Using NSX Advanced Security to fight off hackers and spies

Miquel Arevalo
Network and Security SE Nordics

Every

11 seconds

a new organization falls victim

59%

of all attacks involve double extortion

>4000

ransomware attacks happen daily

Full funded
adversary syndicates

Ransomware

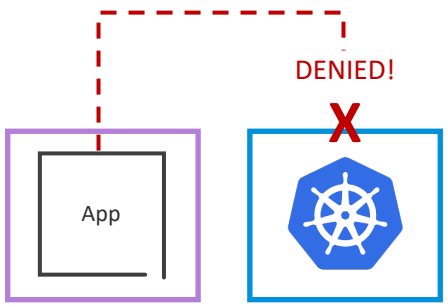
As-a-service

Operationalizing East-West Security

With the NSX Service-defined Firewall

STEP 1

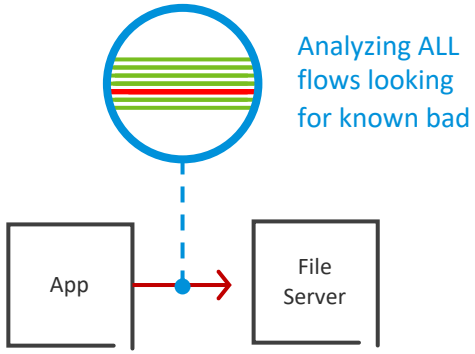
Network & App Segmentation



+

STEP 2

In-band Inspection with distributed IDS/IPS

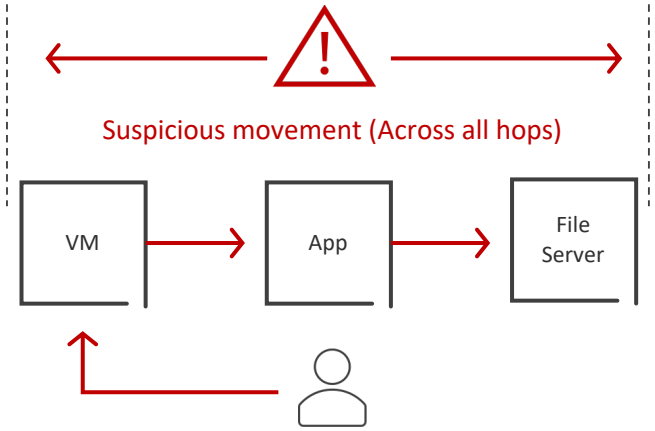


Detect and mitigate **KNOWN** attacks

+

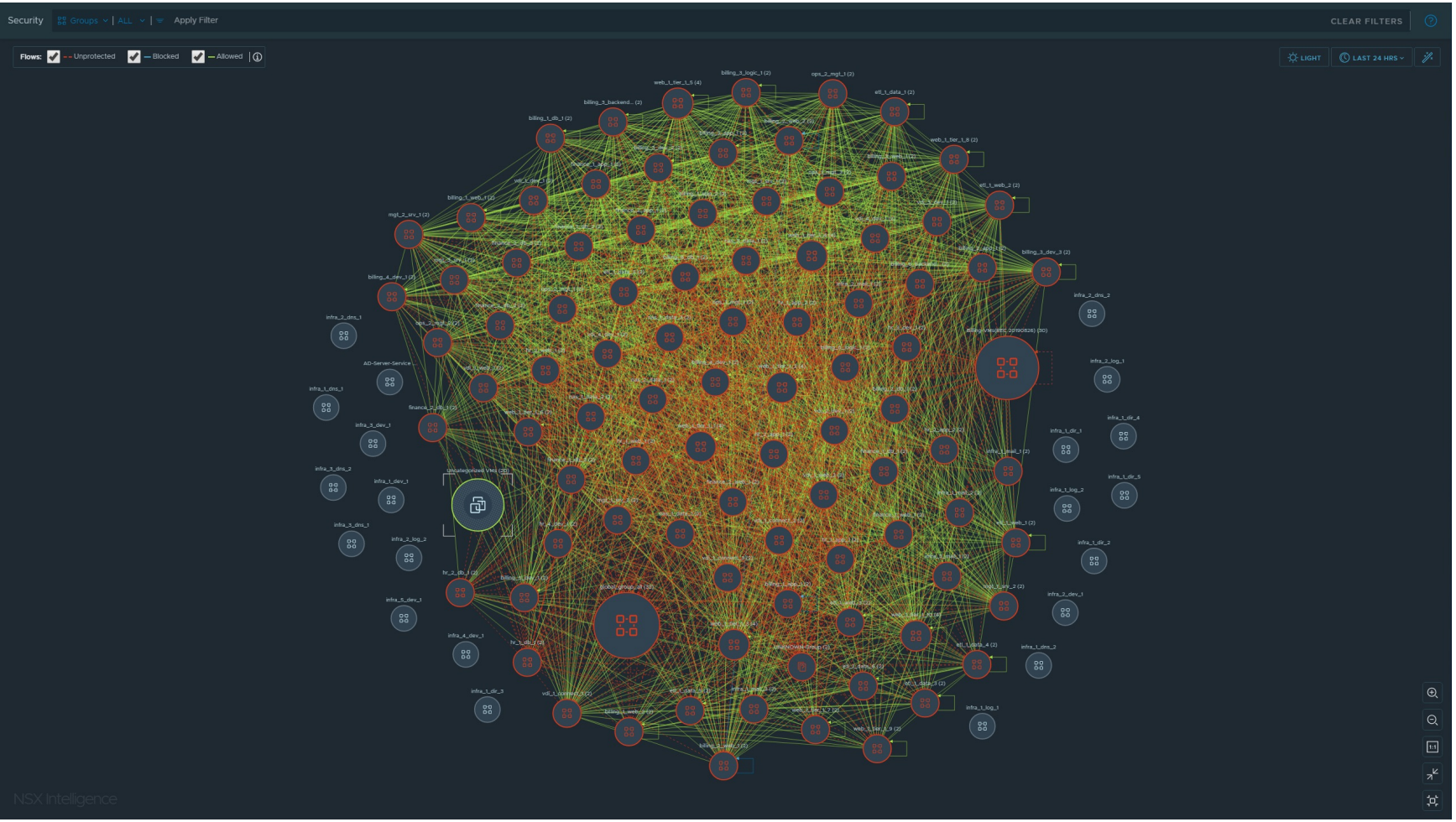
STEP 3

NTA with Sandboxing and NDR



Detect and mitigate **UNKNOWN** attacks

NSX Intelligence



NSX Intelligence provides Visualization of all NSX inventory and flows at scale

Enables visibility of flow status in Group and VM communication maps. Flows are classified as:

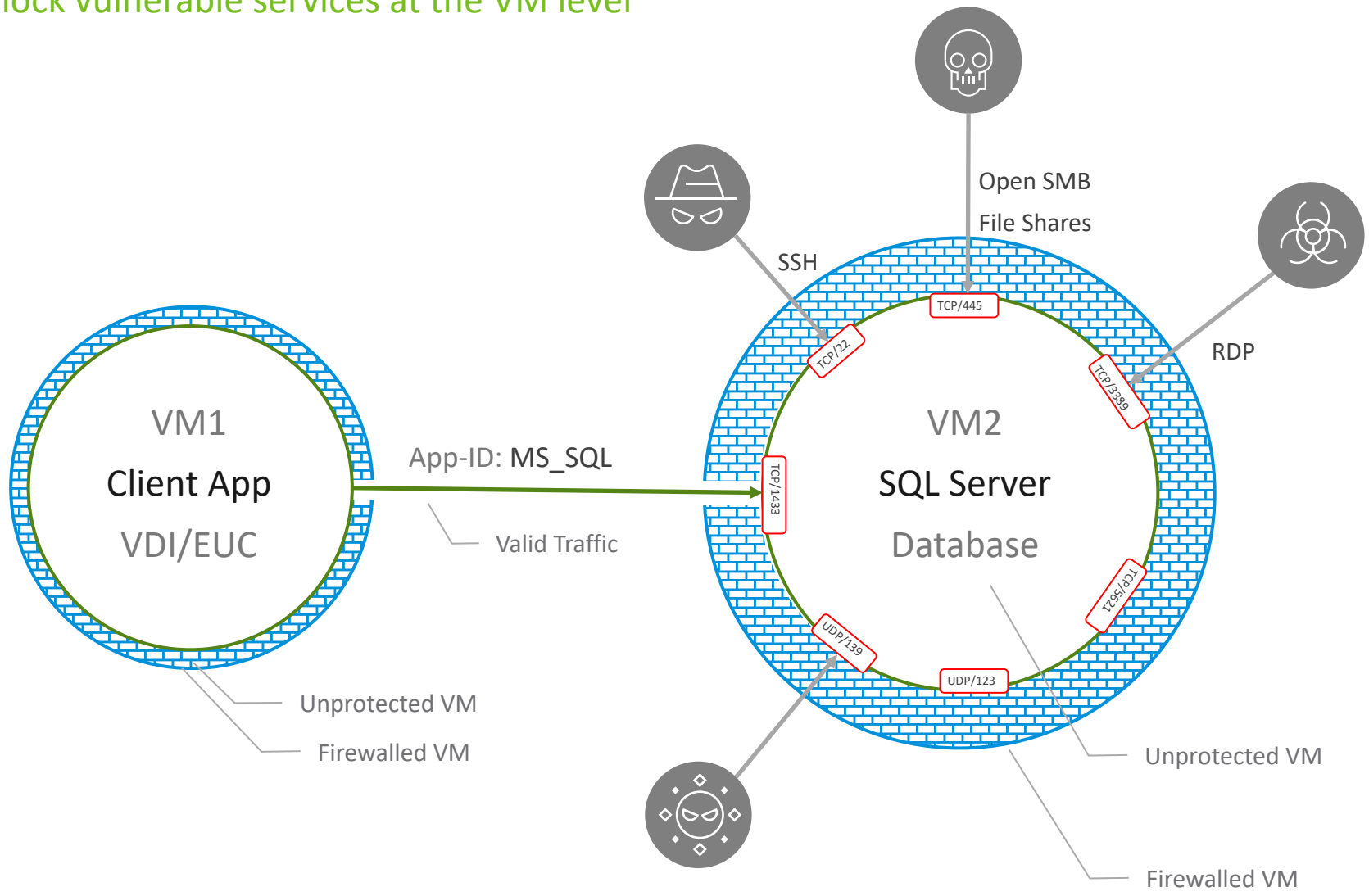
- Unprotected
- Blocked
- Allowed

Highlighting a specific group will show related flows

Rich filtering to drill down into more specific views

Distributed Firewall

Block vulnerable services at the VM level



No firewall = vulnerable to many attack vectors

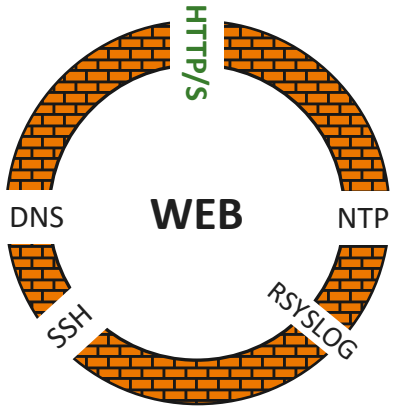
Accidental exposure of services

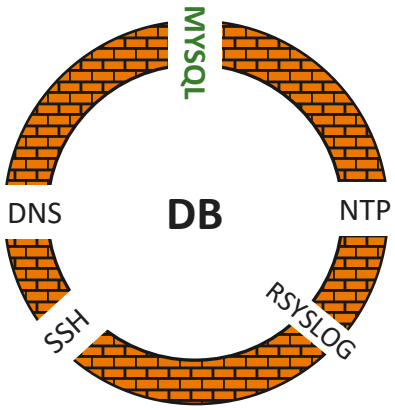
Goal: Block unused services = reduce the attack surface

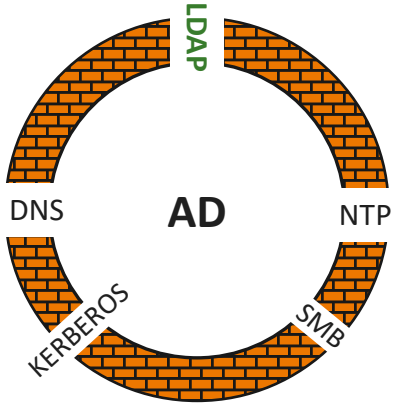
750 App-IDs for protocol aware firewall rules

NSX DFW prevents use of unwanted ports/protocols/applications

But still exposes legitimate applications







Latest version of Apache 2.4.57 in April 2023

Vulnerability CVE-2023-25690

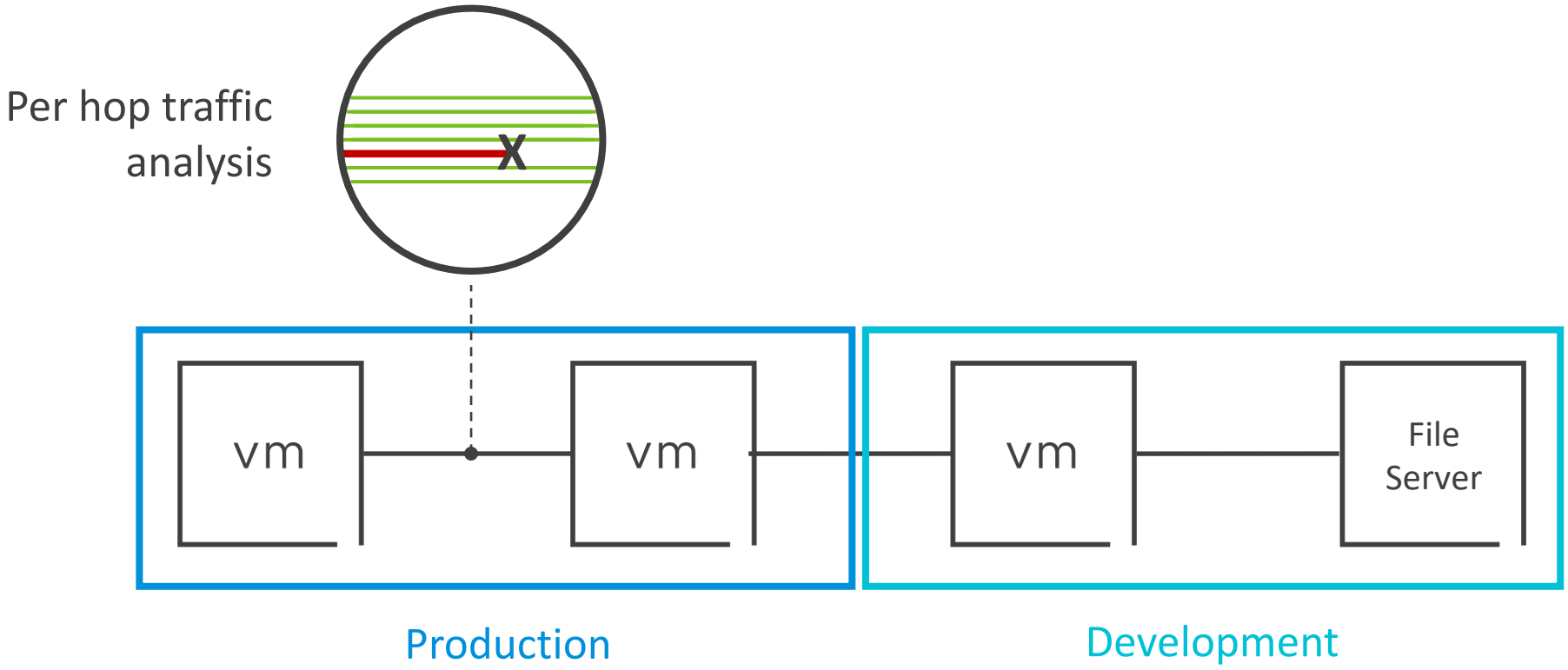
…result in bypass of access controls…

…cache poisoning…

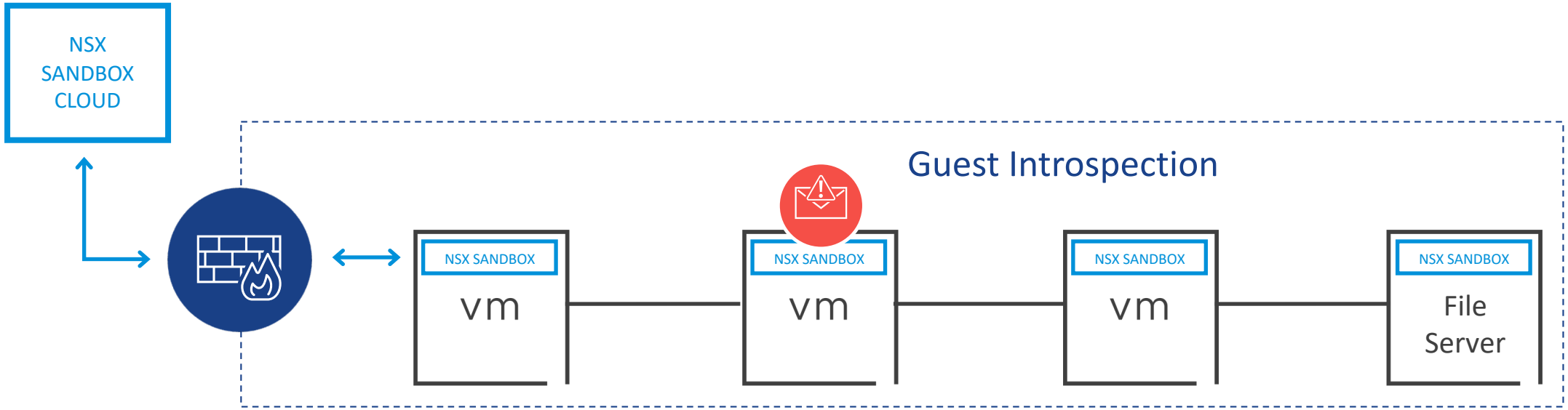
…recommended to update to 2.4.56

2.4.56 was released end of January 2023

NSX Distributed IDS/IPS

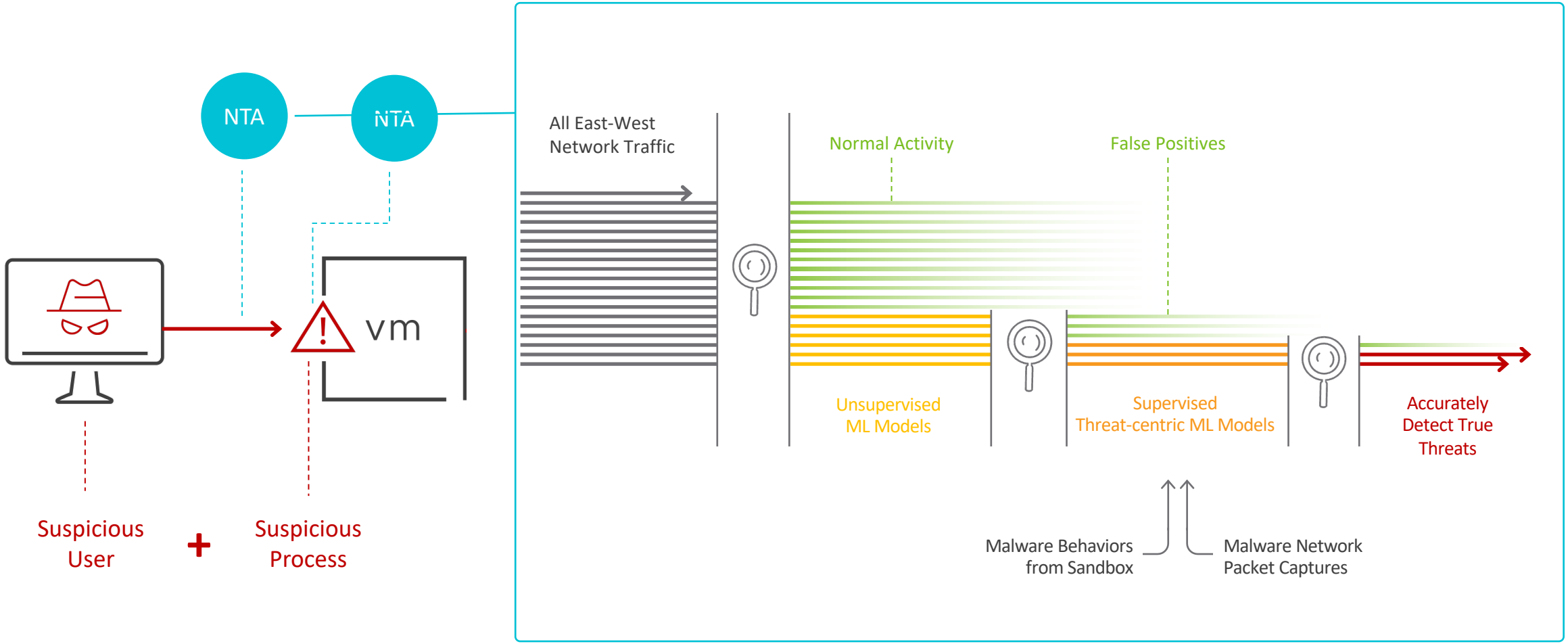


NSX Sandbox


NSX
SANDBOX
CLOUD
Guest Introspection
NSX SANDBOX
vm
NSX SANDBOX
vm
NSX SANDBOX
vm
NSX SANDBOX
File
Server

Network Traffic Analysis

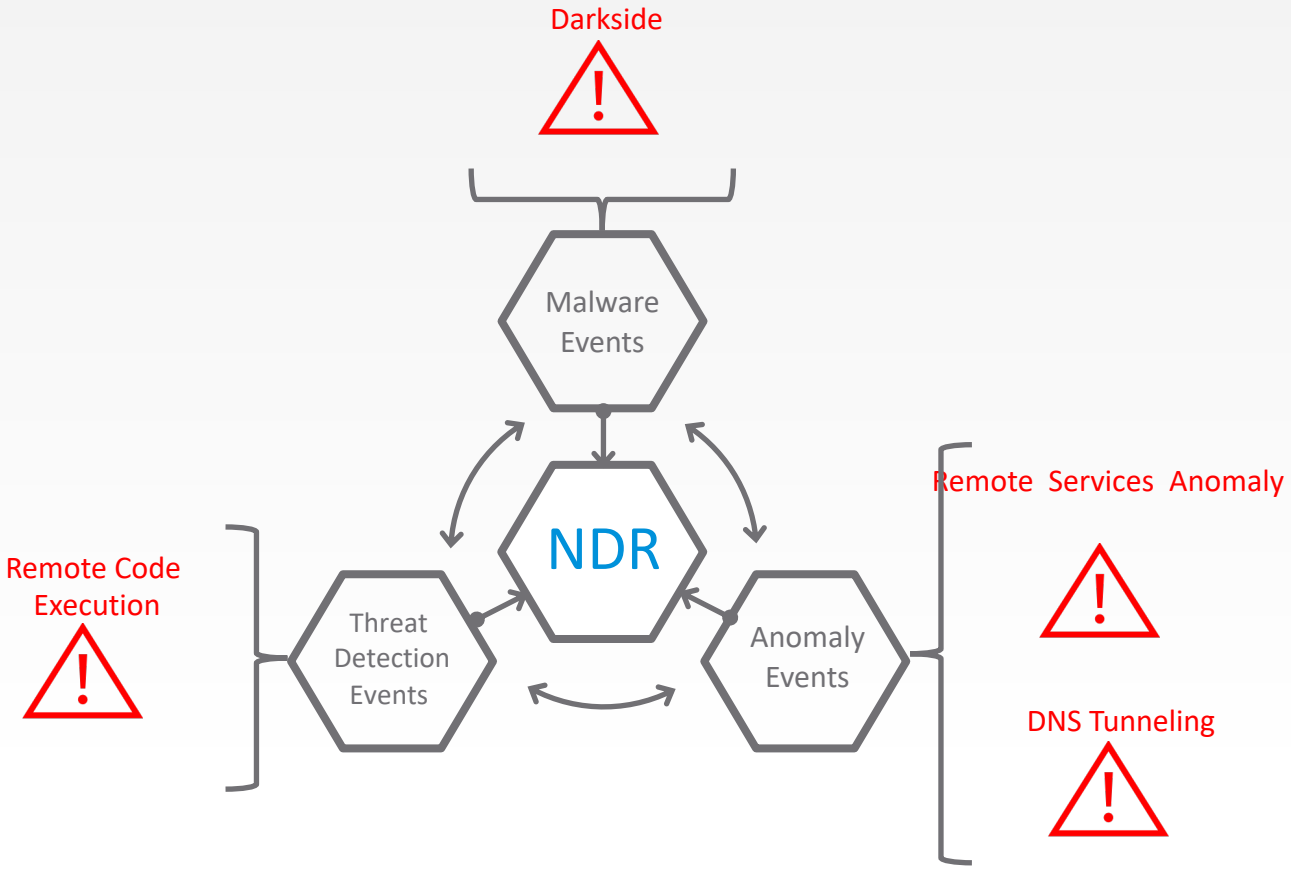
Sandbox
IDS/IPS
NTA

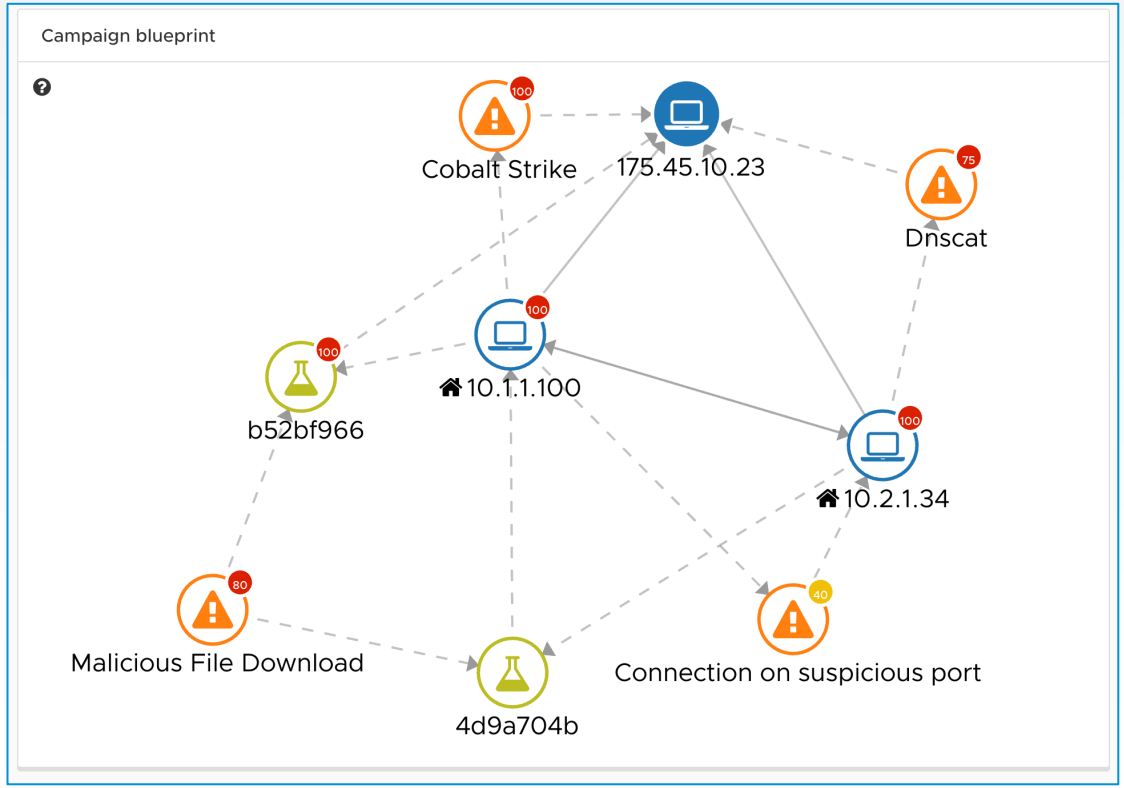


No Tapping

Visibility & Enforcement across the Attack Chain

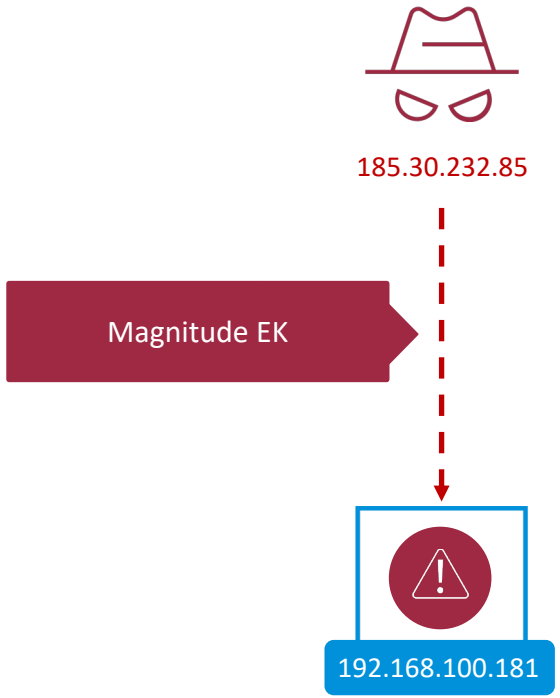
Network Detection and Response





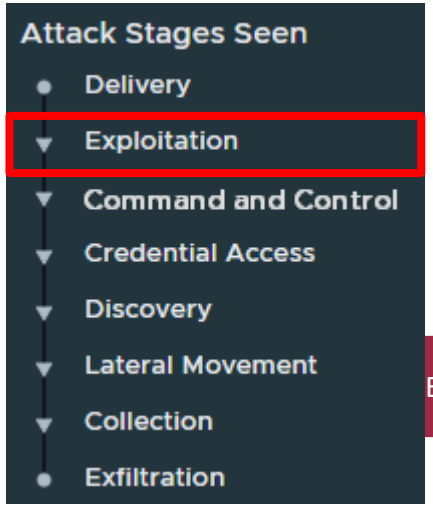
Modern malware is adaptable, multi-staged, multi-faceted, multi … HYDRA!

Multiple security controls are necessary to detect and mitigate all aspects



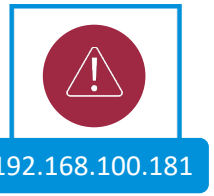
Hypervisor

Hypervisor

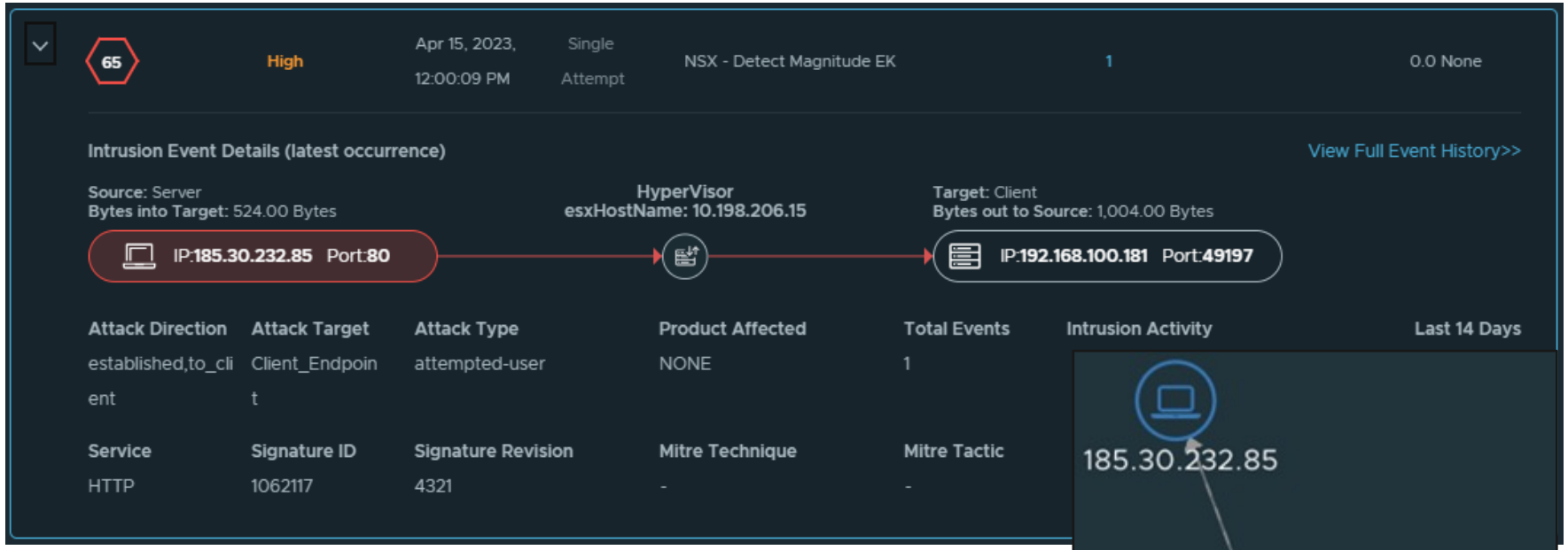


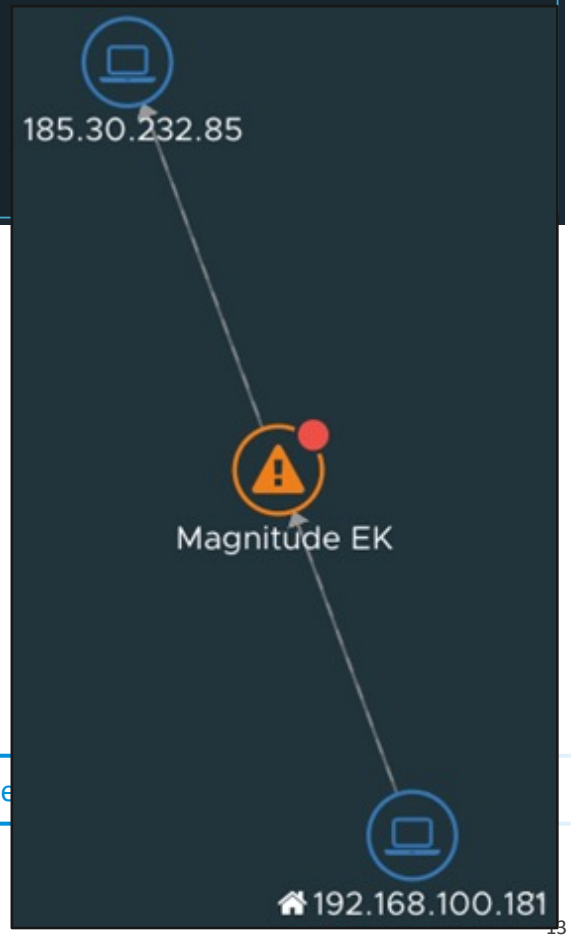
185.30.232.85

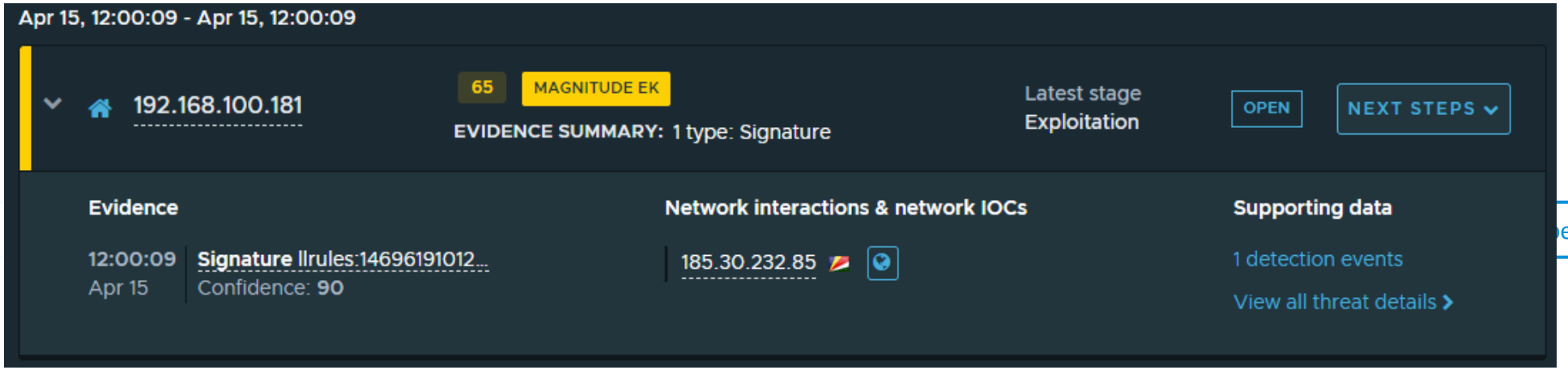
EK

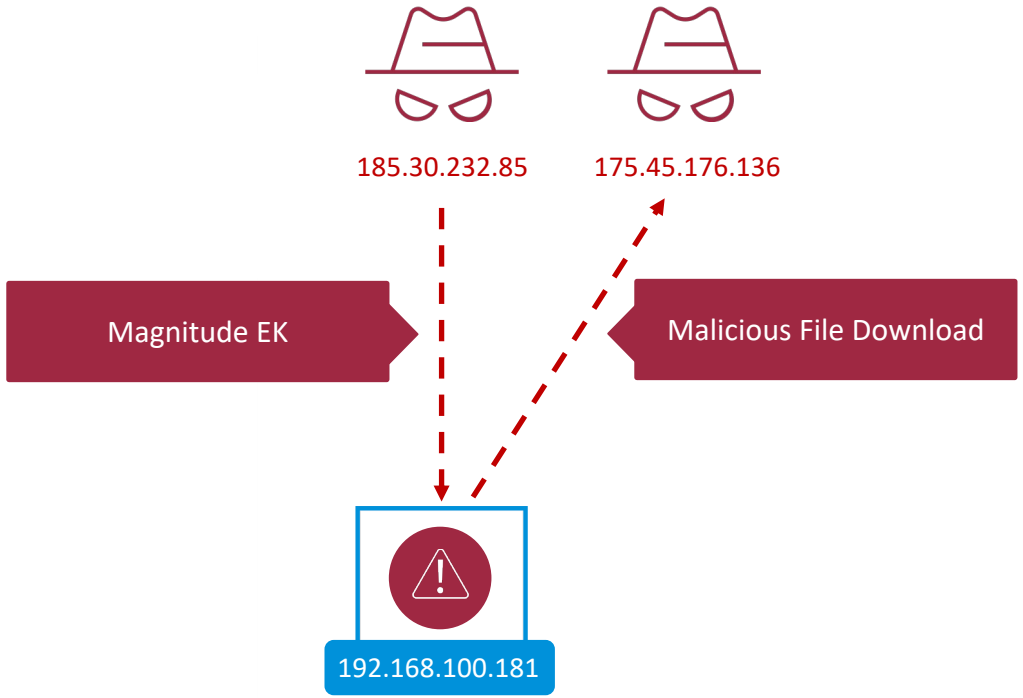


192.168.100.181



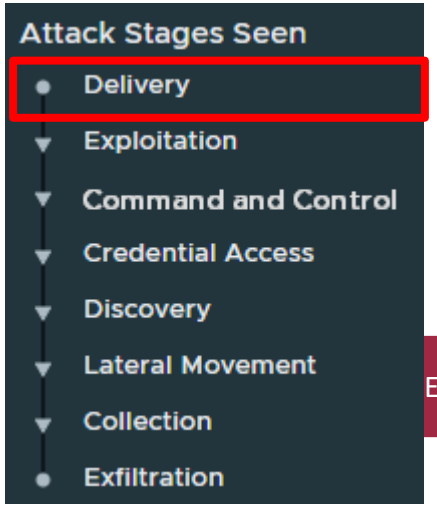






Hypervisor

Hypervisor



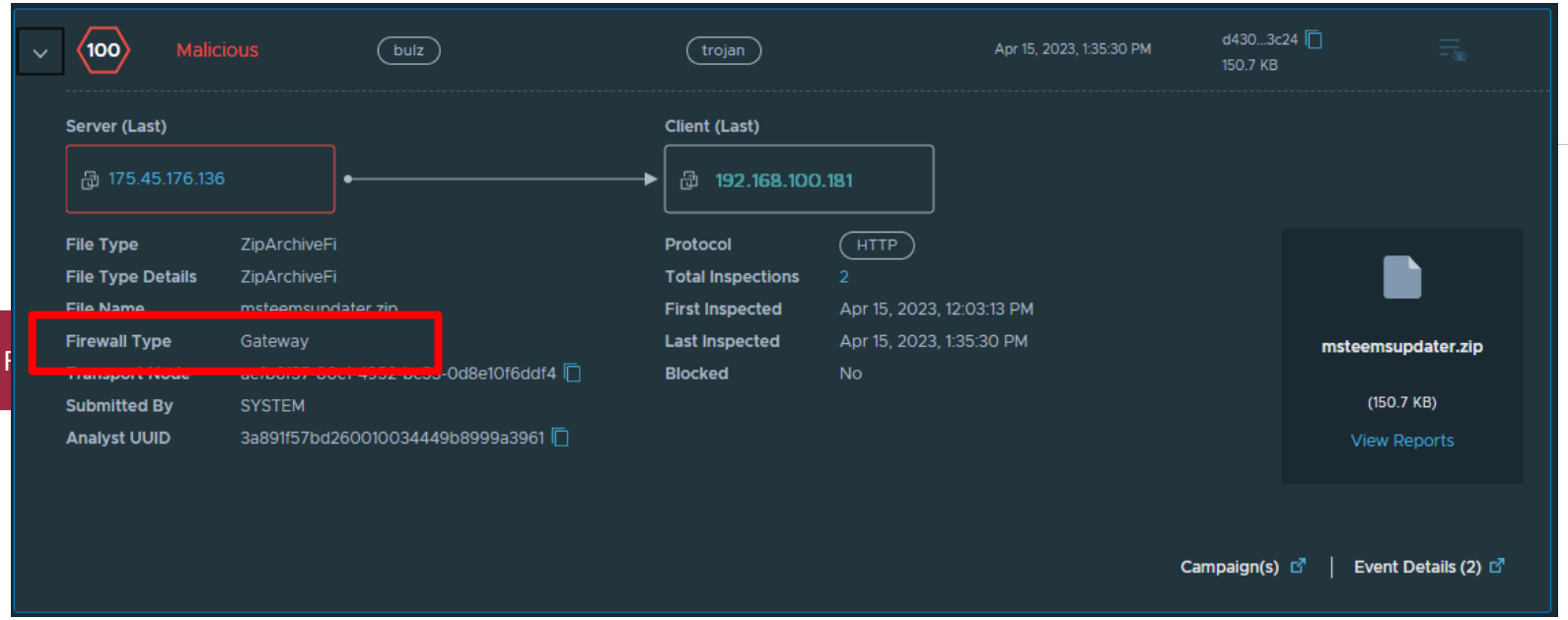
185.30.232.85

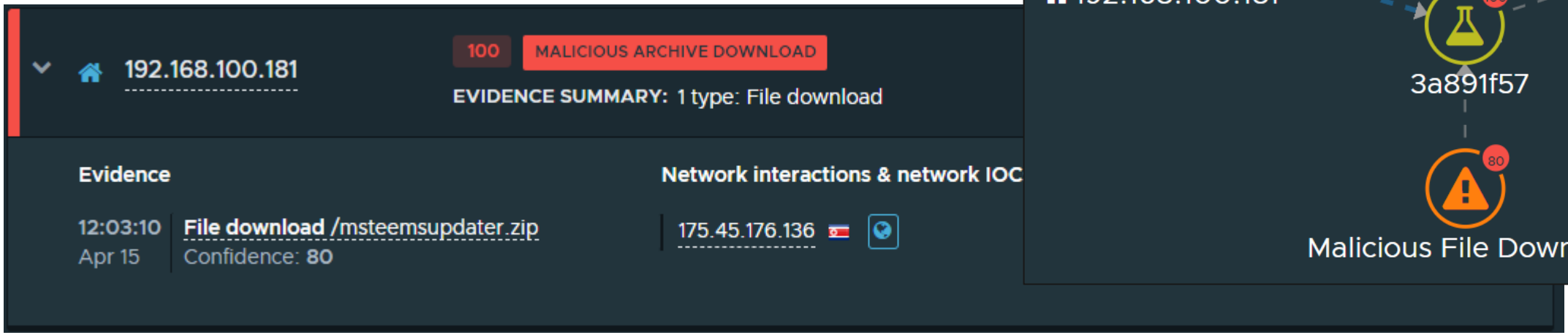
175.45.176.136

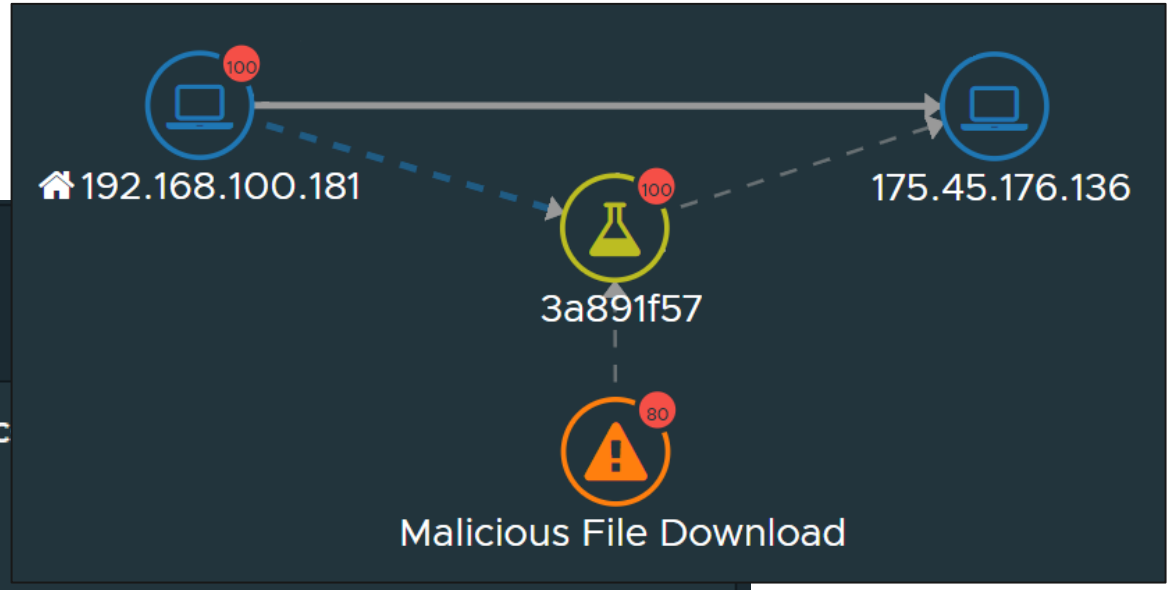
EK

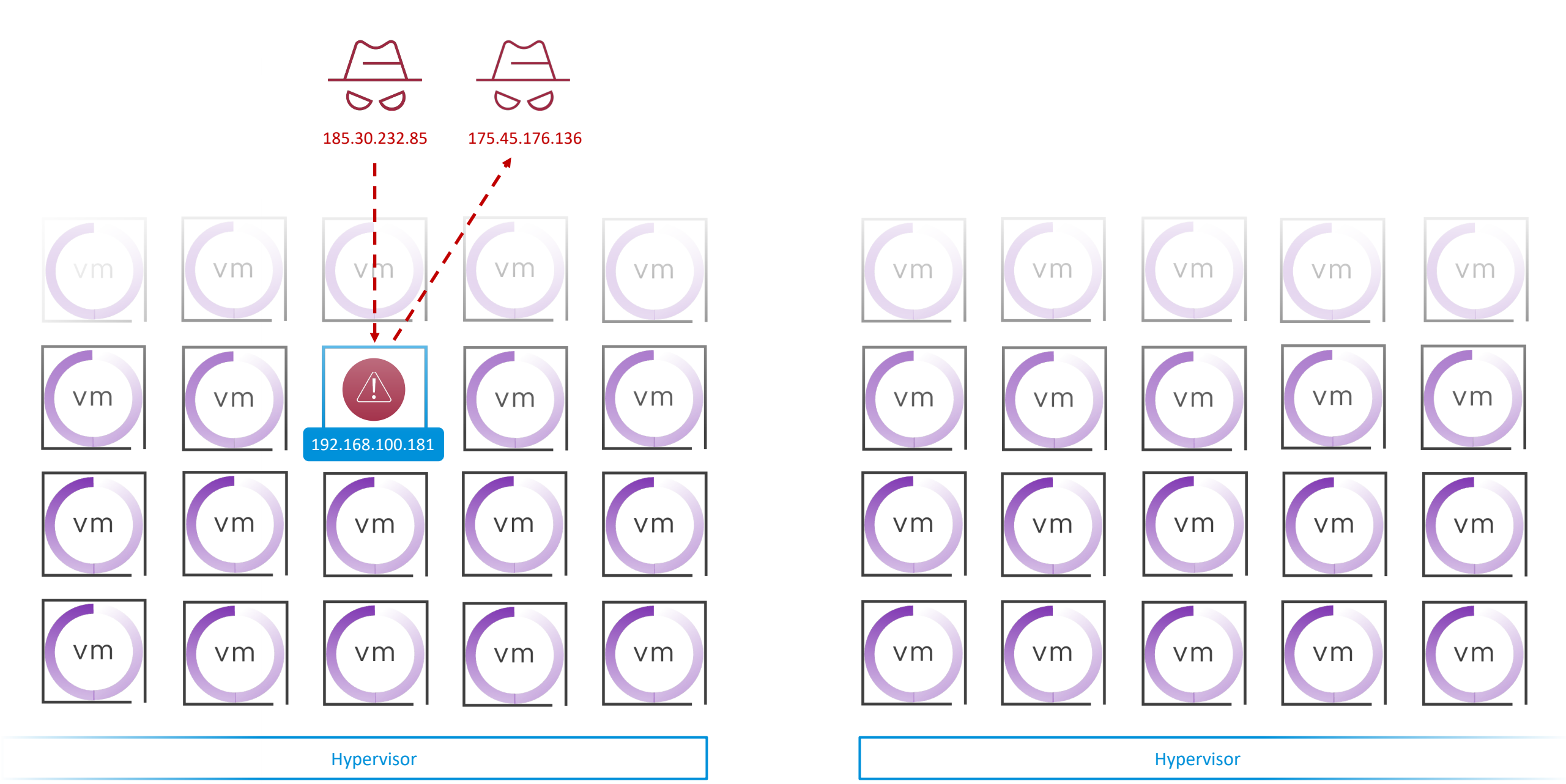
Malicious F

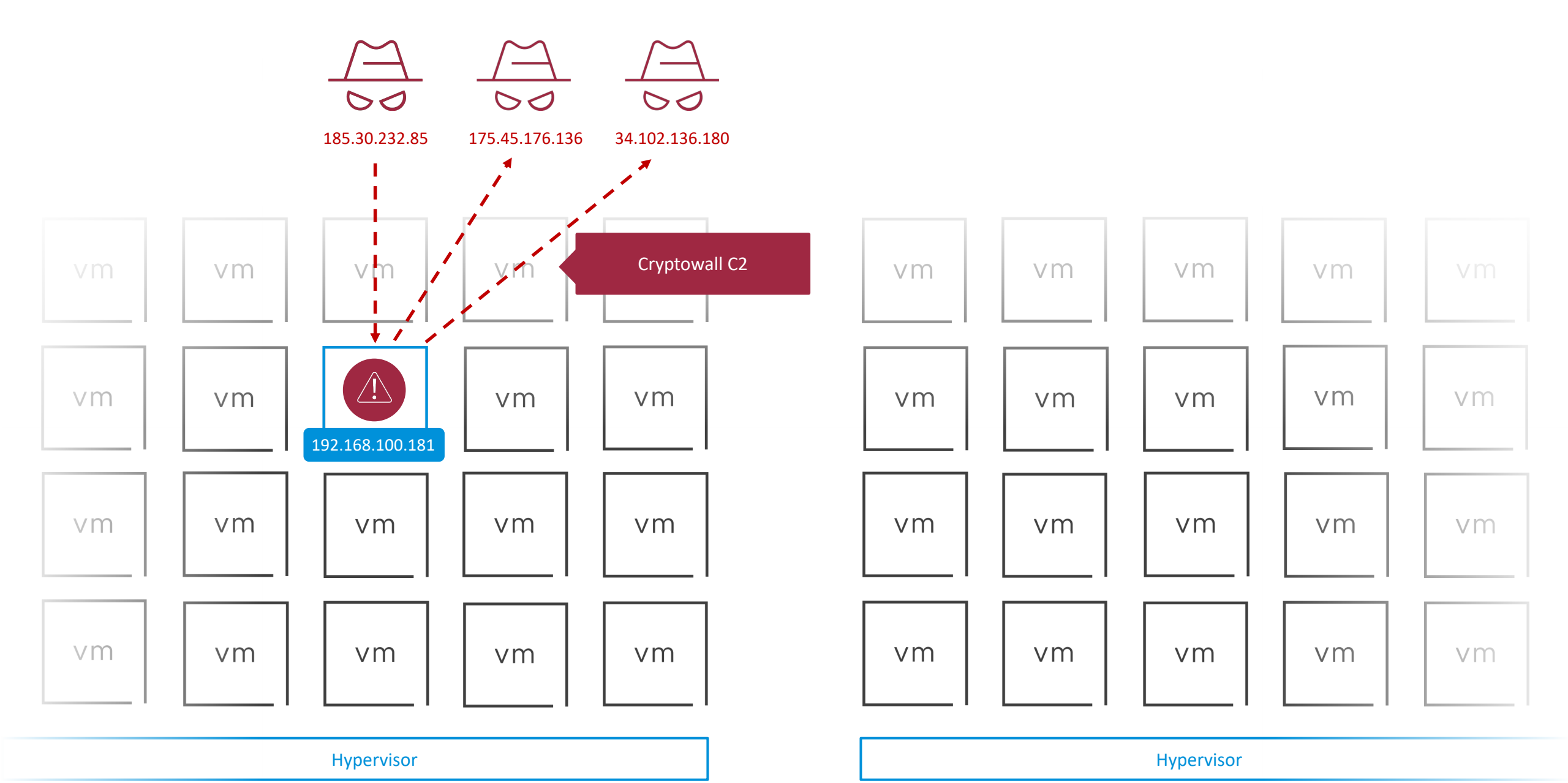
192.168.100.181

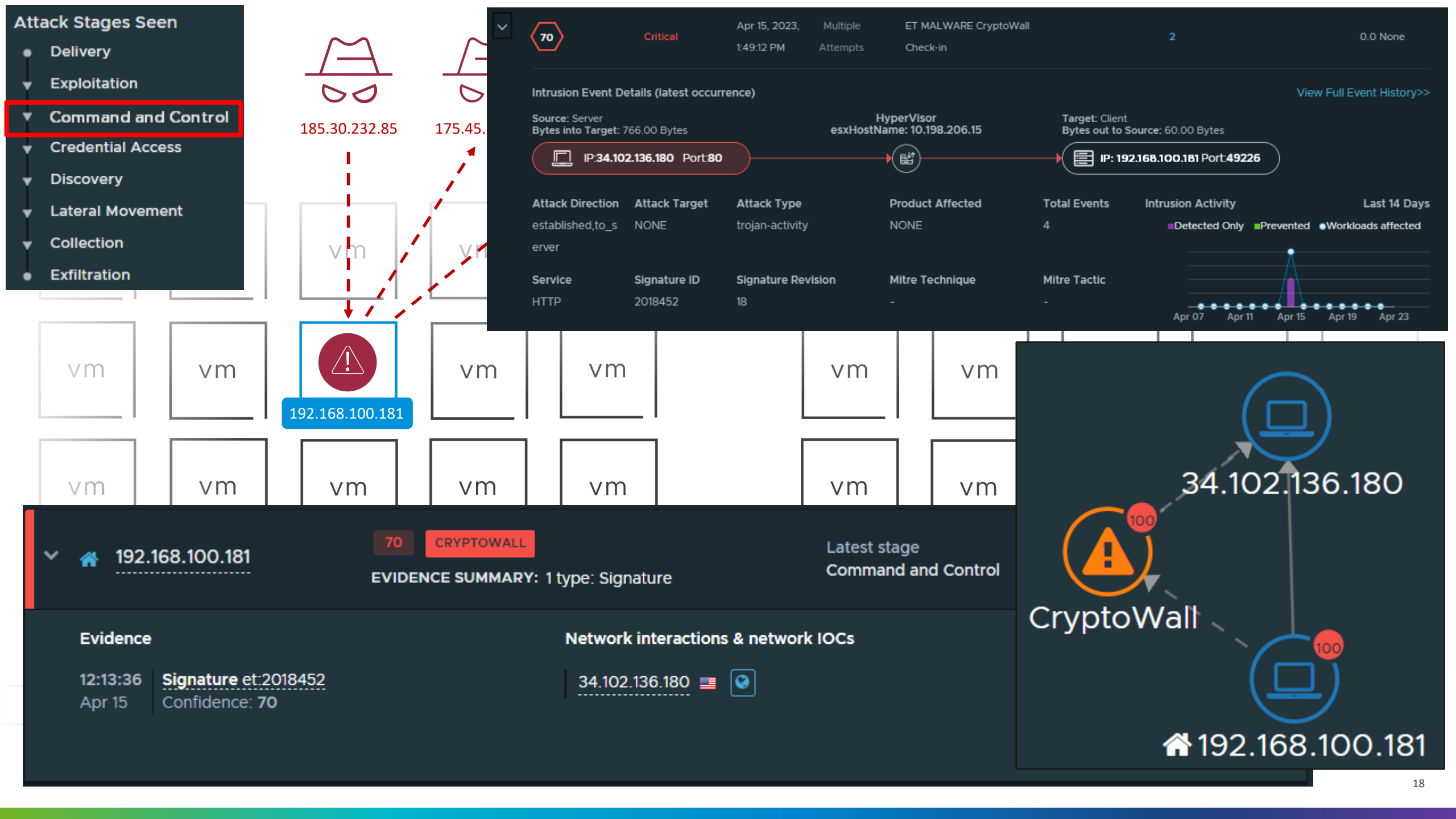


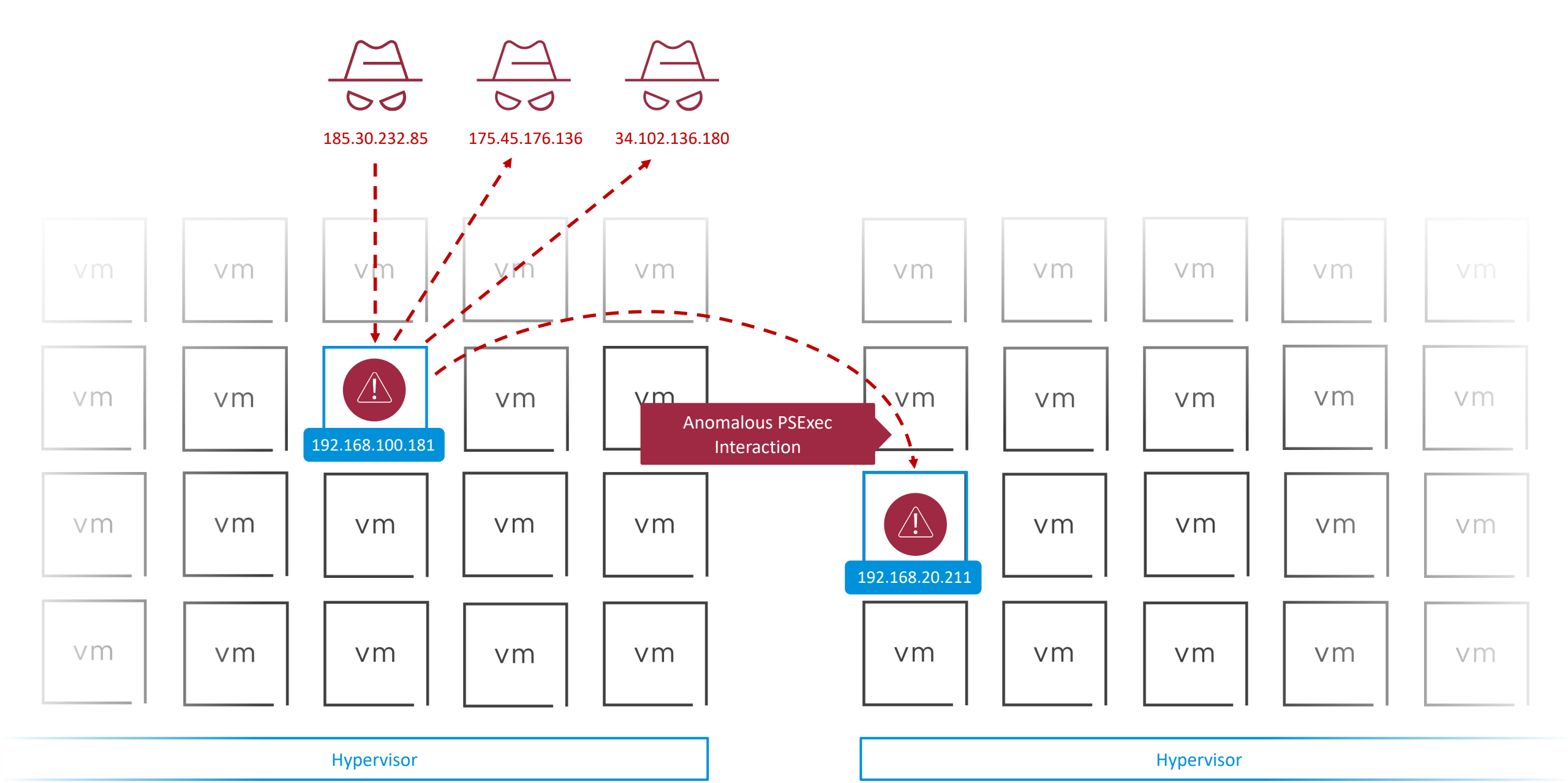


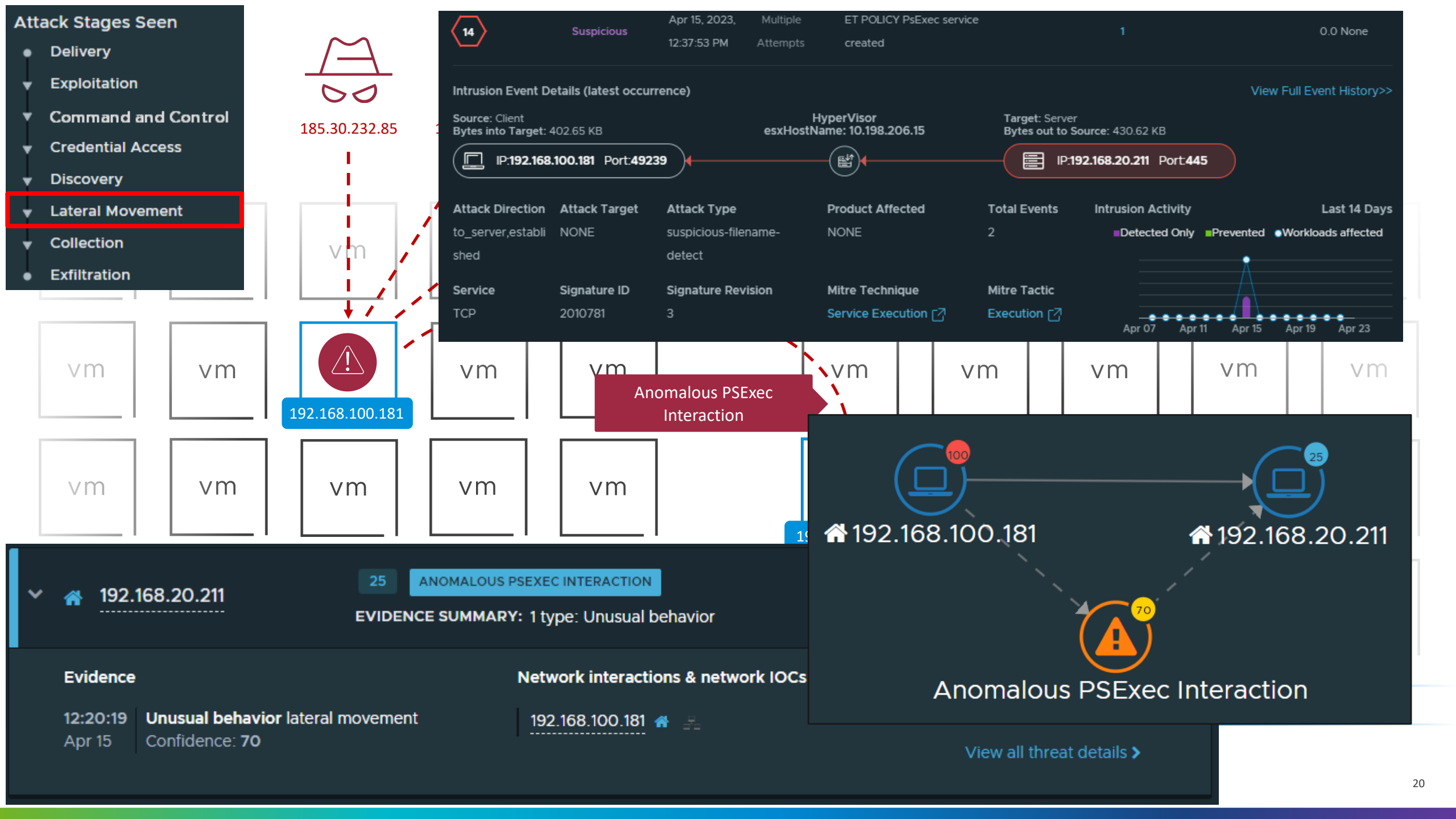


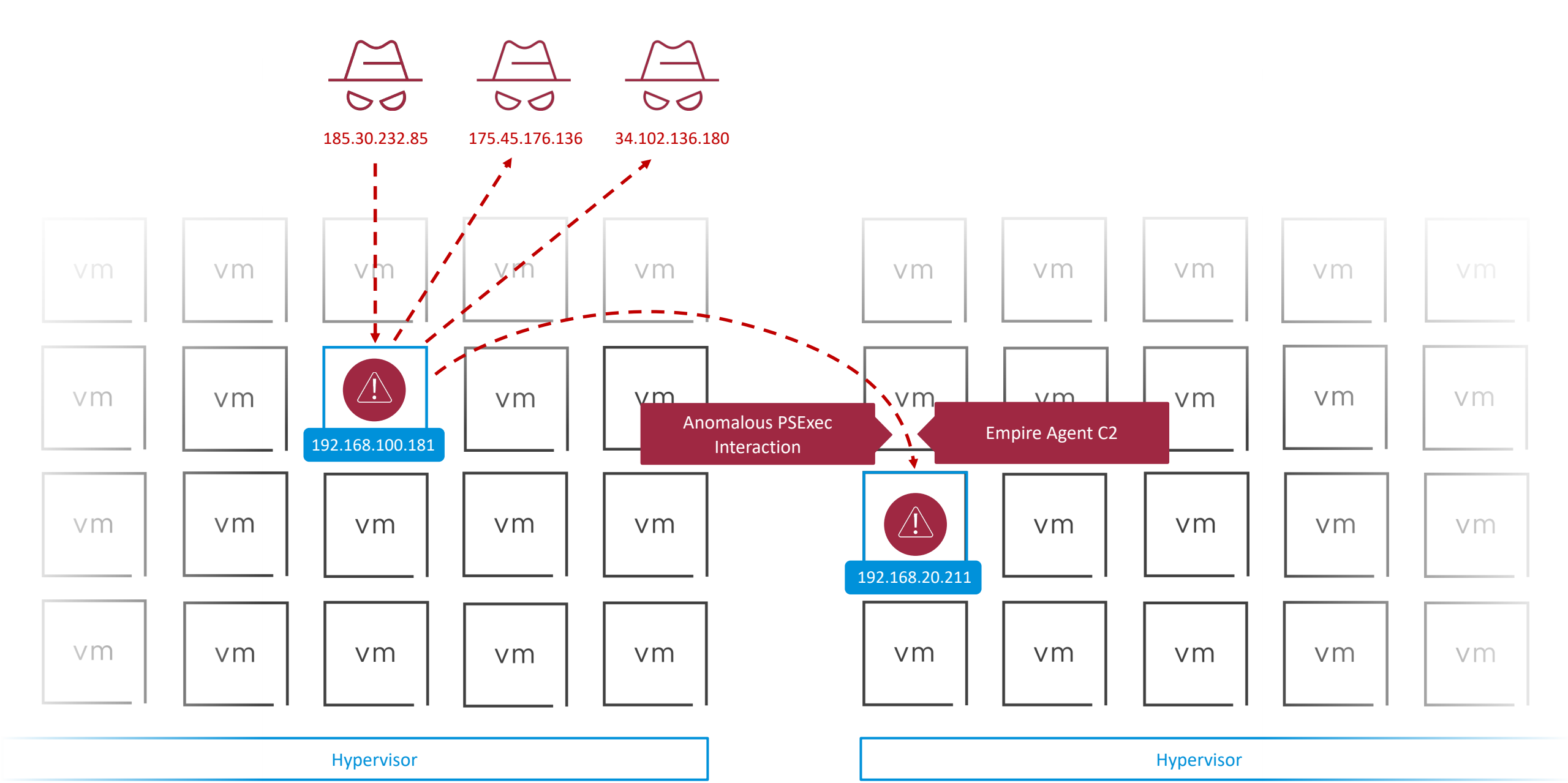

185.30.232.85
175.45.176.136
vm
192.168.100.181
Hypervisor
Hypervisor

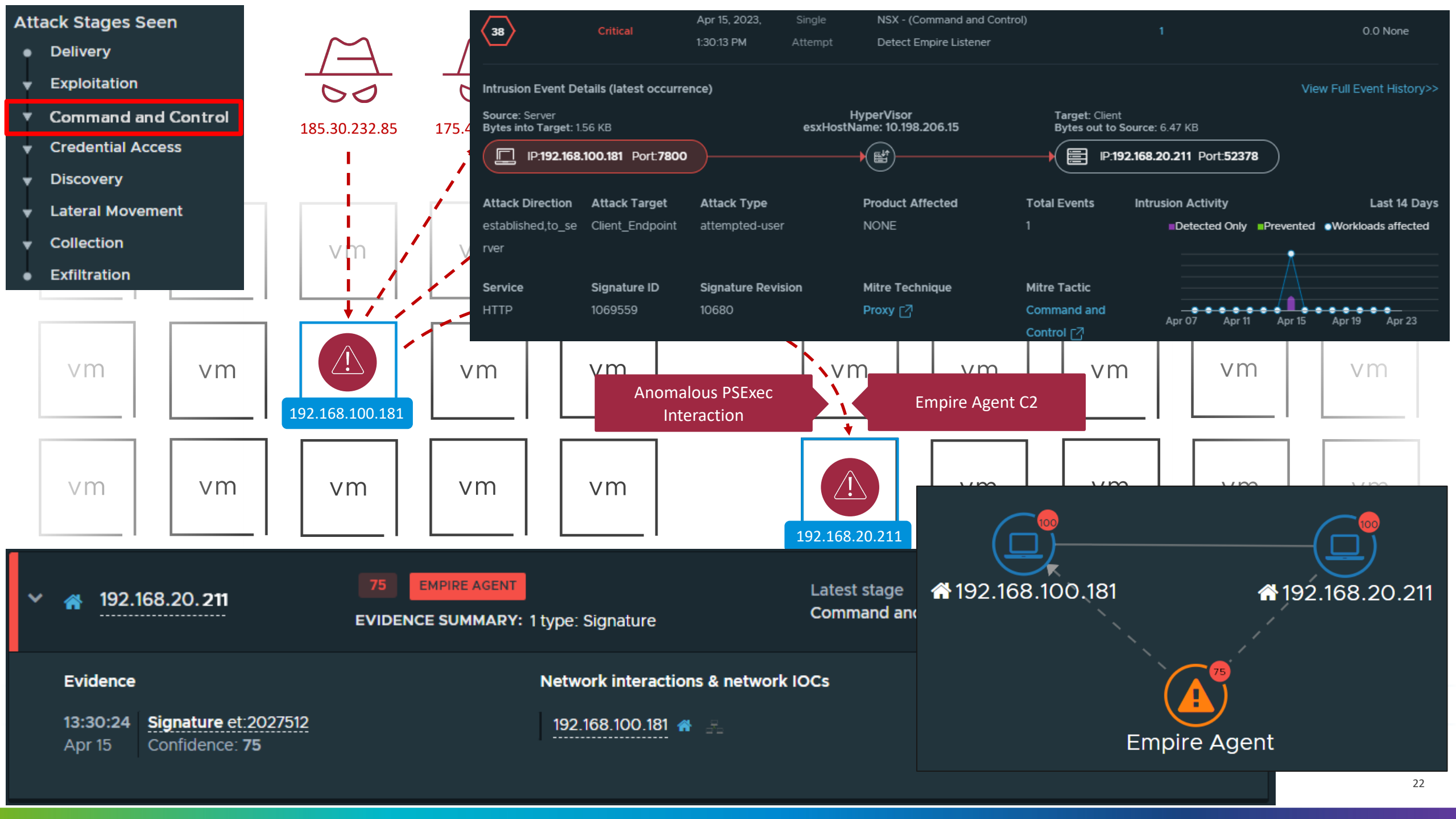

185.30.232.85
175.45.176.136
34.102.136.180
Cryptowall C2
192.168.100.181
vm
Hypervisor
Hypervisor

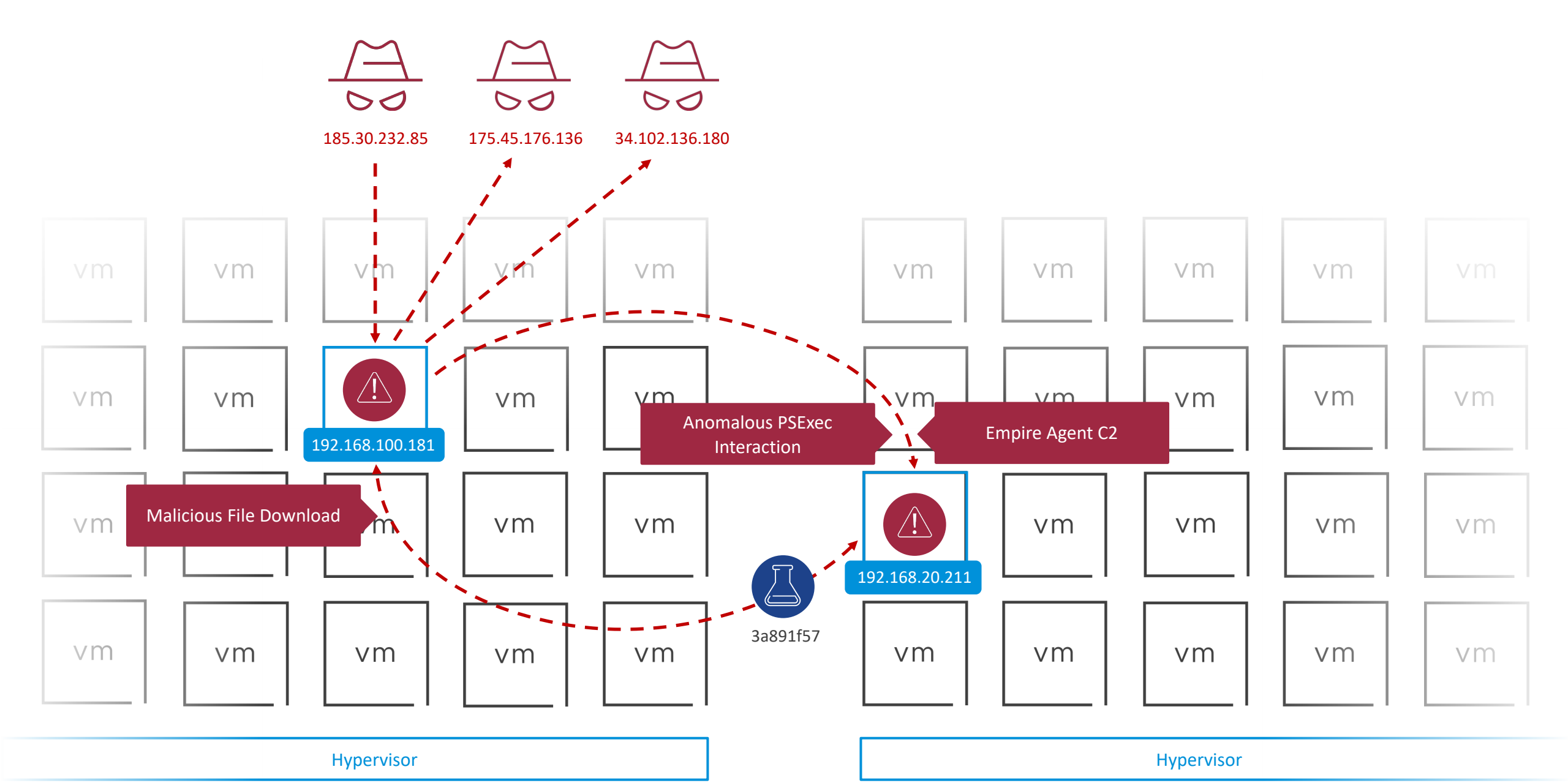

Attack Stages Seen
Delivery
Exploitation
Command and Control
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
185.30.232.85
175.45.
70
Critical
Apr 15, 2023, 1:49:12 PM
Multiple Attempts
ET MALWARE CryptoWall Check-in
2
0.0 None
Intrusion Event Details (latest occurrence)
View Full Event History>>
Source: Server
Bytes into Target: 766.00 Bytes
HyperVisor
esxHostName: 10.198.206.15
Target: Client
Bytes out to Source: 60.00 Bytes
IP:34.102.136.180 Port:80
IP: 192.168.100.181 Port:49226
Attack Direction
established,to_server
Attack Target
NONE
Attack Type
trojan-activity
Product Affected
NONE
Total Events
4
Intrusion Activity
Detected Only
Prevented
Workloads affected
Last 14 Days
Apr 07
Apr 11
Apr 15
Apr 19
Apr 23
Service
HTTP
Signature ID
2018452
Signature Revision
18
Mitre Technique
-
Mitre Tactic
-
vm
192.168.100.181
192.168.100.181
70
CRYPTOWALL
EVIDENCE SUMMARY: 1 type: Signature
Latest stage
Command and Control
Evidence
12:13:36
Apr 15
Signature et:2018452
Confidence: 70
Network interactions & network IOCs
34.102.136.180
34.102.136.180
100
CryptoWall
100
192.168.100.181

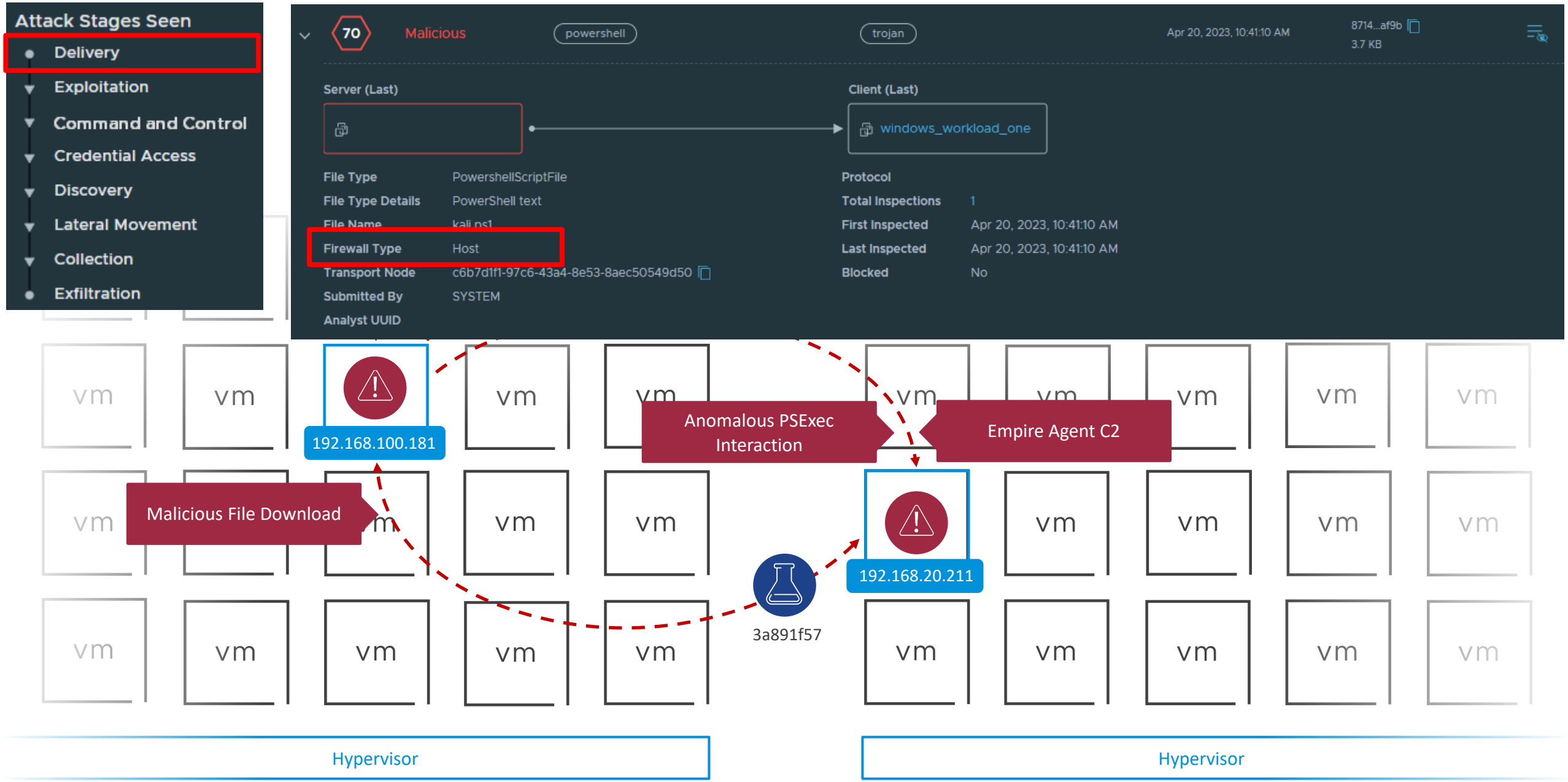

185.30.232.85
175.45.176.136
34.102.136.180
vm
192.168.100.181
Anomalous PSExec Interaction
192.168.20.211
Hypervisor
Hypervisor

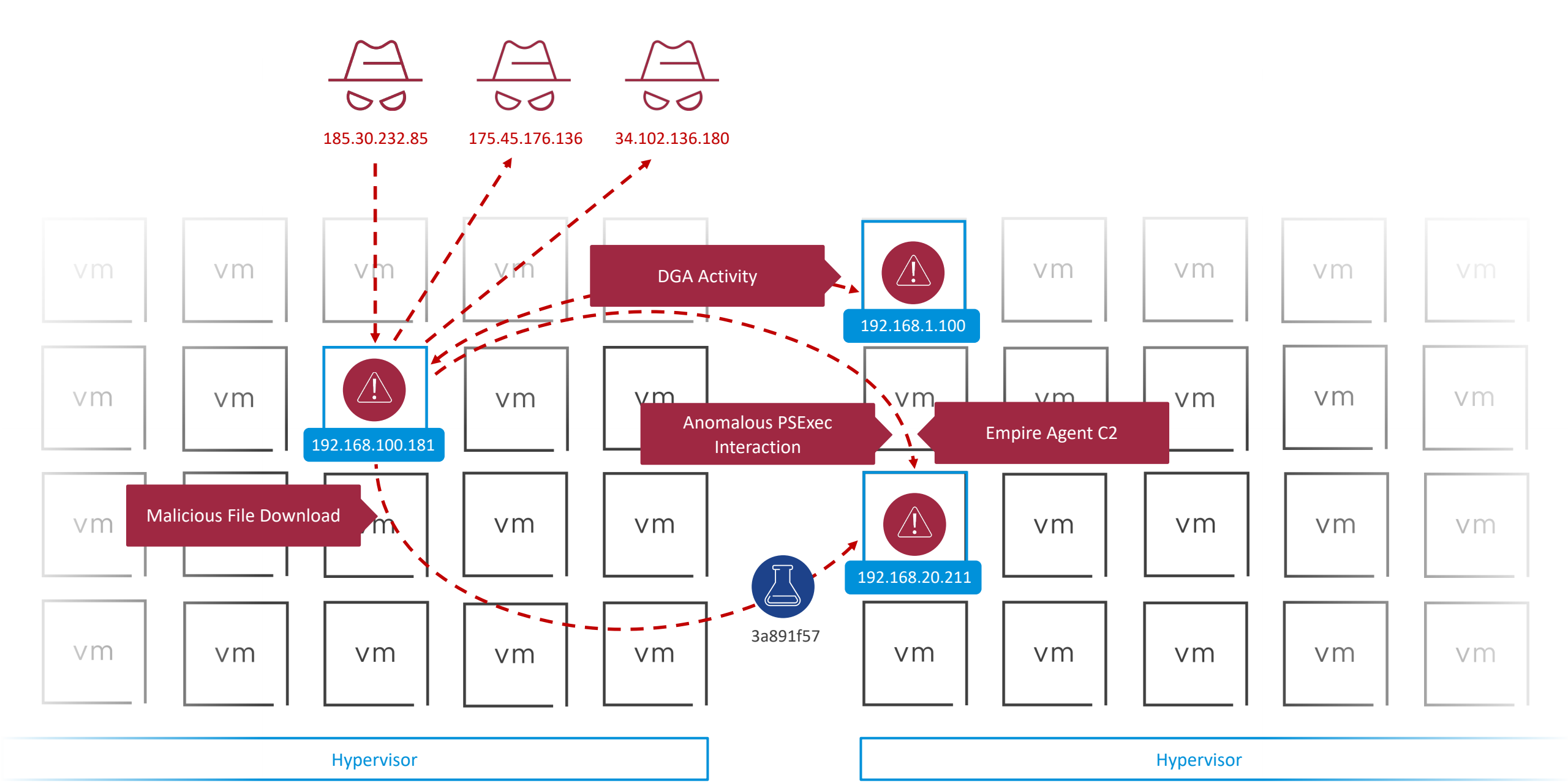

Attack Stages Seen
Delivery
Exploitation
Command and Control
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
185.30.232.85
14
Suspicious
Apr 15, 2023, 12:37:53 PM
Multiple Attempts
ET POLICY PsExec service created
1
0.0 None
Intrusion Event Details (latest occurrence)
View Full Event History>>
Source: Client
Bytes into Target: 402.65 KB
HyperVisor
esxHostName: 10.198.206.15
Target: Server
Bytes out to Source: 430.62 KB
IP:192.168.100.181 Port:49239
IP:192.168.20.211 Port:445
Attack Direction
to_server,established
Attack Target
NONE
Attack Type
suspicious-filename-detect
Product Affected
NONE
Total Events
2
Intrusion Activity
Detected Only
Prevented
Workloads affected
Last 14 Days
Apr 07
Apr 11
Apr 15
Apr 19
Apr 23
Service
TCP
Signature ID
2010781
Signature Revision
3
Mitre Technique
Service Execution
Mitre Tactic
Execution
192.168.100.181
Anomalous PSExec Interaction
100
25
192.168.100.181
192.168.20.211
70
Anomalous PSExec Interaction
192.168.20.211
25
ANOMALOUS PSEXEC INTERACTION
EVIDENCE SUMMARY: 1 type: Unusual behavior
Evidence
12:20:19
Apr 15
Unusual behavior lateral movement
Confidence: 70
Network interactions & network IOCs
192.168.100.181
View all threat details

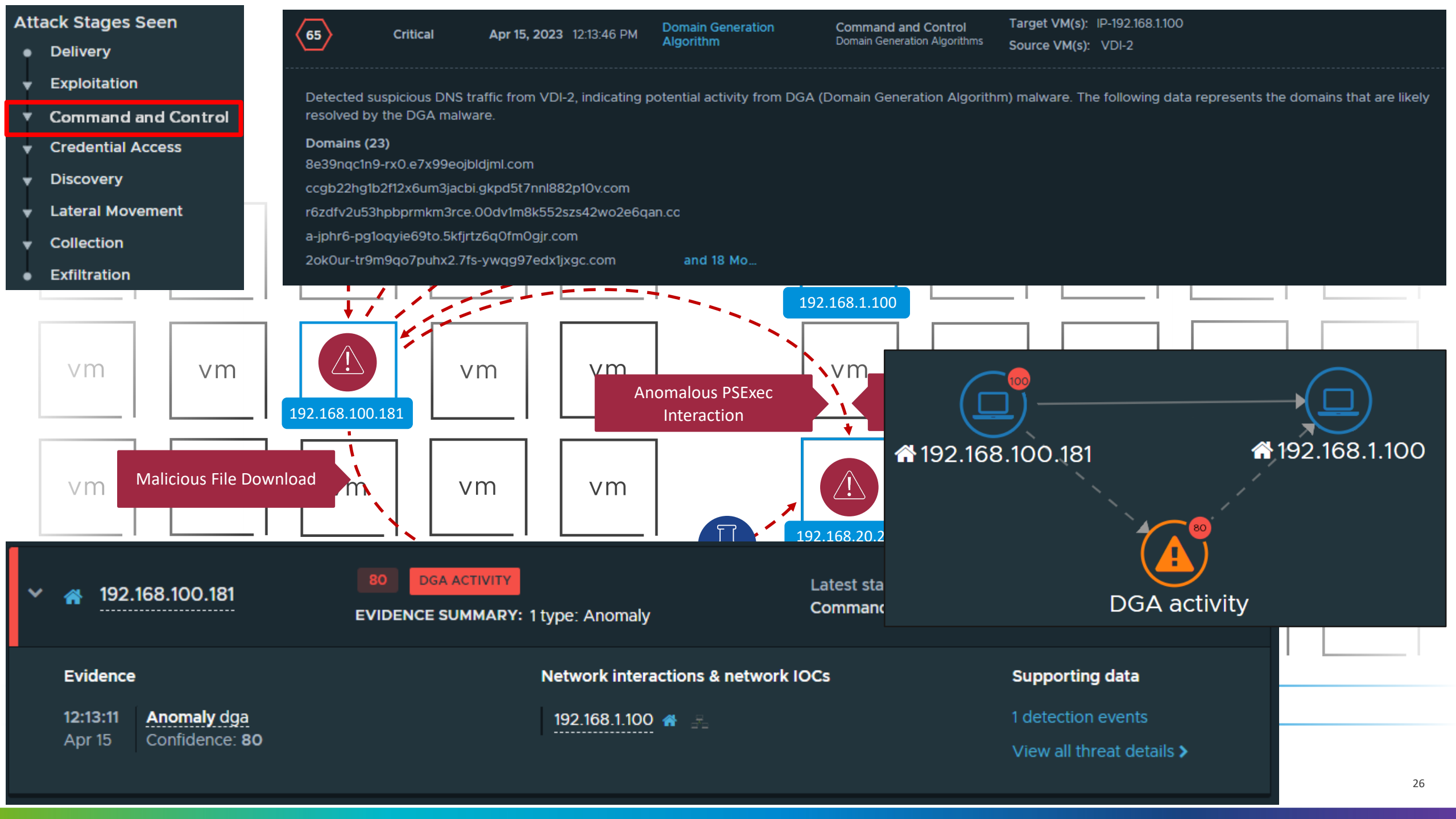

185.30.232.85
175.45.176.136
34.102.136.180
192.168.100.181
Anomalous PSExec Interaction
Empire Agent C2
192.168.20.211
Hypervisor
Hypervisor

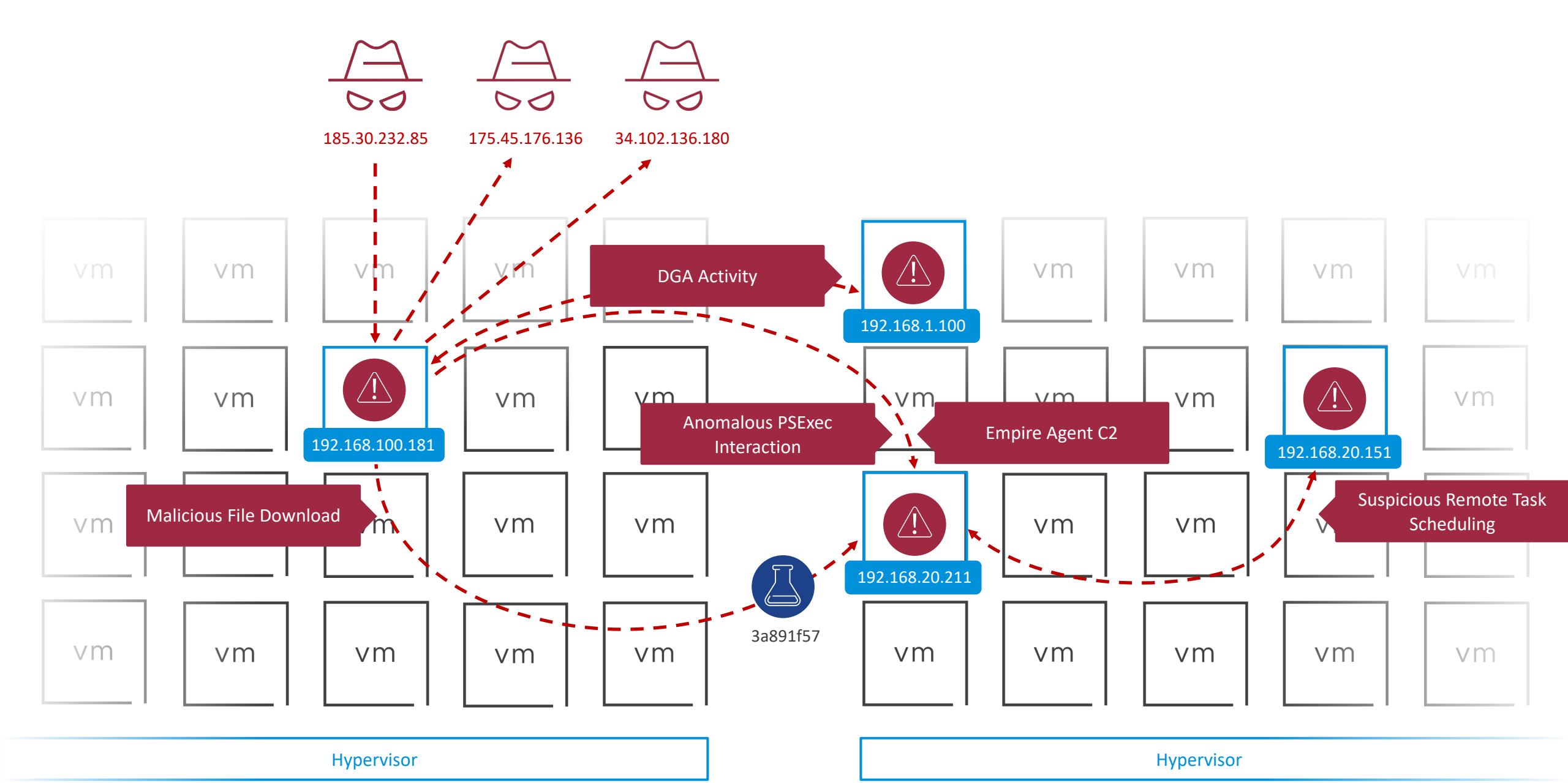

Attack Stages Seen
Delivery
Exploitation
Command and Control
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
185.30.232.85
38
Critical
Apr 15, 2023, 1:30:13 PM
Single Attempt
NSX - (Command and Control) Detect Empire Listener
1
0.0 None
Intrusion Event Details (latest occurrence)
View Full Event History>>
Source: Server
Bytes into Target: 1.56 KB
HyperVisor
esxHostName: 10.198.206.15
Target: Client
Bytes out to Source: 6.47 KB
IP:192.168.100.181 Port:7800
IP:192.168.20.211 Port:52378
Attack Direction
established,to_server
Attack Target
Client_Endpoint
Attack Type
attempted-user
Product Affected
NONE
Total Events
1
Intrusion Activity
Detected Only
Prevented
Workloads affected
Last 14 Days
Apr 07
Apr 11
Apr 15
Apr 19
Apr 23
Service
HTTP
Signature ID
1069559
Signature Revision
10680
Mitre Technique
Proxy
Mitre Tactic
Command and Control
192.168.100.181
Anomalous PSExec Interaction
Empire Agent C2
192.168.20.211
192.168.20.211
75
EMPIRE AGENT
EVIDENCE SUMMARY: 1 type: Signature
Latest stage
Command and
Evidence
13:30:24
Apr 15
Signature et:2027512
Confidence: 75
Network interactions & network IOCs
192.168.100.181
100
100
192.168.100.181
192.168.20.211
75
Empire Agent

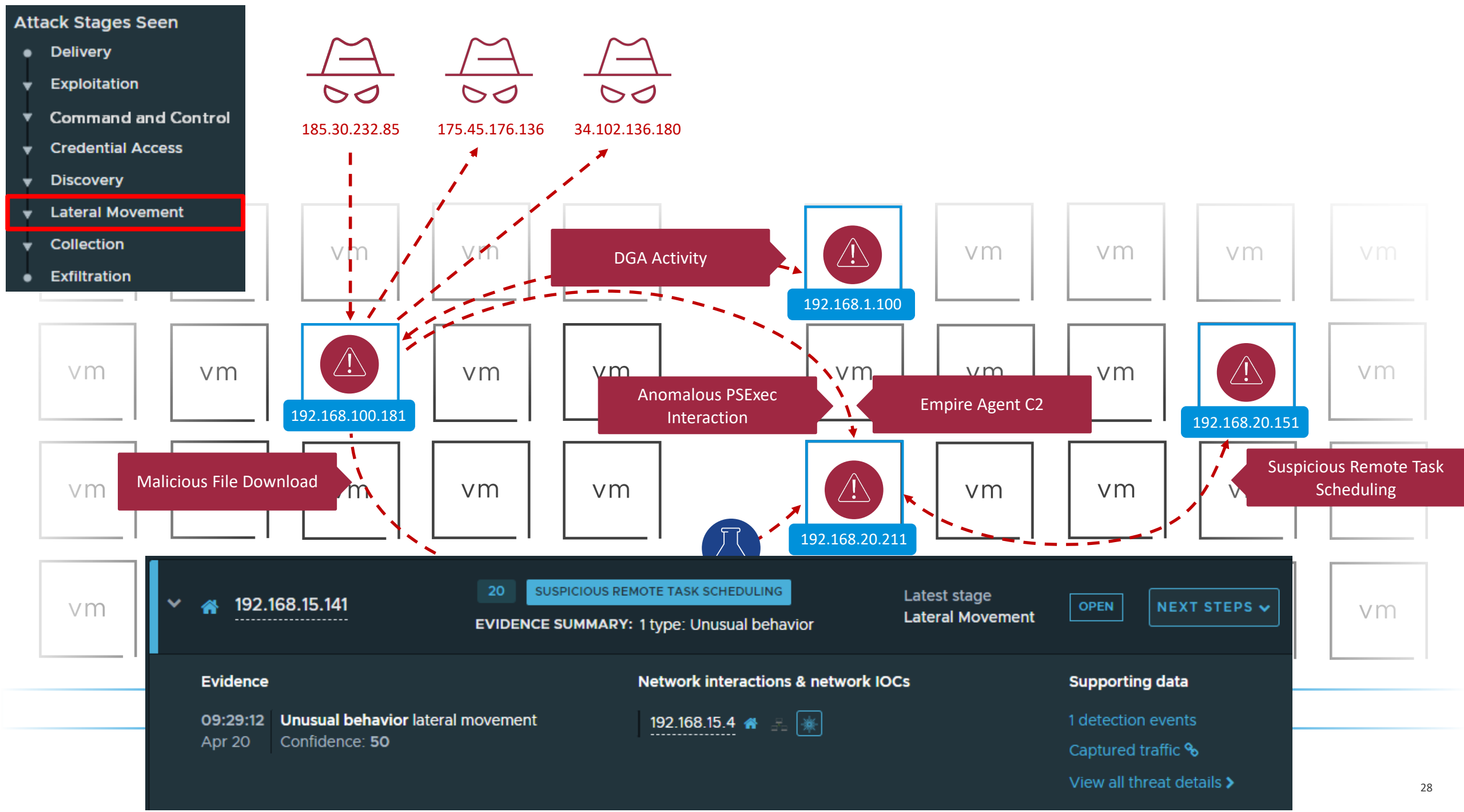

185.30.232.85
175.45.176.136
34.102.136.180
192.168.100.181
Anomalous PSExec Interaction
Empire Agent C2
Malicious File Download
192.168.20.211
3a891f57
Hypervisor
Hypervisor

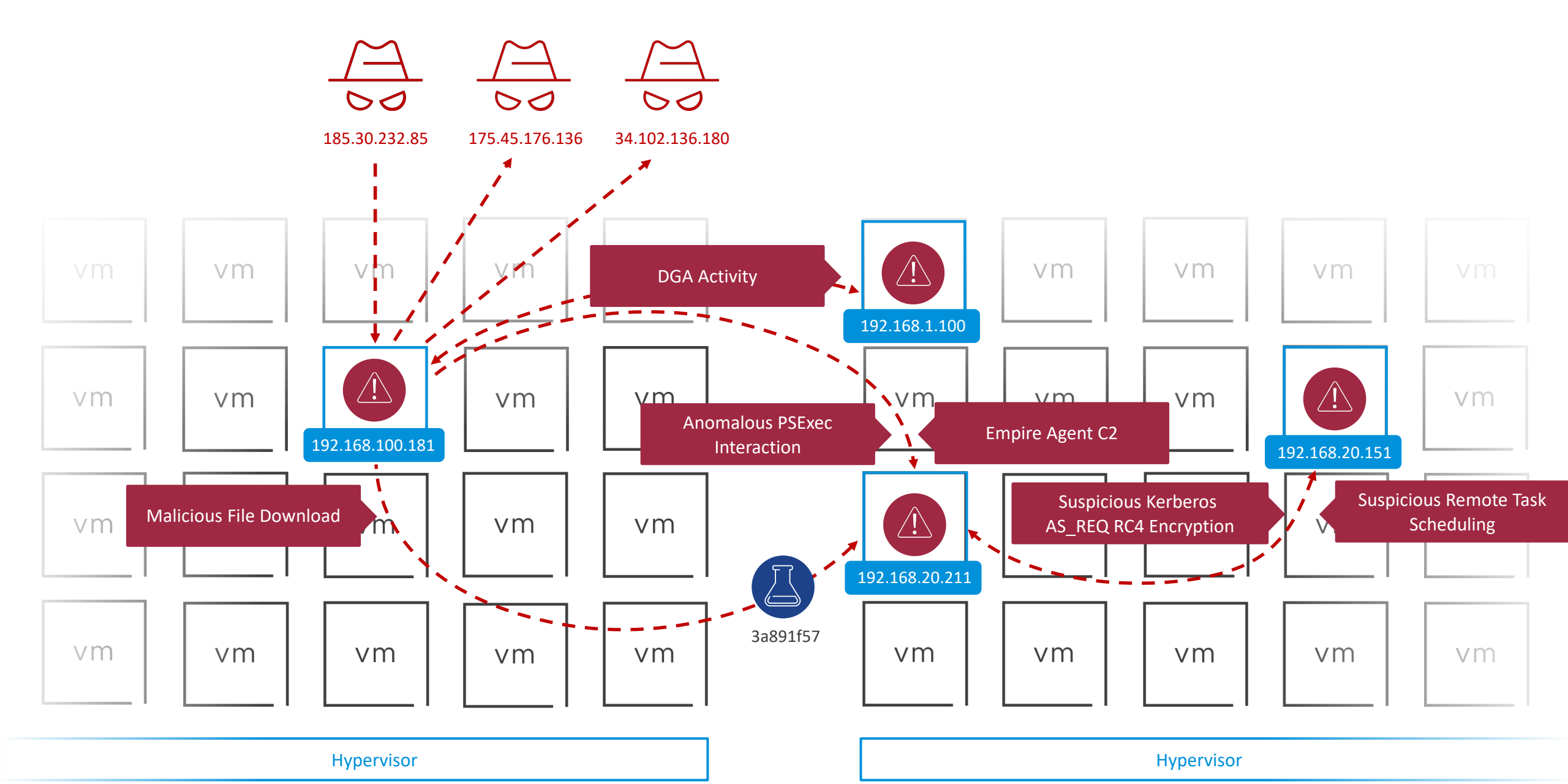

Attack Stages Seen
Delivery
Exploitation
Command and Control
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
70
Malicious
powershell
trojan
Apr 20, 2023, 10:41:10 AM
8714...af9b
3.7 KB
Server (Last)
Client (Last)
windows_workload_one
File Type
PowershellScriptFile
File Type Details
PowerShell text
File Name
kali.ps1
Firewall Type
Host
Transport Node
c6b7d1f1-97c6-43a4-8e53-8aec50549d50
Submitted By
SYSTEM
Analyst UUID
Protocol
Total Inspections
1
First Inspected
Apr 20, 2023, 10:41:10 AM
Last Inspected
Apr 20, 2023, 10:41:10 AM
Blocked
No
vm
192.168.100.181
Anomalous PSExec Interaction
Empire Agent C2
Malicious File Download
192.168.20.211
3a891f57
Hypervisor
Hypervisor

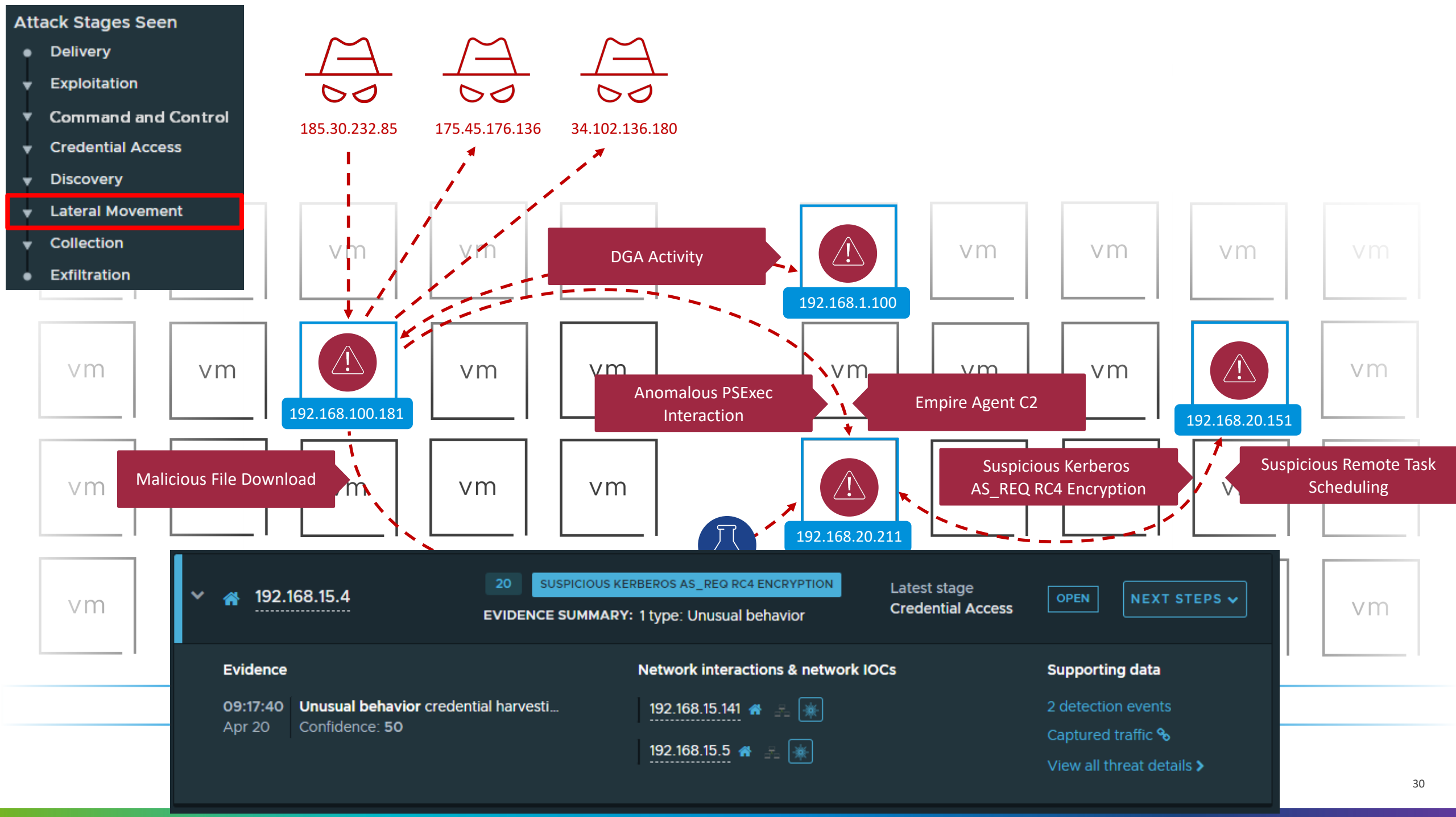

185.30.232.85
175.45.176.136
34.102.136.180
DGA Activity
192.168.1.100
192.168.100.181
Anomalous PSExec Interaction
Empire Agent C2
Malicious File Download
192.168.20.211
3a891f57
Hypervisor
Hypervisor

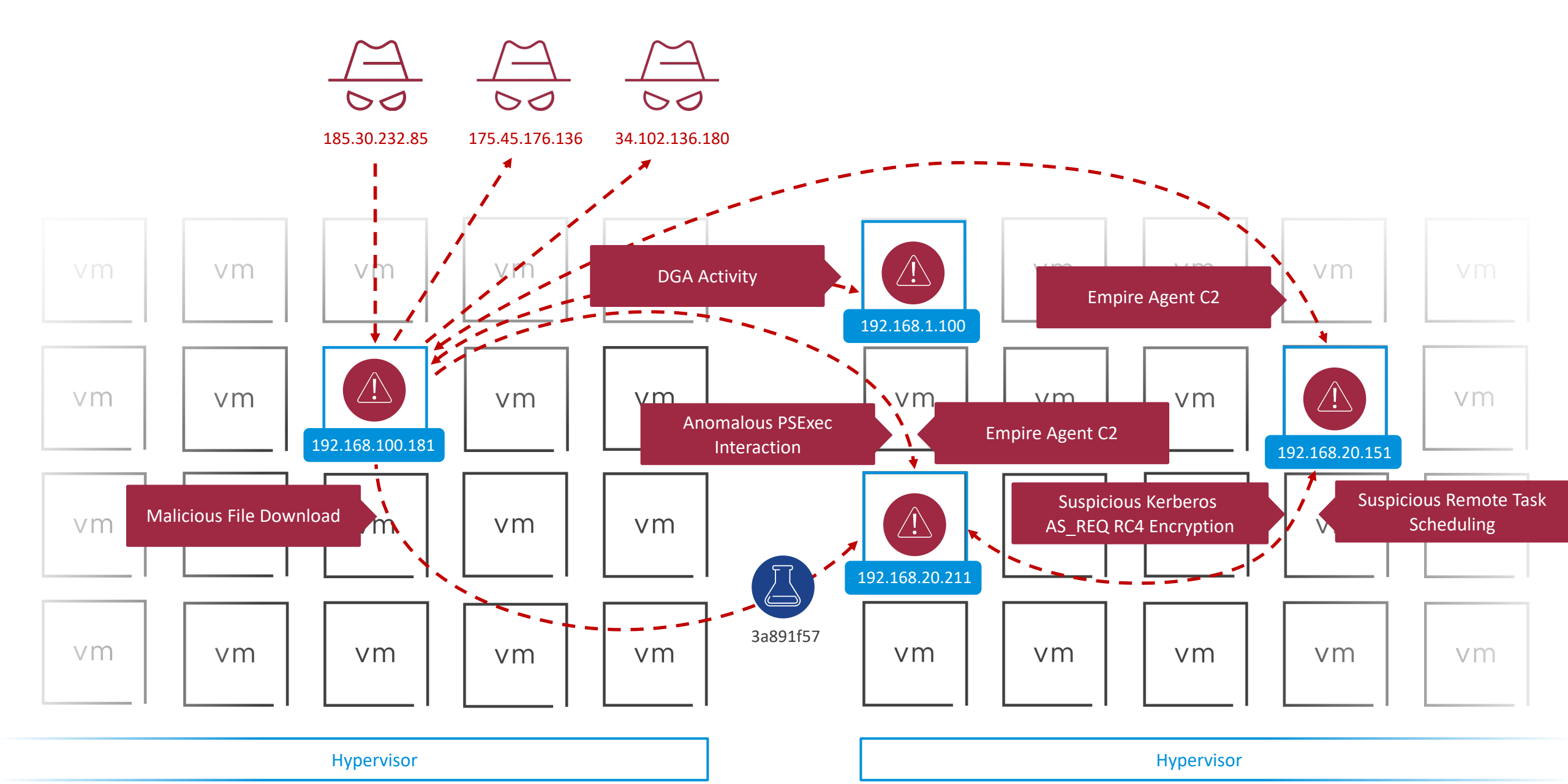

Attack Stages Seen
Delivery
Exploitation
Command and Control
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
65
Critical
Apr 15, 2023 12:13:46 PM
Domain Generation Algorithm
Command and Control
Domain Generation Algorithms
Target VM(s): IP-192.168.1.100
Source VM(s): VDI-2
Detected suspicious DNS traffic from VDI-2, indicating potential activity from DGA (Domain Generation Algorithm) malware. The following data represents the domains that are likely resolved by the DGA malware.
Domains (23)
8e39nqc1n9-rx0.e7x99eojbldjml.com
ccgb22hg1b2f12x6um3jacbi.gkpd5t7nnl882p10v.com
r6zdfv2u53hpbprmkm3rce.00dv1m8k552szs42wo2e6qan.cc
a-jphr6-pg1oqyie69to.5kfjrtz6q0fm0gjr.com
2ok0ur-tr9m9qo7puhx2.7fs-ywqg97edx1jxgc.com
and 18 Mo...
192.168.1.100
vm
192.168.100.181
Anomalous PSExec Interaction
Malicious File Download
192.168.20.2
100
192.168.100.181
192.168.1.100
80
DGA activity
192.168.100.181
80
DGA ACTIVITY
EVIDENCE SUMMARY: 1 type: Anomaly
Latest sta
Commanc
Evidence
12:13:11
Apr 15
Anomaly dga
Confidence: 80
Network interactions & network IOCs
192.168.1.100
Supporting data
1 detection events
View all threat details >

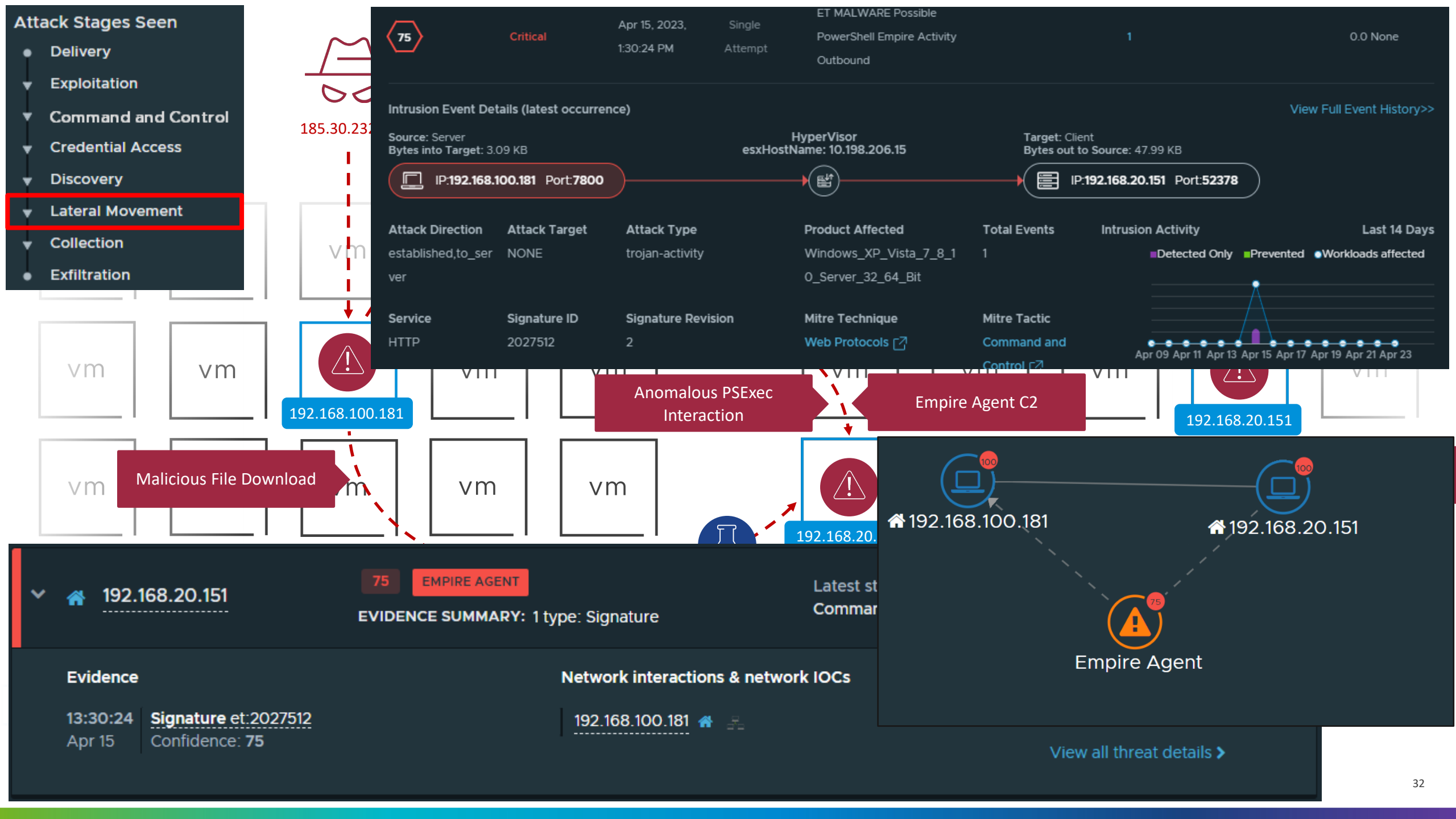

185.30.232.85
175.45.176.136
34.102.136.180
DGA Activity
192.168.1.100
192.168.100.181
Anomalous PSExec Interaction
Empire Agent C2
192.168.20.151
Malicious File Download
Suspicious Remote Task Scheduling
192.168.20.211
3a891f57
Hypervisor
Hypervisor

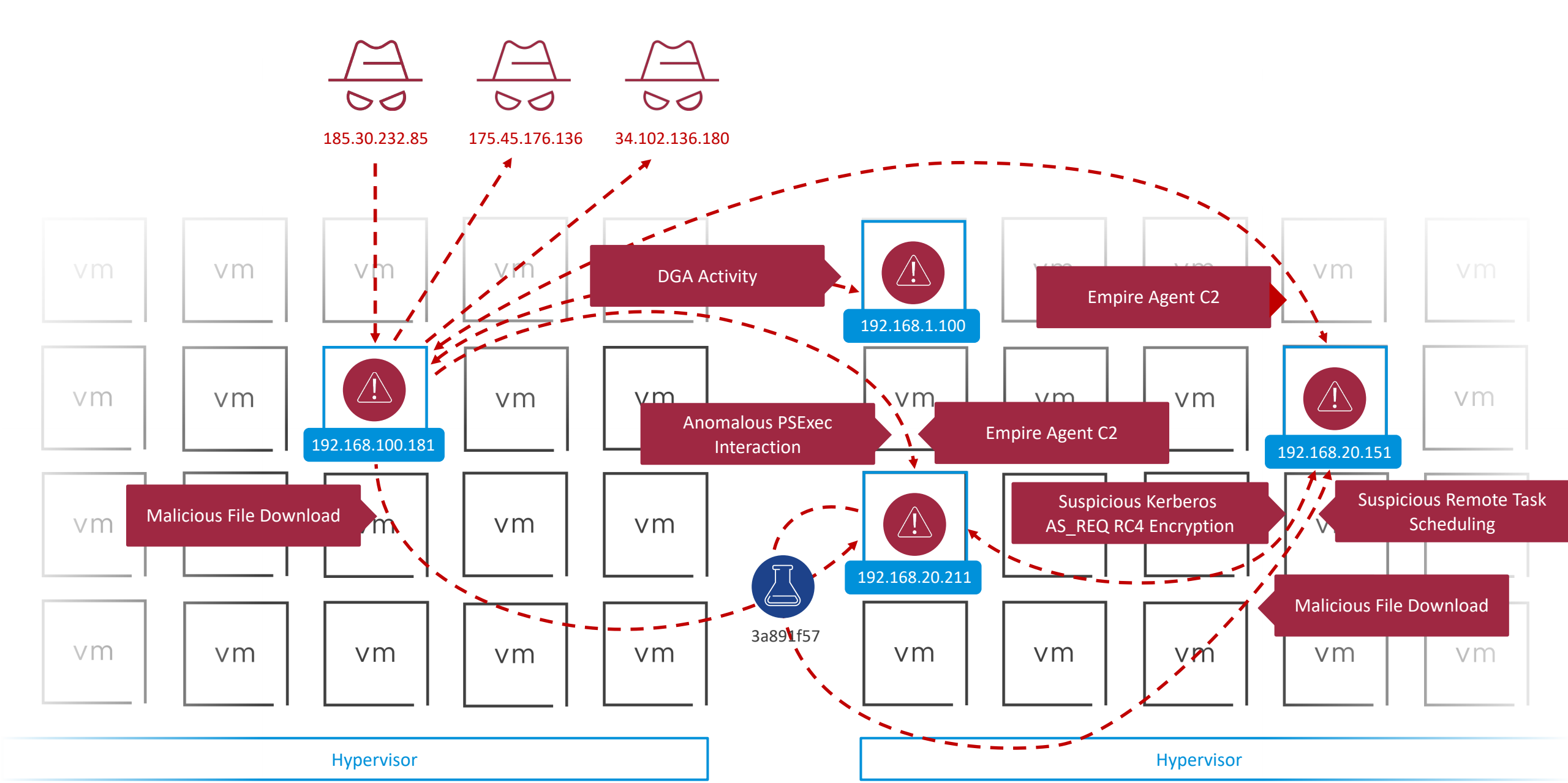

Attack Stages Seen
Delivery
Exploitation
Command and Control
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
185.30.232.85
175.45.176.136
34.102.136.180
DGA Activity
192.168.1.100
192.168.100.181
Anomalous PSExec Interaction
Empire Agent C2
192.168.20.151
Malicious File Download
Suspicious Remote Task Scheduling
192.168.20.211
192.168.15.141
20
SUSPICIOUS REMOTE TASK SCHEDULING
EVIDENCE SUMMARY: 1 type: Unusual behavior
Latest stage
Lateral Movement
OPEN
NEXT STEPS
Evidence
09:29:12
Apr 20
Unusual behavior lateral movement
Confidence: 50
Network interactions & network IOCs
192.168.15.4
Supporting data
1 detection events
Captured traffic
View all threat details

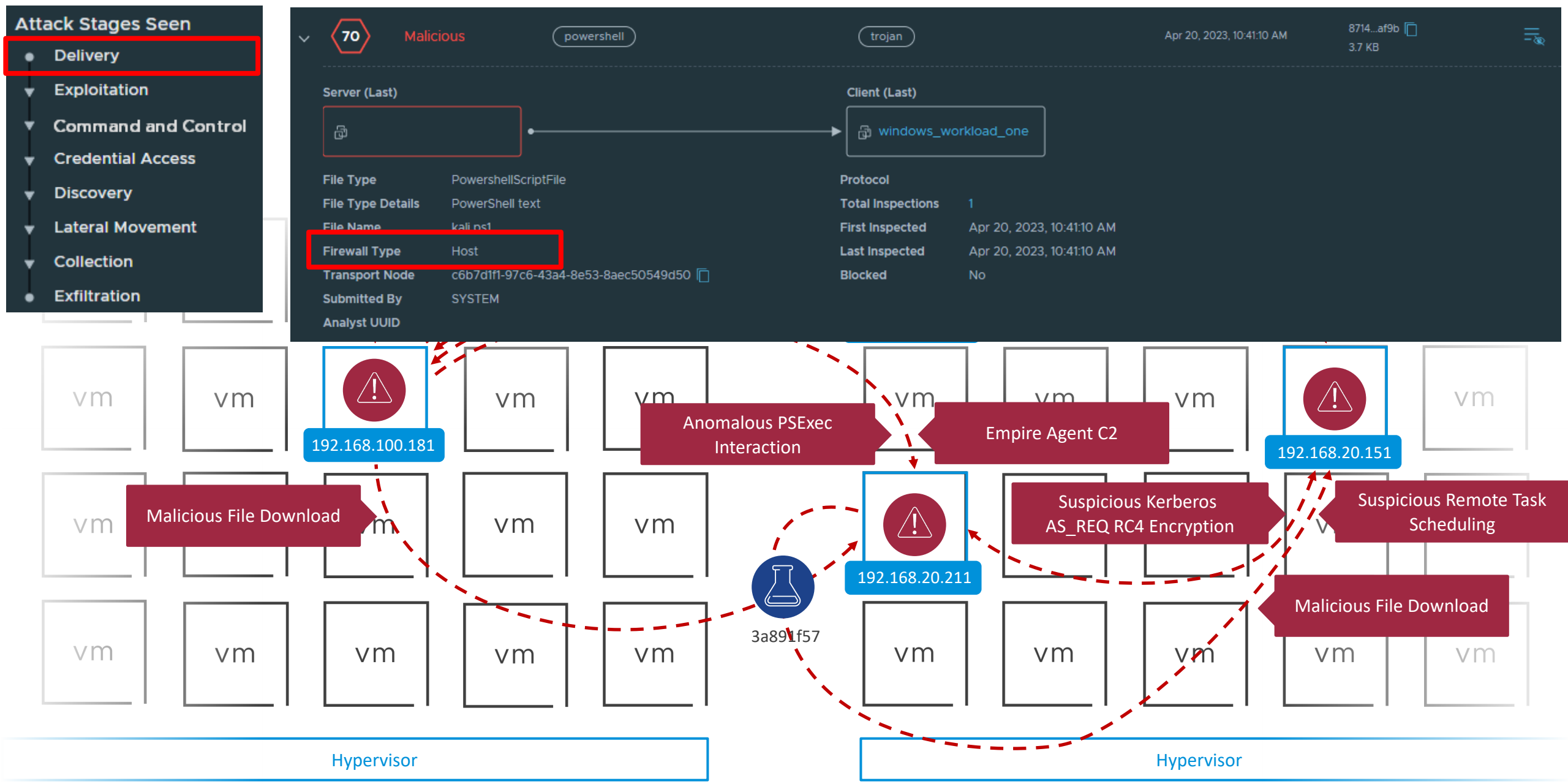

185.30.232.85
175.45.176.136
34.102.136.180
DGA Activity
192.168.1.100
192.168.100.181
Anomalous PSExec Interaction
Empire Agent C2
192.168.20.151
Malicious File Download
Suspicious Kerberos AS_REQ RC4 Encryption
Suspicious Remote Task Scheduling
192.168.20.211
3a891f57
Hypervisor
Hypervisor

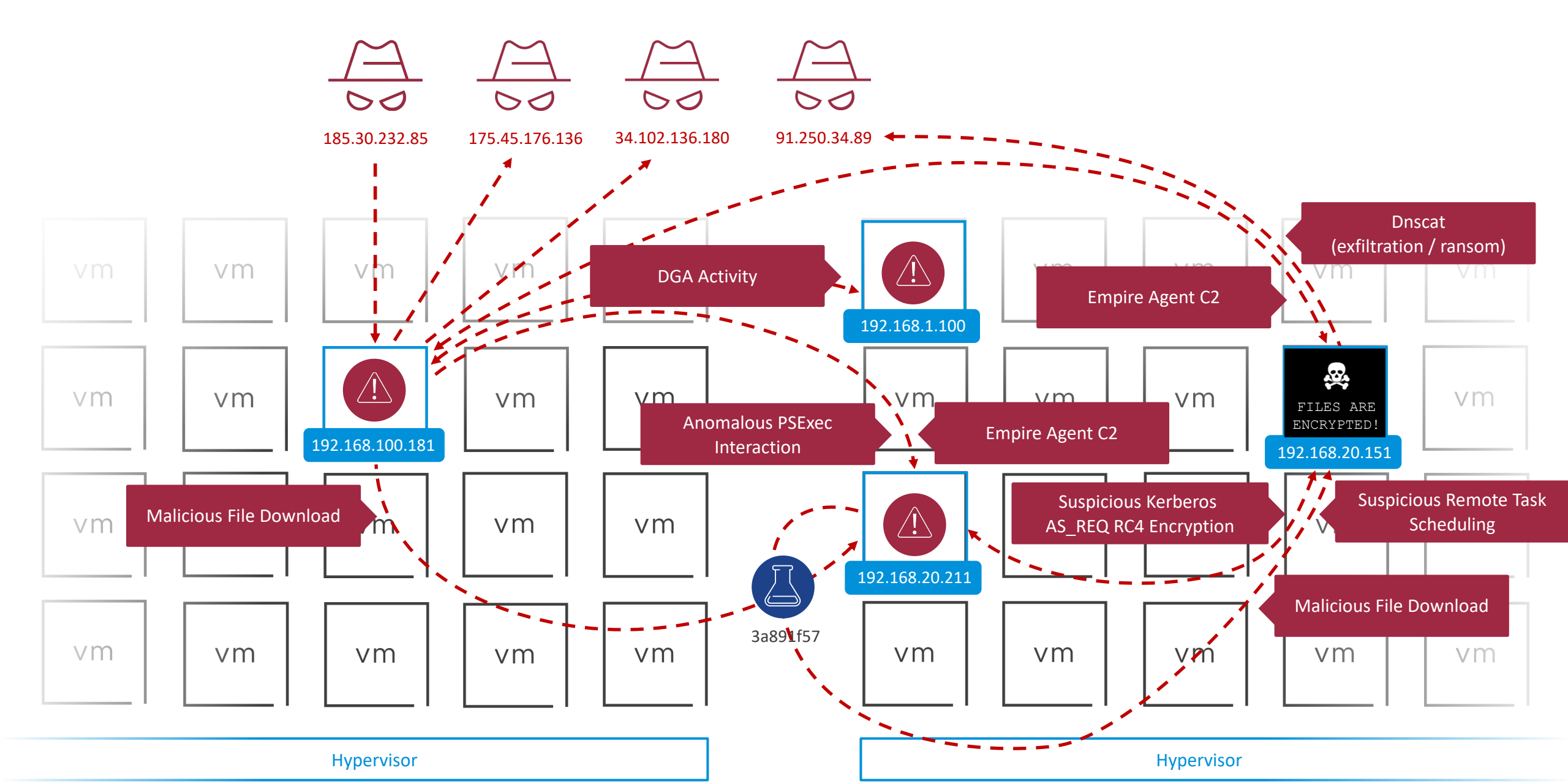

Attack Stages Seen
Delivery
Exploitation
Command and Control
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
185.30.232.85
175.45.176.136
34.102.136.180
DGA Activity
192.168.1.100
192.168.100.181
Anomalous PSExec Interaction
Empire Agent C2
192.168.20.151
Malicious File Download
Suspicious Kerberos AS_REQ RC4 Encryption
Suspicious Remote Task Scheduling
192.168.20.211
192.168.15.4
20
SUSPICIOUS KERBEROS AS_REQ RC4 ENCRYPTION
EVIDENCE SUMMARY: 1 type: Unusual behavior
Latest stage
Credential Access
OPEN
NEXT STEPS
Evidence
09:17:40
Apr 20
Unusual behavior credential harvesti...
Confidence: 50
Network interactions & network IOCs
192.168.15.141
192.168.15.5
Supporting data
2 detection events
Captured traffic
View all threat details

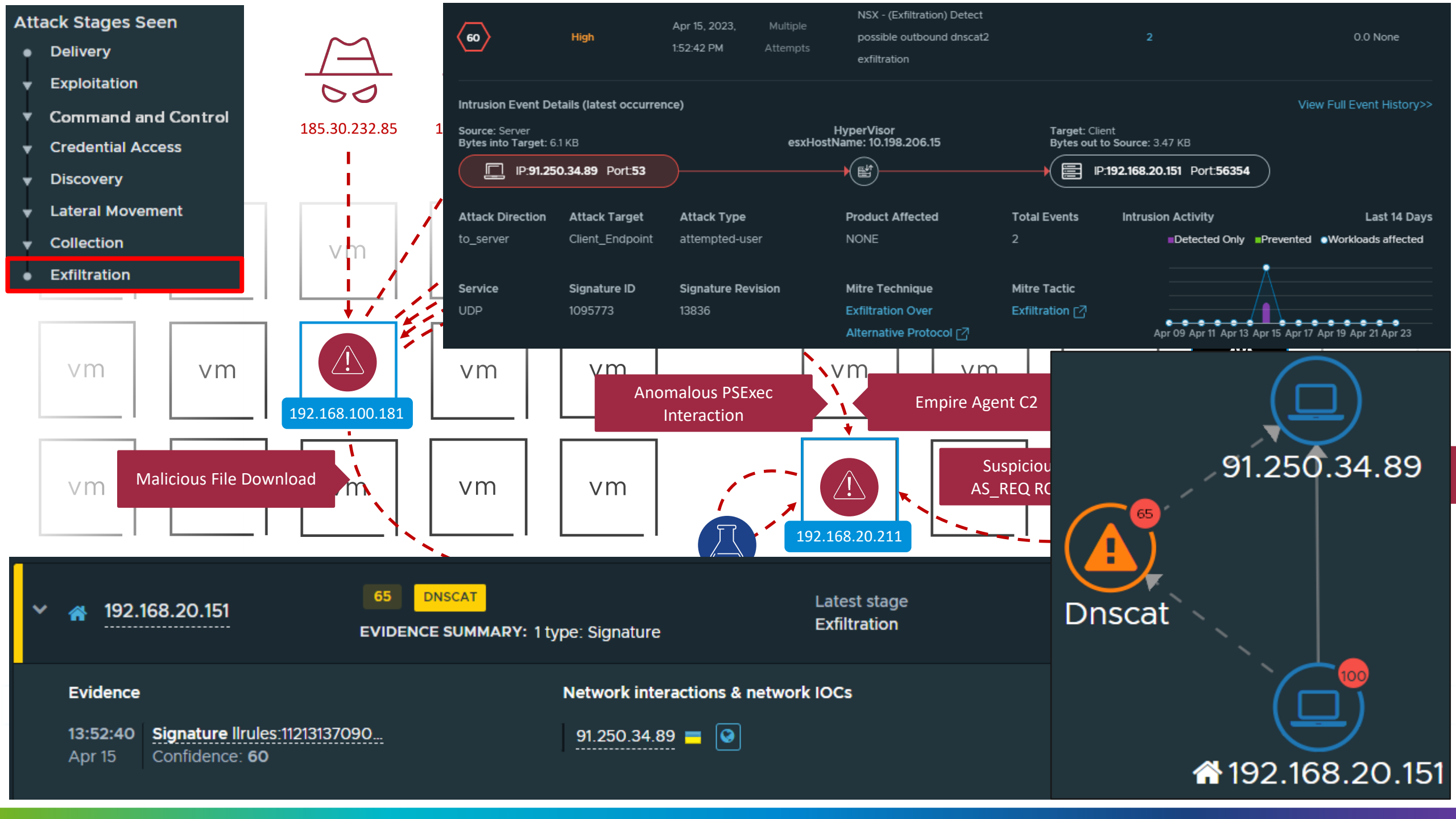

185.30.232.85
175.45.176.136
34.102.136.180
DGA Activity
192.168.1.100
Empire Agent C2
192.168.100.181
Anomalous PSExec Interaction
Empire Agent C2
192.168.20.151
Malicious File Download
Suspicious Kerberos AS_REQ RC4 Encryption
Suspicious Remote Task Scheduling
192.168.20.211
3a891f57
Hypervisor
Hypervisor


Attack Stages Seen
Delivery
Exploitation
Command and Control
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
75
Critical
Apr 15, 2023, 1:30:24 PM
Single Attempt
ET MALWARE Possible PowerShell Empire Activity Outbound
1
0.0 None
Intrusion Event Details (latest occurrence)
View Full Event History>>
Source: Server
Bytes into Target: 3.09 KB
HyperVisor
esxHostName: 10.198.206.15
Target: Client
Bytes out to Source: 47.99 KB
IP:192.168.100.181 Port:7800
IP:192.168.20.151 Port:52378
Attack Direction
established,to_server
Attack Target
NONE
Attack Type
trojan-activity
Product Affected
Windows_XP_Vista_7_8_10_Server_32_64_Bit
Total Events
1
Intrusion Activity
Last 14 Days
Detected Only
Prevented
Workloads affected
Apr 09 Apr 11 Apr 13 Apr 15 Apr 17 Apr 19 Apr 21 Apr 23
Service
HTTP
Signature ID
2027512
Signature Revision
2
Mitre Technique
Web Protocols
Mitre Tactic
Command and Control
185.30.23
192.168.100.181
192.168.20.151
Anomalous PSExec Interaction
Empire Agent C2
Malicious File Download
192.168.20.151
75
EMPIRE AGENT
EVIDENCE SUMMARY: 1 type: Signature
Evidence
13:30:24
Apr 15
Signature et:2027512
Confidence: 75
Network interactions & network IOCs
192.168.100.181
View all threat details
100
100
192.168.100.181
192.168.20.151
75
Empire Agent


185.30.232.85
175.45.176.136
34.102.136.180
DGA Activity
192.168.1.100
Empire Agent C2
192.168.100.181
Anomalous PSExec Interaction
Empire Agent C2
192.168.20.151
Malicious File Download
Suspicious Kerberos AS_REQ RC4 Encryption
Suspicious Remote Task Scheduling
192.168.20.211
3a891f57
Malicious File Download
Hypervisor
Hypervisor


Attack Stages Seen
Delivery
Exploitation
Command and Control
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
70
Malicious
powershell
trojan
Apr 20, 2023, 10:41:10 AM
8714...af9b
3.7 KB
Server (Last)
Client (Last)
windows_workload_one
File Type
PowershellScriptFile
File Type Details
PowerShell text
File Name
kali.ps1
Firewall Type
Host
Transport Node
c6b7d1f1-97c6-43a4-8e53-8aec50549d50
Submitted By
SYSTEM
Analyst UUID
Protocol
Total Inspections
1
First Inspected
Apr 20, 2023, 10:41:10 AM
Last Inspected
Apr 20, 2023, 10:41:10 AM
Blocked
No
192.168.100.181
Anomalous PSExec Interaction
Empire Agent C2
192.168.20.151
Malicious File Download
Suspicious Kerberos AS_REQ RC4 Encryption
Suspicious Remote Task Scheduling
192.168.20.211
3a891f57
Malicious File Download
Hypervisor
Hypervisor


185.30.232.85
175.45.176.136
34.102.136.180
91.250.34.89
DGA Activity
192.168.1.100
Empire Agent C2
Dnscat
(exfiltration / ransom)
192.168.100.181
Anomalous PSExec
Interaction
Empire Agent C2
FILES ARE
ENCRYPTED!
192.168.20.151
Malicious File Download
Suspicious Kerberos
AS_REQ RC4 Encryption
Suspicious Remote Task
Scheduling
192.168.20.211
3a891f57
Malicious File Download
Hypervisor
Hypervisor


Attack Stages Seen
Delivery
Exploitation
Command and Control
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
185.30.232.85
60
High
Apr 15, 2023, 1:52:42 PM
Multiple Attempts
NSX - (Exfiltration) Detect possible outbound dnscat2 exfiltration
2
0.0 None
Intrusion Event Details (latest occurrence)
View Full Event History>>
Source: Server
Bytes into Target: 6.1 KB
IP:91.250.34.89 Port:53
HyperVisor
esxHostName: 10.198.206.15
Target: Client
Bytes out to Source: 3.47 KB
IP:192.168.20.151 Port:56354
Attack Direction
to_server
Attack Target
Client_Endpoint
Attack Type
attempted-user
Product Affected
NONE
Total Events
2
Intrusion Activity
Last 14 Days
Detected Only
Prevented
Workloads affected
Apr 09 Apr 11 Apr 13 Apr 15 Apr 17 Apr 19 Apr 21 Apr 23
Service
UDP
Signature ID
1095773
Signature Revision
13836
Mitre Technique
Exfiltration Over Alternative Protocol
Mitre Tactic
Exfiltration
192.168.100.181
Malicious File Download
Anomalous PSExec Interaction
Empire Agent C2
192.168.20.211
Suspiciou
AS_REQ RC
192.168.20.151
65
DNSCAT
EVIDENCE SUMMARY: 1 type: Signature
Latest stage
Exfiltration
Evidence
13:52:40
Apr 15
Signature lIrules:11213137090...
Confidence: 60
Network interactions & network IOCs
91.250.34.89
91.250.34.89
65
Dnscat
100
192.168.20.151

Thank You