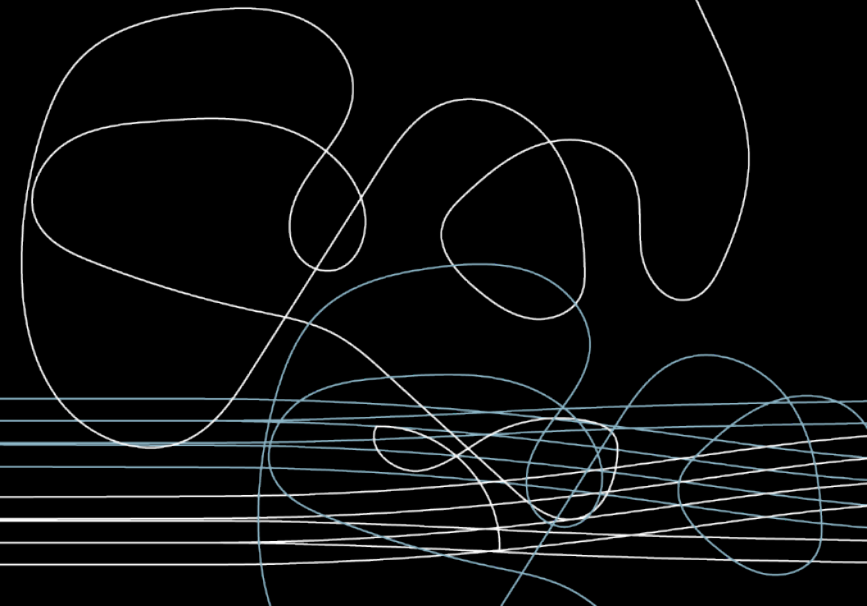




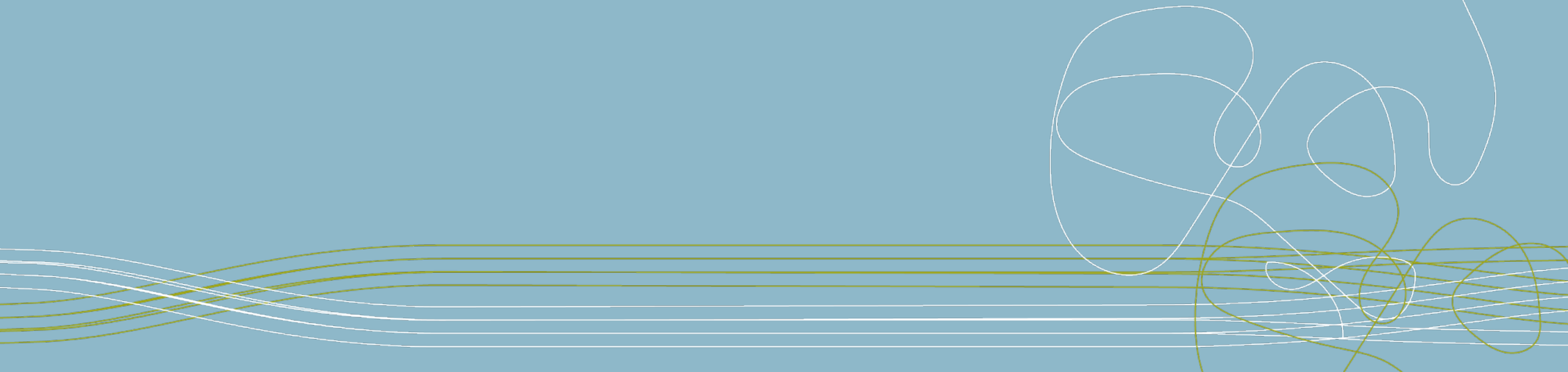
Security Brief

Detecting and Responding to PrintNightmare



ōrdr

Identify Print Nightmare Vulnerable systems



Navigate to the Security Tab

Click Here



Locate Vulnerable Assets

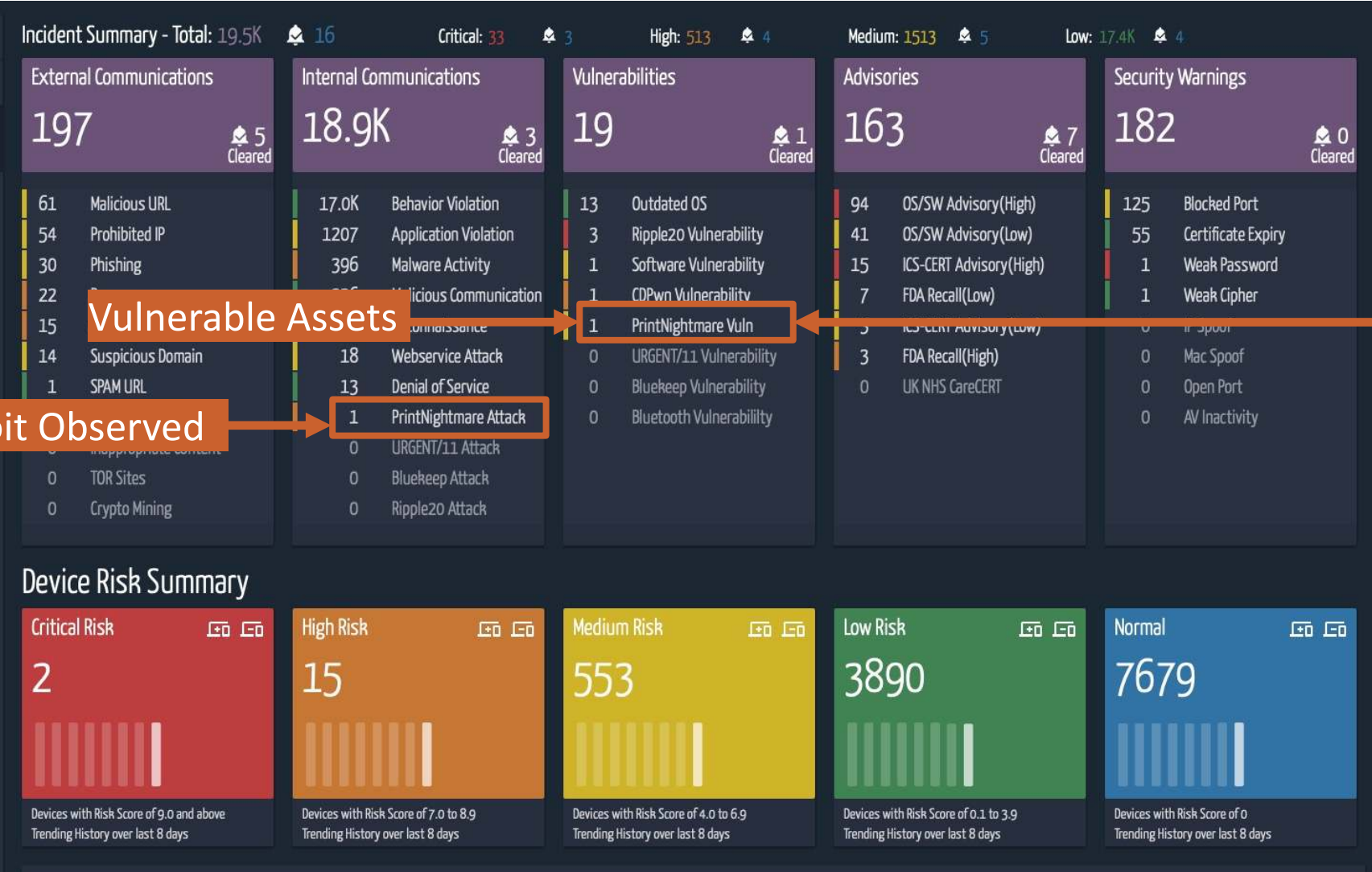
Active Exploit Observed

Slide 8 and beyond cover this

Vulnerable Assets

Click Here

Following slides cover this



Uncover all assets with a running vulnerable print spooler

Security Incidents of Category : PrintNightmare Vuln

Incident List as of 10/22/2021 10:57:06 AM

Total 1 Incident

Any Visible Field

=

case insensitive substring to match ...

Manage

No.	Risk	Score	Incident Category	Incident Type	Last Occurrence	Devices	Cleared	Peer Id	Actions
1	● medium	6	PrintNightmare Vuln	CVE-2021-34527:Windows Print Spooler Remot	10/15/2021 01:04 AM	3843	0		

List of Devices									
Total 3842 Devices match 1 filter									
Clear all criteria Filter of Device with Alarm									
No.	Mac Address	IP Address	Device Name	Group	Profile	Risk	Vuln	Info	
1	7C:67:A2:66:E0:86	10.36.100.111	windows-358.ordr.net	Workstations	Intel-Workstation	normal	critical		
2	00:D0:68:63:CB:E9	10.36.138.124	ie33-266.ordr.net	Medical Devices	Philips-iE33-Ultrasound	low	critical		
3	00:0C:C6:62:43:DF	10.36.138.160	statstrip-257.ordr.net	Medical Devices	NovaBioMedical-StatStrip-G	normal	medium		
4	D4:95:24:60:DD:58	10.36.168.24	c100-637.ordr.net	Retail Devices	Clover Networks-C100-POS	normal	critical		
5	00:10:8D:64:ED:C0	10.37.116.89	york-591.ordr.net	Facility Devices	Johnson Controls-Building	low	critical		
6	00:68:EB:64:BE:C2	10.36.161.59	hpz230workstation-566	Workstations	HP-Workstation	normal	critical		
7	00:D0:68:67:65:DD	10.36.124.252	ie33-477.ordr.net	Medical Devices	Philips-iE33-Ultrasound	low	critical		
8	A4:8C:DB:62:E5:C5	10.36.163.1	thinkpad	Others	Lenovo-Default	normal	critical		
9	A4:8C:DB:62:81:FC	10.36.163.91	thinkpad	Others	Lenovo-Default	normal	critical		
10	00:1E:64:67:4C:B3	10.36.127.206	pmcare31cmfspdusperc	Medical Devices	GE-SuperC-X-ray Angiograph	low	medium		
11	40:AC:8D:60:FC:38	10.39.184.74	timedclockplus-494.ordr	Facility Devices	Data Management-TimeClock	low	critical		
12	2C:41:38:67:CF:0E	10.36.139.213	infinia-512.ordr.net	Medical Devices	GE-Infinia-Gamma Camera	low	medium		
13	38:60:77:61:EE:C6	10.36.139.96	encore2-543.ordr.net	Medical Devices	Siemens-Encore2-SPECT Sy	low	medium		
14	00:0B:A3:61:72:C7	10.36.168.83	logiclogo8.2-684.ordr.n	Industrial Devices	Siemens-PLC	low	critical		
15	00:80:17:61:8B:A3	10.36.139.55	logiqe-499.ordr.net	Medical Devices	GE-Logiqe-Ultrasound	low	critical		
16	00:0D:87:61:13:96	10.39.146.134	Agilent plateloc	Life Science Devices	Agilent-PlateLoc-Thermal M	normal	medium		
17	00:00:63:63:98:C0	10.36.160.37	hpz800workstation-223	Others	BarcoCon-Default	normal	critical		
18	00:0C:6E:62:B5:B1	10.39.146.224	CyTOF 2	Life Science Devices	Fluidigm-CyTOF 2-Mass cyt	normal	critical		

[Click Here](#)

Export this list and do what MS says

MSFT - recommends that customer follow these steps immediately:

- In ALL cases, apply the CVE-2021-34527 security update. The update will not change existing registry settings
- After applying the security update, review the registry settings documented in the CVE-2021-34527 advisory
- If the registry keys documented do not exist, no further action is required
- If the registry keys documented exist, in order to secure your system, you must confirm that the following registry keys are set to 0 (zero) or are not present:
 - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint
 - NoWarningNoElevationOnInstall = 0 (DWORD) or not defined (default setting)
 - UpdatePromptSettings = 0 (DWORD) or not defined (default setting)
- For more in-depth guidance, please see [KB5005010: Restricting installation of new printer drivers after applying the July 6, 2021 updates](#) and [CVE-2021-34527](#).
- If our investigation identifies additional issues, we will take action as needed to help protect customers

Microsoft Documented Workarounds: (if patch is not available)

Find Systems With Print Spoolers

1. Users are urged to disable the “Print Spooler” service on servers that do not require it. Microsoft has provided a series of workarounds to be applied. Determine if the Print Spooler service is running (run as a Domain Admin)
2. Run the following as a Domain Admin: `Get-Service -Name Spooler`
3. If the Print Spooler is running or if the service is not set to disabled, select one of the following options to either disable the Print Spooler service, or to Disable inbound remote printing through Group Policy.

Option 1: Disable Print Spooler

If disabling the Print Spooler service is appropriate for your enterprise, use the following PowerShell commands:

```
Stop-Service -Name Spooler -Force  
Set-Service -Name Spooler -StartupType Disabled
```

Impact of workaround: Disabling the Print Spooler service disables the ability to print both locally and remotely.

Option 2: Disable Remote Printing

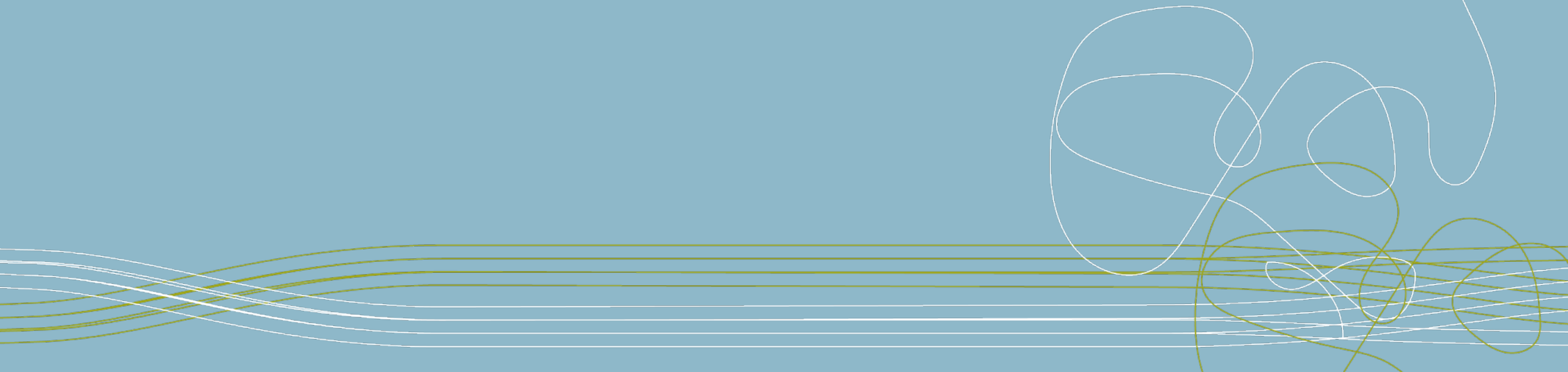
You can also configure the settings via Group Policy as follows:
Computer Configuration / Administrative Templates / Printers

Disable the “Allow Print Spooler to accept client connections:” policy to block remote attacks.

Impact of workaround: This policy will block the remote attack vector by preventing inbound remote printing operations. The system will no longer function as a print server, but local printing to a directly attached device will still be possible.

ōrdr

Active Print Nightmare Attack



Locate Vulnerable Assets



Click Here

Following slides cover this

Identify the offending systems

Security Incidents of Category : PrintNightmare Attack

Incident List as of 10/22/2021 11:29:19 AM

Total 1 Incident

Any Visible Field = case insensitive substring to match ... Manage

No.	Risk	Score	Incident Category	Incident Type	Last Occurrence	Devices	Cleared	Peer Id	Actions
1	high	8	PrintNightmare Attack	Microsoft Windows Print Spooler exploit attempt	8/16/2021 09:11 PM	2	0	192.168.1.157	

Click Here

List of Devices

Total 2 Devices match 1 filter

Any Visible Field = case insensitive substring to match ... Manage

Clear all criteria Filter of Device with Alarm

No.	Mac Address	IP Address	Device Name	Group	Profile	Risk	Vuln	Info
1	00:1C:23:66:9D:7F	192.168.1.157	dellwok-898.ordr.net	Workstations	Dell-Workstation	medium	critical	
2	00:1C:23:65:91:7F	192.168.1.149	dellwork-298.ordr.net	Workstations	Dell-Workstation	medium	critical	

Click Here

To mitigate the threat from these attacks

List of Devices

Total 2 Devices match 1 filter

Push them into a blocklist

Create a CLI

Classification View

Buttons:

- Add to Blocklist (2 Rows)
- Blocklist & Port Shut (2 Rows)
- Remove Blocklist (0 Rows)
- Remove Blocklist & Enable Ports (0 Rows)
- Generate Blocklist CLI
- Fetch Installed Software Info (2 Rows)
- Change VLAN (enforce) (2 Rows)
- Initiate Scan (2 Rows)
- Delete Devices (2 Rows)
- Change Attributes (2 Rows)
- Analyze App Usage (2 Rows)

No.	Mac Address	IP Address	Device Name	Group	Profile	Risk	Vuln	Info
1	00:1C:23:66:9D:7F	192.168.1.157	dellwok-898.ordr.net	Workstations	Dell-Workstation	medium	critical	
2	00:1C:23:65:91:7F	192.168.1.149	dellwork-298.ordr.net	Workstations	Dell-Workstation	medium	critical	

Select the offending hosts

Copy paste this into your switches

```
Device CLI ConfigurationBlocklist Config  
  
CLI for: 10.1.21.2  
mac address-table static 0007.5f63.bdbc vlan 951 drop  
interface GigabitEthernet1/0/31  
shutdown  
  
mac address-table static 0040.8c66.9b4d vlan 951 drop  
interface GigabitEthernet1/0/15  
shutdown  
  
mac address-table static 0007.5f60.6b5c vlan 951 drop  
interface GigabitEthernet1/0/27  
shutdown  
  
mac address-table static accc.8e65.37b8 vlan 951 drop  
interface GigabitEthernet1/0/12  
shutdown  
  
mac address-table static accc.8e65.24bf vlan 951 drop  
interface GigabitEthernet1/0/2  
shutdown  
  
Number of devices for which Config CLI could not be generated: 17
```

ördr

