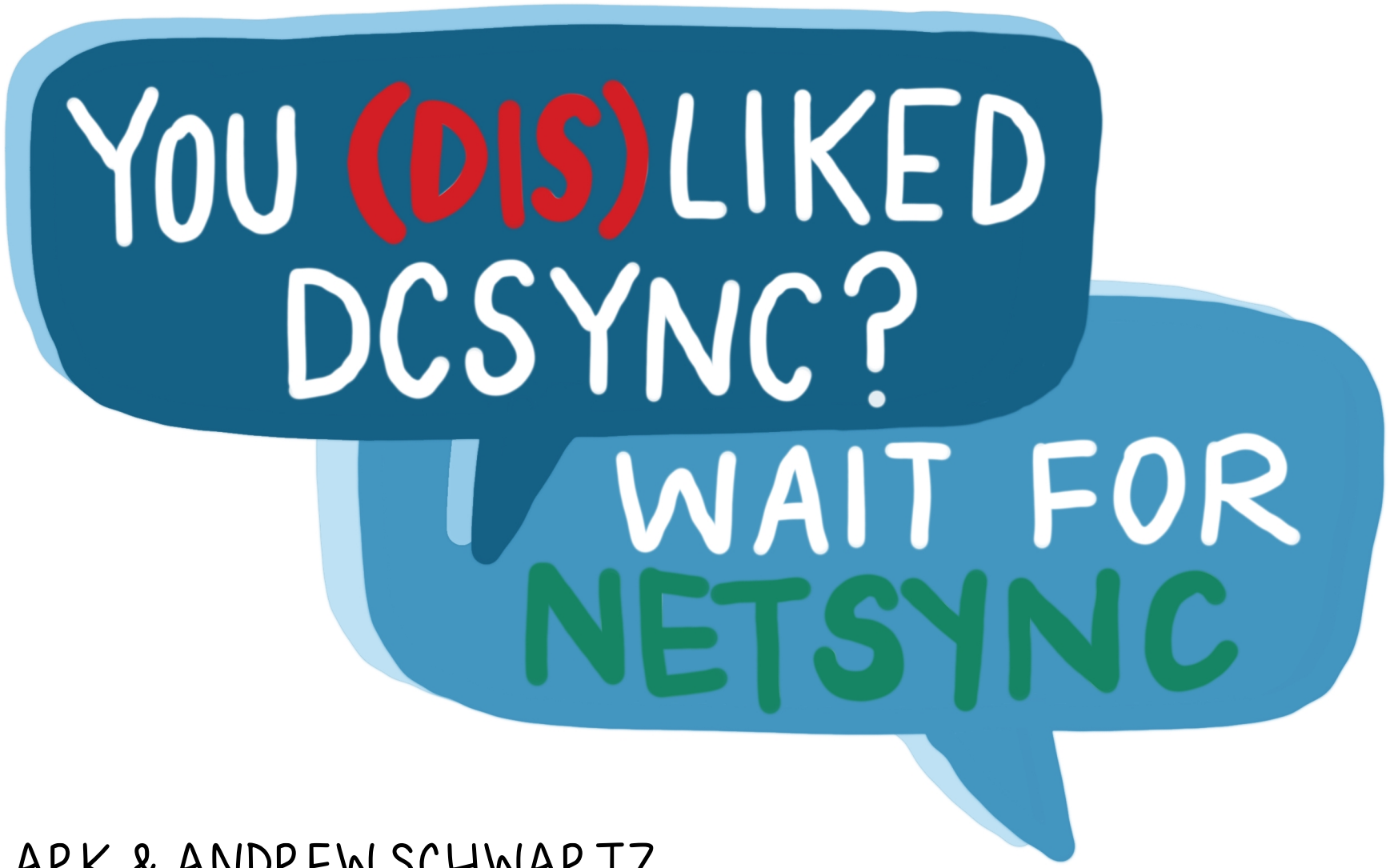
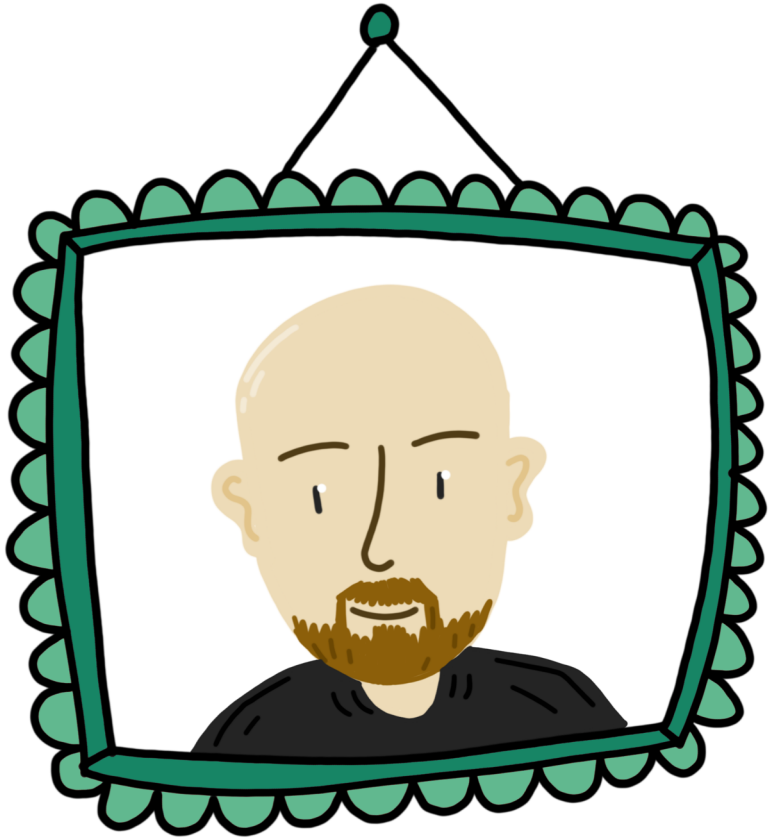


CHARLIE CLARK & ANDREW SCHWARTZ

TEXAS CYBER SUMMIT 2023

TODAY'S TOPICS

- INTRODUCTIONS
- F#*$ U, DCSYNC
- NETSYNC 101
- A NEW NETSYNC POC
- Q&A



CHARLIE CLARK

- @EXPLOITPH
- RED TEAMER @ MDSEC
- OFFENSIVE ADMIN
- STREAMING MEDIA AFICIONADO

ANDREW SCHWARTZ

- @4NDR3W6S
- PRACTICE LEAD @ TRUSTEDSEC
- ATTACK/DETECT ALL THE THINGS
- TOTTENHAM SUPER FAN (COYS!)

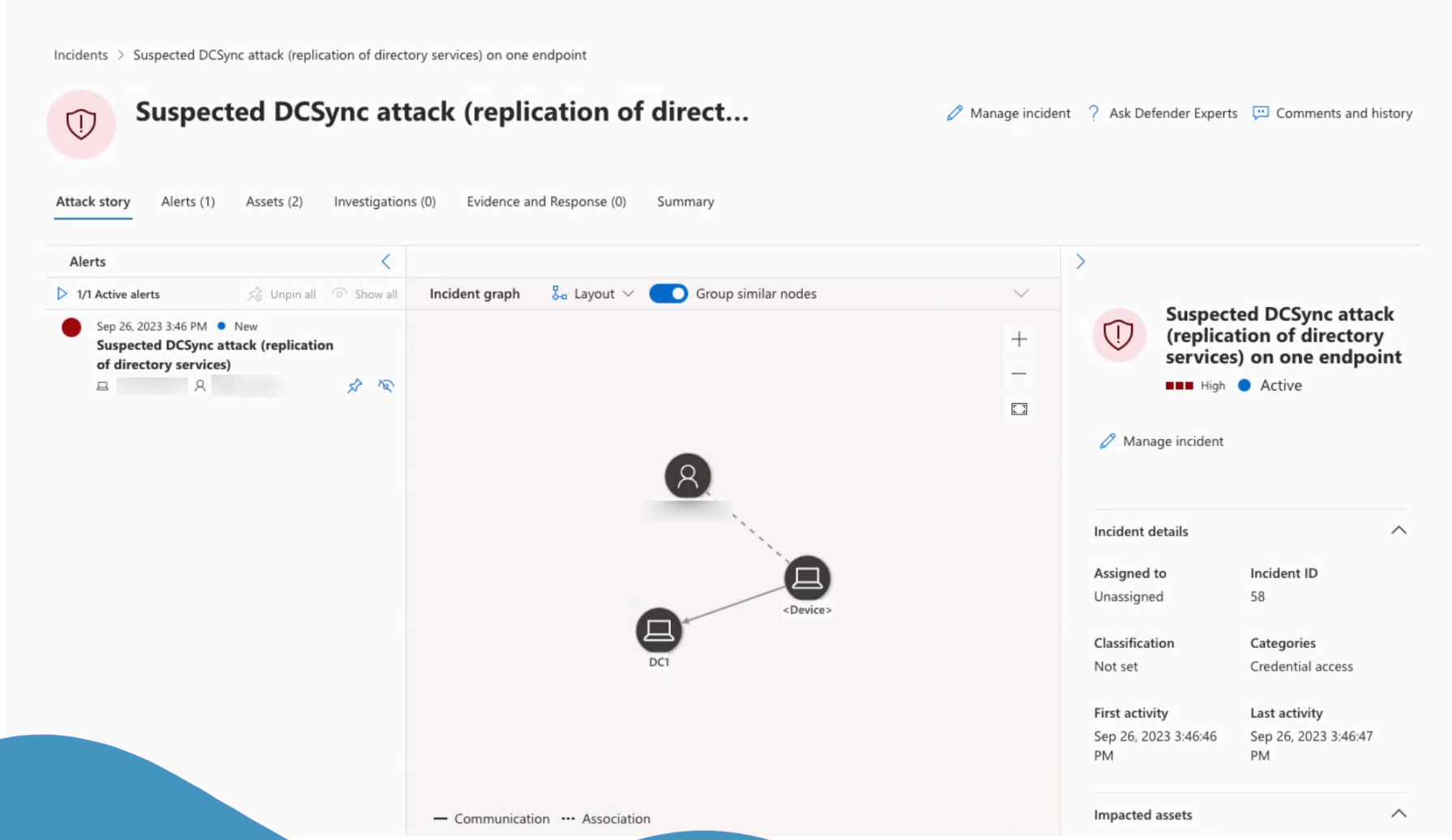
- DEMYSTIFICATION OF NETSYNC
- PRACTICAL APPLICATIONS FOR ATTACKERS & DEFENDERS
- NETSYNC > DCSYNC

- ANY TECHNIQUE CAN BE DETECTED WHEN BEING LOOKED FOR
- AVOID "SYNCING" CREDENTIALS FROM A DC WOULD BE PREFERABLE IF POSSIBLE
- HAVING THE ABILITY TO USE DIFFERENT TECHNIQUES TO ACHIEVE THE SAME GOAL

F#*$ U, DCSYNC

- DCSYNC TARGETS WINDOWS AD DOMAIN CONTROLLERS
- ENABLES ATTACKERS TO REPLICATE ALL OBJECTS' SECRETS
- POPULARITY HAS DIMINISHED ABILITY TO REMAIN UNDETECTED
- EASY TO DETECT W/ WINDOWS EVENTS, NETWORK TRAFFIC, MDI/CROWDSTRIKE IDP, ETC.
- POOR OPSEC:
  - REPLICATING ALL VS. REPLICATING ONE
  - SOURCE OF REPLICATION

F#*$ U, DCSYNC



THANKS TO EDWIN DAVID (@ROOTSECDEV) FOR PROVIDING THIS SCREENSHOT


NETSYNC 101

NETSYNC – "THE CASTRATED DCSYNC"

"SOME WILL SAY IT'S A CASTRATED DCSYNC, SOME WILL SAY IT'S ENOUGH TO PLAY WITH SILVER TICKETS ;)."
– BENJAMIN DELPY (@GENTILKIWI)

- ALSO TARGETS ACTIVE DIRECTORY DOMAIN CONTROLLERS
- USES PROTOCOL DIFFERENT FROM DCSYNC
- FIRST COMMITTED TO MIMIKATZ IN MAY 2016
- POC: ENABLES REPLICATION OF ONLY COMPUTER SECRETS (OR SO WE INITIALLY THOUGHT?)
- MINIMAL EXPOSURE: TWEET BY @GENTILKIWI IN APRIL 2019 & BLOGS BY ANDREW IN OCTOBER 2020

DELPY'S NETSYNC IMPLEMENTATION HIGH LEVEL PROTOCOL BREAKDOWN

CLIENT

SMB2 (PIPE\NETLOGON)

DCERPC (BIND CALL/ACK)

MS-NRPC - SECURE CHANNEL

DOMAIN CONTROLLER

DELPY'S NETSYNC IMPLEMENTATION BREAKDOWN I

MS-NRPC - SECURE CHANNEL ESTABLISHMENTS & MAINTENANCE

CLIENT

CLIENT REQUESTS (AND BINDS) TO THE TARGET DOMAIN CONTROLLER

CLIENT/SERVER NEGOTIATE A SECRET FOR ENCRYPTED COMMUNICATION

CLIENT IS AUTHENTICATED AND REQUESTS TRUST INFORMATION

DOMAIN CONTROLLER RETURNS THE NTLM HASHES IN THE RESPONSE

DOMAIN CONTROLLER

DELPY'S NETSYNC IMPLEMENTATION BREAKDOWN 2

MS-NRPC - SECURE CHANNEL ESTABLISHMENTS & MAINTENANCE

CLIENT

LOGONSRV_HANDLE

NETLOGON_CREDENTIAL

NETLOGON_AUTHENTICATOR

NETLOGON SECURE CHANNEL

DOMAIN CONTROLLER

DELPY'S NETSYNC IMPLEMENTATION BREAKDOWN 3

MS-NRPC - SECURE CHANNEL ESTABLISHMENTS & MAINTENANCE

NETRSERVERREQCHALLENGE REQUEST

CLIENT

DOMAIN CONTROLLER

ORIGINAL ART BY
@CARLOS_PEREZ

DELPY'S NETSYNC IMPLEMENTATION BREAKDOWN 3

MS-NRPC - SECURE CHANNEL ESTABLISHMENTS & MAINTENANCE

NETRSERVERREQCHALLENGE REQUEST

NETRSERVERREQCHALLENGE RESPONSE

CLIENT

DOMAIN CONTROLLER

ORIGINAL ART BY
@CARLOS_PEREZ

DELPY'S NETSYNC IMPLEMENTATION BREAKDOWN 3

MS-NRPC - SECURE CHANNEL ESTABLISHMENTS & MAINTENANCE

NETRSERVERREQCHALLENGE REQUEST

NETRSERVERREQCHALLENGE RESPONSE

NETRSERVERAUTHENTICATE2 REQUEST

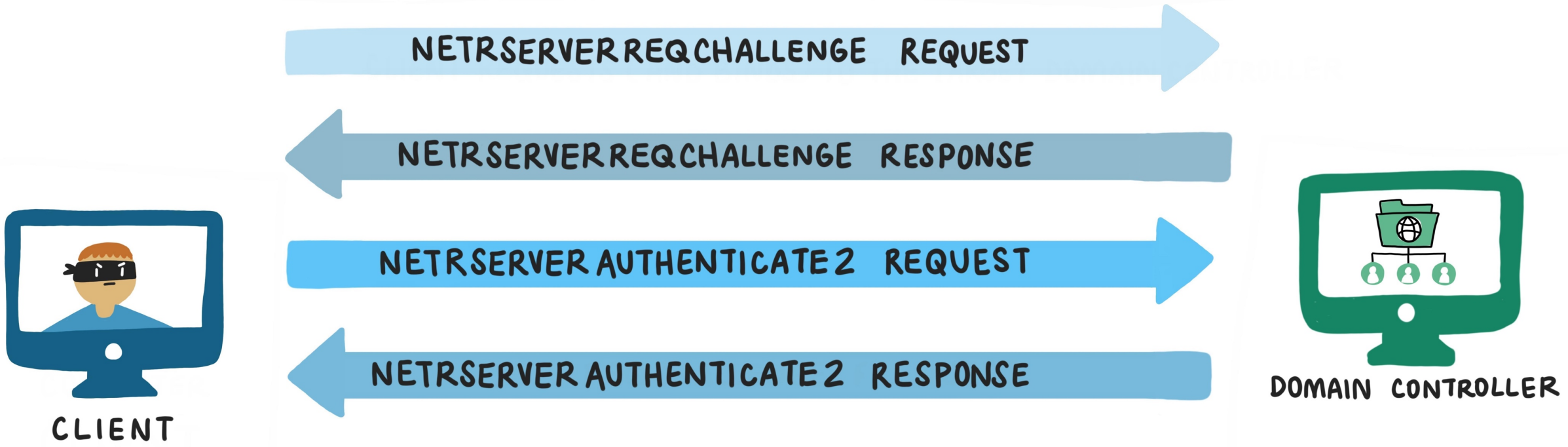
CLIENT

DOMAIN CONTROLLER

ORIGINAL ART BY
@CARLOS_PEREZ

DELPY'S NETSYNC IMPLEMENTATION BREAKDOWN 3

MS-NRPC - SECURE CHANNEL ESTABLISHMENTS & MAINTENANCE



ORIGINAL ART BY
@CARLOS_PEREZ

DELPY'S NETSYNC IMPLEMENTATION BREAKDOWN 3

MS-NRPC - SECURE CHANNEL ESTABLISHMENTS & MAINTENANCE

CLIENT

NETRSERVERREQCHALLENGE REQUEST

NETRSERVERREQCHALLENGE RESPONSE

NETRSERVER AUTHENTICATE2 REQUEST

NETRSERVER AUTHENTICATE2 RESPONSE

NETRSERVER TRUST PASSWORDS GET REQUEST

DOMAIN CONTROLLER

ORIGINAL ART BY
@CARLOS_PEREZ

DELPY'S NETSYNC IMPLEMENTATION BREAKDOWN 3

MS-NRPC - SECURE CHANNEL ESTABLISHMENTS & MAINTENANCE

CLIENT

NETRSERVERREQCHALLENGE REQUEST

NETRSERVERREQCHALLENGE RESPONSE

NETRSERVER AUTHENTICATE2 REQUEST

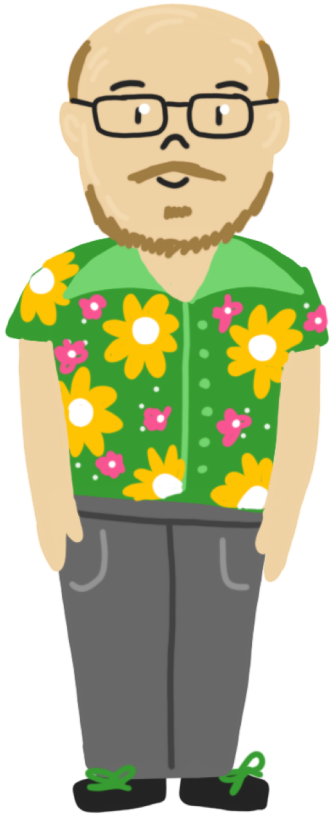
NETRSERVER AUTHENTICATE2 RESPONSE

NETRSERVER TRUSTPASSWORDSGET REQUEST

NETRSERVER TRUSTPASSWORDSGET RESPONSE

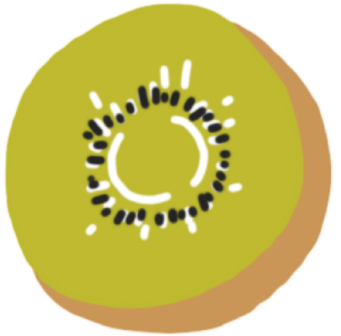
DOMAIN CONTROLLER

ORIGINAL ART BY
@CARLOS_PEREZ



NETSYNC

WITH MIMIKATZ




mimikatz 2.2.0 x64 (oe.eo)
mimikatz #

HOW MSFT BROKE NETSYNC

- INADVERTENTLY BROKE DELPY'S POC DURING ZEROLOGON PATCH RELEASE IN FEB 2021
- PATCH FORCED PACKET PRIVACY/INTEGRITY CONNECTION BETWEEN CLIENT AND DC

NETSYNC

BROKEN MIMIKATZ

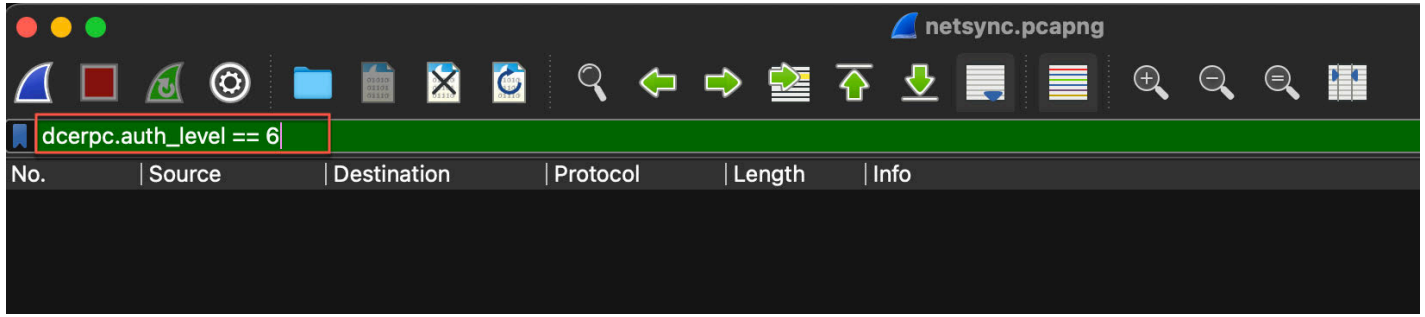

mimikatz 2.2.0 x64 (oe.eo)
mimikatz #

BUILDING A NEW NETSYNC

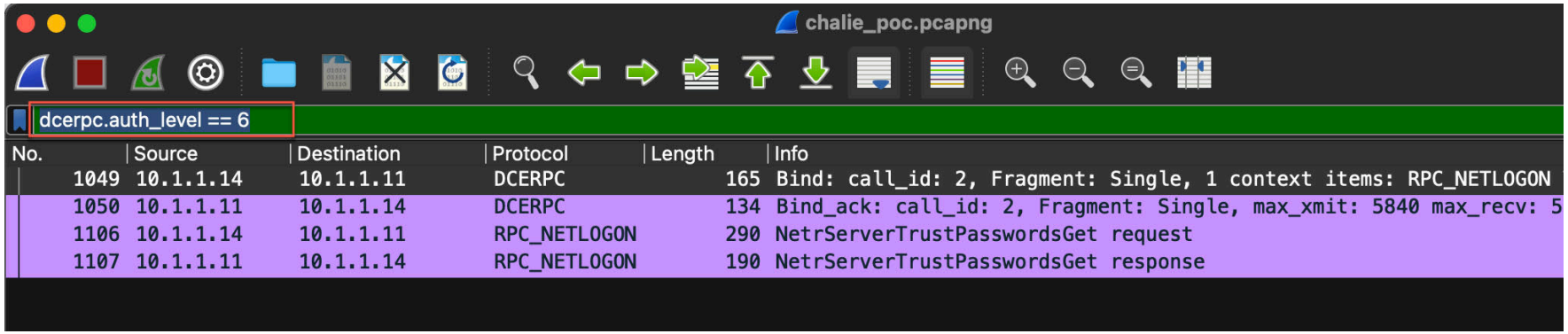
HOW CHARLIE RE-WORKED NETSYNC

- CREATED A NEW POC
- NEW POC FORCES PACKET PRIVACY ON CREDENTIAL RETRIEVAL
- MAKES USE OF AUTH LEVEL 6 - RPC_C_AUTHN_LEVEL_PKT_PRIVACY

HOW CHARLIE RE-WORKED NETSYNC

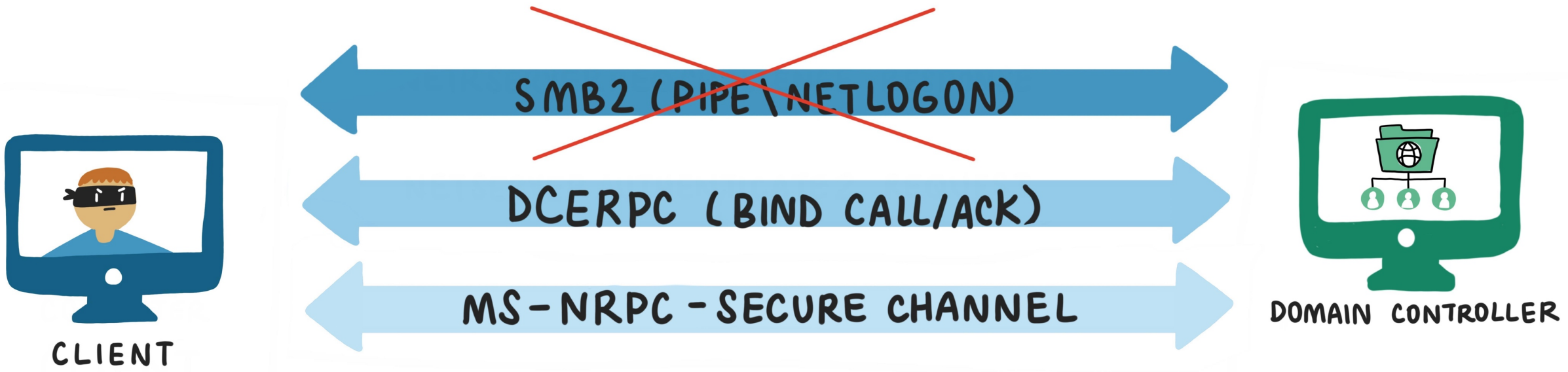


DELPY'S ORIGINAL MIMIKATZ POC

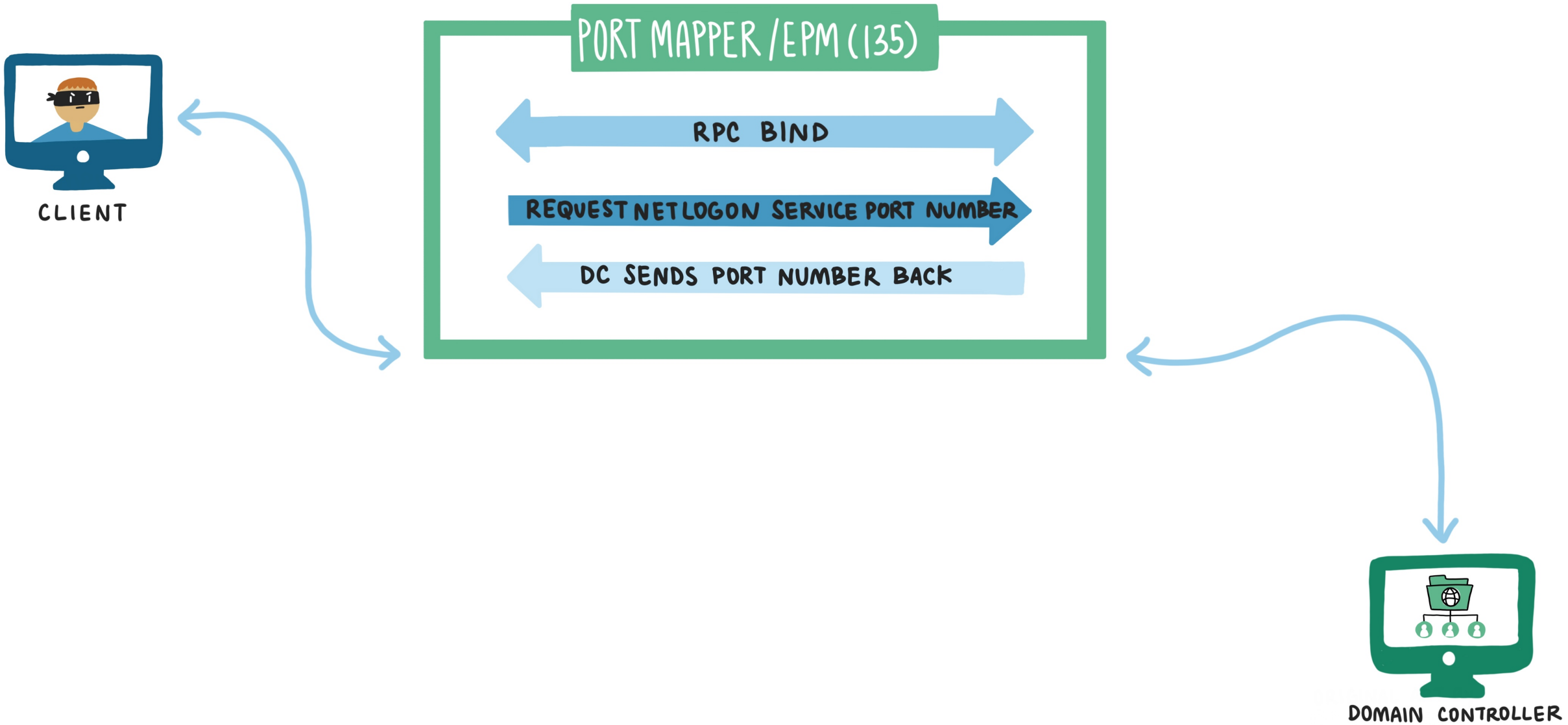


CHARLIE'S NEW POC

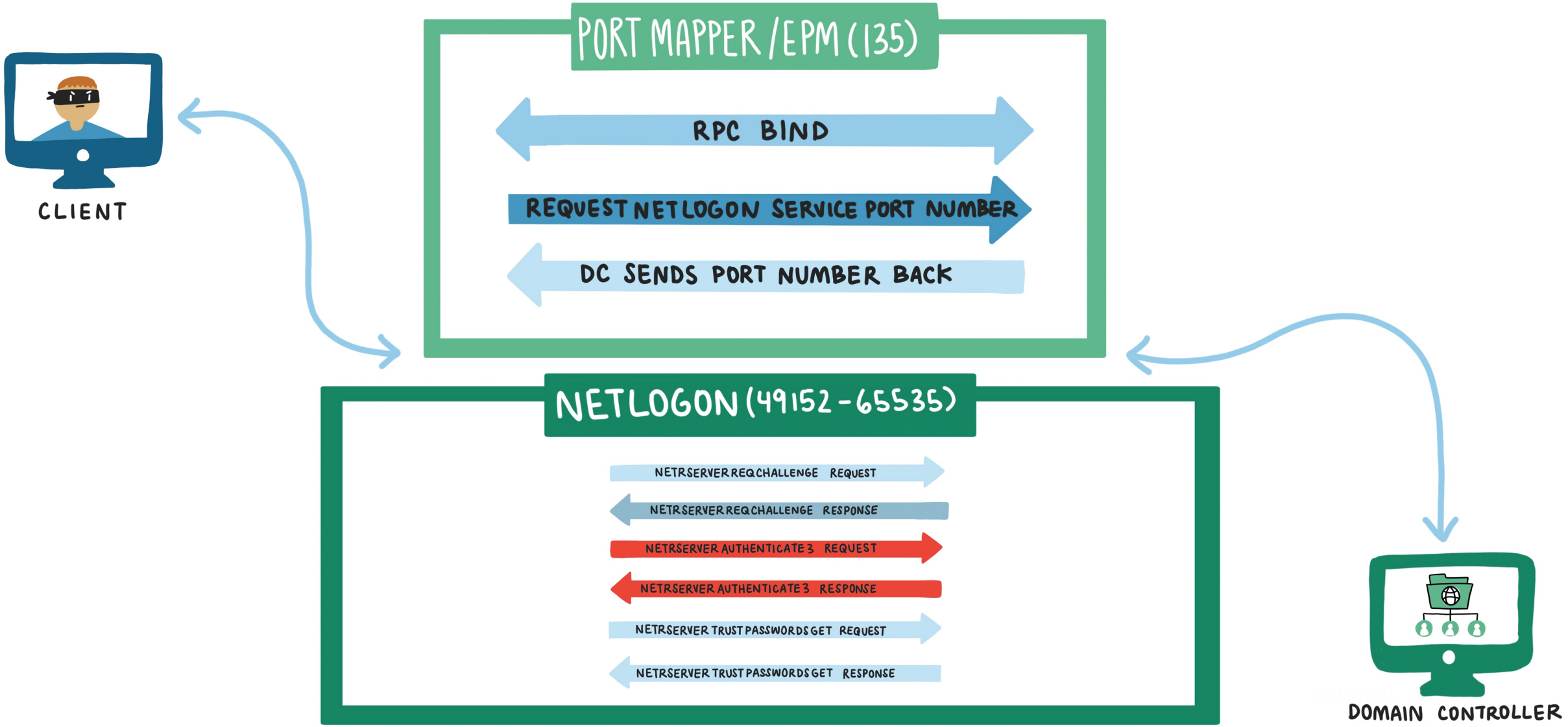
CHARLIE'S NETSYNC IMPLEMENTATION HIGH LEVEL PROTOCOL BREAKDOWN



CHARLIE'S NETSYNC IMPLEMENTATION BREAKDOWN



CHARLIE'S NETSYNC IMPLEMENTATION BREAKDOWN



CHARLIE'S NETSYNC IMPLEMENTATION BREAKDOWN

CLIENT

PORT MAPPER / EPM (135)

RPC BIND

REQUEST NETLOGON SERVICE PORT NUMBER

DC SENDS PORT NUMBER BACK

NETLOGON (49152 - 65535)

TWO RPC BIND CALL/ACK(S) OCCUR PRIOR TO AUTHENTICATION & CREDENTIAL RETRIEVAL

- NETRSERVERREQCHALLENGE REQUEST
- NETRSERVERREQCHALLENGE RESPONSE
- NETRSERVER AUTHENTICATE 3 REQUEST
- NETRSERVER AUTHENTICATE 3 RESPONSE
- NETRSERVER TRUST PASSWORDS GET REQUEST
- NETRSERVER TRUST PASSWORDS GET RESPONSE

DOMAIN CONTROLLER

CHARLIE'S NETSYNC IMPLEMENTATION BREAKDOWN

CLIENT

PORT MAPPER / EPM (135)

RPC BIND

REQUEST NETLOGON SERVICE PORT NUMBER

DC SENDS PORT NUMBER BACK

NETLOGON (49152 - 65535)

TWO RPC BIND CALL/ACK(S) OCCUR PRIOR TO AUTHENTICATION & CREDENTIAL RETRIEVAL

NETRSERVERREQCHALLENGE REQUEST

NETRSERVERREQCHALLENGE RESPONSE

NETRSERVER AUTHENTICATE 3 REQUEST

NETRSERVER AUTHENTICATE 3 RESPONSE

NETRSERVER TRUST PASSWORDS GET REQUEST

NETRSERVER TRUST PASSWORDS GET RESPONSE

PACKET PRIVACY

DOMAIN CONTROLLER

ORIGINAL POC VS. NEW POC

API CALL	ATTACK USE CASE	CHARLIE'S POC	DELPY'S POC
NETRSERVERTRUSTPASSWORDSGET	GETTING NT HASH OF ANY "TRUST" ACCOUNT IN THE DOMAIN	Y	Y
NETRSERVERPASSWORDGET		Y	N
NETRSERVERGETTRUSTINFO		Y	N

- THE AUTHENTICATE API CALL IS IRRELEVANT, IT IS THE CALL ABOVE THAT RETRIEVES THE CREDENTIAL

…THAT IS "NETSYNC"

USER ACCOUNT CONTROL (UAC) CAVEATS

INTERDOMAIN_TRUST_ACCOUNT	2048
WORKSTATION_TRUST_ACCOUNT	4096
SERVER_TRUST_ACCOUNT	8192

- UAC VALUES DETERMINE WHAT CAN BE NETSYNCED
- ANY AD OBJECT USING THESE UAC VALUES CAN BE NETSYNCED
- 8192 ALLOWS NETSYNCING OF ANY ACCOUNT (A:X)
- 2048 OR 4096 LIMITS TO SAME ACCOUNT NETSYNCING (A:A)

UAC TRICKS ☺

- IF YOU CHANGE NORMAL USER ACCOUNT TO BE A WORKSTATION_TRUST_ACCOUNT, THEN YOU CAN NETSYNC IT
- IF YOU CHANGE WORKSTATION_TRUST_ACCOUNT TO BE A SERVER_TRUST_ACCOUNT, THEN YOU CAN USE IT TO NETSYNC OTHER ACCOUNTS
  - THE PRIMARY GROUP AUTOMATICALLY CHANGES TO DOMAIN CONTROLLERS (516)

CHARLIE'S NETSYNC POC


Administrator: Command Prompt
C:\OffensiveAdmin>

GOLDEN NETSYNC

GOLDEN NETSYNC – THE TRUST KEY

- AN ALTERNATIVE TO TOUCHING KRBTGT
- ENCRYPTED WITH TRUST KEY AND NOT KRBTGT. LIKE A GOLDEN TICKET BUT NOT. FOR A LOCAL USER, JUST AS POWERFUL AS A LOCAL TGT (MAKES NO DIFFERENCE)
- FOR INTRA – FORREST
    1) FORGE A REFERRAL WITH THE TRUST KEY
    2) USE THAT REFERRAL TO GET A REFERRAL BACK
    3) REFERRAL FOR LOCAL USER TO REQUEST STs (AS GENUINE AS A LOCAL TGT)

INTRA-FOREST

SERVICE TICKET

REFERRAL TO LOCAL

FORGED REFERRAL

LOCAL DOMAIN CONTROLLER
EARTH-DC.MARVEL.LOCAL

CLIENT

LOCAL FILE SERVER
XANDAR-FS.MARVEL.LOCAL

FOREIGN DOMAIN CONTROLLER
EARTH2012-CHILD.QUANTUMREALM.MARVEL.LOCAL

SERVICE TICKET

REFERRAL TO LOCAL

FORGED REFERRAL

LOCAL FILE SERVER
XANDAR-FS.MARVEL.LOCAL

LOCAL DOMAIN CONTROLLER
EARTH-DC.MARVEL.LOCAL

NETSYNC TRUST KEY

CLIENT

FOREIGN DOMAIN CONTROLLER
EARTH2012-CHILD.QUANTUMREALM.MARVEL.LOCAL

SERVICE TICKET

REFERRAL TO LOCAL

FORGED REFERRAL

LOCAL FILE SERVER
XANDAR-FS.MARVEL.LOCAL

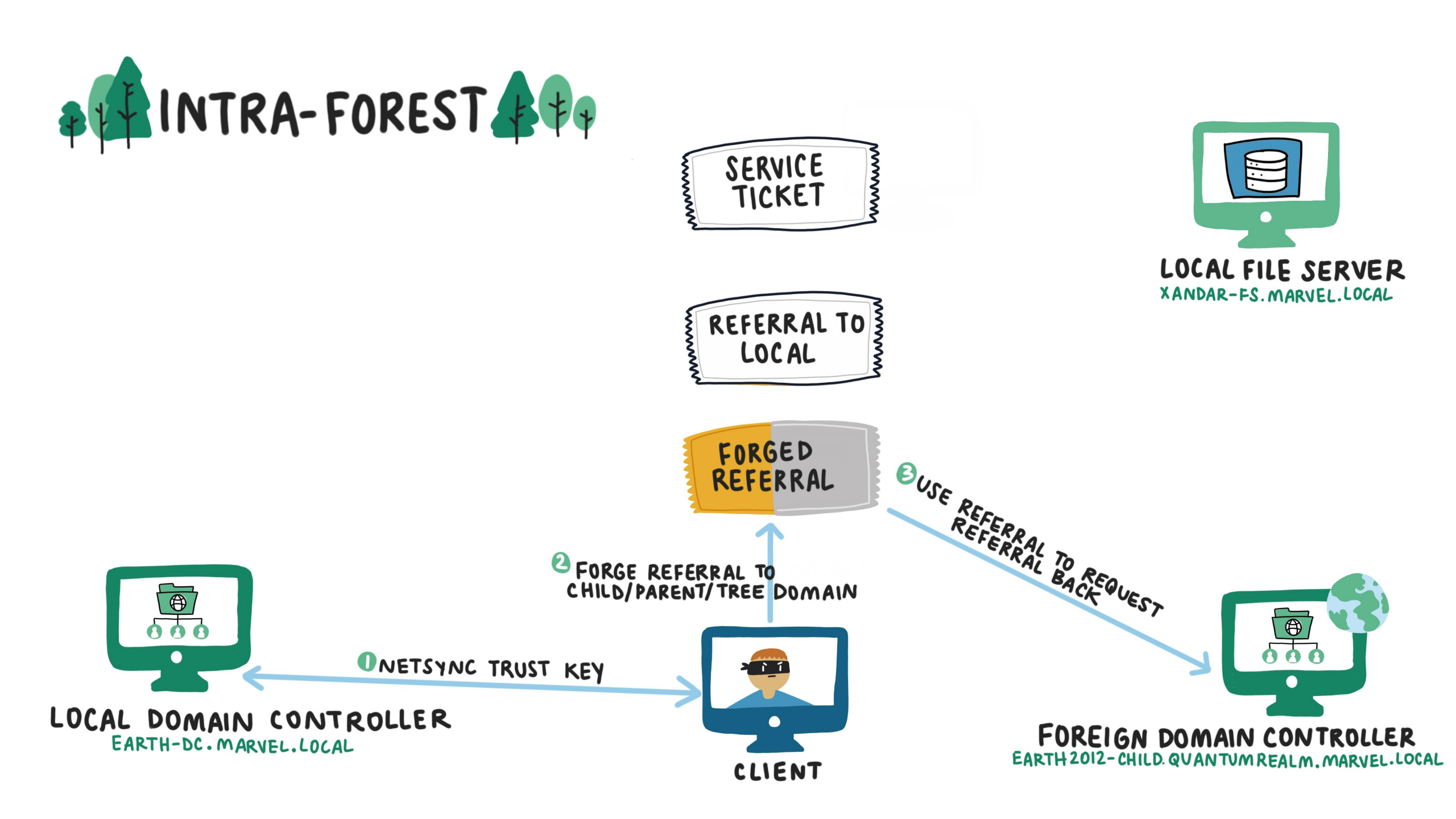
2 FORGE REFERRAL TO CHILD/PARENT/TREE DOMAIN

1 NETSYNC TRUST KEY

LOCAL DOMAIN CONTROLLER
EARTH-DC.MARVEL.LOCAL

CLIENT

FOREIGN DOMAIN CONTROLLER
EARTH2012-CHILD.QUANTUMREALM.MARVEL.LOCAL


INTRA-FOREST
SERVICE TICKET
REFERRAL TO LOCAL
FORGED REFERRAL
LOCAL FILE SERVER
XANDAR-FS.MARVEL.LOCAL
1 NETSYNC TRUST KEY
2 FORGE REFERRAL TO CHILD/PARENT/TREE DOMAIN
3 USE REFERRAL TO REQUEST REFERRAL BACK
LOCAL DOMAIN CONTROLLER
EARTH-DC.MARVEL.LOCAL
CLIENT
FOREIGN DOMAIN CONTROLLER
EARTH2012-CHILD.QUANTUMREALM.MARVEL.LOCAL

INTRA-FOREST

LOCAL FILE SERVER
XANDAR-FS.MARVEL.LOCAL

SERVICE TICKET

REFERRAL TO LOCAL

FORGED REFERRAL

4 RETRIEVE REFERRAL TO LOCAL DOMAIN

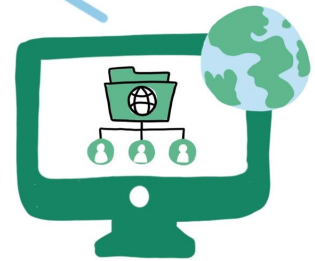
3 USE REFERRAL TO REQUEST REFERRAL BACK

2 FORGE REFERRAL TO CHILD/PARENT/TREE DOMAIN

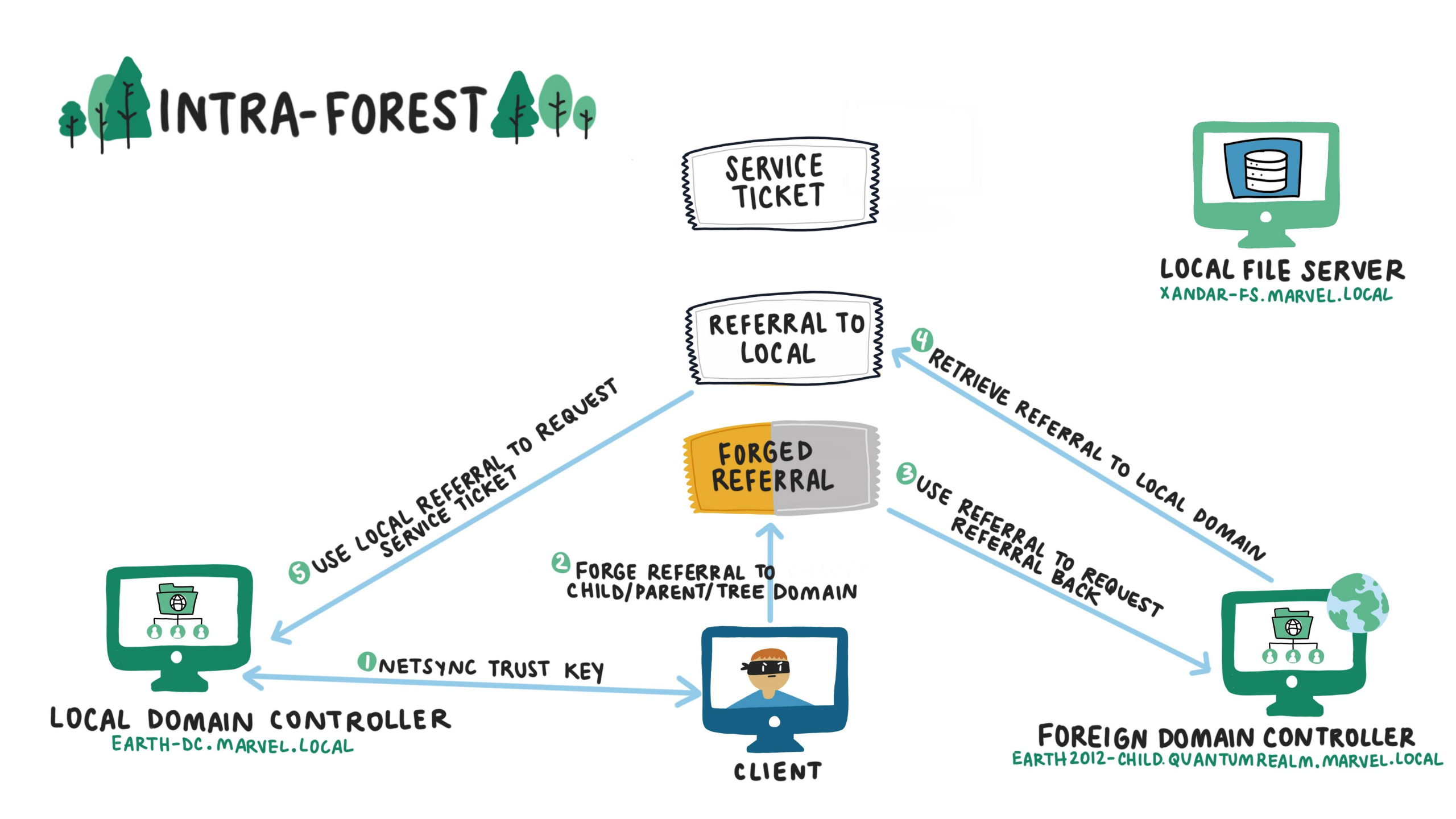
1 NETSYNC TRUST KEY

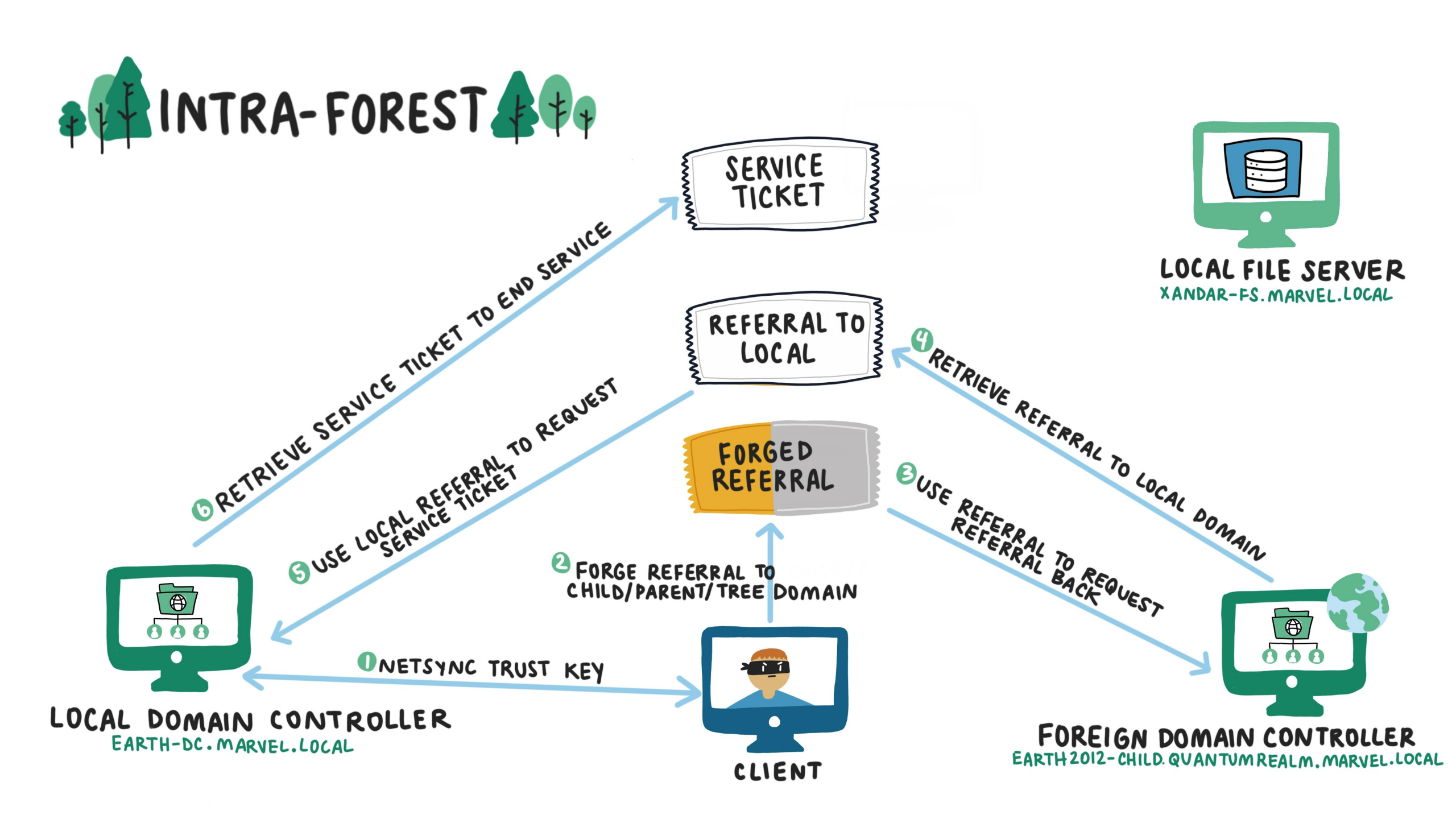
LOCAL DOMAIN CONTROLLER
EARTH-DC.MARVEL.LOCAL

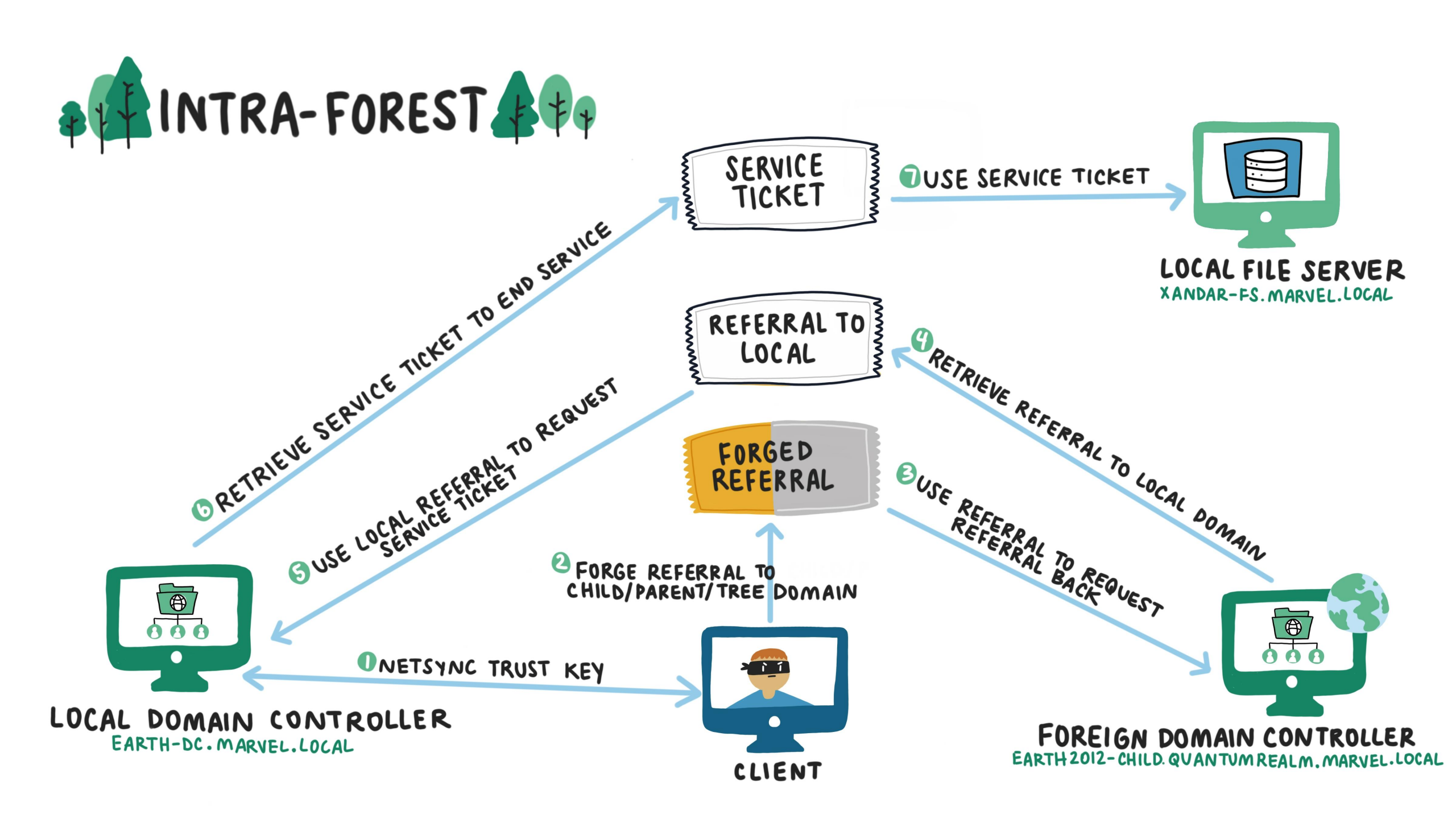
CLIENT



FOREIGN DOMAIN CONTROLLER
EARTH2012-CHILD.QUANTUMREALM.MARVEL.LOCAL


INTRA-FOREST
SERVICE TICKET
REFERRAL TO LOCAL
FORGED REFERRAL
LOCAL FILE SERVER
XANDAR-FS.MARVEL.LOCAL
4 RETRIEVE REFERRAL TO LOCAL DOMAIN
3 USE REFERRAL TO REQUEST REFERRAL BACK
5 USE LOCAL REFERRAL TO REQUEST SERVICE TICKET
2 FORGE REFERRAL TO CHILD/PARENT/TREE DOMAIN
1 NETSYNC TRUST KEY
LOCAL DOMAIN CONTROLLER
EARTH-DC.MARVEL.LOCAL
CLIENT
FOREIGN DOMAIN CONTROLLER
EARTH2012-CHILD.QUANTUMREALM.MARVEL.LOCAL


INTRA-FOREST
SERVICE TICKET
REFERRAL TO LOCAL
FORGED REFERRAL
LOCAL FILE SERVER
XANDAR-FS.MARVEL.LOCAL
6 RETRIEVE SERVICE TICKET TO END SERVICE
5 USE LOCAL REFERRAL TO REQUEST SERVICE TICKET
4 RETRIEVE REFERRAL TO LOCAL DOMAIN
3 USE REFERRAL TO REQUEST REFERRAL BACK
2 FORGE REFERRAL TO CHILD/PARENT/TREE DOMAIN
1 NETSYNC TRUST KEY
LOCAL DOMAIN CONTROLLER
EARTH-DC.MARVEL.LOCAL
CLIENT
FOREIGN DOMAIN CONTROLLER
EARTH2012-CHILD.QUANTUMREALM.MARVEL.LOCAL


INTRA-FOREST
SERVICE TICKET
7 USE SERVICE TICKET
LOCAL FILE SERVER
XANDAR-FS.MARVEL.LOCAL
REFERRAL TO LOCAL
4 RETRIEVE REFERRAL TO LOCAL DOMAIN
FORGED REFERRAL
3 USE REFERRAL TO REQUEST REFERRAL BACK
6 RETRIEVE SERVICE TICKET TO END SERVICE
5 USE LOCAL REFERRAL TO REQUEST SERVICE TICKET
2 FORGE REFERRAL TO CHILD/PARENT/TREE DOMAIN
1 NETSYNC TRUST KEY
LOCAL DOMAIN CONTROLLER
EARTH-DC.MARVEL.LOCAL
CLIENT
FOREIGN DOMAIN CONTROLLER
EARTH2012-CHILD.QUANTUMREALM.MARVEL.LOCAL

GOLDEN NETSYNC CAVEATS

- USED AS AN ALTERNATIVE TO A GOLDEN TICKET
- NO REQUIREMENT TO SYNC THE KRBTGT KEY
- SILVER TICKET WOULD BE MORE OPSEC

GOLDEN NETSYNC


Command Prompt
C:\Temp>
Activate Windows
Go to Settings to activate Windows.

NETSYNC TO THE CLOUD W/ AZUREADSSOACC$

NETSYNC W/ AZUREADSSOACC$

- ACCOUNT THAT ALLOWS FOR SSO BETWEEN ON – PREMISES & AZURE
- IS A **WORKSTATION_TRUST_ACCOUNT**, SO YOU CAN NETSYNC IT
- WITH THIS YOU CAN NOW PIVOT UP TO AZURE!

NETSYNC TO THE CLOUD W/ AZUREADSSOACC$

NETSYNC RED NOTES

NETSYNC OPSEC ADVANTAGES

- ALTERNATIVE TO HEAVILY MONITORED DCSYNC (TOTALLY DIFFERENT ATTACK USING DIFFERENT SUITE MS – DRSR VS MS – NRPC)
- NOT USING PIPE\NETLOGON (DELPY'S ORIGINAL POC)
- HARDER TO DETECT
- CURRENTLY MDI DOESN'T DETECT NETSYNC

GRAPHICS/SLIDES BY:

@MINDSEYECCF
MIND'S EYE
CREATIVE