Seguridad Cloud Native en tiempo de Coronavirus

DragonJAR® SECURITY CONFERENCE

qrco.de/preguntar

SI TIENES PREGUNTAS DURANTE LA CHARLA INGRESA AL CODIGO QR E INGRESA ESTE NUMERO

#22617

DragonJAR® SECURITY CONFERENCE

$Whoami

Antonio Juanilla

1. Autodidacta.
2. DevSecOps.
3. Co-Organizador de HackMadrid%27 y HackBarcelona%27.
4. Miembro del equipo de CTF FlagHunters.
5. Amante de la tecnología.
6. Firme defensor de la democratización de la tecnología para la mejora de la sociedad.

Redes
Twitter: @spectertj
Linkendin:
https://www.linkedin.com/in/spectertj
Github: spectertj
Instagram: spectertj

DragonJAR SECURITY CONFERENCE

Empecemos a hablar de:

Cloud

Cloud Computing

Conocida también como servicios en la nube, informática en la nube, nube de cómputo, nube de conceptos o simplemente «la nube», es un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.

Wikipedia asi lo dice ;D

Empecemos a hablar de:

Cloud native

Cloud Native

Cloud Native (nube nativa) es un patrón de arquitectura de software para desarrollar aplicaciones usando principios esenciales de cloud computing como la escalabilidad, elasticidad y agilidad.

Y también integrando conceptos como Continuous Delivery/integration/deployment o CI-CD, DevOps, microservicios, serverless, y contenedores.

Hablemos del tema para lo que vinimos xD

Cloud Native Security

Cloud Native Security

Se trata de la implementación de elementos y seguridad a lo anteriormente mencionado

Cloud Native Security

- Zero trust.
- Automatización de parcheos y manejo de parcheos.
- Automatización de la seguridad en el ciclo de desarrollo software(SSDLC).
- Visibilidad total y monitorización de amenazas.
- Seguridad como código.

Cloud Native Security

- DevSecOps.
- Escribir playbooks para automatizar respuestas de seguridad.
- Usar herramientas de Cloud Native, como SIEM en la nube.
- Application Gateway.
- WAF nativos.
- Cloud Workload Protection Platform(CWPP).

Diferencias entre Cloud y Datacenter

Datacenters(on premise)

1. Parcheo manual(no siempre) y mantenimiento
2. On premise(tu responsabilidad)
3. Maquinas físicas(hierro)
4. Corre en tu propia red(Intranet)
5. Se necesitan elementos para suplir de corriente a los equipos, energía de respaldo por si se va la electricidad, maquinas de respaldo(backups)
6. Se necesita personal operativo(Ops) disponible 24/7
7. Despliegue de aplicaciones en servidores especificos

VS

Cloud

1. Off premise (no es tu responsabilidad)
2. Auto escalado, no se necesita comprar nada en el progreso
3. Siempre basado en la disponibilidad del internet
4. Infrastructure as a Service(IaaS)
5. Las aplicaciones pueden estar en diferentes y cualquier servidor
6. El mantenimiento no es tu problema
7. Manejo centralizado y visibilidad
8. Disponibilidad geográfica o geográficamente distribuido

DragonJAR® SECURITY CONFERENCE

Seguridad entre Cloud y Datacenter

Datacenters(on premise)

1. Zona
2. Parcheo manual y mantenimiento de los parches
3. Seguridad física
4. Pocas veces es multiregion

VS

Cloud

1. Multiregion
2. Automatizicion de parches con herramientas nativas
3. No es necesaria la seguridad fisica
4. Todo se trabaja con software y tools cloud native

DragonJAR SECURITY CONFERENCE

Ahora cosas que pasan durante el corona virus

Coronavairus!!!! xD

CVE-2020-0796(RCE de SMBv3)

Una explotación efectiva de dicha vulnerabilidad, **permitiría al atacante la ejecución remota de código** en el servidor o cliente SMB. Para un ataque a un servidor, un usuario previamente autenticado podría enviar un paquete especialmente preparado. En el caso de un ataque a la parte cliente del protocolo, sería necesario convencer a un usuario, mediante *phishing* u otras técnicas similares, para que accediese a un servidor SMB malicioso. En ambos casos se produciría una ejecución de código en el equipo objetivo, permitiendo tomar el control del mismo.

Las plataformas afectadas son:

Windows 10 Version 1903

Windows 10 Version 1909

Windows Server 1903

Windows Server 1909

Coronavairus!!!! xD

Mitigación

Mientras salía el parche encontré en la pagina de “unaaldia” se podía ejecutar esto en la consola de **powershell** en las maquina:

Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" DisableCompression -Type DWORD -Value 1 -Force

Esto ha sido para deshabilitar la compresión en el protocolo **SMBv3** *en los servidores.*

Pero ojo también se recalca que esta configuración **no protege a los clientes**, para los cuales la única medida efectiva era bloquear en el firewall las conexiones salientes al puerto **445/TCP** fuera de la red local.

Además sabemos que eso da pereza y mas cuando hay muchas maquinas asi que.

Soluciones efectivas

Trabajo SecDevOps

- *Usar inventarios dinámicos.*
- *Usar soluciones cloud native por ejemplo ejemplo: Azure Automation State Configuration en el caso de usar azure*

Soluciones efectivas

Ansible

```
(inventory) [                @sdid1weu                inventory]$ cat windows.azure_rm.yml
plugin: azure_rm

auth_source: auto

plain_host_names: true

keyed_groups:
- prefix: ''
  key: 'tags["groups"]|default("no_groups_tag")'
  separator: ''
- prefix: location
  key: location
  seperator: ''
- prefix: rg
  key: resource_group
  seperator: ''
- prefix: os
  key: 'os_profile["system"]'
  seperator: ''

conditional_groups:
  aks_agent: "'aks-' in name"
```

DragonJAR® SECURITY CONFERENCE

Soluciones efectivas

Ansible

```
(inventory) [                e@sdid1weu          inventory]$ export AZURE_TENANT="35595a02-
(inventory) [                e@sdid1weu          inventory]$ export AZURE_SUBSCRIPTION_ID="02b3e34b-                                    72"
(inventory) [                @sdid1weu           inventory]$ export AZURE_CLIENT_ID=72be435b-
(inventory) [                e@sdid1weu          inventory]$ export AZURE_SECRET=2b8c9858-bd01-
(inventory) [                @sdid1weug          inventory]$
```

Soluciones efectivas

Ansible

DragonJAR® SECURITY CONFERENCE

Soluciones efectivas

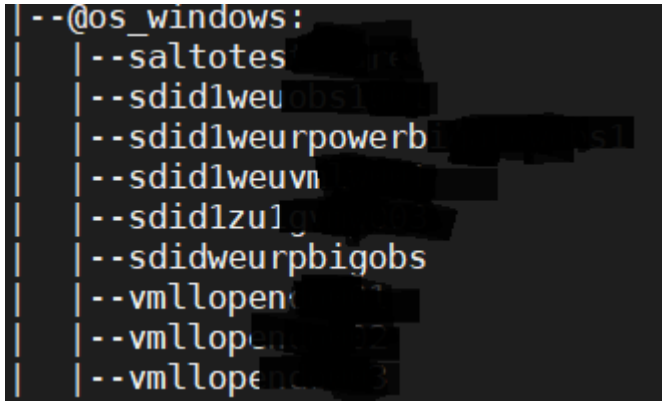
Ansible

```
(inventory) [a                @sdid1we          inventory]$ ansible-inventory -i windows.azure_rm.yml  --graph | grep -v "aks-agent"
@all:
  |--@Authority:
  |  |--sdid1weuvml
  |--@CPR_Frankfurt:
  |  |--sdid1weuvmllslscp
  |--@CPR_Spain:
  |  |--sdid1weuvmllslscp
  |--@EVM_Frankfurt:
  |  |--sdid1weuvmllsl
  |--@EVM_Spain:
  |  |--sdid1weuvmllslsc
  |--@Processing_Server:
  |  |--sdid1weunva-
  |--@Resolver:
  |  |--sdid1weuvml
  |  |--sdid1weuvml
  |  |--sdid1zu1gvml
  |  |--sdid1zu1gvml
  |--@SFTP_Server:
  |  |--sdid1weunva
  |--@agents:
  |  |--sdid1zu1a
  |--@aks_agent:
  |--@ansible:
  |  |--sdid1weug
  |--@besu:
  |  |--sdid1weuvmlls
  |  |--sdid1weuvmlls
  |  |--sdid1weuvmlls
  |  |--sdid1weuvmllsis
  |--@cdemos3:
  |  |--sdid1weuvmll
  |  |--sdid1weuvmll
  |  |--sdid1weuvmll
  |  |--sdid1weuvmll
  |  |--sdid1weuvml
  |  |--sdid1weuvm
  |  |--sdid1weuvmllb
  |  |--sdid1weuvmllsi
```

DragonJAR SECURITY CONFERENCE

Soluciones efectivas

Ansible



Soluciones efectivas

Un buen trabajo con excel

A	B	C	D	E	F	
VM	Fqdn	Resource Group	Location	Status	OsName	Ip
saltotestazure	saltotestazure	sdid1zu1rsgocpazucrit001	eastus	VM running	Windows 10 Pro	107.10
sdid1weuobs1001	sdid1weuobs1	sdid1weursgsdaobscrit001	westeurope	VM running	Windows Server 2016 Datacenter	180.49.
sdid1weurpowerbigatewobs1	sdid1weurpowerb	sdid1weursgsdaobscrit001	westeurope	VM running	Windows Server 2016 Datacenter	10.126.
sdid1weuvmlw001	sdid1weuvmlw001	sdid1weursgvtasstcrit001	westeurope	VM running	Windows Server 2012 R2 Datacenter	180.49.
sdidweurpbigobs	sdidweurpbigobs	sdid1weursgsdaobscrit001	westeurope	VM running	Windows Server 2019 Datacenter	180.49.
vmllopendo001	vmllopendo001	sdid1weursgopendocrit001	westeurope	VM running	Windows Server 2019 Datacenter	180.49.
vmllopendo002	vmllopendo002	sdid1weursgopendocrit001	westeurope	VM running	Windows Server 2019 Datacenter	180.49.
vmllopendo003	vmllopendo003	sdid1weursgopendocrit002	westeurope	VM running	Windows 10 Pro	180.49.

Soluciones efectivas

Un buen trabajo con excel

VM	Fqdn	Resource Group	Location	Status	OsName	Ip
lb01.ocp01.sdi.dev.weu.azure.pa	lb01.ocp01.sdi.dev.weu.azure.paas.cloudcenter.corp	sdid1weursgocpccccrit001	westeurope	VM running	redhat	180.49.4
lb01.ocp01.sdi.dev.zu1.azure.paa	lb01.ocp01.sdi.dev.zu1.azure.paas.cloudcenter.corp	sdid1zu1rsgocpccccrit001	eastus	VM running	redhat	107.104.
lb02.ocp01.sdi.dev.weu.azure.pa	lb02.ocp01.sdi.dev.weu.azure.paas.cloudcenter.corp	sdid1weursgocpccccrit001	westeurope	VM running	redhat	180.49.4
lb02.ocp01.sdi.dev.zu1.azure.paa	lb02.ocp01.sdi.dev.zu1.azure.paas.cloudcenter.corp	sdid1zu1rsgocpccccrit001	eastus	VM running	redhat	107.104.
master01.ocp01.sdi.dev.weu.azu	master01.ocp01.sdi.dev.weu.azure.paas.cloudcenter.corp	sdid1weursgocpccccrit001	westeurope	VM running	redhat	180.49.4
master01.ocp01.sdi.dev.zu1.azur	master01.ocp01.sdi.dev.zu1.azure.paas.cloudcenter.corp	sdid1zu1rsgocpccccrit001	eastus	VM running	redhat	107.104.
master02.ocp01.sdi.dev.weu.azu	master02.ocp01.sdi.dev.weu.azure.paas.cloudcenter.corp	sdid1weursgocpccccrit001	westeurope	VM running	redhat	180.49.4
master02.ocp01.sdi.dev.zu1.azur	master02.ocp01.sdi.dev.zu1.azure.paas.cloudcenter.corp	sdid1zu1rsgocpccccrit001	eastus	VM running	redhat	107.104.
master03.ocp01.sdi.dev.weu.azu	master03.ocp01.sdi.dev.weu.azure.paas.cloudcenter.corp	sdid1weursgocpccccrit001	westeurope	VM running	redhat	180.49.4
master03.ocp01.sdi.dev.zu1.azur	master03.ocp01.sdi.dev.zu1.azure.paas.cloudcenter.corp	sdid1zu1rsgocpccccrit001	eastus	VM running	redhat	107.104.
nodecs001.ocp01.sdi.dev.weu.az	nodecs001.ocp01.sdi.dev.weu.azure.paas.cloudcenter.cor	sdid1weursgocpccccrit001	westeurope	VM running	redhat	180.49.4
nodecs001.ocp01.sdi.dev.zu1.azu	nodecs001.ocp01.sdi.dev.zu1.azure.paas.cloudcenter.corp	sdid1zu1rsgocpccccrit001	eastus	VM running	redhat	107.104.
nodecs002.ocp01.sdi.dev.weu.az	nodecs002.ocp01.sdi.dev.weu.azure.paas.cloudcenter.cor	sdid1weursgocpccccrit001	westeurope	VM running	redhat	180.49.4
nodecs002.ocp01.sdi.dev.zu1.azu	nodecs002.ocp01.sdi.dev.zu1.azure.paas.cloudcenter.corp	sdid1zu1rsgocpccccrit001	eastus	VM running	redhat	107.104.
nodeirs01.ocp01.sdi.dev.weu.azu	nodeirs01.ocp01.sdi.dev.weu.azure.paas.cloudcenter.corp	sdid1weursgocpccccrit001	westeurope	VM running	redhat	180.49.4
nodeirs01.ocp01.sdi.dev.zu1.azur	nodeirs01.ocp01.sdi.dev.zu1.azure.paas.cloudcenter.corp	sdid1zu1rsgocpccccrit001	eastus	VM running	redhat	107.104.

Soluciones efectivas

Comandos para windows

```
PS C:\Users\x364777> az vm run-command invoke  --command-id RunPowerShellScript --name win-vm -g my-resource-group -scripts @script.ps1
```

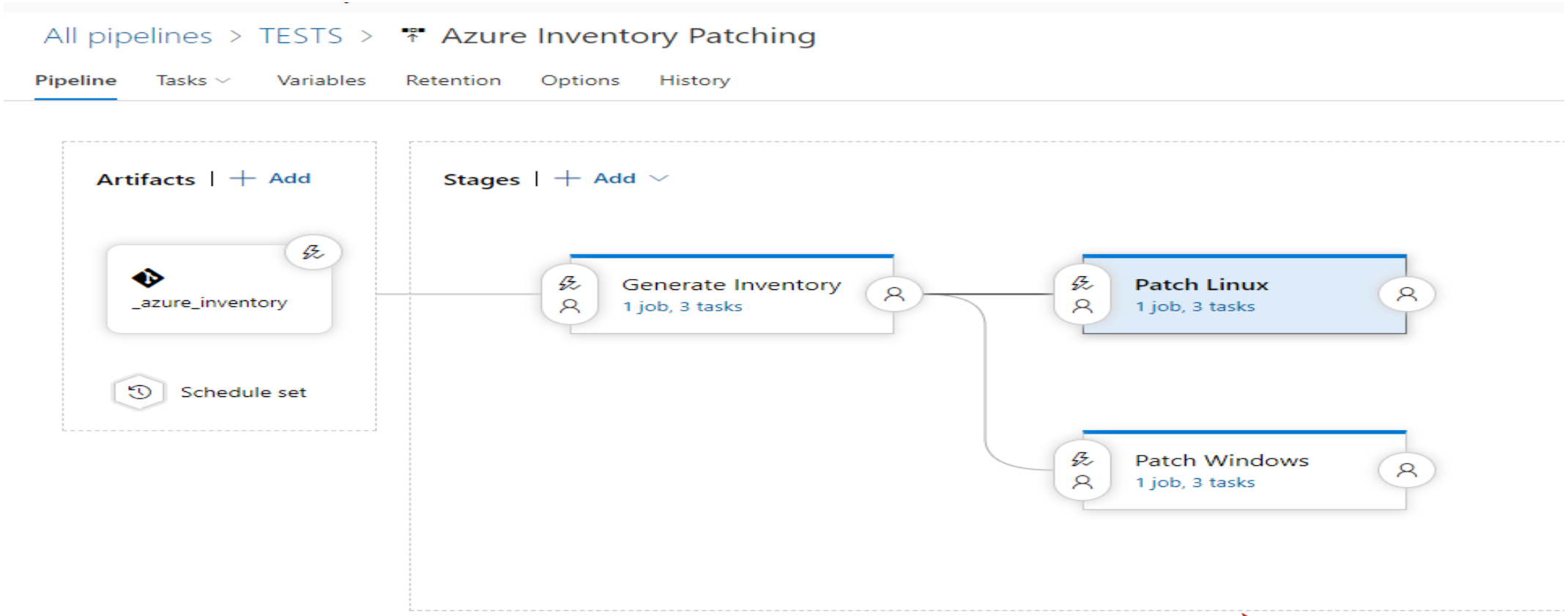
Soluciones efectivas

Comandos para linux

```
PS C:\Users\[redacted]> az vm run-command invoke -g sdid1weursgv[redacted] -n Docker --command-id RunShellScript --scripts "sudo apt-get update && sudo apt-get upgrade"
 - Running ..
```

Soluciones efectivas

Todo lo anterior automatizarlo



DragonJAR SECURITY CONFERENCE

qrco.de/preguntar

SI TIENES PREGUNTAS DURANTE LA CHARLA INGRESA AL CODIGO QR E INGRESA ESTE NUMERO

#22617

DragonJAR® SECURITY CONFERENCE