The bridge to possible

Troubleshoot Cisco Secure Client Network Visibility Module with XDR

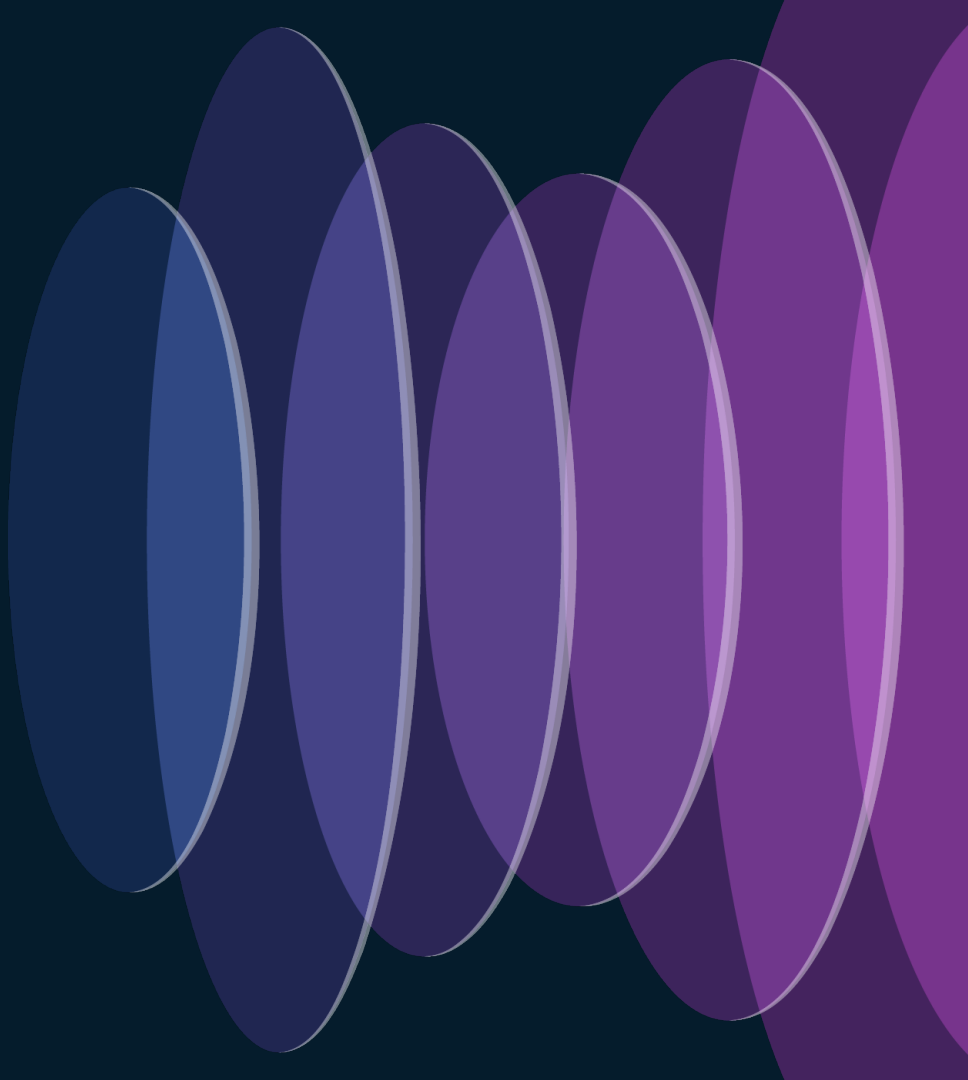
Alex Hidalgo Noriega Security Team Captain - VPN

TACSEC-2011

Agenda

- NVM Overview
- NVM and XDR Integration
- Troubleshooting
- References

NVM Overview



Let’s Clear Some Things Up

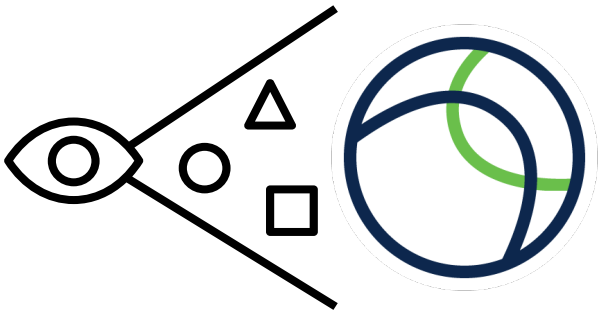
- NVM = Network Visibility Module
- XDR = eXtended Detection and Response
- DART = Diagnostics and Reporting Tool
- CSC = Cisco Secure Client
- SNA = Secure Network Analytics
- SCA = Secure Cloud Analytics

What is NVM?

- Collects rich flow context from an endpoint
- Standalone module or as a CSC Module

Why Would You Want NVM?

- The network now has to accommodate more, more, and more
- Helps you see user and endpoint behavior

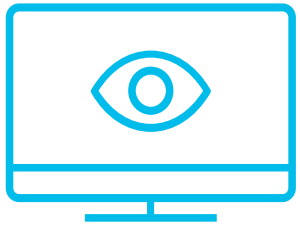


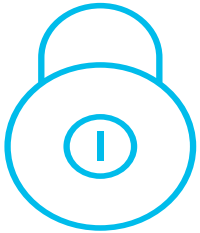
“69% of organizations say their biggest challenge in protecting against insider threats is not enough contextual information from security tools”

–Ponemon Institute, Privileged User Abuse & the Insider Threat, 2014

Benefits of NVM

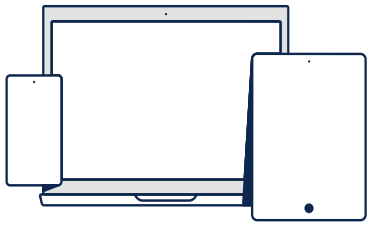
- Gain visibility into user and endpoint behavior
- On and Off-prem collection
- Implement more precise network access policies

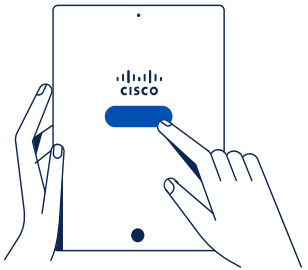




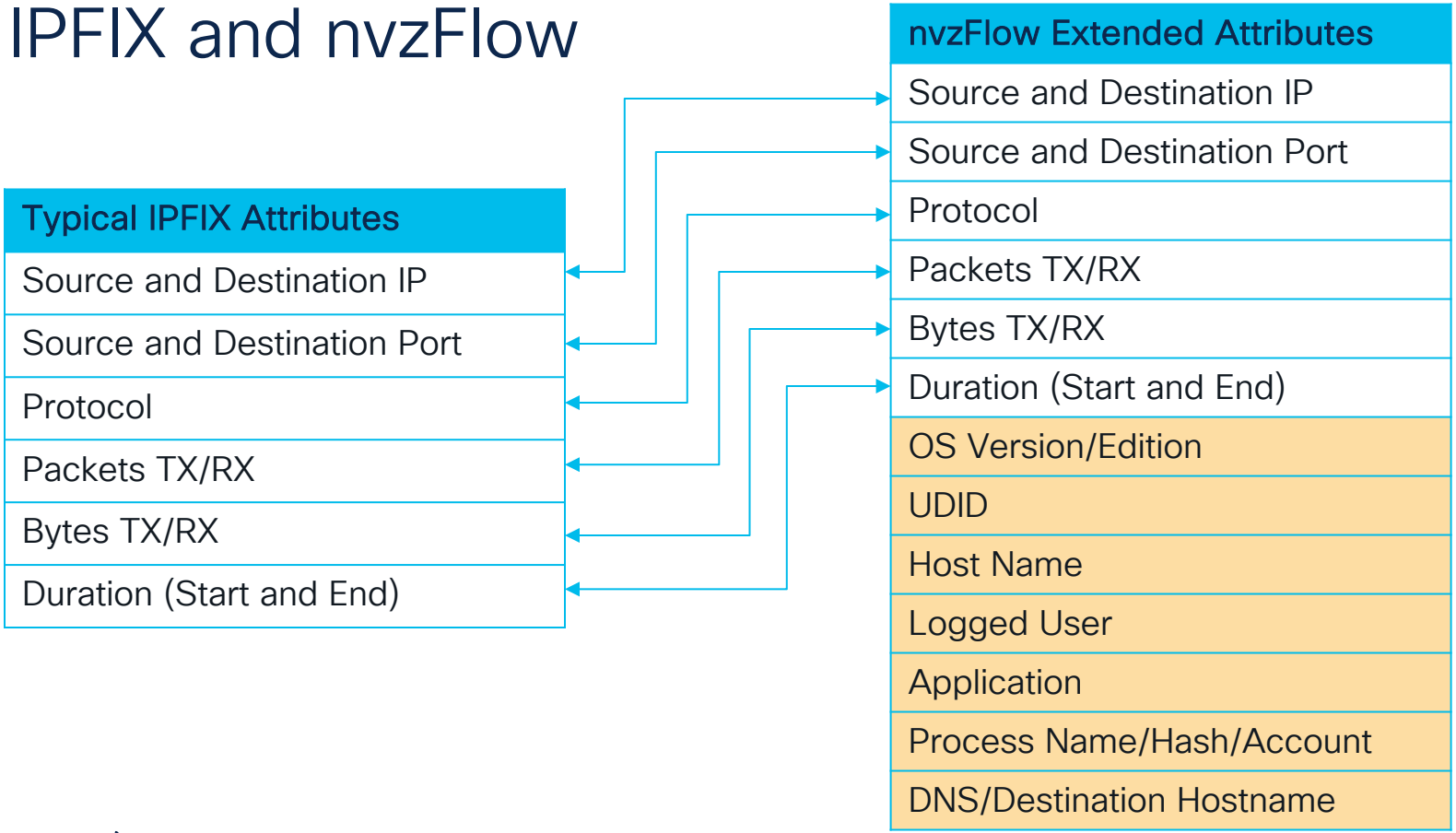
NVM Data Collection

- The Network Visibility Module collects the endpoint telemetry for better visibility into:



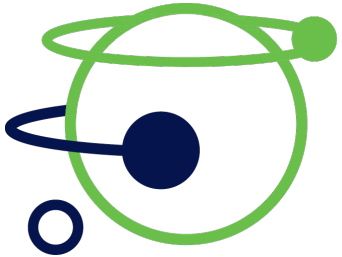


IPFIX and nvzFlow



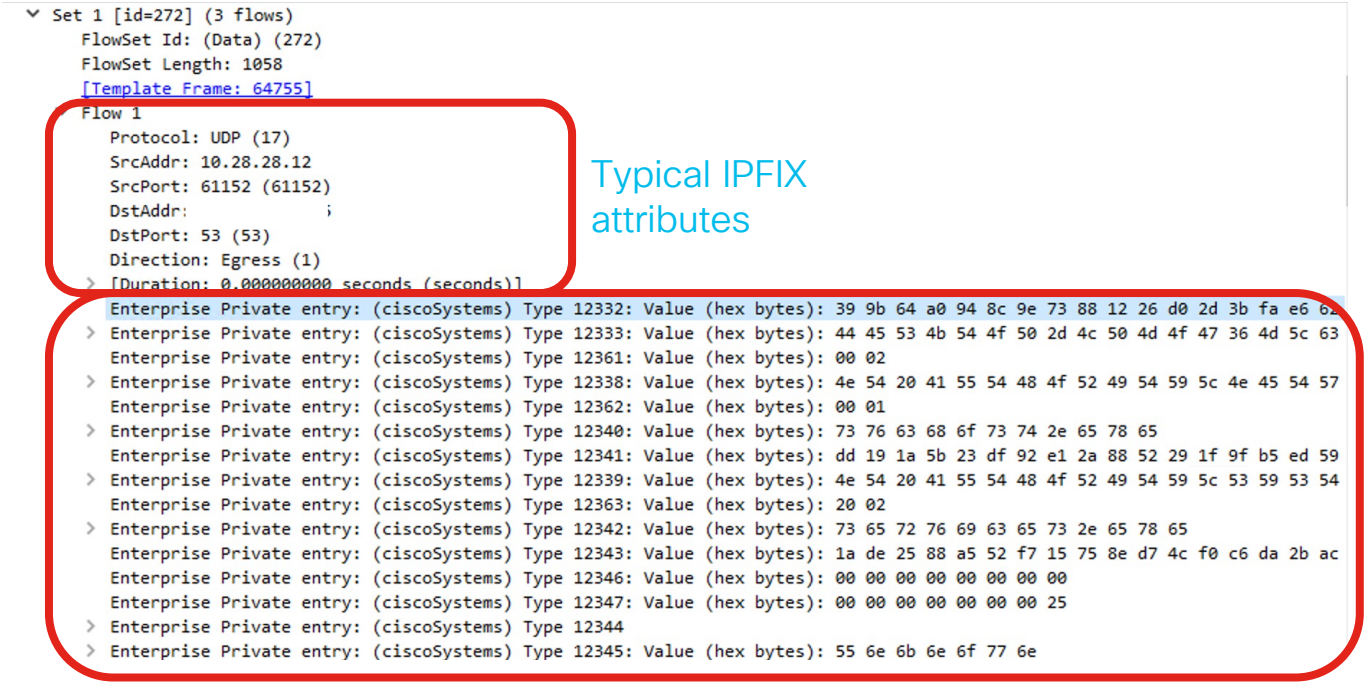
What are my deployment options?

- On-Prem
  - On-Prem Flow Collector (SNA)
- Cloud
  - Allows to integrate with XDR
  - Flow Data
  - Endpoint data
  - Interface data



IPFIX and nzvFlow

- Wireshark capture from On-Prem deployment

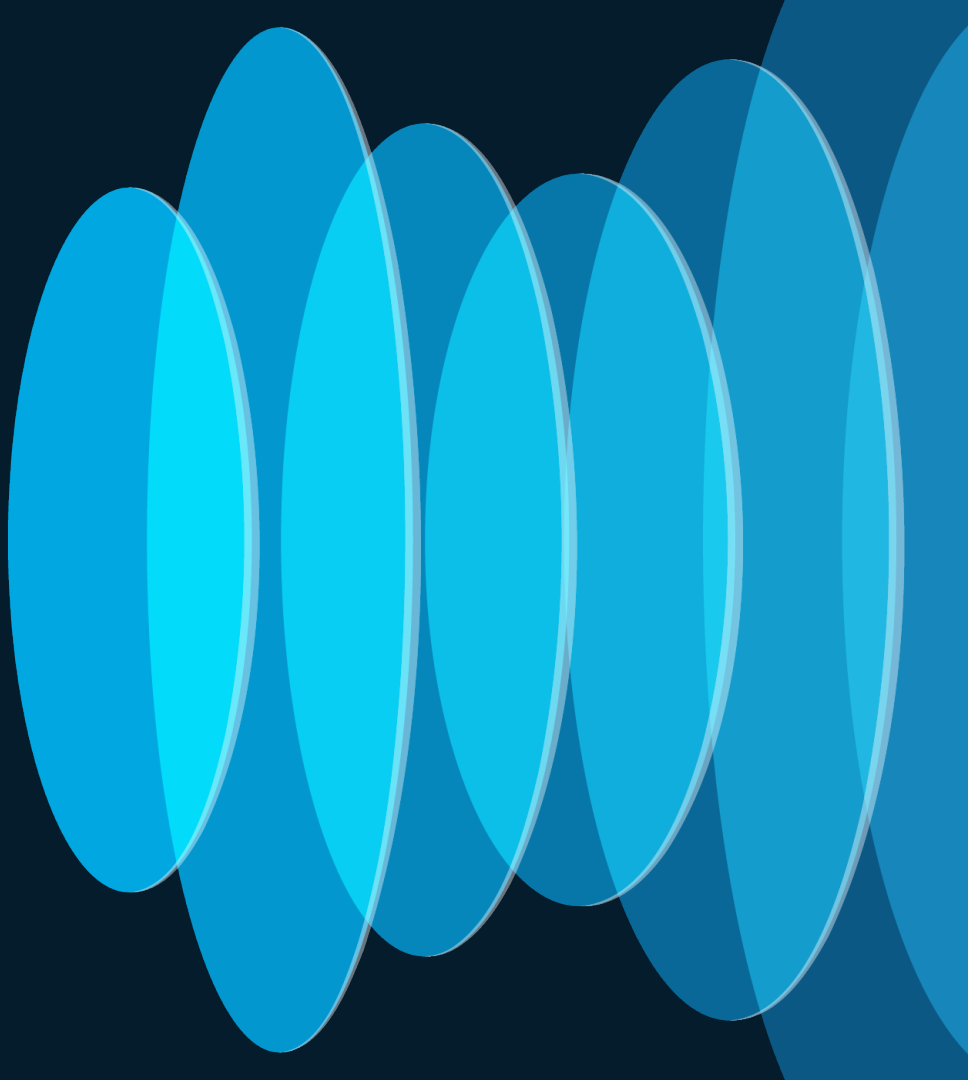


Typical IPFIX attributes

Extended attributes sent by NVM

NVM? It must be new... right?

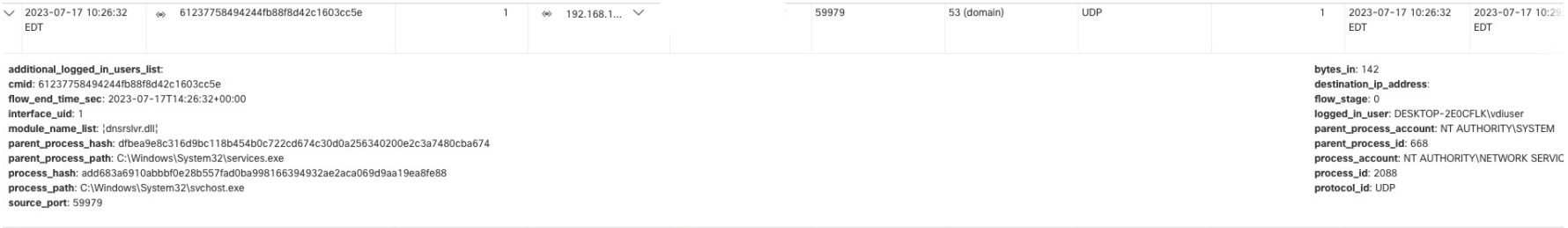
NVM and XDR Integration



NVM + XDR

- Network Visibility Module is now a core part of Cisco XDR.
- XDR collects and correlates data from various sources.
- NVM can send the flow records directly to XDR.
- XDR uses this data to create new detections and correlation.

NVM Flows on XDR



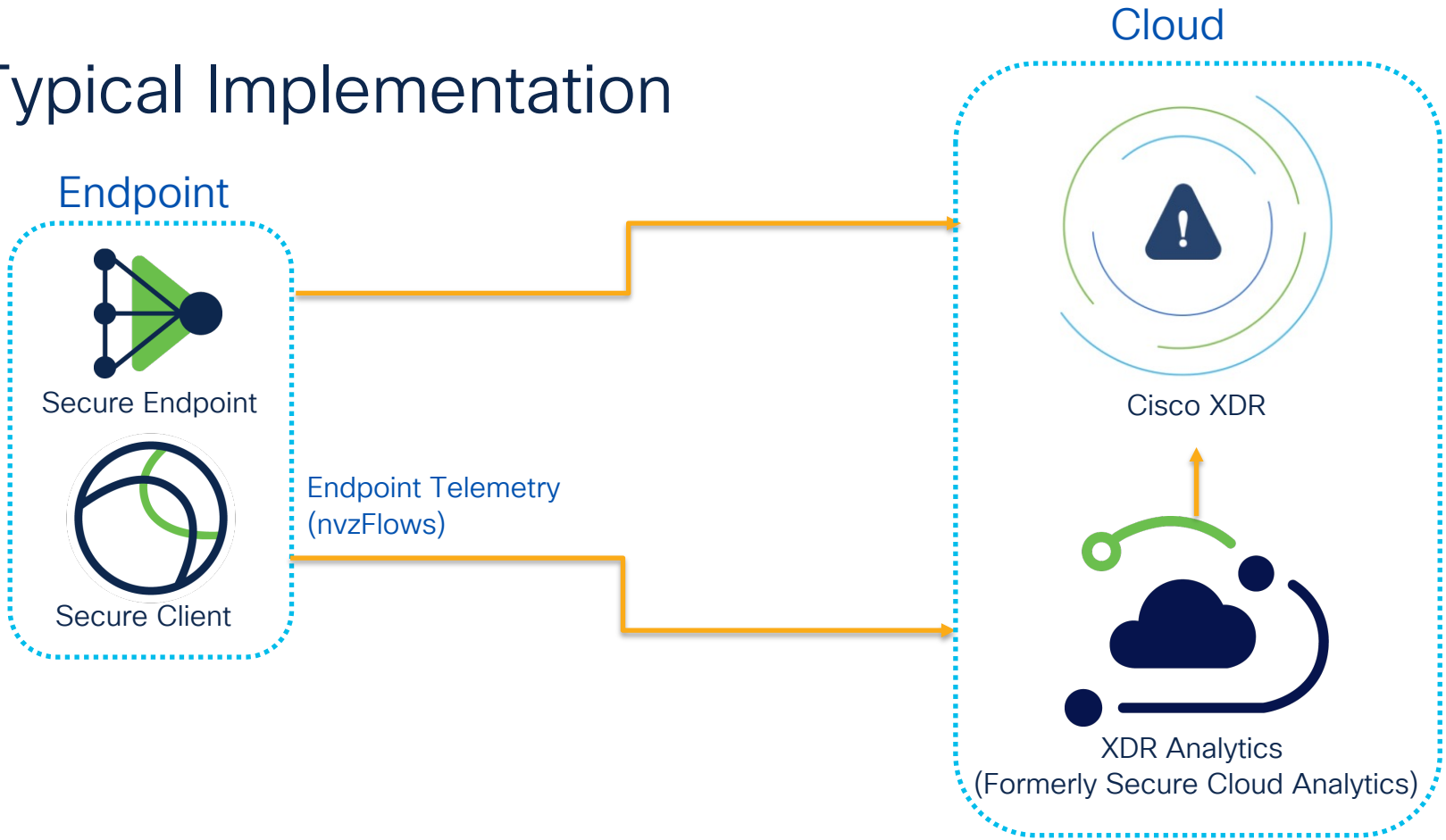
XDR

Secure Endpoint (EDR)

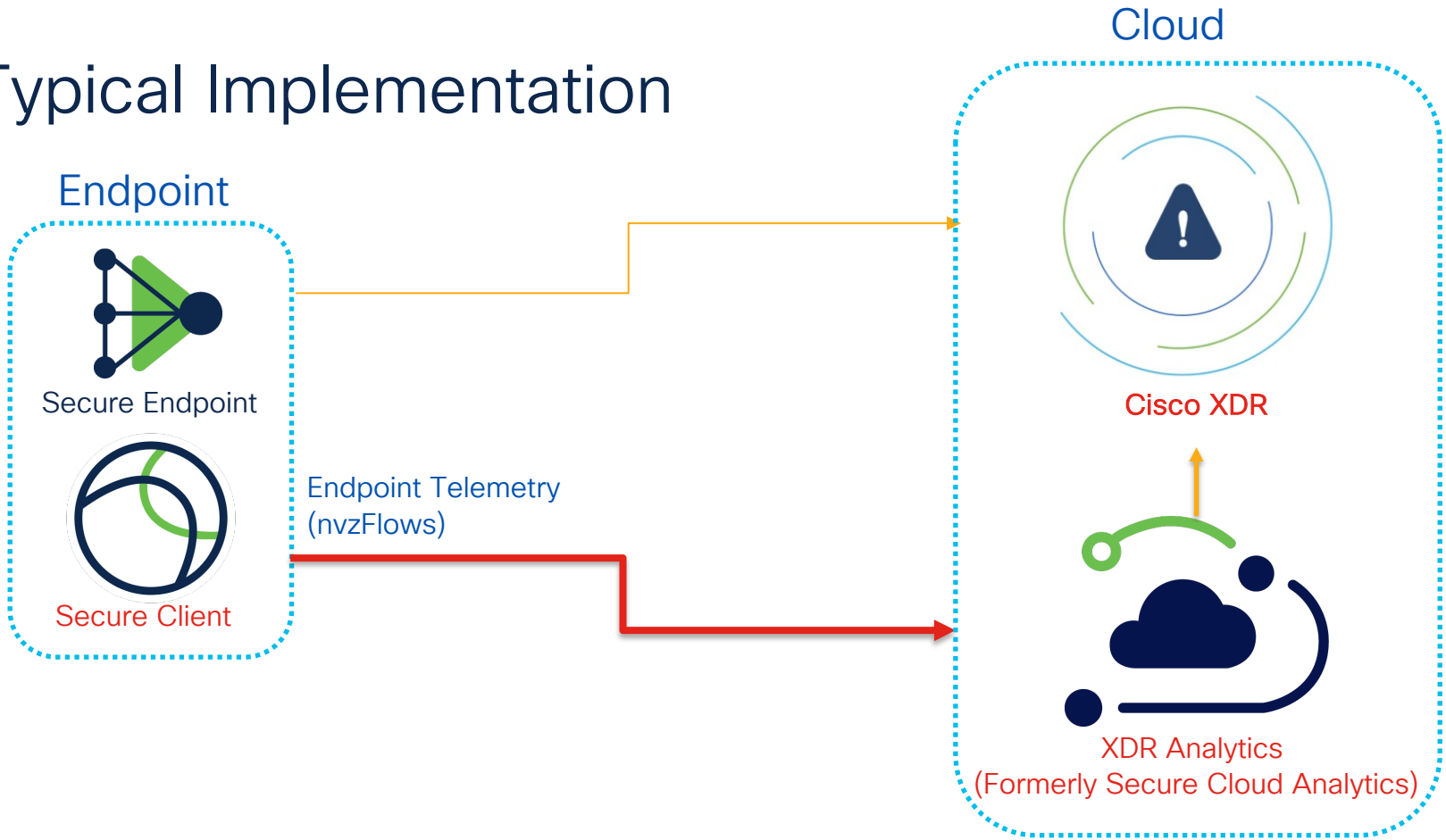
Secure Analytics (NDR)

NVM

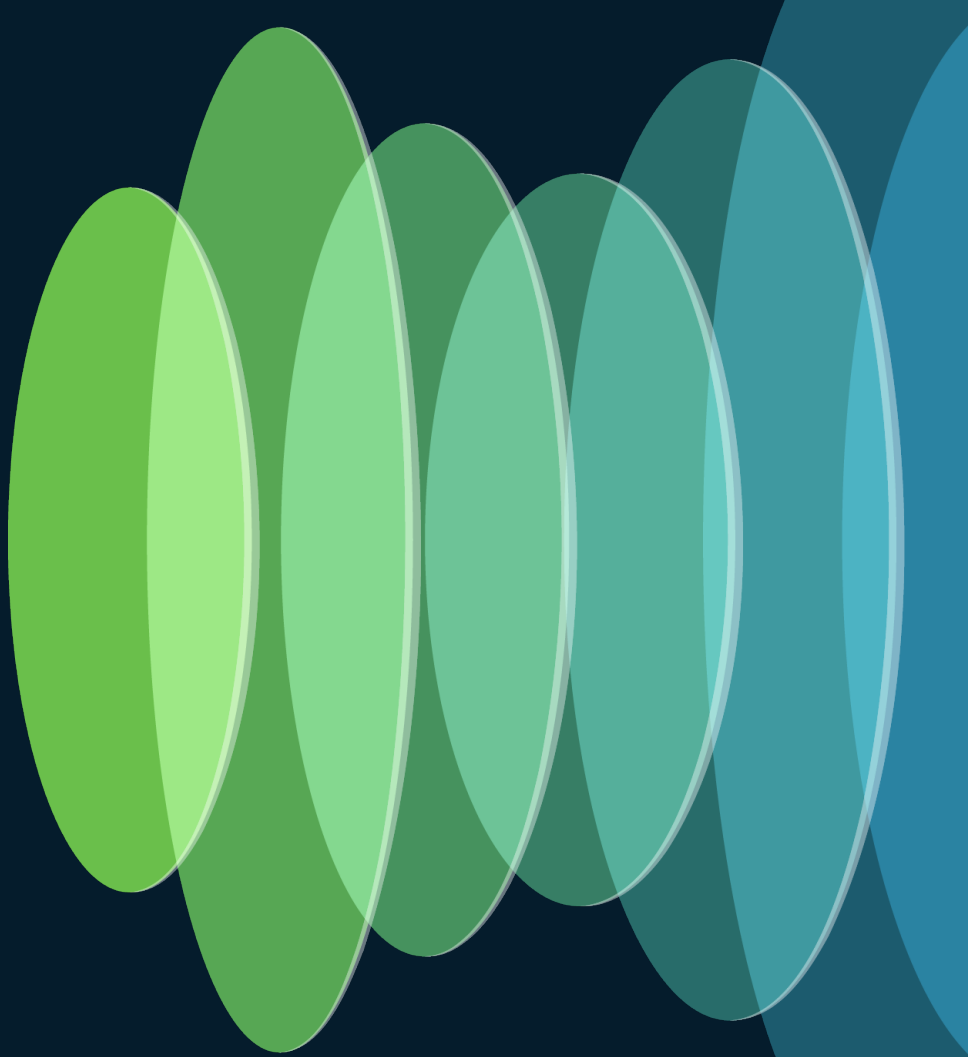
Typical Implementation



Typical Implementation



Troubleshooting

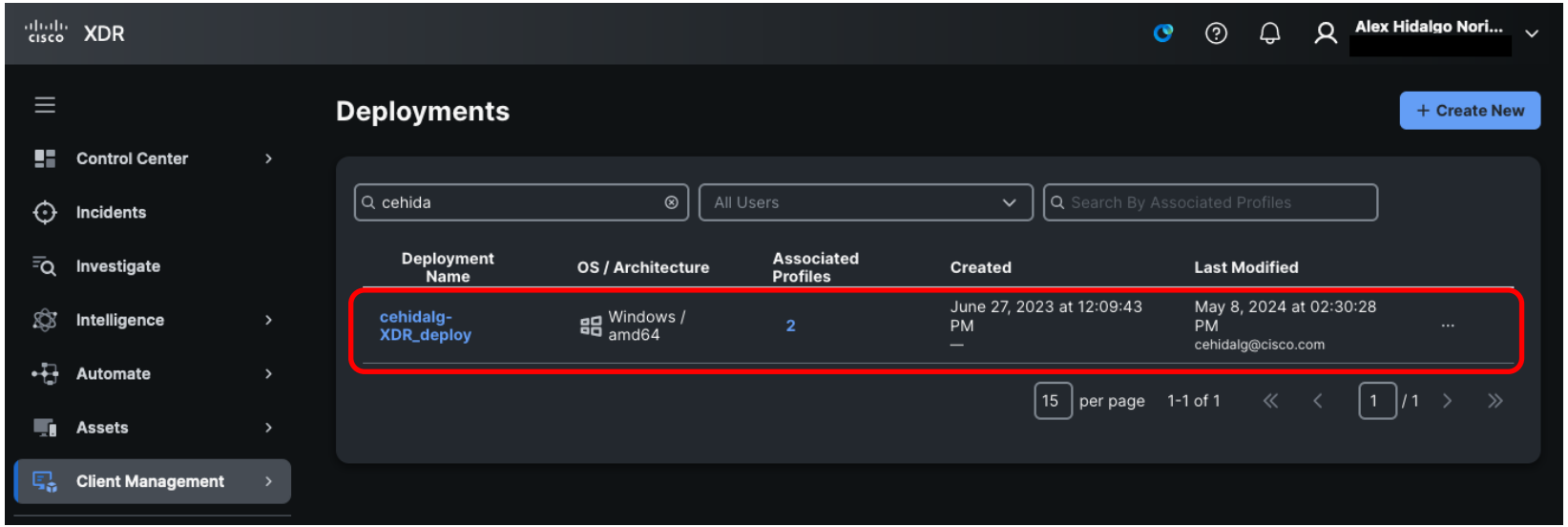


Important Considerations for Cloud Deployment

- NVM-enabled endpoints require 2 profiles
  - NVM_BootstrapProfile.xml
  - NVM_ServiceProfile.xml
- Requires a Cloud Management module

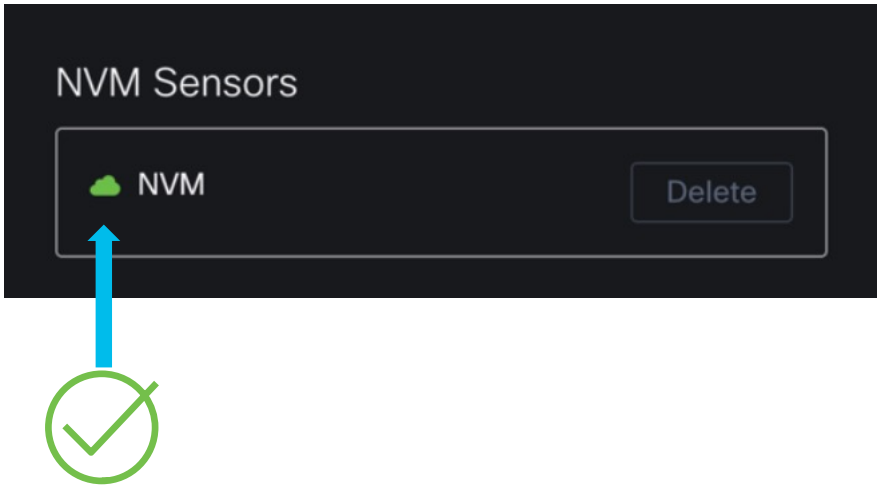
Within XDR

- Client Management > Deployments



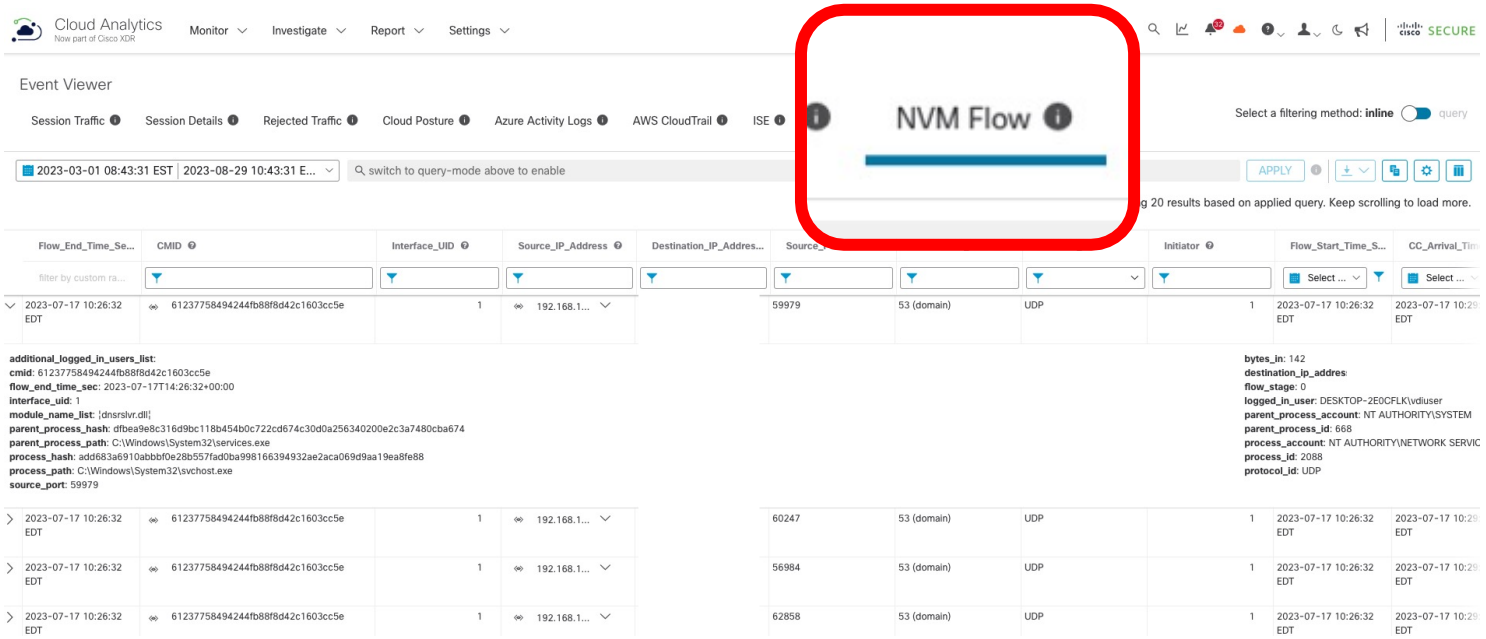
XDR Analytics

- NVM Sensor appears in **XDR Analytics UI > Settings > Sensors**



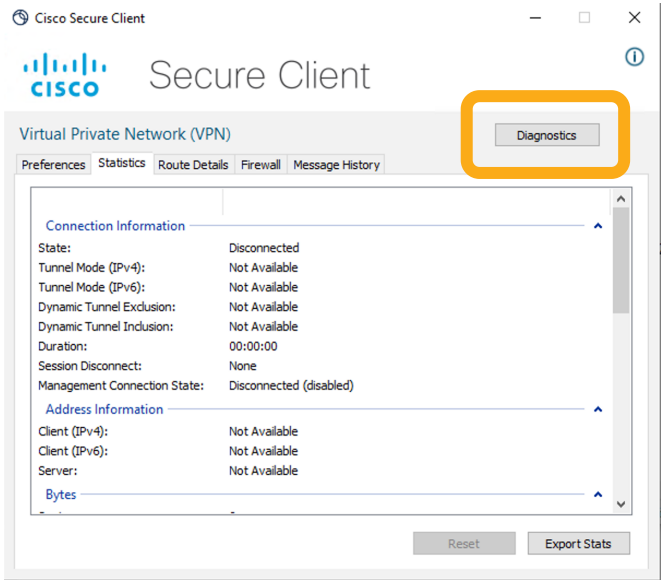
XDR Analytics

- Event Viewer > NVM Flow tab



DART Bundle

- Must be run as an administrator
- How to run DART
  - Use the application
  - Go into Settings>Diagnostics



What to Check on DART?

- Check the presence of cmidstore.json
- Ensure that NVM_BootstrapProfile and NVM_ServiceProfile are in the NVM data folder
- Important folder locations:
  - NVM config location:

    ```
    %ProgramData%\Cisco\Cisco Secure Client\NVM
    ```

  - CM module auth information:

    ```
    %ProgramData%\Cisco\Cisco Secure Client\CM\data\cmidstore.json
    ```

NVM_BootstrapProfile.xml

- Tells the endpoint to what cloud server to send the telemetry
- Client: `%ProgramData%\Cisco\Cisco Secure Client\NVM`

```
<NVMBootstrapProfile
xsi:noNamespaceSchemaLocation="NVMBootstrapProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Cloud>
    <CloudServer>intake.prod.nam.tmc.nvmc.csc.cisco.com</CloudServer>
    <CloudPort>443</CloudPort>
</Cloud>
</NVMBootstrapProfile>
```

NVM_ServiceProfile.xml

- Data Collection Policy
- Client: `%ProgramData%\Cisco\Cisco Secure Client\NVM`

```
<?xml version="1.0" encoding="UTF-8"?>
<NVMProfile xsi:noNamespaceSchemaLocation="NVMProfile.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <ProfileVersion>3</ProfileVersion>
    <CollectorConfiguration>
        <ExportTo>Cloud</ExportTo>
        <PingInterval>5</PingInterval>
    </CollectorConfiguration>
    <TemplateReportInterval>60</TemplateReportInterval>
    <CollectionMode>all</CollectionMode>
    <CollectionCriteria>
        <Broadcast>false</Broadcast>
        <Multicast>false</Multicast>
    </CollectionCriteria>
    <DataCollectionPolicy>
        <Policy>
            <PolicyName>Default DCP for Cloud</PolicyName>
            <NetworkType>VPN,Trusted,Untrusted</NetworkType>
            <Type>include</Type>
             <Fields>SNIP</Fields>
        </Policy>
    </DataCollectionPolicy>
</NVMProfile>
```

CMIDstore.json

- Found in: `%ProgramData%\Cisco\Cisco Secure Client\CM\data\cmidstore.json`


```
{
      "business_id":    "689b3b98-ea90-5b7e-b11e-a7662a4a15cf",
      "ucid_token":
      "v2.public.eyJVQ0lEIjoiYWY2MjgwNTEtZTZiNi00MjljLTg1M2ItNTdiZWUyMTA4MDc5IiwiYmlkIjoiNjg5
YjNiOTgtZWE5MC01YjdlLWIxMWUtYTc2NjJhNGExNWNmIiwiZXhwIjoiMjAyMy0wNi0yN1QyMjo1MDozNloiLCJpYXQiO
iIyMDIzLTA2LTI3VDE4OjUwOjM2WiIsImlzcyI6IkNpc2NvIElkZW50aXR5IFNlcnZpY2VzIiwianRpIjoiMTY4Nzg5MT
gzNi4xNjg3ODkxODM2ODU2OTYwMjM5LjE1NzUwODM3Njk3ODk0MTI3IiwibmJmIjoiMjAyMy0wNi0yN1QxODo1MDozNlo
ifbgLcBkKrIcpfZg1V2aDYQdSq-
rwO3TIIb9vG0S7BRJWIHi5NzWjRAkS92DHXqDvkbH5Xrhv3FGmyzUf22negg8.eyJraWQiOiJrMi5waWQuVUpjNVV2WER
hcVMyVjN6STNpbGpyWS1GWVQyQmd4YW5lSVI1dDRlbjByZzYifQ",
      "ucid":     "af628051-e6b6-429c-853b-57bee2108079",
      "instance_key":    "e603133a-bf3f-4525-8462-306a04436fb6",
      "event_url":       "https://identify.prod.nam.csc.cisco.com/event",
      "catalog_url":     "https://pacman.prod.nam.csc.cisco.com/catalog",
      "checkin_url":     "https://pacman.prod.nam.csc.cisco.com/checkin"
}
```

Debug CMID, Business ID and Token

- Create a file called **nvm_dbg.conf** which contains the number 64
- Place it in the folder:
  - `%ProgramData%\Cisco\Cisco Secure Client\NVM`
- Restart the NVM Service and collect DART again

Debug CMID, Business ID and Token

```
Date         : 07/18/2023
Time         : 18:30:50
Type         : Information
Source       : csc_nvmagent

Description : Function: NVMGrpcClient::updateClientHeader
Thread Id: 0xA7C
File:
C:\temp\build\thehoff\Quicksilver_MR40.868431406334\Quicksilver_MR4\NVM\Cloud\grpc\N
VMGrpcClient.cpp
Line: 343

NVM-CMID CMID is 3db3aaaa-aaaa-4444-beee-137333334ae8
```

Debug CMID, Business ID and Token

```
Date         : 07/18/2023
Time         : 18:30:50
Type         : Information
Source       : csc_nvmagent

Description : Function: NVMGrpcClient::updateClientHeader
Thread Id: 0xA7C
File:
C:\temp\build\thehoff\Quicksilver_MR40.868431406334\Quicksilver_MR4\NVM\Cloud\grpc\N
VMGrpcClient.cpp
Line: 356

NVM-CMID Business ID is 68888888-eaea-5bbb-b11e-a7772a4a15cf
```

Debug CMID, Business ID and Token

```
Date         : 07/18/2023
Time         : 18:30:50
Type         : Information
Source       : csc_nvmagent

Description : Function: NVMGrpcClient::updateClientHeader
Thread Id: 0xA7C
File: C:\temp\build\thehoff\Quicksilver_MR40.868431406334\Quicksilver_MR4\NVM\Cloud\grpc\NVMGrpcClient.cpp
Line: 369

NVM-CMID CM Token is
v2.public.eyJVQ0lEIjoiM2RiMzQzZmEtYTc4OS00MzcxLWJlMDQtMTM3M2U1YjU0YWU4IiwiYmlkIjoiNjg5YjNiOTgtZWE5MC01YjdlLWIxMWUt
YTc2NjJhNGExNWNmIiwiZXhwIjoiMjAyMy0wNy0xOFQyMjoyNzo1M1oiLCJpYXQiOiIyMDIzLTA3LTE4VDE4OjI3OjUzWiIsImlzcyI6IkNpc2NvIE
lkZW50aXR5IFNlcnZpY2VzIiwianRpIjoiMTY4OTcwNDg3My4xNjg5NzA0ODczMDI4NDA0NzM3LjQ3ODU0MDY0NjMwMzU0OTY4IiwibmJmIjoiMjAy
My0wNy0xOFQxODoyNzo1M1oifQKf4gTon77yqEr5-
rkHjIe4oEEpNpMQIo5jgIHLleJEklOZXO7jvqGH3MpJICnLpwdX2hm5ruSBzRDLLAYJYgU.eyJraWQiOiJrMi5waWQuVUpjNVV2WERhcVMyVjN6STN
pbGpyWS1GWVQyQmd4YW5lSVI1dDRlbjByZzYifQ
```

- Can be decoded with https://token.dev/paseto/

DART Bundle

- Ensure NVM detects it’s in cloud mode
  - Found on DART: Cisco Secure Client/Network Visibility Module/Logs/NetworkVisibility.txt

```
Description : Function: CNVMProfile::IsCloudProfile
Thread Id: 0x232C
File: C:\temp\build\thehoff\Raccoon_MR20.823301788814\Raccoon_MR2\NVM\Common\NVMProfile.cpp
Line: 1082

cloud mode
```

Enable dynamic logs

TAC Tip

- As per the *Bootstrap Profile,* the Cloud Port is 443
- Add the following to the NVM_ServiceProfile.xml:

```
<TroubleShoot>
    <Pattern>NVM-TRACE-FLOWS</Pattern>
</TroubleShoot>
```

- Restart the NVM Service and collect DART again

Dynamic Logs

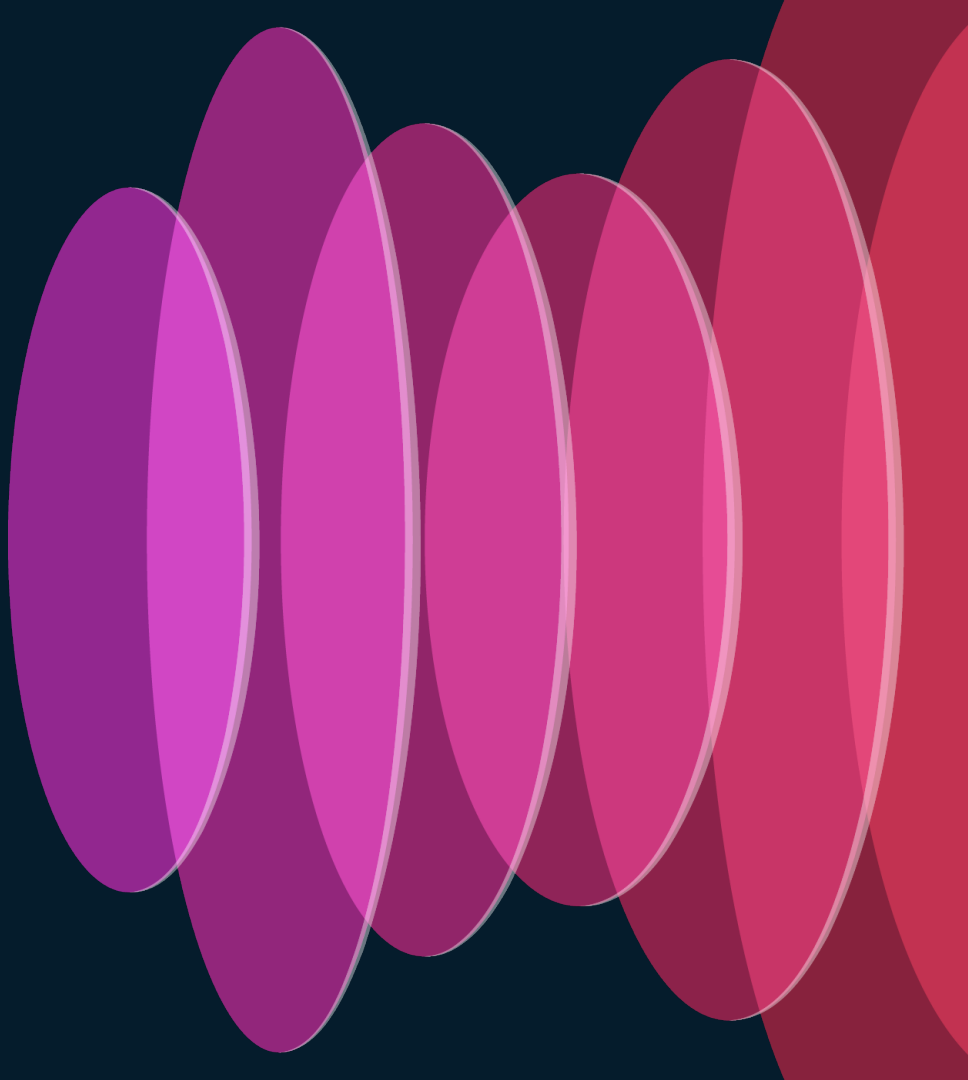
- Found on DART: Cisco Secure Client/Network Visibility Module/Logs/NetworkVisibility.txt

```
Date         : 03/04/2024
Time         : 11:34:30
Type         : Information
Source       : csc_nvmagent

Description : Function: NVMFlowObject::matchesDebugPattern
Thread Id: 0x27C0
File: C:\temp\build\thehoff\Raccoon_MR10.719617947665\Raccoon_MR1\NVM\Agent\NVMFlowObject.cpp
Line: 2014

NVM-TRACE-FLOWS: Tracking flow with id: 9901 and data FlowId: 9901
Pid: 18824 PPid: 9632
Network : [192.168.1.12:56702] --> [10.10.1.11:1900]  Flow Direction: 0  Flow Report Stage: 0  Protocol: UDP  Flow Start second:
1709548470  Flow End second: 1709548470  Flow Start Millisecond: 1709548470558  Flow End Millisecond: 1709548470739  L4 Byte
count In: 348  L4 Byte count Out: 0
Process Name: spotify.exe  Process Path: C:\Users\ad1303\AppData\Roaming\Spotify\Spotify.exe  Process hash:
ff41926b051f78215cb191369de73516aaaaaaaaf2c82644dc1627f8e077692c
Process Args: --autostart --minimized
Process Username: MD-S\AD1303   Process user account type: 32769  Proc Integrity Level 8192
Parent process Name: explorer.exe  Parent process Path: C:\Windows\explorer.exe  Parent process hash:
698eeeeeeeeeee876d0aaaaaaaaaaaaaaa9cb24f31d6d288888888c1929ed04b5
Parent Process Args: --autostart --minimized
Parent process username: MD-S\AD1303  Parent process user account type: 32769   Parent Proc Integrity Level 8192
Logged in username: MD-S\AD1303  Logged in user account type: 32769
DNS suffix: Unknown  Destination hostname: Unknown
```

Key Takeaways

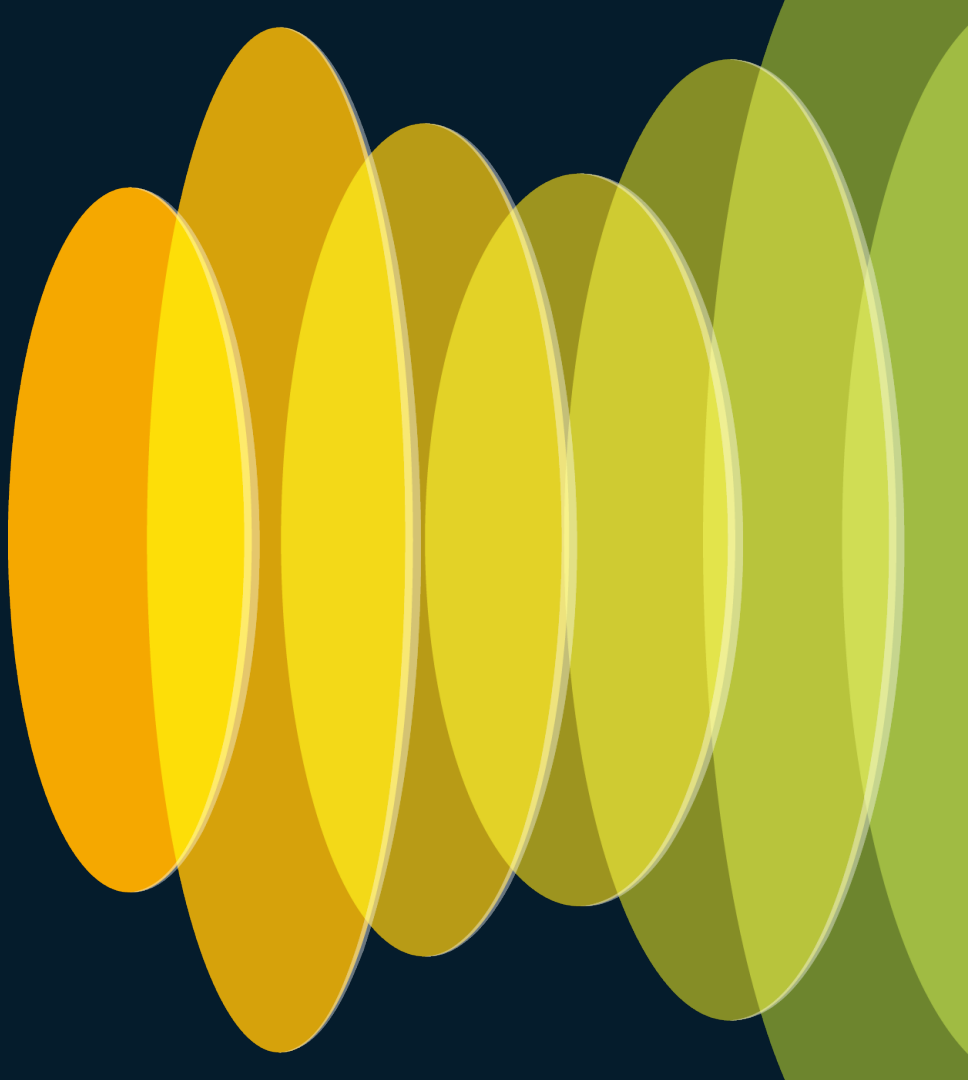


Key Takeaways

- Remember the troubleshooting flow
- From the DART bundle is important to verify:
  - If Bootstrap and Service Profiles are installed
  - Enable dynamic logs and verify CMIDstore.json information 

- NVM is a core part of XDR and useful for filling in visibility gaps
- Cisco Secure Client is more than VPN!

References



References

- Cisco AnyConnect Network Visibility Module
- Introduction to the nvzFlow protocol
- Cisco XDR (BRKSEC-2113)
- https://token.dev/paseto/

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand
- Don’t miss out “XDR on the Endpoint” (BRKSEC-2156) by Steve McBride
- Tomorrow @ 2:30pm PDT

Contact me at: cehidalg@cisco.com

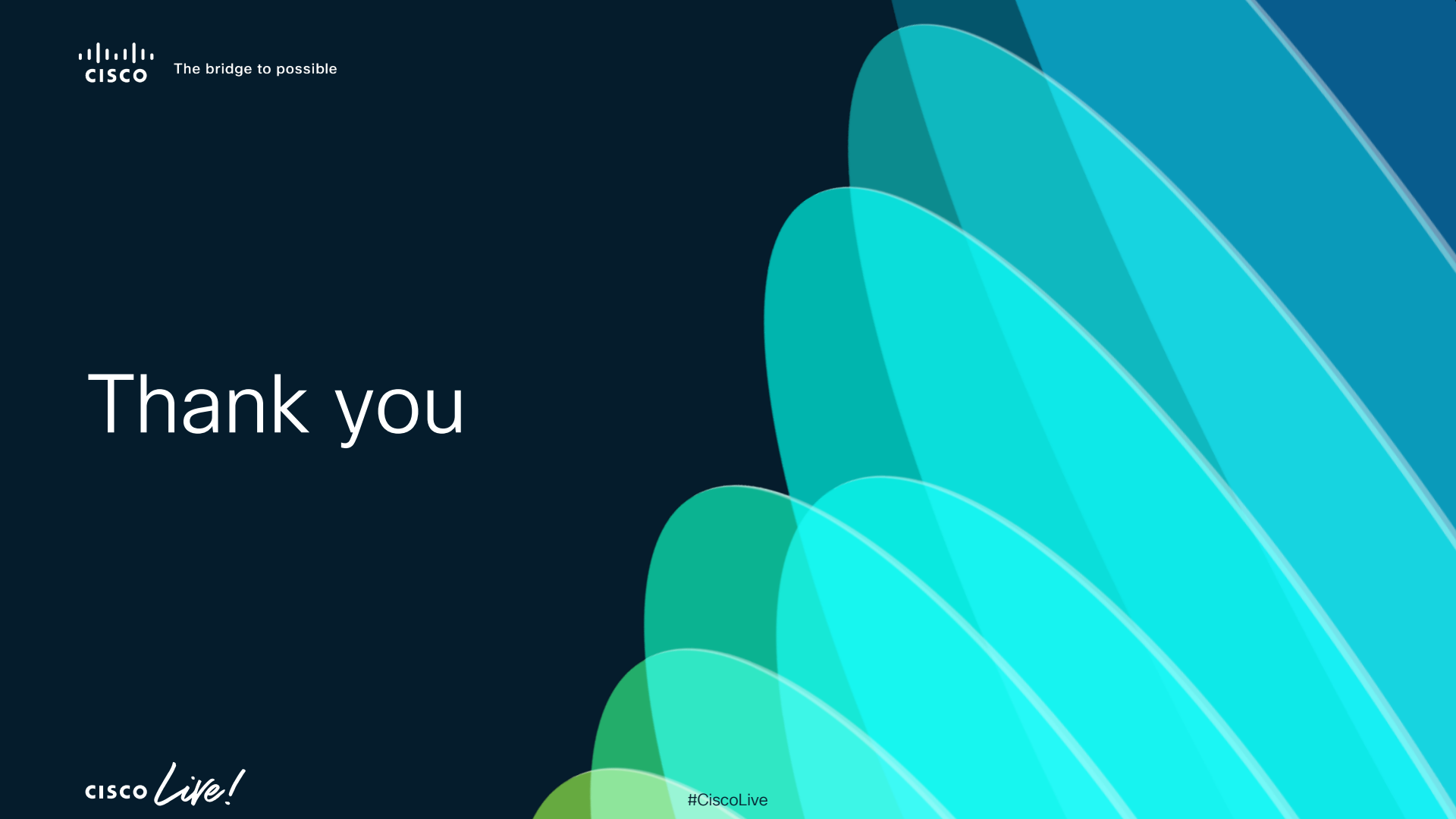
Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**


The bridge to possible
Thank you
cisco Live!
#CiscoLive