

+

2019

2

+

1.	AWS		3
1.1	AWS Batch	Amazon EC2 A1	3
1.2	Amazon ECS	GPU EC2	3
1.3	AWS Site-to-Site VPN	IKEv2	4
1.4	Amazon GuardDuty		4
1.5	AWS Well-Architected Tool		4
1.6	AWS IoT Device Defender		5
1.7	AWS Elemental MediaConvert		5
2.	VMWare		6
2.1	VMware	AetherPal.....	6
3.	GOOGLE		6
3.1	Google	Alooma -	6
3.2		Ontology(ONT)	6
4.	Azure		7
5.			7
5.1		200	7
6.			7
6.1		“ ” PC	7
6.2			8
7.			9
7.1			9
1.	Openstack		9
2.	Easystack		9
2.1	EasyStack	Kyligence	9
3.	99CLOUD		9
1.			10

1.1		2019	..10
1.2		Adobe ColdFusion	10
1.3		“ ”	11
1.4			13
2.			14
2.1	EDR	IT168	14
3.			15
3.1		“2019 ”	15
4.			16
4.1		40	16
5.			16
5.1	Cloud-in-a-box	“2019 ”	16
6.			17
6.1			17
7.	360		17
7.1	360	2019.1	17
8.			18
9.	Fortinet		18
9.1	Fortinet	SD-WAN	18
10.	Checkpoint		19
1.	RunC		19
2.	Docker	Windows Server 2019	20
3.	Linkerd 2.2		20
1.	CNNVD		21
2.	M365		21
3.			22
4.			22
5.		GitHub	22
6.	GCA		23
7.	WinRAR		23
1.			24
1.1	Symantec	Luminate Security	24

	AWS		AWS Batch	Amazon
EC2 A1	Amazon ECS	GPU	EC2	
AWS Site-to-Site VPN		IKEv2	AWS Well-Architected Tool	
		AWS Elemental MediaConvert		
	Amazon GuardDuty			AWS IoT
Device Defender			VMware	
	AetherPal	Google	Alooma-	
	Ontology(ONT)			200
				PC
	EasyStack	Kyligence		
2019			Adobe ColdFusion	
			EDR	IT168
				2019
		40		
Cloud-in-a-box	2019			
			360	
		2019.1		Fortinet

SD-WAN

RunC

root

Docker

Windows Server 2019 Linkerd 2.2

linksd pod

1.0

App

Microsoft 365

Adobe

Experience Manager

NSA

GHIDRA

USB-C

USB

1

3

Luminate

Illumio

6500

E

vArmour

4400

E

Perimeterx

4300

C

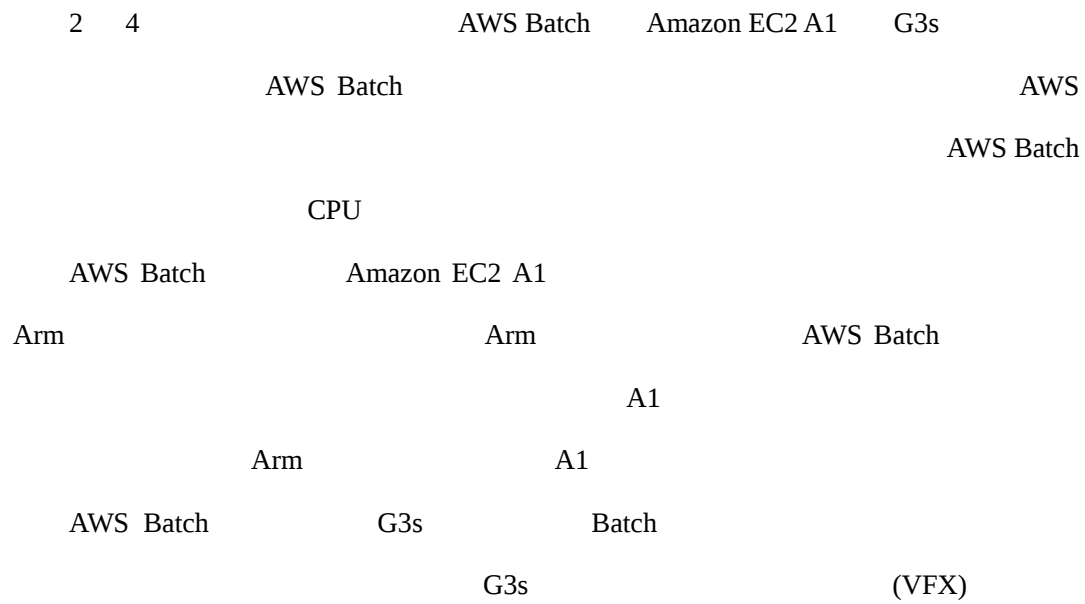
2019 2 27

+

1. AWS

1.1 AWS Batch

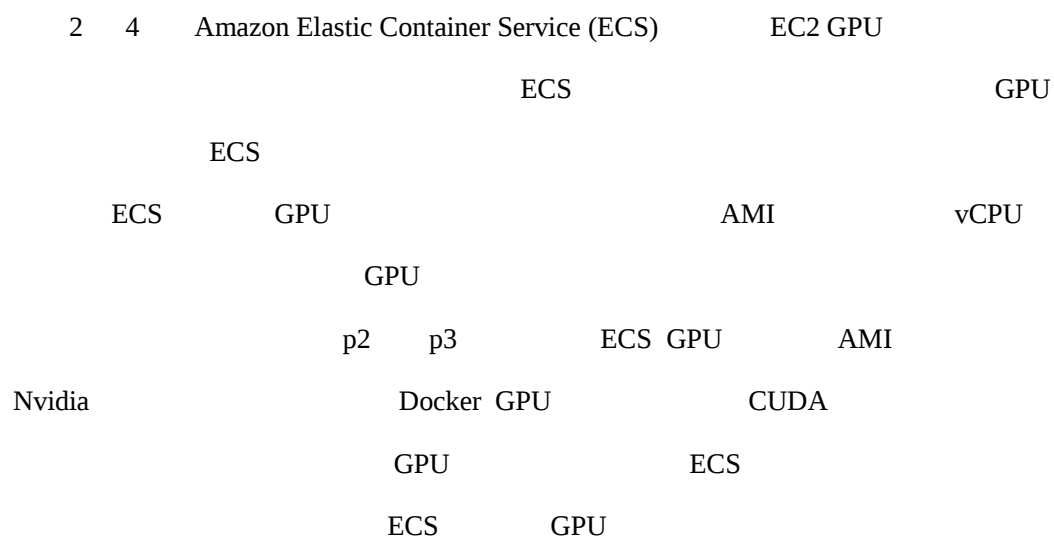
Amazon EC2 A1



1.2 Amazon ECS

GPU

EC2



1.3 AWS Site-to-Site VPN

IKEv2

2	6	AWS Site-to-Site VPN			Internet Key Exchange
2 (IKEv2)		VPN	IKEv2	IKEv1	VPN
			VPN		
				VPN	
		IKE		AWS	
		AWS Classic VPN			

1.4 Amazon GuardDuty

AWS

AWS

AWS

AWS

Well-Architected

1.6 AWS IoT Device Defender

2 19 AWS IoT Device Defender

AWS IoT Device Defender

AWS IoT

Core

90

AWS IoT Device Defender

AWS

1.7 AWS Elemental MediaConvert

2 21 AWS Elemental MediaConvert

MediaConvert

SCTE-35

MediaConvert

(ESAM) XML

VOD

AWS Elemental MediaConvert

2. VMWare

2.1 VMware

AetherPal

2 18 VMware

AetherPal

AetherPal

VMware

Shankar Iyer

VMware

Workspace One

Workspace One

AetherPal

Remote Support

AetherPal

4500

Remote Support

POS

3. GOOGLE

3.1 Google

Alooma -

2 20

2 19

Google

Alooma

Alooma 2013

API

4

50

Google

Google

3.2

Ontology(ONT)

2 25

Ontology (ONT)

ont_dev_Platform

Ontology

2018 12

Azure

Ontology

4. **Azure**

5.

5.1 **200**

1 30

2019

Q3

2018

213.6

200

111.7

4

20

40%

500

80%

678

AI

5

50%

PC

GDC

i7-8709G

PC Farm

/ / /

AR/VR

i7-8709G

MediaSDK

1080p /50~60 FPS

6.2

2 26

30 50

100

1000

7.

7.1

2 20

AI

1.

1.1

2019



2 3

2019

2000

1.2

Adobe ColdFusion

2019

2

12

Adobe

Adobe ColdFusion

APSB19-10

ADLab

CVE-2019-7091

ColdFusion 11 Update 15

ColdFusion 2016 Update 7

ColdFusion 2018 Update 1

V6.0 2019 2 15

6070

607000204

<https://www.venustech.com.cn/article/type/1/146.html>

gateway-config.xml

JavaBeanAdapter

APSB19-10

<https://helpx.adobe.com/security/products/coldfusion/apsb19-10.html>

Adobe ColdFusion

RCE

https://mp.weixin.qq.com/s/8_D8xwXwgETItMmJRgp6XQ

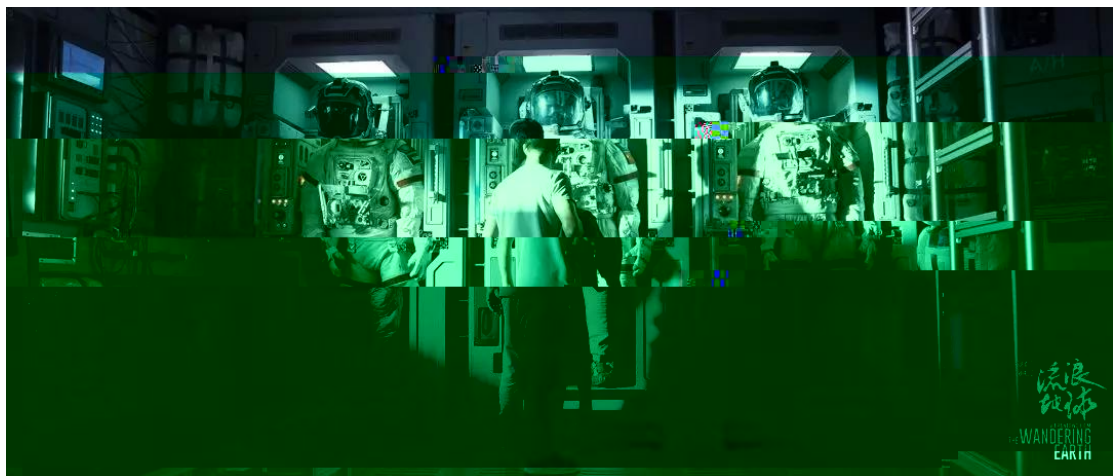
1.3

CSA SOC SA AEM
 CVS NBA BSM LAS
 Detector

SIEM SOC BDSA
 PSP UTT

AN ML
 UEBA AA Visualization
 Tran-Matrix Opt. KG QD TH

PAC PBC PCC PSC SRC



1.4

2019

5406

3363

2043



2012

2.

2.1 **EDR IT168**

EDR

IT

IT168

2018

1

2017 5

2018

2018

2

Web

2.0

EDR

EDR

1

EDR

2

EDR

EDR

EDR

3

EDR

/

Web

IOC

2.0

\

\

EDR

EPP

EDR

EDR

20W+

3.

3.1

2019

+

2019

02

IPv6

X10800

4.

4.1

40

GSMA

Verizon 40

2022

60% GDP

5G

50

2025

60

GSMA

5G

5.

5.1

Cloud-in-a-box

2019

Cloud-in-a-box

2019

6.

6.1

2018

3

7. 360

7.1

	+	2019	02		
2018	12	4.3%		12	4.3%

NGFW IPS
Fortinet Nirav Shah Fortinet
SD-WAN SD-WAN Fortinet
Fortinet NGFW CPE
SD-WAN
Fortinet 2018 7 SD-WAN
WAN SD-WAN
VM Fortinet SD-WAN
WAN

10. Checkpoint

1. RunC

RunC root
RunC Docker CRI-O containerd Kubernetes
CLI
runC runC
root
CVE-2019-5736 Adam Iwaniuk Borys Poplawski runC
runC
root
docker exec
root
runC LXC
docker runc Debian Ubuntu

Docker v18.06.2 v18.09.2

2. Docker Windows Server 2019

Docker	Docker Enterprise	Windows Server 2019
Long Term Servicing Channel	LTSC	Server 1809
SAC	Windows Server 2019	SAC
		LTSC
	IP	

3. Linkerd 2.2

2	12	Linkerd 2.2	
			CLI
endpoints	Linkerd		logs
		CNI	
NET_ADMIN			
			2.1
	Linkerd		
		Linkerd 2.2	
isRetryable		timeout	
	retryBudget		
			Kubernetes
	Linkerd		pods
	pods		

1. CNNVD

Microsoft Office

CNNVD-201902-356 CVE-2019-0540

Windows

CNNVD-201902-405 CVE-2019-0590

Microsoft SharePoint

CNNVD-201902-349 CVE-2019-0594

2. M365

Zimperium

M365

100

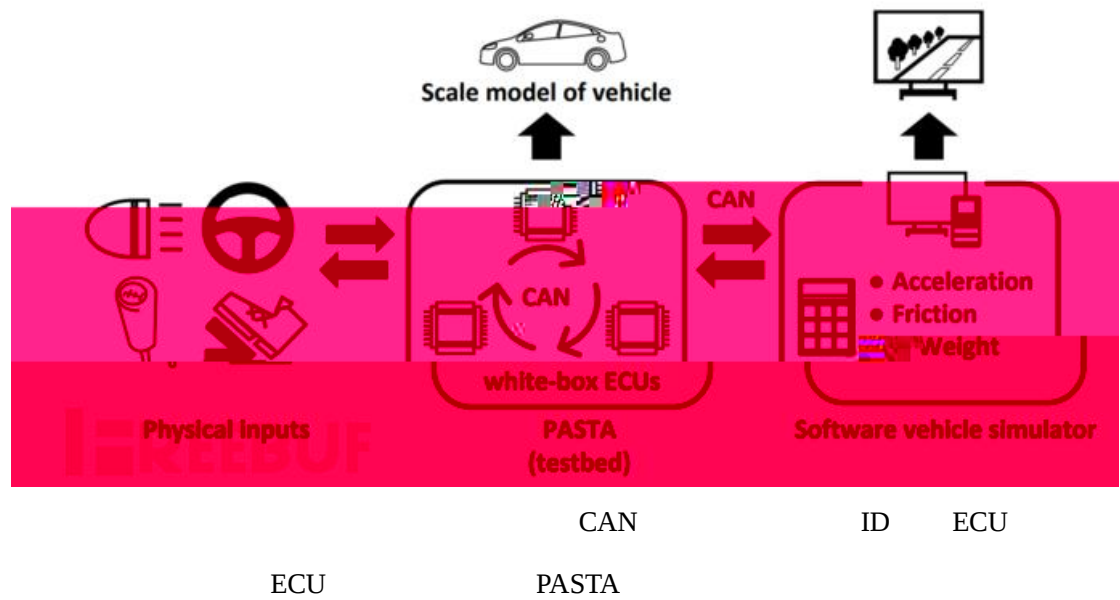
M365

APP

PASTA

Takuya

Yoshida Tsuyoshi Toyama



6. GCA

GCA

GCA

Alexander Niejelow

7. WinRAR

2019	2	20	checkpoint	WinRAR	ace	
DLL				2019	2	22
			360			WinRAR
CVE-2018-20250			ACE			
ModifiedVersion3.rar				WinRAR		

1.

1.1 Symantec Luminate Security

2 12 Symantec Luminate Security

Luminate

2.

2.1 vArmour 4400 E

2 6 vArmour AllegisCyber NightDragon Security 4400 E

vArmour

2.2 Illumio 6500 E

2 7 Illumio J.P. Morgan Asset Management 6500 E

Illumio

Illumio

2.3 PerimeterX 4300 C

2 11 PerimeterX PerimeterX 4 4300 D

Perimeterx

Perimeterx BOT

PX Bot Defender

