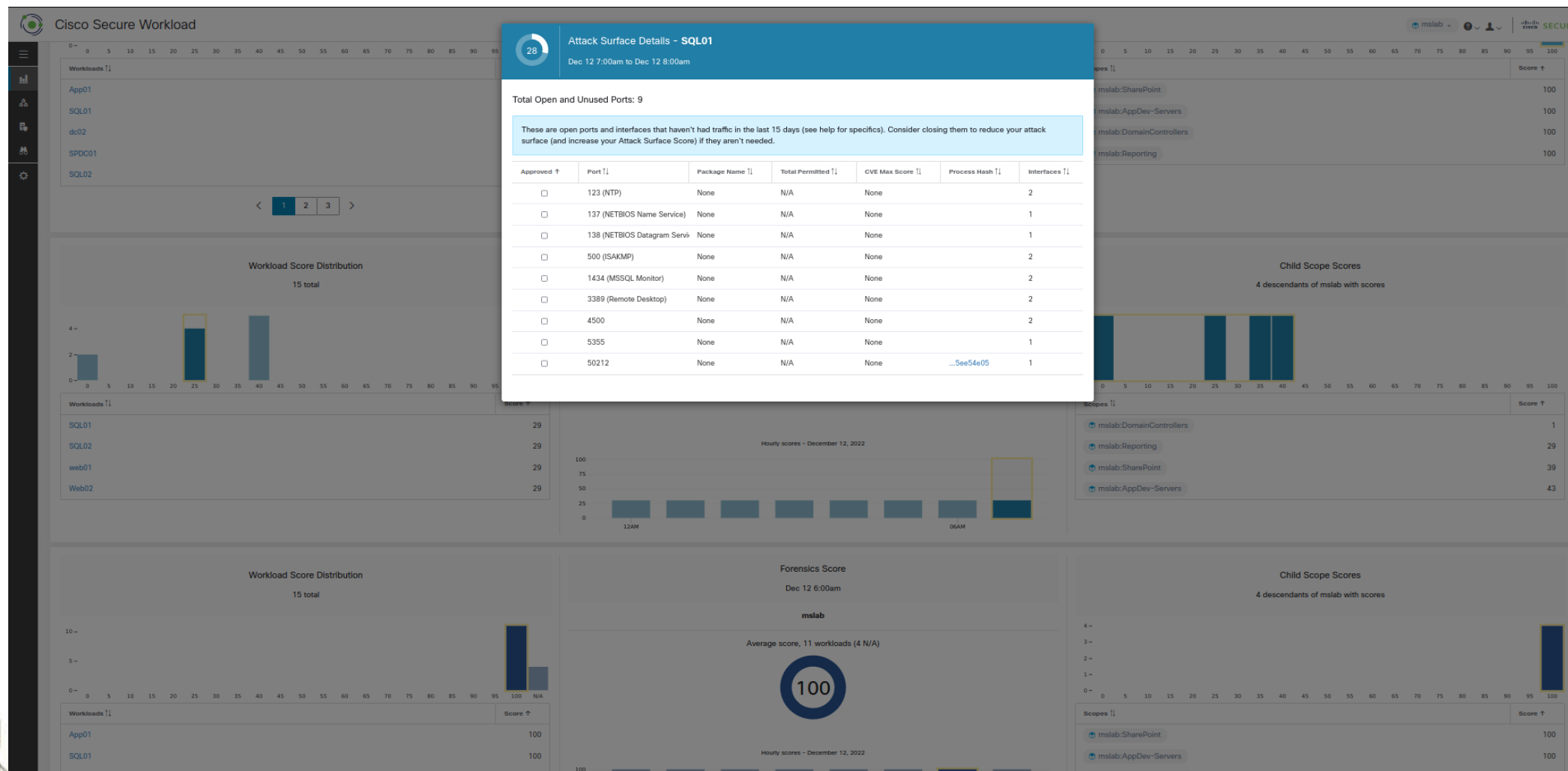








SEVENET





# Informacja o procesach



Cisco Secure Workload

mslab

SECURE

App01

Enforcement

MSServer2012R2Datacenter - Version 6.3 (OS Build 9600.)

Agent Health

Good

Enforcement Health

Good

LABELS AND SCOPES

AGENT HEALTH

LONG LIVED PROCESSES

PROCESS SNAPSHOTS

INTERFACES

PACKAGES

VULNERABILITIES

CONFIG

STATS

ENFORCEMENT HEALTH

CONCRETE POLICIES

CONTAINER POLICIES

NETWORK ANOMALIES

FILE HASHES

Long Lived Processes

Enter attributes... Filter

Displaying 23 of 23

| Process Command Line                   | User Name           | PID  | Parent PID | Libraries Count | Last Exec Content Change       | Uptime (Seconds) | Process Binary Hash                                            |
|----------------------------------------|---------------------|------|------------|-----------------|--------------------------------|------------------|----------------------------------------------------------------|
| taskeng.exe                            | NT AUTHORITY\SYSTEM | 1956 | 804        | 27              | Nov 21 2014 09:07:03 am (CET)  | 0d-0h:5m:14s     | 425a1a21a4dbc212c3c3db5f8fecdd6235e7e7e2f2fce3affe3f9f80aa24a5 |
| C:\Program Files (x86)\Google\Updat... | NT AUTHORITY\SYSTEM | 2692 | 1988       | 31              | Aug 30 2022 03:03:28 am (CEST) | 12d-11h:55m:50s  | c94dcb40543cb405474597c7e7c9d8ef558b1422797752625db9ca4faf5    |
| C:\Program Files (x86)\Google\Updat... | NT AUTHORITY\SYSTEM | 2100 | 1988       | 26              | Aug 30 2022 03:03:28 am (CEST) | 12d-11h:55m:50s  | 5df635fd14558c0a25ceecd2ad51fbc0d129a8fe681d36ecc9e7254ae0e0   |
| C:\Windows\system32\conhost.exe        | NT AUTHORITY\SYSTEM | 2628 | 2084       | 11              | Nov 21 2014 09:08:27 am (CET)  | 15d-8h:43m:14s   | 6bd1f5ab9250206ab3836529299055e272ecaa35a72cbd0230cb20ff1cc    |
| C:\Program Files\Cisco Tetration\Te... | NT AUTHORITY\SYSTEM | 2084 | 2680       | 37              | Oct 25 2021 05:29:18 pm (CEST) | 15d-8h:43m:14s   | bf94440e74b57a5df49be5c01ca201c0aa2f8da1bbdbdfeff72d3c0c65ee5  |
| TetEnfC.exe conf/enforcer.cfg          | NT AUTHORITY\SYSTEM | 524  | 2072       | 20              | Oct 25 2021 05:30:54 pm (CEST) | 15d-8h:52m:36s   | 1ae9ec339564b38d9a1165fe84c45d0951c100b5f2d8df2c9145a6a9452    |
| C:\Windows\system32\conhost.exe        | NT AUTHORITY\SYSTEM | 1136 | 2072       | 11              | Nov 21 2014 09:08:27 am (CET)  | 15d-8h:52m:36s   | 6bd1f5ab9250206ab3836529299055e272ecaa35a72cbd0230cb20ff1cc    |
| C:\Program Files\Cisco Tetration\Te... | NT AUTHORITY\SYSTEM | 2072 | 3068       | 31              | Oct 25 2021 05:30:54 pm (CEST) | 15d-8h:52m:36s   | fca6d1d5d6c11a27cce9e216aee53765113a949ce6819ccf069766d7fe6f   |
|                                        | NT AUTHORITY\SYSTEM | 3068 | 488        | 0               | Oct 25 2021 05:28:16 pm (CEST) | 15d-8h:52m:36s   | b4e2684808942902273fd80b85be01ec8ac225150b81350d7446e35ae8     |
| C:\Windows\system32\conhost.exe        | NT AUTHORITY\SYSTEM | 2576 | 2752       | 11              | Nov 21 2014 09:08:27 am (CET)  | 15d-8h:52m:36s   | 6bd1f5ab9250206ab3836529299055e272ecaa35a72cbd0230cb20ff1cc    |
| C:\Windows\system32\conhost.exe        | NT AUTHORITY\SYSTEM | 2208 | 388        | 11              | Nov 21 2014 09:08:27 am (CET)  | 15d-8h:52m:36s   | 6bd1f5ab9250206ab3836529299055e272ecaa35a72cbd0230cb20ff1cc    |
| C:\Program Files\Cisco Tetration\te... | NT AUTHORITY\SYSTEM | 2752 | 2680       | 49              | Oct 25 2021 05:28:02 pm (CEST) | 15d-8h:52m:36s   | 55dbae051bd2b918242683a714e66a109c0737590244e026dc8f04c477     |
| C:\Program Files\Cisco Tetration\Te... | NT AUTHORITY\SYSTEM | 388  | 2680       | 11              | Oct 25 2021 05:28:12 pm (CEST) | 15d-8h:52m:36s   | ae1263213c5948ce58bad17dc059224e01f213d1e17b55c9d84e10e5a      |
| C:\Program Files\Cisco Tetration\Te... | NT AUTHORITY\SYSTEM | 2680 | 488        | 10              | Oct 25 2021 05:28:16 pm (CEST) | 15d-8h:52m:36s   | b4e2684808942902273fd80b85be01ec8ac225150b81350d7446e35ae8     |
| C:\Program Files\VMware\VMware Tool... | NT AUTHORITY\SYSTEM | 1376 | 488        | 43              | Sep 20 2017 09:23:52 am (CEST) | 1d-12h:35m:50s   | 45fd4d9a021339199d4757046bf4f8717e2eb5af2c88ac90d263f42171f    |
| C:\Program Files\VMware\VMware Tool... | NT AUTHORITY\SYSTEM | 1356 | 488        | 95              | Sep 20 2017 09:44:30 am (CEST) | 1d-12h:35m:51s   | e43e1920d4159960940c3c6b4f35970d7d5f0db83b875bf1545f9df7cde    |
| C:\Program Files\VMware\VMware Tool... | NT AUTHORITY\SYSTEM | 1328 | 488        | 47              | Sep 20 2017 09:06:16 pm (CEST) | 1d-12h:35m:51s   | 1843e1fd4e1a72889898925f9e9d4f1710f14f15f373a733a733a733a      |

May 20 6:37:00pm

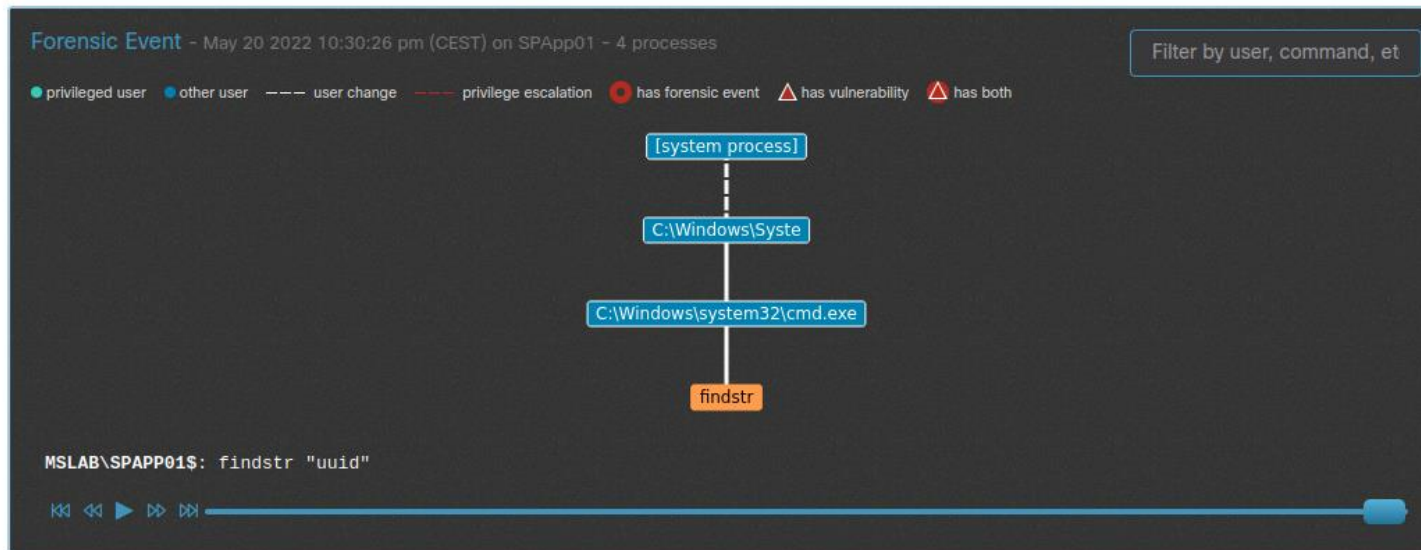
Tetration - Anomalous Unseen Command

findstr

SPApp01

Unseen Command

HIGH



findstr

### Unseen Command

**Rule** Tetration - Anomalous Unseen Command

**Bin attr ctime** 0

**Bin attr mtime** 0

**Bin attr size** 0

**Bin exec path** C:\Windows\System32\findstr.exe

**Cmdline** findstr "uuid"

**Cmdline anomaly info score** N/A

**Event time usec** 1653078627174036700 - May 20 2022 10:30:27 pm (CEST)

**Parent cmdline** C:\Windows\system32\cmd.exe /c type sensor\_id | findstr "uuid"

**Parent exepath** C:\Windows\System32\cmd.exe

**Parent uptime** 0

**Parent username** MSLAB\SPAPP01\$

**Sensor uptime** 4337618755319

**Severity** HIGH

**Process ID** 4452

**Parent Process ID** 3524

**User** MSLAB\SPAPP01\$

**Execution path** C:\Windows\System32\findstr.exe

**Start time** May 20 2022 10:30:26 pm (CEST) on SPApp01

**Full command**

findstr "uuid"





# Agent, tak Agent ale czy na pewno?



Cisco Secure Workload

sevenet.pl



SECURE

Your browser is not fully supported. For best results, please use Google Chrome.

Labeling and grouping your workloads is essential to the power of Secure Workload. We can help you get started. [Run the wizard now.](#)

## Software Agents Configure

[Installer](#) [Upgrade](#) [Convert to Enforcement Agent](#) [Configure](#) [Monitor](#) [Distribution](#) [Agent List](#)

### Agent Config Profiles

Create Profile

| Name    | Config                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Actions |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| Default | <div><div>Enforcement</div><div><div>✓ Enforcement</div><div>✓ Windows Enforcement Mode - WFP</div><div>✗ Preserve Rules</div><div>✓ Allow Broadcast</div><div>✓ Allow Multicast</div><div>✓ Allow Link Local Addresses</div><div>✓ CPU Quota Mode - Adjusted (3%)</div><div>✓ Memory Quota Limit - 512MB</div></div><div><div>Flow Visibility</div><div><div>✓ Flow Analysis Fidelity - Detailed</div><div>✓ Data Plane</div><div>✓ Auto-Upgrade</div><div>✓ PID Lookup</div><div>✓ CPU Quota Mode - Adjusted (3%)</div><div>✓ Memory Quota Limit - 512MB</div><div>✗ Cleanup Period</div></div><div><div>Process Visibility and Forensics</div><div><div>✓ Forensics</div><div>✓ Process Visibility</div><div>✓ Package Visibility</div><div>✗ Meltdown Exploit Detection</div><div>✓ CPU Quota Mode - Adjusted (3%)</div><div>✓ Memory Quota Limit - 256MB</div></div></div></div></div> |         |

[View Deleted Agent Config Profiles](#)

### Agent Config Intents

Create Intent

Apply profile **Default** to filter **Everything**

[View Deleted Agent Config Intents](#)





# DZIĘKUJĘ ZA UWAGĘ

Kontakt:

[marcin\\_kornafel@sevenet.pl](mailto:marcin_kornafel@sevenet.pl)

