+

2018 12

.....ii

..... 1

\+ *..... 3*

..... 3

1.

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

.....12

1.
1.1 12
1.2 13
1.3 TSOC Gartner SIEM 14
1.4 15
1.5 VenusEye- 16
2.
2.1 EDR 16
3.
3.1 Gartner 17
4.
4.1 18
5.
5.1 “ +” 18
6.
6.1 EDR 19
7.
7.1 360 IDC 19
8.
9.
9.1 Fortinet 20
10.

.....21

.....24

.....27

1.1 Artic Wolf Networks RootSecure 27

2.1 Avanan 2500 B 27

AWS Windows Server 1809

EC2 AMI,Amazon MQ ,AWS Server Migration Service

,Amazon EKS Kubernetes 1.11

, Amazon DynamoDB ,Amazon EC2

AWS Storage Gateway

Amazon MQ PCI ISO VMware

Stack-V Azure

200%

OpenStack EasyStack

TSOC Gartner SIEM

VenusEye-

EDR Gartner

“

+ ” EDR 360 IDC

Fortinet

Kubernetes1.13 Kubernetes

+

1. AWS

1.1 Windows Server 1809 EC2 AMI

12 4 AWS Windows Server 1809 (LI)
Amazon (AMI) Windows Server
Windows Server Kubernetes
Windows
Amazon EC2 Windows Server 1809 AWS
Windows Server (LI)
Windows Server 1809 AMI AWS Amazon EC2
Windows Server 1809 AMI Windows

1.2 Amazon MQ PCI ISO

12 5 Amazon MQ PCI ISO
Amazon MQ Apache ActiveMQ

Amazon MQ PCI DSS
AWS Artifact PCI AWS PCI

Amazon MQ ISO 9001 27001 27017

1.3 **AWS Server Migration Service**

12 6 AWS Server Migration Service (SMS)

Amazon EC2

Server Migration Service

AWS Server Migration Service Sgeas(er)9.nfairv È c À,•6})îÌ×)à]ðë1 0+E÷ Sr67r6847(

2．VMWare

2.1 VMware Stack-V

12 5 VMware NYSE: VMW

—— Stack-V

IaaS

VMware

Stack-V

3．GOOGLE

4. Azure

4.1 + =Azure UP

Azure Azure

Azure

2018 Azure

/BIOS Azure

50

IO CPU

Azure

“ ”

Azure

5.

5.1

CTO

CEO

“ ”

TOP10 2005

EasyStack OpenStack

OpenStack Ceph

2．Easystack

2.1 **EasyStack**

OpenStack ECS

Neutron AZ

IT

2017 OpenStack

OpenStack

Neutron Availability Zone(Neutron AZ)

Neutron AZ

2.2 **EasyStack**

EasyStack ECS

2018

1350 ——

2.3 EasyStack

“ 5G ”

“ ”

“

” ERP WMS EMS MES

IOT

ETSI MEC

MEC

1.

1.1

12 5 “

. ”

/

+

Web

ADLab 2015

2016 Cloud DC Open

2017

ADLab CNVD/CNNVD/CVE

1500 CNCERT

1.3 TSOC Gartner SIEM

IT Gartner 2018 Magic Quadrant for Security Information and Event Management TSOC Gartner SIEM

Gartner SIEM

2018 Gartner SIEM 200
330 ABC AI Big
Data Cloud TSOC
UEBA
TSOC
2000 / 2.0
GDPR ISO27001 TSOC

1.4

12 13

-

CERT 90%

1.5 **VenusEye-**

VenusEye

“ ”

VenusEye

VenusEye

VenusEye Portal SaaS API

TIC

2.

2.1 **EDR**

“ ”

+ 2018 12

+ 2018 12

“ + ”

6.

6.1 **EDR**

EDR2.0.7 ®

®

PC

Web

7. 360

7.1 **360** **IDC**

11 30 IDC 2018

360

360 Alpha ——TIP

—— SaaS API

360 NGSOC 360

EDR

360

IDC 360

IP

IOC

8.

9. Fortinet

9.1 **Fortinet**

Fortinet

Fortinet NGFW

Web Security Service WSS Fortinet

Security Fabric

Web Security Service WSS

Fortinet FortiGate WSS

Fortinet Security Fabric

Fortinet SD-WAN

TIPP Web Security

Service

10. Checkpoint

1. Rancher ARM K8S

2018 12 11 Kubernetes Rancher Labs Rancher

Arm

Rancher Kubernetes Engine (RKE) Rancher OS Arm Rancher

x86 Arm

Arm x86 Kubernetes

Rancher Kubernetes Rancher

Arm Kubernetes

“ Arm Neoverse

” Arm Kevin Ryan “ Arm Rancher

Neoverse ”

2. Kubernetes 1.13

Kubernetes 2018 -Kubernetes1.13

Kubernetes

kubeadm

CSI CoreDNS DNS

alpha

9 alpha kubelet

9 Kubelet

Kubelet CSI

CNI Kubelet

9 Pod

9 APIServer DryRun beta “ ”

kubectl apiserver bug

9 Kubectl Diff beta kubectl

9 beta

3. Kubernetes

Kubernetes Kubernetes Kubernetes API

Server Rancher Laba Darren Shepherd

CVE-2018-1002105

+ 2018 12

+ 2018 12

3397 IP 653

2611 4.8

127 1

3. iOS 12.1.1 RCE

Apple iCloud Safari iTunes macOS Mojave High Sierra Sierra iOS 2.1.2 tvOS 12.1.1 iOS 12.1.1

iOS 12.1.1 ID “ ”

“

” iCloud

4. SNDBOX AI

Blackhat Europe SNDBOX

SNDBOX SNDBOX

SNDBOX API

WMI

“ ” AI

SNDBOX HTTP POST

SNDBOX JSON

SNDBOX

5. CNNVD

Microsoft Internet Explorer

CNNVD-201812-458 CVE-2018-8619 Microsoft Excel CNNVD-201812-466

CVE-2018-8597

6. Windows 10 Windows Sandbox

Windows 10 Windows

Sandbox Windows Sandbox

Windows

Sandbox Sandbox Sandbox



BIOS Windows

Features Windows Sandbox Windows Sandbox

7.

“ 1+3 ”

8.