



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*

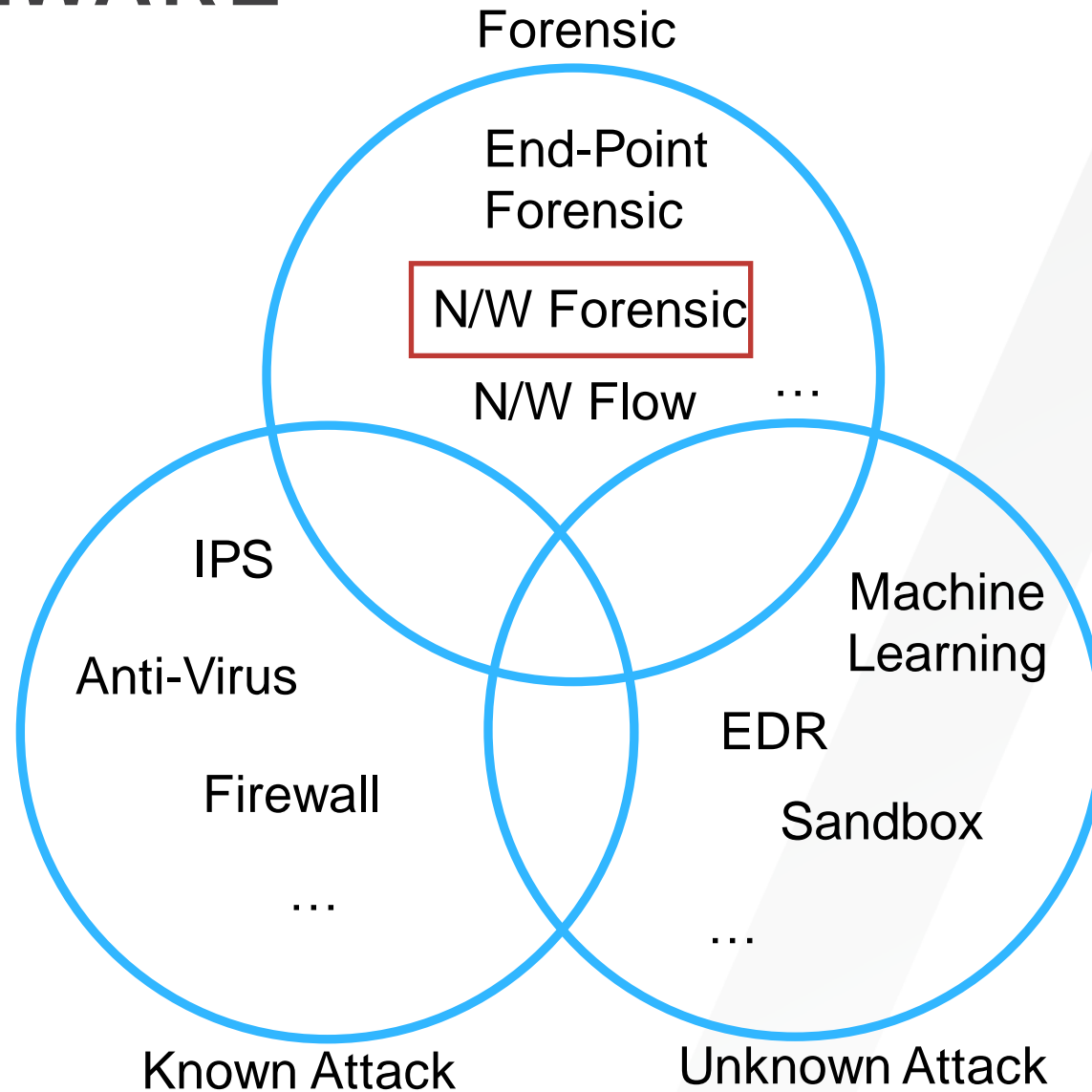
LANEIGE *Mamonde* *innisfree*

◆ *ETUDE HOUSE* ◆ H E R A IOPE

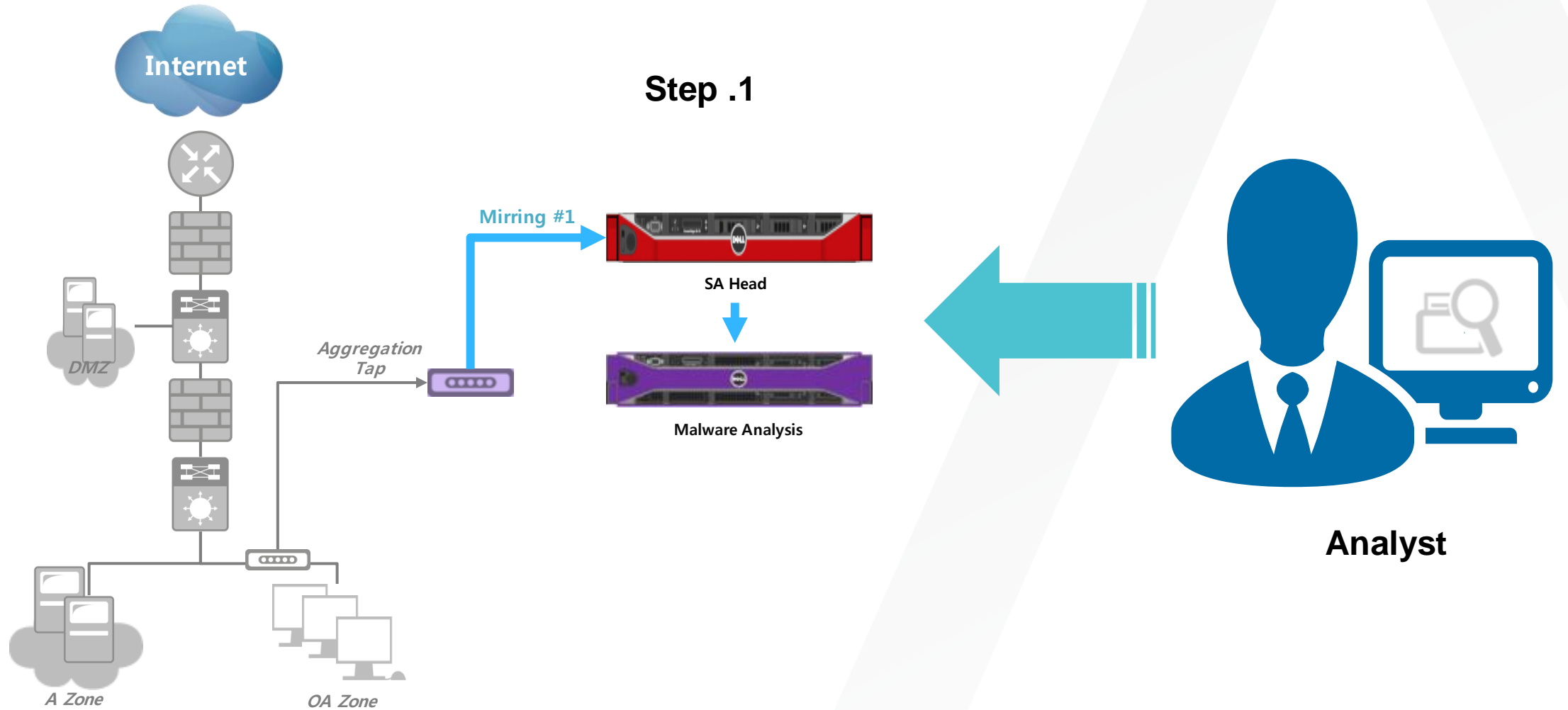
primera HANYUL 韓律 LIRIKOS
MARINE ENERGY



FIND A MALWARE



1ST ARCHITECTURE



WORKING WITH NETWITNESS(SA)

The screenshot displays the NetWitness Security Analyst (SA) interface. The top navigation bar includes 'Investigation', 'Navigate', 'Events', and 'Malware Analysis'. Below this, a secondary bar shows 'SA - Broker', 'Last 3 Hours', and various filters like 'Query', 'Profile', 'test1', 'Total', 'Descending', 'Event Count', 'Save Events', and 'Actions'. A search bar is on the right. The main content area shows a timeline for 'Last 3 Hours' from 2017-07-06 14:41:00 to 17:40:59. Below the timeline, a list of events is shown, categorized by risk level:

- Decoder Source** (1 value):
 - apdec01 (26,499,430)
- Risk: Informational** (20 of 20+ values):
 - dns low ttl (>100,000 - 4%) - http1.1 without server header (>100,000 - 4%) - http1.1 without referer header (>100,000 - 5%) - unknown service over ssl port (>100,000 - 7%) - http over non-standard port (>100,000 - 8%) - http post missing content-type (>100,000 - 8%) - http direct to ip request (>100,000 - 9%) - high risk filetypes (>100,000 - 10%) - http1.1 without accept header (>100,000 - 10%) - unknown service over http port (>100,000 - 13%) - js eval no docwrite (>100,000 - 15%) - nginx http server (>100,000 - 17%) - http1.0 unsupported host header (>100,000 - 22%) - http1.0 without referer header (>100,000 - 22%) - http1.0 unsupported connection header (>100,000 - 26%) - http1.1 without connection header (>100,000 - 36%) - byod mobile web agent (>100,000 - 38%) - common document formats (>100,000 - 55%) - http1.1 without user-agent header (>100,000 - 69%) - http1.1 server location redirect (>100,000 - 72%) ... [show more](#)
- Risk: Suspicious** (20 of 20+ values):
 - plaintext passwords (>100,000 - 4%) - dns extremely low ttl (>100,000 - 6%) - direct to ip http request (>100,000 - 14%) - ssl certificate missing subject organizational name (>100,000 - 32%) - dns large number of answers (>100,000 - 45%) - iframe hidden values (>100,000 - 54%) - dns large number of additional records (>100,000 - 88%) - possible sql injection (>100,000 - 93%) - dns large number of authority records (83,360) - js var replace chars (80,934) - ssl certificate missing issuer organizational name (74,888) - ssl certificate self-signed (72,407) - plaintext http password (67,409) - possible base64 http form data (51,641) - smb session on non-smb port (26,038) - dns extremely large number of answers (14,356) - archive extension mismatch (9,234) - ssl certificate chain incomplete (6,094) - javascript doc (2,385) - tunneling remote control client website (1,618) ... [show more](#)
- Risk: Warning** (12 values):
 - rogue dhcp server detected (>100,000 - 59%) - exe many dos header anomalies (1,378) - http large byte range (169) - href host doesn't match displayed host (129) - abnormal exe (57) - pdf inconsistent xref size (34) - cryptolocker beaconing (31) - locky malware (13) - exe linker major ver too high (4) - iframe src pdf (2) - taidoor malware (1) - pdf with nested filters (1)
- Action Event** (20 of 20+ values):
 - get (>100,000 - 13%) - response (>100,000 - 21%) - post (>100,000 - 23%) - bind (>100,000 - 43%) - destination unreachable (>100,000 - 44%) - name query (>100,000 - 57%) - refresh (>100,000 - 61%) - search (>100,000 - 70%) - echo (>100,000 - 71%) - echo reply (>100,000 - 77%) - login (>100,000 - 93%) - registration (55,061) - kerberos tgs request (48,181) - request (30,415) - kerberos tgs reply (27,653) - kerberos as request (24,080) - set named pipe state (23,820) - time exceeded (21,282) - propfind (19,109) - head (17,955) ... [show more](#)
- Attachment** (20 of 20+ values):
 - f.txt (1,898) - smime.p7s (1,103) - resource.jpg (1,100) - printbmp_265541.jpg (949) - 추천웹툰_르렌스를구해줘.png (915) - uoclke.min.js (466) - jquery-2.1.1.min.js (441) - json2.min.js (358) - jquery-2.1.1.js (346) - raven-3.13.1.min.js (340) - underscore-1.8.3.min.js (326) - minidaum-dwhite.min.js (295) - footer_logo.png (281) - 1.jpg (267) - non_close.png (233) - img0001.jpg (232) - play_safa.png (228) - ad_min.js (211) - uoclke_min_20150408_2.css (197) - jquery.1.11.0.min.js (190) ... [show more](#)

WORKING WITH NETWITNESS(MA)

Events List

Back to Summary | Delete Events | Download Files

Sort By: High Confidence | Static | Filter

Static	Network	Community	Sandbox	AV	Date Archived	Session Time	# Files	Source Address	Identity	Destination Addr	Destination Country	Alias Host	Event Type	Service	Destination Organiza
100	67	35			2017-07-03T12:03:...	2017-07-03T10:44:...	2						Network	80	
100	61				2017-07-04T04:12:...	2017-07-03T19:15:...	3						Network	80	
100	36	15			2017-07-03T21:40:...	2017-07-03T16:00:...	1						Network	80	
100	26	67			2017-07-03T21:40:...	2017-07-03T16:01:...	18						Network	80	
100	62	20			2017-07-04T07:05:...	2017-07-04T07:30:...	25						Network	80	
100	72	0			2017-07-03T22:56:...	2017-07-03T16:37:...	1						Network	80	
100	77	16			2017-07-03T10:23:...	2017-07-03T09:59:...	13						Network	80	
100	47	0			2017-07-04T07:41:...	2017-07-04T08:03:...	1						Network	80	
100	42	15			2017-07-04T01:25:...	2017-07-03T17:54:...	25						Network	80	
100	26	35			2017-07-04T01:19:...	2017-07-03T17:51:...	18						Network	80	
100	77	16			2017-07-04T01:19:...	2017-07-03T17:51:...	19						Network	80	
100	42	0			2017-07-04T07:40:...	2017-07-04T08:03:...	1						Network	80	
100	57	20			2017-07-03T14:15:...	2017-07-03T11:41:...	25						Network	80	
100	77	5			2017-07-04T01:12:...	2017-07-03T17:46:...	25						Network	80	
100	42	0			2017-07-03T17:29:...	2017-07-03T13:56:...	1						Network	80	
100	26	67			2017-07-03T16:44:...	2017-07-03T13:29:...	18						Network	80	
100	57	20			2017-07-03T18:47:...	2017-07-03T14:34:...	25						Network	80	
100	43	0			2017-07-03T11:51:...	2017-07-03T10:38:...	3						Network	80	
100	47	0			2017-07-03T17:29:...	2017-07-03T13:56:...	1						Network	80	
100	58	33			2017-07-03T17:57:...	2017-07-03T14:09:...	69						Network	80	
100	100	0			2017-07-03T18:14:...	2017-07-03T14:18:...	1						Network	80	
100	72	20			2017-07-04T00:42:...	2017-07-03T17:32:...	25						Network	80	
100	62	5			2017-07-03T20:45:...	2017-07-03T15:33:...	25						Network	80	
100	47	52			2017-07-03T19:13:...	2017-07-03T14:44:...	59						Network	80	

Page 1 of 1 | 100

Displaying 1 - 64 of 64

WORKING WITH NETWITNESS(MA)



















⚡ Actions ☺

Analysis Results for Event 797759587

Scanned service	# Files	Network Score	Static Score	Community Score	Sandbox Score
Malware Analysis Service	1	100	100	0	N/A

Archived at 2017-07-03T18:14:41
Event Type Network

Top 10 Indicators of Compromise

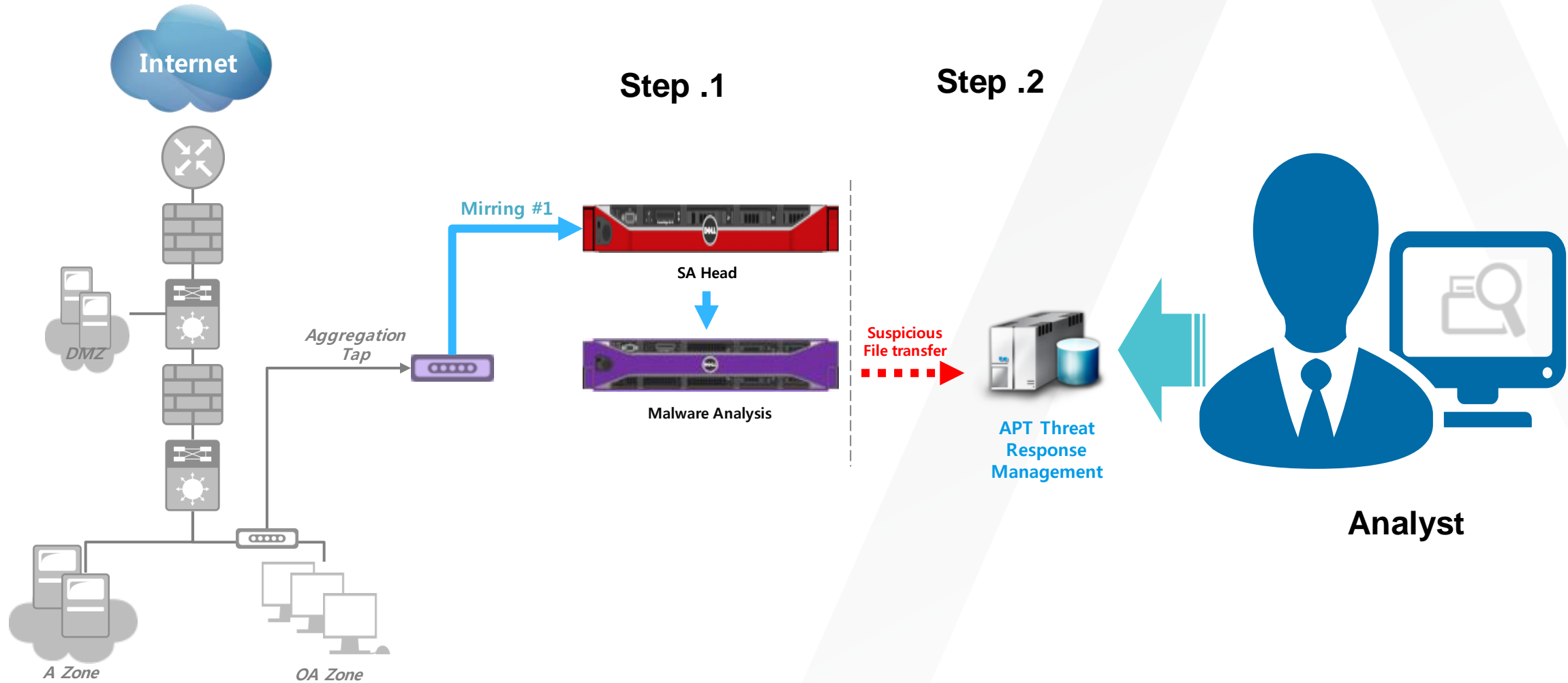
-   **Static ShellCode: Document Contains ShellCode (Kernel32.dll Base Address Lookup Found)**
Section Name: .rdata, virtual size: 1bf6b, virtual address: 1d3e00, raw size: 1bf80, raw address: 1d3e00, reloc address: 0, line numbers: 0, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_NOT_PAGED, IMAGE_SCN_MEM_READ
MOV reg, DWORD PTR FS:[30h] signature found at offset: 0x68cc
Instructions: xor ecx, ecx | mov eax, fs:[ecx+30h]
-   **Static (PE) - Artifact: DLL Injection Target ()**
Yara rule: Injection in file: rsa_mw_pe_artifacts.yara has detected a malicious string: at offset: 761712
-   **Static (PE) - Artifact: DLL Injection Target ()**
Yara rule: InjectionCsrssExe in file: rsa_mw_pe_artifacts.yara has detected a malicious string: csrss.exe at offset: 409410
-   **Network - Port/Protocol: HTTP Port/Protocol Mismatch (Port 80)**
Destination IP: , Protocol: 2048, Port: 5465, Service: 80, Alias: , TLD: , Country: Private
-   **Network - Alerts: Contains Suspicious Alerts**
direct to ip http request, abnormal exe, packer cryptx
-   **Network - Alerts: Contains Informational Alerts**
http over non-standard port, http1.1 without accept header, high risk filetypes, http1.1 without referer header, http direct to ip request
-   **Static (PE) - Artifact: Security Weakening - cmd.exe usage**
Yara rule: WeakenCmdExe in file: rsa_mw_pe_artifacts.yara has detected a malicious string: cmd.exe /c at offset: 400560
-   **Static (PE) - Artifact: AutoStart File (Task Scheduler Folder)**
Yara rule: AutoStartTaskScheduler in file: rsa_mw_pe_artifacts.yara has detected a malicious string: Windows%\Tasks at offset: 796593
-   **Static (PE) - DLL Imports: Contains String Artifacts that indicate Bad DLL Import/Export Fingerprint**
String Artifact Found [CreateRemoteThread]

100 Network Analysis Results

I NEED SOME MORE

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

2ND ARCHITECTURE



WORKING WITH MIDDLEWARE

File Analysis

Registered Date&Time	<input type="text"/>	Analysis ID	<input type="text"/>	Alias Host	<input type="text"/>	
File Name	<input type="text"/>	MD5	<input type="text"/>	SHA256	<input type="text"/>	
Collect Date Time	<input type="text"/>	Src Ip	<input type="text"/>	DST IP	<input type="text"/>	
Owner ID	<input type="text"/>	Event ID	<input type="text"/>	<input type="checkbox"/> App Rule	Session Id	<input type="text"/>
Static Score	30 <input type="text"/>	Nextgen Score	0 <input type="text"/>	Community Score	0 <input type="text"/>	

Reset Search

Total 1,580

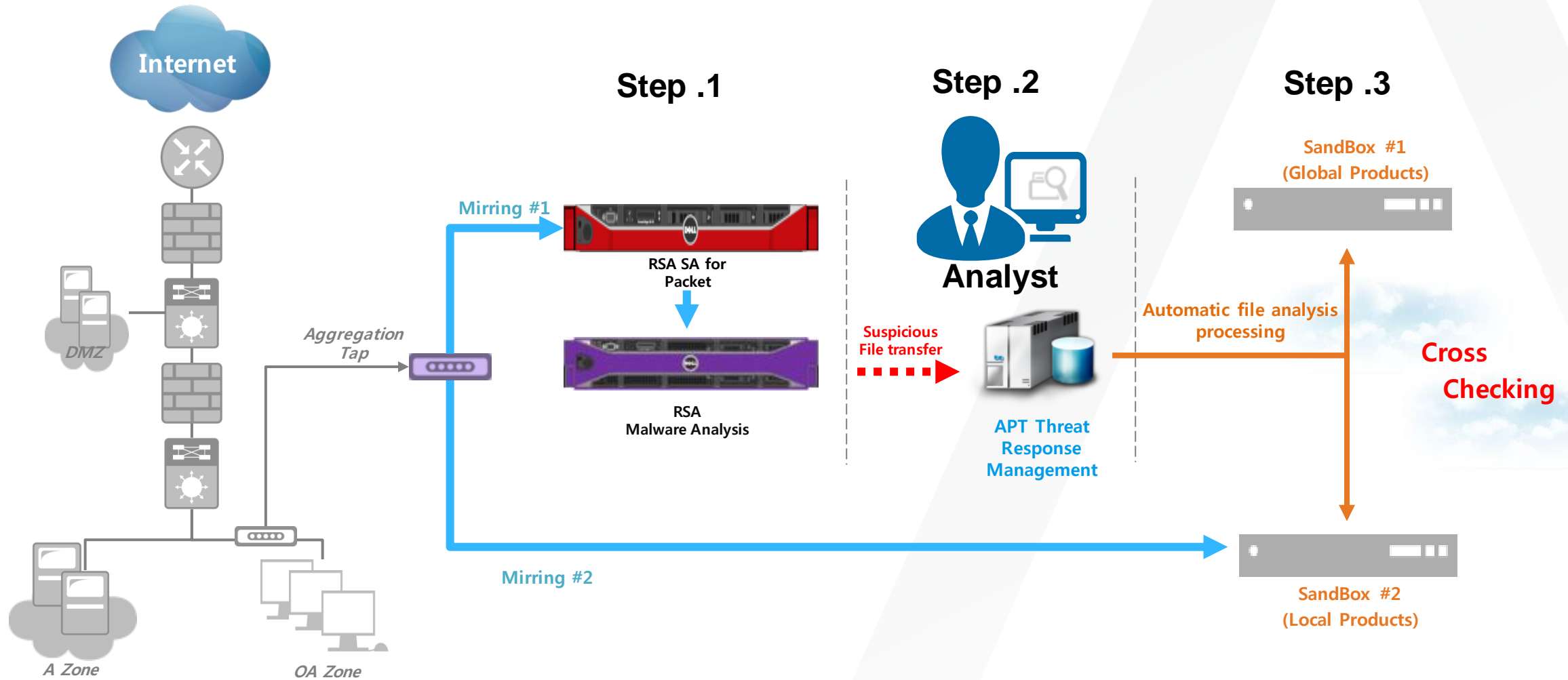
↓ 10 ↓

<input type="checkbox"/>	Analysis ID	Registered Date&...	Event ID	Session Id	File Name	Static Score	Nextgen Sc...	Community ...	MD5	SHA256	Collect Date Time	Owner ID	Src Ip	DST IP	Alias Host	History Yn
<input type="checkbox"/>	FA170706030600		806331996	37041836...		61.0	87.0	0.0	dcb...	ba75f...						X
<input type="checkbox"/>	FA170706030591		806331276	37041928...		43.0	57.0	0.0	9578...	3eb6f...						X
<input type="checkbox"/>	FA170706030588		806327973	37041773...		31.0	62.0	0.0	3a9ff...	bbad:...						X
<input type="checkbox"/>	FA170706030587		806327973	37041773...		31.0	62.0	0.0	be7e...	7ab0f...						X
<input type="checkbox"/>	FA170706030584		806327973	37041773...		91.0	62.0	0.0	19f3f...	d5f78...						X
<input type="checkbox"/>	FA170706030583		806327973	37041773...		91.0	62.0	0.0	7f74...	59f36...						X
<input type="checkbox"/>	FA170706030581		806327973	37041773...		30.0	62.0	0.0	36b8...	cdc3:...						X
<input type="checkbox"/>	FA170706030580		806327973	37041773...		66.0	62.0	0.0	7079...	7c89f...						X

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

File Analysis

Registered Date&Time [] ~ [] Analysis ID [] Alias Host []

File Name [] MD5 [] SHA256 []

Collect Date Time [] ~ [] Src Ip [] DST IP []

Owner ID [] Event ID [] App Rule Session Id []

Static Score 30 ~ [] Nextgen Score 0 ~ [] Community Score 0 ~ []

Malware Type 전체 Malignant Normal Further analysis Malignant after further analysis Unnecessary Wait Before Request Analyzing Do Not Analyze Failed

SANBOX #1 [] SANBOX #2 []

Reset Search

Total 1,580

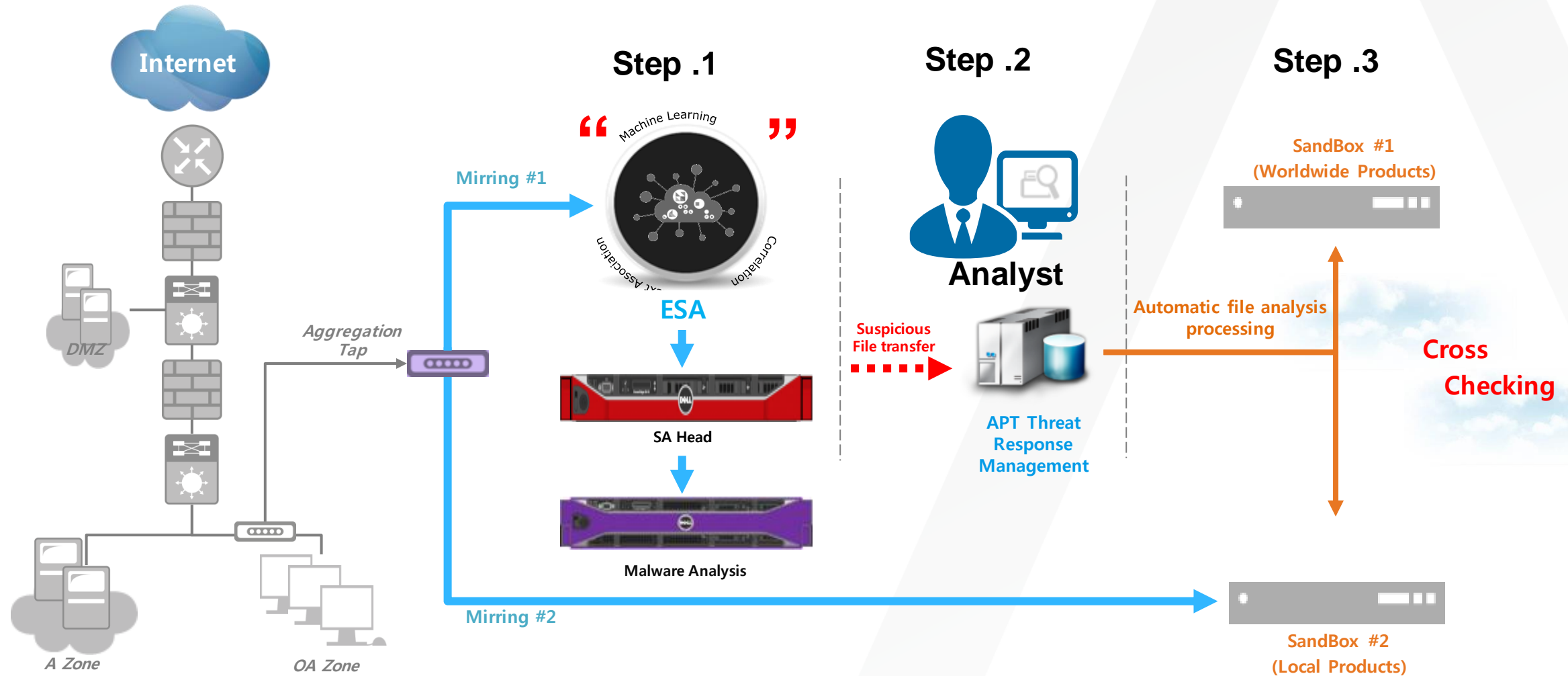
10

	Analysis ID	Registered Date&...	Event ID	Session Id	File Name	Static Score	Nextgen Sc...	Community ...	MD5	SHA256	Collect Date Time	Owner ID	Src Ip	DST IP	Alias Host	History Yn	Malware Type	SANBOX #1
<input type="checkbox"/>	FA170706030600		806331996	37041836...		61.0	87.0	0.0	dcbb ...	ba75t ...						X	Analyzing	
<input type="checkbox"/>	FA170706030591		806331276	37041928...		43.0	57.0	0.0	9578 ...	3eb6i ...						X	Analyzing	
<input type="checkbox"/>	FA170706030588		806327973	37041773...		31.0	62.0	0.0	3a9fl ...	bbad: ...						X	Analyzing	
<input type="checkbox"/>	FA170706030587		806327973	37041773...		31.0	62.0	0.0	be7e ...	7ab0t ...						X	Analyzing	
<input type="checkbox"/>	FA170706030584		806327973	37041773...		91.0	62.0	0.0	19f3i ...	d5f78 ...						X	Analyzing	
<input type="checkbox"/>	FA170706030583		806327973	37041773...		91.0	62.0	0.0	7774: ...	59f36 ...						X	Analyzing	
<input type="checkbox"/>	FA170706030581		806327973	37041773...		30.0	62.0	0.0	36b8 ...	cdc3: ...						X	Analyzing	
<input type="checkbox"/>	FA170706030580		806327973	37041773...		66.0	62.0	0.0	7079 ...	7c89e ...						X	Analyzing	

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

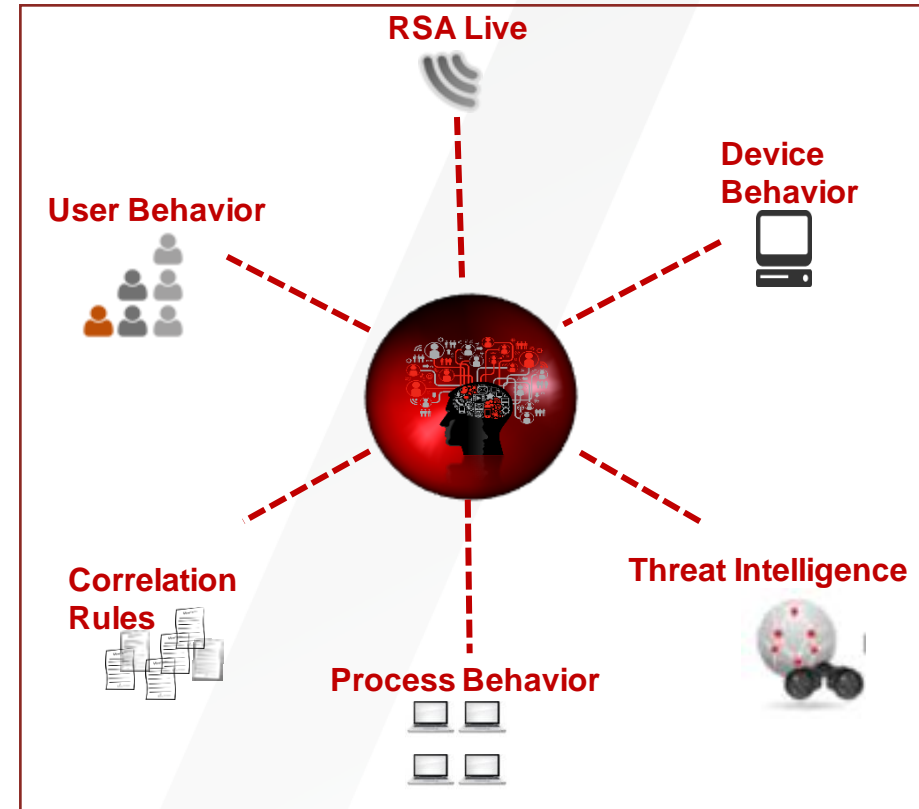


IMPROVEMENT POINT

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



APJ SUMMIT

ENABLING BUSINESS DRIVEN SECURITY

THANK YOU

@RSAAPJ #RSAAPJ