The Cloud Migration Playbook

Part 1: A Simple Primer To Complexity

Who Am I?

Jason Sewell
Sr. Security Engineer
@sewell_jason

Background
Web Application Developer
DevOps => DevSecOps
InfoSec/Penetration Tester
OWASP Hawaii Chapter Lead

AWS Certifications
AWS SysOps Associate
AWS Security Specialist
AWS Solutions Architect
(TBD)

Who Are You?

I am...

- A CISO
- A Technical Director
- An Engineering Manager
- A Security-Minded Advocate

I want to...

- Lift and shift existing on-prem applications to AWS
- Understand the attack surface of our AWS resources
- Validate that proper security measures are in place in our AWS environment

What do we want to accomplish today?

and Amazon shoppers exposed ...

Data ... llions of e... The Capital One Data Breach ...

Imperva Data Breach Caused by ...

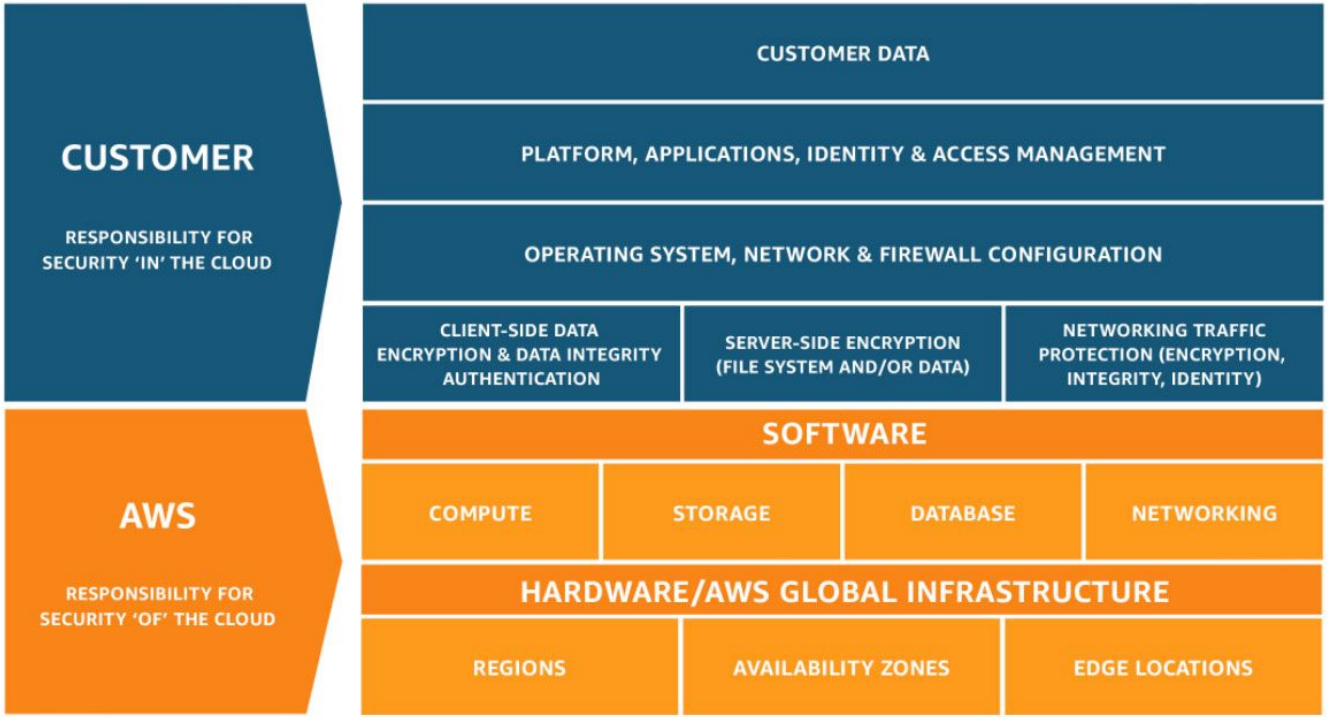
Cloud Infrastructure ... nfigurations Still Plague Indust... A Look at What ...

... nprotected AWS Server exposes over 350m passwords ...

... en AWS API ...

Eight million EU retail sales records exposed on AWS MongoDB

Where To Begin?



The AWS Shared Security Model

But is it really shared…?

“Through 2025, 99% of cloud security failures will be the customer’s fault.”

Source: Gartner, https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

Q: What’s the main thing we have to worry about?

A: Misconfigurations

Year over year from 2018 to 2019, the number of records exposed by cloud misconfigurations rose by 80%, as did the total cost to companies associated with those lost records.

In 2018 and 2019, 68% of the companies that suffered a data breach caused by a cloud misconfiguration were founded prior to 2010.

Source: DivvyCloud, 2020 Cloud Misconfigurations Report

Know Your Defaults

Convenience vs Security

DISCLAIMER: Also easier said than done...

“It’s the same stuff, just in the cloud right?”

Kinda.

First Things First

When performing a lift-and-shift or cloud migration you should start threat modeling and hardening 4 common areas:

- Identity
- Data Storage
- Networking
- Compute

Identity

IAM

“Identity is the new perimeter”

- Over 6000 unique permissions in AWS

  ...and growing

- Difficult to manage and visualize permission boundaries
- IAM is hard

Attacks

- Account Takeover
  - Brute Force Attempts
  - Password Spraying
  - Social Engineering
- Credential Theft
  - Privilege Escalation
  - Resource Allocation
  - Persistence

IAM (not gonna do this)

Show Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

Cancel

IAM > Groups > **badmins**

Summary

Group ARN:	arn:aws:iam::086629858357:group/badmins
Users (in this group):	9
Path:	/
Creation Time:	2020-09-20 16:52 HST

Users | Permissions | Access Advisor

This view shows all users in this group: **9 Users**

hong-networking	Remo
past-employee	Remo
jill	Remove User from Group
contractor-person	Remove User from Group
brian	Remove User from Group
jon-developer	Remove User from Group
new-employee	Remove User from Group
jennifer	Remove User from Group

Users > contractor-person

Summary

User ARN	arn:aws:iam::086629858357:user/contractor-person
Path	/
Creation time	2020-09-20 16:56 HST

Permissions | Groups (1) | Tags (1) | Security credentials | Access Advisor

Sign-in credentials

Summary	• Console sign-in link signin.aws.amazon.com/console
Console password	Enabled (never signed in) | Manage
Assigned MFA device	Not assigned Manage
Signing certificates	None

Access keys

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share practice, we recommend frequent key rotation. Learn more

Create access key

Access key ID	Created	Last used
	2020-09-20 16:56 HST	N/A

Defenses

- Single Sign On/Federation (SSO)
- MFA Enforcement
- No Root User API keys
- User Key Rotation
- Role-Based Access Control (RBAC)
- Least Privilege IAM policies
  - Use conditional policies
  - No wildcards
  - No AdministratorAccess
- Disable unused regions

Data Storage

S3

“Your favorite data breach news source”

- S3
- RDS
- DynamoDB
- Elasticache
- SQS
- ...more

Attacks

- Bucket Enumeration
- Data Exfiltration
- Resource Tampering
- Payload Staging

Bucket Enumeration

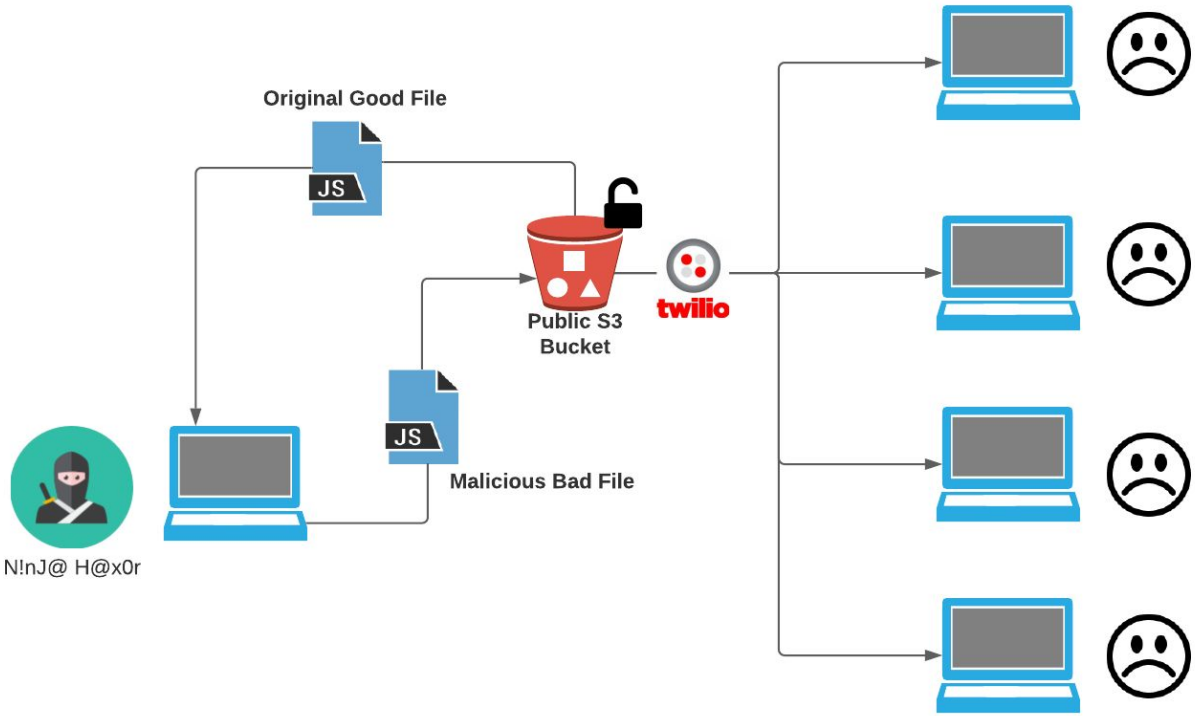
GRAYHAT WARFARE
cause white is boring

Home | Filter Buckets | Search Files | Docs / API | Top Keywords

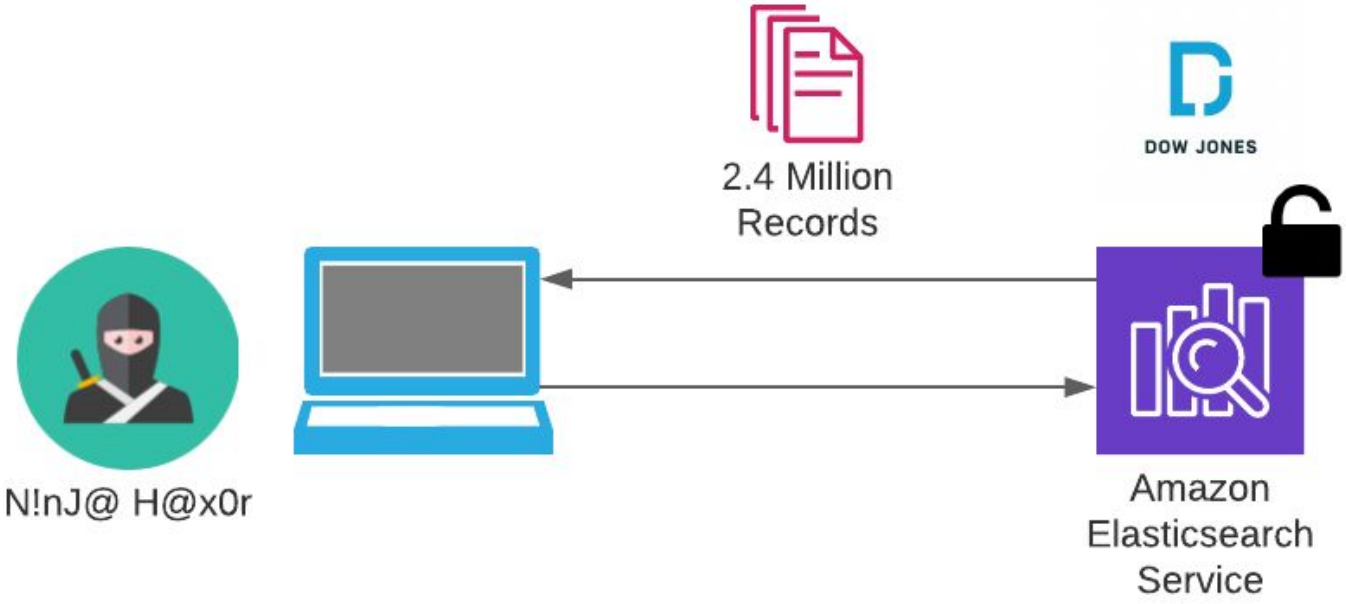
Files
1.197 of 3.639 billion (?)

Buckets
54515 of 296387 (?)

Resource Tampering



Data Exfiltration



Defenses

- S3: Turn on Block Public Access
- S3: Strict Bucket Policies
- RDS/Elasticache: No public access, encrypt snapshots
- SQS: No public queues, encrypt messages
- DynamoDB: Strict IAM controls

Compute

EC2

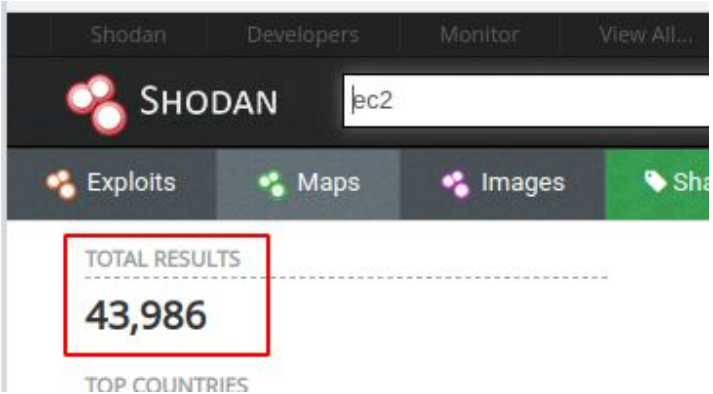
The same old servers, except different.

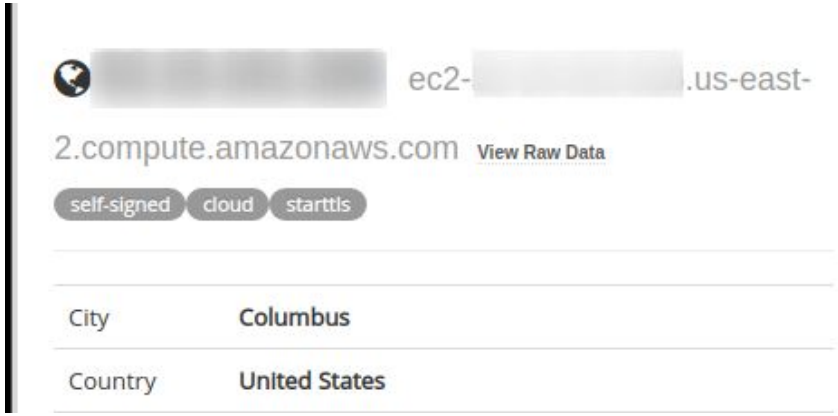
- It’s still a server..
- ...but in a whole new environment.

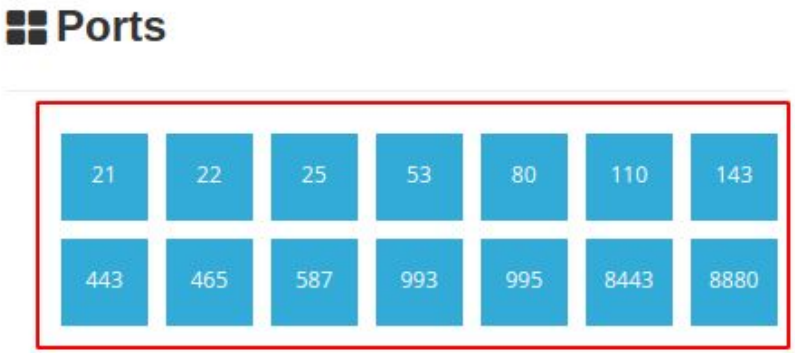
Attacks

- Service Enumeration
- Application Exploit
  - SSRF
  - RCE
- Post-Exploit
  - Instance Metadata Access
  - Lateral Movement
  - Cryptojacking
  - Unencrypted Volume Access

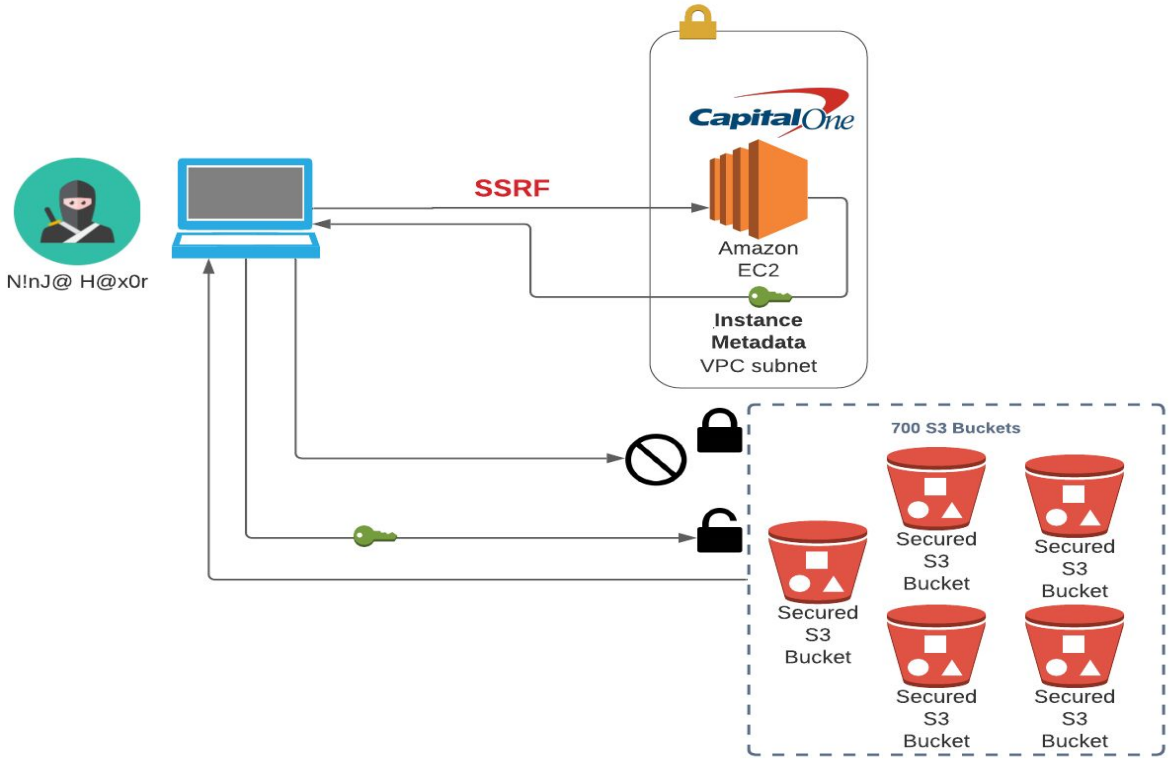
Service Enumeration



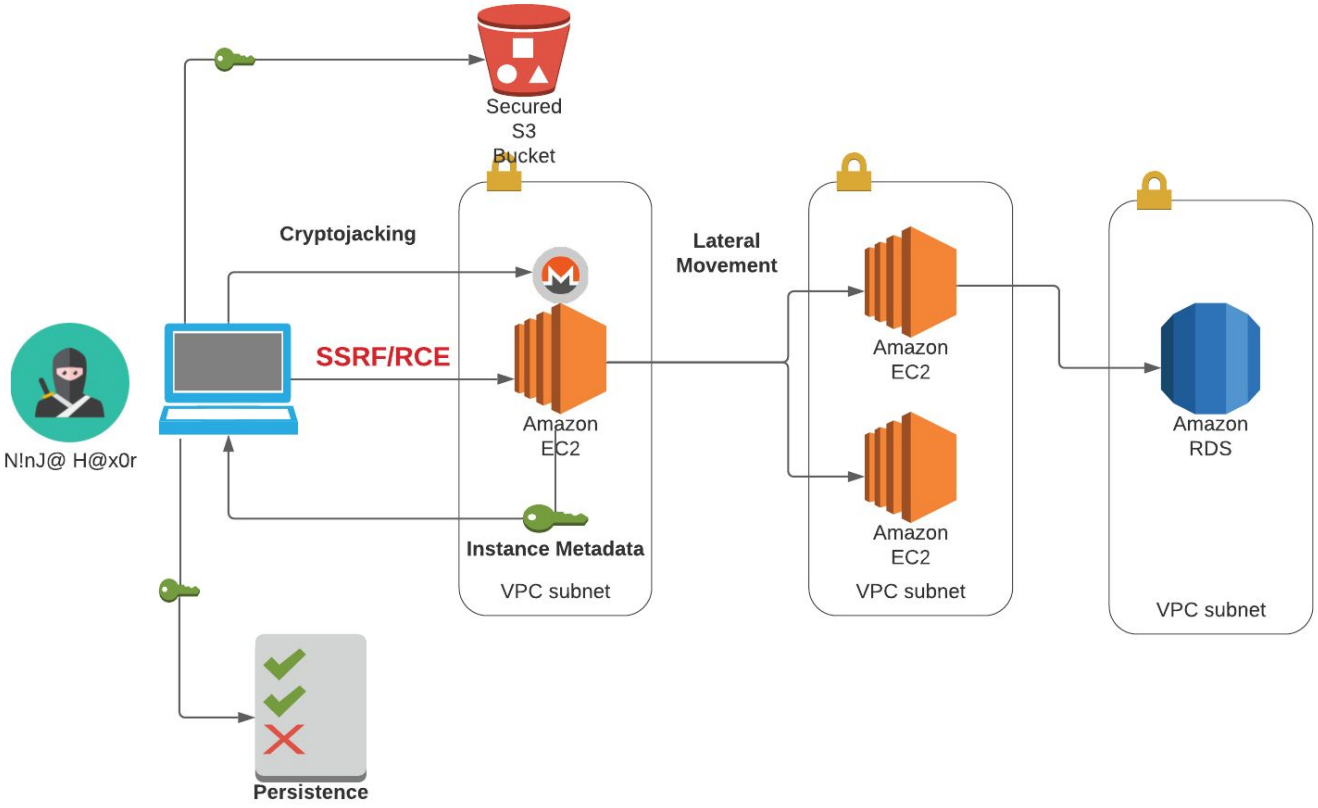




Application Exploit (SSRF)



Post-Exploitation



Defenses

- Server Hardening
- Remove Default Users
- Load Balancers & WAF
- Encrypt Volumes
- Protect Instance Metadata

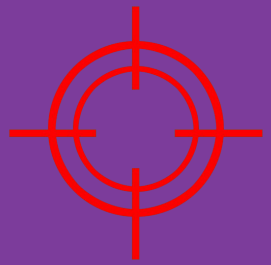
Networking

VPC

The same old network, except different.

- Networking is hard
- Networking in the cloud is hard AND different

- Service Discovery
- Data Exfiltration
- Lateral Movement (VPC Peering, VPN, Direct Connect)
- Security Group Backdoor(IAM/EC2)
- Traffic Monitoring



Attacks

Defenses

- Network Segmentation
- Create Strict Security Group and NACL Rules
- Assign SG Rules to Other Internal SGs
- Use VPC Endpoints for Internal Traffic

OK..so how do we manage this?

Migrate Your Practices, Not Just Your Applications.

Automation

Unleash the robot army.

- DevSecOps / Security Engineering
- Infrastructure as Code
- Monitor Events
- Automate Remediation
- Vulnerability Scanning

Cloud Security Maturity Model

LEVEL 1
No Automation

Manually managing policies/procedures, mostly through console.

Architectures resemble traditional infrastructure (e.g. low use of serverless and high reliance on network security controls).

IAM mostly ad-hoc with little to no federation.

LEVEL 2
Simple Automation (SecOps)

Basic provisioning.

Some FaaS/Lambda.

Project specific, not coordinated across accounts.

Initial use of infrastructure as code (Terraform/ CloudFormation), but security not consistently engaged in design/review.

Federation on some accounts, but limited use of MFA due to difficulties supporting teams (especially on the command line).

LEVEL 3
Manually Executed Scripts

Initial automation typically scripted through FaaS/Lambda.

Automation still executed manually.

Some third party tooling (orchestration with other tools), Federation on most accounts with widespread MFA, but still gaps on consistency.

Security starting to review, design and promote use of CloudFormation/Terraform.

LEVEL 4
Guardrails

Automation expands into guardrails across multiple accounts.

Expanding library of automation.

Big shift from manual creation and execution to running automations off a centralized platform with centralized management and reporting.

Consistent use of federation and MFA, with some gaps supporting toolchains.

LEVEL 5
Automation Everywhere

Centrally managed.

Covering all of the domains.

Integrated into infrastructure as code environment.

Built-in to the stack with provisioning automation.

Federation and MFA working consistently across toolchains (e.g. command line support).

https://www.iansresearch.com/resources/cloud-security-maturity-model/what-is-the-csmm

Where do you go from here...?

Thank You.

We Can Help:
info@occamsec.com

https://www.linkedin.com/company/occamsec/

https://twitter.com/OccamSec