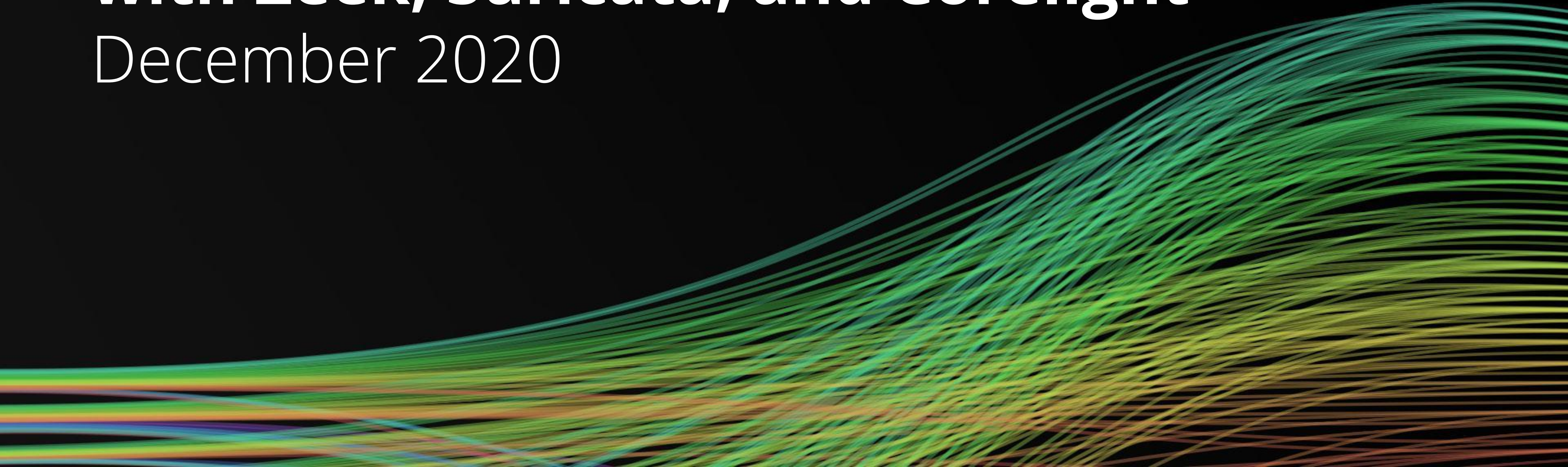
corelight

Finding SolarWinds / SUNBURST backdoors with Zeek, Suricata, and Corelight

December 2020



Today's speakers

Aaron Soto
Director of Learning

corelight

Alex Kirk
Global Principal, Suricata

corelight

Agenda

1. A brief landscape
2. What we know & how we know it
3. Reviewing Suricata rules
4. Importing Suricata rulesets from public repositories
5. Applying future knowledge to past Zeek data
6. Searching through Zeek/Corelight data for IOCs

Landscape

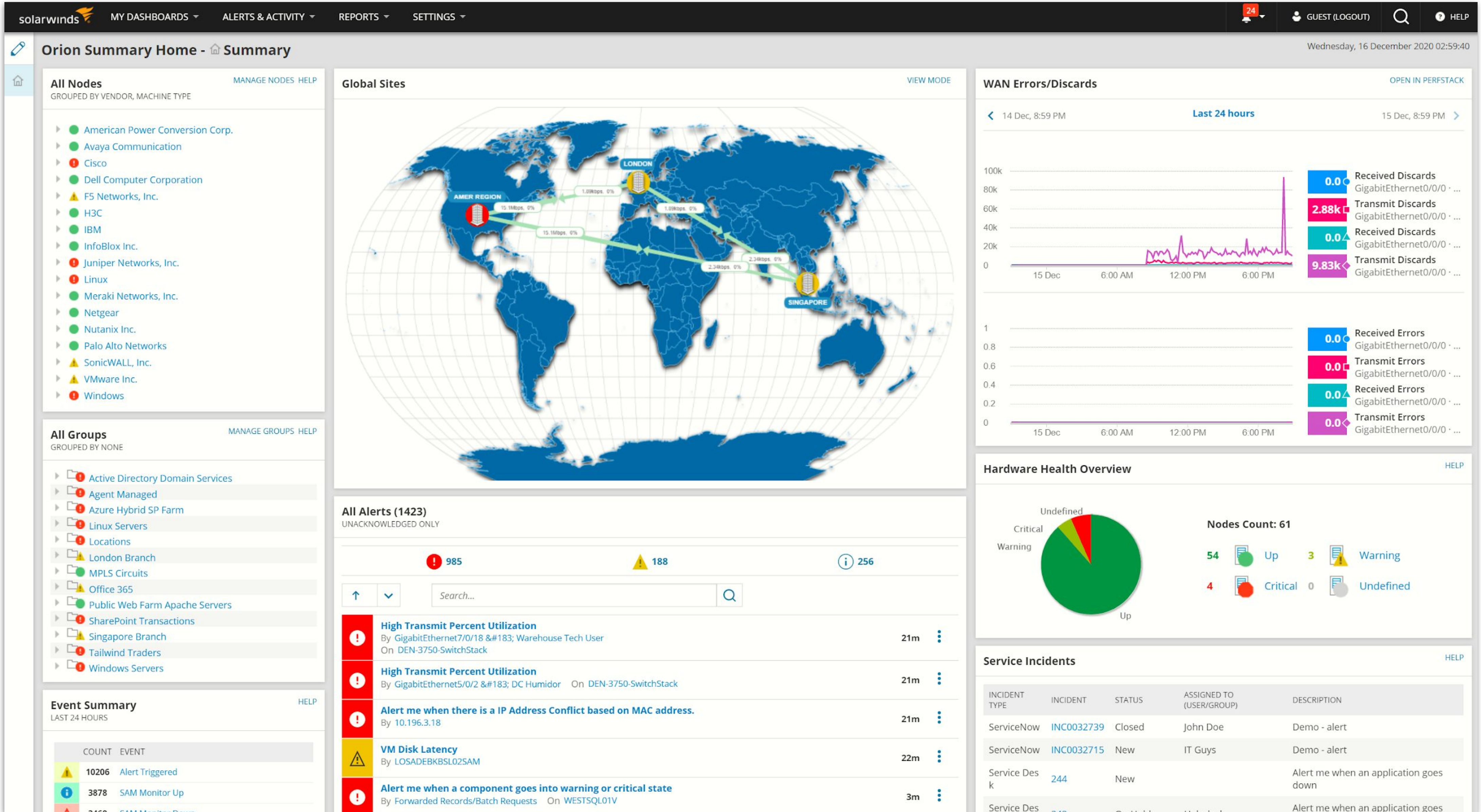
Landscape

1. What is an NMS? (Hint: not an NSM)
2. Who is SolarWinds? What is Orion?
3. Who uses it?
4. What is a supply chain attack?
5. How might a supply chain attack against an NMS affect me?
6. How can Suricata IDS rules protect me?
7. How does Corelight/Zeek data protect me?

What is an NMS?

- **Network Management Systems** automate the monitoring of individual resources and respond to outages immediately.
- Originally, NMS relied on basic SNMP polls and traps.
- Today, NMS involves credentialed access to virtual and cloud environments, network hardware, and critical servers.

Who is SolarWinds? What is Orion?



Orion Summary Home - Summary

Wednesday, 16 December 2020 02:59:40

All Nodes
GROUPED BY VENDOR, MACHINE TYPE
MANAGE NODES HELP

- American Power Conversion Corp.
- Avaya Communication
- Cisco
- Dell Computer Corporation
- F5 Networks, Inc.
- H3C
- IBM
- InfoBlox Inc.
- Juniper Networks, Inc.
- Linux
- Meraki Networks, Inc.
- Netgear
- Nutanix Inc.
- Palo Alto Networks
- SonicWALL, Inc.
- VMware Inc.
- Windows

All Groups
GROUPED BY NONE
MANAGE GROUPS HELP

- Active Directory Domain Services
- Agent Managed
- Azure Hybrid SP Farm
- Linux Servers
- Locations
- London Branch
- MPLS Circuits
- Office 365
- Public Web Farm Apache Servers
- SharePoint Transactions
- Singapore Branch
- Tailwind Traders
- Windows Servers

Event Summary
LAST 24 HOURS
HELP

	COUNT	EVENT
⚠	10206	Alert Triggered
ⓘ	3878	SAM Monitor Up
▲	3468	SAM Monitor Down

Global Sites
VIEW MODE

All Alerts (1423)
UNACKNOWLEDGED ONLY

985 188 256

Search...

High Transmit Percent Utilization
By GigabitEthernet7/0/18 &#183; Warehouse Tech User
On DEN-3750-SwitchStack
21m

High Transmit Percent Utilization
By GigabitEthernet5/0/2 &#183; DC Humidor On DEN-3750-SwitchStack
21m

Alert me when there is a IP Address Conflict based on MAC address.
By 10.196.3.18
21m

VM Disk Latency
By LOSADEBKBSL02SAM
22m

Alert me when a component goes into warning or critical state
By Forwarded Records/Batch Requests On WESTSQL01V
3m

WAN Errors/Discards
OPEN IN PERFSTACK

14 Dec, 8:59 PM   Last 24 hours   15 Dec, 8:59 PM

0.0 Received Discards GigabitEthernet0/0/0 · ...
2.88k Transmit Discards GigabitEthernet0/0/0 · ...
0.0 Received Discards GigabitEthernet0/0/0 · ...
9.83k Transmit Discards GigabitEthernet0/0/0 · ...

0.0 Received Errors GigabitEthernet0/0/0 · ...
0.0 Transmit Errors GigabitEthernet0/0/0 · ...
0.0 Received Errors GigabitEthernet0/0/0 · ...
0.0 Transmit Errors GigabitEthernet0/0/0 · ...

Hardware Health Overview
HELP

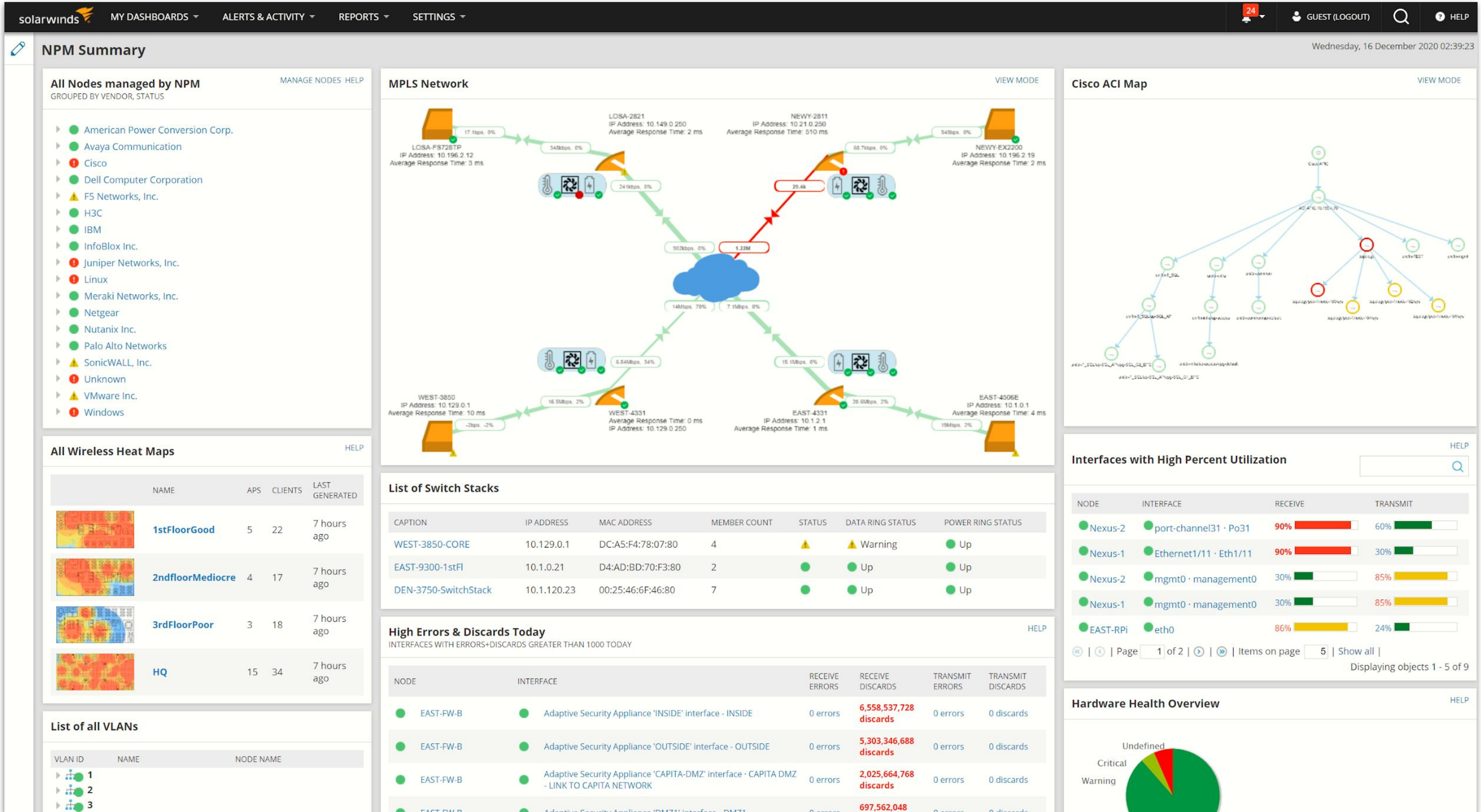
Nodes Count: 61

54 Up 3 Warning
4 Critical 0 Undefined

Service Incidents
HELP

INCIDENT TYPE	INCIDENT	STATUS	ASSIGNED TO (USER/GROUP)	DESCRIPTION
ServiceNow	INC0032739	Closed	John Doe	Demo - alert
ServiceNow	INC0032715	New	IT Guys	Demo - alert
Service Desk	244	New		Alert me when an application goes down
Service Des	[illegible]	[illegible]	[illegible]	Alert me when an application goes

Who is SolarWinds? What is Orion?



NPM Summary

Wednesday, 16 December 2020 02:39:23

All Nodes managed by NPM

GROUPED BY VENDOR, STATUS

MANAGE NODES HELP

- ● American Power Conversion Corp.
- ● Avaya Communication
- ● Cisco
- ● Dell Computer Corporation
- ⚠ F5 Networks, Inc.
- ● H3C
- ● IBM
- ● InfoBlox Inc.
- ● Juniper Networks, Inc.
- ● Linux
- ● Meraki Networks, Inc.
- ● Netgear
- ● Nutanix Inc.
- ● Palo Alto Networks
- ⚠ SonicWALL, Inc.
- ● Unknown
- ⚠ VMware Inc.
- ● Windows

MPLS Network

VIEW MODE

Cisco ACI Map

VIEW MODE

All Wireless Heat Maps

HELP

	NAME	APS	CLIENTS	LAST GENERATED
	1stFloorGood	5	22	7 hours ago
	2ndfloorMediocre	4	17	7 hours ago
	3rdFloorPoor	3	18	7 hours ago
	HQ	15	34	7 hours ago

List of all VLANs

VLAN ID	NAME	NODE NAME
1		
2		
3		

List of Switch Stacks

CAPTION	IP ADDRESS	MAC ADDRESS	MEMBER COUNT	STATUS	DATA RING STATUS	POWER RING STATUS
WEST-3850-CORE	10.129.0.1	DC:A5:F4:78:07:80	4	⚠	⚠ Warning	● Up
EAST-9300-1stFl	10.1.0.21	D4:AD:BD:70:F3:80	2	●	● Up	● Up
DEN-3750-SwitchStack	10.1.120.23	00:25:46:6F:46:80	7	●	● Up	● Up

High Errors & Discards Today

INTERFACES WITH ERRORS+DISCARDS GREATER THAN 1000 TODAY

HELP

	NODE		INTERFACE	RECEIVE ERRORS	RECEIVE DISCARDS	TRANSMIT ERRORS	TRANSMIT DISCARDS
●	EAST-FW-B	●	Adaptive Security Appliance 'INSIDE' interface - INSIDE	0 errors	6,558,537,728 discards	0 errors	0 discards
●	EAST-FW-B	●	Adaptive Security Appliance 'OUTSIDE' interface - OUTSIDE	0 errors	5,303,346,688 discards	0 errors	0 discards
●	EAST-FW-B	●	Adaptive Security Appliance 'CAPITA-DMZ' interface · CAPITA DMZ - LINK TO CAPITA NETWORK	0 errors	2,025,664,768 discards	0 errors	0 discards
●	EAST-FW-B	●	Adaptive Security Appliance 'DMZ1' interface - DMZ1	0 errors	697,562,048	0 errors	0 discards

Interfaces with High Percent Utilization

HELP

NODE	INTERFACE	RECEIVE	TRANSMIT
● Nexus-2	● port-channel31 · Po31	90%	60%
● Nexus-1	● Ethernet1/11 · Eth1/11	90%	30%
● Nexus-2	● mgmt0 · management0	30%	85%
● Nexus-1	● mgmt0 · management0	30%	85%
● EAST-RPi	● eth0	86%	24%

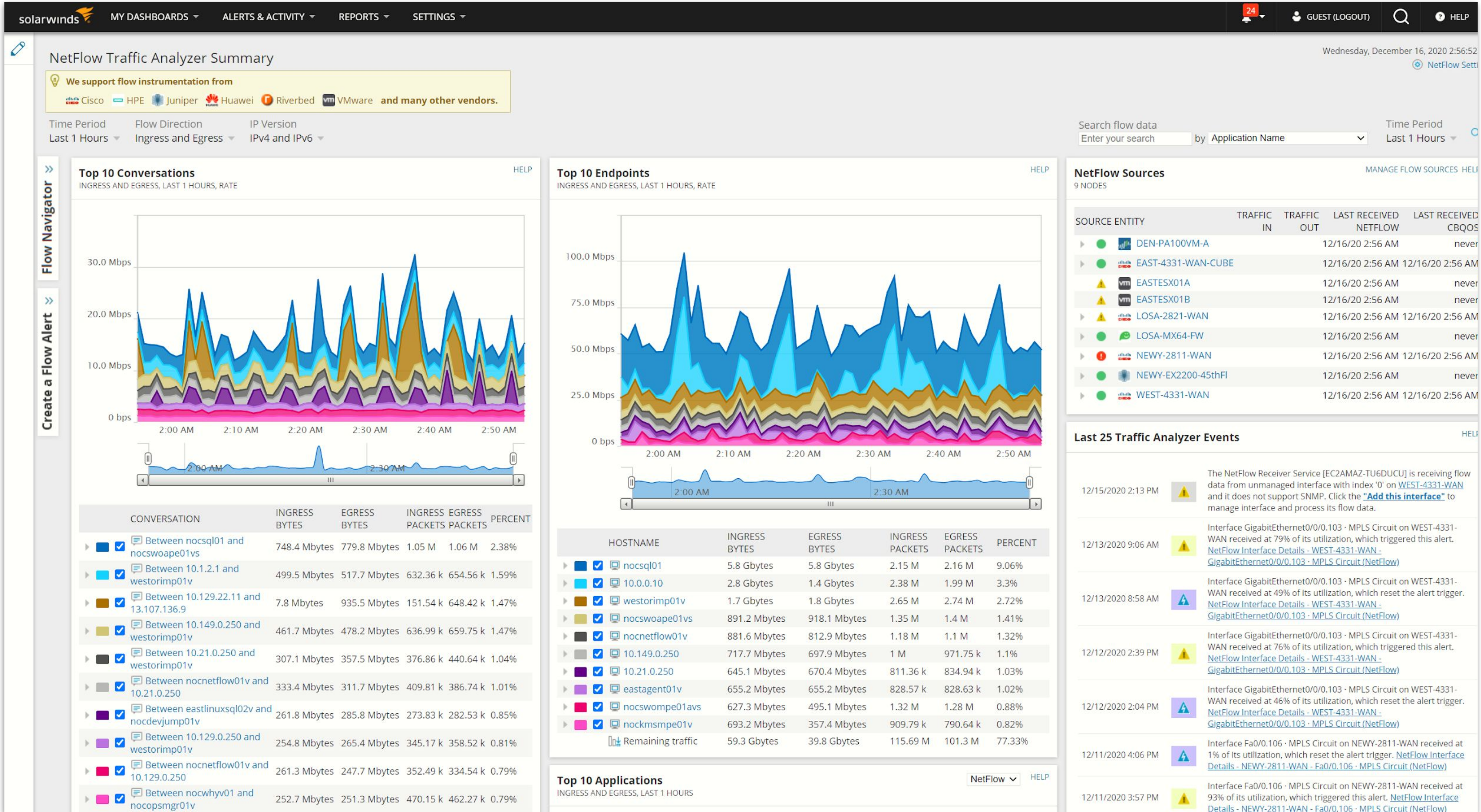
| Page 1 of 2 | | Items on page 5 | Show all |

Displaying objects 1 - 5 of 9

Hardware Health Overview

HELP

Who is SolarWinds? What is Orion?



NetFlow Traffic Analyzer Summary

Wednesday, December 16, 2020 2:56:52

NetFlow Sett

We support flow instrumentation from

Cisco HPE Juniper Huawei Riverbed VMware **and many other vendors.**

Time Period: Last 1 Hours

Flow Direction: Ingress and Egress

IP Version: IPv4 and IPv6

Search flow data: Enter your search by Application Name

Time Period: Last 1 Hours

Top 10 Conversations

INGRESS AND EGRESS, LAST 1 HOURS, RATE

	CONVERSATION	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
☑	Between nocsql01 and nocswoape01vs	748.4 Mbytes	779.8 Mbytes	1.05 M	1.06 M	2.38%
☑	Between 10.1.2.1 and westorimp01v	499.5 Mbytes	517.7 Mbytes	632.36 k	654.56 k	1.59%
☑	Between 10.129.22.11 and 13.107.136.9	7.8 Mbytes	935.5 Mbytes	151.54 k	648.42 k	1.47%
☑	Between 10.149.0.250 and westorimp01v	461.7 Mbytes	478.2 Mbytes	636.99 k	659.75 k	1.47%
☑	Between 10.21.0.250 and westorimp01v	307.1 Mbytes	357.5 Mbytes	376.86 k	440.64 k	1.04%
☑	Between nocnetflow01v and 10.21.0.250	333.4 Mbytes	311.7 Mbytes	409.81 k	386.74 k	1.01%
☑	Between eastlinuxsql02v and nocdevjump01v	261.8 Mbytes	285.8 Mbytes	273.83 k	282.53 k	0.85%
☑	Between 10.129.0.250 and westorimp01v	254.8 Mbytes	265.4 Mbytes	345.17 k	358.52 k	0.81%
☑	Between nocnetflow01v and 10.129.0.250	261.3 Mbytes	247.7 Mbytes	352.49 k	334.54 k	0.79%
☑	Between nocwhyv01 and nocopsmgr01v	252.7 Mbytes	251.3 Mbytes	470.15 k	462.27 k	0.79%

Top 10 Endpoints

INGRESS AND EGRESS, LAST 1 HOURS, RATE

	HOSTNAME	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
☑	nocsql01	5.8 Gbytes	5.8 Gbytes	2.15 M	2.16 M	9.06%
☑	10.0.0.10	2.8 Gbytes	1.4 Gbytes	2.38 M	1.99 M	3.3%
☑	westorimp01v	1.7 Gbytes	1.8 Gbytes	2.65 M	2.74 M	2.72%
☑	nocswoape01vs	891.2 Mbytes	918.1 Mbytes	1.35 M	1.4 M	1.41%
☑	nocnetflow01v	881.6 Mbytes	812.9 Mbytes	1.18 M	1.1 M	1.32%
☑	10.149.0.250	717.7 Mbytes	697.9 Mbytes	1 M	971.75 k	1.1%
☑	10.21.0.250	645.1 Mbytes	670.4 Mbytes	811.36 k	834.94 k	1.03%
☑	eastagent01v	655.2 Mbytes	655.2 Mbytes	828.57 k	828.63 k	1.02%
☑	nocswompe01avs	627.3 Mbytes	495.1 Mbytes	1.32 M	1.28 M	0.88%
☑	nockmsmpe01v	693.2 Mbytes	357.4 Mbytes	909.79 k	790.64 k	0.82%
	Remaining traffic	59.3 Gbytes	39.8 Gbytes	115.69 M	101.3 M	77.33%

Top 10 Applications

INGRESS AND EGRESS, LAST 1 HOURS

NetFlow Sources

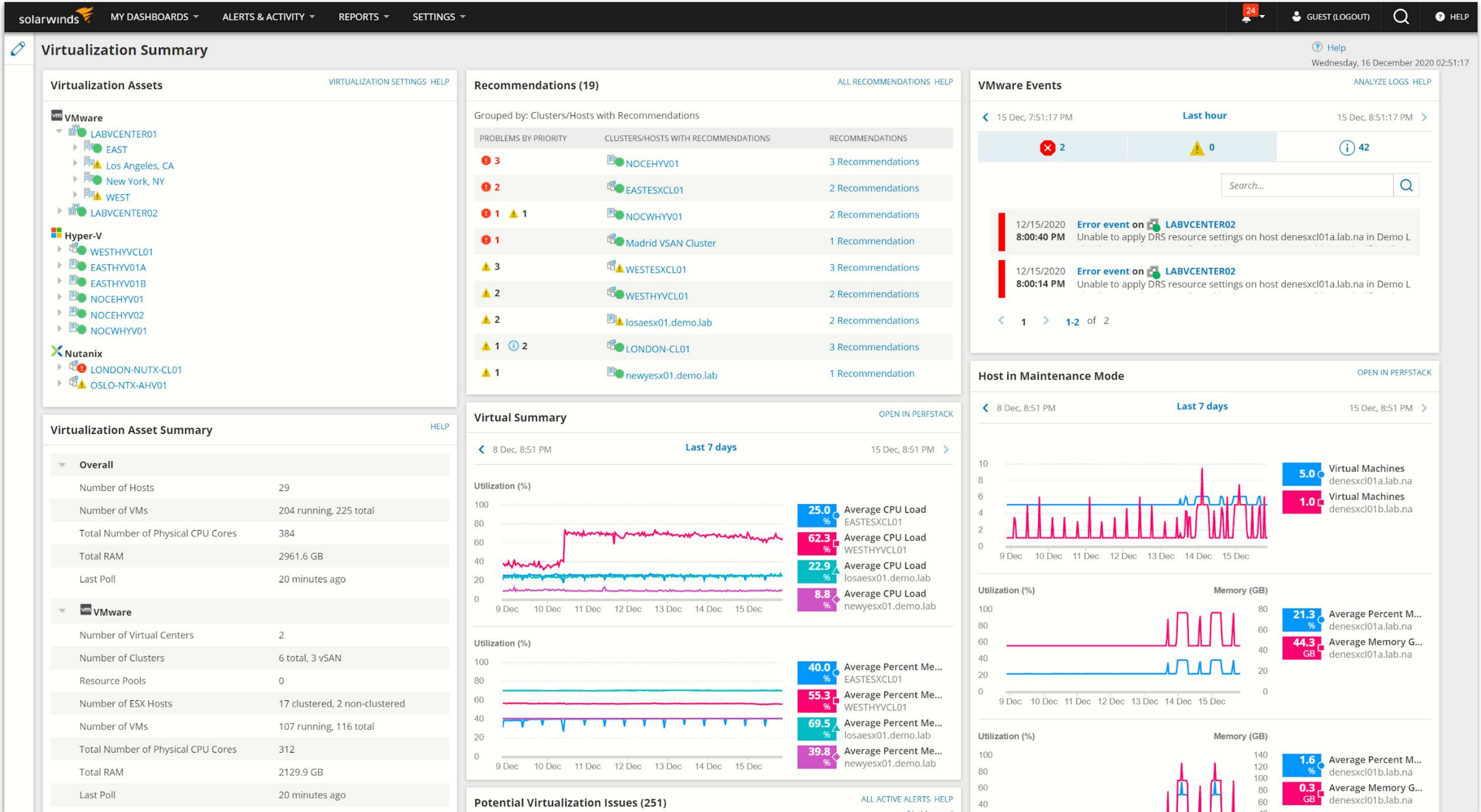
9 NODES

	SOURCE ENTITY	TRAFFIC IN	TRAFFIC OUT	LAST RECEIVED NETFLOW	LAST RECEIVED CBQOS
●	DEN-PA100VM-A			12/16/20 2:56 AM	never
●	EAST-4331-WAN-CUBE			12/16/20 2:56 AM	12/16/20 2:56 AM
⚠	EASTESX01A			12/16/20 2:56 AM	never
⚠	EASTESX01B			12/16/20 2:56 AM	never
⚠	LOSA-2821-WAN			12/16/20 2:56 AM	12/16/20 2:56 AM
●	LOSA-MX64-FW			12/16/20 2:56 AM	never
!	NEWY-2811-WAN			12/16/20 2:56 AM	12/16/20 2:56 AM
●	NEWY-EX2200-45thFl			12/16/20 2:56 AM	never
●	WEST-4331-WAN			12/16/20 2:56 AM	12/16/20 2:56 AM

Last 25 Traffic Analyzer Events

12/15/2020 2:13 PM	⚠	The NetFlow Receiver Service [EC2AMAZ-TU6DUCU] is receiving flow data from unmanaged interface with index '0' on WEST-4331-WAN and it does not support SNMP. Click the **"Add this interface"** to manage interface and process its flow data.
12/13/2020 9:06 AM	⚠	Interface GigabitEthernet0/0/0.103 · MPLS Circuit on WEST-4331-WAN received at 79% of its utilization, which triggered this alert. NetFlow Interface Details - WEST-4331-WAN - GigabitEthernet0/0/0.103 · MPLS Circuit (NetFlow)
12/13/2020 8:58 AM	⚠	Interface GigabitEthernet0/0/0.103 · MPLS Circuit on WEST-4331-WAN received at 49% of its utilization, which reset the alert trigger. NetFlow Interface Details - WEST-4331-WAN - GigabitEthernet0/0/0.103 · MPLS Circuit (NetFlow)
12/12/2020 2:39 PM	⚠	Interface GigabitEthernet0/0/0.103 · MPLS Circuit on WEST-4331-WAN received at 76% of its utilization, which triggered this alert. NetFlow Interface Details - WEST-4331-WAN - GigabitEthernet0/0/0.103 · MPLS Circuit (NetFlow)
12/12/2020 2:04 PM	⚠	Interface GigabitEthernet0/0/0.103 · MPLS Circuit on WEST-4331-WAN received at 46% of its utilization, which reset the alert trigger. NetFlow Interface Details - WEST-4331-WAN - GigabitEthernet0/0/0.103 · MPLS Circuit (NetFlow)
12/11/2020 4:06 PM	⚠	Interface Fa0/0.106 · MPLS Circuit on NEWY-2811-WAN received at 1% of its utilization, which reset the alert trigger. NetFlow Interface Details - NEWY-2811-WAN - Fa0/0.106 · MPLS Circuit (NetFlow)
12/11/2020 3:57 PM	⚠	Interface Fa0/0.106 · MPLS Circuit on NEWY-2811-WAN received at 93% of its utilization, which triggered this alert. NetFlow Interface Details - NEWY-2811-WAN - Fa0/0.106 · MPLS Circuit (NetFlow)

Who is SolarWinds? What is Orion?



Virtualization Summary

Help
Wednesday, 16 December 2020 02:51:17

Virtualization Assets

VIRTUALIZATION SETTINGS HELP

- VMware
  - LABVCENTER01
    - EAST
    - Los Angeles, CA
    - New York, NY
    - WEST
  - LABVCENTER02
- Hyper-V
  - WESTHYVCL01
  - EASTHYV01A
  - EASTHYV01B
  - NOCEHYV01
  - NOCEHYV02
  - NOCWHYV01
- Nutanix
  - LONDON-NUTX-CL01
  - OSLO-NTX-AHV01

Virtualization Asset Summary

HELP

Overall	
Number of Hosts	29
Number of VMs	204 running, 225 total
Total Number of Physical CPU Cores	384
Total RAM	2961.6 GB
Last Poll	20 minutes ago
VMware	
Number of Virtual Centers	2
Number of Clusters	6 total, 3 vSAN
Resource Pools	0
Number of ESX Hosts	17 clustered, 2 non-clustered
Number of VMs	107 running, 116 total
Total Number of Physical CPU Cores	312
Total RAM	2129.9 GB
Last Poll	20 minutes ago

Recommendations (19)

ALL RECOMMENDATIONS HELP

Grouped by: Clusters/Hosts with Recommendations

PROBLEMS BY PRIORITY	CLUSTERS/HOSTS WITH RECOMMENDATIONS	RECOMMENDATIONS
❗ 3	NOCEHYV01	3 Recommendations
❗ 2	EASTESXCL01	2 Recommendations
❗ 1 ⚠ 1	NOCWHYV01	2 Recommendations
❗ 1	Madrid VSAN Cluster	1 Recommendation
⚠ 3	WESTESXCL01	3 Recommendations
⚠ 2	WESTHYVCL01	2 Recommendations
⚠ 2	losaesx01.demo.lab	2 Recommendations
⚠ 1 ⓘ 2	LONDON-CL01	3 Recommendations
⚠ 1	newyesx01.demo.lab	1 Recommendation

Virtual Summary

OPEN IN PERFSTACK

8 Dec, 8:51 PM — Last 7 days — 15 Dec, 8:51 PM

Utilization (%)

25.0 %	Average CPU Load EASTESXCL01
62.3 %	Average CPU Load WESTHYVCL01
22.9 %	Average CPU Load losaesx01.demo.lab
8.8 %	Average CPU Load newyesx01.demo.lab

Utilization (%)

40.0 %	Average Percent Me... EASTESXCL01
55.3 %	Average Percent Me... WESTHYVCL01
69.5 %	Average Percent Me... losaesx01.demo.lab
39.8 %	Average Percent Me... newyesx01.demo.lab

Potential Virtualization Issues (251)

ALL ACTIVE ALERTS HELP

VMware Events

ANALYZE LOGS HELP

15 Dec, 7:51:17 PM — Last hour — 15 Dec, 8:51:17 PM

☒ 2 ⚠ 0 ⓘ 42

Search...

12/15/2020 **8:00:40 PM** **Error event on** LABVCENTER02
Unable to apply DRS resource settings on host denesxcl01a.lab.na in Demo L

12/15/2020 **8:00:14 PM** **Error event on** LABVCENTER02
Unable to apply DRS resource settings on host denesxcl01a.lab.na in Demo L

1 1-2 of 2

Host in Maintenance Mode

OPEN IN PERFSTACK

8 Dec, 8:51 PM — Last 7 days — 15 Dec, 8:51 PM

5.0	Virtual Machines denesxcl01a.lab.na
1.0	Virtual Machines denesxcl01b.lab.na

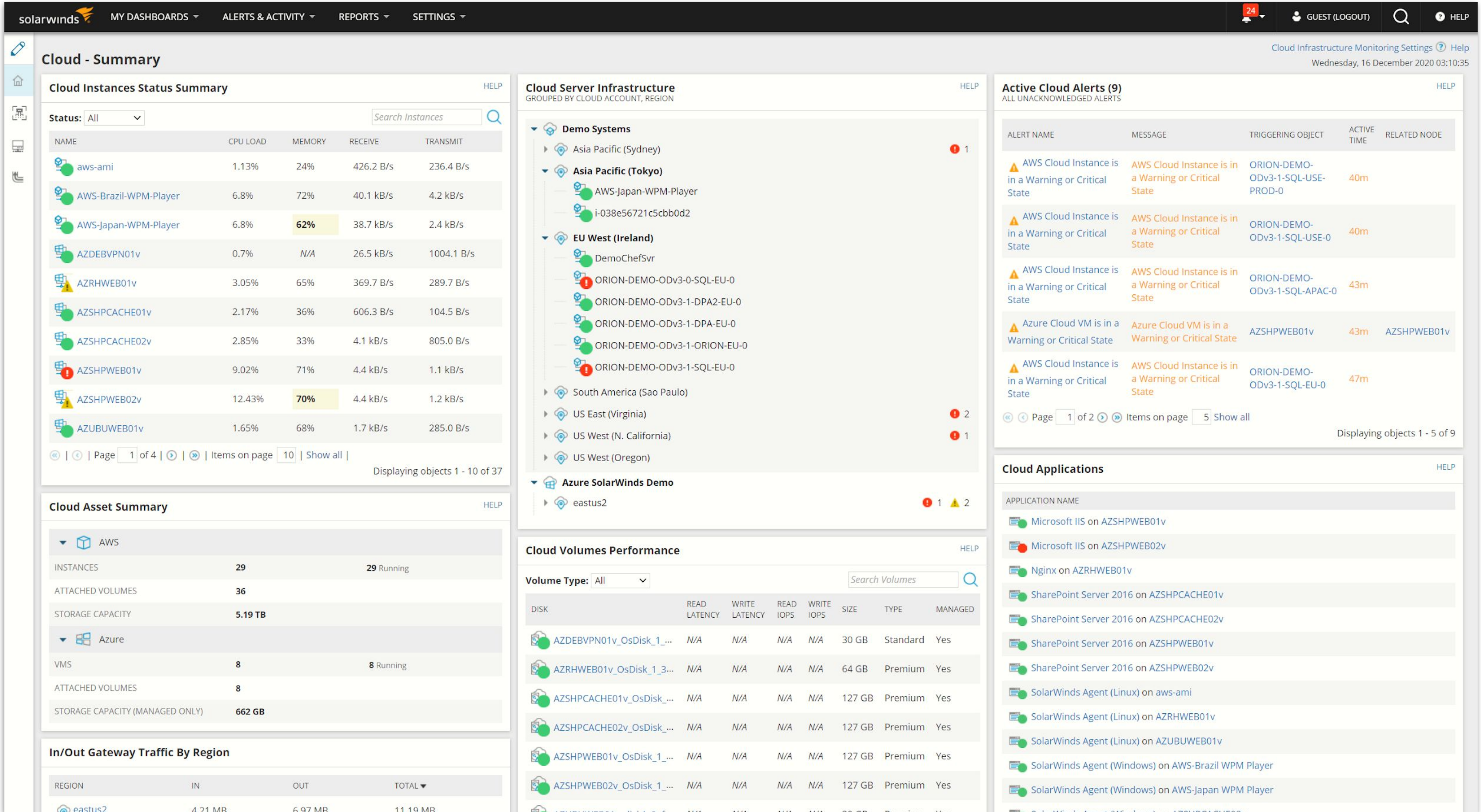
Utilization (%) Memory (GB)

21.3 %	Average Percent M... denesxcl01a.lab.na
44.3 GB	Average Memory G... denesxcl01a.lab.na

Utilization (%) Memory (GB)

1.6 %	Average Percent M... denesxcl01b.lab.na
0.3 GB	Average Memory G... denesxcl01b.lab.na

Who is SolarWinds? What is Orion?



Cloud Infrastructure Monitoring Settings Help

Wednesday, 16 December 2020 03:10:35

Cloud - Summary

Cloud Instances Status Summary

HELP

Status: All

Search Instances

NAME	CPU LOAD	MEMORY	RECEIVE	TRANSMIT
aws-ami	1.13%	24%	426.2 B/s	236.4 B/s
AWS-Brazil-WPM-Player	6.8%	72%	40.1 kB/s	4.2 kB/s
AWS-Japan-WPM-Player	6.8%	62%	38.7 kB/s	2.4 kB/s
AZDEBVPN01v	0.7%	N/A	26.5 kB/s	1004.1 B/s
AZRHWEB01v	3.05%	65%	369.7 B/s	289.7 B/s
AZSHPCACHE01v	2.17%	36%	606.3 B/s	104.5 B/s
AZSHPCACHE02v	2.85%	33%	4.1 kB/s	805.0 B/s
AZSHPWEB01v	9.02%	71%	4.4 kB/s	1.1 kB/s
AZSHPWEB02v	12.43%	70%	4.4 kB/s	1.2 kB/s
AZUBUWEB01v	1.65%	68%	1.7 kB/s	285.0 B/s

| Page 1 of 4 | | Items on page 10 | Show all |

Displaying objects 1 - 10 of 37

Cloud Asset Summary

HELP

AWS		
INSTANCES	29	29 Running
ATTACHED VOLUMES	36	
STORAGE CAPACITY	5.19 TB	
Azure		
VMS	8	8 Running
ATTACHED VOLUMES	8	
STORAGE CAPACITY (MANAGED ONLY)	662 GB	

In/Out Gateway Traffic By Region

REGION	IN	OUT	TOTAL ▾
eastus2	4.21 MB	6.97 MB	11.19 MB

Cloud Server Infrastructure

GROUPED BY CLOUD ACCOUNT, REGION

HELP

- Demo Systems
  - Asia Pacific (Sydney) ● 1
  - Asia Pacific (Tokyo)
    - AWS-Japan-WPM-Player
    - i-038e56721c5cbb0d2
  - EU West (Ireland)
    - DemoChefSvr
    - ORION-DEMO-ODv3-0-SQL-EU-0
    - ORION-DEMO-ODv3-1-DPA2-EU-0
    - ORION-DEMO-ODv3-1-DPA-EU-0
    - ORION-DEMO-ODv3-1-ORION-EU-0
    - ORION-DEMO-ODv3-1-SQL-EU-0
  - South America (Sao Paulo)
  - US East (Virginia) ● 2
  - US West (N. California) ● 1
  - US West (Oregon)
- Azure SolarWinds Demo
  - eastus2 ● 1 ▲ 2

Cloud Volumes Performance

HELP

Volume Type: All

Search Volumes

DISK	READ LATENCY	WRITE LATENCY	READ IOPS	WRITE IOPS	SIZE	TYPE	MANAGED
AZDEBVPN01v_OsDisk_1_...	N/A	N/A	N/A	N/A	30 GB	Standard	Yes
AZRHWEB01v_OsDisk_1_3...	N/A	N/A	N/A	N/A	64 GB	Premium	Yes
AZSHPCACHE01v_OsDisk_...	N/A	N/A	N/A	N/A	127 GB	Premium	Yes
AZSHPCACHE02v_OsDisk_...	N/A	N/A	N/A	N/A	127 GB	Premium	Yes
AZSHPWEB01v_OsDisk_1_...	N/A	N/A	N/A	N/A	127 GB	Premium	Yes
AZSHPWEB02v_OsDisk_1_...	N/A	N/A	N/A	N/A	127 GB	Premium	Yes

Active Cloud Alerts (9)

ALL UNACKNOWLEDGED ALERTS

HELP

ALERT NAME	MESSAGE	TRIGGERING OBJECT	ACTIVE TIME	RELATED NODE
AWS Cloud Instance is in a Warning or Critical State	AWS Cloud Instance is in a Warning or Critical State	ORION-DEMO-ODv3-1-SQL-USE-PROD-0	40m	
AWS Cloud Instance is in a Warning or Critical State	AWS Cloud Instance is in a Warning or Critical State	ORION-DEMO-ODv3-1-SQL-USE-0	40m	
AWS Cloud Instance is in a Warning or Critical State	AWS Cloud Instance is in a Warning or Critical State	ORION-DEMO-ODv3-1-SQL-APAC-0	43m	
Azure Cloud VM is in a Warning or Critical State	Azure Cloud VM is in a Warning or Critical State	AZSHPWEB01v	43m	AZSHPWEB01v
AWS Cloud Instance is in a Warning or Critical State	AWS Cloud Instance is in a Warning or Critical State	ORION-DEMO-ODv3-1-SQL-EU-0	47m	

Page 1 of 2 Items on page 5 Show all

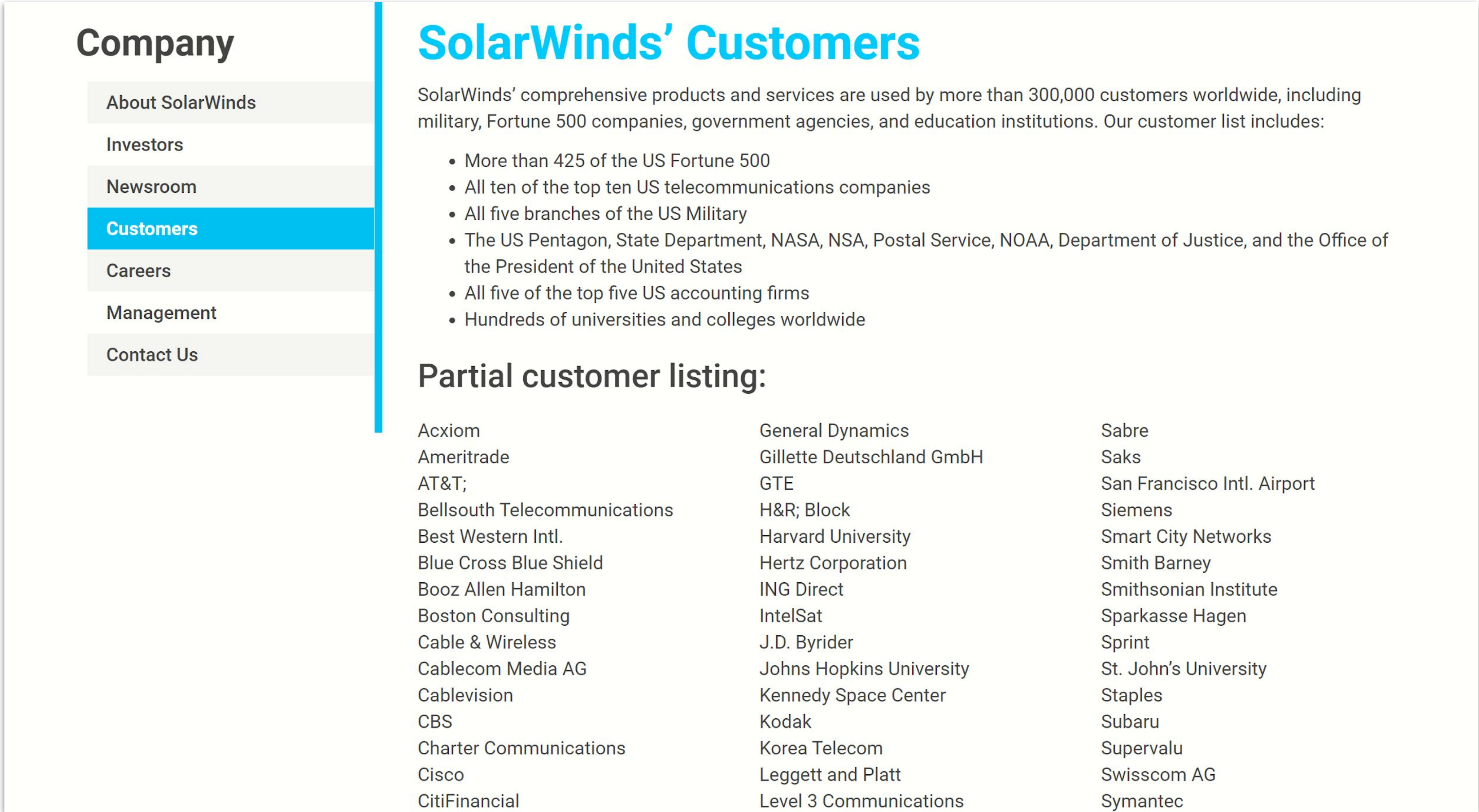
Displaying objects 1 - 5 of 9

Cloud Applications

HELP

APPLICATION NAME
Microsoft IIS on AZSHPWEB01v
Microsoft IIS on AZSHPWEB02v
Nginx on AZRHWEB01v
SharePoint Server 2016 on AZSHPCACHE01v
SharePoint Server 2016 on AZSHPCACHE02v
SharePoint Server 2016 on AZSHPWEB01v
SharePoint Server 2016 on AZSHPWEB02v
SolarWinds Agent (Linux) on aws-ami
SolarWinds Agent (Linux) on AZRHWEB01v
SolarWinds Agent (Linux) on AZUBUWEB01v
SolarWinds Agent (Windows) on AWS-Brazil WPM Player
SolarWinds Agent (Windows) on AWS-Japan WPM Player

Who uses SolarWinds Orion?



SolarWinds' Customers

SolarWinds' comprehensive products and services are used by more than 300,000 customers worldwide, including military, Fortune 500 companies, government agencies, and education institutions. Our customer list includes:

- More than 425 of the US Fortune 500
- All ten of the top ten US telecommunications companies
- All five branches of the US Military
- The US Pentagon, State Department, NASA, NSA, Postal Service, NOAA, Department of Justice, and the Office of the President of the United States
- All five of the top five US accounting firms
- Hundreds of universities and colleges worldwide

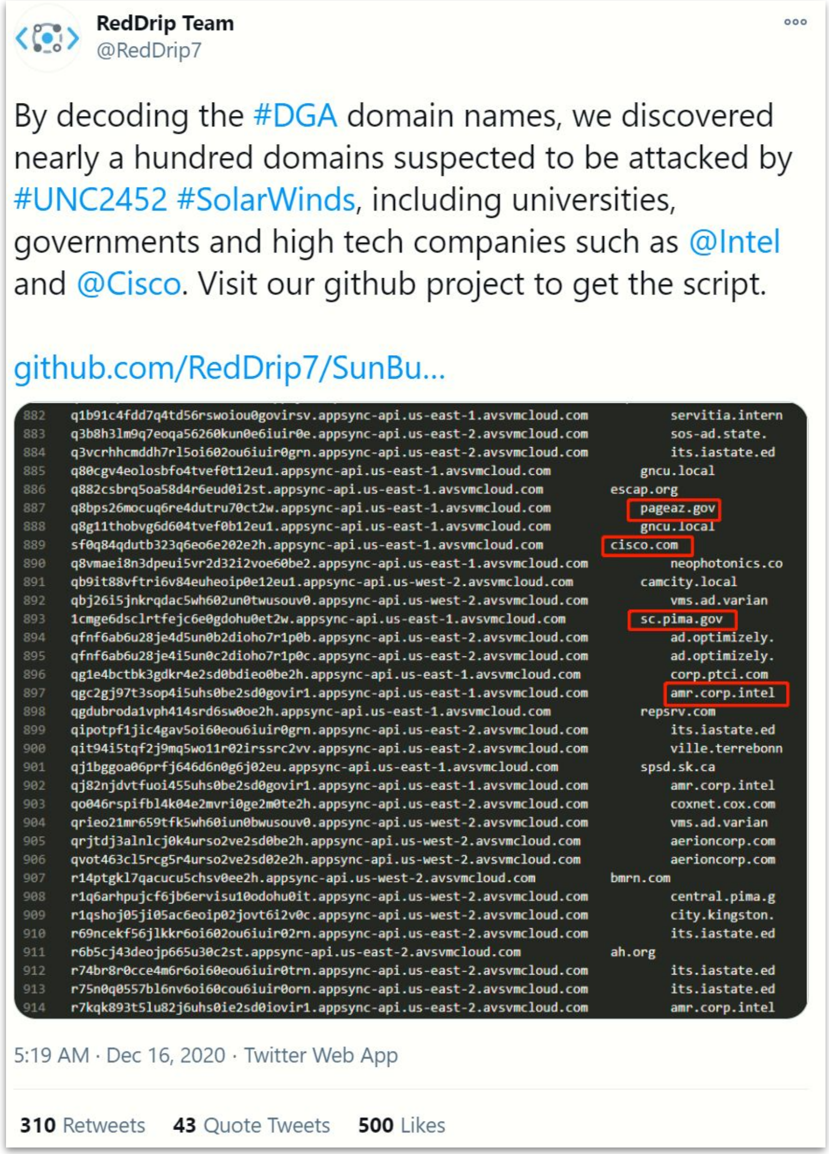
Partial customer listing:

Acxiom
Ameritrade
AT&T;
Bellsouth Telecommunications
Best Western Intl.
Blue Cross Blue Shield
Booz Allen Hamilton
Boston Consulting
Cable & Wireless
Cablecom Media AG
Cablevision
CBS
Charter Communications
Cisco
CitiFinancial

General Dynamics
Gillette Deutschland GmbH
GTE
H&R; Block
Harvard University
Hertz Corporation
ING Direct
IntelSat
J.D. Byrider
Johns Hopkins University
Kennedy Space Center
Kodak
Korea Telecom
Leggett and Platt
Level 3 Communications

Sabre
Saks
San Francisco Intl. Airport
Siemens
Smart City Networks
Smith Barney
Smithsonian Institute
Sparkasse Hagen
Sprint
St. John's University
Staples
Subaru
Supervalu
Swisscom AG
Symantec

Who uses SolarWinds Orion?



RedDrip Team
@RedDrip7

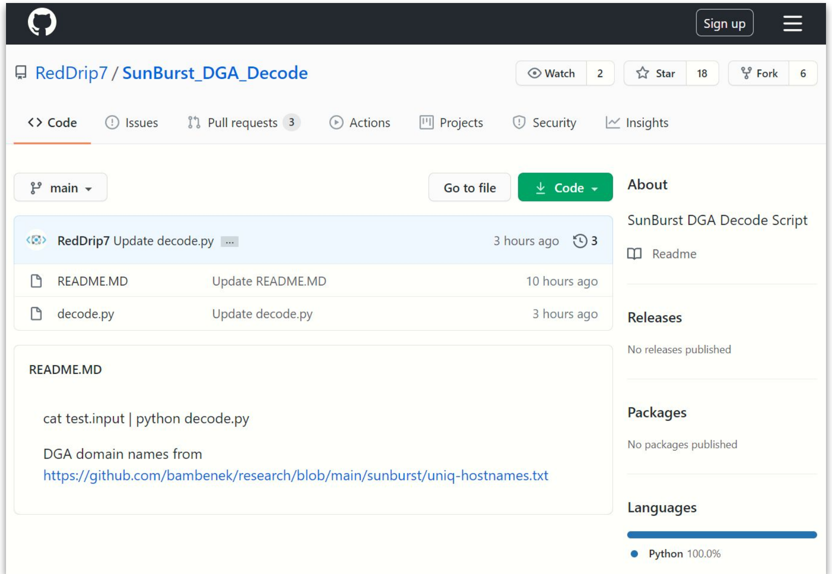
By decoding the #DGA domain names, we discovered nearly a hundred domains suspected to be attacked by #UNC2452 #SolarWinds, including universities, governments and high tech companies such as @Intel and @Cisco. Visit our github project to get the script.

github.com/RedDrip7/SunBu...

```
q1b91c4fdd7q4td56rswoiou0govirsv.appsync-api.us-east-1.avsvmcloud.com         servitia.intern
q3b8h3lm9q7eoqa56260kun0e6iuir0e.appsync-api.us-east-2.avsvmcloud.com         sos-ad.state.
q3vcrhhcmddh7rl5oi602ou6iuir0grn.appsync-api.us-east-2.avsvmcloud.com         its.iastate.ed
q80cgv4eolosbfo4tvef0t12eu1.appsync-api.us-east-1.avsvmcloud.com          gncu.local
q882csbrq5oa58d4r6eud0i2st.appsync-api.us-east-1.avsvmcloud.com         escap.org
q8bps26mocuq6re4dutru70ct2w.appsync-api.us-east-1.avsvmcloud.com          pageaz.gov
q8g11thobvg6d604tvef0b12eu1.appsync-api.us-east-1.avsvmcloud.com          gncu.local
sf0q84qdutb323q6eo6e202e2h.appsync-api.us-east-1.avsvmcloud.com         cisco.com
q8vmaei8n3dpeui5vr2d32i2voe60be2.appsync-api.us-east-1.avsvmcloud.com         neophotonics.co
qb9it88vftri6v84euheoip0e12eu1.appsync-api.us-west-2.avsvmcloud.com         camcity.local
qbj26i5jnkrqdac5wh602un0twusouv0.appsync-api.us-west-2.avsvmcloud.com         vms.ad.varian
1cmge6dsclrtfejc6e0gdohu0et2w.appsync-api.us-east-1.avsvmcloud.com          sc.pima.gov
qfnf6ab6u28je4d5un0b2dioho7r1p0b.appsync-api.us-east-2.avsvmcloud.com         ad.optimizely.
qfnf6ab6u28je4i5un0c2dioho7r1p0c.appsync-api.us-east-2.avsvmcloud.com         ad.optimizely.
qg1e4bctbk3gdkr4e2sd0bdieo0be2h.appsync-api.us-east-1.avsvmcloud.com          corp.ptci.com
qgc2gj97t3sop4i5uhs0be2sd0govir1.appsync-api.us-east-1.avsvmcloud.com         amr.corp.intel
qgdubroda1vph414srd6sw0oe2h.appsync-api.us-east-1.avsvmcloud.com          repsrv.com
qipotpf1jic4gav5oi60eou6iuir0grn.appsync-api.us-east-2.avsvmcloud.com         its.iastate.ed
qit94i5tqf2j9mq5wo11r02irssrc2vv.appsync-api.us-east-2.avsvmcloud.com         ville.terrebonn
qj1bggoa06prfj646d6n0g6j02eu.appsync-api.us-east-1.avsvmcloud.com         spsd.sk.ca
qj82njdvtfuoi455uhs0be2sd0govir1.appsync-api.us-east-1.avsvmcloud.com         amr.corp.intel
qo046rspifbl4k04e2mvri0ge2m0te2h.appsync-api.us-east-2.avsvmcloud.com         coxnet.cox.com
qrieo21mr659tfk5wh60iun0bwusouv0.appsync-api.us-west-2.avsvmcloud.com         vms.ad.varian
qrjtdj3alnlcj0k4urso2ve2sd0be2h.appsync-api.us-west-2.avsvmcloud.com          aerioncorp.com
qvot463cl5rcg5r4urso2ve2sd02e2h.appsync-api.us-west-2.avsvmcloud.com          aerioncorp.com
r14ptgkl7qacucu5chsv0ee2h.appsync-api.us-west-2.avsvmcloud.com        bmrn.com
r1q6arhpujcf6jb6ervisu10odohu0it.appsync-api.us-west-2.avsvmcloud.com         central.pima.g
r1qshoj05ji05ac6eoip02jovt6i2v0c.appsync-api.us-west-2.avsvmcloud.com         city.kingston.
r69ncekf56jlkkr6oi602ou6iuir02rn.appsync-api.us-east-2.avsvmcloud.com         its.iastate.ed
r6b5cj43deojp665u30c2st.appsync-api.us-east-2.avsvmcloud.com          ah.org
r74br8r0cce4m6r6oi60eou6iuir0trn.appsync-api.us-east-2.avsvmcloud.com         its.iastate.ed
r75n0q0557bl6nv6oi60cou6iuir0orn.appsync-api.us-east-2.avsvmcloud.com         its.iastate.ed
r7kqk893t5lu82j6uhs0ie2sd0iovir1.appsync-api.us-east-2.avsvmcloud.com         amr.corp.intel
```

5:19 AM · Dec 16, 2020 · Twitter Web App

310 Retweets **43** Quote Tweets **500** Likes



RedDrip7 Update decode.py		3 hours ago 3
README.MD	Update README.MD	10 hours ago
decode.py	Update decode.py	3 hours ago

README.MD

cat test.input | python decode.py

DGA domain names from https://github.com/bambenek/research/blob/main/sunburst/uniq-hostnames.txt

About

SunBurst DGA Decode Script

Readme

Releases

No releases published

Packages

No packages published

Languages

Python 100.0%

What is a supply chain attack?

- Attacks on external dependencies (eg. libraries and packages)
- Attacks against build infrastructure
- Attacks against trusted/purchased hardware
- Attacks on a vendor's infrastructure

Previous examples:

- Typo-squatting colorama in PyPi repository
- Takeover of bb-builder NPM package to steal passwords
- SuperMicro hardware network backdoor (2015)
- Attacks against vendor infrasture (eg. Target)

How might an NMS supply chain attack affect me?

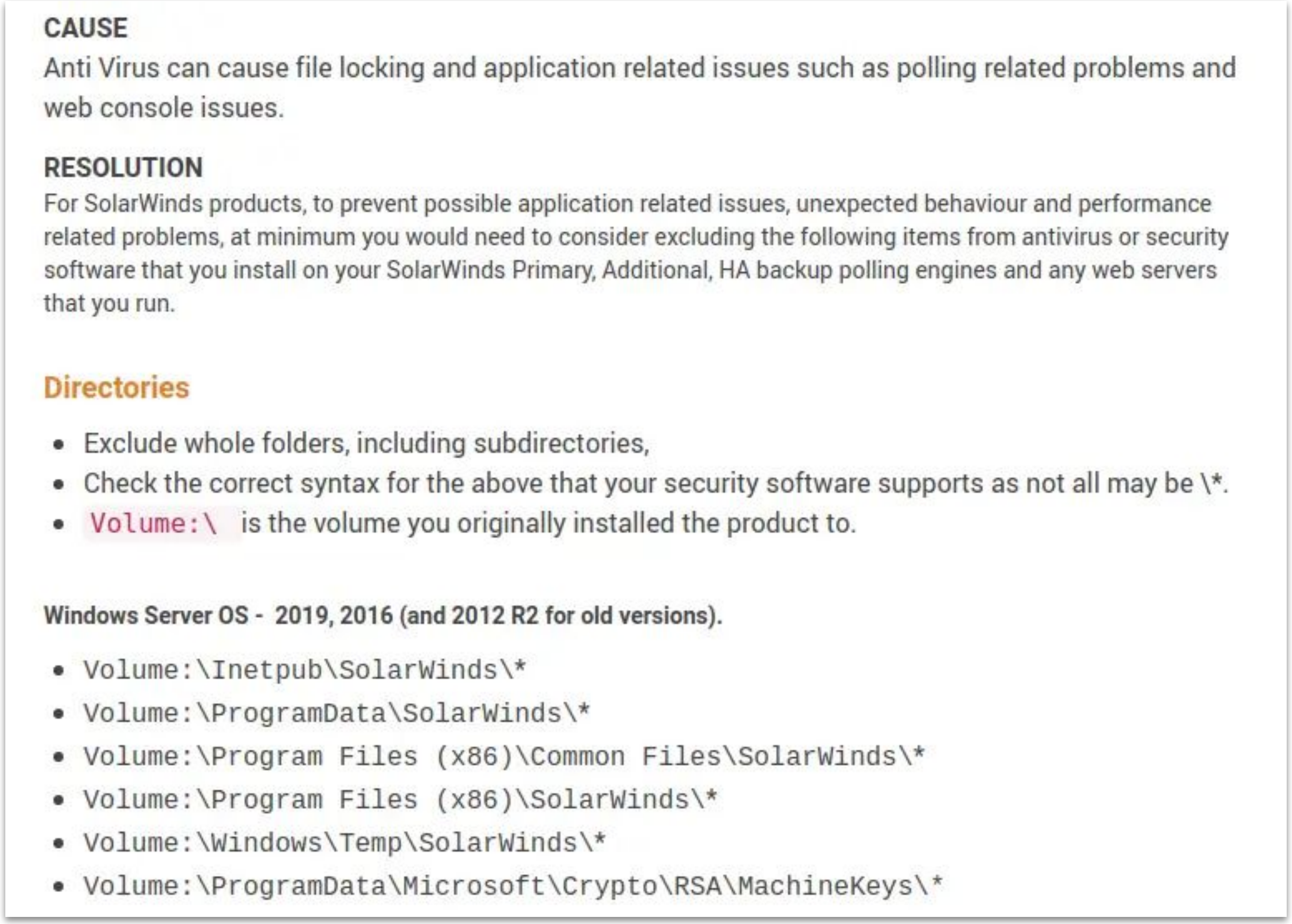
When you deploy an NMS, there are generally some base assumptions:

- NMS requires regular access a wide range of resources
- NMS requires credentials to perform in-depth monitoring
- NMS requires privileges to restart hosts/services

In short:

- An NMS is extremely difficult to lock down or monitor.
- Compromise of the NMS provides direct access to credentials and a launching point for direct and invasive attacks.

How might an NMS supply chain attack affect me?



CAUSE

Anti Virus can cause file locking and application related issues such as polling related problems and web console issues.

RESOLUTION

For SolarWinds products, to prevent possible application related issues, unexpected behaviour and performance related problems, at minimum you would need to consider excluding the following items from antivirus or security software that you install on your SolarWinds Primary, Additional, HA backup polling engines and any web servers that you run.

Directories

- Exclude whole folders, including subdirectories,
- Check the correct syntax for the above that your security software supports as not all may be *.
- `Volume:\` is the volume you originally installed the product to.

Windows Server OS - 2019, 2016 (and 2012 R2 for old versions).

- `Volume:\Inetpub\SolarWinds\*`
- `Volume:\ProgramData\SolarWinds\*`
- `Volume:\Program Files (x86)\Common Files\SolarWinds\*`
- `Volume:\Program Files (x86)\SolarWinds\*`
- `Volume:\Windows\Temp\SolarWinds\*`
- `Volume:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\*`

Source: http://support.solarwinds.com/SuccessCenter/s/article/Files-and-directories-to-exclude-from-antivirus-scanning-for-Orion-Platform-products

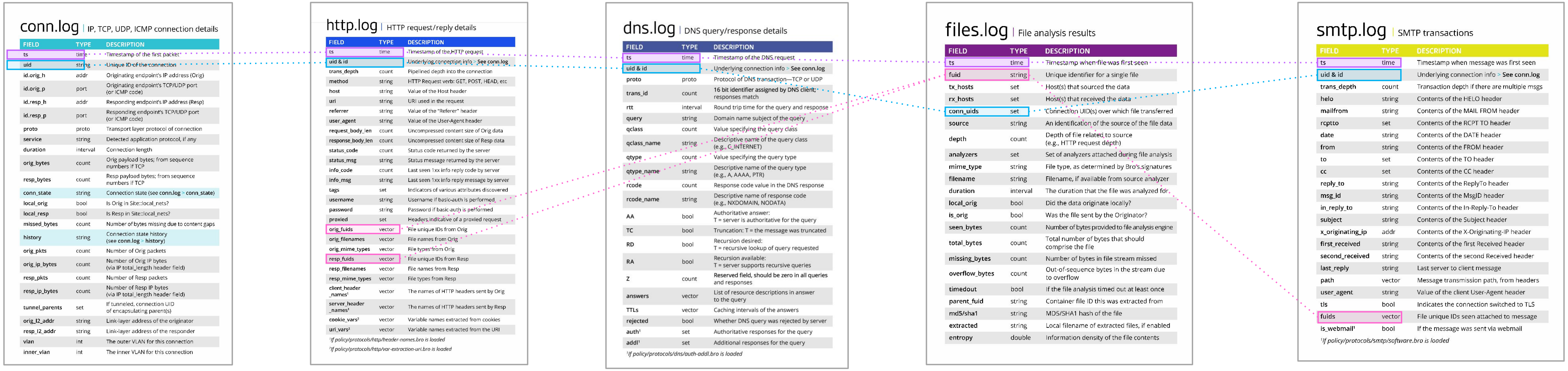
How can Suricata IDS rules protect me?

Suricata rulesets are quick to update, often automated, allowing indicators of compromise (IOCs) to be widely distributed and quickly flagged, helping you find the needle in the haystack:

- IP Addresses
- Domains
- HTTP headers and data (eg. POST data contents)
- Payload data (HTML strings, JavaScript commands, etc.)

IDS rules protect you from today, moving forward.

How does Corelight/Zeek data protect me?



conn.log | IP, TCP, UDP, ICMP connection details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of the first packet
uid	string	Unique ID of the connection
id.orig_h	addr	Originating endpoint's IP address (Orig)
id.orig_p	port	Originating endpoint's TCP/UDP port (or ICMP code)
id.resp_h	addr	Responding endpoint's IP address (Resp)
id.resp_p	port	Responding endpoint's TCP/UDP port (or ICMP code)
proto	proto	Transport layer protocol of connection
service	string	Detected application protocol, if any
duration	interval	Connection length
orig_bytes	count	Orig payload bytes; from sequence numbers if TCP
resp_bytes	count	Resp payload bytes; from sequence numbers if TCP
conn_state	string	Connection state (see **conn.log** > **conn_state**)
local_orig	bool	Is Orig in Site::local_nets?
local_resp	bool	Is Resp in Site::local_nets?
missed_bytes	count	Number of bytes missing due to content gaps
history	string	Connection state history (see **conn.log** > **history**)
orig_pkts	count	Number of Orig packets
orig_ip_bytes	count	Number of Orig IP bytes (via IP total_length header field)
resp_pkts	count	Number of Resp packets
resp_ip_bytes	count	Number of Resp IP bytes (via IP total_length header field)
tunnel_parents	set	If tunneled, connection UID of encapsulating parent(s)
orig_l2_addr	string	Link-layer address of the originator
resp_l2_addr	string	Link-layer address of the responder
vlan	int	The outer VLAN for this connection
inner_vlan	int	The inner VLAN for this connection

http.log | HTTP request/reply details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of the HTTP request
uid & id		Underlying connection info > **See conn.log**
trans_depth	count	Pipelined depth into the connection
method	string	HTTP Request verb: GET, POST, HEAD, etc
host	string	Value of the Host header
uri	string	URI used in the request
referrer	string	Value of the "Referer" header
user_agent	string	Value of the User-Agent header
request_body_len	count	Uncompressed content size of Orig data
response_body_len	count	Uncompressed content size of Resp data
status_code	count	Status code returned by the server
status_msg	string	Status message returned by the server
info_code	count	Last seen 1xx info reply code by server
info_msg	string	Last seen 1xx info reply message by server
tags	set	Indicators of various attributes discovered
username	string	Username if basic-auth is performed
password	string	Password if basic-auth is performed
proxied	set	Headers indicative of a proxied request
orig_fuids	vector	File unique IDs from Orig
orig_filenames	vector	File names from Orig
orig_mime_types	vector	File types from Orig
resp_fuids	vector	File unique IDs from Resp
resp_filenames	vector	File names from Resp
resp_mime_types	vector	File types from Resp
client_header_names[1]	vector	The names of HTTP headers sent by Orig
server_header_names[1]	vector	The names of HTTP headers sent by Resp
cookie_vars[2]	vector	Variable names extracted from cookies
uri_vars[2]	vector	Variable names extracted from the URI

[1] *If policy/protocols/http/header-names.bro is loaded*

[2] *If policy/protocols/http/var-extraction-uri.bro is loaded*

dns.log | DNS query/response details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of the DNS request
uid & id		Underlying connection info > **See conn.log**
proto	proto	Protocol of DNS transaction—TCP or UDP
trans_id	count	16 bit identifier assigned by DNS client; responses match
rtt	interval	Round trip time for the query and response
query	string	Domain name subject of the query
qclass	count	Value specifying the query class
qclass_name	string	Descriptive name of the query class (e.g., C_INTERNET)
qtype	count	Value specifying the query type
qtype_name	string	Descriptive name of the query type (e.g., A, AAAA, PTR)
rcode	count	Response code value in the DNS response
rcode_name	string	Descriptive name of response code (e.g., NXDOMAIN, NODATA)
AA	bool	Authoritative answer: T = server is authoritative for the query
TC	bool	Truncation: T = the message was truncated
RD	bool	Recursion desired: T = recursive lookup of query requested
RA	bool	Recursion available: T = server supports recursive queries
Z	count	Reserved field, should be zero in all queries and responses
answers	vector	List of resource descriptions in answer to the query
TTLs	vector	Caching intervals of the answers
rejected	bool	Whether DNS query was rejected by server
auth[1]	set	Authoritative responses for the query
addl[1]	set	Additional responses for the query

[1] *If policy/protocols/dns/auth-addl.bro is loaded*

files.log | File analysis results

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp when file was first seen
fuid	string	Unique identifier for a single file
tx_hosts	set	Host(s) that sourced the data
rx_hosts	set	Host(s) that received the data
conn_uids	set	Connection UID(s) over which file transferred
source	string	An identification of the source of the file data
depth	count	Depth of file related to source (e.g., HTTP request depth)
analyzers	set	Set of analyzers attached during file analysis
mime_type	string	File type, as determined by Bro's signatures
filename	string	Filename, if available from source analyzer
duration	interval	The duration that the file was analyzed for
local_orig	bool	Did the data originate locally?
is_orig	bool	Was the file sent by the Originator?
seen_bytes	count	Number of bytes provided to file analysis engine
total_bytes	count	Total number of bytes that should comprise the file
missing_bytes	count	Number of bytes in file stream missed
overflow_bytes	count	Out-of-sequence bytes in the stream due to overflow
timedout	bool	If the file analysis timed out at least once
parent_fuid	string	Container file ID this was extracted from
md5/sha1	string	MD5/SHA1 hash of the file
extracted	string	Local filename of extracted files, if enabled
entropy	double	Information density of the file contents

smtp.log | SMTP transactions

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp when message was first seen
uid & id		Underlying connection info > **See conn.log**
trans_depth	count	Transaction depth if there are multiple msgs
helo	string	Contents of the HELO header
mailfrom	string	Contents of the MAIL FROM header
rcptto	set	Contents of the RCPT TO header
date	string	Contents of the DATE header
from	string	Contents of the FROM header
to	set	Contents of the TO header
cc	set	Contents of the CC header
reply_to	string	Contents of the ReplyTo header
msg_id	string	Contents of the MsgID header
in_reply_to	string	Contents of the In-Reply-To header
subject	string	Contents of the Subject header
x_originating_ip	addr	Contents of the X-Originating-IP header
first_received	string	Contents of the first Received header
second_received	string	Contents of the second Received header
last_reply	string	Last server to client message
path	vector	Message transmission path, from headers
user_agent	string	Value of the client User-Agent header
tls	bool	Indicates the connection switched to TLS
fuids	vector	File unique IDs seen attached to message
is_webmail[1]	bool	If the message was sent via webmail

[1] *If policy/protocols/smtp/software.bro is loaded*

Corelight/Zeek provides comprehensive historical network metadata:

- Non-judgemental - it's a flight recorder.
- Easy to search, index, archive, and store.
- Directly linked to Suricata alerts for full context in a single-pivot.
- Gives you hindsight where IDS alerts cannot.

What we know and how we know it

Sources

1. **FireEye** initial breach: https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html

2. **FireEye** blog: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

3. **FireEye** IOCs: https://github.com/fireeye/sunburst_countermeasures

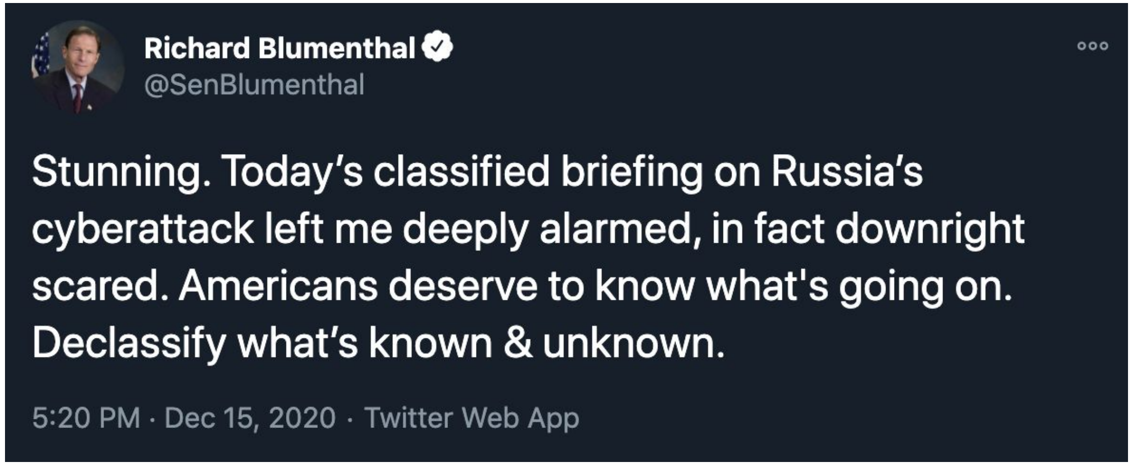
4. **Washington Post**: Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce

5. **Bambenek** IOCs: https://github.com/bambenek/research/

6. **Volexity** blog: https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/

7. **SolarWinds** SEC Filing: https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm

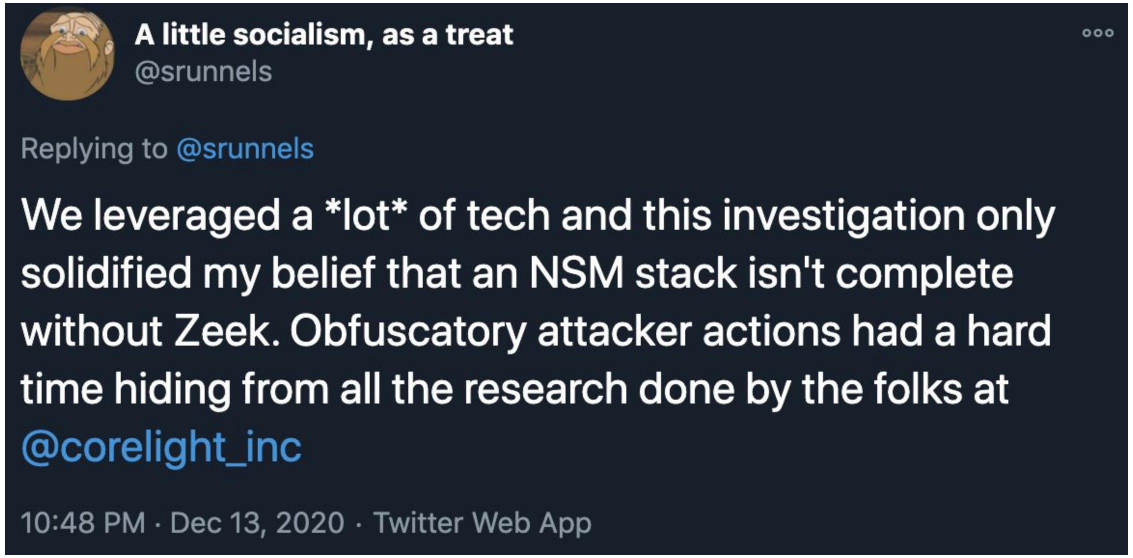
Informal sources



Richard Blumenthal
@SenBlumenthal

Stunning. Today’s classified briefing on Russia’s cyberattack left me deeply alarmed, in fact downright scared. Americans deserve to know what's going on. Declassify what’s known & unknown.

5:20 PM · Dec 15, 2020 · Twitter Web App



A little socialism, as a treat
@srunnels

Replying to @srunnels

We leveraged a *lot* of tech and this investigation only solidified my belief that an NSM stack isn't complete without Zeek. Obfuscatory attacker actions had a hard time hiding from all the research done by the folks at @corelight_inc

10:48 PM · Dec 13, 2020 · Twitter Web App

Timeline

March - June 2020: "compromise of the Orion software build system" affecting Orion products downloaded/updated during this time. Less than 18k of 33k customers affected. (Source: Solarwinds SEC filing)

December 8, 2020: FireEye announces they'd been hacked. Red Team tools stolen, but no zero-day exploits or unknown techniques. Releases IOCs.

December 13, 2020: US CISA releases emergency directive to begin forensic analysis and "immediately disconnect or power down SolarWinds Orion products."

December 14, 2020: FireEye posts details with IOCs and attributes UNC2452
December 14, 2020: Reuters, Washington Post reveal that US Treasury, Commerce breached, along with "consulting, technology, telecom, and oil and gas companies." Attributed to Russian SVR (aka APT29 / Cozy Bear)

December 15, 2020: SolarWinds expected to release hotfix.

Attacker Techniques

Commonly used techniques:

- Domain Generation Algorithms (DGA)
- Scalable and shared cloud-based infrastructure
- Cobalt Strike beacons

Uncommon / Novel techniques:

- Compromise of SolarWinds certificate used to build Orion updates (but how?)
- Blending in with naming conventions used by the development team
- Attacker changed hostnames to match those within victim environment
- Avoiding detection and analysis using payload delays (12-14 days) and IP exclusions for local sinkholes and Microsoft-owned IP ranges

Detection Opportunities

IP addresses tied to the victim’s home country to remove obvious detections

Still presents an opportunity for “time travel” detection

- Legitimate credential owner accesses a remote service from City A…
- Attacker uses the same credentials from City B 10 minutes later…
- But City A & City B are hours apart

Detection Opportunities

Leaked in RDP SSL certificate data **on servers outside the victim IP range**

FEYE recommendation to search (Shodan) scan data for RDP systems with hostnames from victim environment

Zeek logs this detail for all monitored RDP sessions - but also can easily track outbound RDP destinations

Domain IOCs

	FireEye	EmergingThreats	Volexity
avsvmcloud.com	X	X	X
digitalcollege.org	X	X	X
freescanonline.com	X	X	X
thedoccloud.com	X	X	X
deftsecurity.com	X	X	
virtualdataserver.com	X	X	
incomeupdate.com	X	X	
zupertech.com	X	X	
databasegalore.com	X	X	
panhardware.com	X	X	
highdatabase.com	X	X	
websitetheme.com	X	X	
webcodez.com			X
virtualwebdata.com			X
seobundlekit.com			X
lcomputers.com			X
solartrackingsystem.net			X
kubecloud.com			X
globalnetworkissues.com			X

Where do I get the Suricata rules?

Emerging Threats feed

All signatures released by FireEye were imported into the ET Open set within < 24 hours of each public drop

SIDs 2031264-2031270, 2031273-2031297, 2031299-2031308 - FEYE red team tools

SIDs 2031321-2031370 - Sunburst

Came with notable performance/accuracy improvements over FireEye GitHub

Raw signature imports

Possible to import signatures directly from GitHub - get files as plaintext to start

SID management is your responsibility! Some of the FireEye rules overlapped with Talos

For those using suricata-update, the “--local <path>” option can be pointed to the downloaded file

Rules files are plain text, so public sources can be manually integrated with any other process

Reviewing Suricata rules

Hostname detail signatures

```
alert tcp any any <> any 443 (msg:"Backdoor.SUNBURST"; content:"|16
03|"; depth:2; content:"avsvmcloud.com"; distance:0; sid:77600845;
rev:1;)
```

```
alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"ET MALWARE [Fireeye]
Backdoor.SUNBURST SSL Cert Inbound (avsvmcloud .com)";
flow:established,to_client; tls.cert_subject; dotprefix;
content:".avsvmcloud.com"; endswith; fast_pattern;
reference:[...]; classtype:trojan-activity; sid:2031341; rev:2;
metadata:[...];)
```

Similar HTTP rules published by FEYE (with similar upgrades from ET)

ET added DNS lookup rules as well

URL structure signatures

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE
[Fireeye] Backdoor.SUNBURST M2"; flow:established,to_server;
http.uri; content:"/swip/upd/SolarWinds.CortexPlugin.Components.xml";
http.host; content:!".solarwinds.com"; endswith;
reference:[...]; classtype:trojan-activity; sid:2031337; rev:2;
metadata:[...];)
```

Specific URL structure used by updates for my tool, going to a host not owned by the vendor

Proactive potential: what URLs do my tools legitimately use today? Can I detect those structures being sent to unusual hosts?

Beacon content signatures - headers

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE
[Fireeye] Backdoor.BEACON M1"; flow:established,to_server;

http.method; content:"POST";

http.request_body; content:"name=|22|"; content:"|22 3b|filename=|22|";
content:"|22 0a|Content-Type|3a|"; fast_pattern;

reference:[...]; classtype:trojan-activity; sid:2031323; rev:2;
metadata:[...])
```

Beacon content signatures - payloads

```
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ET MALWARE
[Fireeye] Backdoor.BEACON M3"; flow:established,from_server;

file.data; content:"<title>Woman-Five-How-To-Why-Your-Celebrating-
Learn-Brand</title>"

reference:[...]; classtype:trojan-activity; sid:2031356; rev:2;
metadata:[...])
```

Applying future knowledge to past data

Applying future knowledge to past data

Attackers have already had a chance to clean up

Attackers with good tradecraft clean up as soon as possible

This is (yet again) why it is important to retain months of network forensic data

Don’t expect the more specific indicators to have any real longevity

Searching through Zeek/Corelight data for IOCs

IOCs

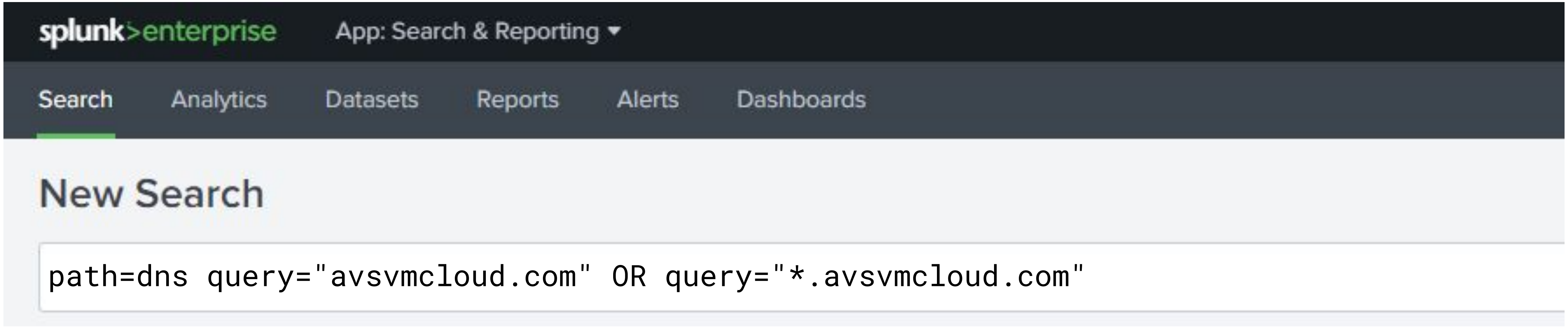
In order of confidence, here are the IOCs to focus on:

- Domain names
- HTTP requests
- X.509 Certificates
- IP addresses
- File hashes

IOCs

In order of confidence, here are the IOCs to focus on:

- **Domain names**
- HTTP requests
- X.509 Certificates
- IP addresses
- File hashes

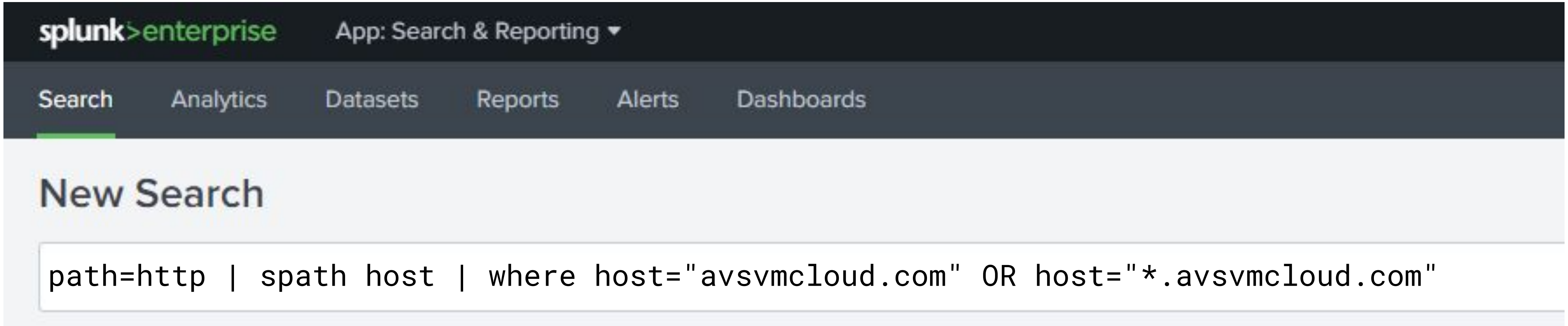


```
path=dns query="avsvmcloud.com" OR query="*.avsvmcloud.com"
```

IOCs

In order of confidence, here are the IOCs to focus on:

- **Domain names**
- **HTTP requests**
- X.509 Certificates
- IP addresses
- File hashes

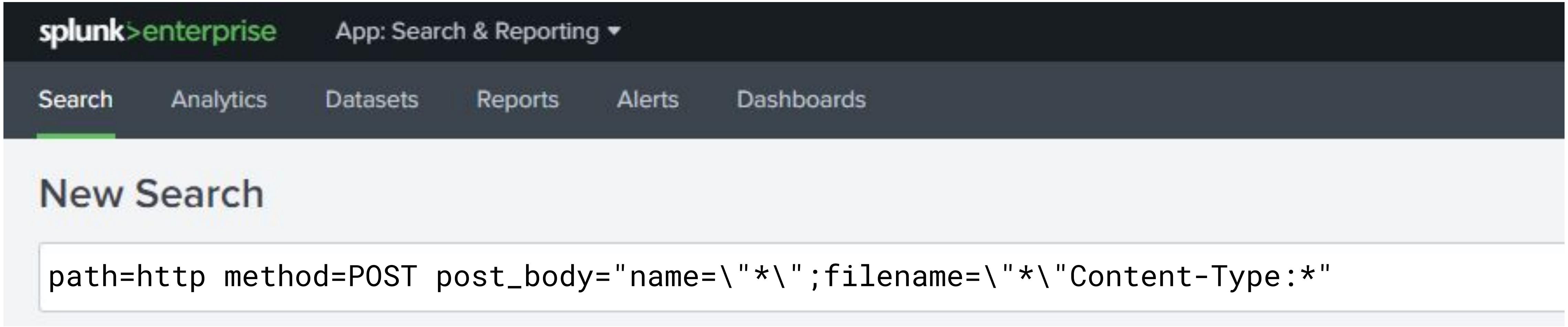


```
path=http | spath host | where host="avsvmcloud.com" OR host="*.avsvmcloud.com"
```

IOCs

In order of confidence, here are the IOCs to focus on:

- Domain names
- **HTTP requests**
- X.509 Certificates
- IP addresses
- File hashes

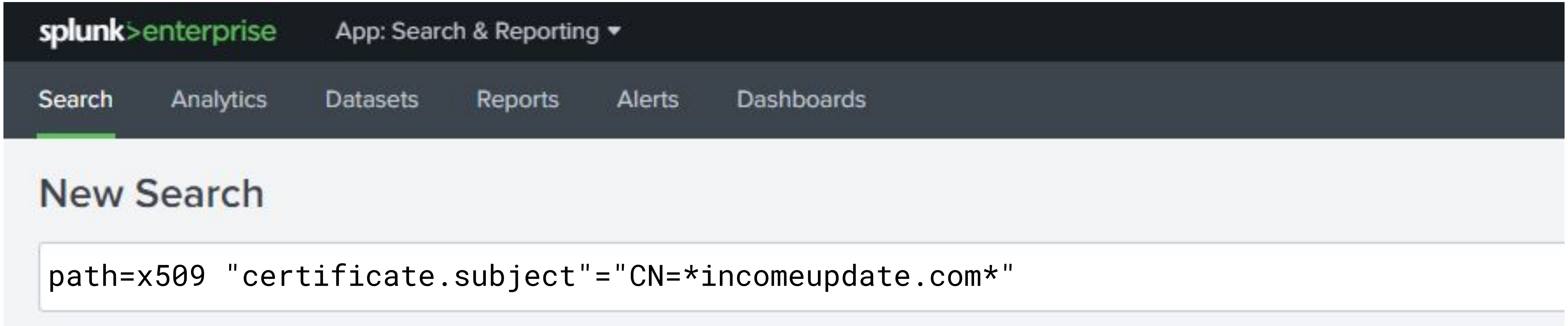


```
path=http method=POST post_body="name=\"*\";filename=\"*\"Content-Type:*"
```

IOCs

In order of confidence, here are the IOCs to focus on:

- Domain names
- HTTP requests
- **X.509 Certificates**
- IP addresses
- File hashes

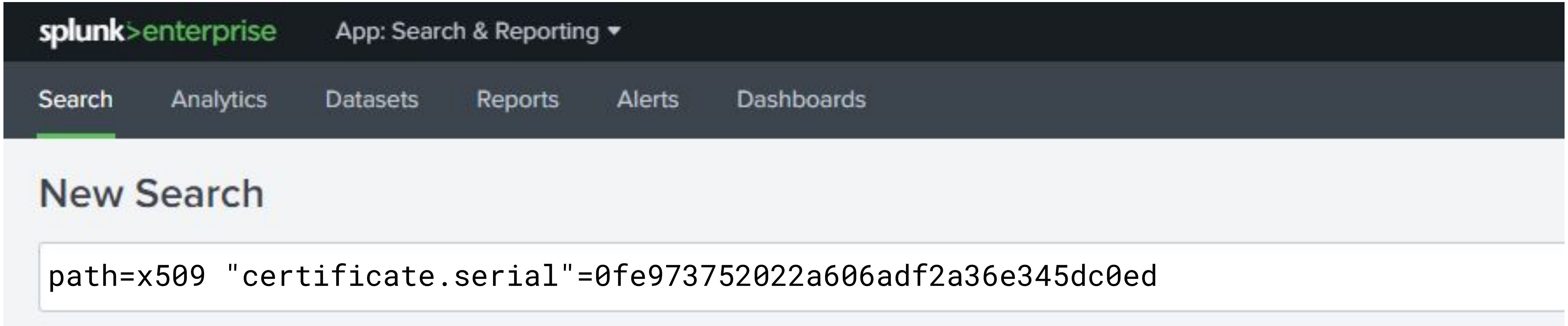


```
path=x509 "certificate.subject"="CN=*incomeupdate.com*"
```

IOCs

In order of confidence, here are the IOCs to focus on:

- Domain names
- HTTP requests
- **X.509 Certificates**
- IP addresses
- File hashes

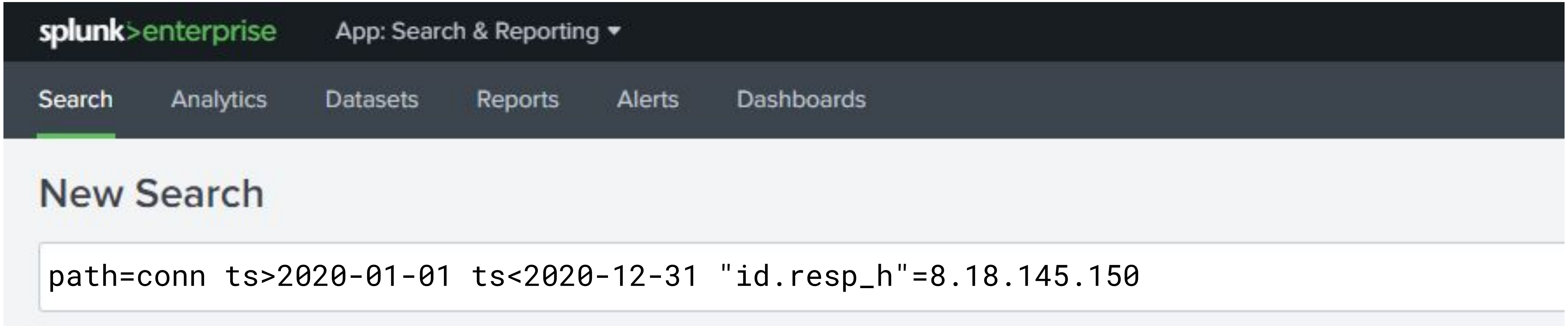


```
path=x509 "certificate.serial"=0fe973752022a606adf2a36e345dc0ed
```

IOCs

In order of confidence, here are the IOCs to focus on:

- Domain names
- HTTP requests
- X.509 Certificates
- **IP addresses**
- File hashes

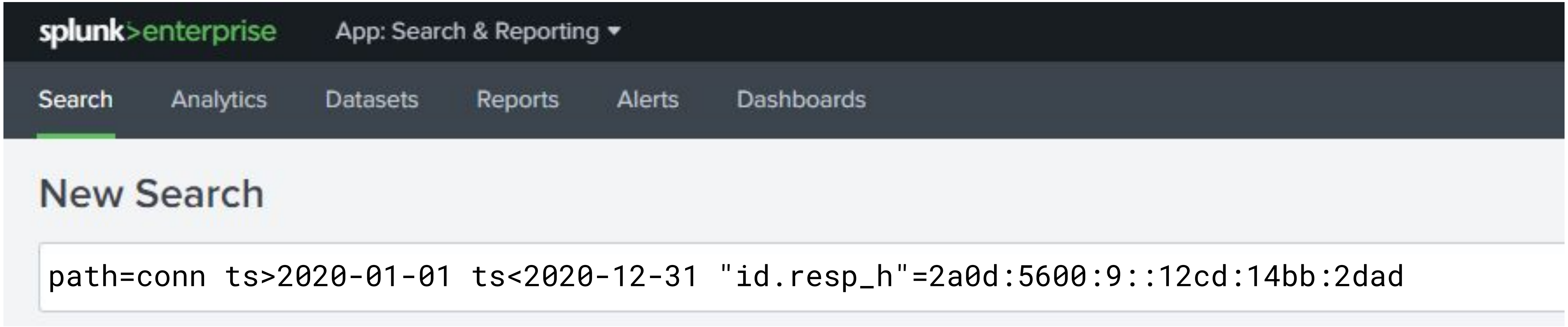


```
path=conn ts>2020-01-01 ts<2020-12-31 "id.resp_h"=8.18.145.150
```

IOCs

In order of confidence, here are the IOCs to focus on:

- Domain names
- HTTP requests
- X.509 Certificates
- **IP addresses**
- File hashes

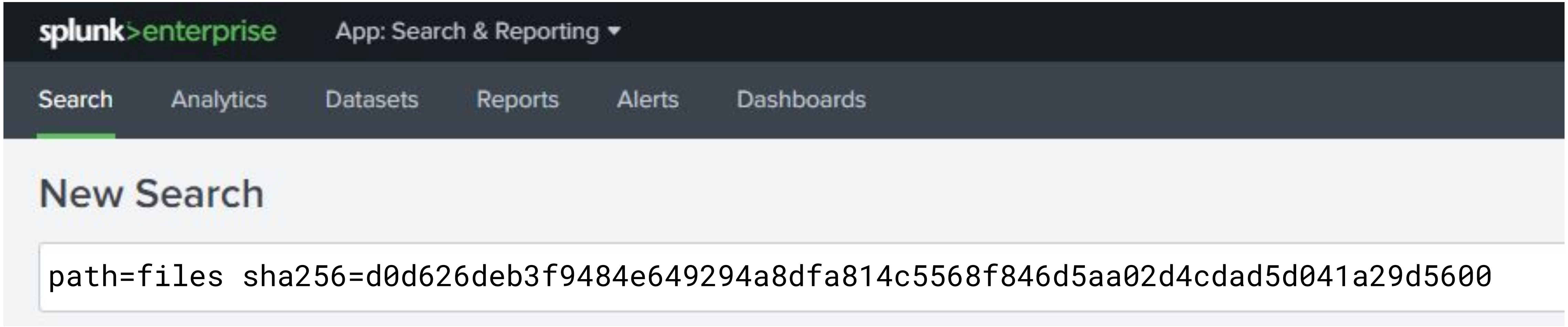


```
path=conn ts>2020-01-01 ts<2020-12-31 "id.resp_h"=2a0d:5600:9::12cd:14bb:2dad
```

IOCs

In order of confidence, here are the IOCs to focus on:

- Domain names
- HTTP requests
- X.509 Certificates
- IP addresses
- **File hashes**



```
path=files sha256=d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600
```

Do I have SolarWinds?

Potential queries to determine if you have SolarWinds products:

- HTTP User-Agent of "SolarWindsOrionImprovementClient/*"
- DNS resolution of "api.solarwinds.com" or "downloads.solarwinds.com" (daily) "licensestatusserver.solarwinds.com"or "licenseserver.solarwinds.com" (intermittent)

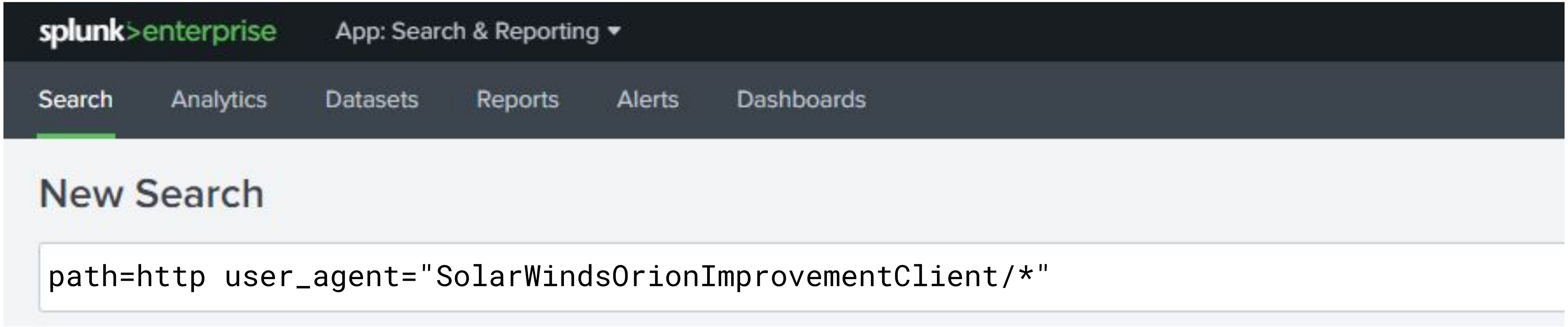
(This will likely return results for other SolarWinds products other than Orion)

Do I have SolarWinds?

Potential queries to determine if you have SolarWinds products:

- **HTTP User-Agent of "SolarWindsOrionImprovementClient/*"**
- DNS resolution of "api.solarwinds.com" or "downloads.solarwinds.com" (daily) "licensestatusserver.solarwinds.com"or "licenseserver.solarwinds.com" (intermittent)

(This will likely return results for other SolarWinds products other than Orion)



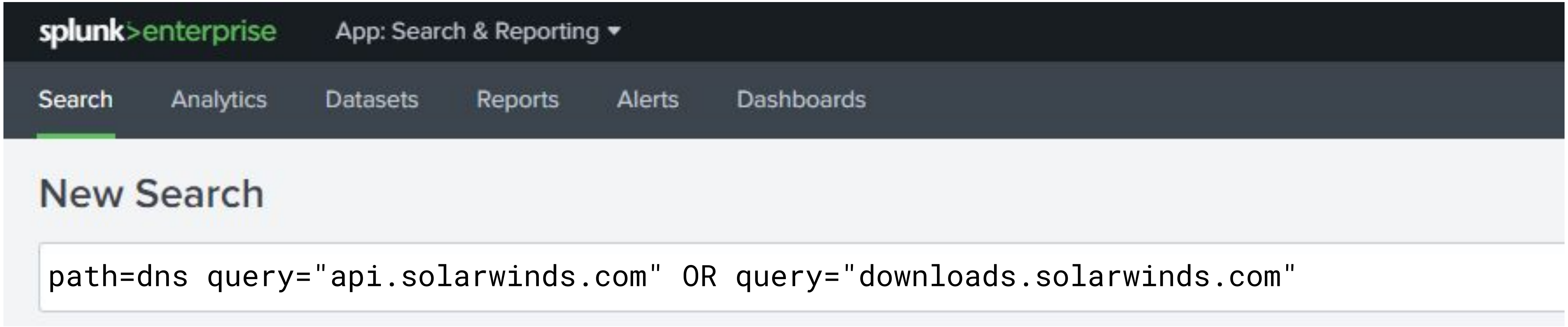
```
path=http user_agent="SolarWindsOrionImprovementClient/*"
```

Do I have SolarWinds?

Potential queries to determine if you have SolarWinds products:

- HTTP User-Agent of "SolarWindsOrionImprovementClient/*"
- **DNS resolution of "api.solarwinds.com" or "downloads.solarwinds.com" (daily)** "licensestatusserver.solarwinds.com"or "licenseserver.solarwinds.com" (intermittent)

(This will likely return results for other SolarWinds products other than Orion)



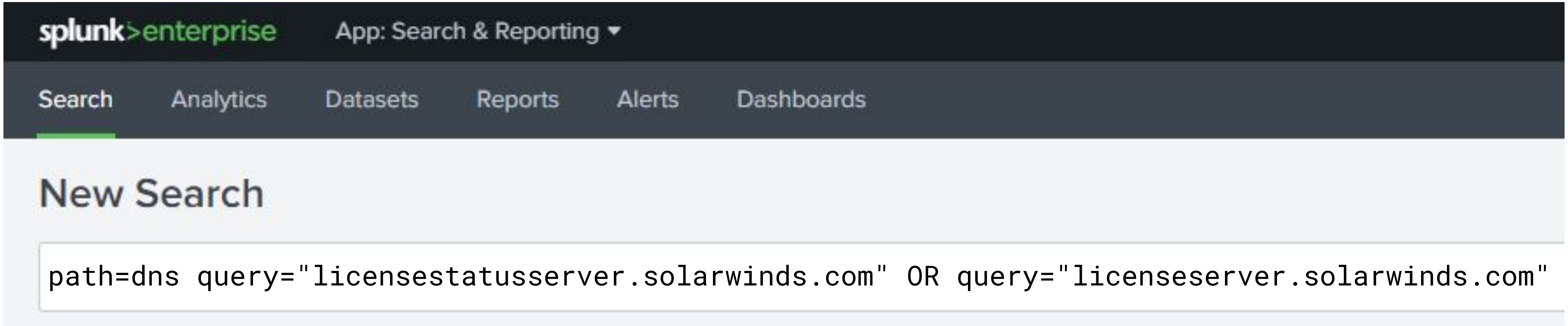
```
path=dns query="api.solarwinds.com" OR query="downloads.solarwinds.com"
```

Do I have SolarWinds?

Potential queries to determine if you have SolarWinds products:

- HTTP User-Agent of "SolarWindsOrionImprovementClient/*"
- DNS resolution of "api.solarwinds.com" or "downloads.solarwinds.com" (daily) **"licensestatusserver.solarwinds.com"or "licenseserver.solarwinds.com" (intermittent)**

(This will likely return results for other SolarWinds products other than Orion)



```
path=dns query="licensestatusserver.solarwinds.com" OR query="licenseserver.solarwinds.com"
```

Resources

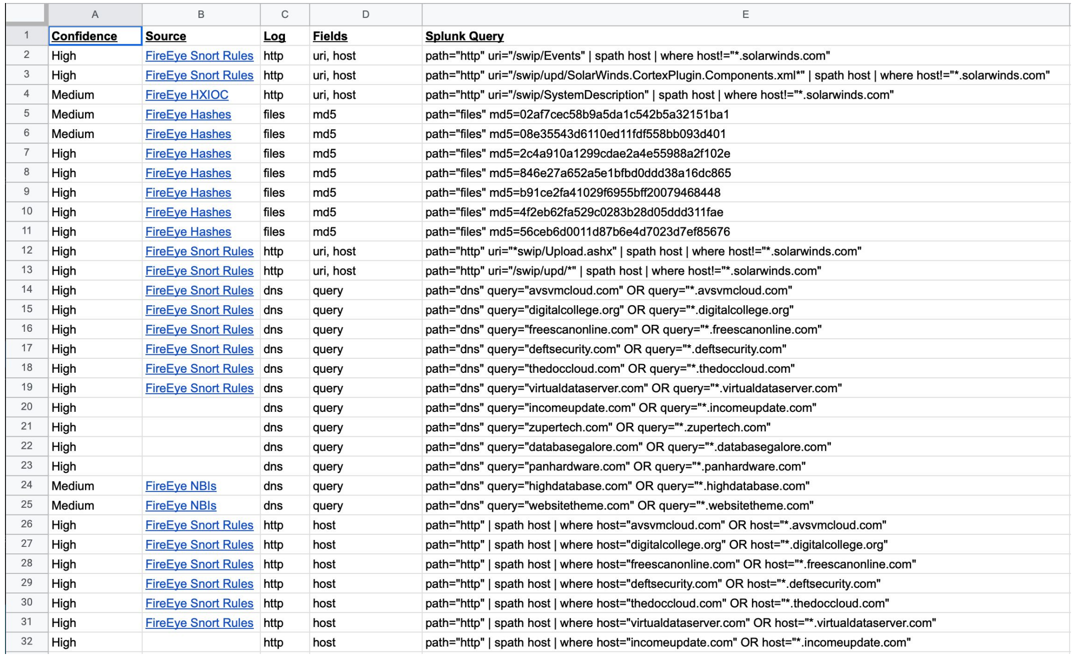
Watch these sources for updates!

- FireEye IOCs: https://github.com/fireeye/sunburst_countermeasures
- ET Rules: https://rules.emergingthreats.net/open/suricata-5.0/
- Sigma Rules: https://socprime.com/blog/sunburst-backdoor-detection-solarwinds-supply-chain-attack-on-fireeye-and-us-agencies/
- Corelight Blog: https://corelight.blog/tag/solarigate/

Q+A

(… and one more thing …)

Searching Corelight data for Solarigate IOCs



	A	B	C	D	E
1	**Confidence**	**Source**	**Log**	**Fields**	**Splunk Query**
2	High	FireEye Snort Rules	http	uri, host	path="http" uri="/swip/Events" | spath host | where host!="*.solarwinds.com"
3	High	FireEye Snort Rules	http	uri, host	path="http" uri="/swip/upd/SolarWinds.CortexPlugin.Components.xml*" | spath host | where host!="*.solarwinds.com"
4	Medium	FireEye HXIOC	http	uri, host	path="http" uri="/swip/SystemDescription" | spath host | where host!="*.solarwinds.com"
5	Medium	FireEye Hashes	files	md5	path="files" md5=02af7cec58b9a5da1c542b5a32151ba1
6	Medium	FireEye Hashes	files	md5	path="files" md5=08e35543d6110ed11fdf558bb093d401
7	High	FireEye Hashes	files	md5	path="files" md5=2c4a910a1299cdae2a4e55988a2f102e
8	High	FireEye Hashes	files	md5	path="files" md5=846e27a652a5e1bfbd0ddd38a16dc865
9	High	FireEye Hashes	files	md5	path="files" md5=b91ce2fa41029f6955bff20079468448
10	High	FireEye Hashes	files	md5	path="files" md5=4f2eb62fa529c0283b28d05ddd311fae
11	High	FireEye Hashes	files	md5	path="files" md5=56ceb6d0011d87b6e4d7023d7ef85676
12	High	FireEye Snort Rules	http	uri, host	path="http" uri="*swip/Upload.ashx" | spath host | where host!="*.solarwinds.com"
13	High	FireEye Snort Rules	http	uri, host	path="http" uri="/swip/upd/*" | spath host | where host!="*.solarwinds.com"
14	High	FireEye Snort Rules	dns	query	path="dns" query="avsvmcloud.com" OR query="*.avsvmcloud.com"
15	High	FireEye Snort Rules	dns	query	path="dns" query="digitalcollege.org" OR query="*.digitalcollege.org"
16	High	FireEye Snort Rules	dns	query	path="dns" query="freescanonline.com" OR query="*.freescanonline.com"
17	High	FireEye Snort Rules	dns	query	path="dns" query="deftsecurity.com" OR query="*.deftsecurity.com"
18	High	FireEye Snort Rules	dns	query	path="dns" query="thedoccloud.com" OR query="*.thedoccloud.com"
19	High	FireEye Snort Rules	dns	query	path="dns" query="virtualdataserver.com" OR query="*.virtualdataserver.com"
20	High		dns	query	path="dns" query="incomeupdate.com" OR query="*.incomeupdate.com"
21	High		dns	query	path="dns" query="zupertech.com" OR query="*.zupertech.com"
22	High		dns	query	path="dns" query="databasegalore.com" OR query="*.databasegalore.com"
23	High		dns	query	path="dns" query="panhardware.com" OR query="*.panhardware.com"
24	Medium	FireEye NBIs	dns	query	path="dns" query="highdatabase.com" OR query="*.highdatabase.com"
25	Medium	FireEye NBIs	dns	query	path="dns" query="websitetheme.com" OR query="*.websitetheme.com"
26	High	FireEye Snort Rules	http	host	path="http" | spath host | where host="avsvmcloud.com" OR host="*.avsvmcloud.com"
27	High	FireEye Snort Rules	http	host	path="http" | spath host | where host="digitalcollege.org" OR host="*.digitalcollege.org"
28	High	FireEye Snort Rules	http	host	path="http" | spath host | where host="freescanonline.com" OR host="*.freescanonline.com"
29	High	FireEye Snort Rules	http	host	path="http" | spath host | where host="deftsecurity.com" OR host="*.deftsecurity.com"
30	High	FireEye Snort Rules	http	host	path="http" | spath host | where host="thedoccloud.com" OR host="*.thedoccloud.com"
31	High	FireEye Snort Rules	http	host	path="http" | spath host | where host="virtualdataserver.com" OR host="*.virtualdataserver.com"
32	High		http	host	path="http" | spath host | where host="incomeupdate.com" OR host="*.incomeupdate.com"

https://solarigate.training.corelight.io

Caveats:

- These IOCs come from the community (FireEye, Volexity, John Bambenek, SANS)
- Splunk queries use JSON, are written to be overly broad, and may tax your cluster
- Zeek-Cut queries are more prone to error (both false positives and false negatives)

Q+A

Aaron Soto
Director of Learning
aaron.soto@corelight.com
Twitter: **@_surefire_**

Alex Kirk
Global Principal
akirk@corelight.com
Twitter: **@alexgkirk**

corelight
info@corelight.com
www.corelight.com

Watch our blog post for updates:
https://corelight.blog/2020/12/15/finding-sunburst-backdoor-with-zeek-logs-and-corelight/

We will post recording, slide deck and Corelight / Zeek IOCs URL shortly.