ōrdr

Security Brief

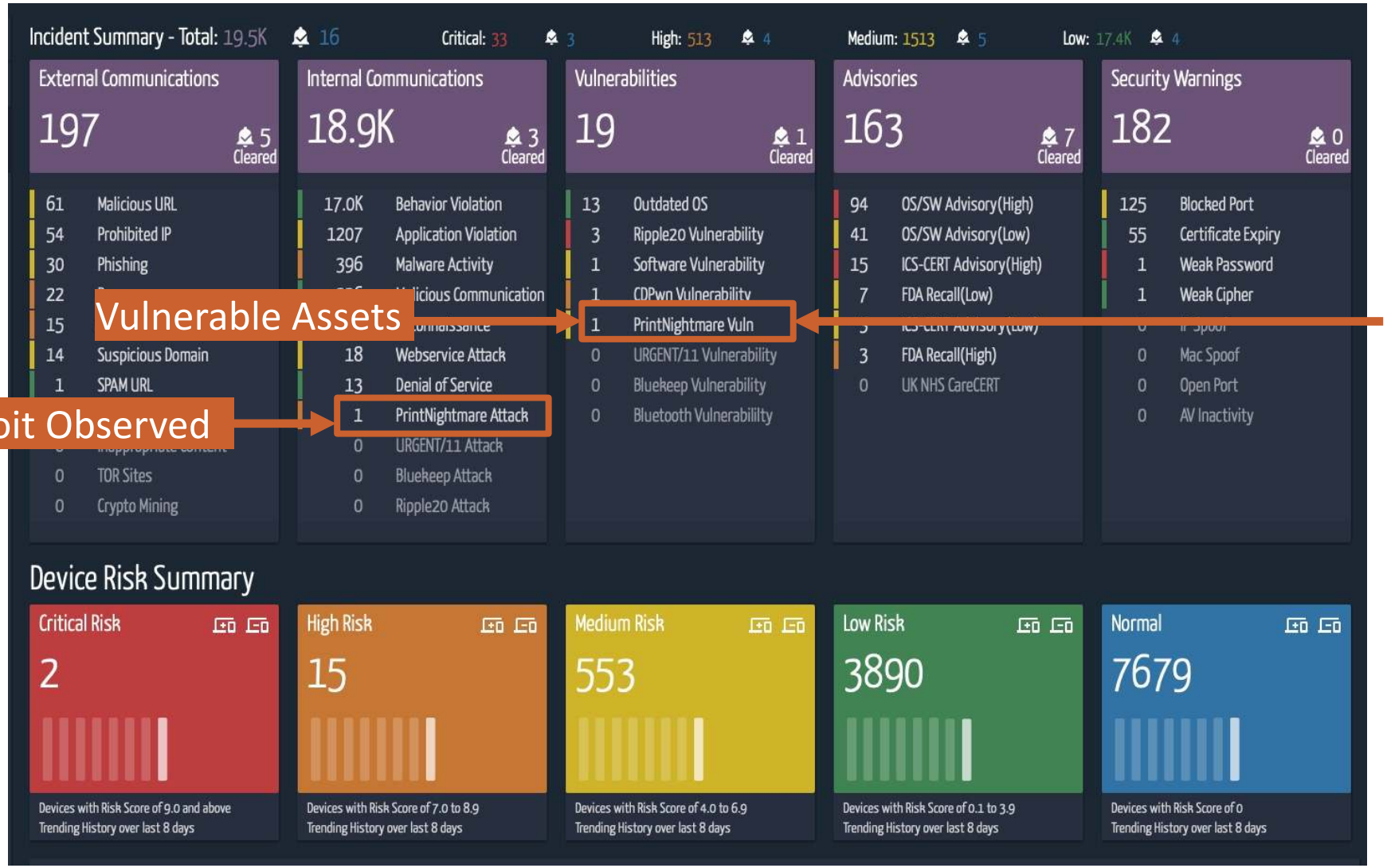
Detecting and Responding to PrintNightmare

Identify Print Nightmare Vulnerable systems

Navigate to the Security Tab

Click Here

Locate Vulnerable Assets



Vulnerable Assets

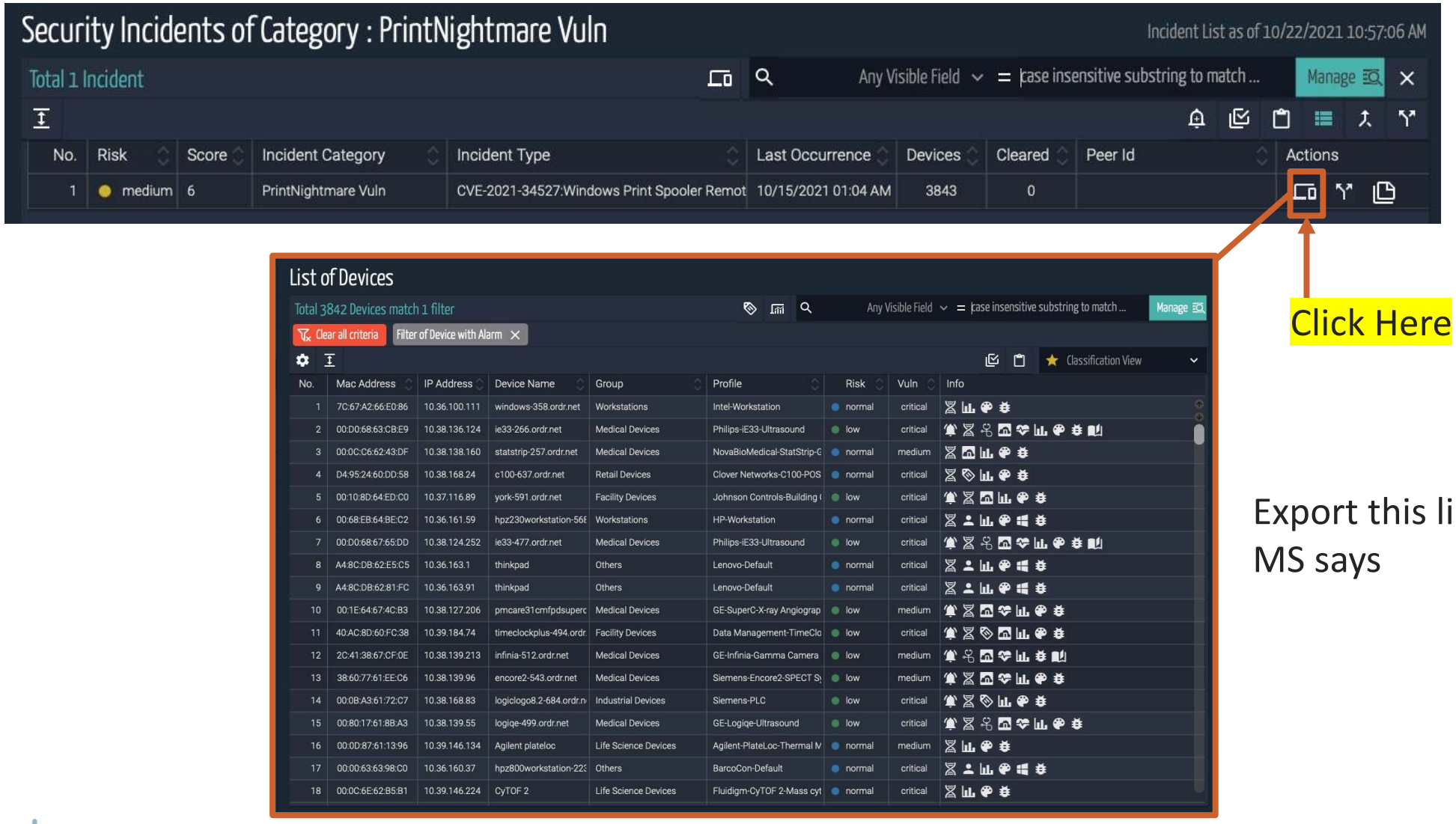
Active Exploit Observed

Slide 8 and beyond cover this

Click Here

Following slides cover this

Uncover all assets with a running vulnerable print spooler



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

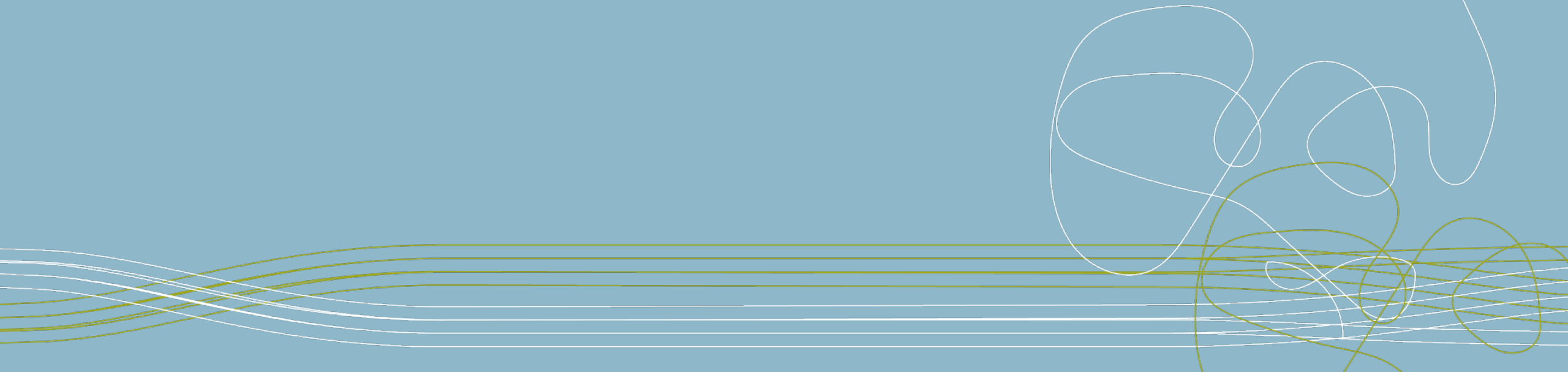
You can also configure the settings via Group Policy as follows: *Computer Configuration / Administrative Templates / Printers*

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

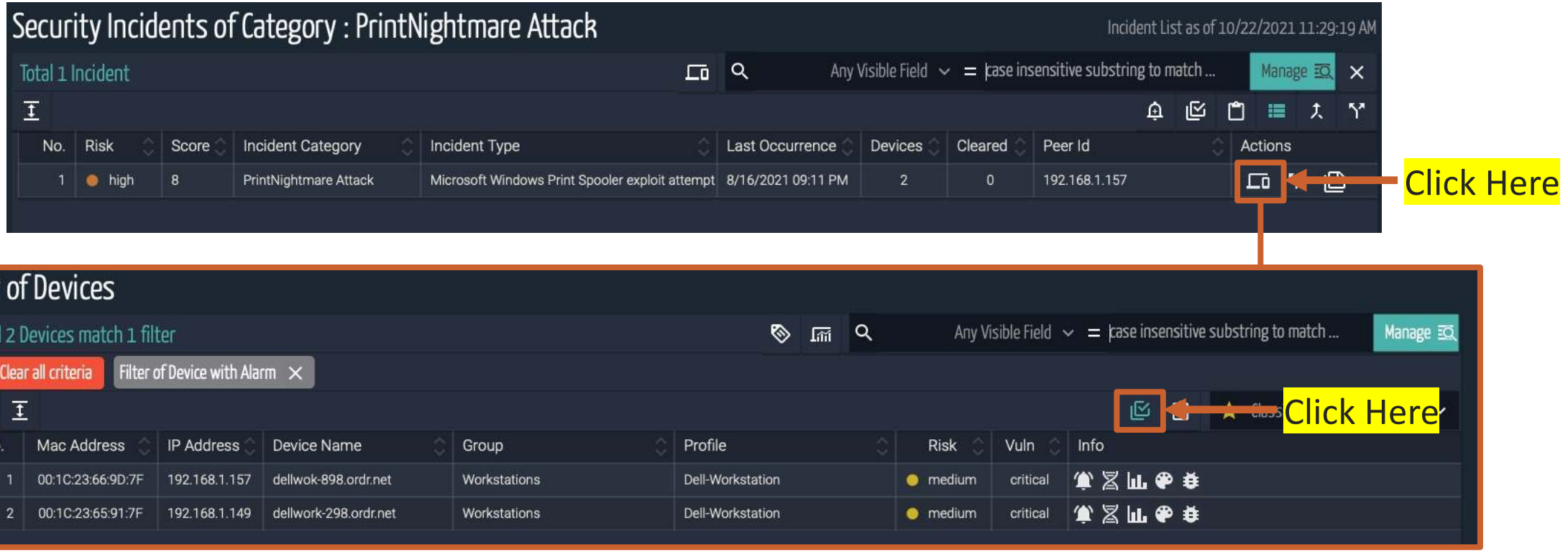


Locate Vulnerable Assets

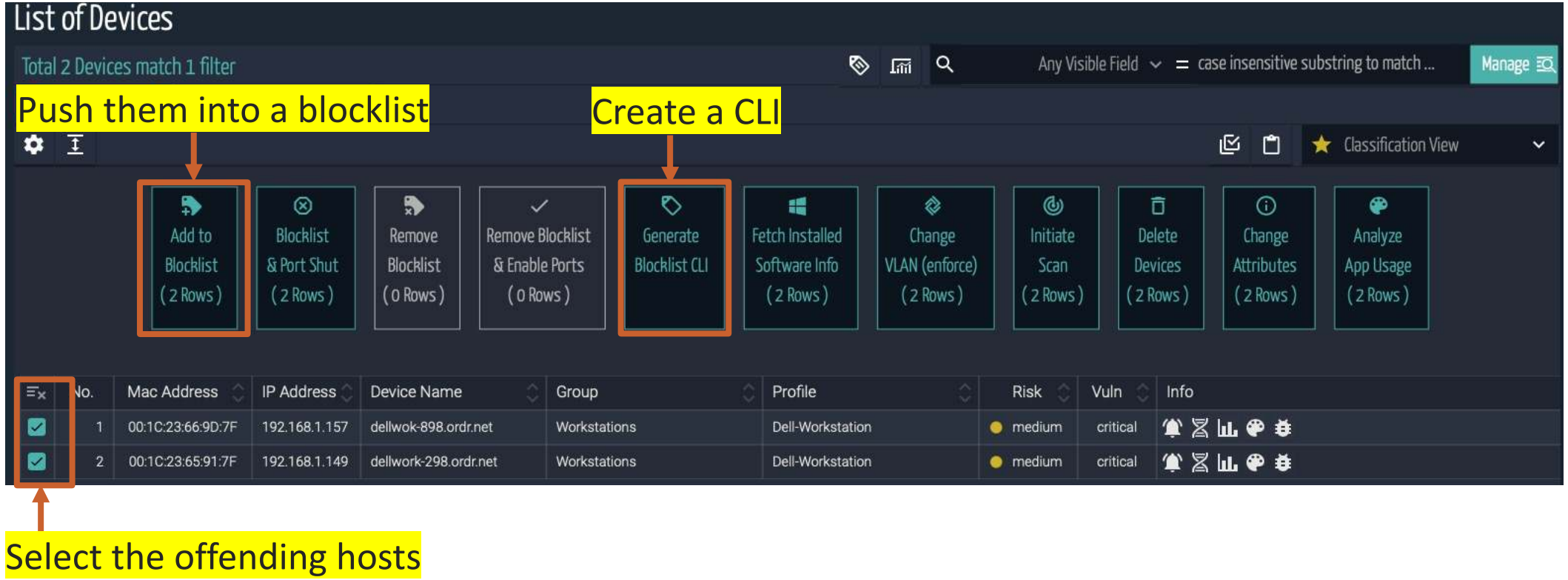
Click Here

Following slides cover this

Identify the offending systems



To mitigate the threat from these attacks



Copy paste this into your switches


ōrdr