ṗ Ɛ + ŋ̈

2018 12

Ɛ ŋ Ʉ

.....ii
Ɛ ɳ ṕ 1
ṕ Ɛ + ɳ 3
ȁ Ɛ ɩ 3
1. AWS Ɛ ɳ 3
1.1 Windows Server 1809 EC2 AMI.....3
1.2 Amazon MQ PCI ISO 3
1.3 AWS Server Migration Service 4
1.4 EKS Kubernetes 1.11 4
1.5 AWS Storage Gateway 5

à Ɛ η ⅰ ـ 12
1. 12
1.1 پس ٭ٹجی ٔ 12
1.2 η ٭ 13
1.3 TSOC ʼP Gartner SIEM Ꞓ 14
1.4 Ɛ ˆ Ꞓ نجی 15
1.5 VenusEye η g 16
2. 16
2.1 EDR ˆ Ꞓ ′ 16
3. 17
3.1 Gartner ˅ η ⅰ 17
4. ˅ 18
4.1 ˅ η η à ẇ 18
5. 18
5.1 “ η +” 18
6. 19
6.1 EDR 19
7. 360.....19
7.1 360 η IDC 19
8. 20
9. Fortinet 20
9.1 Fortinet Ɛ η ˅ 20
10. Checkpoint 21
à ھ ب̈ ηـ 21
1. Rancherà ARM à à K8S 21
2. Kubernetes 1.13 21
3. Kubernetes η 22
4. Azure ھ ˅ ACS 24
ɾJ à η ٭٭ پس ب̈ 24
1. ʼE η ⅰ ê ε ˅ η ˆ
˜ Ì 24
2. 2018 η ẇ 24
3. iOS 12.1.1 ˇ ৯ à RCE 25
4. SNDBOX ʻ ɢ AI 25
5. CNNVD ٔ ɢ η 26
6. ˇ Windows 10 Windows Sandbox.....26

7. ê ÿˆ 2018˜ Ì̃ 26
8. ˙ ê ˙ Ì̃ 27
Ɛ à̃ ŋ à̃ Ɦ 27
1. 27
1.1 Artic Wolf Networks RootSecure 27
2. 27
2.1 Avanan 2500 B 27

Ɛ ŋ۔ ṗ

Ɛ ɨ ˘ AWS ˊ ˘ ɢ Windows Server 1809

EC2 AMI,Amazon MQ ˊ ,AWS Server Migration Service

˗ ʒ ˥ ʤ ,Amazon EKS Kubernetes 1.11

ˇ ˊ , ŋ Amazon DynamoDB ,Amazon EC2

˘ AWS Storage Gateway ˊ ˘

ʊ̈ Amazon MQ PCI ˇ ISO ’ VMware Ɛ

Stack-V Ɛ ˭ ’ Azure ʌ ꞁ ’ ʊ̈ ˘

ʌ Ɛ ’ Ɛ ˭

200% Â

Ɛ ˘ ‘ OpenStack ‘ Ɛ ’ EasyStack

ˆ ꞁ Ɛ ˘ à à ’ Ɛ

ˇ ŋ Ɛ ˘ ˭ Â

Ɛ ŋ ɨ ˘ ˇ ʤ

ʃ ŋ ’ ˘ ˬ ʃ g ˘

TSOC ‘P Gartner SIEM ꞁ ˘ Ɛ ˆ ꞁ

ʤ VenusEye- ŋ g ’

EDR ˆ ꞁ ’ ’ Gartner ˅

ŋ ɨ ’ ˅ ŋ ŋ à ʊ ’ “

ŋ + ” ’ EDR ’ 360 ŋ IDC

’ Fortinet Ɛ ŋ ˗ Â

ᶜᶜ ˘ Kubernetes1.13 ˘ ˜ Kubernetes

ṗ Ɛ + ŋ

à Ɛ ɩ

1. AWS Ɛ ŋ

1.1 ɢ Windows Server 1809 EC2 AMI

12 4 ˘ AWS ɢ Windows Server 1809 (LI) Amazon ˝E (AMI)˘ Ḃ ˘ Windows Server Â Windows Server ˘ Kubernetes ˘ ɢ ɢ ˘ ˛ Windows ą ᴰ Â

Amazon EC2 Windows Server 1809b< TJ EMWindows Server 2511 (1809) 11 41b< T.0BD

1.3 AWS Server Migration Service

12 6 AWS Server Migration Service (SMS) a

Amazon EC2 Â

Server Migration Service

Â

AWS Server Migration Service

2. VMWare Ɛ ŋ

2.1 VMware Ɛ Stack-V Ɛ

12 5 ˘ ŋ VMwarê NYSE: VMW˜ ŋ Ɛ

˥ ˡ Ɛ ˘ ĩ ˮ Ɛ ˥ —— Ɛ Stack-V

ˊ ą ˘ ĩ Â ˘ Ɛ ɢ IaaS

˘ VMware à à Ũ ˅ ẇ˘

˥ ˚˚ ˘ س à ɛ ˮ Ɛ ˮ

Â

Stack-V ⁝ Ɛ ˘ Ḃ ˅ à Ḃ

˥ ̀E Ɛ˘ Ɛ Ɛ ˘ Ɛ à à

à ˅ Ɛ ˥ ꞁ Â Ɛ ˥ ˡ ˘ Ɛ

ṗ ̀E Ɛ˚˚ س ˅ ˥ ʌ ŭ ẇ Â ˘ Ɛ

˥ ق˘ ʒ ˅ ˘ ʒ

ˏ à à ŋ Â

3. GOOGLE Ɛ

Â

4. Azure Ɛ

4.1 + =Azure UP

Azure Azure Â

Azure a

Â

2018 Azure

à /BIOS Â Azure

50 Â

Â

Azure Â

à IO CPU Â

Azure

Azure Â

Â Â Â

Â

5. Ɛ

5.1

CTO Ɛ Ɦ

Ɛ

Ɦ CEO Q Â Q

Â “ ” Ɦ

TOP10 2005

à Â

˘ ˛ Ɛ ˘ ꝏ

ꝏ ˇ Ɛ ⅃ Ɛ ⁼ Â ˘ ˛

˘ ˘ ŭ ˚˚ ꝏ ˙I Â ⅃ ˘ ˛

Ɛ EasyStack˘ ˛ ˛ OpenStack ˛ Ɛ˘

OpenStack ȁ Ceph Ɛ ˘ ꝏ ᵖ Â

2. Easystackᵤ

2.1 EasyStack ˆ Ꞓ Ɛ

OpenStack ˚˚ Ɛ ˘ ꝏ ECS Ɛ Ɛ˘

Ɛ Neutron AZ Ɛ Â

Ɛ ˘ ˇ ⅃ ⅃

ꝏ ˘ ˙E IT Ɛ ˘

ᵤ Ɛ Â

⅃ 2017 ˘ ᵤ ꝏ OpenStack ˚˚ Ɛ ˘

˚˚ OpenStack Ɛ ˙E Â ˘ ˚˚ Ɛ ˘

ꝏ Neutron Availability Zone(Neutron AZ) ˘ ρ̇

Neutron AZ Â ˘ ˘ ꝏ

Â

2.2 EasyStack ˆ Ꞓ Ɛ

EasyStack ECS Ɛ Ɛ Ɛ ˘

Ɛ Â

ρ̇ ť ˙E ȁ ˙E ˛

˛ ˘ ρ̇ ˛ ˙E Â ˘

˘ Ɛ Â

ŭ ˛ ˘ ꝏ Â ρ̇

˘ ˊ ť ˊ ˘ 2018 ˘ ˊ

1350 Â ť ˘ ˊ ˘ ρ̇ ˛ ˙E ——

˙E ˆ ˜ ˊ ˊ ȁ ˙E

˙E ȁ ˇ ˜ ˛ Â

˘ Ɛ ˘ Ɛ

˛ ˘ ̀E ˛ ˘ ̀E ﺟﺞ Â

2.3 EasyStack Ɛ

˘ ˇ ˛ Â ˘

˘ ﺟﺞ ˘ ˛

ˇ Â

“ 5G Ɛ ” ˘ Ɛ Ɛ ʒ ˘

ằ ˟ ˽ ʒ “ ” ṗ ˘ ڃ

ˡ g ＝ Â

˘ Ɛ ê Ɛ ằ ˘

Ì ʒ ˽ Â ˘ “˽ ằ ằ

ằ ằ ằ ” ˘ ERP ằ WMS ằ EMS ằ MES ˘ Ɛ

˘ ˟ ˟ ằ ˘ ˘ ˟

＝

˘ ɾ ˘ ˘

ʒ ˘ ˘ ɢ IOT ˇ ì

˘ ETSI MEC ‰ à ˋI à ˇ à ˀ

MEC Â

à Ɛ ŋ ˀ ‿

1.

1.1 پس ٹنجی ٔ

12 5 ˘ ˋE ˏ “ Ɛ

پس ٹنجی ٔ . ˝˘ ī̃

ٔ ˘ Ɛ پس ٹنجی ٔ Â à ˋE

à ◖ / Ɛ à ◖

Â

ή ε + ηᵃ

ɳ à ɳ à à à Web ŭ

Â

ˆ ADLab˜ 2015 ɳ ˘

ĩ ´ ɳ Â2016 ˘ Cloud DC Open

ˈE ˘ Ɛ ɳ = Â 2017 ˘ ɳ

Â ˘ ˆ ADLab˜ CNVD/CNNVD/CVE ʌ

1500 ˘ CNCERT ɳ

˘ Ɦ Â

1.3 TSOC ˈP Gartner SIEM Ɦ

˘ IT ج Gartner ɜ 2018 ê Magic Quadrant for Security Information and Event Management Ì ˘ TSOC ˈP Gartner SIEM

Ɦ ˘ ˅ Gartner SIEM ɳ ʌ ˏ

2018 ˘ Gartner ʒ SIEM ˚˚ س ˘ ɛ 200 ˙

ʒ 330 ˘ ˙ ɢ ŋ ɻ ˚˚ س ABC˜ AI à Big

Data à Cloud˜ à ŋ ŭ ɨ Â TSOC

˘ ɢ ɷ ˜ à ˆ UEBA˜ ˘

ʒ ŋ Â TSOC ṗ

2000 ˘ / ˘ ŋ à 2.0 à

GDPR à ISO27001 ‰ ˘ TSOC

ŋ Â

1.4 Ɛ ˆ ɨ ɷ

12 13 ˘ ˘ à ˘ ˘ ɻ ˈ

ŋ Ɛ ˜ Â ŋ Ɛ - Ɛ

˘ Ʒ Â

CERT ˘ 90% ŋ ŋ Â Ɛ

ŋ ŋ Ɛ Â ȳ ˘ ȣ à

à ŋ ˘ Ɛ ˘ ʌ ŋ ˘ Â

1.5 VenusEye- ŋ ȣ

ˆ VenusEye˜ Ꞁ à

à à ˇ ˘ ŋ

˘ ṗ “ ” Â

ˆ VenusEye˜ à à à

à ˘ ˇ ˇ ˇ Â ɢ

ˆ VenusEye˜ ˇ à à ˇ Ꞁ’

ˆ VenusEye˜ Portal ˇE ˇ ˘ ˘ ˇ SaaS API à à

‰ à ˆ TIC˜ à ˇ ˘ ˘ ’

à à à ˘ à ˘

Â

2.

2.1 EDR ˆ Ꞁ ’

“ ’ ”

ṗ ε + ŋ̈ 2018 12

ṗ ε + ŋ̈ 2018 12

“ ŋ + ” ˘ à Ɛ ŭ

ˡ ŋ ˩ = Â

ỉ Ɛ ŋ = ŋ Ꞁ ˅ ˘ ˡ Ɛ

ŋ ˩ ˘ ˆ ɾ à à ˅ ˘ ŋ ˩ ,

ˆ ɤ Ɛ ŋ ỉ˘ ŭ ˘

ŋ ˩ ˘ , ŋ ˩ ˭ ˊ ˘ ŋ ˩ ˊ ˘

˩ ف ˅ Â

6.

6.1 EDR

৲ EDR2.0.7 ˘ ® ŋ ŭ ɤ

˭ à ˭ ˎ ŋ ˺ ˺ ⁺ Â ® ŋ ŭ

˘ Ꞁ’ ṗ

˘ , ˝E˝ ŋ ,

à à à ŋ Ꞁ Â ˺ ˺ ⁺

˩ ⁺ à PC à à à ˺ ˺ à ⁺ ŋ Â ˎ

˺ ˺ à à à ˆ ŭ

à ŭ , ˜ ~ à

Ŭ’ à Web à ŋ à ŭ

˭ ˎ ˈ à ĩ à

Ꞁ ˭ ˭ ˅ ĩ Â

7. 360

7.1 360 ŋ IDC

11 30 ˘ ڂ ˋE IDC ɤ 2018 ŋ ˩ Â

˘ 360 ŋ ˘ ŋ

˺ ˺ ⁺ Â

˘ 360 ɤ Alpha à ——TIP à

—— à ˩ à Ɛ SaaS API ˺ ˺

ŋ ȝ ṗ ˏ ˆ à

à ˀ ˏ à ŋ ˚ ˚ ˜ ˘ 360 à NGSOC à ẇ à 360

à EDR à Ɛ ŋ à ŋ ŋ ˚ ˚ ˇ ˏ ȝ Ħ ˘

ˡ = ˘ ˊ ˋ ṗ Â ˘ 360

Ħ ˘ ŋ Â

IDC ˘ 360 ŋ ŋ ˏ ẇ Â ɢ

ṗ ŋ ˘ ˡ à ˹ à à

ŋ ˚ ˚ ŝ ŋ à à ẇ à ˜ ˘

ˀ ˘ ˝E˜ ˡ ŋ IP ˘

ŭ à Â ˚ ˚ ˘

IOC Â

8.

Â

9. Fortinet

9.1 Fortinet Ɛ ŋ ˏ

˘ ŋ ˀ ˹ ŋ = Fortinet

˘ Fortinet ˆ NGFW˜ ˋ Ɛ ŋ ˏ

Web Security Service WSS˜ ˘ = Fortinet

Security Fabric Â

Web Security Service WSS˜ ɢ ą Ɛ´ ŋ ˏ ˘

˘ ˘ Ɛ ˘ ˀ ˏ ˡ ŋ ˘

Â Fortinet FortiGate WSS ˘ ˚ ˚ ŝ

ˡ ŋ Ɛ ˋ = Âť

= Fortinet Security Fabric ˘ ˡ ˘

˘ ˹ ف Â ˘ Fortinet SD-WAN ε

ˆ TIPP˜ ˘ ˋI Web Security

Service ŋ ˏ Â ˘ ť ˹ Â

ˡ Ɛ à ˇ ŋ ˊ Â

10. Checkpoint

Â

à ᶜᵐ ŭ ŋ

1. Rancher à ARM à à K8S

2018 12 11 ˘ Kubernetes Rancher Labs Rancher

ˋE Arm ˘ ˇ Â˙ ˘

Rancher Kubernetes Engine (RKE) ŭ Rancher OS Arm Rancher ˍ ᶜᵐ

x86 ˘ ŭ ˇ Arm ˘

Arm ˇ x86 Kubernetes ˡ ɤ ŋ = Â ą

˘ Rancher ˡ Kubernetes = Â ˘ Rancher

ˇ Arm ˡ ɢ Kubernetes = Â

“ Arm Neoverse ᶜᵐ - Ꞿ ˡ

ɤ ẇ ”˘ Arm = Kevin Ryan ˋ “ Arm Rancher

ɤ ɪ Ɛ Neoverse Ꞿ Â ”

2. Kubernetes 1.13

Kubernetes 2018 ṗ -Kubernetes1.13 ˍ

ˆ Kubernetes ˘ ì Ŭ ح و ˆ

Â kubeadm

à Ŭ ˆ CSI˜ ŭ CoreDNS DNS Â

ŭ

Â ṗ ŭ alpha

ą Â

ï

9 alpha Â ع ɪ kubelet

Â

9 Kubelet ´Y Â ï

Kubelet ˇنجی نجی ˆ à CSI

CNI ˜ Kubelet Â

9 ⅄ Â ï ą Pod

⅄ Â

9 APIServer DryRun beta Â “ ”

ɪ kubectl apiserverˇ = bug Â

9 Kubectl Diff beta Â ï kubectl و

Â

9 ą ⅄ ⅄ Ŭ beta Â ï

⅄ ą ⅄ Ŭ ˆ ˜ Â

3. Kubernetes ŋ

Kubernetes ŋ Kubernetes˚˚ پس ŋ Kubernetes API Server Rancher Laba Darren Shepherd

CVE-2018-1002105 Â

ṗ Ɛ + ŋ‿ 2018 12 Ɛ ŋ Ɦ

ṗ Ɛ + ŋ̈ 2018 12

ˋE ˜ Ɛ ŋ ẇ ˇ ˥ ŋ Ɦ Â

ẗ ˇ Ɦ ȁ Ɛ Ȧ ŋ ˜

ŋ 3397 ˇ IP ȁ 653 ˇ ȁ

ȁ 2611 ˇ ŋ ŋ 4.8 ˇ ȁ

ȁ ŋ Ɦ 127 ˇ ẗ ŋ 1 Â

ˇ ȣ ˇ ȁ

˭ Âŭ ˇ ˭ ŋ ˇ

Â

3. iOS 12.1.1 ˇ ȣ ȁ RCE

Apple ȣ ẗ ˚ ˚ ˇ iCloud ȁSafari ȁTunes ȁmacOS Mojave ȁHigh Sierra ȁ Sierra ȁ iOS 2.1.2 ȁ tvOS 12.1.1 ŭ iOS 12.1.1 Â ȣ ŋ ˇ ȁ ˇ Â ˇ ˚ ˚ ˇ

Â

ˇ iOS 12.1.1 ȣ ID ą ˇ ȣ “ ” ą

ˇ ˇ = ȣ “

” iCloud Â

4. SNDBOX ˈ ɢ AI

Blackhat Europe ȣ SNDBOX ˥ ˇ ˥

˥ ˇ ˇ˭ Â

ˊ ˇ ȁ Â ą ẗ ˇ

ˈ ˇ SNDBOX ˪ Â SNDBOX ˩

Â ˇ SNDBOX ˇ ŭ API ȁ ˊY

ˇ ŭ WMI Â

“ ” ˫ ÂAI

ẗ ȣ ˇ ą Â

SNDBOX Â ˫ ˇ HTTP POST

Â SNDBOX JSON Â ˘ SNDBOX ˚ ¬ ˚ ¬ ť Â

5. CNNVD ˚ ɢ ŋ

˘ ʒ ŋ ̀E ˘ Microsoft Internet Explorer ŋ ˆ CNNVD-201812-458 ȁCVE-2018-8619˜ ȁMicrosoft Excel ŋ ˆ CNNVD-201812-466 ȁ CVE-2018-8597˜ Â ˊ Â ˚ ˚ ˘ ف Â ˘ ˘ ŭ ف˘ Â

6. ˘ Windows 10 Windows Sandbox

˘ Windows 10 ʒ Windows Sandbox˘ ŋ Â Windows Sandbox ˘ ˘ ف Â Windows Sandbox Sandbox ˘ Sandbox ˚ ˘

[redacted]

˘ BIOS ˊ ˆ ح˜ ˘ Windows Features Windows Sandbox˘ Windows Sandbox Â

7.

ằ ằ ’ ŋ ˘ “ 1+3”

˘ ˅ ằ ằ ŋ Â

8. ˹ ê ˺ Ỉ