
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC315

Security best practices for Amazon Cognito applications

Mahmoud Matouk

Principal Solutions Architect – AWS Identity
Amazon Web Services

Rachit Dhall

Software Development Manager – Amazon Cognito
Amazon Web Services

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

300-level chalk talk – Questions are welcome

Using Amazon Cognito services for CIAM

Identity layer threats and mitigation best practices

Preparing and responding to security incidents

Summary and call to action

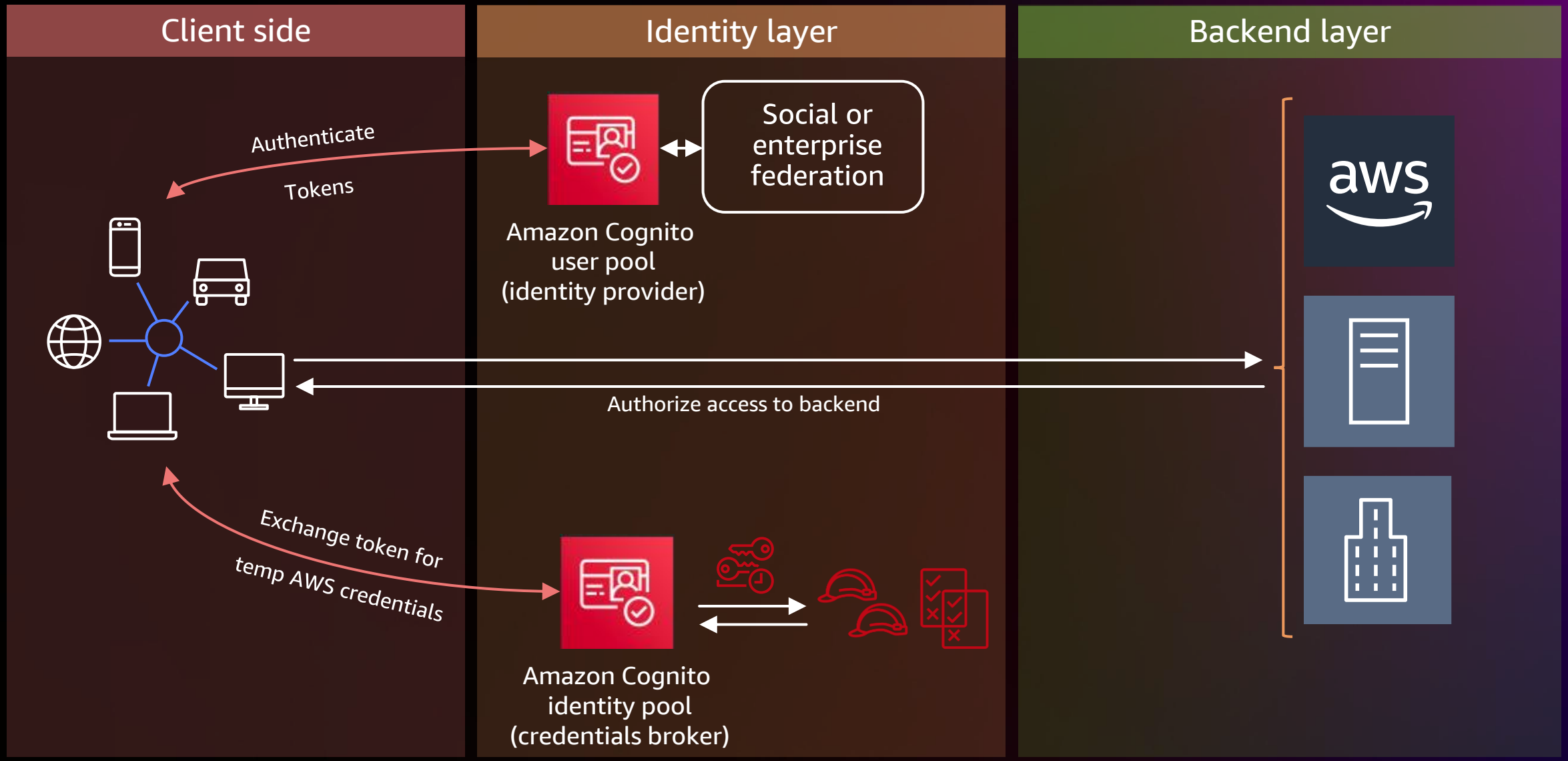
Open Q&A

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Do you use Amazon Cognito in production today?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Using Amazon Cognito services for CIAM



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Building CIAM solutions on AWS



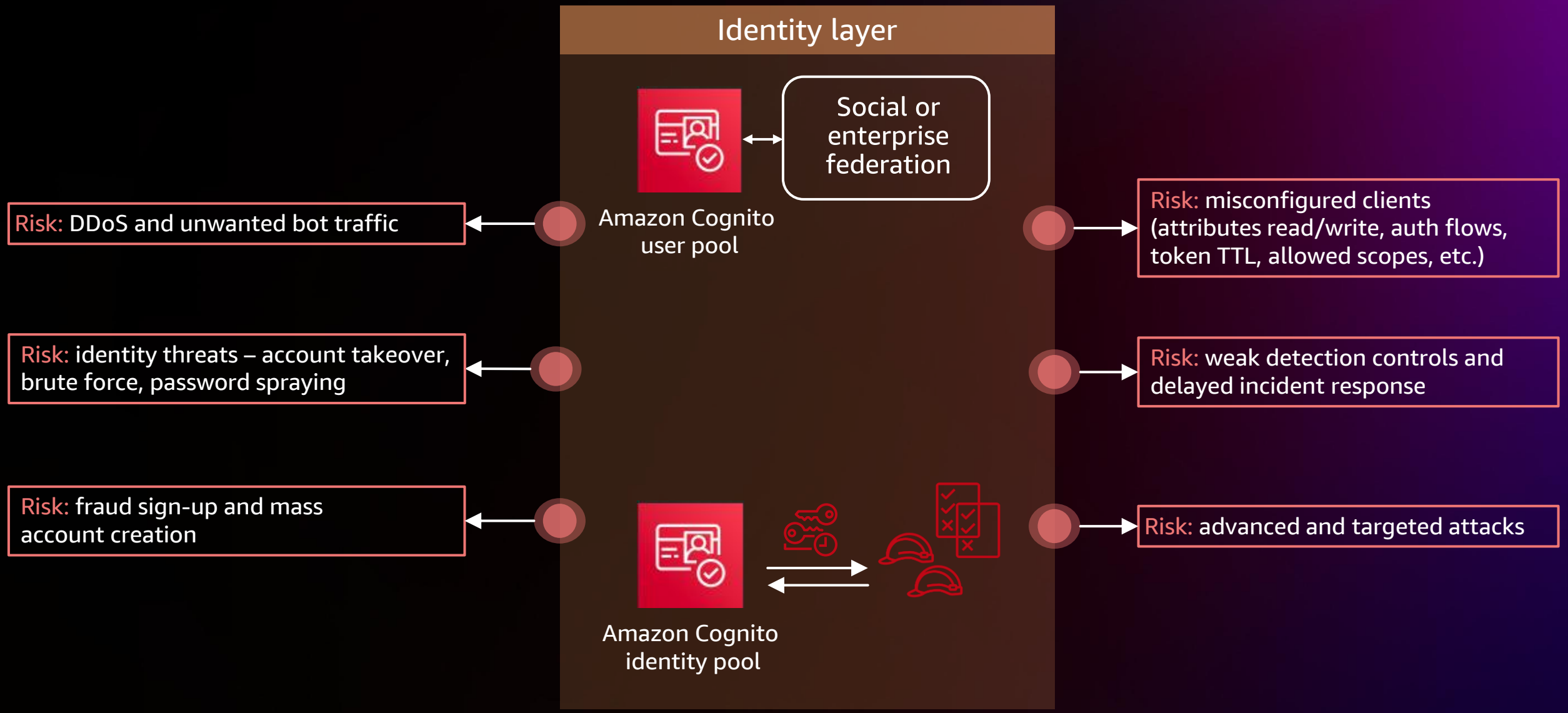
Amazon Cognito workshop

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Threats to identity layer

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Threats to identity layer



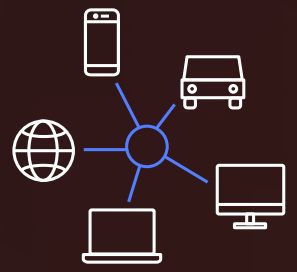
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Best practices and mitigation strategies

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Best practices to mitigate risks

Client side



Client applications

Identity layer

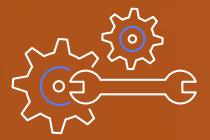


Amazon Cognito user pool

Application



Strong factors



Automation



Optimize

Infrastructure



AWS WAF



Rate limiting



Filtering rule



Bot control

Monitoring



Amazon CloudWatch



Alarm



Logs

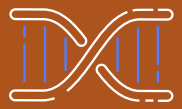


Automation

Advanced



Advanced security



Proxy and backed authentication

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Planning your incident response

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Planning incident response

Planning

- WAF rules
- Utilization alarms
- Logs streamed to CloudWatch
- Predefined queries
- Dashboards in CloudWatch
- Runbook

Detection

- Understand alarms and their meanings
- Analyze logs to identify sources
- Determine impact

Find the top 25 IP addresses that triggered a NotAuthorizedException error

```
filter eventSource = "cognito-idp.amazonaws.com" and errorCode=
"NotAuthorizedException" | stats count(*) as count by
sourceIPAddress, eventName | sort count desc | limit 25
```

Mitigation

- Block unauthorized clients
- Adjust rate limiting rules
- Scale out your resources
- Rotate Amazon Cognito application clients if possible
- Automated runbook

Post-incident analysis

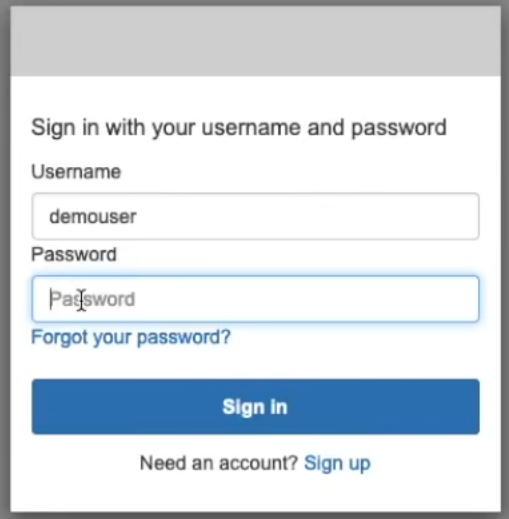
- Analyze logs
- Optimize flows, alarms, and logs and be better prepared

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Let’s see it in action . . .

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.


Sign in with your username and password
Username
demouser
Password
Password
Forgot your password?
Sign in
Need an account? Sign up

Automating incident response

Planning

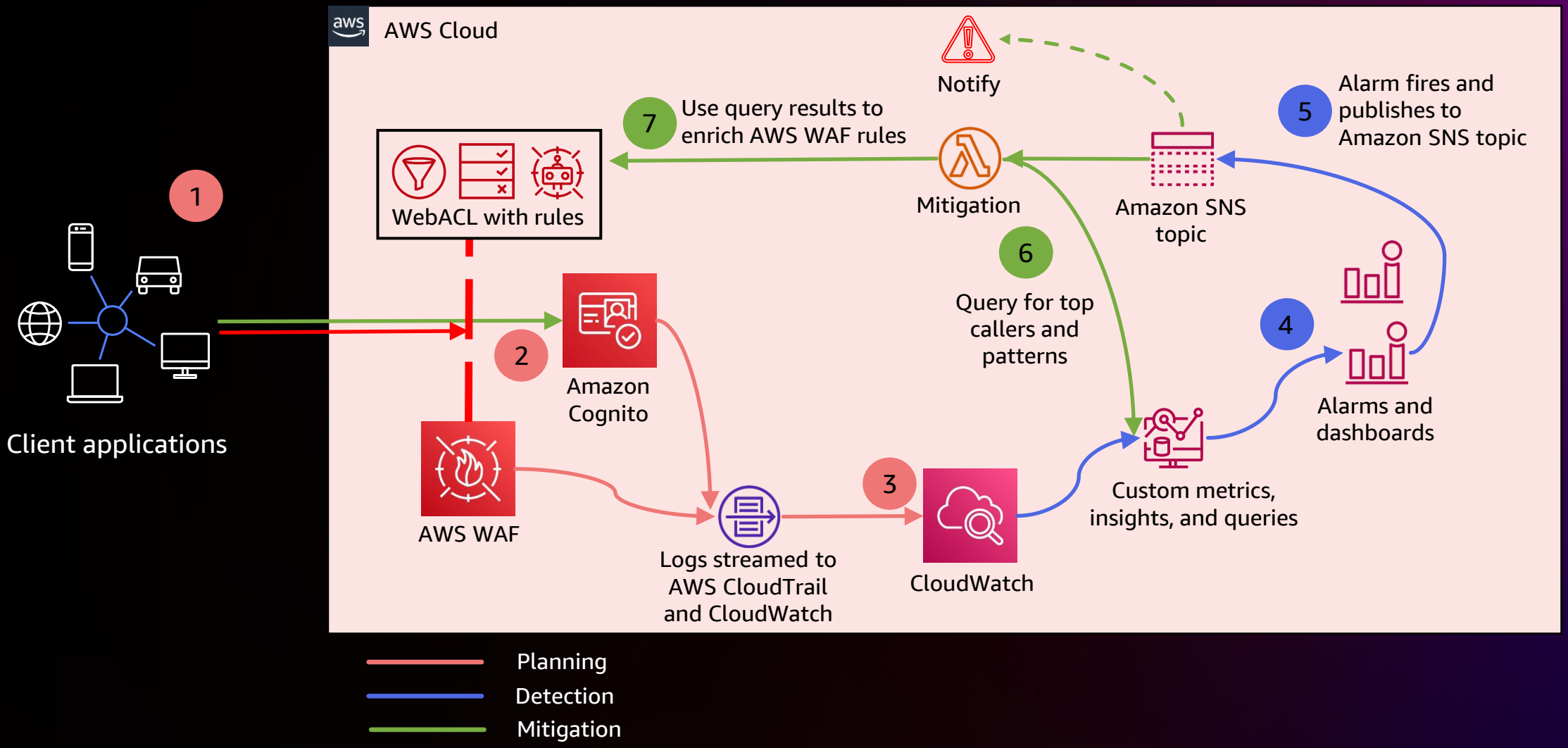
Detection

Mitigation



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Automating incident response



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Best practices for Amazon Cognito applications

- Review your application and API calls and optimize if needed
- Avoid manual changes to production resources
- Strengthen your security (MFA, CAPTCHA, strong factors)
- Understand metrics and review your quota and utilization
- Prepare your environment (dashboards, alarms, AWS WAF web ACL)
- Stream logs to CloudWatch and prepare queries for faster analysis
- Build incident response runbook and test regularly with AWS GameDays
- Automate mitigation actions that can be safely automated
- Run load and penetration testing on your application from end to end
- Implement best practices of the web frameworks you use

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Recommended sessions

NET315 – **Strengthen your web application defenses using AWS WAF**

BOA326 – **Lift and shift a web application to serverless: Yes, it's possible!**

STP203 – **Security from day one: Establishing a baseline**

SEC317 – **Implementing traffic inspection capabilities at scale on AWS**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.