

超級攤位 L09

遊戲攤位 P01 & P02

徵才攤位 CT08



The Fast and The Rigged
急速賽道之神秘訊號



Cybercans 2
紅色動員令

互動/諮詢
送好禮



奧義智慧展區全攻略

4F 攤位號碼

L09

9/20 (二)

- 11:10-11:40
奧義第三部曲——
企業資安設計之路 (Live 直播)
- 12:20-12:40
MDR 實務分享—以金融業為例
- 13:40-14:00
AD 安全—可視化的入侵與攻擊
路徑模擬服務
- 15:20-15:40
車載安全夥伴分享：鴻海研究院

9/21 (三)

- 12:00-12:20
紅隊演練夥伴分享：戴夫寇爾
- 12:40-13:00
MDR 實務分享—
以高科技製造業為例
- 13:40-14:00
藍隊演練夥伴分享：菱鏡
- 15:20-15:40
AD 安全—可視化的入侵與
攻擊路徑模擬服務

9/22 (四)

- 11:00-11:20
FinSec 夥伴分享：勤業眾信
- 12:20-13:20
《Cybercans 2：紅色動員令》
桌遊名人賽
- 14:20-14:40
MDR 實務分享—以金融業為例

從地端威脅演進到雲端安全

我們是

> Boik Su

- > Senior Cyber Security Researcher
- > 專注於雲端安全、AD 安全、網頁安全及威脅狩獵
- > HITCON, ROOTCON, HackerOne

> Dange Lin

- > Senior Cyber Security Researcher
- > 專注於汽車安全、雲端安全、機器學習與情資分析等領域
- > HITCON, MOPCON, CYBERSEC

大綱

- > 雲端安全摘要及指導
- > 案例分享
- > 結論



雲端安全摘要及指導

領域上有的

- > Official Guideline
- > Center for Internet Security (CIS)
 - > AWS, GCP, Azure, Oracle Cloud, etc
- > DisruptOps, an innovator in Cloud Security
 - > Top 10 Cloud Attack Killchains
- > Community
 - > Cloud Security Orienteering, AWS Security Ramp-Up Guide



[Privacy](#) [Careers](#) [Disclosure Policy](#) [Technical Advisories](#) [Public Reports](#) [2021 Research Report](#)

[Contact Us](#)

The Extended AWS Security Ramp-Up Guide

Rami McCarthy Cloud & Containerization, North American Research, Research, Tutorial/Study Guide
 April 24, 2020 8 Minutes

On November 25th, AWS released the [Ramp-Up Learning Guide for AWS Cloud Security, Governance, and Compliance](#). The Security Ramp-Up is a curated list of educational AWS resources. The goal is “to teach in-demand cloud skills and real-world knowledge that you can rely on to keep up with cloud security, governance, and compliance developments and grow your career.” The Ramp-Up is an excellent document, that describes a logical progression in first-party training resources, from the official [Overview of Amazon Web Services](#) through the [AWS Certified Specialty – Security exam](#), and beyond.

Principles

- Breadth, then Depth
- Anomaly Detection
- Inside Out & Outside In

Archeology

- What do you own & where?
- Environments → Workloads → Resources

ion

- Identity Perimeter
- Network Perimeter
- Apps/Services

anning

- Driving Org Changes
- Align to Maturity Curves

BACK KILLCHAINS

Service API

Account Struct

Trust

3rd

Cloud Custodian



To put it simply

雲端資安體質強化流程



Discovery - 盤點資產

- > 雲端使得企業邊界變得更模糊
- > 雲端環境下，admin 根本不知道有哪些資產
 - > RD 用自己的帳號開發
 - > 開帳號給外部合作夥伴
- > 這些資產必須被集中管理與維護
- > 定義出高敏感資產



盤點資產技巧

- > 盤點已知帳戶
- > 詢問 Technical Account Manager，有無與公司網域關連帳號
- > 搜尋公司 email，有無註冊雲端服務的信
- > 搜尋 network logs，有無訪問雲端服務中控臺紀錄
- > 詢問財務團隊，有無雲端服務支付紀錄
- > 公開詢問公司員工
- > 找出與現有帳戶關聯的帳戶



https://summitroute.com/blog/2018/06/18/how_to_inventory_aws_accounts/
<https://tldrsec.com/blog/cloud-security-orienteeing/>

工具

- > aws-inventory
- > Steampipe
- > Prowler
- > ScoutSuite

評估與量化

Discovery

Assessment

Prioritization

決策與執行

Remediation

量測與改進

Maturity

Red Team

Assessment – 評估風險

- > 找出雲端中的錯誤設定
- > 雲端三大問題面向
 - > Identity Perimeter
 - > Network Perimeter
 - > Hosted Applications/Services
- > 用工具、Guideline、Checklist 評估
 - > CIS benchmark
 - > Maturity Roadmap by Scott Piper



CIS benchmark - AWS

1.4 Ensure no 'root' user account access key exists (Automated)

Audit:

Perform the following to determine if the 'root' user account has access keys:

From Console:

1. Login to the AWS Management Console
2. Click `Services`
3. Click `IAM`
4. Click on `Credential Report`
5. This will download a `.csv` file which contains credential usage for all IAM users within an AWS Account - open this file
6. For the `<root_account>` user, ensure the `access_key_1_active` and `access_key_2_active` fields are set to `FALSE`.

From Command Line:

Run the following command:

```
aws iam get-account-summary | grep "AccountAccessKeysPresent"
```

If no 'root' access keys exist the output will show "AccountAccessKeysPresent": 0,.

If the output shows a "1" than 'root' keys exist, refer to the remediation procedure below.

Prioritization – 排序威脅

- > 去年單位出過的資安事件
- > 目前公司內外的潛在威脅
- > 最近同業出現的資安事件
- > 老闆在意的資安新聞
- > 保護公司定義的高敏感資產
- > 年度威脅排行榜
 - > Cloud Security Alliance
 - > DisruptOps

評估與量化

Discovery

Assessment

Prioritization

決策與執行












Remediation

量測與改進

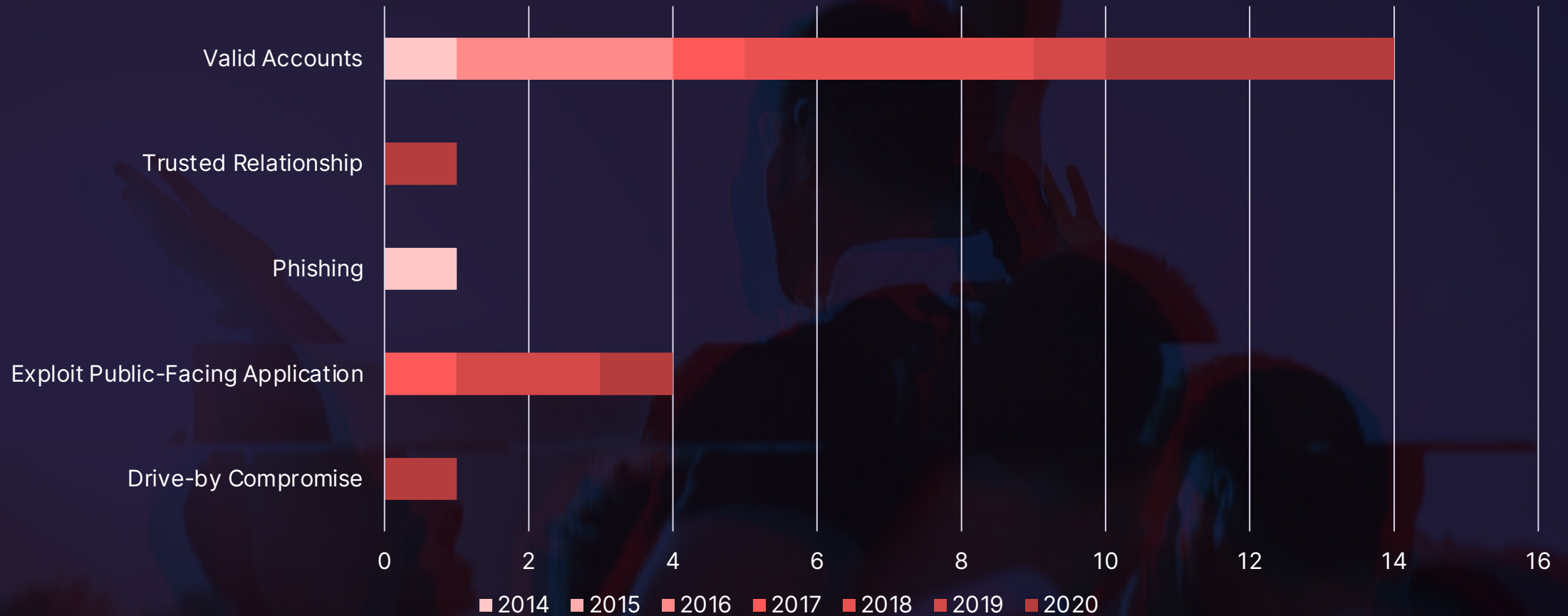
Maturity

Red Team

CSA - Top Threats to Cloud Computing Pandemic Eleven

Survey Results Rank	Survey Average Score	Issue Name
1	7.729927	 Insufficient ID, Credential, Access and Key Mgt, Privileged Accounts
2	7.592701	 Insecure Interfaces and APIs
3	7.424818	 Misconfiguration and Inadequate Change Control
4	7.408759	 Lack of Cloud Security Architecture and Strategy
5	7.275912	 Insecure Software Development
6	7.214493	 Unsecure Third Party Resources
7	7.143066	 System Vulnerabilities
8	7.114659	 Accidental Cloud Data Disclosure/ Disclosure
9	7.097810	 Misconfiguration & Exploitation of Serverless & Container Workloads
10	7.088534	 Organized Crime/ Hackers/ APT
11	7.085631	 Cloud Storage Data Exfiltration

量化：2014~2020 重大雲端威脅統計



以上雲端事件來自於：Learning from AWS (Customer) Security Incidents[2020]

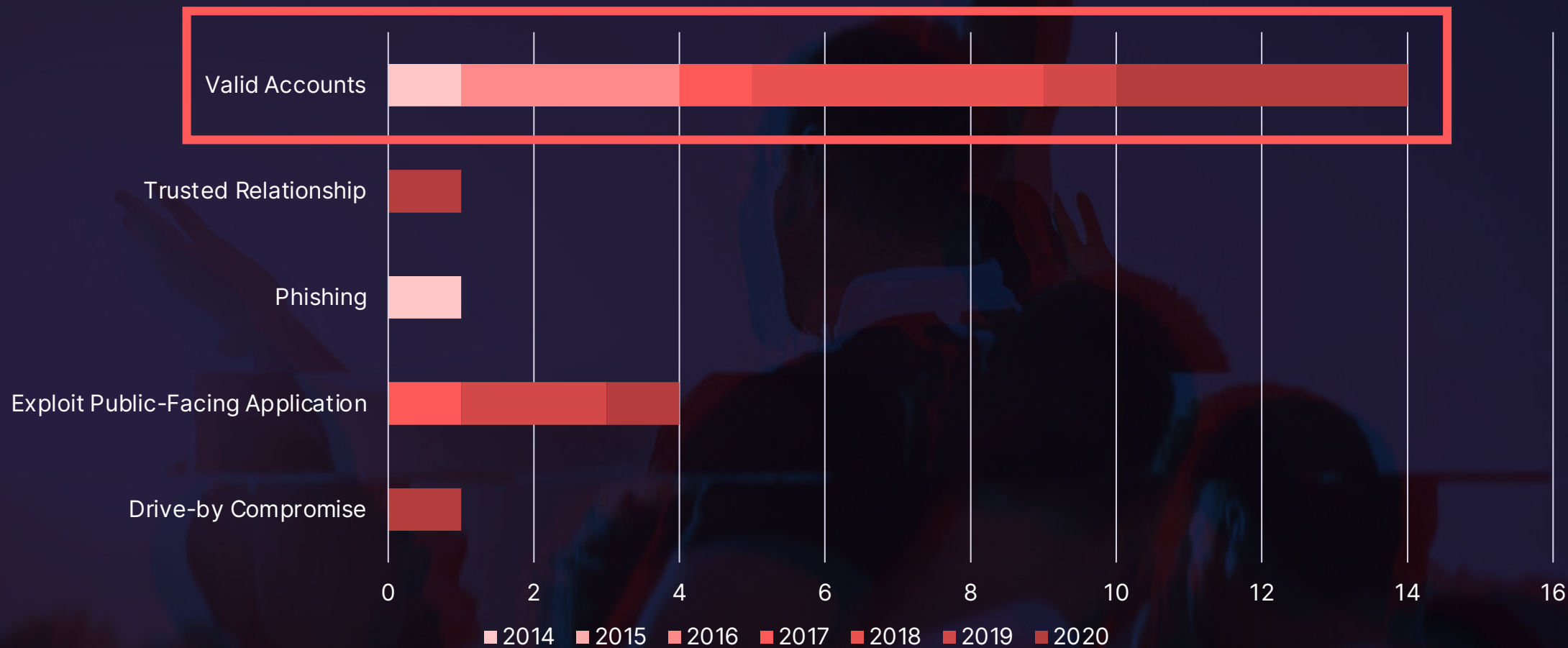
Remediation

- > 針對前述找到的問題依序進行修補
- > 將 Guideline 中的 Best Practices 引入開發流程
- > 使用框架或 Benchmark 定期檢視流程



屬於 Identity
Perimeter

Example：決策



Example：執行

> 針對 CIS Benchmark 中的 IAM 章節優先執行緩解

1 Identity and Access Management.....	14
1.1 Maintain current contact details (Manual)	15
1.2 Ensure security contact information is registered (Manual).....	17
1.3 Ensure security questions are registered in the AWS account (Manual)	19
1.4 Ensure no 'root' user account access key exists (Automated)	21
1.5 Ensure MFA is enabled for the 'root' user account (Automated)	23
1.6 Ensure hardware MFA is enabled for the 'root' user account (Automated)	26
1.7 Eliminate use of the 'root' user for administrative and daily tasks (Automated).....	29
1.8 Ensure IAM password policy requires minimum length of 14 or greater (Automated).....	31
1.9 Ensure IAM password policy prevents password reuse (Automated)	33
1.10 Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password (Automated)	35

Red Team & Maturity

- > 驗證問題已完成修補
- > 透過紅隊的攻擊量測防禦能量
- > 評估雲端成熟度
 - > AWS Well-Architected Framework
- > 持續改良自動化，提升運營效率



Cloud Security Maturity Model





案例分享

A decorative graphic on the left side of the slide. It consists of several overlapping geometric shapes in shades of orange and red, with a white outline of a large right-pointing arrow. The background of the slide is a dark blue with a subtle grid pattern.

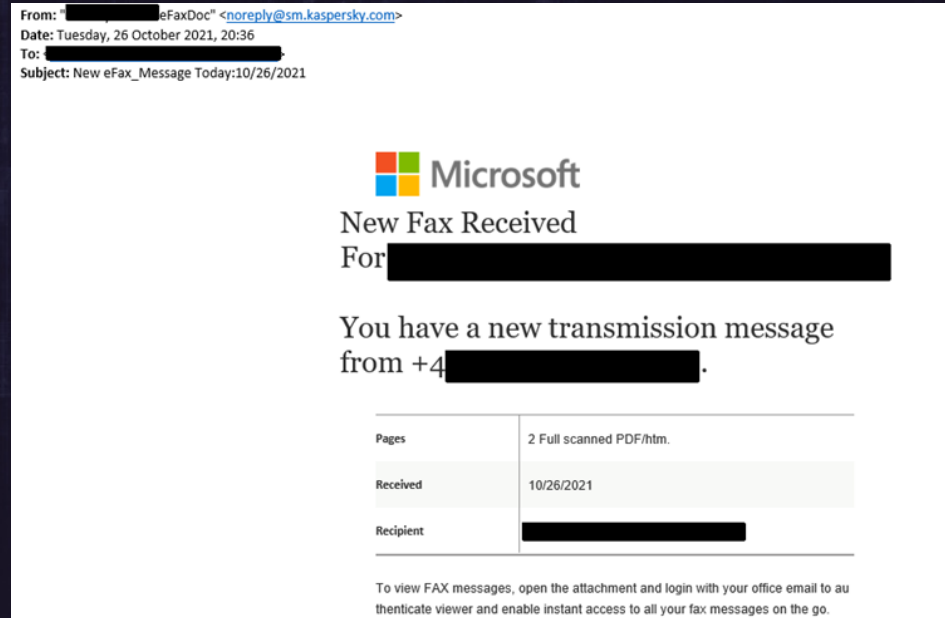
Case 1

Kaspersky's SES Token Leaked

Kaspersky's SES Token Leaked

- > Amazon SES is a scalable email service
- > Kaspersky issued a SES token to a third-party contractor

kaspersky



評估與量化

Discovery

Assessment

Prioritization

決策與執行

Remediation

量測與改進

Maturity

Red Team

> SES service in operation



- > SES service in operation
- > Should've identified a token was sent to a 3rd-party



- > SES service in operation
- > Should've identified a token was sent to a 3rd-party
- > It's an IAM issue, and it's prevalent and important



- > SES service in operation
- > Should've identified a token was sent to a 3rd-party
- > It's an IAM issue, and it's prevalent and important
- > Monitors its usage and revokes when needed



- > SES service in operation
- > Should've identified a token was sent to a 3rd-party
- > It's an IAM issue, and it's prevalent and important
- > Monitors its usage and revokes when needed
- > Automation & Monitoring



A decorative graphic on the left side of the slide. It consists of several overlapping geometric shapes in shades of orange and red, some with a fine grid pattern. A white outline of a right-pointing chevron is positioned to the left of the main text.

Case 2

Newly Build

[REDACTED] from On-Prem to Cloud

- > Been stick to on-prem solutions for years
- > A growing number of users take advantage of their services
- > Needs a flexible, robust and comprehensive solution

The AWS logo is displayed on a dark gray rectangular background. It features the text "powered by" in a small, white, sans-serif font above the word "aws" in a larger, white, sans-serif font. Below "aws" is the orange Amazon smile arrow, which starts under the 'a' and ends under the 's'.

評估與量化

Discovery

Assessment

Prioritization

決策與執行

Remediation

量測與改進

Maturity

Red Team

> Well documented & Assets Management

> Steampipe

> Yor

> READMEs

> ...



> Well documented & Assets Management

> Steampipe

> Yor

> READMEs

> ...

What security groups are open to the world?

Security

```
select
  group_name,
  group_id
from
  aws_vpc_security_group_rule
where
  type = 'ingress'
  and cidr_ip = '0.0.0.0/0';
```



> Well documented & Assets Management

> Steampipe

> Yor

> READMEs

> ...

```
10     Name      = "${local.resource_prefix.value}-data"
11     Environment = local.resource_prefix.value
12   }
13 }
14
15 resource "aws_s3_bucket_object" "data_object" {
16   bucket = aws_s3_bucket.data.id
17   key    = "customer-master.xlsx"
18   source = "resources/customer-master.xlsx"
19
19   tags = {
20     Name      = "${local.resource_prefix.value}-customer-master"
21     Environment = local.resource_prefix.value
22   }
23 }
```

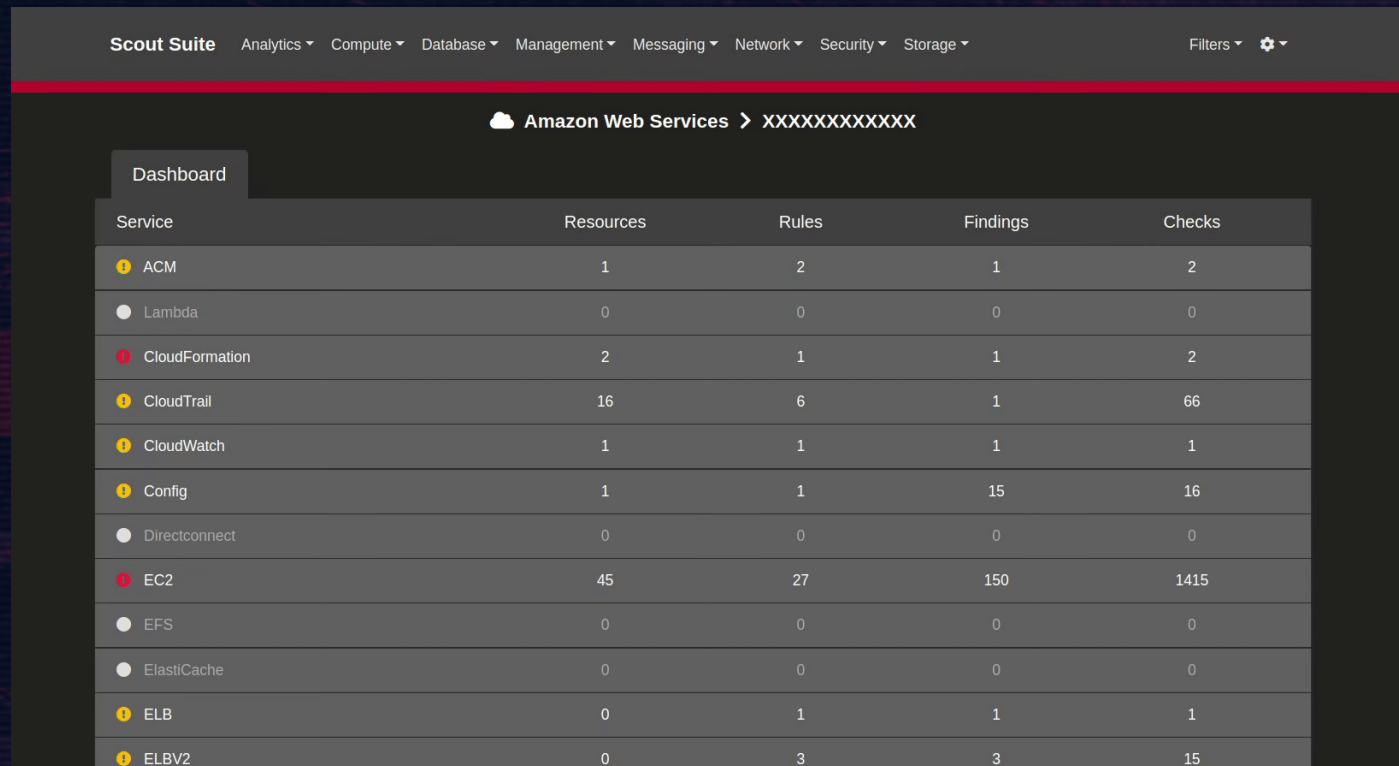
PROBLEMS 25 OUTPUT TERMINAL DEBUG CONSOLE

M-C02DV323ML87:terrigoat sguere\$ brew tap bridgecrewio/tap

- > Well documented & Assets Management
- > Different tools for different purposes
 - > ScoutSuite
 - > SonarQube
 - > ...



- > Well documented & Assets Management
- > Different tools for different purposes
 - > ScoutSuite
 - > SonarQube
 - > ...



The screenshot displays the Scout Suite web interface. At the top, there is a navigation bar with the 'Scout Suite' logo and several menu items: Analytics, Compute, Database, Management, Messaging, Network, Security, and Storage. To the right of these menus are 'Filters' and a settings gear icon. Below the navigation bar, the main content area shows a breadcrumb trail: 'Amazon Web Services > XXXXXXXXXXXX'. A 'Dashboard' tab is selected. The main content is a table with five columns: Service, Resources, Rules, Findings, and Checks. The table lists various AWS services with their respective counts. Each service row starts with a status icon (yellow for warnings, red for errors, and grey for no issues).

Service	Resources	Rules	Findings	Checks
⚠️ ACM	1	2	1	2
🔴 Lambda	0	0	0	0
⚠️ CloudFormation	2	1	1	2
⚠️ CloudTrail	16	6	1	66
⚠️ CloudWatch	1	1	1	1
⚠️ Config	1	1	15	16
🔴 Directconnect	0	0	0	0
⚠️ EC2	45	27	150	1415
🔴 EFS	0	0	0	0
🔴 ElastiCache	0	0	0	0
⚠️ ELB	0	1	1	1
⚠️ ELBV2	0	3	3	15

- > Well documented & Assets Management
- > Different tools for different purposes
 - > ScoutSuite
 - > SonarQube
 - > ...

```
246     if (Provider.class == roleTypeClass) {  
247         Type providedType = ReflectionUtils.getLastTypeGenericArgument(dependencyD  
248         2 Class providedClass = 1 ReflectionUtils.getTypeClass(providedType);  
249  
250         if (this.componentManager.hasComponent(providedType, dependencyDescriptor.  
251             || 3 providedClass.isAssignableFrom(List.class) || providedClass.isA
```

A "NullPointerException" could be thrown; "providedClass" is nullable here.

 Bug  Major

 cert, cwe

```
252         continue;  
253     }
```

RELIABILITY

 0  Bugs

Quality Gate

Passed

All conditions passed

SECURITY

 0  Vulnerabilities

 1 Hotspots

MAINTAINABILITY

 4 Code Smells

 5  Debt
min

- > Well documented & Assets Management
- > Different tools for different purposes
- > Prioritizes issues from the business impacts
 - > What matters to the company
 - > Go wide then deep (not to be too hyperfixation on DiD)
 - > Consult with professionals



- > Well documented & Assets Management
- > Different tools for different purposes
- > Prioritizes issues from the business impacts
- > Mitigates issues with top-down approach
 - > Tooling, Guideline, Best Practices, etc



- > Well documented & Assets Management
- > Different tools for different purposes
- > Prioritizes issues from the business impacts
- > Mitigates issues with top-down approach
- > Red Team



- > Well documented & Assets Management
- > Different tools for different purposes
- > Prioritizes issues from the business impacts
- > Mitigates issues with top-down approach
- > Red Team



結論



EVERYTHING
STARTS FROM
SECURITY



接下來，行動！

- > 短期
 - > 開始盤點雲端資產
- > 中期
 - > 導入體質強化流程
 - > Prioritization 與 Remediation 建議找外部資安團隊協助
- > 長期
 - > 提升雲端成熟度，朝集中且自動化邁進

Thank You 🙏
Any Question?



EVERYTHING
STARTS
FROM
SECURITY