CWL
CyberWarFare Labs

Detection Techniques for Identifying AWS IAM Targeted Attacks

© All Rights Reserved CyberwarFare Labs

About CyberWarFare Labs :

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements. The company has two primary divisions :

1. Cyber Range Labs

2. Up-Skilling Platform

aws
Cloud Security
RED TEAM
PURPLE TEAM
BLUE TEAM
AD
WEB
On-Premise Security
CI/CD
PLATFORM
NETWORK

INFINITE LEARNING EXPERIENCE

© All Rights Reserved CyberwarFare Labs

CWL
CyberWarFare Labs

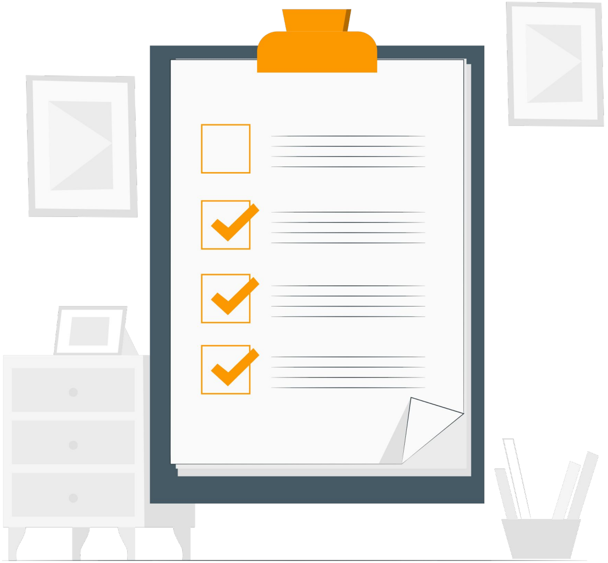
About Speaker :

Harisuthan S

(Senior Security Engineer)

He Is a Blue Team Security researcher, bringing over 3+ years of experience in cyber defence. possesses a deep understanding of Blue Team methodologies including investigation and detection over cyber attacks,

© All Rights Reserved CyberwarFare Labs



Agenda

- Basic Introduction about IAM and IAM targeted attacks
- List of Essential AWS services for Safeguarding IAM
- Detection Techniques for Identifying IAM Targeted Attacks
- Conclusion

© All Rights Reserved CyberwarFare Labs

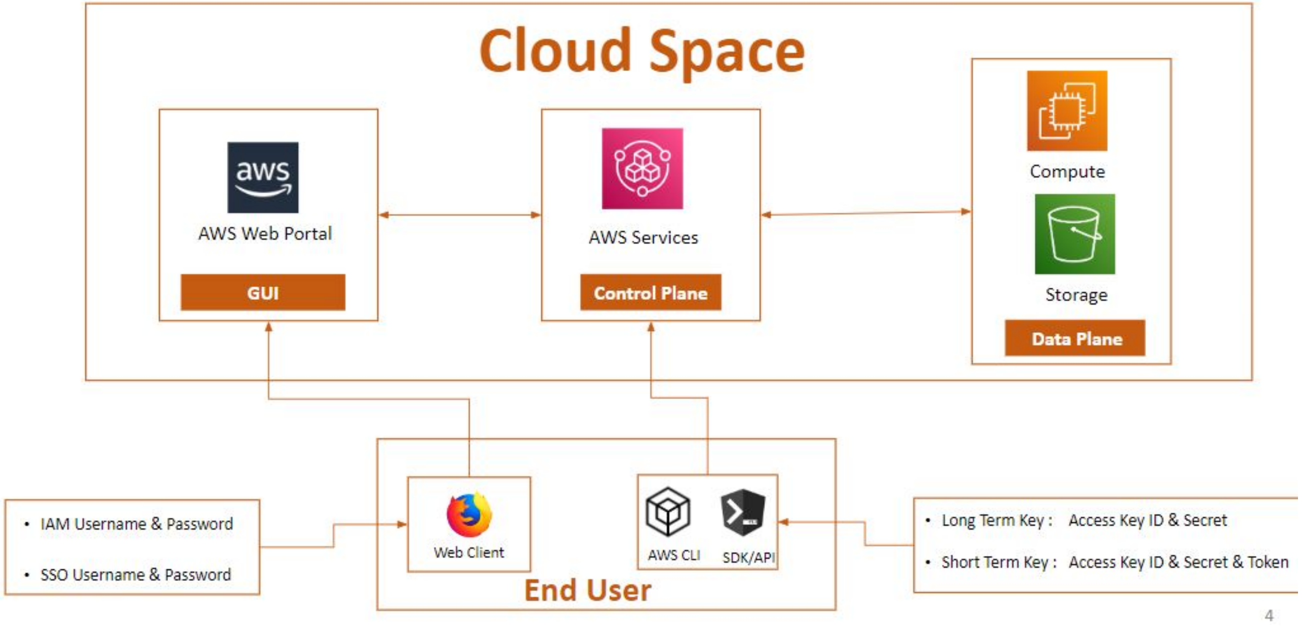
Basic Introduction about AWS IAM Service

© All Rights Reserved CyberwarFare Labs

AWS IAM : Identity Access Management

- AWS Identity and Access Management (IAM) is a AWS service that helps you securely control access to AWS resources.
- It allows you to manage users, groups, and permissions, ensuring that only authorized individuals and applications have the necessary access to perform specific tasks. With IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.
- It supports features like multi-factor authentication (MFA), identity federation, and fine-grained access control, making it a crucial component for maintaining security and compliance in AWS environments

AWS IAM : Identity Access Management



Cloud Space

AWS Web Portal

GUI

AWS Services

Control Plane

Compute

Storage

Data Plane

- IAM Username & Password
- SSO Username & Password

Web Client

AWS CLI

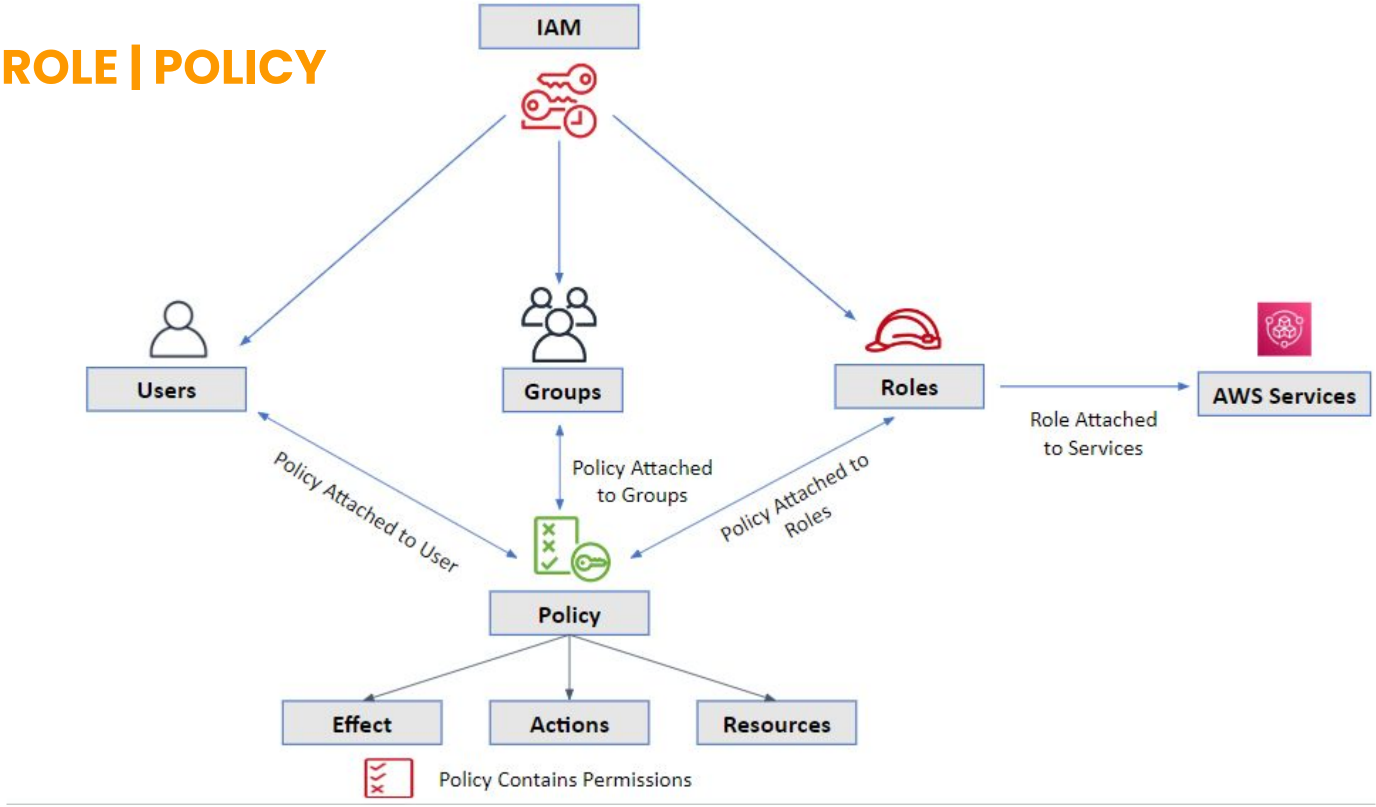
SDK/API

End User

- Long Term Key : Access Key ID & Secret
- Short Term Key : Access Key ID & Secret & Token

© All Rights Reserved CyberwarFare Labs

USER | ROLE | POLICY



© All Rights Reserved CyberwarFare Labs

AWS S3 : Simple Storage Service

1. Investigating Multiple Failed Login Activities

2. Investigating MFA Failed Logged-In activity

3. Investigating suspicious activities of User Granted with Full Privileges

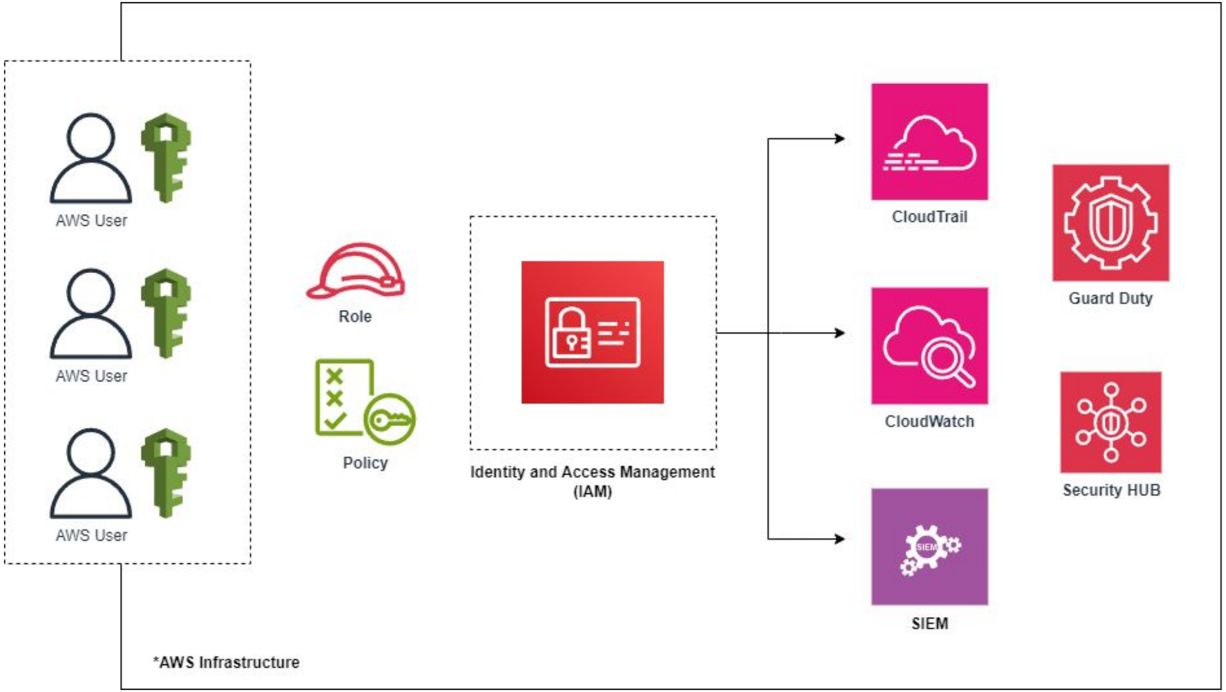
© All Rights Reserved CyberwarFare Labs

List of AWS services to protect IAM

- CloudTrail
- Guard Duty
- CloudWatch
- AWS Macie
- SIEM

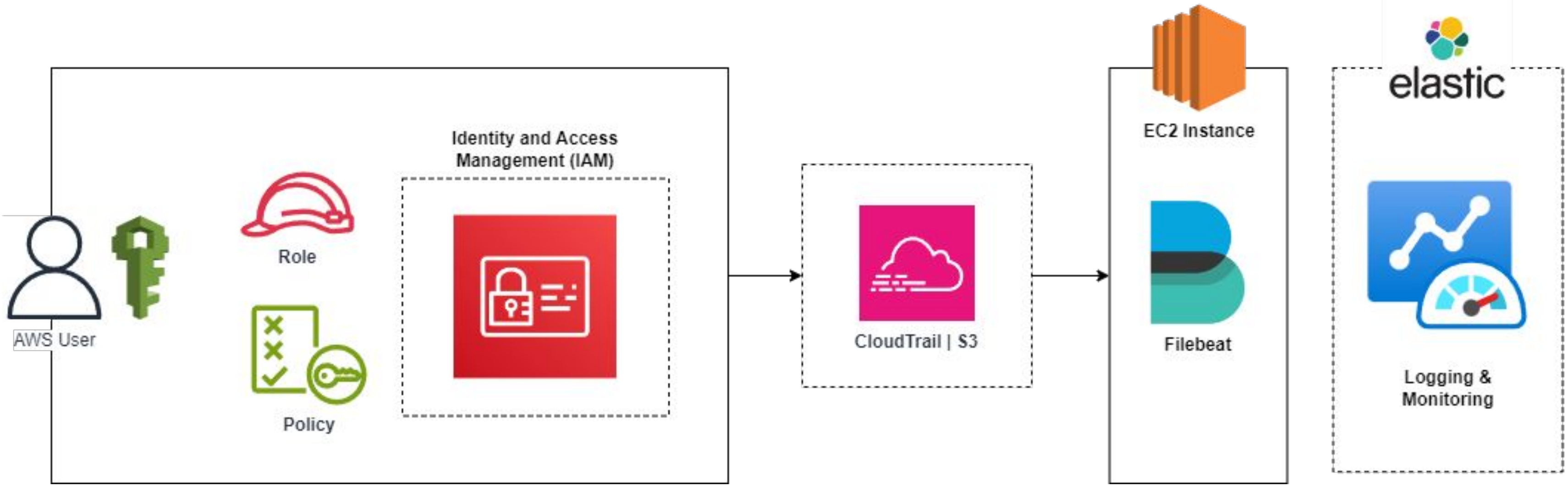
© All Rights Reserved CyberwarFare Labs

Monitoring & Logging AWS IAM



© All Rights Reserved CyberwarFare Labs

IAM Monitoring Architecture

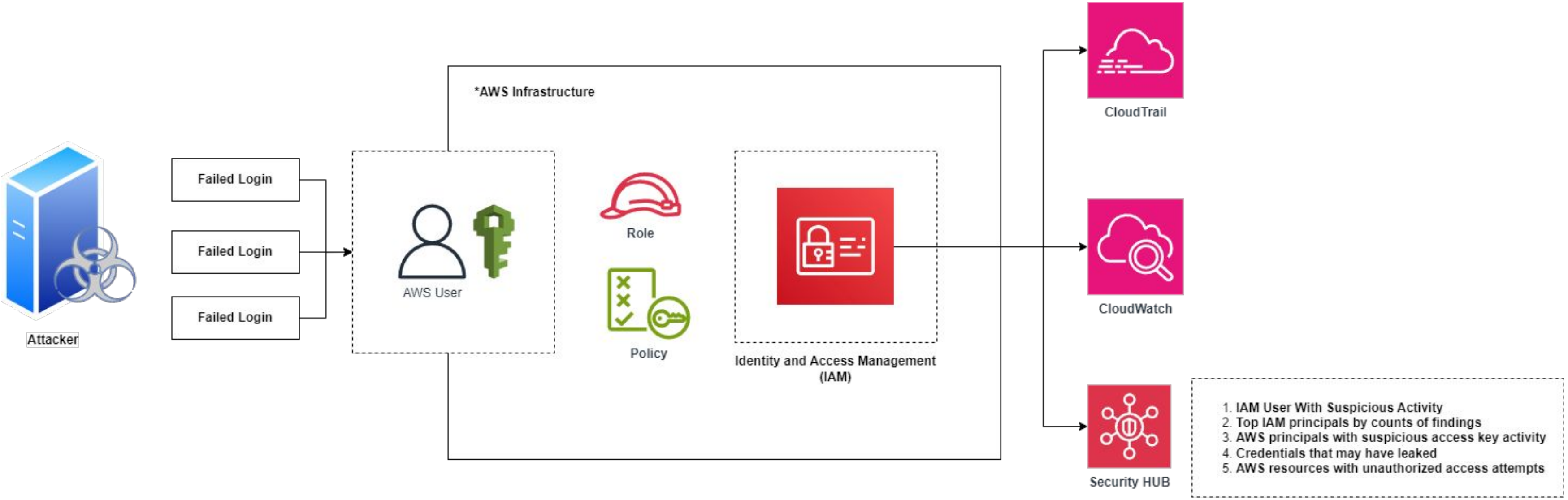


© All Rights Reserved CyberwarFare Labs

Investigating Multiple Failed Login Activities

© All Rights Reserved CyberwarFare Labs

Investigating Multiple Failed Login Activities

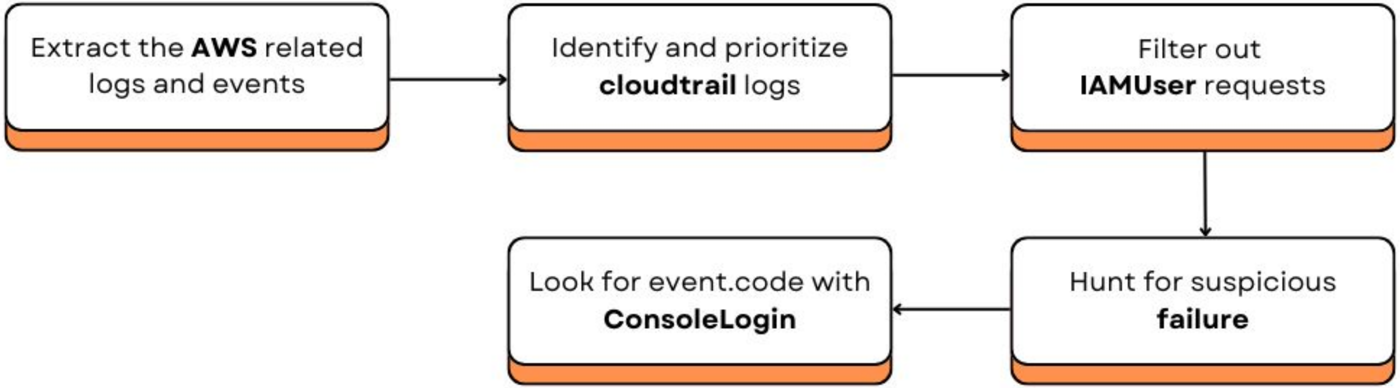


1. IAM User With Suspicious Activity
2. Top IAM principals by counts of findings
3. AWS principals with suspicious access key activity
4. Credentials that may have leaked
5. AWS resources with unauthorized access attempts

© All Rights Reserved CyberwarFare Labs

CWL CyberWarFare Labs

Investigative Mind-Map for Investigating Multiple Failed Login Activities



Extract the **AWS** related logs and events

Identify and prioritize **cloudtrail** logs

Filter out **IAMUser** requests

Hunt for suspicious **failure**

Look for event.code with **ConsoleLogin**

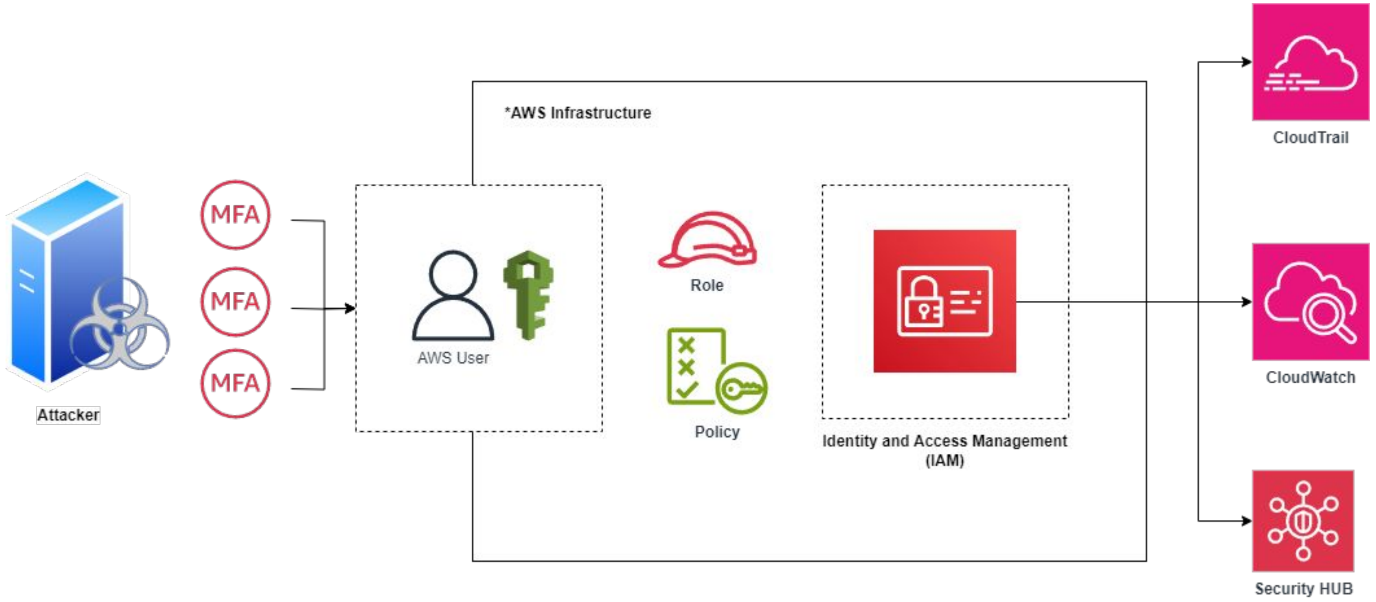
© All Rights Reserved CyberwarFare Labs

CWL
CyberWarFare Labs

Investigating MFA Failed Login Activities

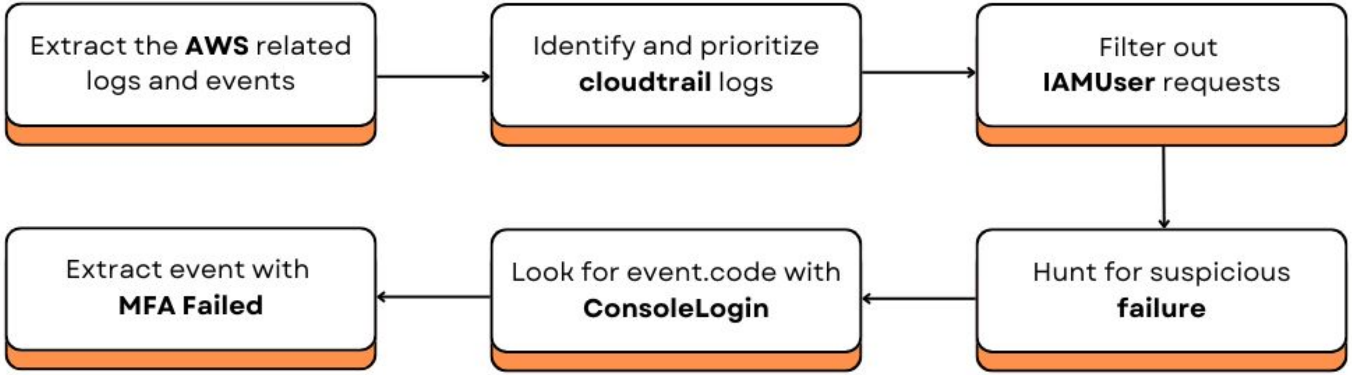
© All Rights Reserved CyberwarFare Labs

Investigating MFA Failed Login Activities



© All Rights Reserved CyberwarFare Labs

Investigative Mind-Map for Investigating Multiple Failed Login Activities



Extract the **AWS** related logs and events

Identify and prioritize **cloudtrail** logs

Filter out **IAMUser** requests

Hunt for suspicious **failure**

Look for event.code with **ConsoleLogin**

Extract event with **MFA Failed**

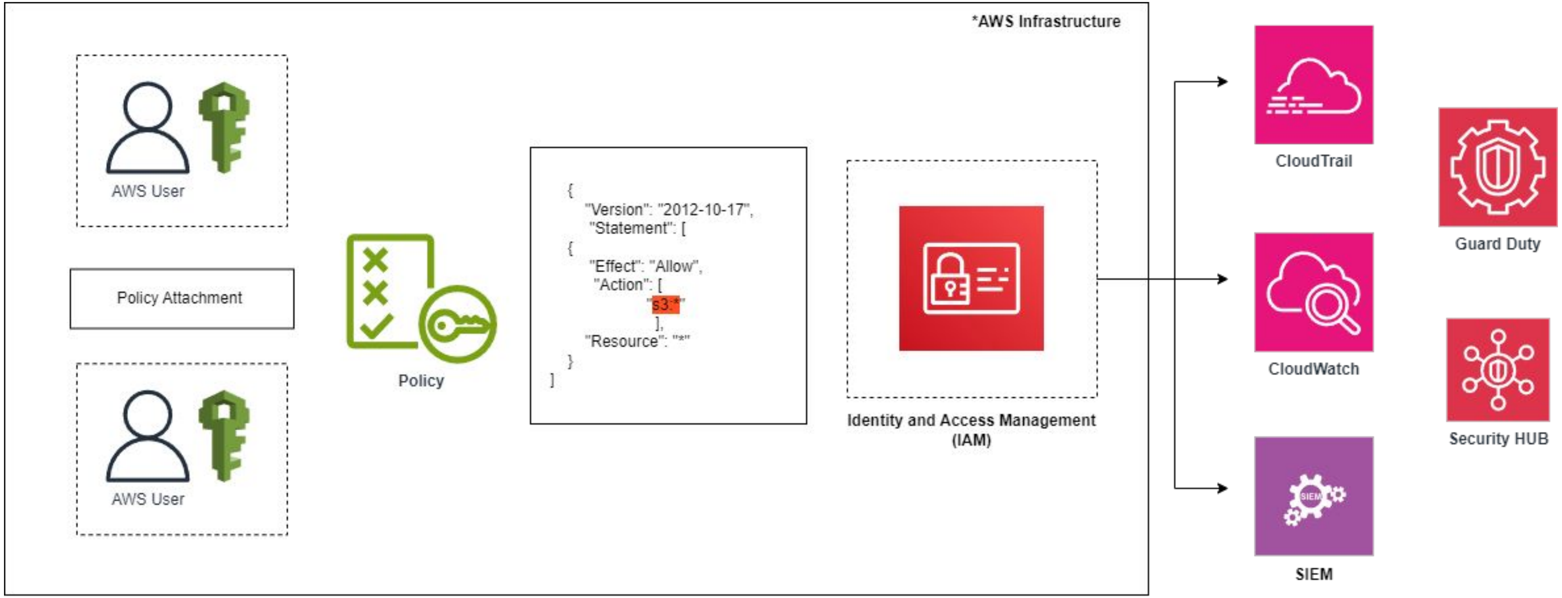
© All Rights Reserved CyberwarFare Labs

CWL
CyberWarFare Labs

Investigating suspicious activities of User Granted with Full Privileges

© All Rights Reserved CyberwarFare Labs

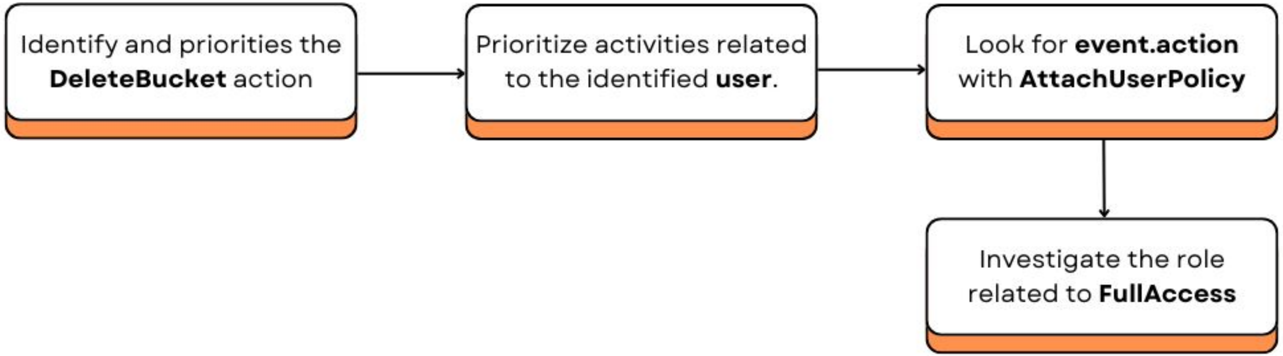
Investigating suspicious activities of User Granted with Full Privileges



```
{
   "Version": "2012-10-17",
    "Statement": [
{
    "Effect": "Allow",
     "Action": [
               "s3:*"
                ],
   "Resource": "*"
}
]
```

© All Rights Reserved CyberwarFare Labs

Investigative Mind-Map for Investigating Multiple Failed Login Activities



Identify and priorities the **DeleteBucket** action

Prioritize activities related to the identified **user**.

Look for **event.action** with **AttachUserPolicy**

Investigate the role related to **FullAccess**

© All Rights Reserved CyberwarFare Labs

Giveaways & Benefits Details :

- Get a chance to win our most popular course “Blue Team Fundamentals Course (BTF)”

  Participate in the giveaway here:

  https://www.linkedin.com/feed/update/urn:li:activity:7217045965499748353/
- Get Attendance Certificate
- Video Recording of this webinar
- Downloadable PDF Link of this slide

© All Rights Reserved CyberwarFare Labs

CWL
CyberWarFare Labs

CWL
CyberWarFare Labs

cyberwarfare.live

Cyber Security Analyst
(C3SA)

GET
90% OFF

Use this coupon code
“C3SA90OFF”
Offer valid for 1 week only

Upgrade to the Premium & Get Certified today!

ENROLL NOW

© All Rights Reserved CyberwarFare Labs

Thank You

© All Rights Reserved CyberwarFare Labs