SEVENET

cisco Partner
Gold Certified

Zero Trust w środowiskach aplikacyjnych

Marcin Kornafel
Sevenet S.A.

Tomasz Jedynak
Cisco Systems

Zero Trust

SEVENET

Zaufanie

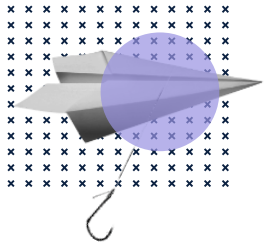
Wymuszenie

Ciągła weryfikacja

Podejście Zero Trust

SEVENET

Ograniczenie ryzyku

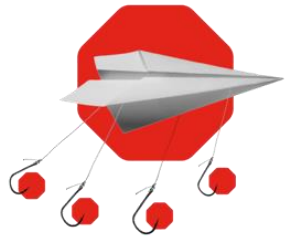


Zmniejszenie ryzyka naruszenia bezpieczeństwa

Zyskaj widoczność

Identyfikacja ryzyka i symptomów naruszenia bezpieczeństwa

Redukcja powierzchni ataku



Zatrzymanie włamania i ograniczenie lateral movement

Filozofia Zero Trust

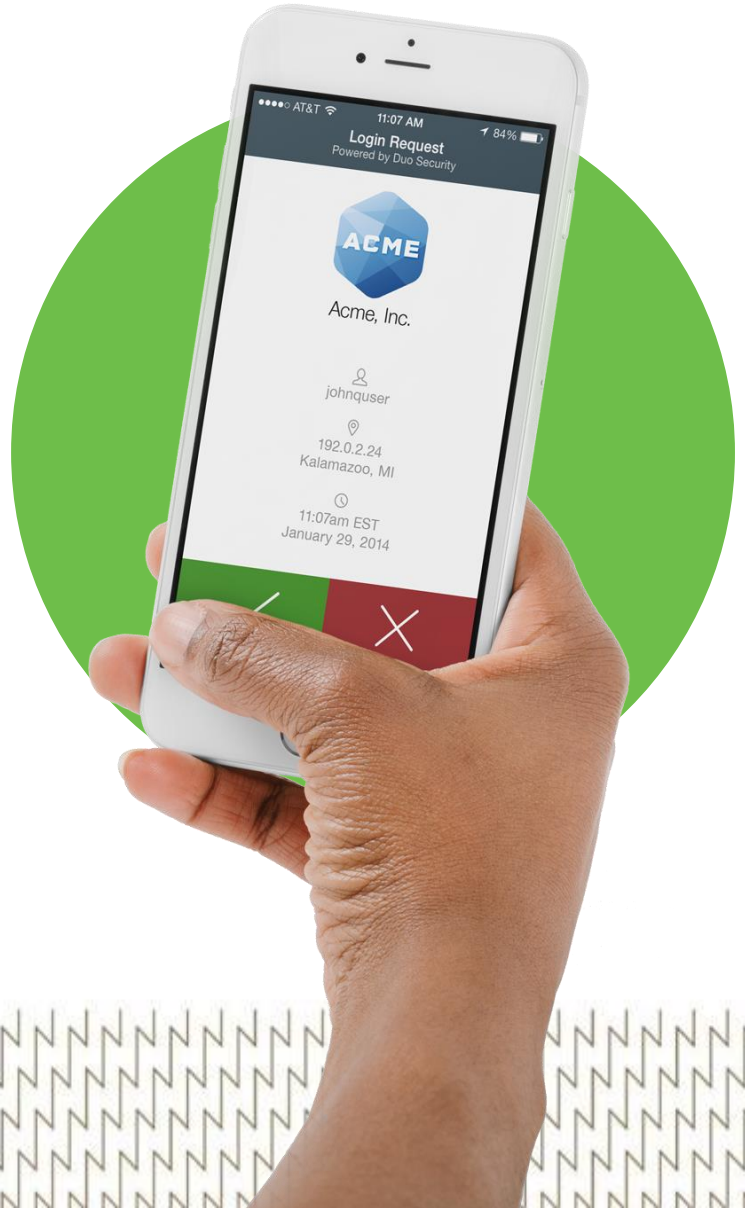
Włącz kontrolę opartą na polityce
dla każdego żądania dostępu w środowisku korporacyjnym

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

Segmentacja sieci
i zasobów roboczych poprzez egzekwowanie odpowiedniej polityki

Uwierzytelnienie użytkownika

SEVENET



99%

Eksploitowanych podatności jest znana przez organizacje przez przynajmniej rok

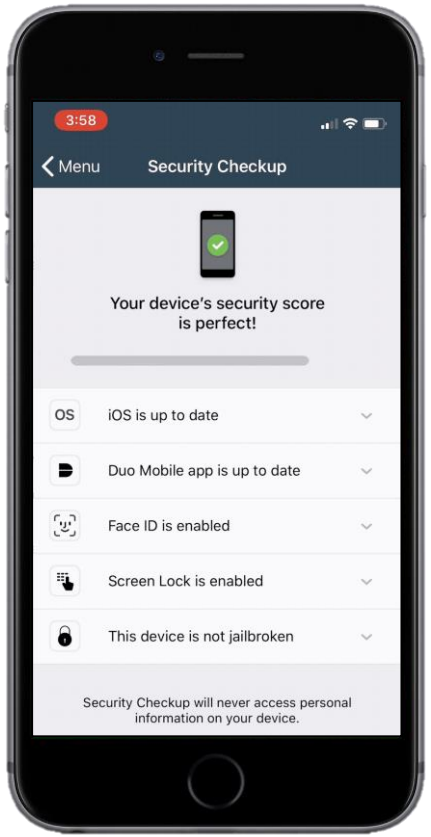
Source: Gartner, Dale Gardner, 2018 Security Summit

81%

Włamań wykorzystuje skradzione lub złamane hasła

Source: Verizon 2018 Data Breach Investigations Report

Weryfikacja tożsamości



Wearables

Push

Phone Call

Soft Token

Biometrics

U2F

Hardware Tokens

SMS

Zabezpiecz dostęp do dowolnej aplikacji

SEVENET

Aplikacje własne

C# Java python node Ruby

Środowiska Microsoft

Forefront Windows Office 365 Microsoft Active Directory Federation Services Active Directory Outlook

Usługi Chmurowe

Active Directory Federation Services onelogin Centrify okta PingIdentity

Unix (SSH)

FreeBSD Linux redhat ubuntu

VPN

OPENVPN paloalto Array Check Point Barracuda f5 FORTINET cisco JUNIPER

Aplikacje Chmurowe

Dropbox salesforce Google Apps workday amazon web services box Office 365 Cisco webex slack

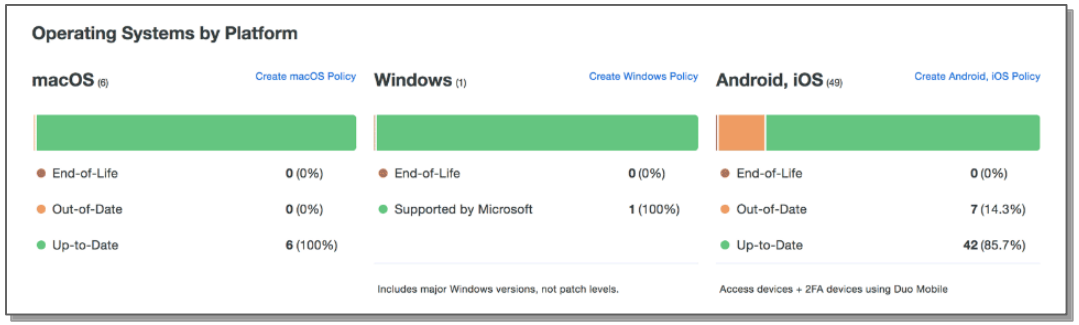
Aplikacje Web

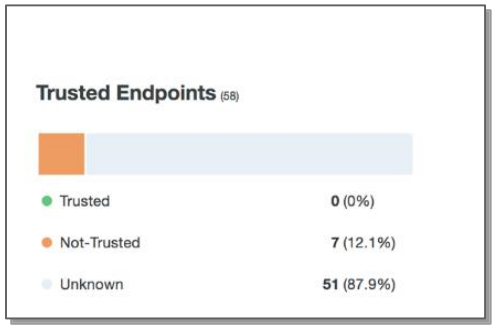
splunk> Drupal Atlassian Confluence WordPress Atlassian JIRA Shibboleth

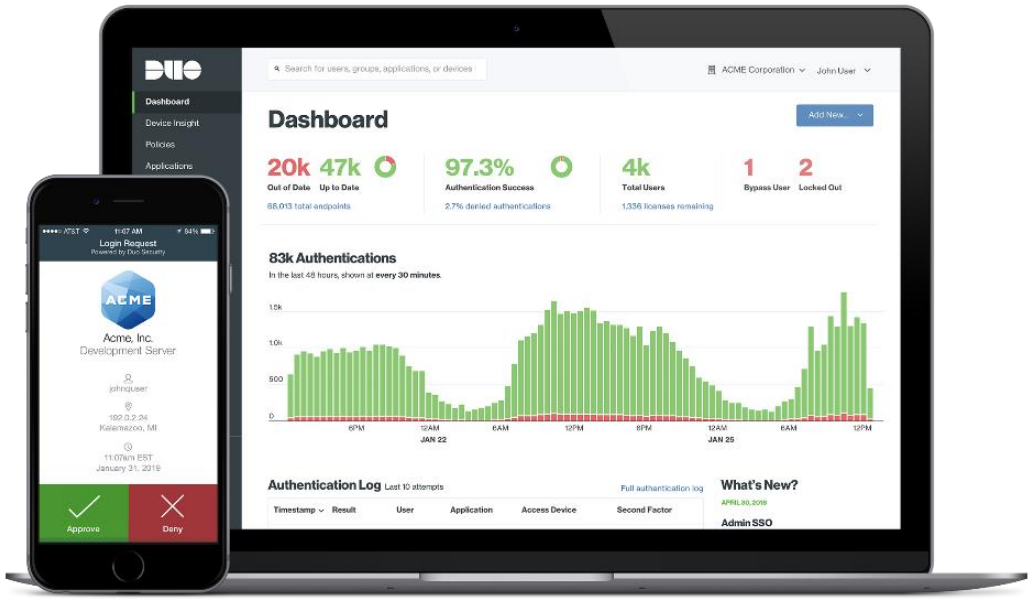
Aplikacje SAML 2.0

Google Apps amazon web services Office 365 salesforce box

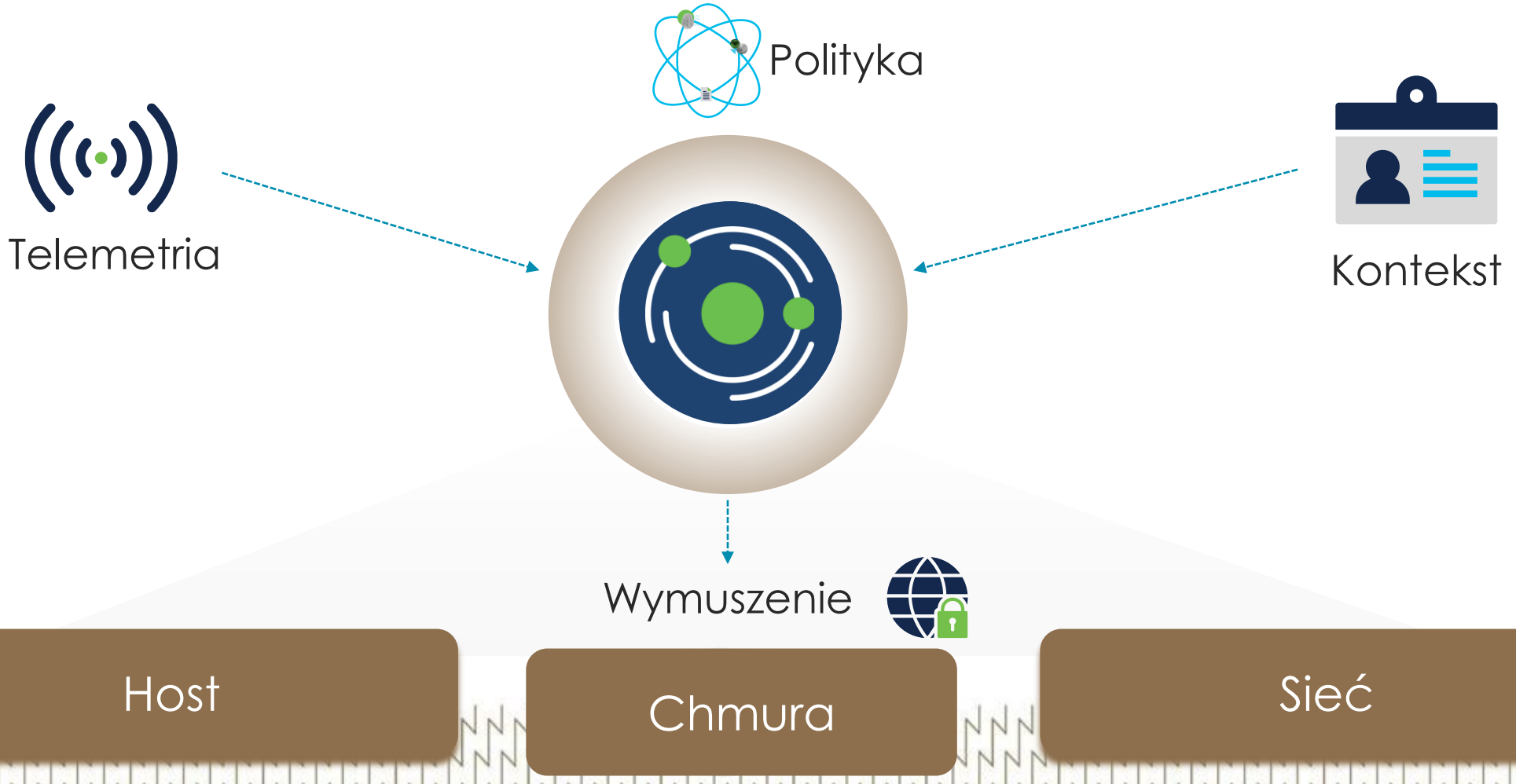
Pełna widoczność



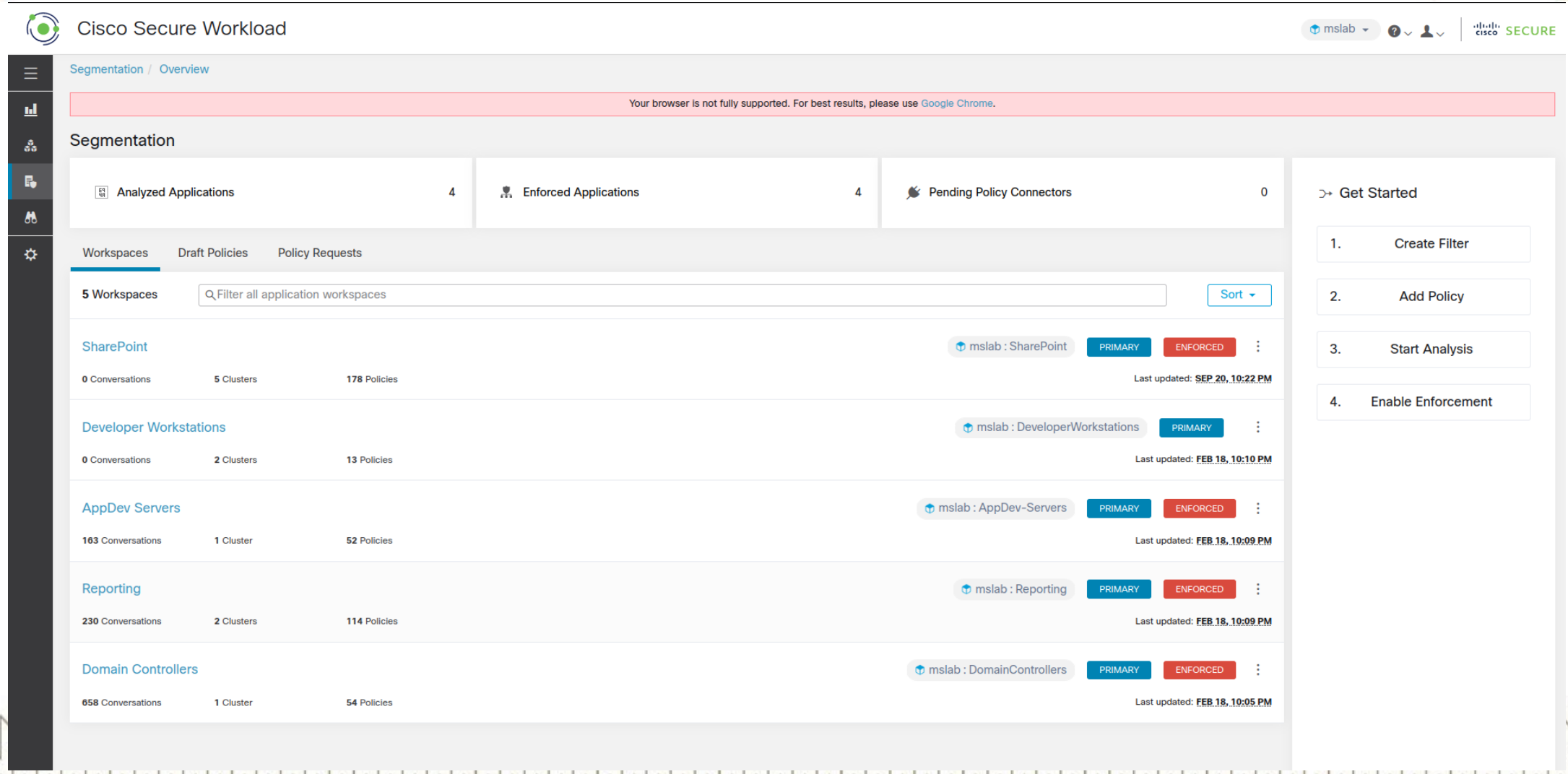




Mikrosegmentacja + Dane “Big Data”

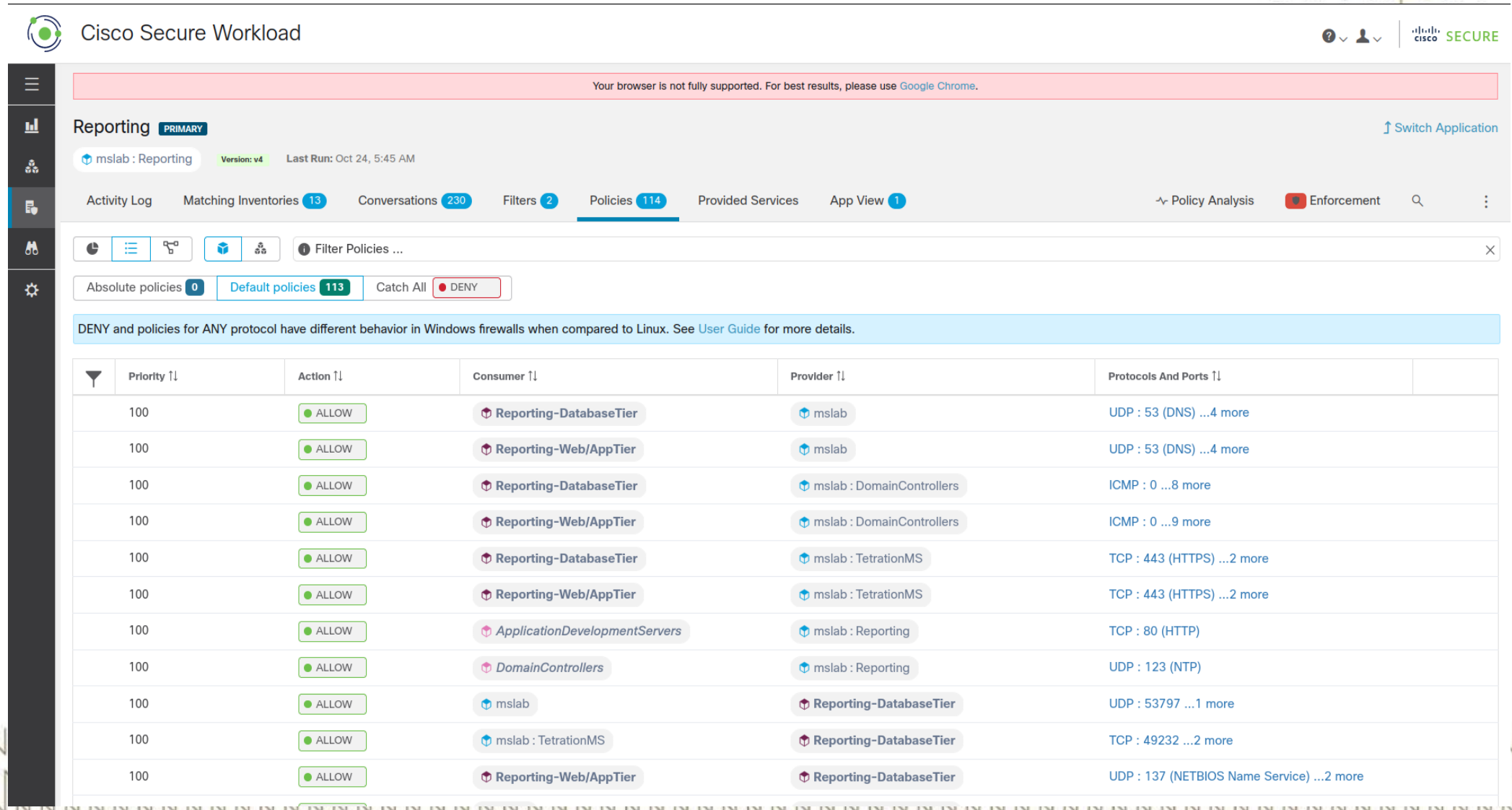

Polityka
Telemetria
Kontekst
Wymuszenie
Host
Chmura
Sieć

Mikrosegmentacja

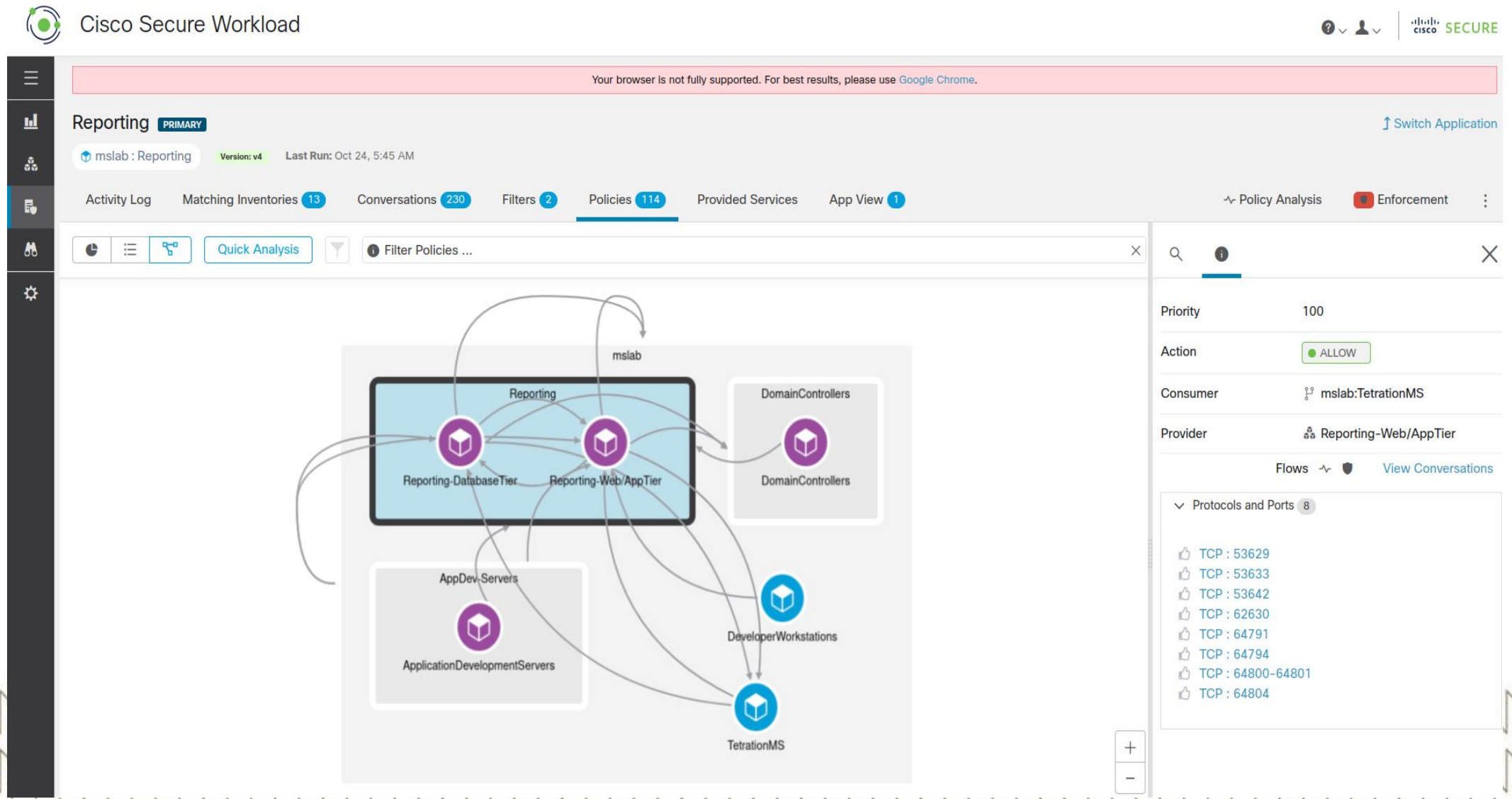


Polityki dla serwera

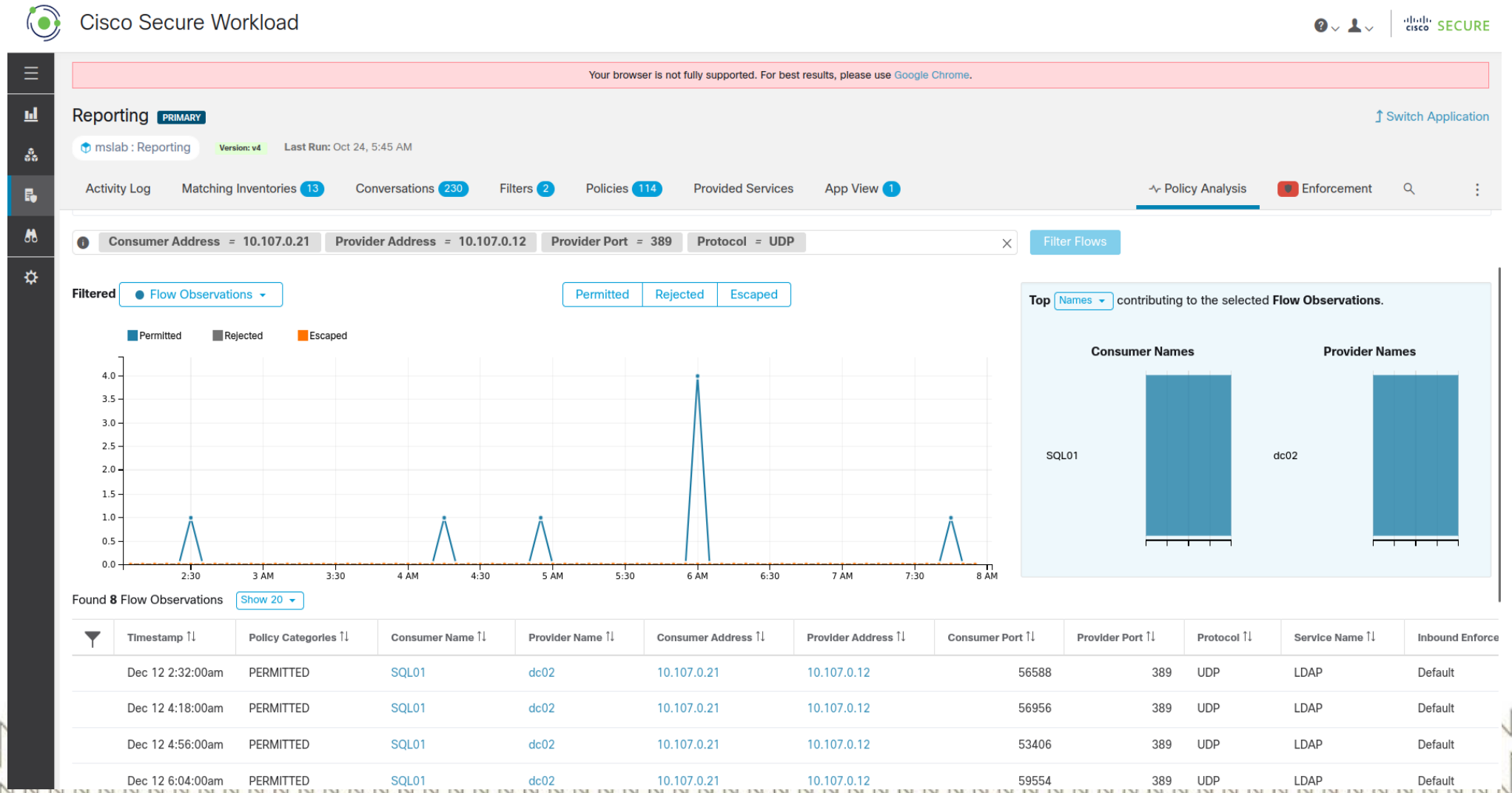
SEVENET



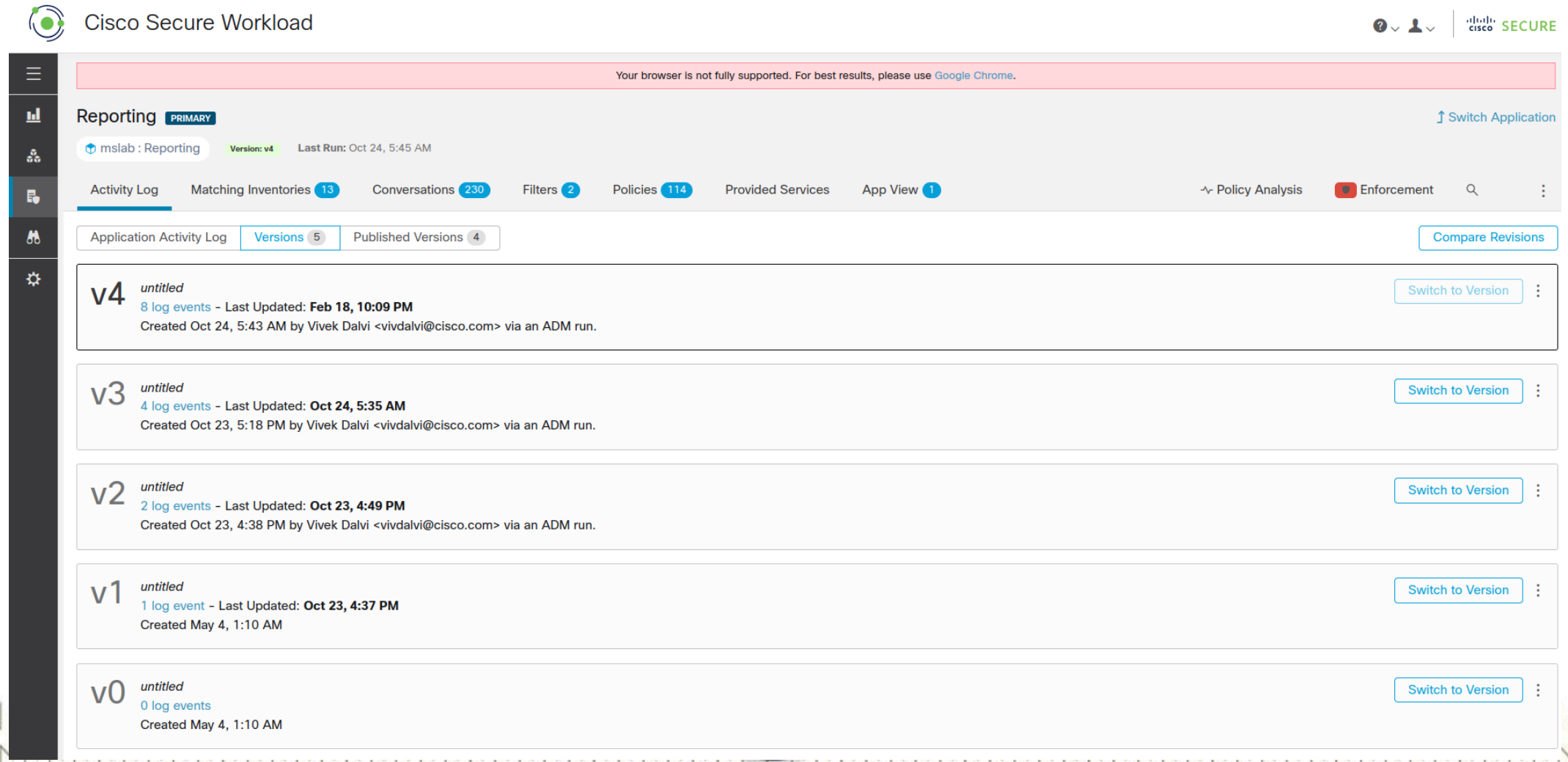
„Pajęczyna”


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
Quick Analysis
Filter Policies ...
mslab
Reporting
Reporting-DatabaseTier
Reporting-Web/AppTier
DomainControllers
DomainControllers
AppDev-Servers
ApplicationDevelopmentServers
DeveloperWorkstations
TetrationMS
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

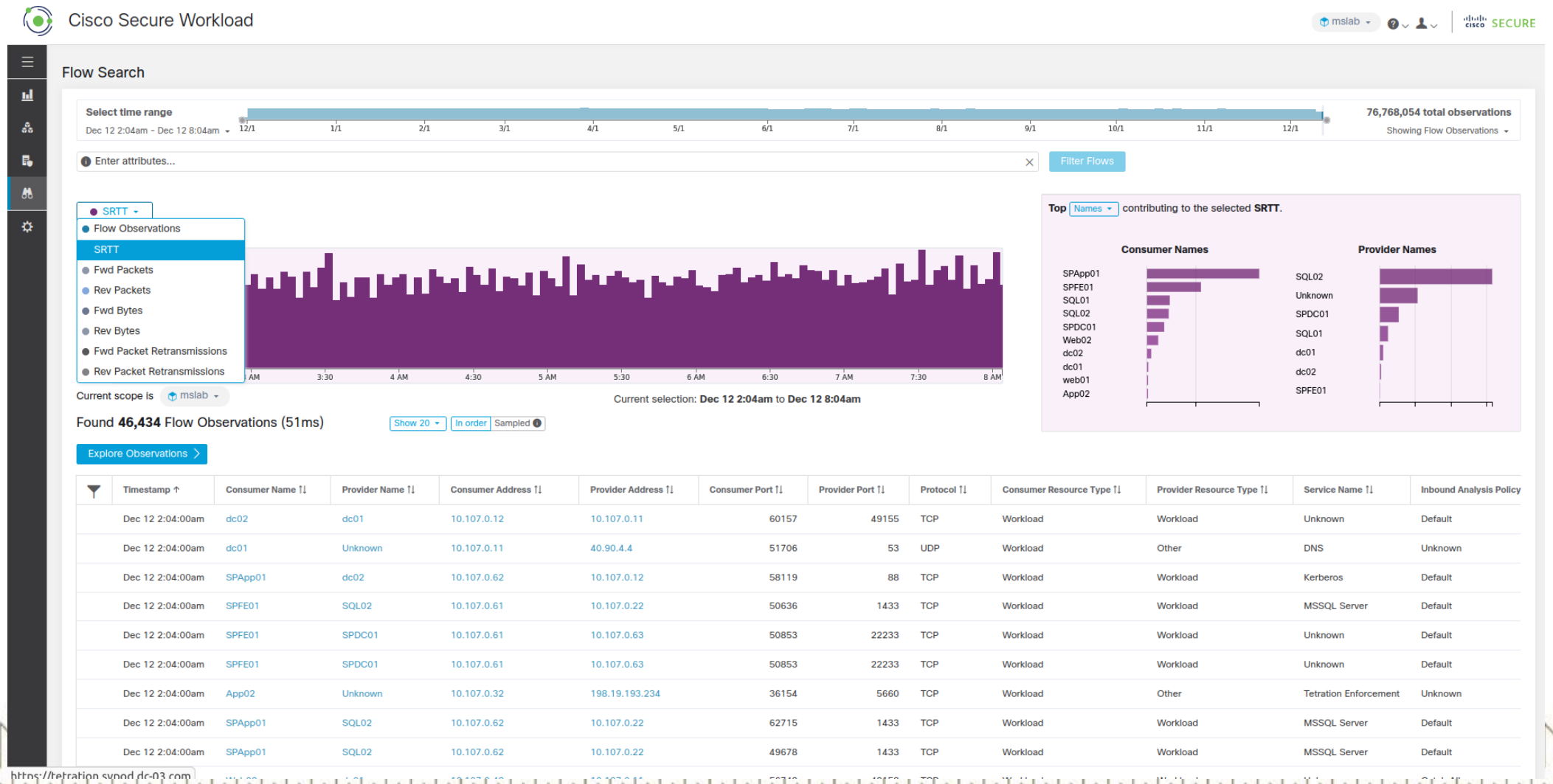
Test polityk



Wersje zmian



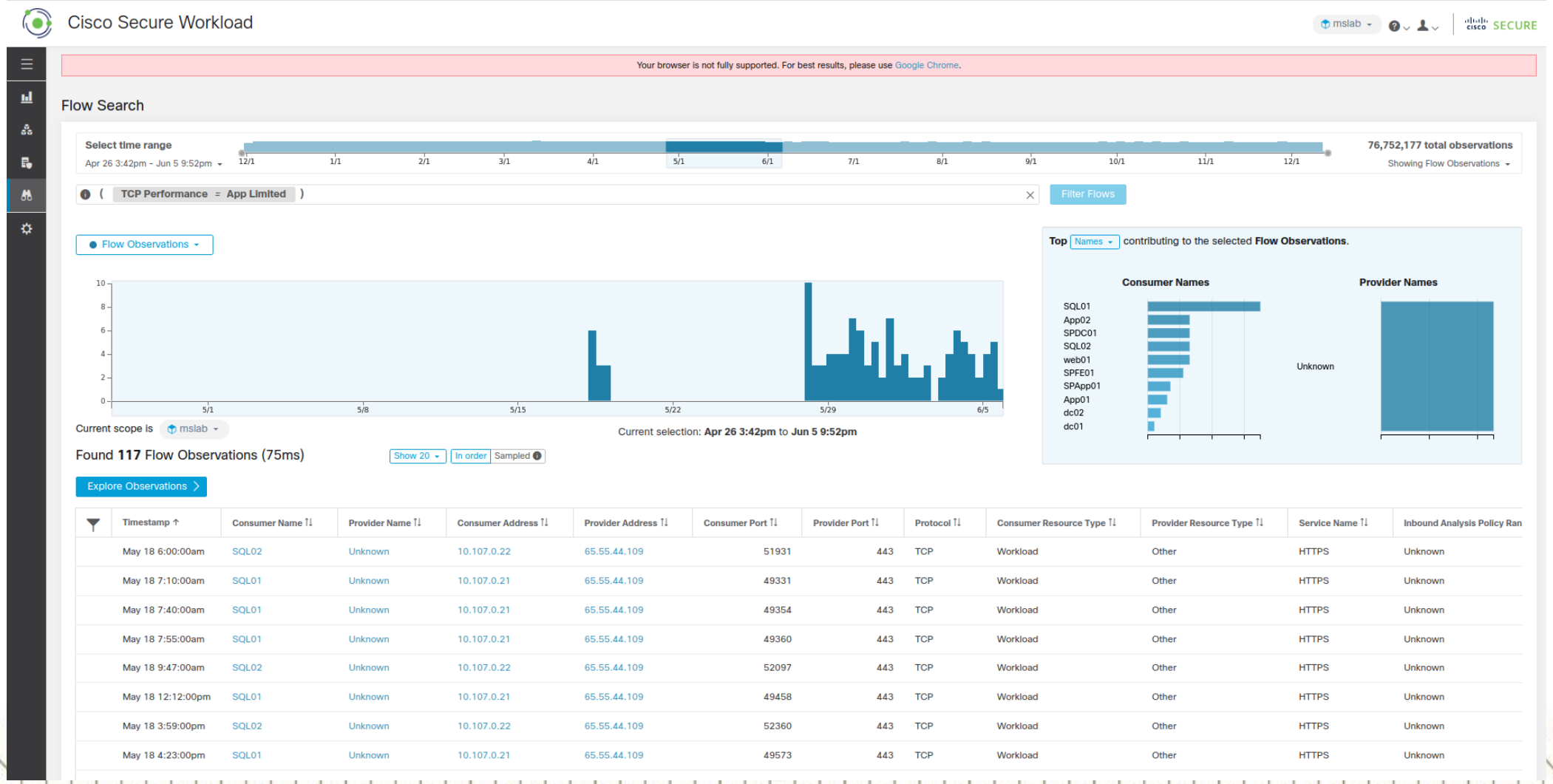
Dane „Big Data”



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
Dec 12 2:04:00am	dc02	dc01	10.107.0.12	10.107.0.11	60157	49155	TCP	Workload	Workload	Unknown	Default
Dec 12 2:04:00am	dc01	Unknown	10.107.0.11	40.90.4.4	51706	53	UDP	Workload	Other	DNS	Unknown
Dec 12 2:04:00am	SPApp01	dc02	10.107.0.62	10.107.0.12	58119	88	TCP	Workload	Workload	Kerberos	Default
Dec 12 2:04:00am	SPFE01	SQL02	10.107.0.61	10.107.0.22	50636	1433	TCP	Workload	Workload	MSSQL Server	Default
Dec 12 2:04:00am	SPFE01	SPDC01	10.107.0.61	10.107.0.63	50853	22233	TCP	Workload	Workload	Unknown	Default
Dec 12 2:04:00am	SPFE01	SPDC01	10.107.0.61	10.107.0.63	50853	22233	TCP	Workload	Workload	Unknown	Default
Dec 12 2:04:00am	App02	Unknown	10.107.0.32	198.19.193.234	36154	5660	TCP	Workload	Other	Tetration Enforcement	Unknown
Dec 12 2:04:00am	SPApp01	SQL02	10.107.0.62	10.107.0.22	62715	1433	TCP	Workload	Workload	MSSQL Server	Default
Dec 12 2:04:00am	SPApp01	SQL02	10.107.0.62	10.107.0.22	49678	1433	TCP	Workload	Workload	MSSQL Server	Default

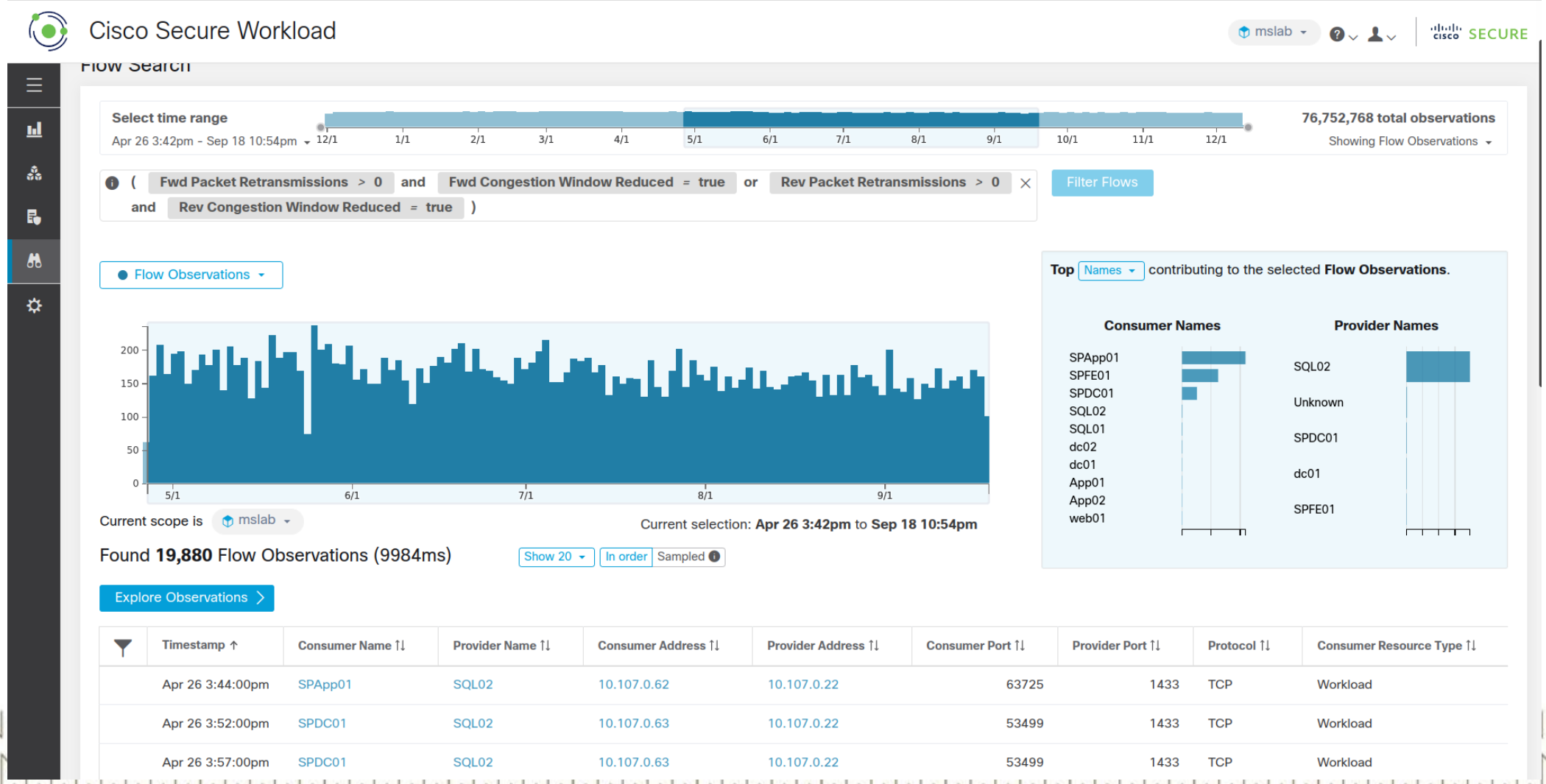
Zajrzyjmy głębiej

Opóźnienia w aplikacji



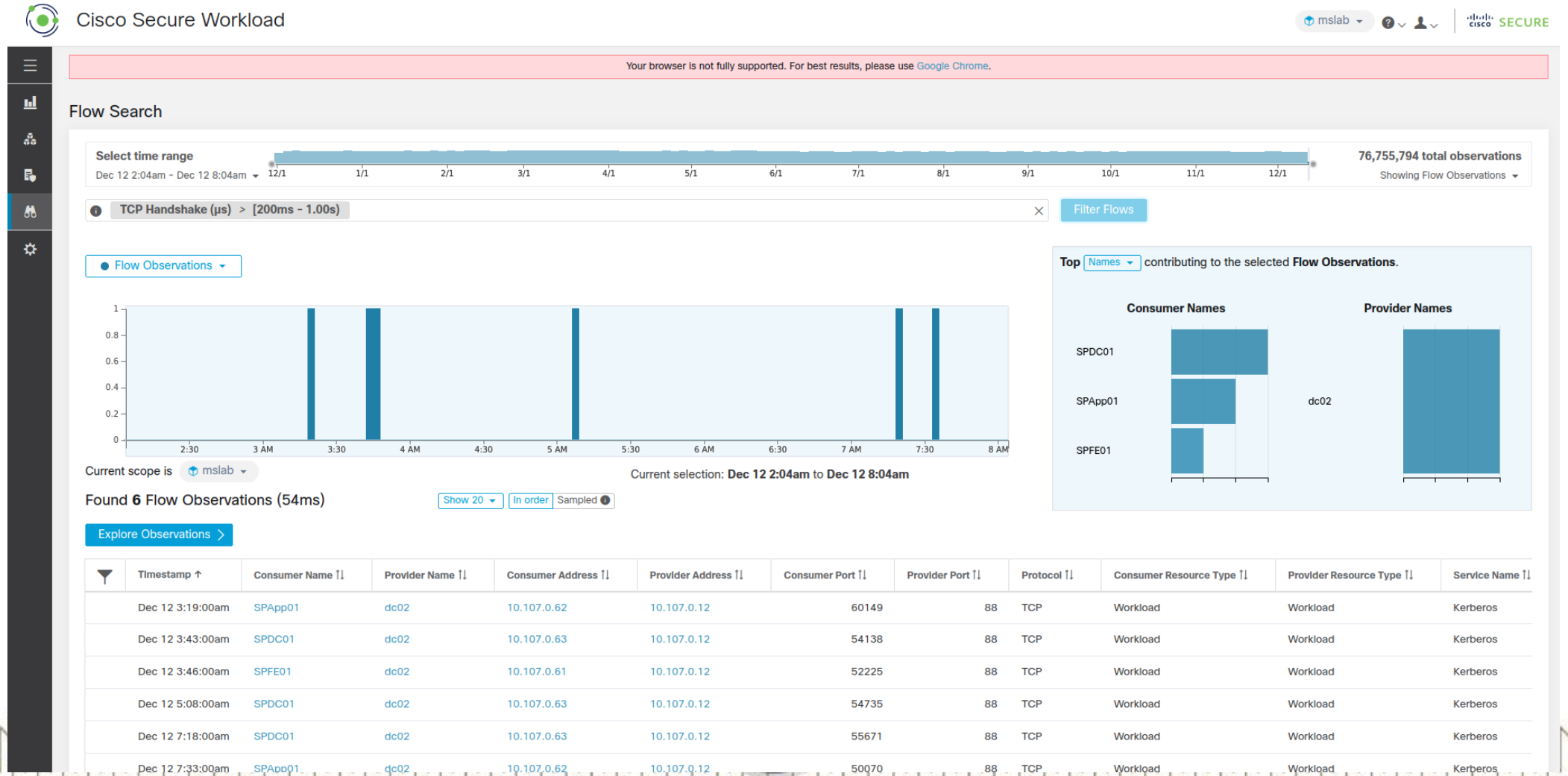
Timestamp ↑	Consumer Name	Provider Name	Consumer Address	Provider Address	Consumer Port	Provider Port	Protocol	Consumer Resource Type	Provider Resource Type	Service Name	Inbound Analysis Policy Ran
May 18 6:00:00am	SQL02	Unknown	10.107.0.22	65.55.44.109	51931	443	TCP	Workload	Other	HTTPS	Unknown
May 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

Opóźnienia na sieci



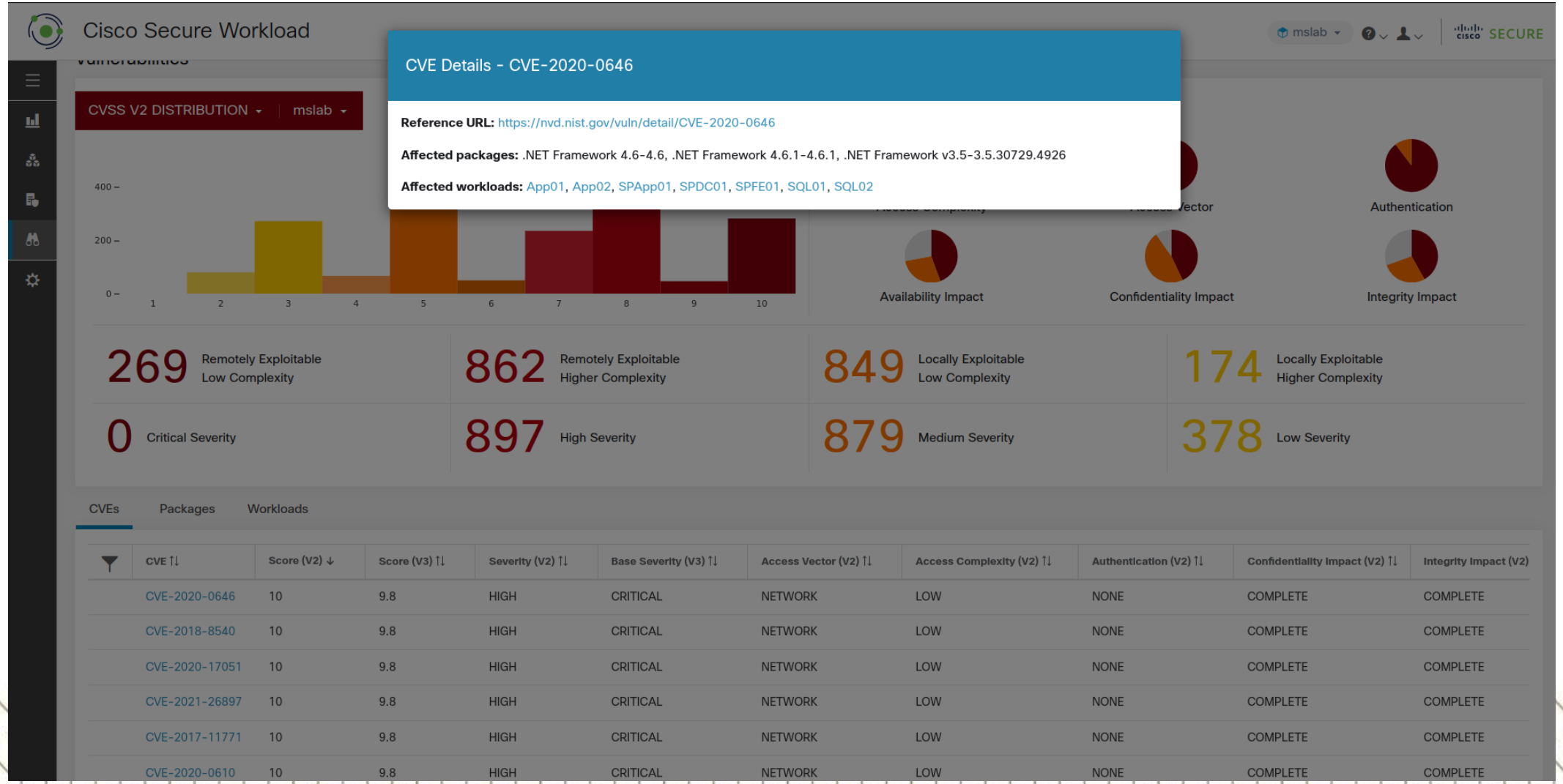
Timestamp ↑	Consumer Name	Provider Name	Consumer Address	Provider Address	Consumer Port	Provider Port	Protocol	Consumer Resource Type
Apr 26 3:44:00pm	SPApp01	SQL02	10.107.0.62	10.107.0.22	63725	1433	TCP	Workload
Apr 26 3:52:00pm	SPDC01	SQL02	10.107.0.63	10.107.0.22	53499	1433	TCP	Workload
Apr 26 3:57:00pm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

Co jeszcze można ...

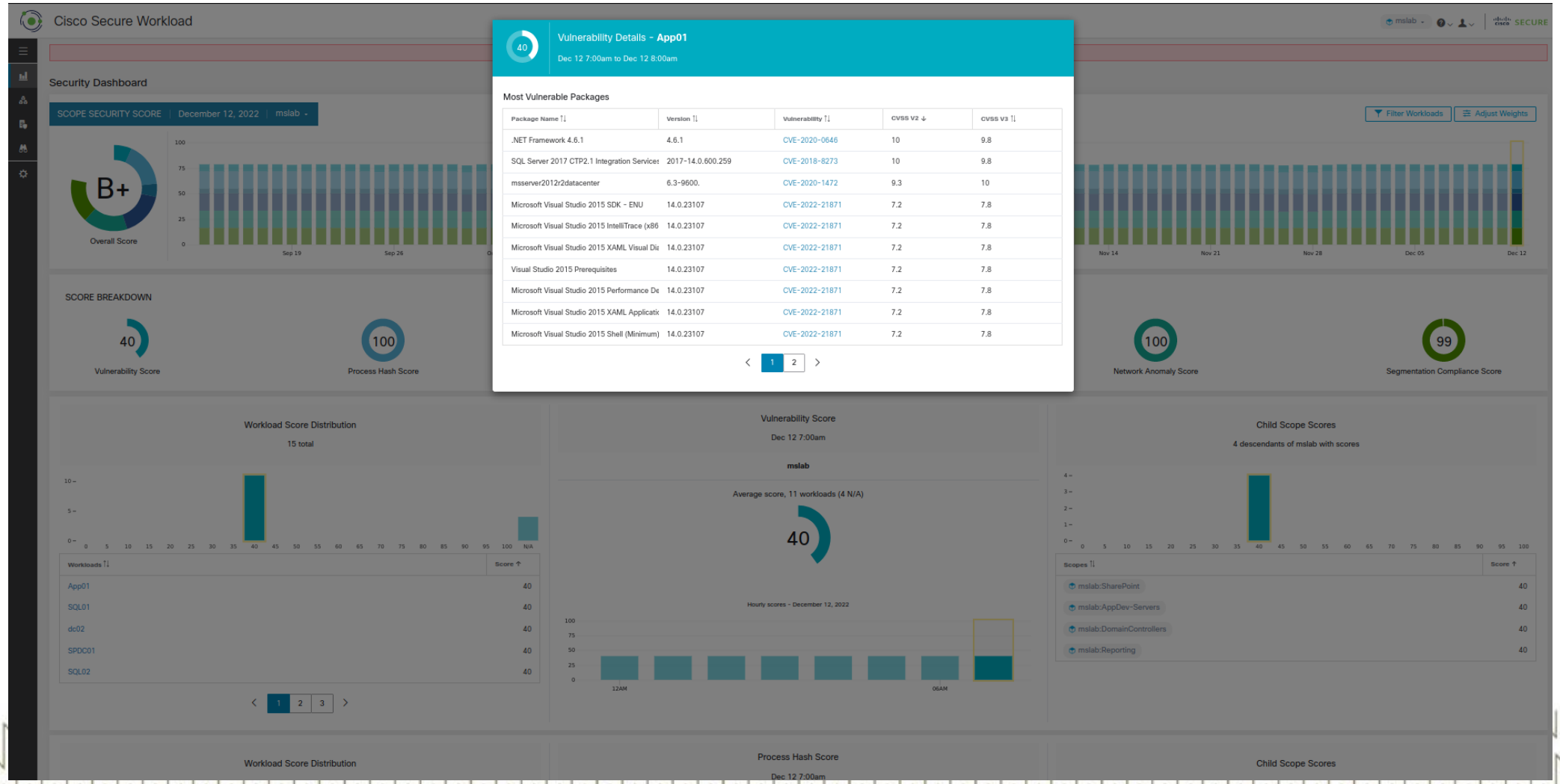


Timestamp	Consumer Name	Provider Name	Consumer Address	Provider Address	Consumer Port	Provider Port	Protocol	Consumer Resource Type	Provider Resource Type	Service Name
Dec 12 3:19:00am	SPApp01	dc02	10.107.0.62	10.107.0.12	60149	88	TCP	Workload	Workload	Kerberos
Dec 12 3:43:00am	SPDC01	dc02	10.107.0.63	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

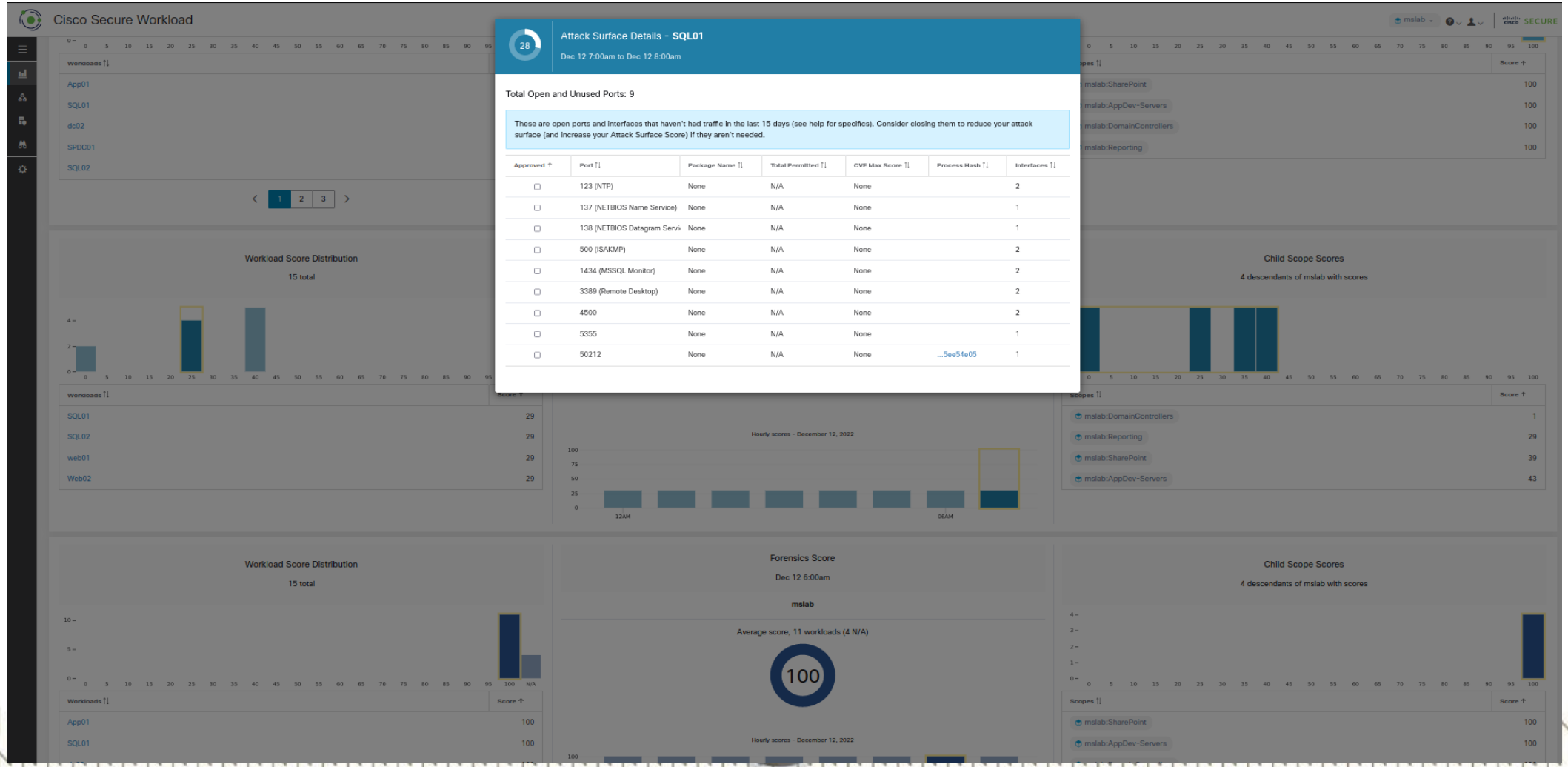
Podatność Środowiska



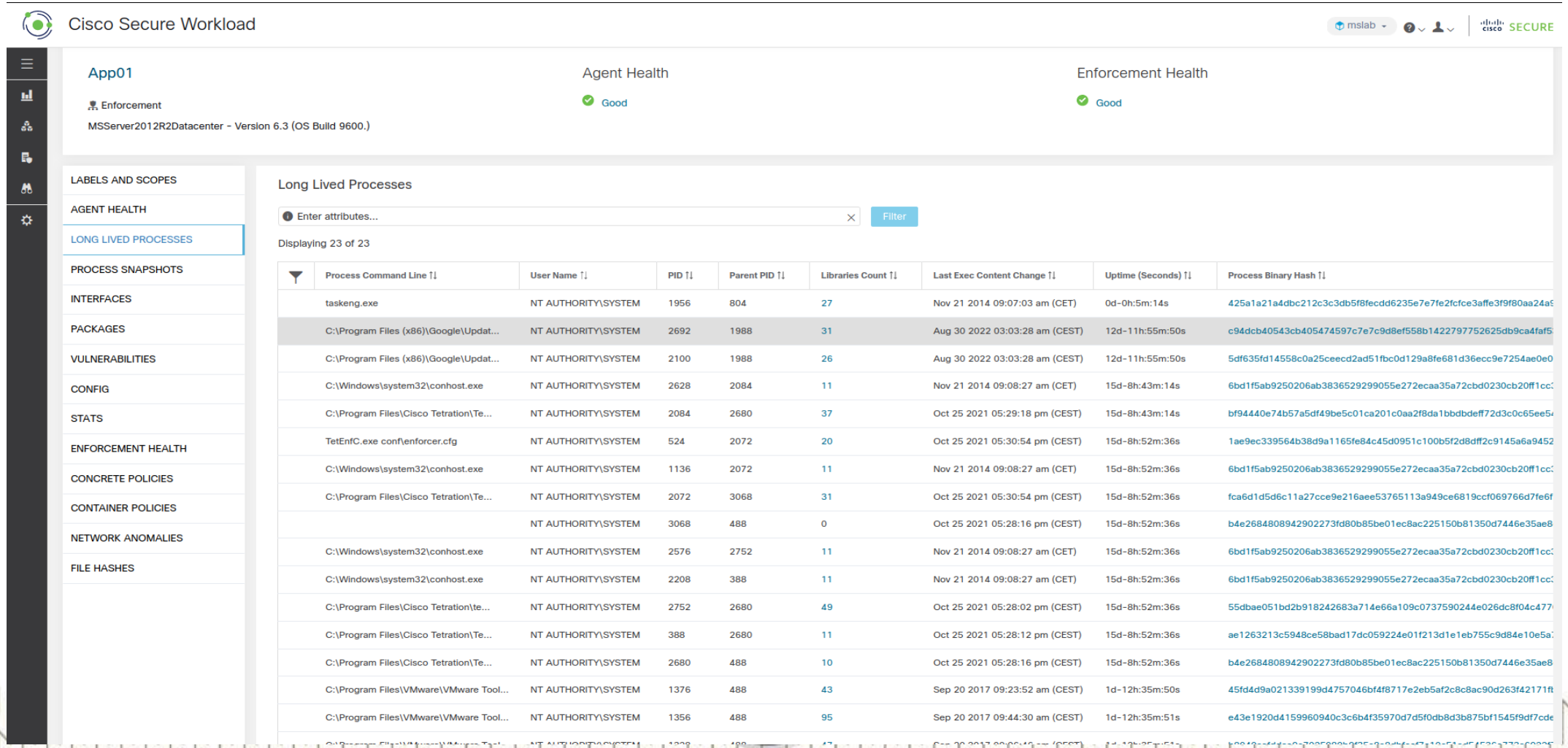
Podatności serwerów



Nie używane porty



Informacja o procesach

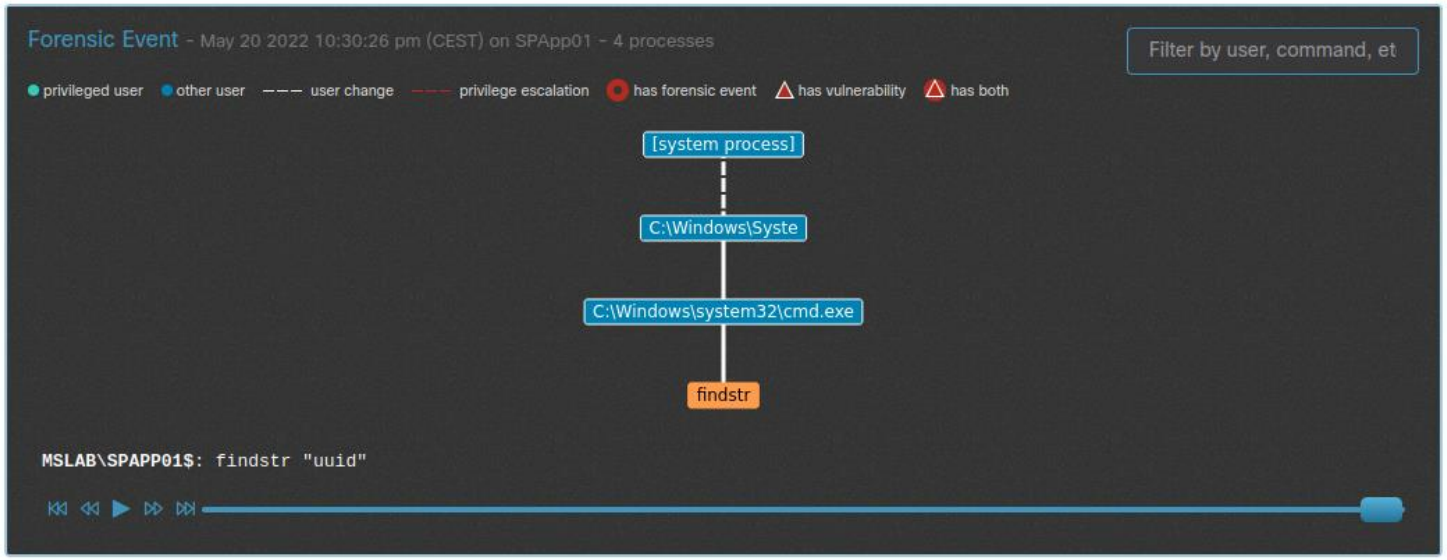


Process Command Line	User Name	PID	Parent PID	Libraries Count	Last Exec Content Change	Uptime (Seconds)	Process Binary Hash
taskeng.exe	NT AUTHORITY\SYSTEM	1956	804	27	Nov 21 2014 09:07:03 am (CET)	0d-0h:5m:14s	425a1a21a4dbc212c3c3db5f8fecdd6235e7e7fe2fcfce3affe3f9f80aa24a5
C:\Program Files (x86)\Google\Updat...	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	6bd1f5ab9250206ab3836529299055e272ecaa35a72cbd0230cb20ff1cc3
C:\Program Files\Cisco Tetration\Te...	NT AUTHORITY\SYSTEM	2084	2680	37	Oct 25 2021 05:29:18 pm (CEST)	15d-8h:43m:14s	bf94440e74b57a5df49be5c01ca201c0aa2f8da1bbdbdeff72d3c0c65ee54
TetEnfC.exe conf\enforcer.cfg	NT AUTHORITY\SYSTEM	524	2072	20	Oct 25 2021 05:30:54 pm (CEST)	15d-8h:52m:36s	1ae9ec339564b38d9a1165fe84c45d0951c100b5f2d8dff2c9145a6a9452
C:\Windows\system32\conhost.exe	NT AUTHORITY\SYSTEM	1136	2072	11	Nov 21 2014 09:08:27 am (CET)	15d-8h:52m:36s	6bd1f5ab9250206ab3836529299055e272ecaa35a72cbd0230cb20ff1cc3
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	6bd1f5ab9250206ab3836529299055e272ecaa35a72cbd0230cb20ff1cc3
C:\Windows\system32\conhost.exe	NT AUTHORITY\SYSTEM	2208	388	11	Nov 21 2014 09:08:27 am (CET)	15d-8h:52m:36s	6bd1f5ab9250206ab3836529299055e272ecaa35a72cbd0230cb20ff1cc3
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	ae1263213c5948ce58bad17dc059224e01f213d1e1eb755c9d84e10e5a7
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	45fd4d9a021339199d4757046bf4f8717e2eb5af2c8c8ac90d263f42171f
C:\Program Files\VMware\VMware Tool...	NT AUTHORITY\SYSTEM	1356	488	95	Sep 20 2017 09:44:30 am (CEST)	1d-12h:35m:51s	e43e1920d4159960940c3c6b4f35970d7d5f0db8d3b875bf1545f9df7cde

Śledzenie procesów

SEVENET

May 20 6:37:00pm	Tetration - Anomalous Unseen Command	findstr	SPApp01	Unseen Command	HIGH



O procesach cd.

SEVENET

findstr

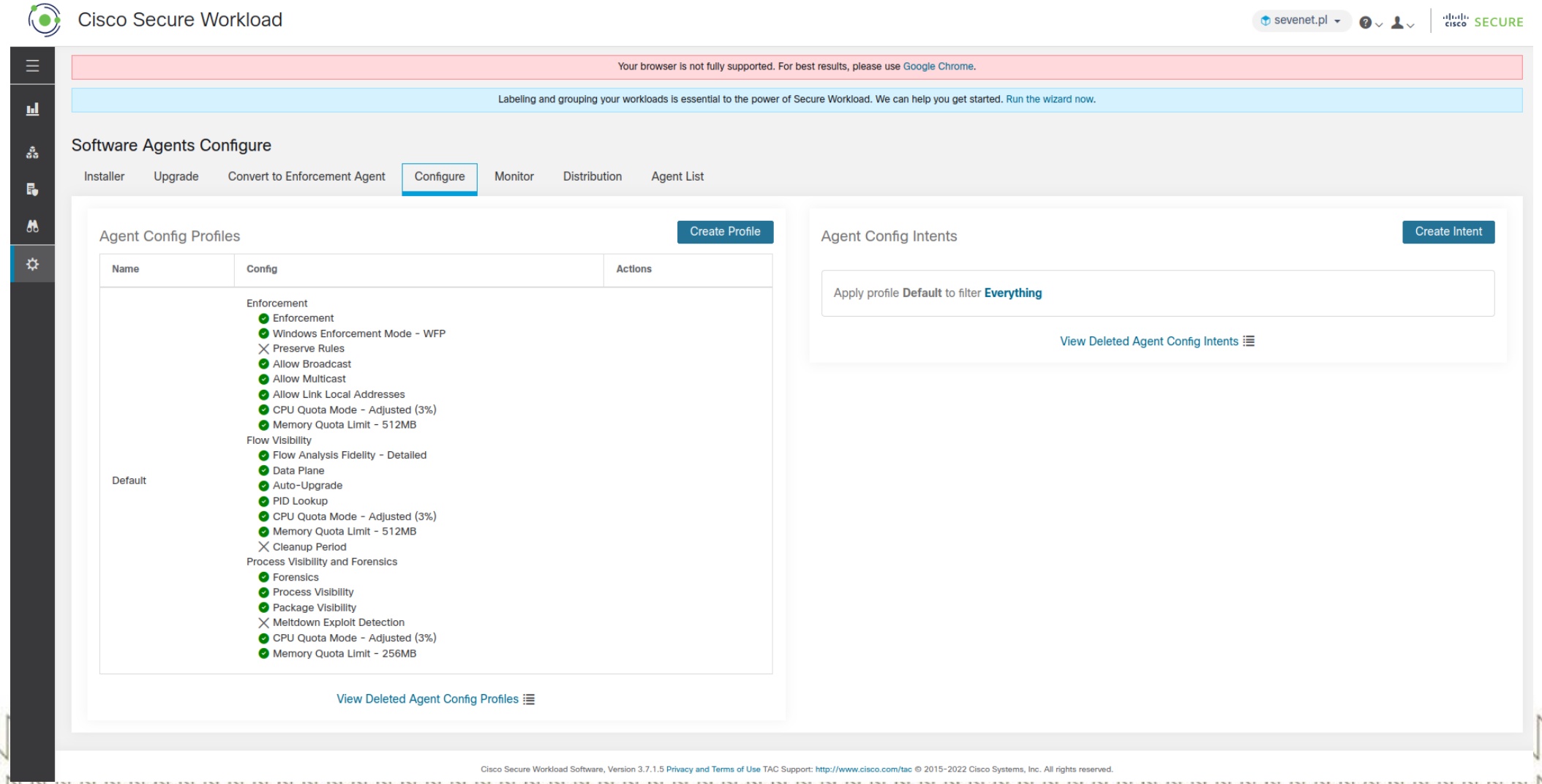
Unseen Command

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?



DZIĘKUJĘ ZA UWAGĘ

Kontakt:
marcin_kornafel@sevenet.pl