RSA APJ SUMMIT
ENABLING BUSINESS DRIVEN SECURITY

THREAT DETECTION & RESPONSE

HOW A SMALLER SECURITY TEAM EFFECTIVELY FIGHTS MALWARE

Jae Yun, Cho(JY Cho)
Amorepacific

INTRODUCE

- Member of KUCIS(Korea University Clubs of Information Security)
- Worked at LG

  : CERT / IR / Penetration tester
- Working at Amorepacific

  : CERT / IR / Security Check / Security Monitoring and Planning

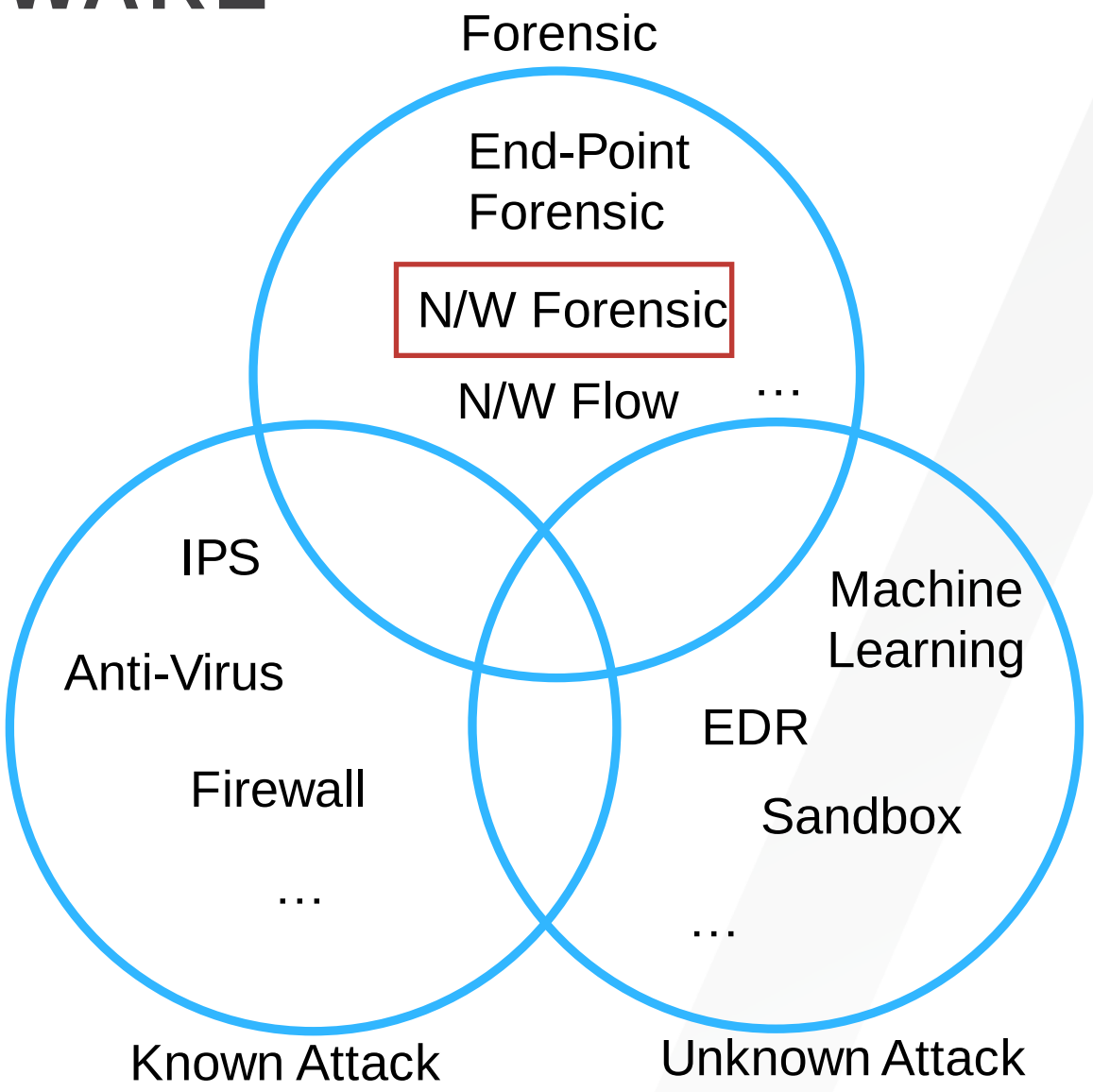
AMOREPACIFIC Sulwhasoo

LANEIGE Mamonde innisfree

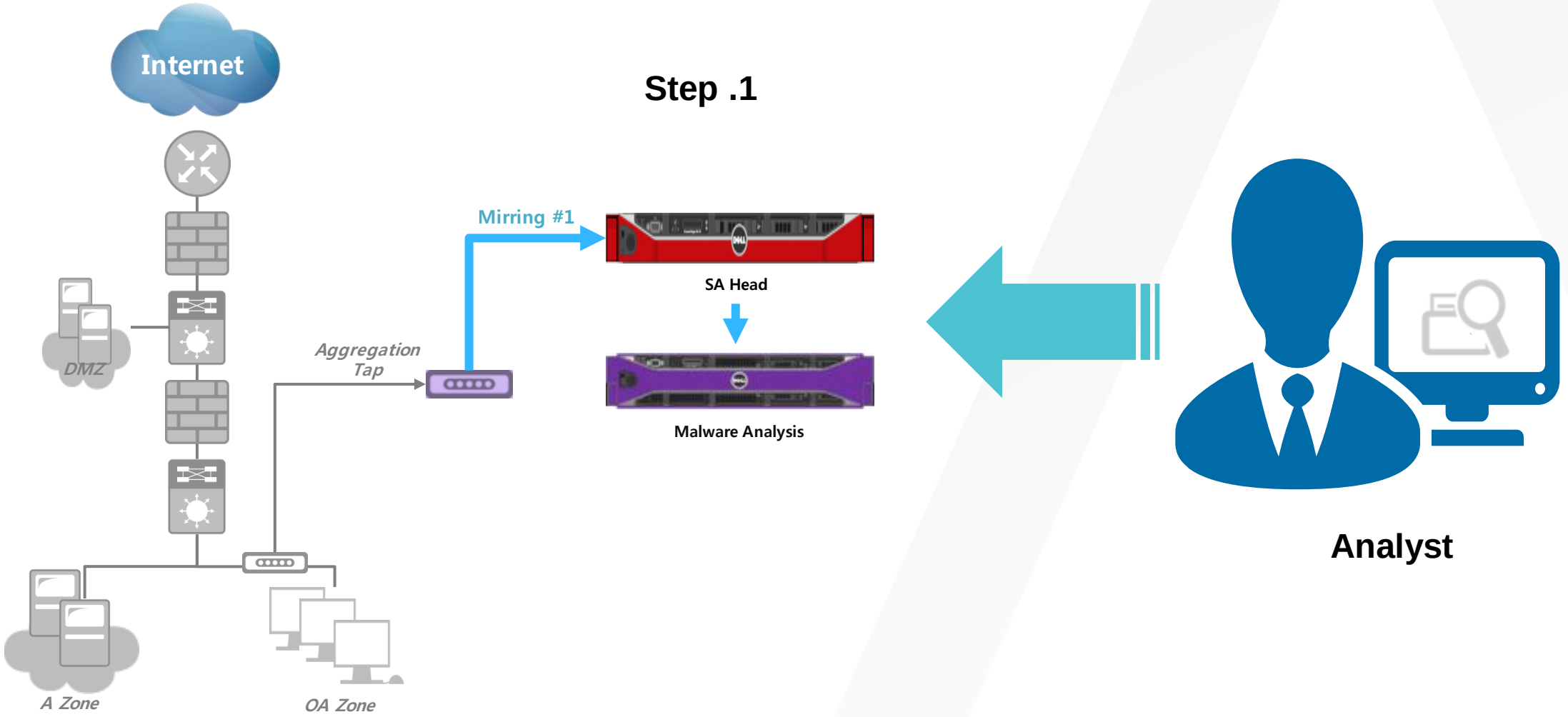
ETUDE HOUSE HERA IOPE

primera HANYUL LIRIKOS MARINE ENERGY

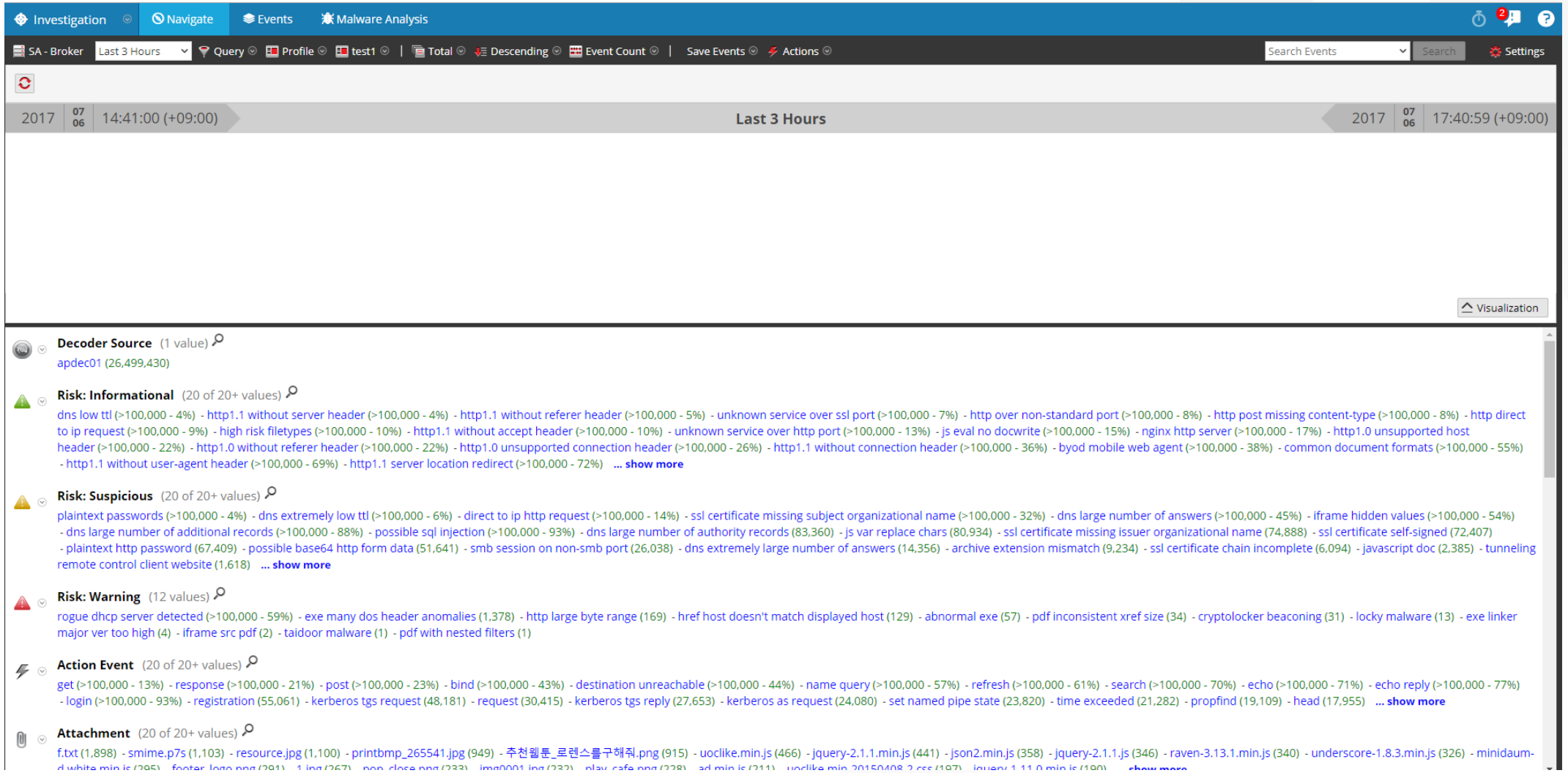
FIND A MALWARE



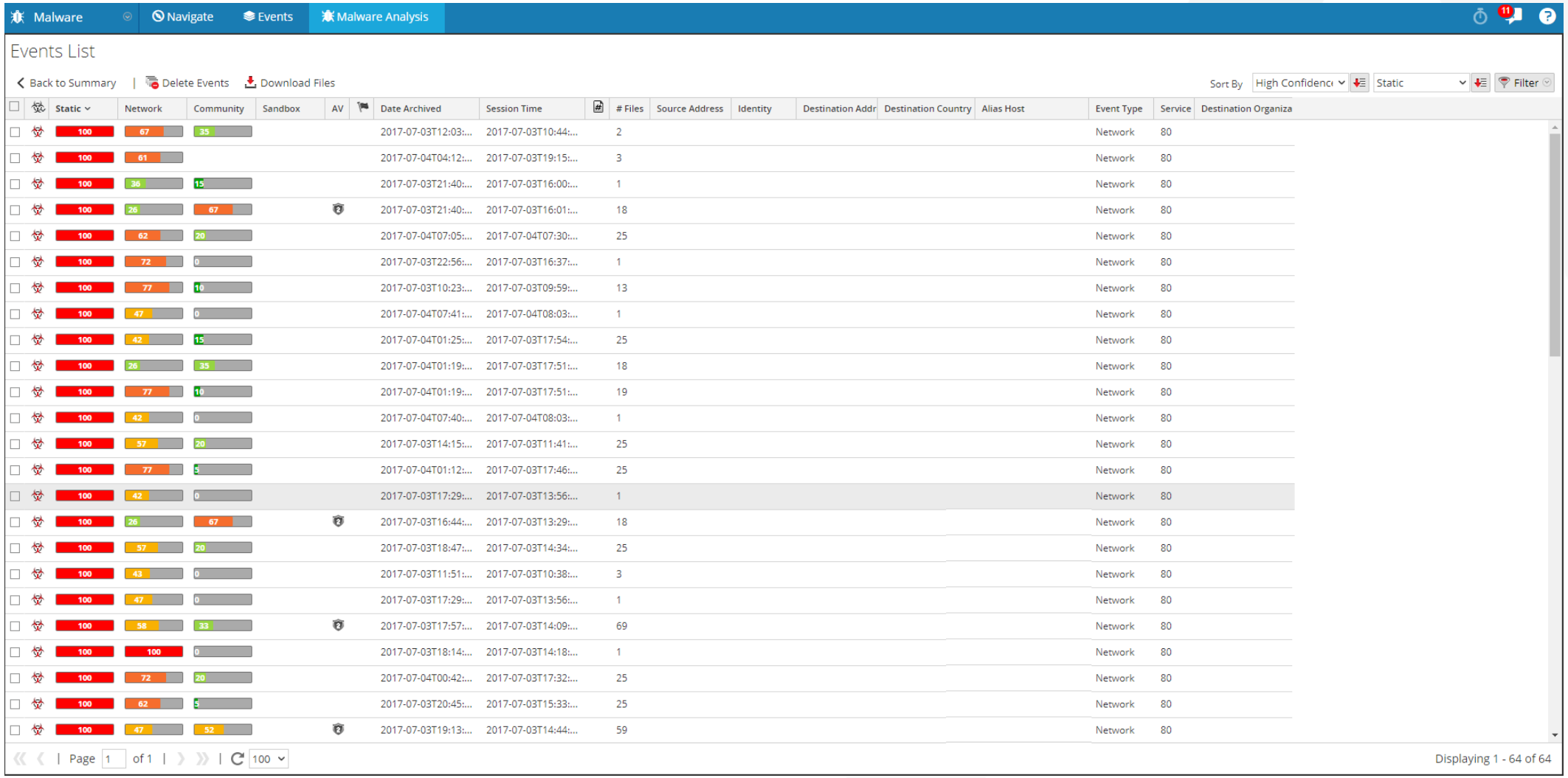
1ST ARCHITECTURE



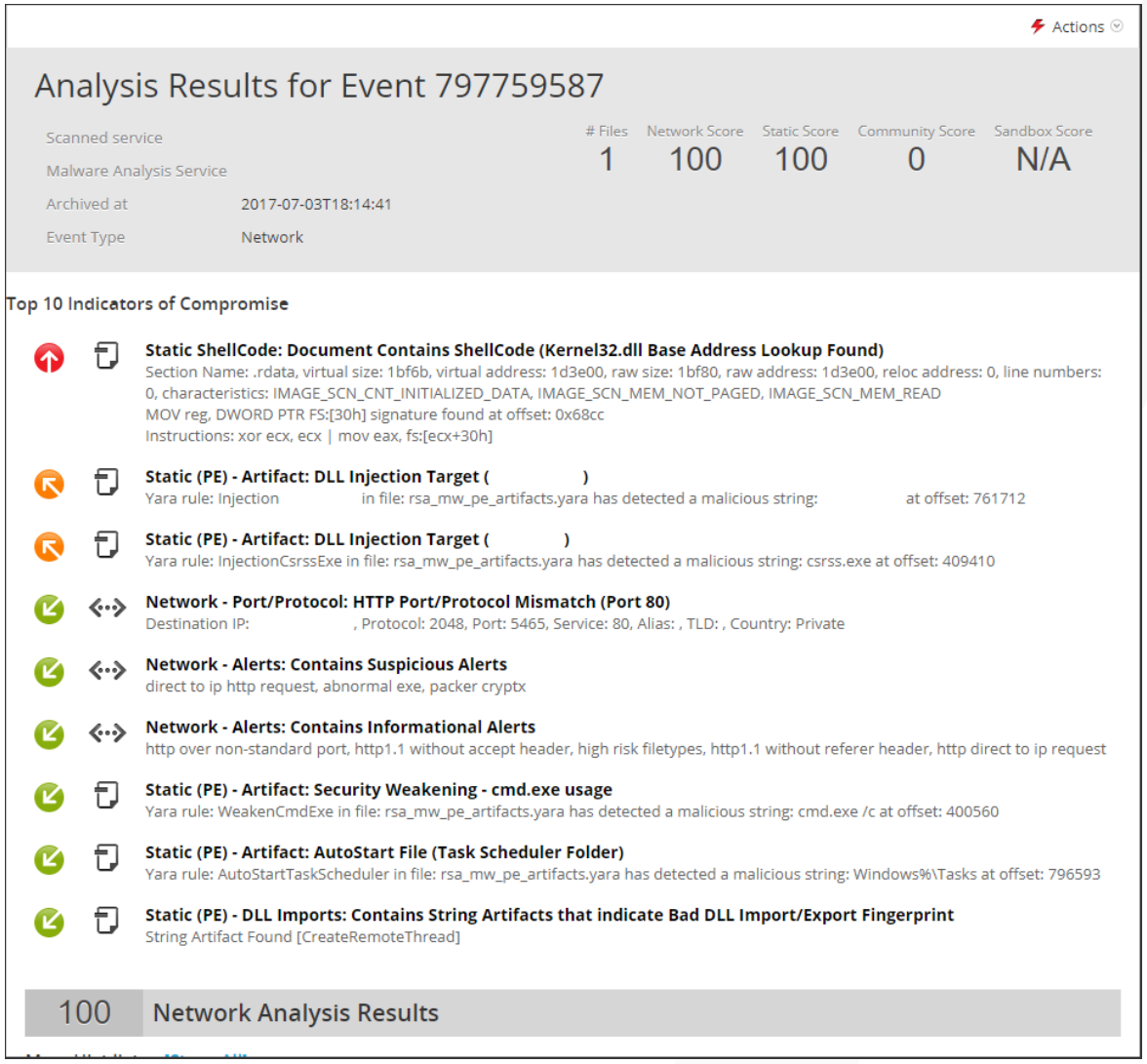
WORKING WITH NETWITNESS(SA)



WORKING WITH NETWITNESS(MA)



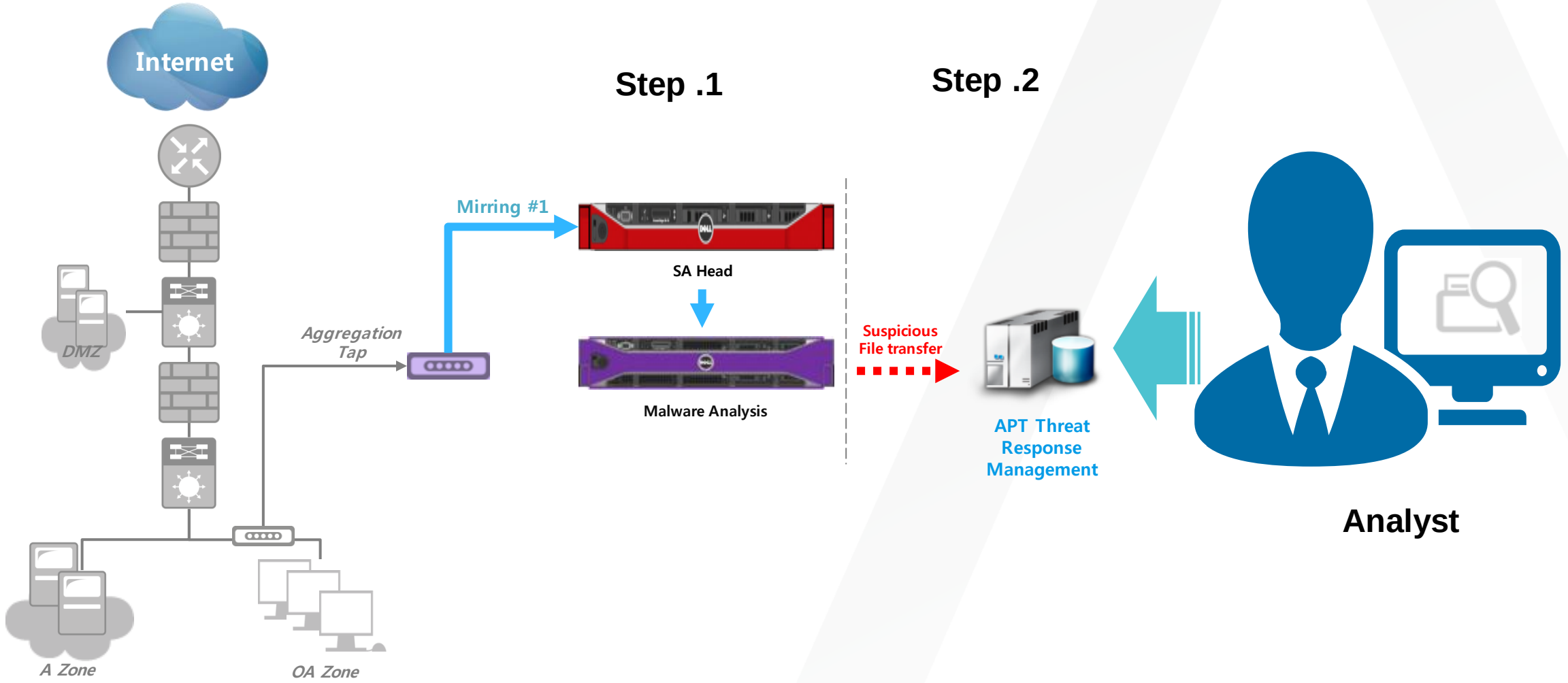
WORKING WITH NETWITNESS(MA)



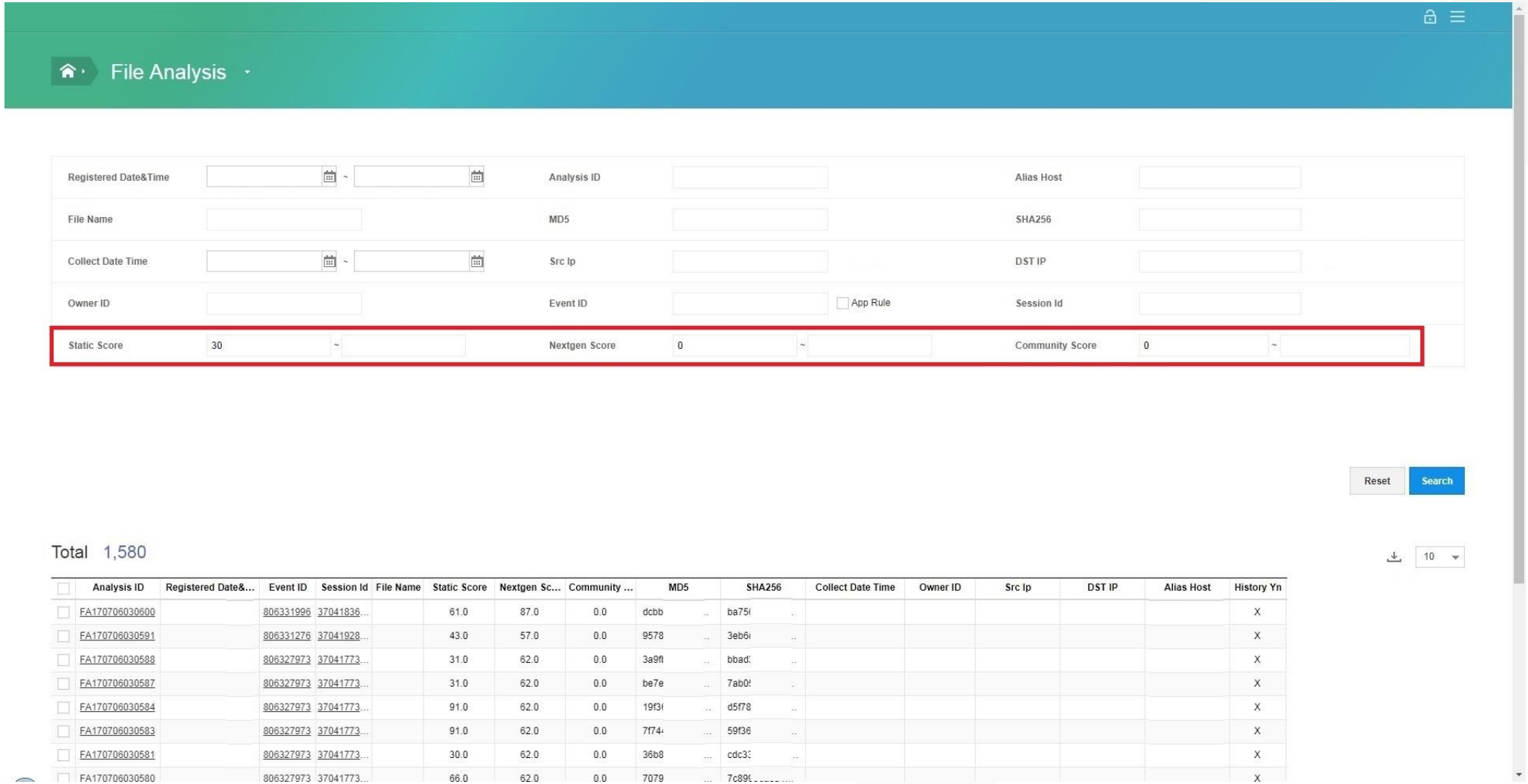
I NEED SOME MORE

- Effectiveness of NETWITNESS
- A little lack of function
- Process Needed for malware analysis

2ND ARCHITECTURE



WORKING WITH MIDDLEWARE

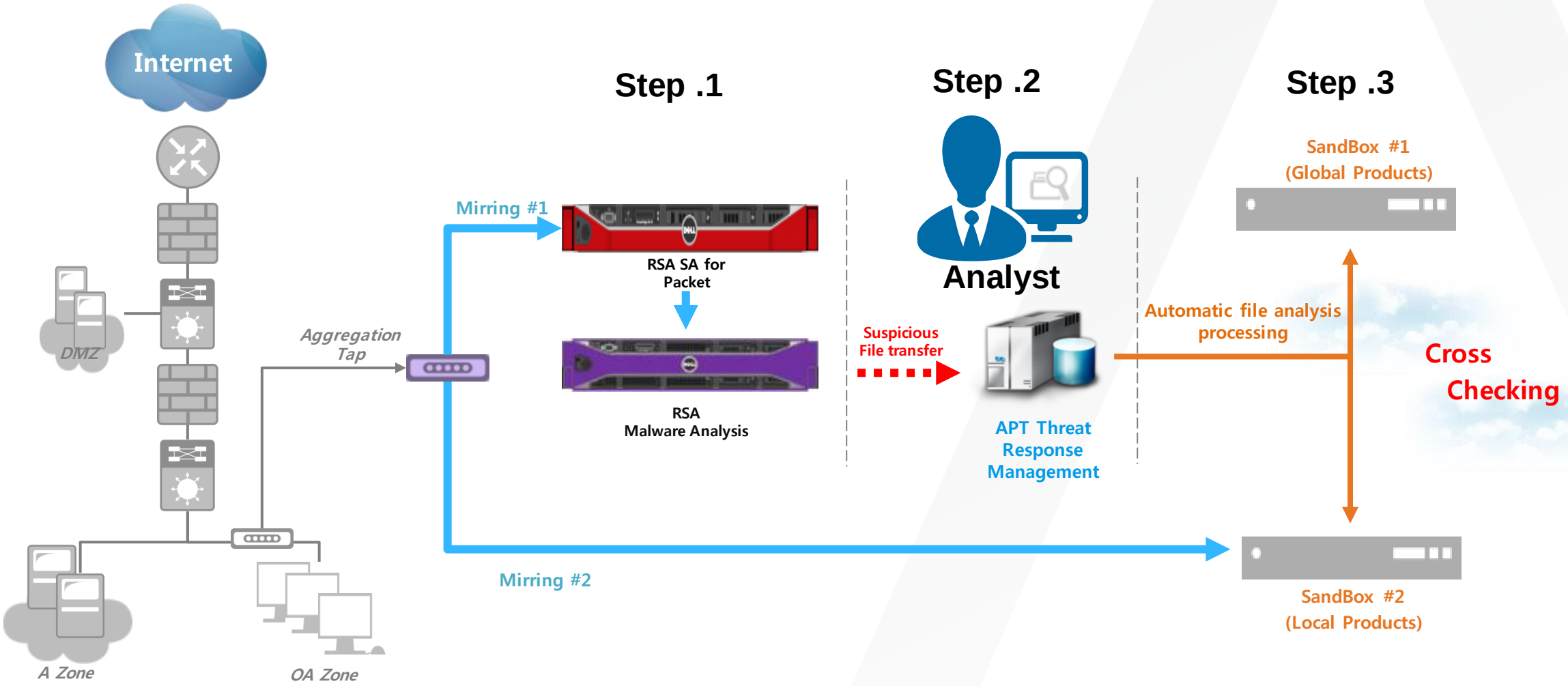


JOURNEY TO SPOTTING THE RIGHT MALWARE

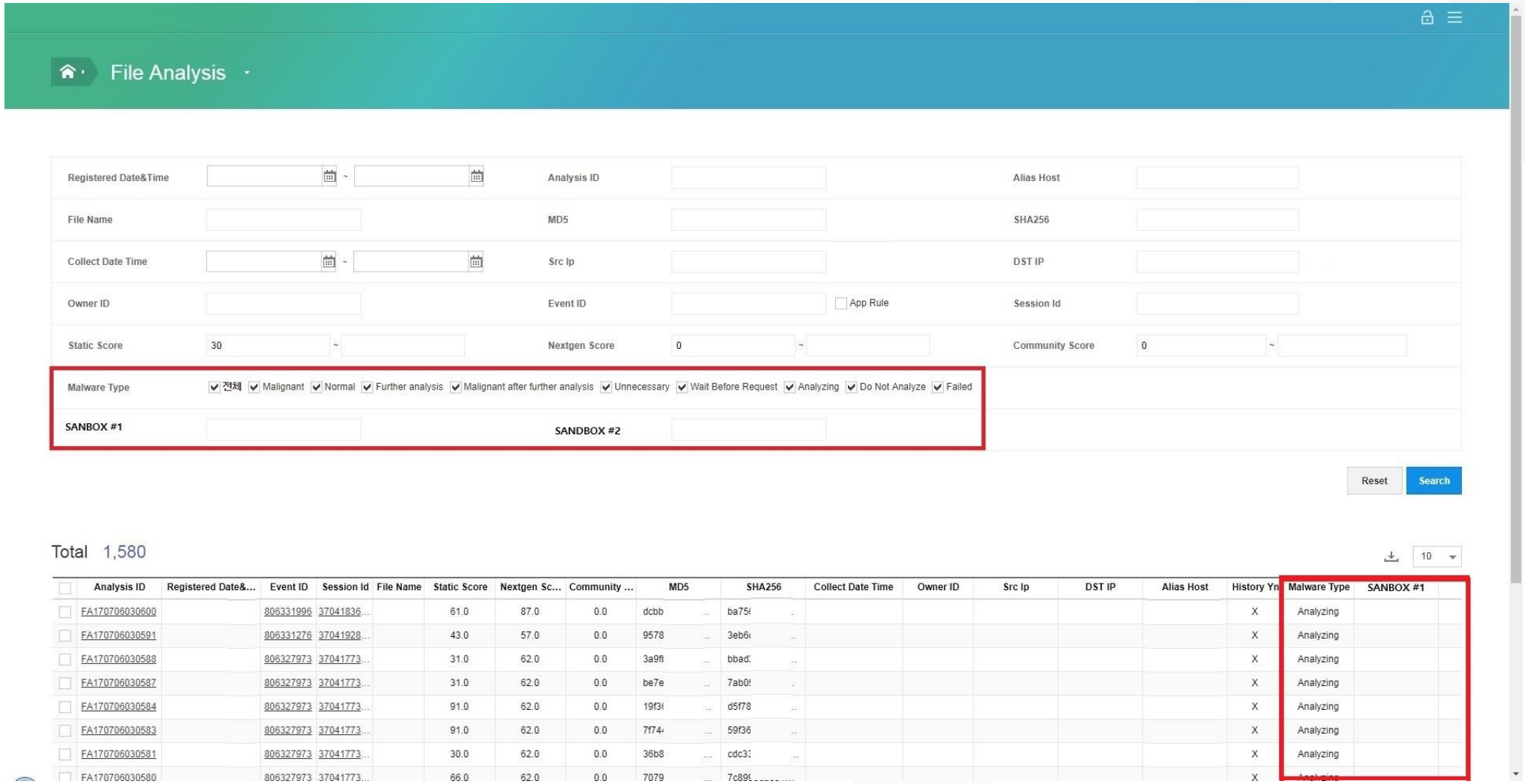
- Setting up standard for analysis

- Unexpected problems encountered
  - Increasing number of analysis target
  - Having difficulties of figuring out malwares
  - Lack of man power

3RD ARCHITECTURE



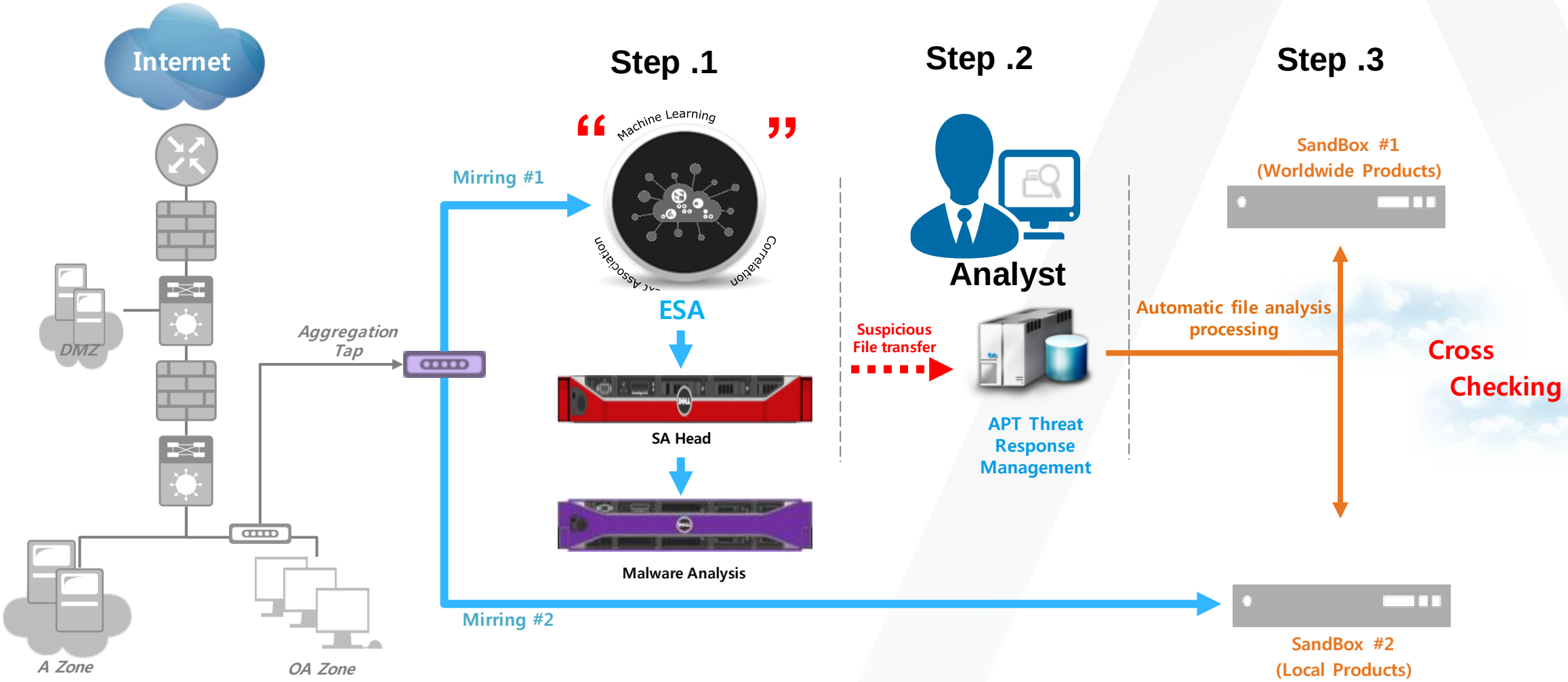
WORKING WITH SANDBOX



WORKING PROCESS STANDARD

- Sandboxing analysis of our setting up standard
- Traffic analysis of malwares
- Blocking a malware landing page / distribution page / waypoint page
- Infected PC block a network right off
- Infected PC re-install

IMPROVEMENT POINT



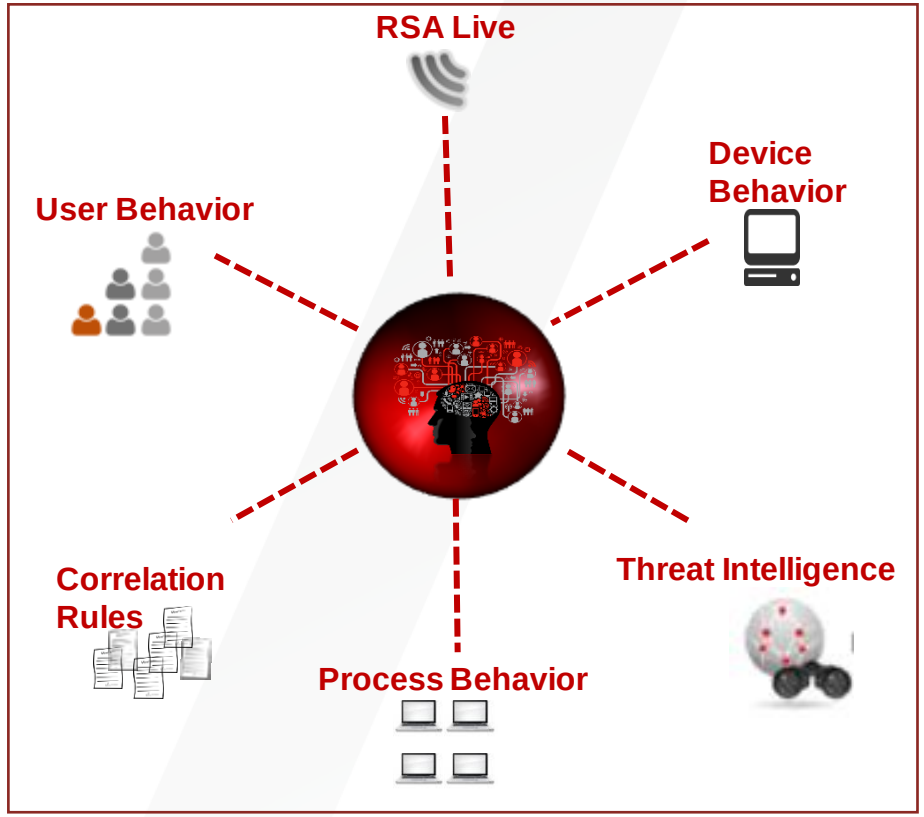
IMPROVEMENT POINT

USING RSA ESA DETECT BASE ON BEHAVIOR THREAT

USING MACHINE-LEARNING FIND A TRAFFIC THREAT IN QUICKLY

Detect of probable C&C traffic using ESA

ESA Helps detect an unknown attack in the initial phase of an attack



THINGS TO EXPECT FROM ESA

- Analysis of C&C traffic via SSL malwares
- Analysis of fileless malwares
- Analysis of infected PC
- Analysis of obfuscation traffic

RSA

APJ SUMMIT

ENABLING BUSINESS DRIVEN SECURITY

THANK YOU