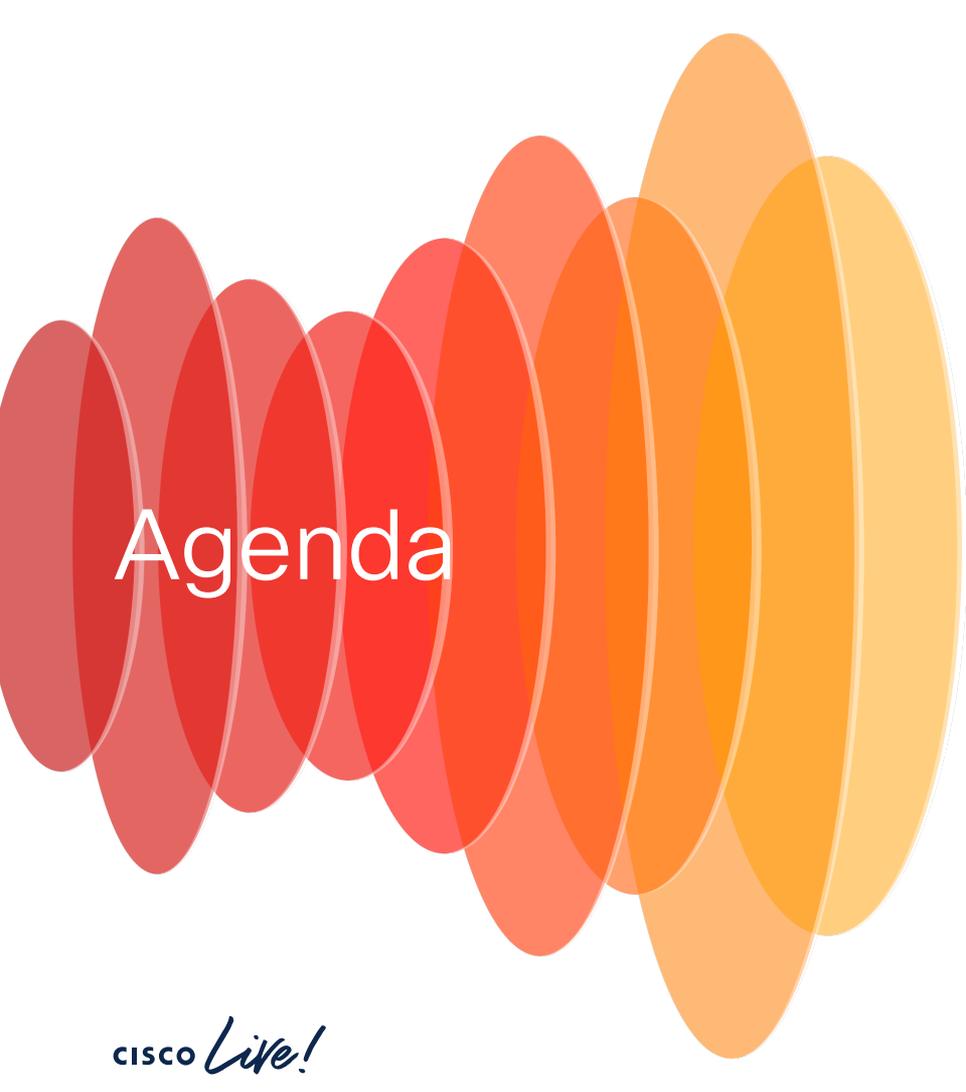


# Troubleshoot Cisco Secure Client Network Visibility Module with XDR

Alex Hidalgo Noriega Security Team Captain - VPN

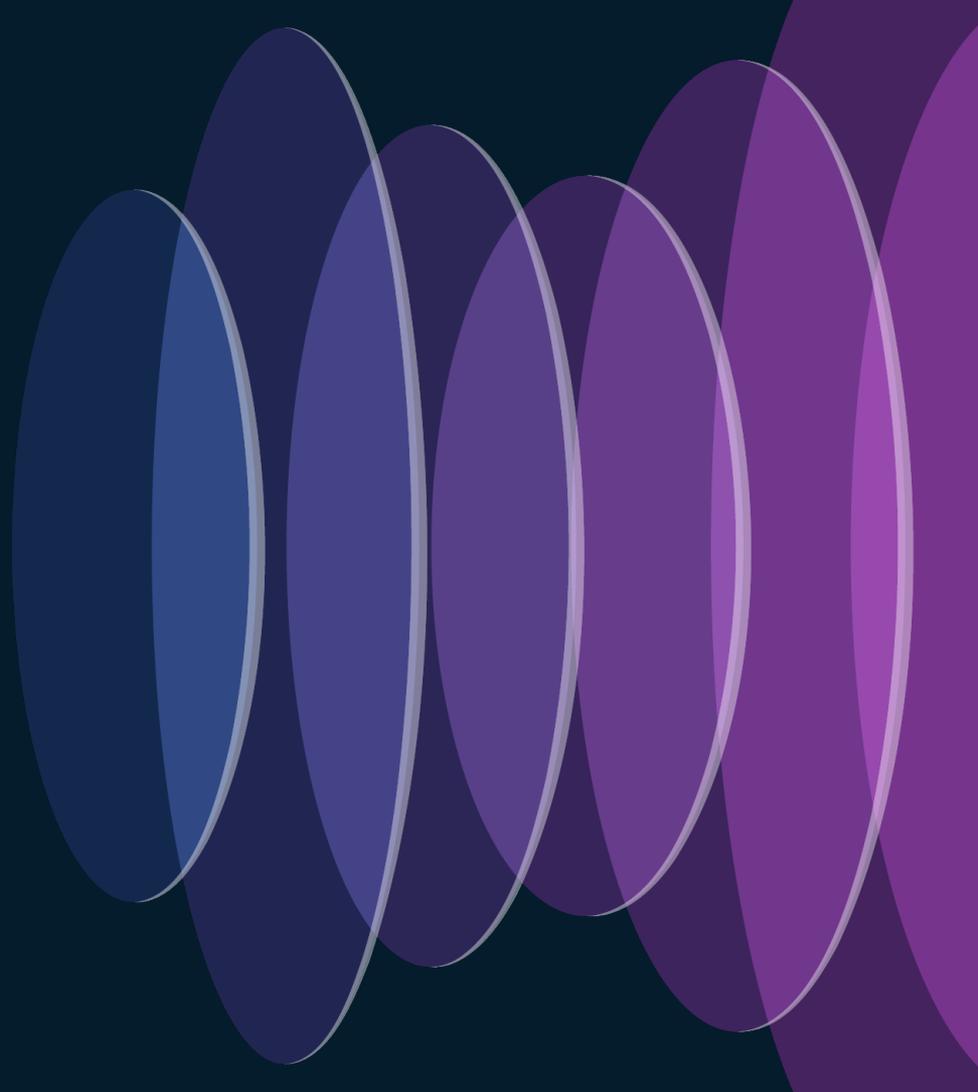
TACSEC-2011



# 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

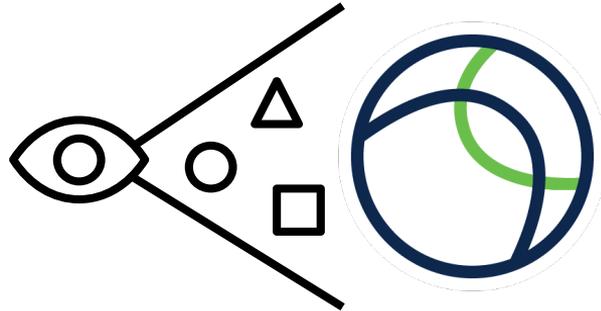
# What is NVM?

- 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



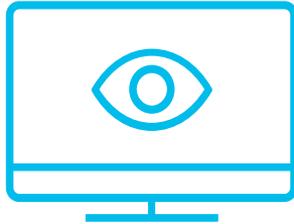
*“69% of organizations say their biggest challenge in protecting against insider threats is not enough contextual information from security tools”*

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



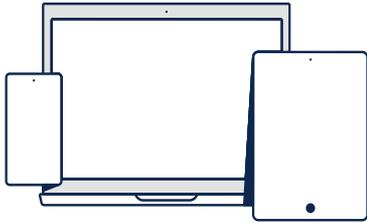
# Benefits of NVM

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



# NVM Data Collection

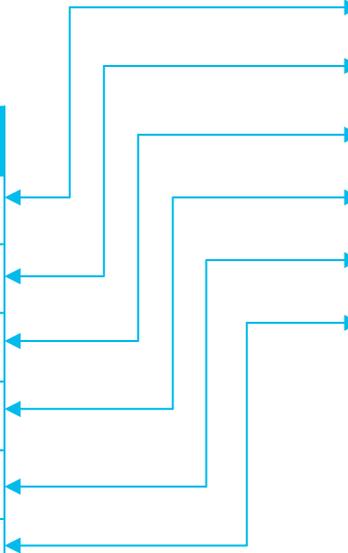
- The Network Visibility Module collects the endpoint telemetry for better visibility into:



# IPFIX and nvzFlow

Typical IPFIX Attributes
Source and Destination IP
Source and Destination Port
Protocol
Packets TX/RX
Bytes TX/RX
Duration (Start and End)

nvzFlow Extended Attributes
Source and Destination IP
Source and Destination Port
Protocol
Packets TX/RX
Bytes TX/RX
Duration (Start and End)
OS Version/Edition
UDID
Host Name
Logged User
Application
Process Name/Hash/Account
DNS/Destination Hostname



# 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

```
▼ Set 1 [id=272] (3 flows)
  FlowSet Id: (Data) (272)
  FlowSet Length: 1058
  [Template Frame: 64755]
  Flow 1
    Protocol: UDP (17)
    SrcAddr: 10.28.28.12
    SrcPort: 61152 (61152)
    DstAddr: ;
    DstPort: 53 (53)
    Direction: Egress (1)
    [Duration: 0.00000000 seconds (seconds)]
    Enterprise Private entry: (ciscoSystems) Type 12332: Value (hex bytes): 39 9b 64 a0 94 8c 9e 73 88 12 26 d0 2d 3b fa e6 62
    Enterprise Private entry: (ciscoSystems) Type 12333: Value (hex bytes): 44 45 53 4b 54 4f 50 2d 4c 50 4d 4f 47 36 4d 5c 63
    Enterprise Private entry: (ciscoSystems) Type 12361: Value (hex bytes): 00 02
    Enterprise Private entry: (ciscoSystems) Type 12338: Value (hex bytes): 4e 54 20 41 55 54 48 4f 52 49 54 59 5c 4e 45 54 57
    Enterprise Private entry: (ciscoSystems) Type 12362: Value (hex bytes): 00 01
    Enterprise Private entry: (ciscoSystems) Type 12340: Value (hex bytes): 73 76 63 68 6f 73 74 2e 65 78 65
    Enterprise Private entry: (ciscoSystems) Type 12341: Value (hex bytes): dd 19 1a 5b 23 df 92 e1 2a 88 52 29 1f 9f b5 ed 59
    Enterprise Private entry: (ciscoSystems) Type 12339: Value (hex bytes): 4e 54 20 41 55 54 48 4f 52 49 54 59 5c 53 59 53 54
    Enterprise Private entry: (ciscoSystems) Type 12363: Value (hex bytes): 20 02
    Enterprise Private entry: (ciscoSystems) Type 12342: Value (hex bytes): 73 65 72 76 69 63 65 73 2e 65 78 65
    Enterprise Private entry: (ciscoSystems) Type 12343: Value (hex bytes): 1a de 25 88 a5 52 f7 15 75 8e d7 4c f0 c6 da 2b ac
    Enterprise Private entry: (ciscoSystems) Type 12346: Value (hex bytes): 00 00 00 00 00 00 00 00
    Enterprise Private entry: (ciscoSystems) Type 12347: Value (hex bytes): 00 00 00 00 00 00 00 25
    Enterprise Private entry: (ciscoSystems) Type 12344
    Enterprise Private entry: (ciscoSystems) Type 12345: Value (hex bytes): 55 6e 6b 6e 6f 77 6e
```

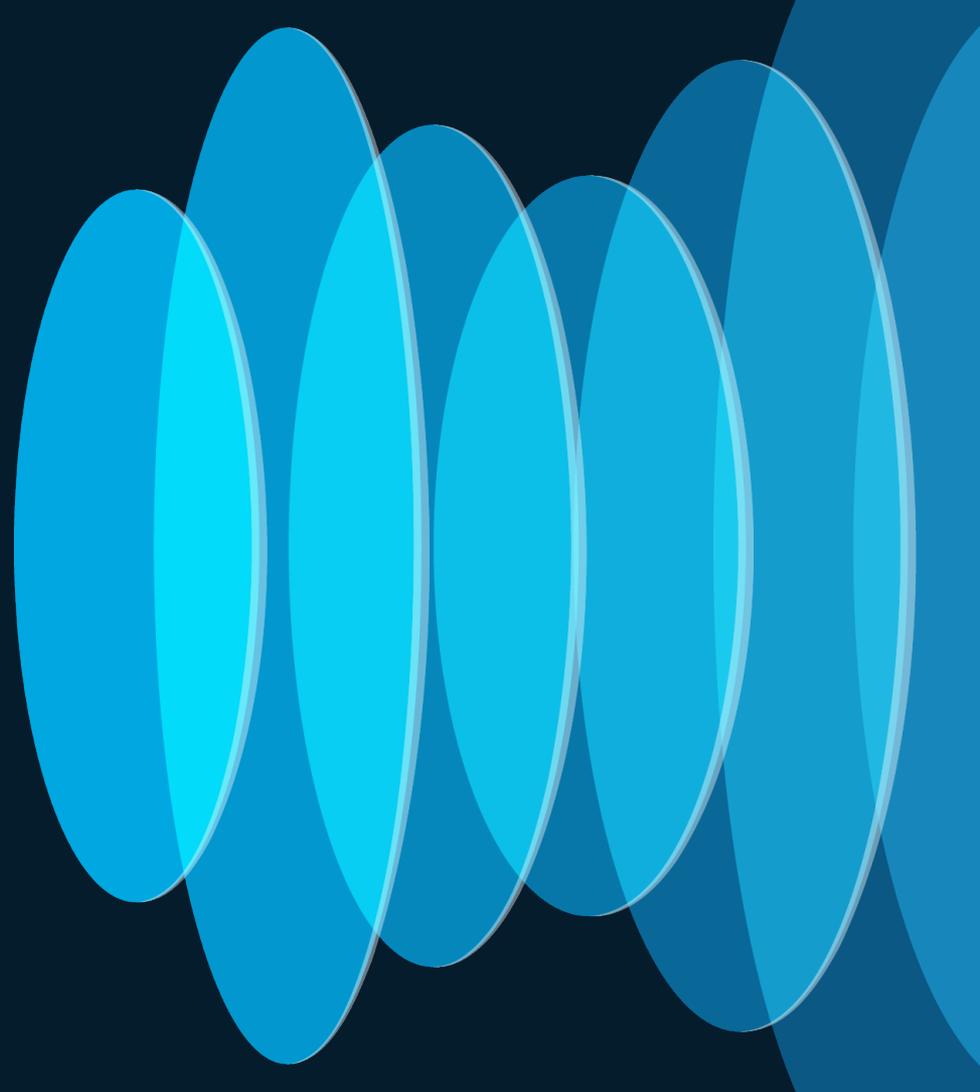
Typical IPFIX attributes

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.

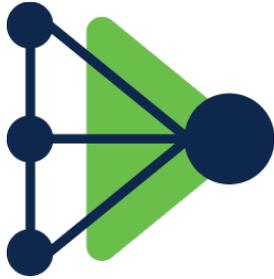
# NVM Flows on XDR

2023-07-17 10:26:32 EDT	61237758494244fb88f8d42c1603cc5e	1	192.168.1...	59979	53 (domain)	UDP	1	2023-07-17 10:26:32 EDT	2023-07-17 10:29: EDT
-------------------------	----------------------------------	---	--------------	-------	-------------	-----	---	-------------------------	-----------------------

**additional\_logged\_in\_users\_list:**  
**cmdid:** 61237758494244fb88f8d42c1603cc5e  
**flow\_end\_time\_sec:** 2023-07-17T14:26:32+00:00  
**interface\_uid:** 1  
**module\_name\_list:** [dnrsrsvr.dll]  
**parent\_process\_hash:** dfbea9e8c31fd9bc118b454b0c722cd674c30d0a256340200e2c3a7480cba674  
**parent\_process\_path:** C:\Windows\System32\services.exe  
**process\_hash:** add683a6910abbbf0e28b557fad0ba998166394932ae2aca069d9aa19ea8fe88  
**process\_path:** C:\Windows\System32\svchost.exe  
**source\_port:** 59979

**bytes\_in:** 142  
**destination\_ip\_address:**  
**flow\_stage:** 0  
**logged\_in\_user:** DESKTOP-2E0CFLK\vdiuser  
**parent\_process\_account:** NT AUTHORITY\SYSTEM  
**parent\_process\_id:** 668  
**process\_account:** NT AUTHORITY\NETWORK SERVICE  
**process\_id:** 2088  
**protocol\_id:** UDP

# XDR

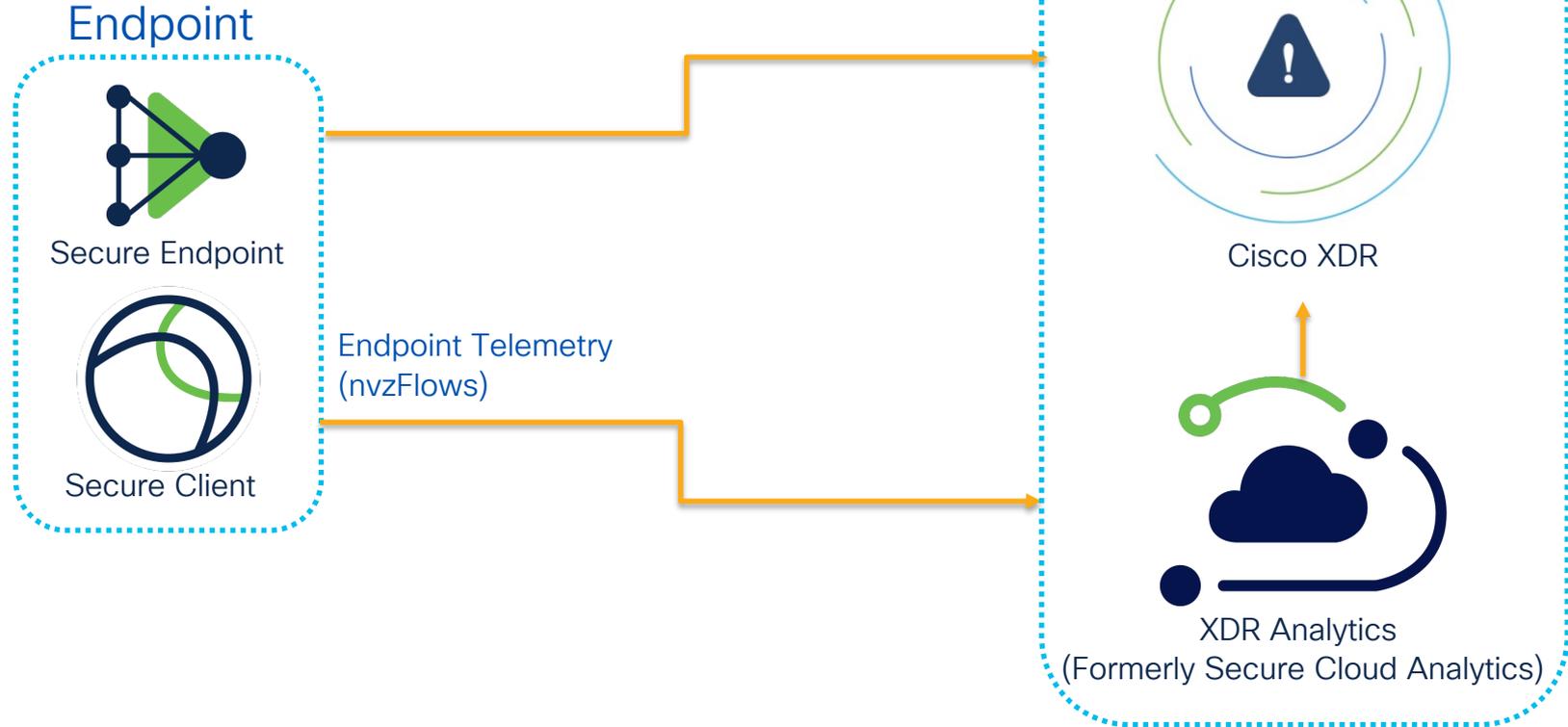


Secure Endpoint  
(EDR)

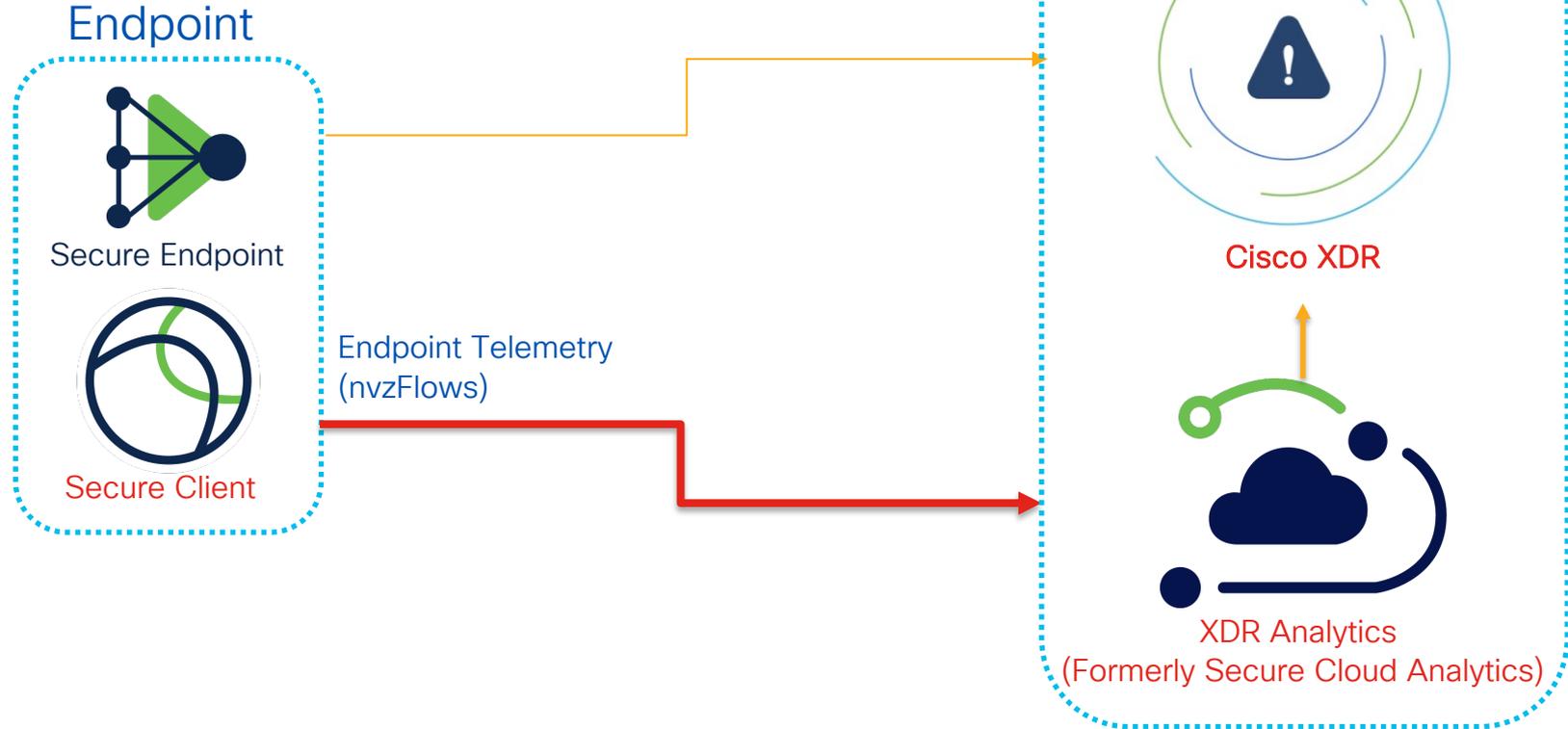
Secure Analytics  
(NDR)

NVM

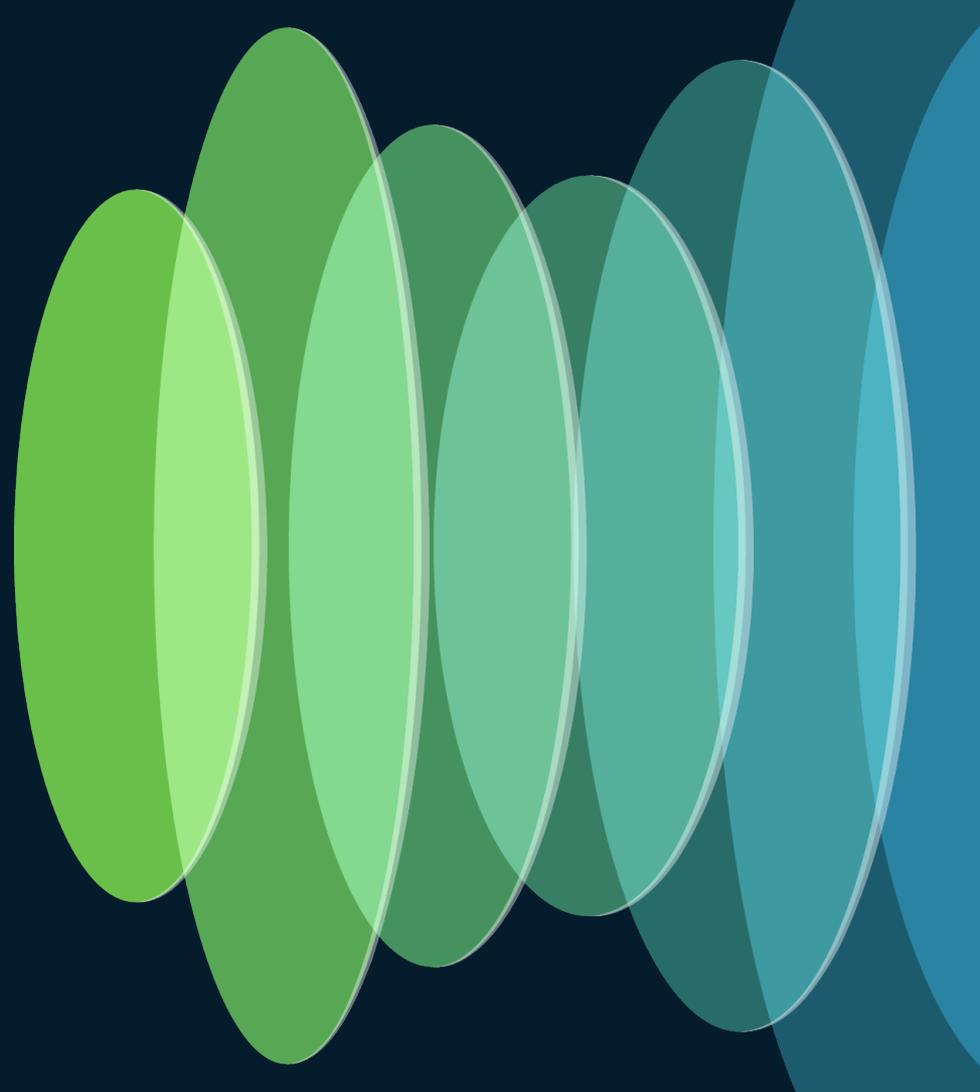
# Typical Implementation



# 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

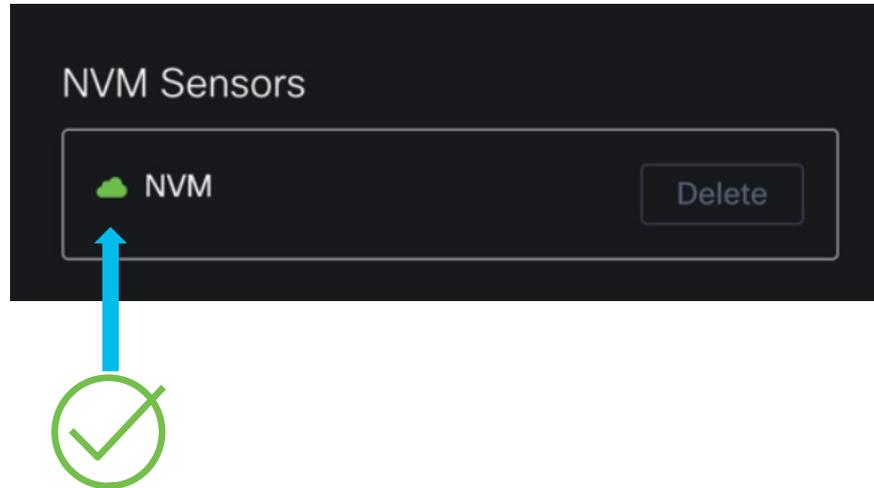
The screenshot shows the Cisco XDR interface. The top navigation bar includes the Cisco logo, 'XDR', and user information for 'Alex Hidalgo Nori...'. The left sidebar contains navigation options: Control Center, Incidents, Investigate, Intelligence, Automate, Assets, and Client Management (which is highlighted). The main content area is titled 'Deployments' and features a '+ Create New' button. Below the title is a search bar with 'cehida' entered, a dropdown menu set to 'All Users', and a search filter 'Search By Associated Profiles'. A table lists the deployment details:

Deployment Name	OS / Architecture	Associated Profiles	Created	Last Modified
cehidalg-XDR_deploy	Windows / amd64	2	June 27, 2023 at 12:09:43 PM	May 8, 2024 at 02:30:28 PM cehidalg@cisco.com

At the bottom of the table, there is a pagination control showing '15 per page', '1-1 of 1', and a page indicator '1 / 1'.

# XDR Analytics

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



# XDR Analytics

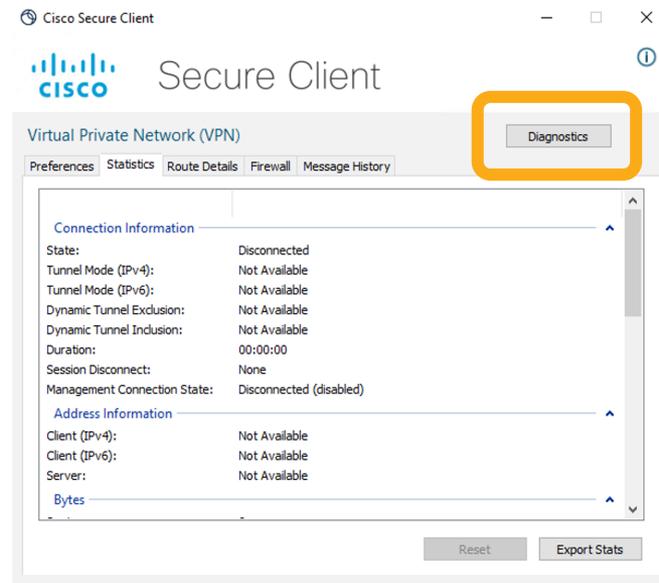
- Event Viewer > NVM Flow tab

The screenshot shows the Cisco Cloud Analytics Event Viewer interface. The 'NVM Flow' tab is highlighted with a red rounded rectangle. The interface includes a navigation bar with 'Monitor', 'Investigate', 'Report', and 'Settings'. Below the navigation bar, there are filters for 'Session Traffic', 'Session Details', 'Rejected Traffic', 'Cloud Posture', 'Azure Activity Logs', 'AWS CloudTrail', and 'ISE'. A search bar is present with a placeholder 'switch to query-mode above to enable'. The main content area displays a table of network flow events. The first row is expanded to show detailed information.

Flow_End_Time_Se...	CMID	Interface_UID	Source_IP_Address	Destination_IP_Addres...	Source...	Initiator	Flow_Start_Time_S...	CC_Arrival_Tim
2023-07-17 10:26:32 EDT	61237758494244fb88f8d42c1603cc5e	1	192.168.1...		59979	53 (domain) UDP	2023-07-17 10:26:32 EDT	2023-07-17 10:28 EDT
additional_logged_in_users_list: cmid: 61237758494244fb88f8d42c1603cc5e flow_end_time_sec: 2023-07-17T14:26:32+00:00 interface_uid: 1 module_name_list: [dnrsalvr.dll] parent_process_hash: dfbea9e8c316d9bc118b454b0c722cd674c30d0a256340200e2c3a7480c8a674 parent_process_path: C:\Windows\System32\services.exe process_hash: ad8f683a8910abaf0e28b5577ad0ba998166394932ae2aca069d9aa19ea8fe88 process_path: C:\Windows\System32\svchost.exe source_port: 59979		bytes_in: 142 destination_ip_address: flow_stage: 0 logged_in_user: DESKTOP-2E0CFLK\vduser parent_process_account: NT AUTHORITY\SYSTEM parent_process_id: 668 process_account: NT AUTHORITY\NETWORK SERVICE process_id: 2088 protocol_id: UDP						
> 2023-07-17 10:26:32 EDT	61237758494244fb88f8d42c1603cc5e	1	192.168.1...		60247	53 (domain) UDP	2023-07-17 10:26:32 EDT	2023-07-17 10:28 EDT
> 2023-07-17 10:26:32 EDT	61237758494244fb88f8d42c1603cc5e	1	192.168.1...		56984	53 (domain) UDP	2023-07-17 10:26:32 EDT	2023-07-17 10:28 EDT
> 2023-07-17 10:26:32 EDT	61237758494244fb88f8d42c1603cc5e	1	192.168.1...		62858	53 (domain) UDP	2023-07-17 10:26:32 EDT	2023-07-17 10:28 EDT

# 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>
```



# 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_nvagent
```

```
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_nvagent
```

```
Description : Function: NVMGrpcClient::updateClientHeader
```

```
Thread Id: 0xA7C
```

```
File:
```

```
C:\temp\build\thehoff\Quicksilver_MR40.868431406334\Quicksilver_MR4\NVM\Cloud\grpc\NVMGrpcClient.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_nvAGENT
```

```
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.eyJVQ01EiJoiM2RiMzQzZmEtYTc0S00MzcxLWJlMDQtMTM3M2U1YjU0YWU4IiwiaWlkIjoibjg5YjNiOTgtZWE5MC01Yjd1LWlWxMWUt
YTc2NjJhNGExNWNmIiwiaXhwIjoibjg5YjNiOTgtZWE5MC01Yjd1LWlWxMWUtY2VzIiwianRpIjoibjg5YjNiOTgtZWE5MC01Yjd1LWlWxMWUt
lkZW50aXR5IiwiaWF0IjoiMTY4OTcwNDg3My4xNjg5NzA0ODczMDI4NDAA0NzM3LjQ3ODU0MDY0NjMwMzU0OTY4IiwibmJmIjoibjg5YjNiOTgtZWE5MC01Yjd1LWlWxMWUt
My0wNy0xOFQxODoyNz0lMloifQKf4gTon77yqEr5-
rkHjIe4oEEpNpMQIo5jgIHLleJEk10ZX07jvqGH3MpJICnLpWdX2hm5ruSBzRDLLAYJYgU.eyJraWQiOiJrMi5waWQuVUpjNVV2WERhcVMYVjN6STN
pbGpyWS1GWVQyQmd4YW51SVIldDRlbyByZzYifQ
```

- 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



- 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_nvagent
```

```
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: ff41926b051f78215cb191369de73516aaaaaaaaaf2c82644dc1627f8e077692c
```

```
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:
```

```
698eeeeeeeeeeee876d0aaaaaaaaaaaaaaaa9cb24f31d6d288888888c1929ed04b5
```

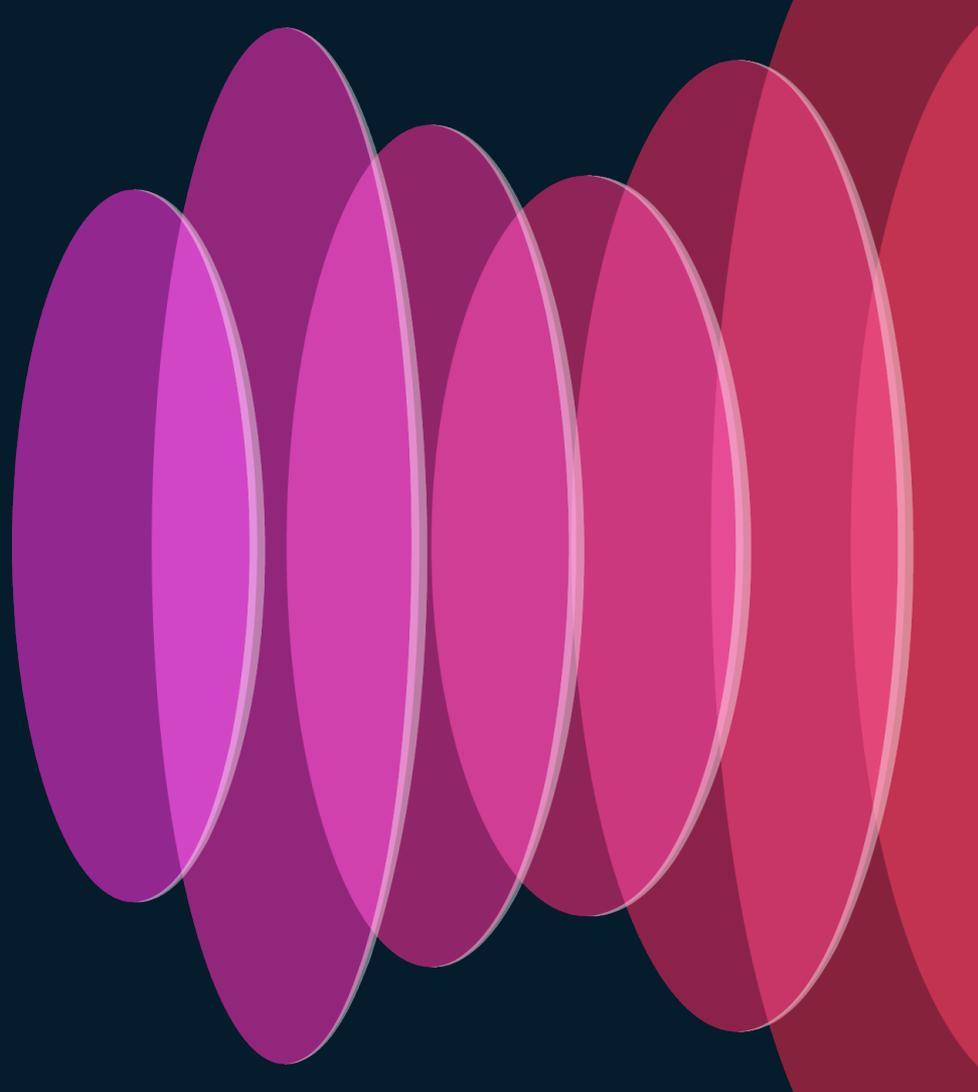
```
Parent Process Args: --autostart --minimized
```

```
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



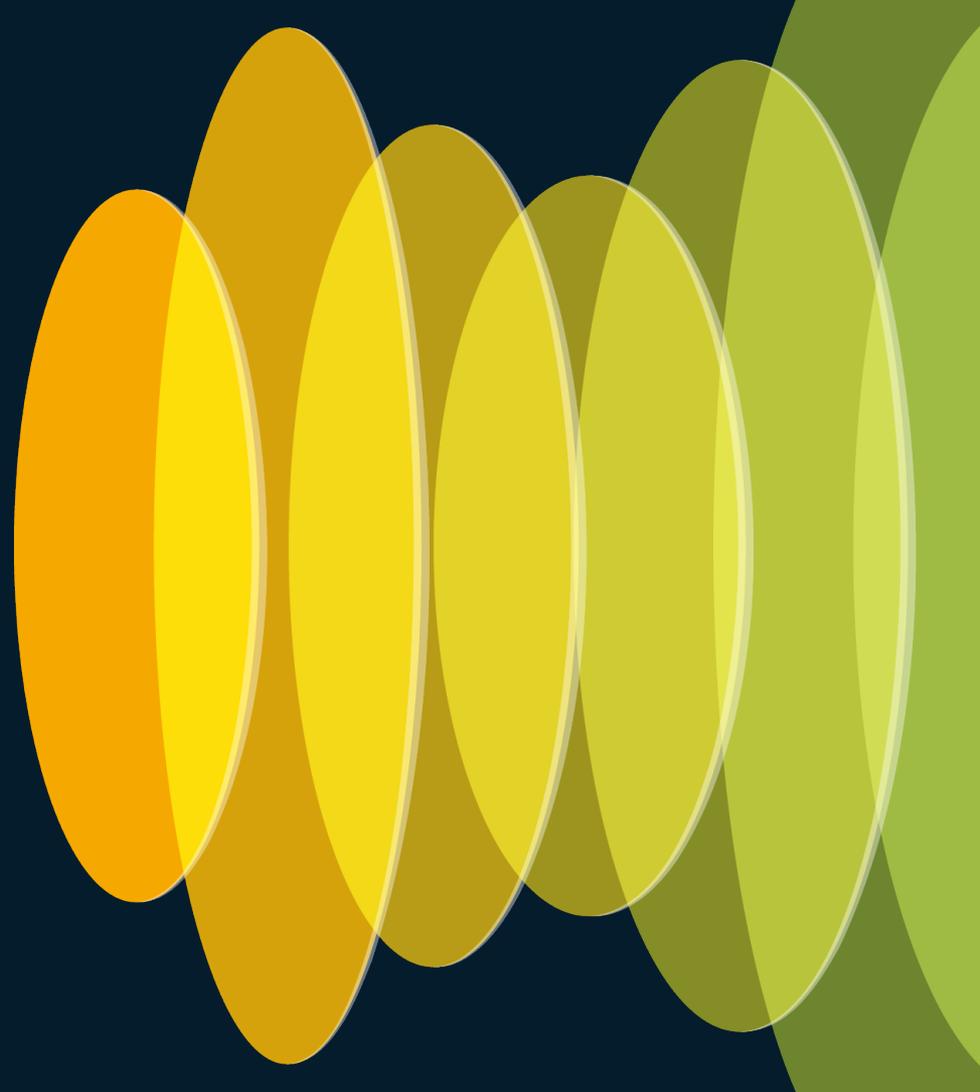
# Key Takeaways

- 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!

TAC Tip



# 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](http://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](mailto: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