AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

COM303

Be prepared: Security is shifting left

Gert Leenders
Solutions Architect, Cofounder of Element7, and AWS DevTools Hero
DPG Media IT

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- A word on security and shifting left
- Git
- CI/CD
- DTAP
- Day to day
- A word on architecture
- How to respond

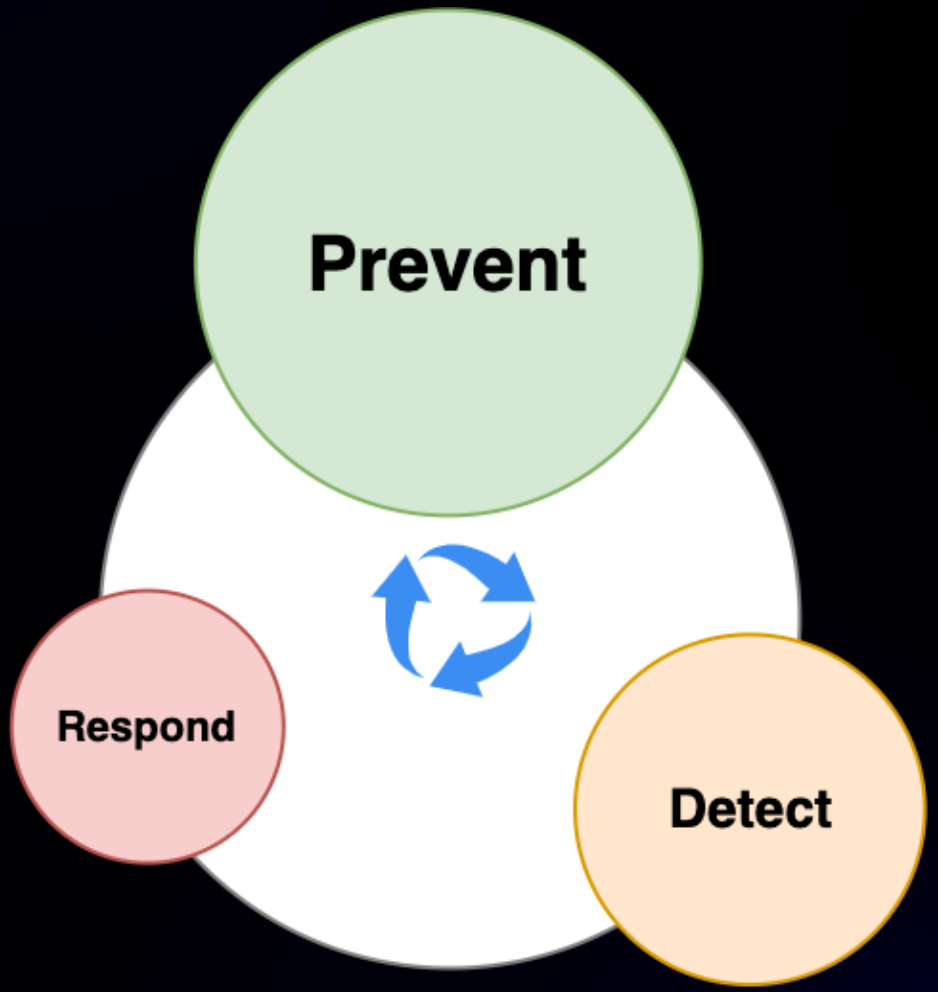
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- A word on security and shifting left
- Git
- CI/CD
- DTAP
- Day to day
- A word on architecture
- How to respond

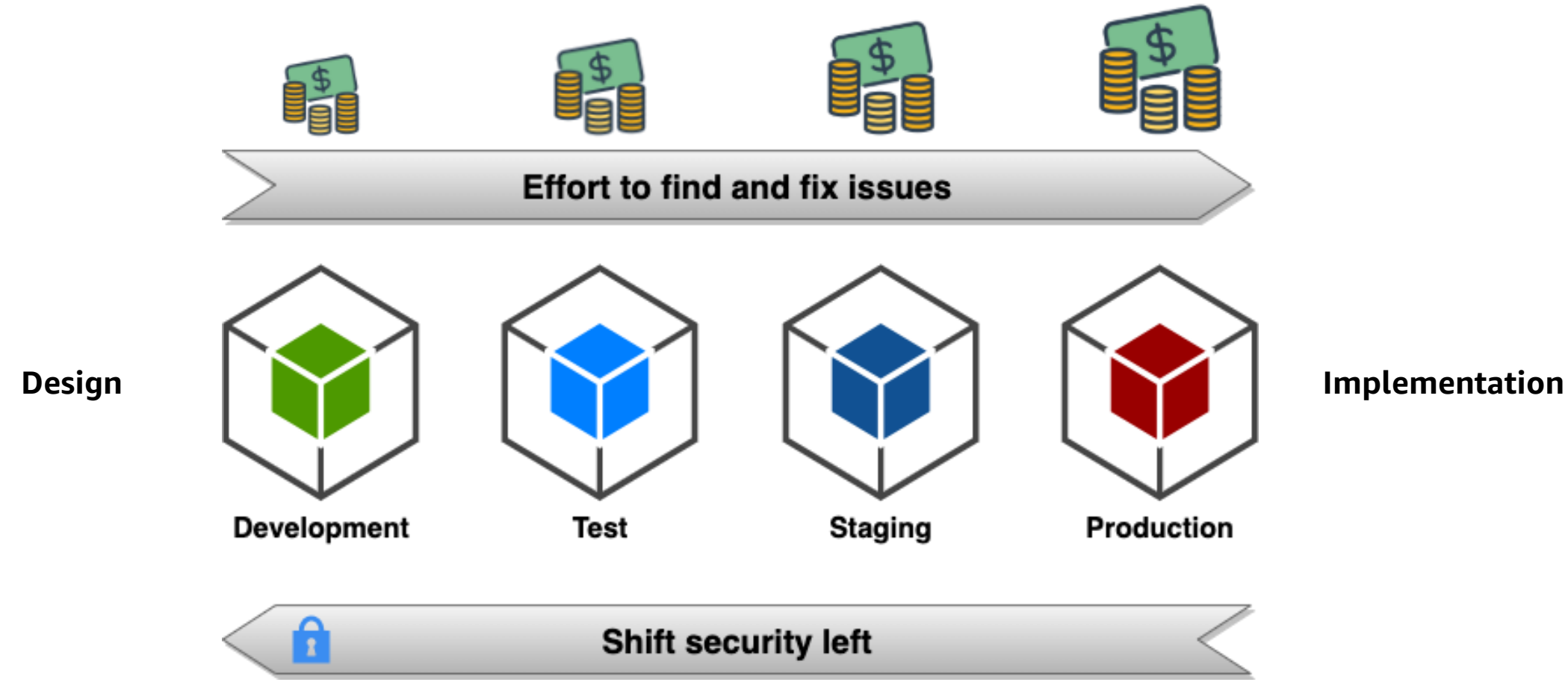
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A word on security



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A word on security shifting left



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Embrace YBIYRI

Cross-functional teams
YBIYRI



DevOps





Security

Extra skills & time

SecDevOps

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

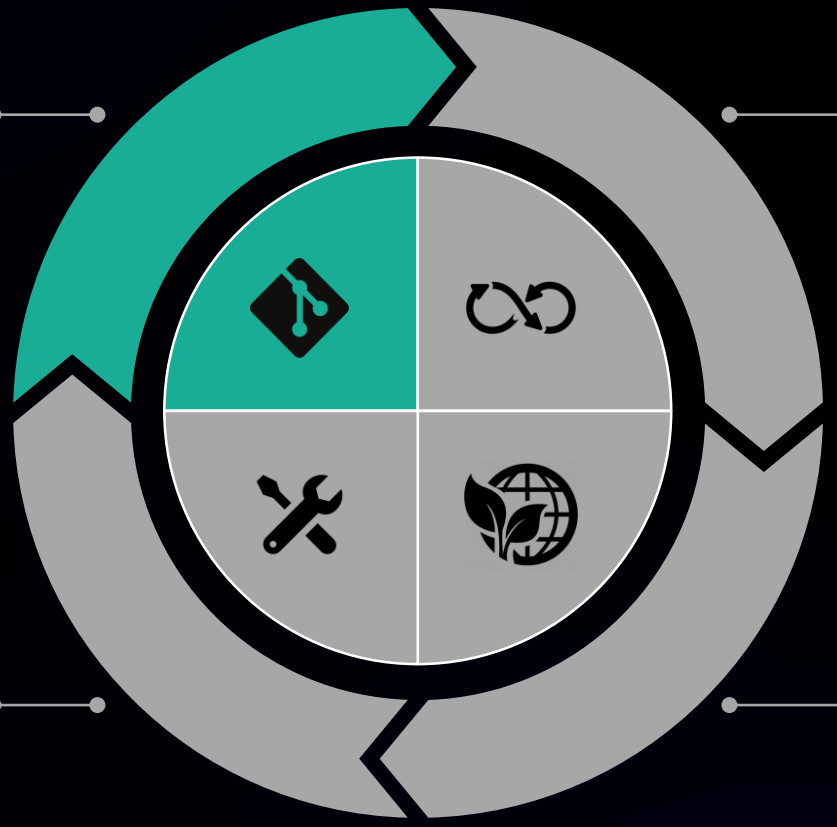
Agenda

- A word on security and shifting left
- **Git**
- CI/CD
- DTAP
- Day to day
- A word on architecture
- How to respond

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

SDLC: Git

GIT
Single source of truth GitOps
infrastructure as code (IaC)



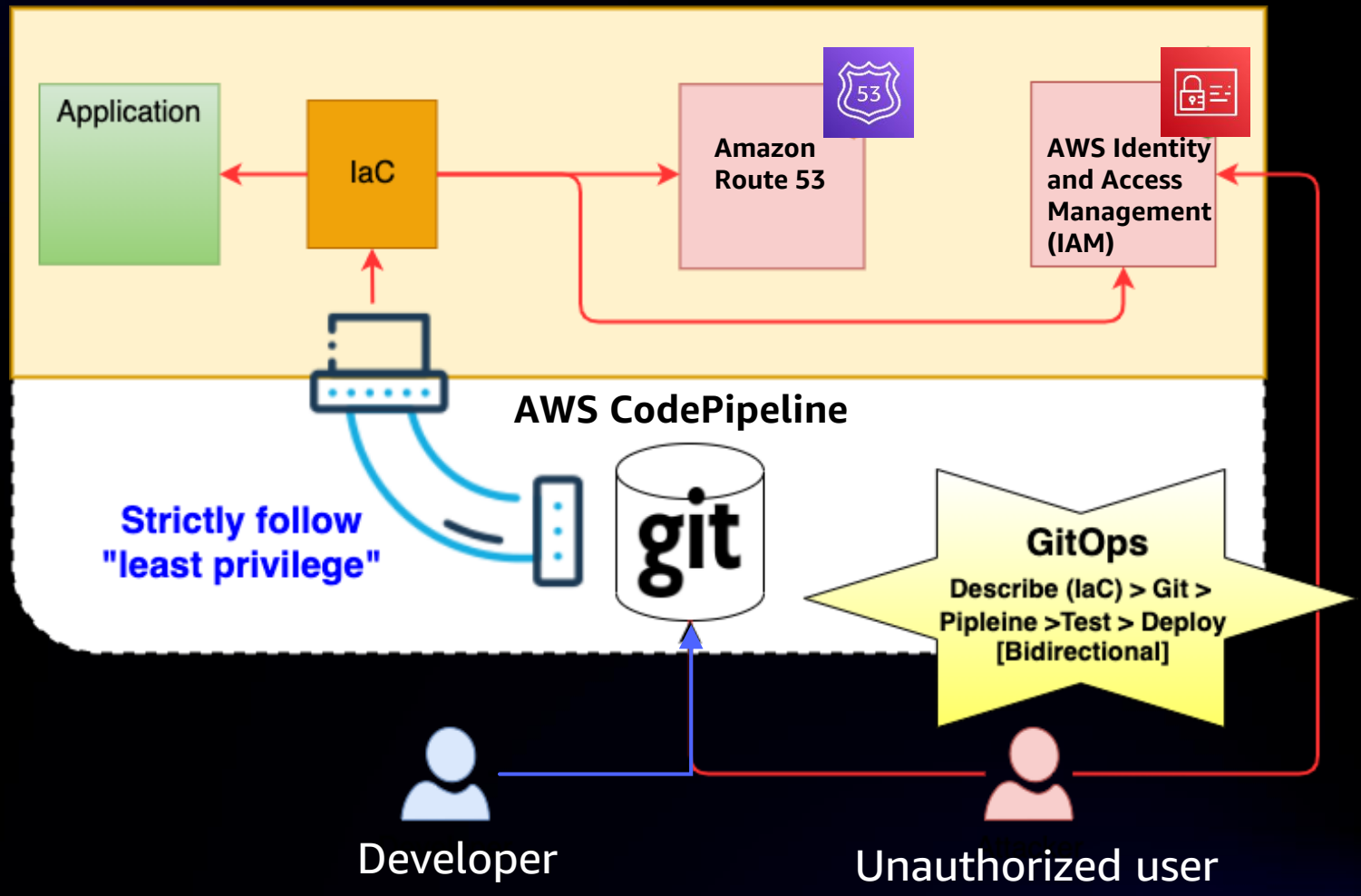
CI/CD
Continuous integration
and continuous delivery

Maintenance
Application maintenance
CSPM

DTAP
Development, test,
acceptance, production

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Git: A possible backdoor



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Git: Only commit secure code

Pick your tools for IaC





github.com/toniblyx/my-arsenal-of-aws-security-tools

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

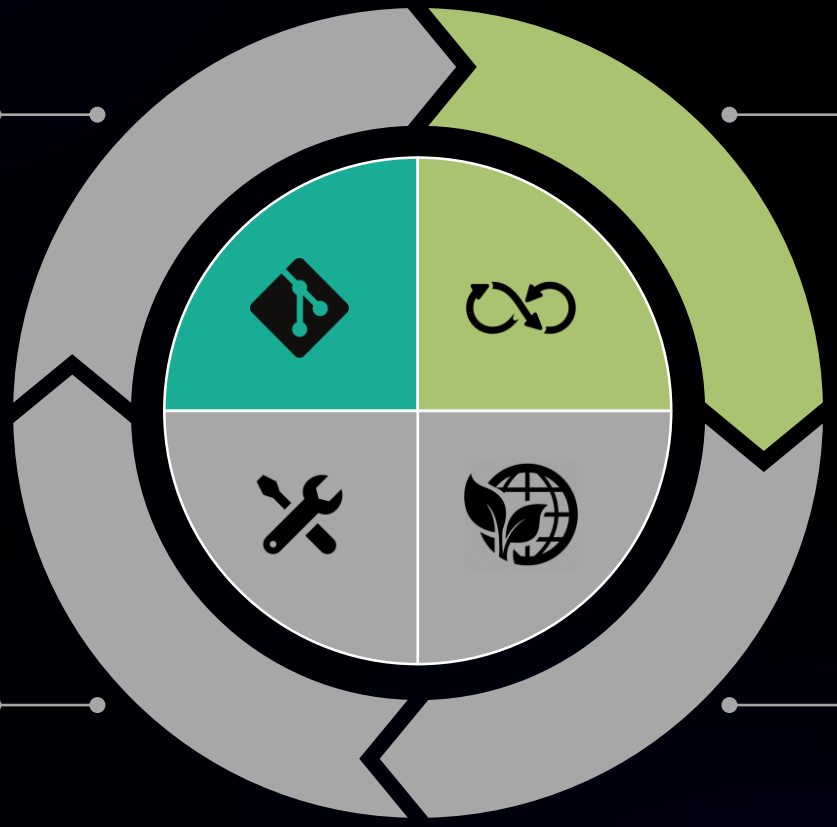
Agenda

- A word on security and shifting left
- Git
- **CI/CD**
- DTAP
- Day to day
- A word on architecture
- How to respond

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

SDLC: CI/CD

GIT
Single source of truth GitOps
infrastructure as code (IaC)



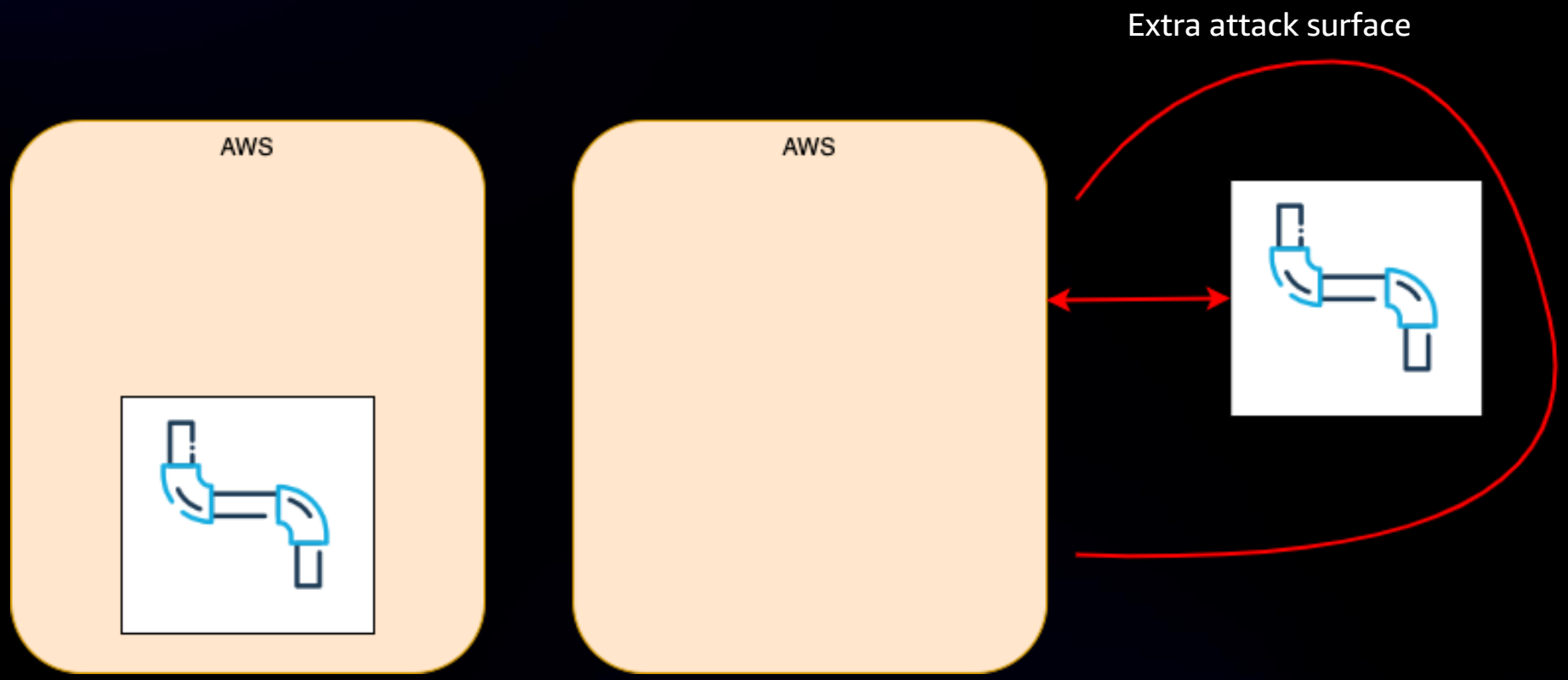
CI/CD
Continuous integration
and continuous delivery

Maintenance
Application maintenance
CSPM

DTAP
Development, test,
acceptance, production

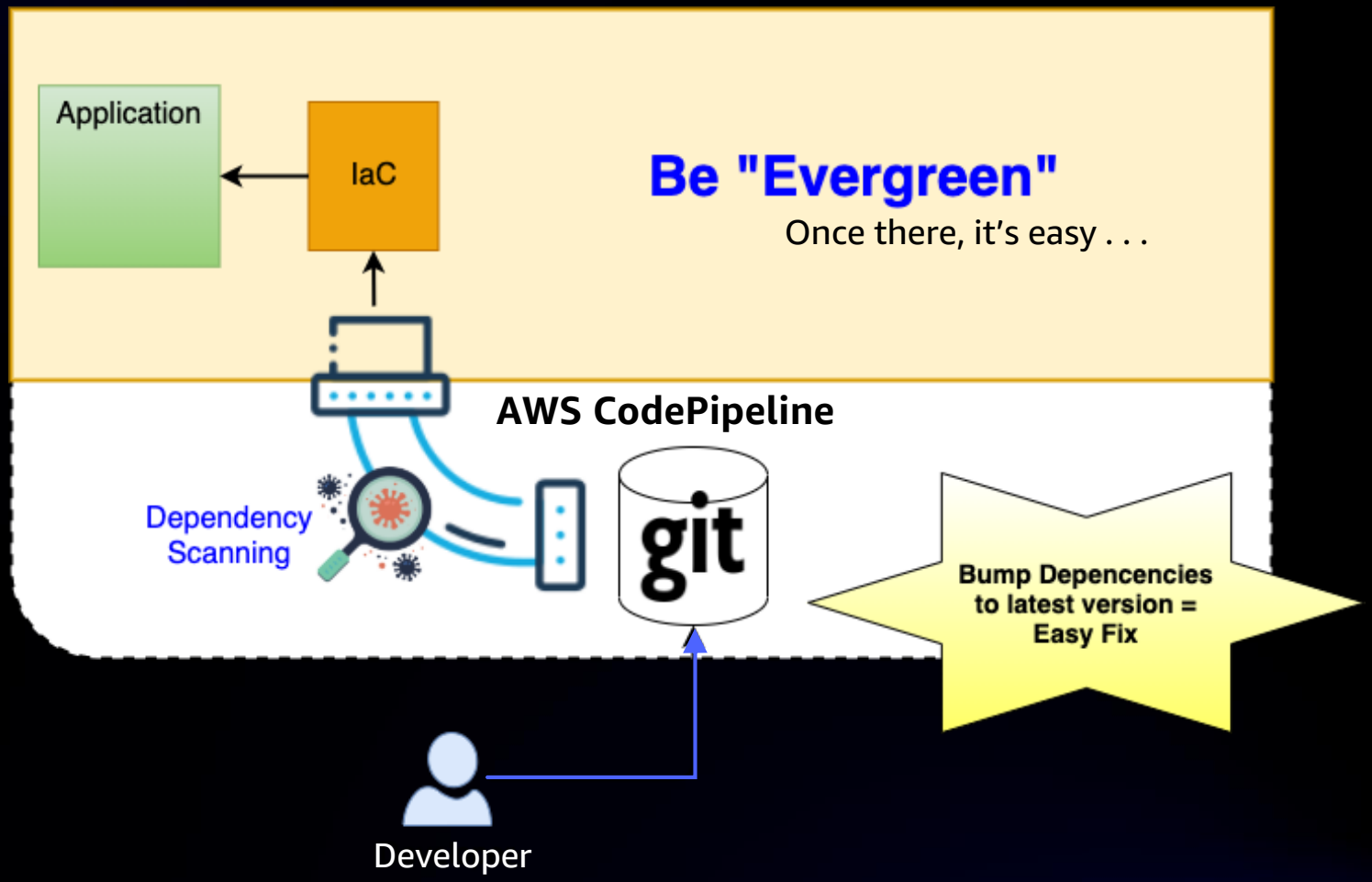
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CI/CD pipeline design: Limit attack surface



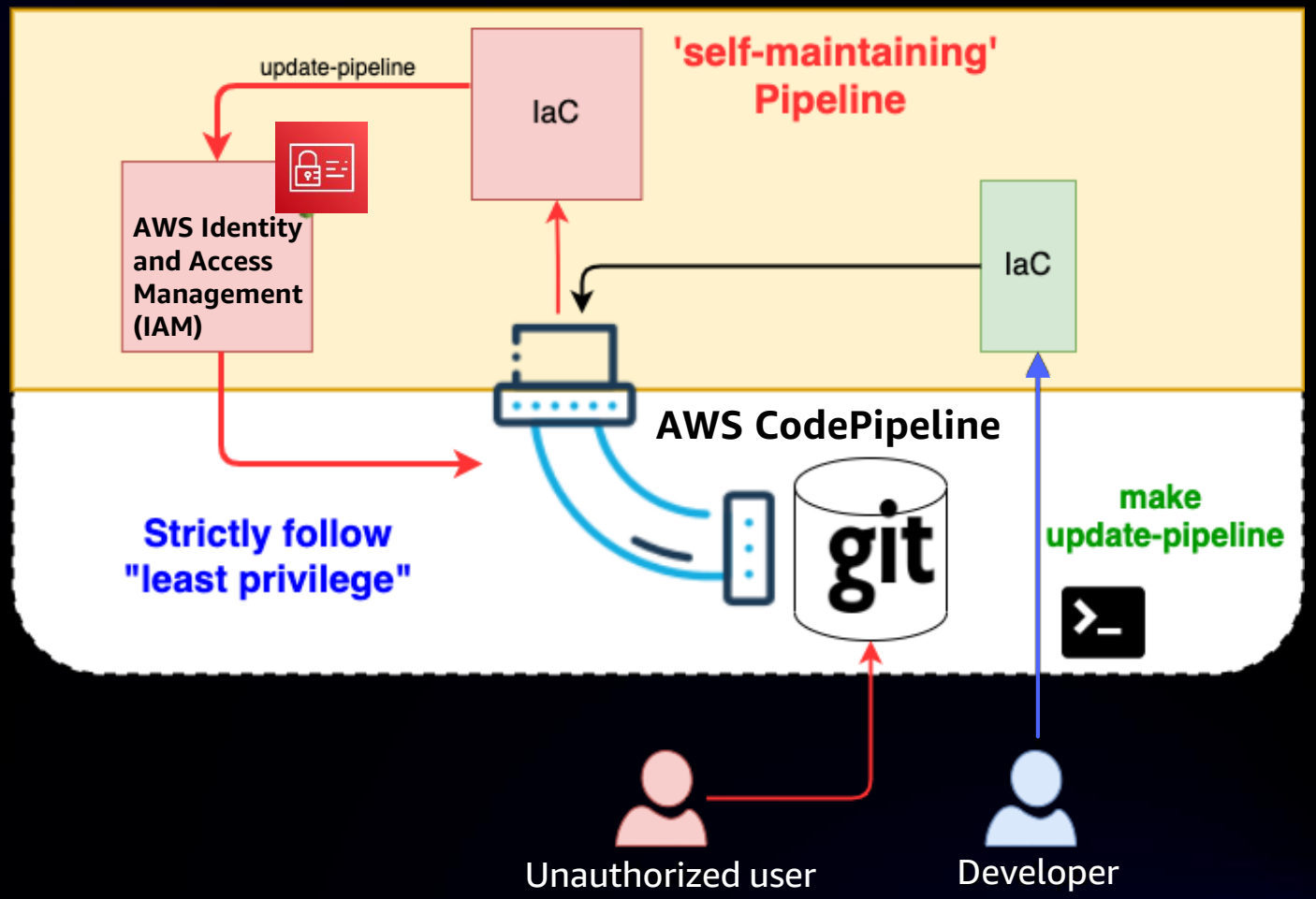
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CI/CD pipeline design: Evergreen



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CI/CD pipeline design: Self-maintaining



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

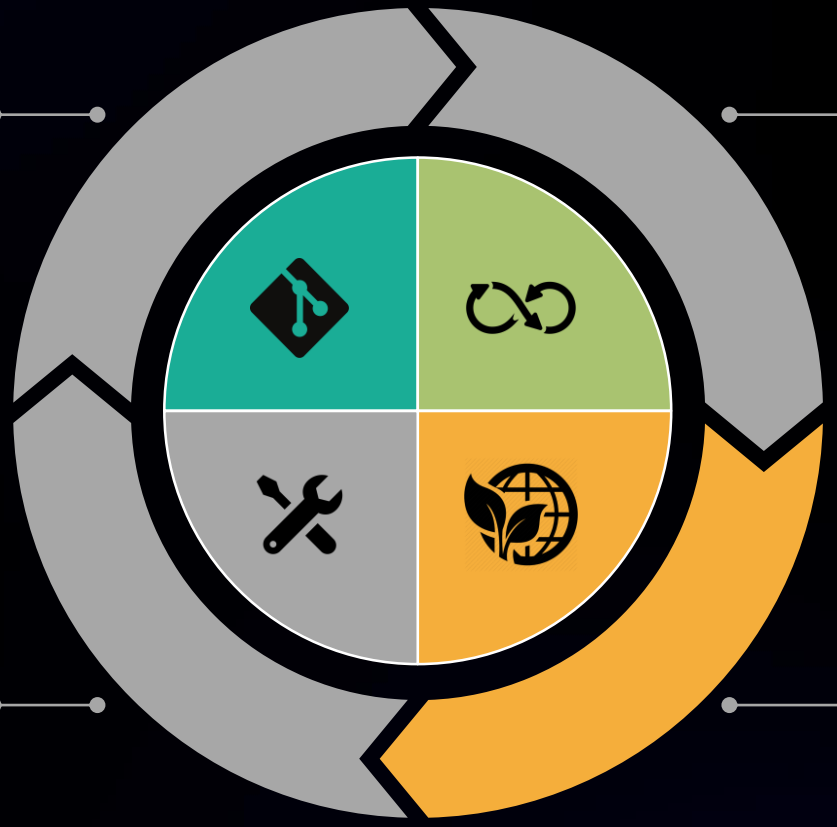
Agenda

- A word on security and shifting left
- Git
- CI/CD
- **DTAP**
- Day to day
- A word on architecture
- How to respond

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

SDLC: DTAP

GIT
Single source of truth GitOps
infrastructure as code (IaC)



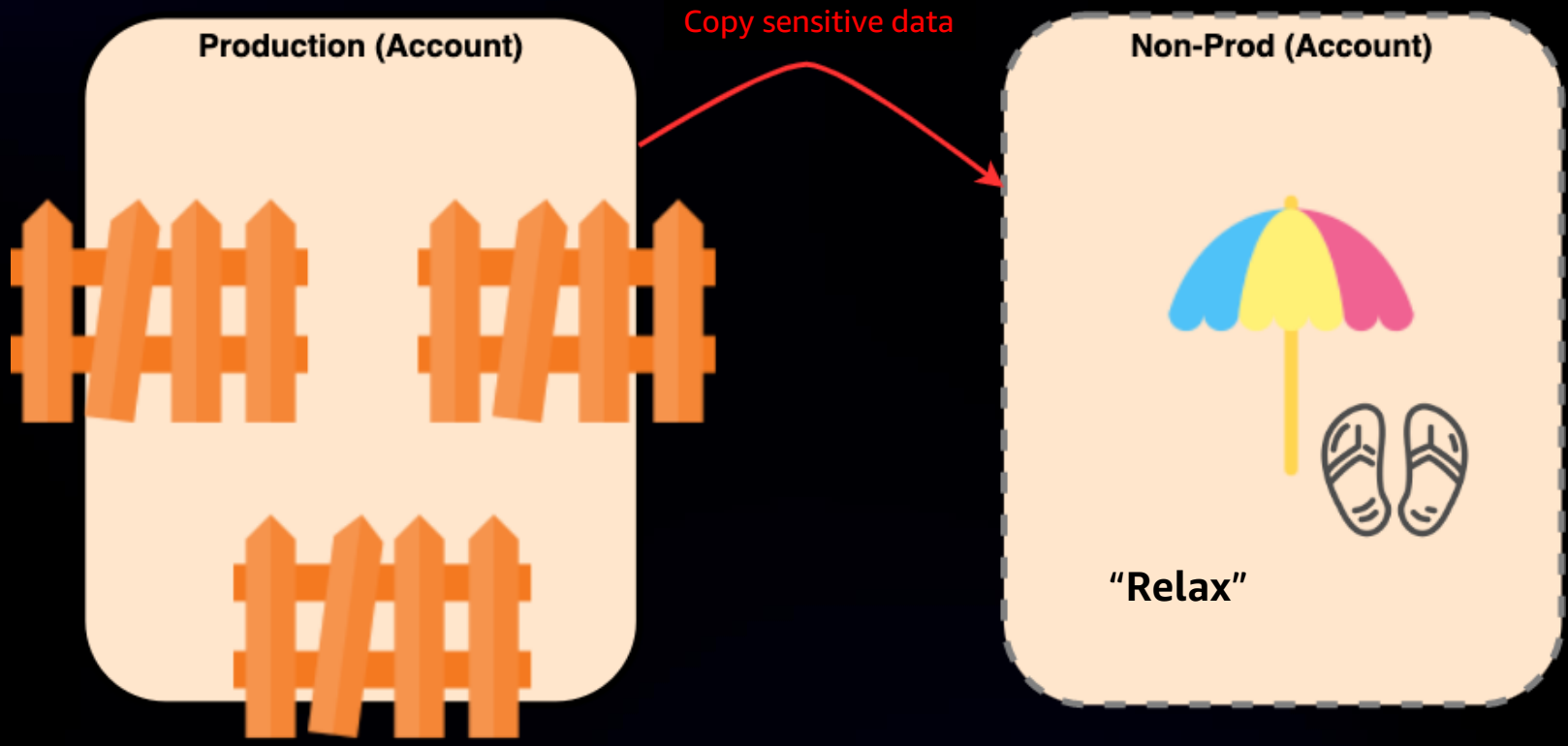
CI/CD
Continuous integration
and continuous delivery

Maintenance
Application maintenance
CSPM

DTAP
Development, test,
acceptance, production

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

DTAP: Close encounters



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

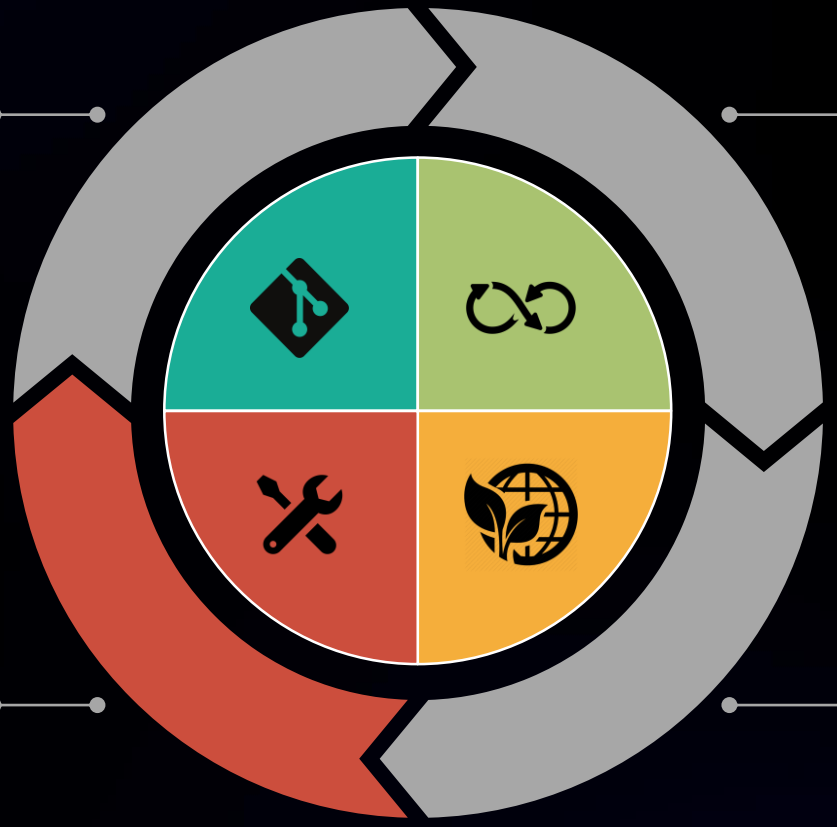
Agenda

- A word on security and shifting left
- Git
- CI/CD
- DTAP
- **Day to day**
- A word on architecture
- How to respond

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

SDLC: Maintenance

GIT
Single source of truth GitOps
infrastructure as code (IaC)



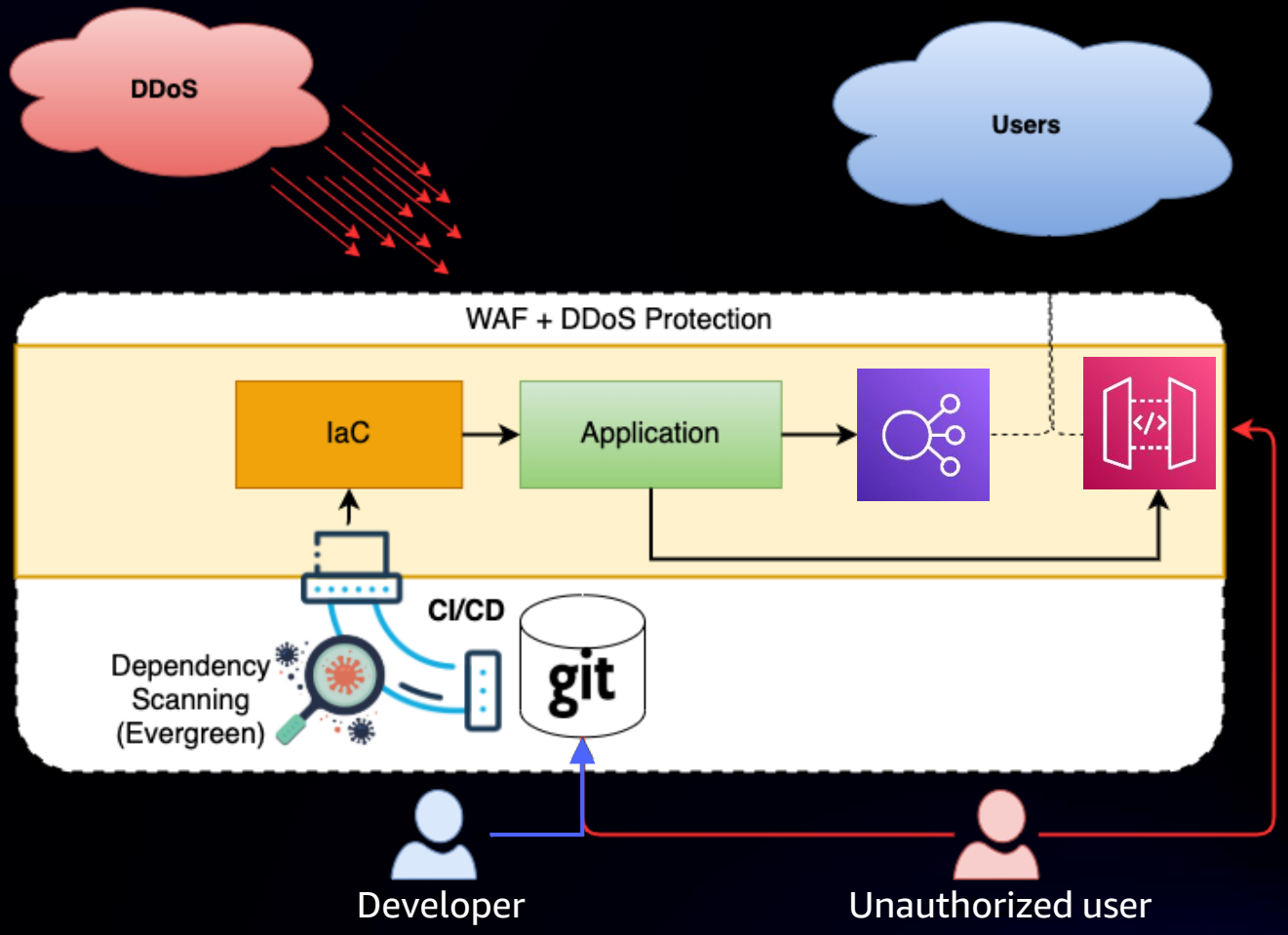
CI/CD
Continuous integration
and continuous delivery

Maintenance
Application maintenance
CSPM

DTAP
Development, test,
acceptance, production

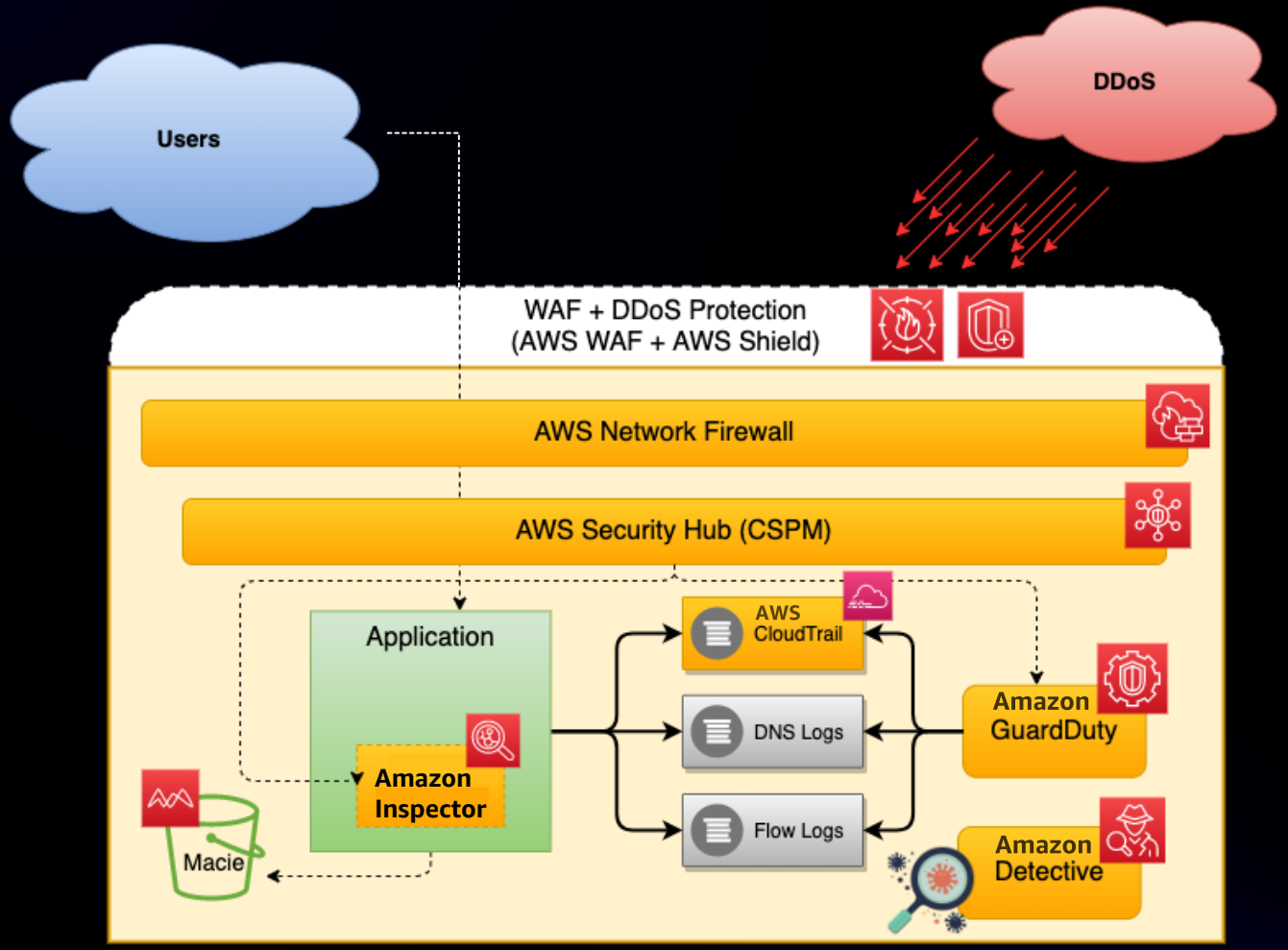
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Know your application's attack surface



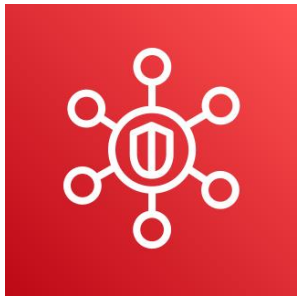
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Surround yourself with the proper services



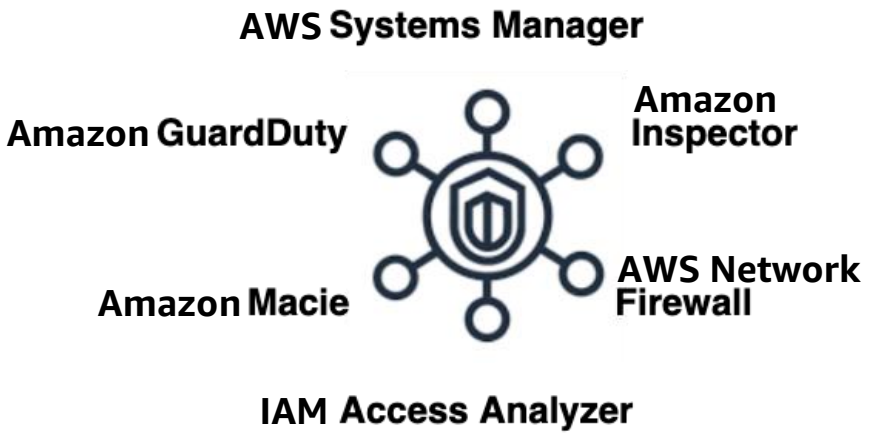
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CSPM: It's all about attitude



AWS Security Hub

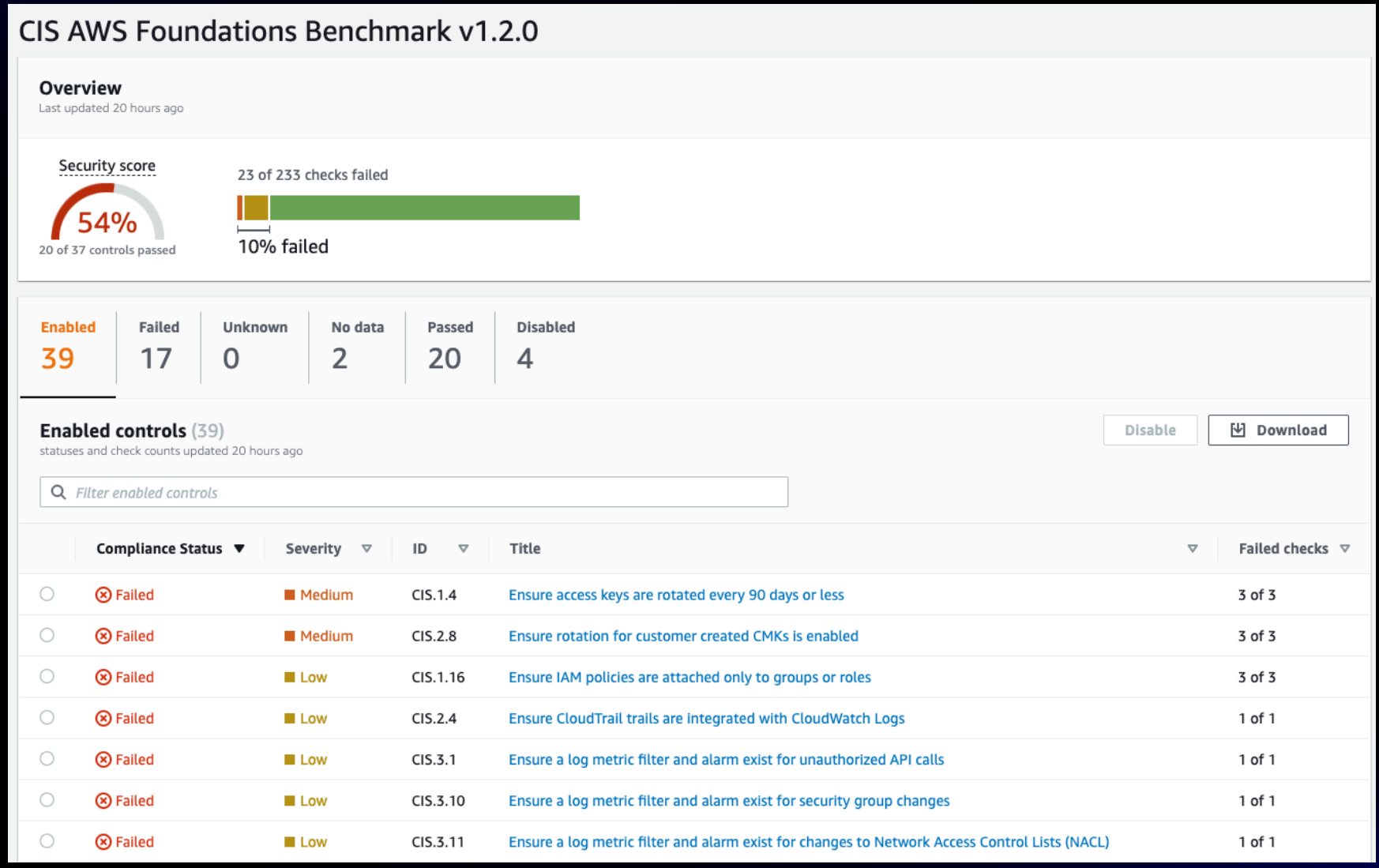




Standard	Passed	Failed	Score ▲
AWS Foundational Security Best Practices v1.0.0	86	26	77%
CIS AWS Foundations Benchmark v1.2.0	33	4	89%

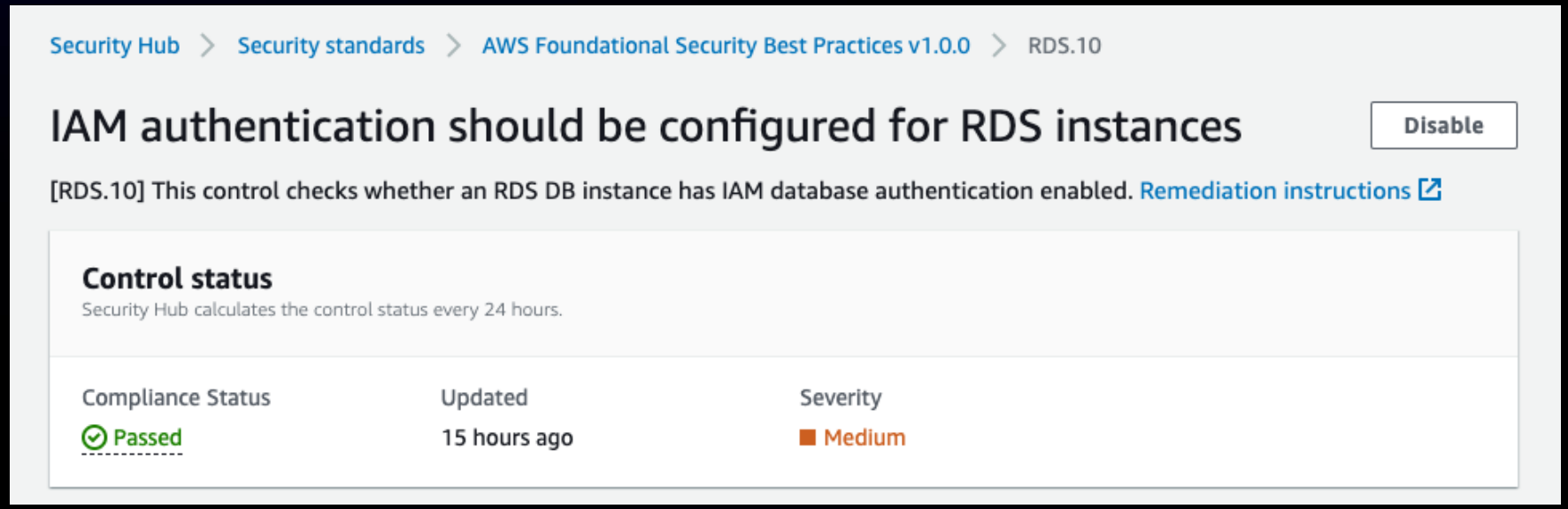
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CSPM: AWS Security Hub is your guide



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CSPM: It’s not all that obvious



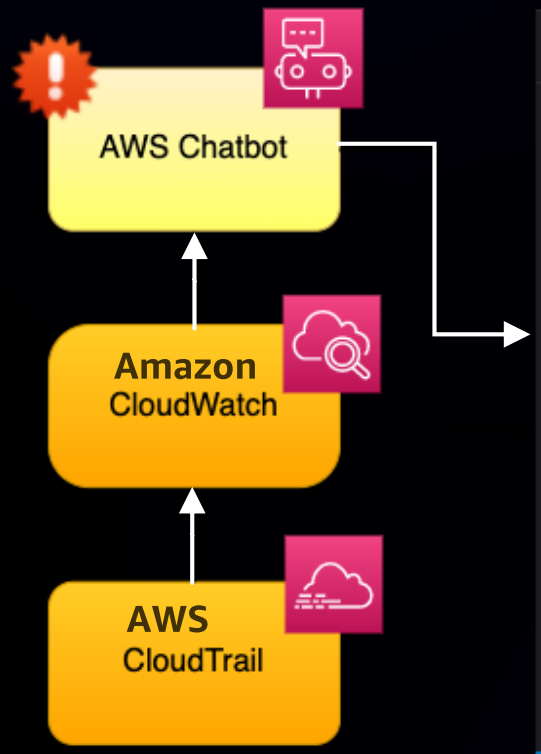
Think twice

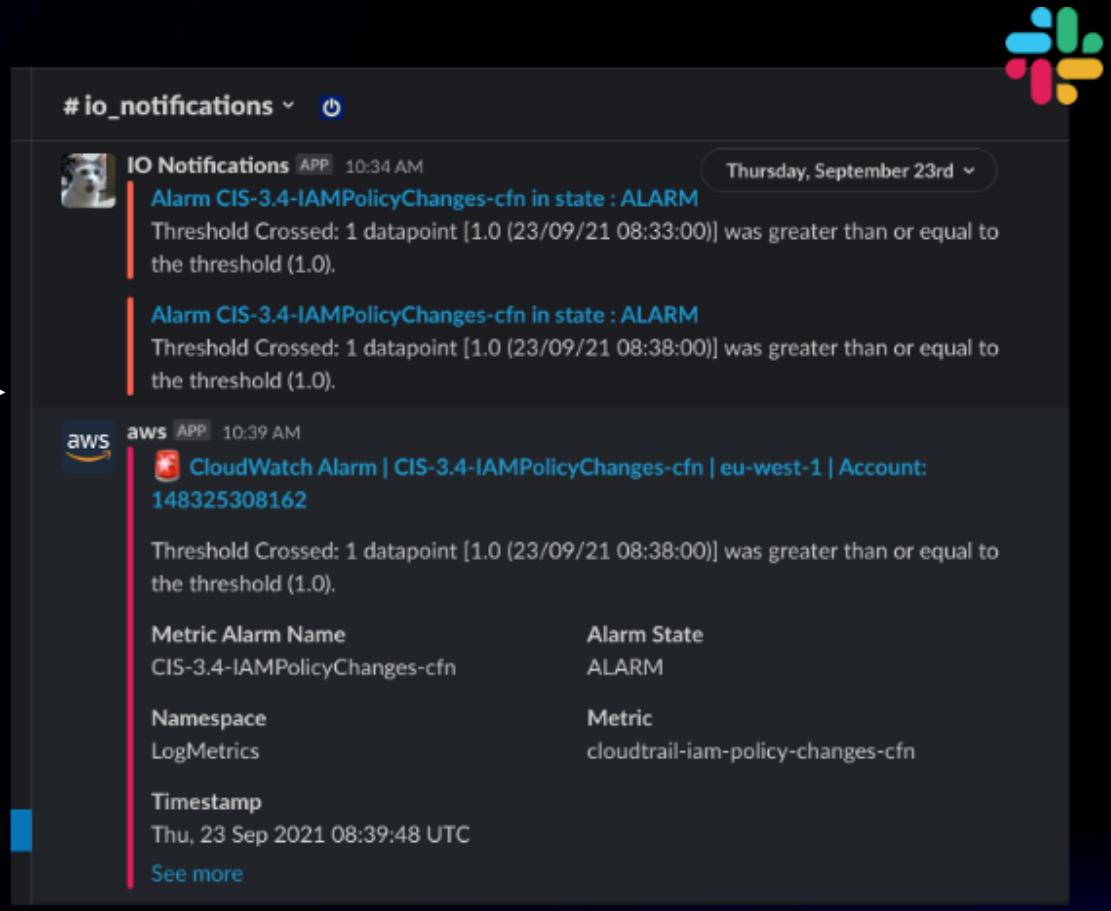
Ask yourself: What risk am I mitigating here?

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CSPM: Create awareness

[CIS.3.10] Ensure a log metric filter and alarm exist for security group changes . . .

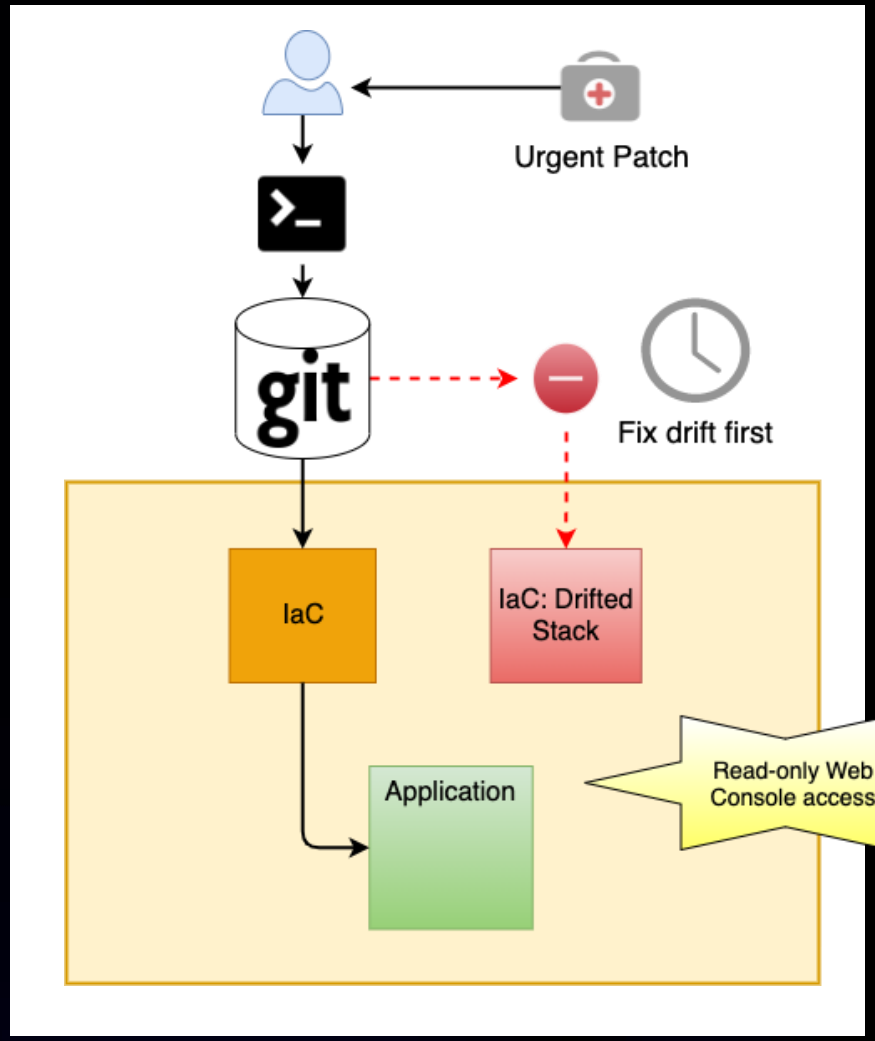




© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Avoid configuration drift

IT COULD HURT YOU IN A MAJOR WAY



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- A word on security and shifting left
- Git
- CI/CD
- DTAP
- Day to day
- **A word on architecture**
- How to respond

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



AWS Well-Architected

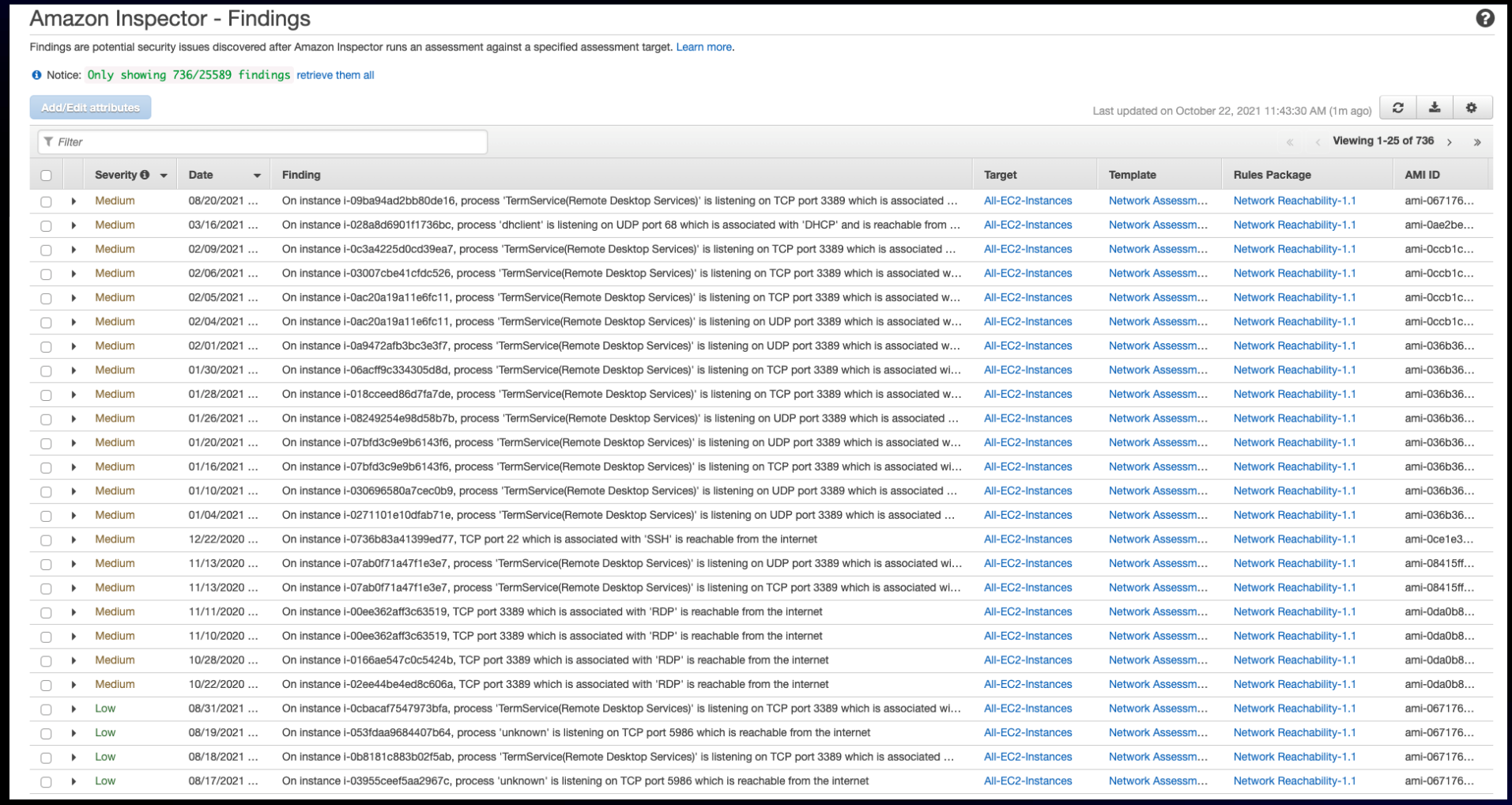
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use the AWS agents



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon Inspector



Amazon Inspector - Findings

Findings are potential security issues discovered after Amazon Inspector runs an assessment against a specified assessment target. Learn more.

Notice: `Only showing 736/25589 findings` retrieve them all

Add/Edit attributes

Last updated on October 22, 2021 11:43:30 AM (1m ago)

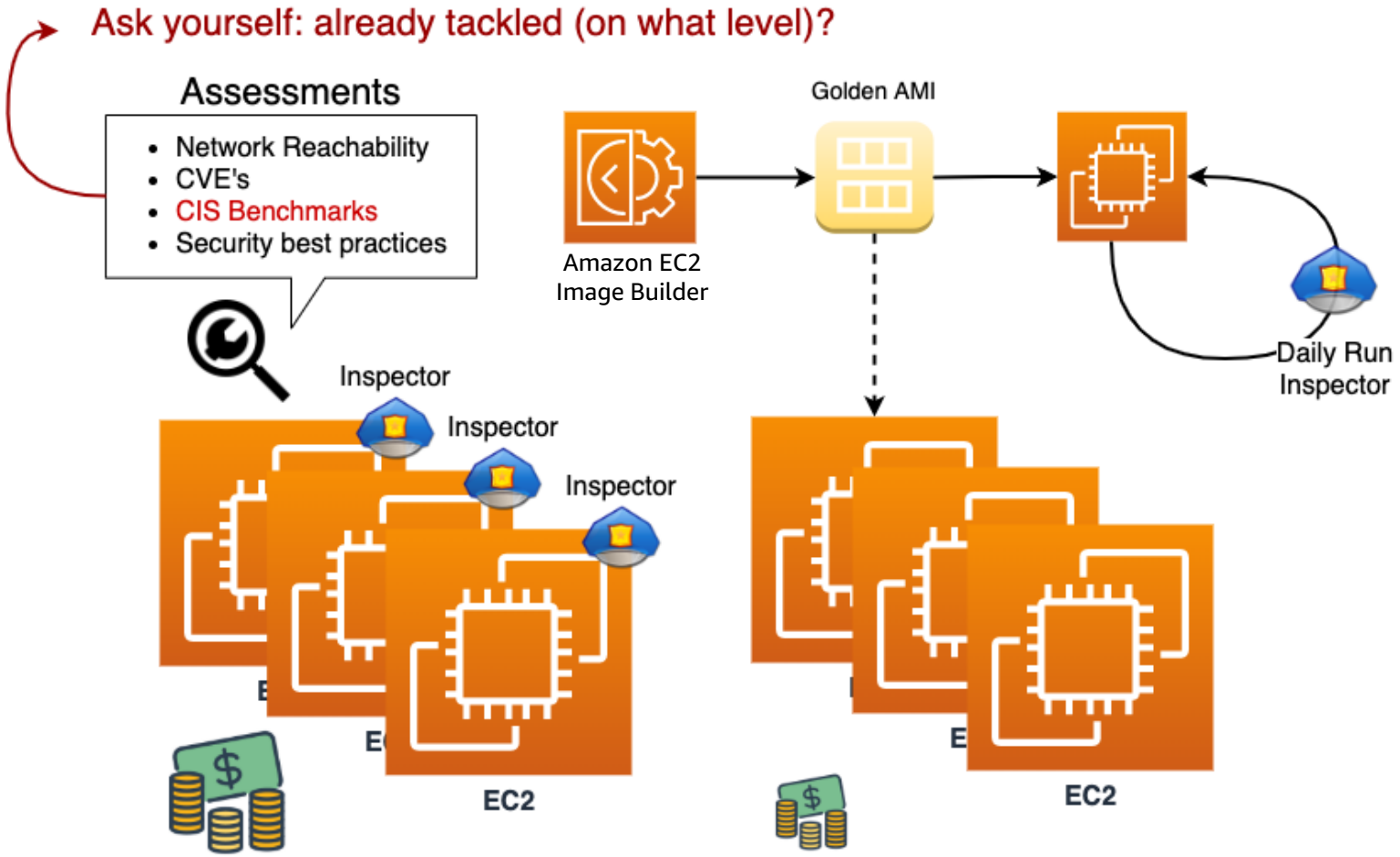
Filter

Viewing 1-25 of 736

Severity	Date	Finding	Target	Template	Rules Package	AMI ID
Medium	08/20/2021 ...	On instance i-09ba94ad2bb80de16, process 'TermService(Remote Desktop Services)' is listening on TCP port 3389 which is associated ...	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-067176...
Medium	03/16/2021 ...	On instance i-028a8d6901f1736bc, process 'dhclient' is listening on UDP port 68 which is associated with 'DHCP' and is reachable from ...	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-0ae2be...
Medium	02/09/2021 ...	On instance i-0c3a4225d0cd39ea7, process 'TermService(Remote Desktop Services)' is listening on TCP port 3389 which is associated ...	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-0ccb1c...
Medium	02/06/2021 ...	On instance i-03007cbe41cfdc526, process 'TermService(Remote Desktop Services)' is listening on TCP port 3389 which is associated w...	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-0ccb1c...
Medium	02/05/2021 ...	On instance i-0ac20a19a11e6fc11, process 'TermService(Remote Desktop Services)' is listening on TCP port 3389 which is associated w...	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-0ccb1c...
Medium	02/04/2021 ...	On instance i-0ac20a19a11e6fc11, process 'TermService(Remote Desktop Services)' is listening on UDP port 3389 which is associated w...	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-0ccb1c...
Medium	02/01/2021 ...	On instance i-0a9472afb3bc3e3f7, process 'TermService(Remote Desktop Services)' is listening on UDP port 3389 which is associated w...	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-036b36...
Medium	01/30/2021 ...	On instance i-06acff9c334305d8d, process 'TermService(Remote Desktop Services)' is listening on TCP port 3389 which is associated wi...	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-036b36...
Medium	01/28/2021 ...	On instance i-018cceed86d7fa7de, process 'TermService(Remote Desktop Services)' is listening on TCP port 3389 which is associated w...	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-036b36...
Medium	01/26/2021 ...	On instance i-08249254e98d58b7b, process 'TermService(Remote Desktop Services)' is listening on UDP port 3389 which is associated ...	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-036b36...
Medium	01/20/2021 ...	On instance i-07bfd3c9e9b6143f6, process 'TermService(Remote Desktop Services)' is listening on UDP port 3389 which is associated w...	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-036b36...
Medium	01/16/2021 ...	On instance i-07bfd3c9e9b6143f6, process 'TermService(Remote Desktop Services)' is listening on TCP port 3389 which is associated wi...	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-036b36...
Medium	01/10/2021 ...	On instance i-030696580a7cec0b9, process 'TermService(Remote Desktop Services)' is listening on UDP port 3389 which is associated ...	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-036b36...
Medium	01/04/2021 ...	On instance i-0271101e10dfab71e, process 'TermService(Remote Desktop Services)' is listening on UDP port 3389 which is associated ...	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-036b36...
Medium	12/22/2020 ...	On instance i-0736b83a41399ed77, TCP port 22 which is associated with 'SSH' is reachable from the internet	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-0ce1e3...
Medium	11/13/2020 ...	On instance i-07ab0f71a47f1e3e7, process 'TermService(Remote Desktop Services)' is listening on UDP port 3389 which is associated wi...	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-08415ff...
Medium	11/13/2020 ...	On instance i-07ab0f71a47f1e3e7, process 'TermService(Remote Desktop Services)' is listening on TCP port 3389 which is associated wi...	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-08415ff...
Medium	11/11/2020 ...	On instance i-00ee362aff3c63519, TCP port 3389 which is associated with 'RDP' is reachable from the internet	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-0da0b8...
Medium	11/10/2020 ...	On instance i-00ee362aff3c63519, TCP port 3389 which is associated with 'RDP' is reachable from the internet	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-0da0b8...
Medium	10/28/2020 ...	On instance i-0166ae547c0c5424b, TCP port 3389 which is associated with 'RDP' is reachable from the internet	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-0da0b8...
Medium	10/22/2020 ...	On instance i-02ee44be4ed8c606a, TCP port 3389 which is associated with 'RDP' is reachable from the internet	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-0da0b8...
Low	08/31/2021 ...	On instance i-0cbacaf7547973bfa, process 'TermService(Remote Desktop Services)' is listening on TCP port 3389 which is associated wi...	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-067176...
Low	08/19/2021 ...	On instance i-053fdaa9684407b64, process 'unknown' is listening on TCP port 5986 which is reachable from the internet	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-067176...
Low	08/18/2021 ...	On instance i-0b8181c883b02f5ab, process 'TermService(Remote Desktop Services)' is listening on TCP port 3389 which is associated ...	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-067176...
Low	08/17/2021 ...	On instance i-03955ceef5aa2967c, process 'unknown' is listening on TCP port 5986 which is reachable from the internet	All-EC2-Instances	Network Assessm...	Network Reachability-1.1	ami-067176...

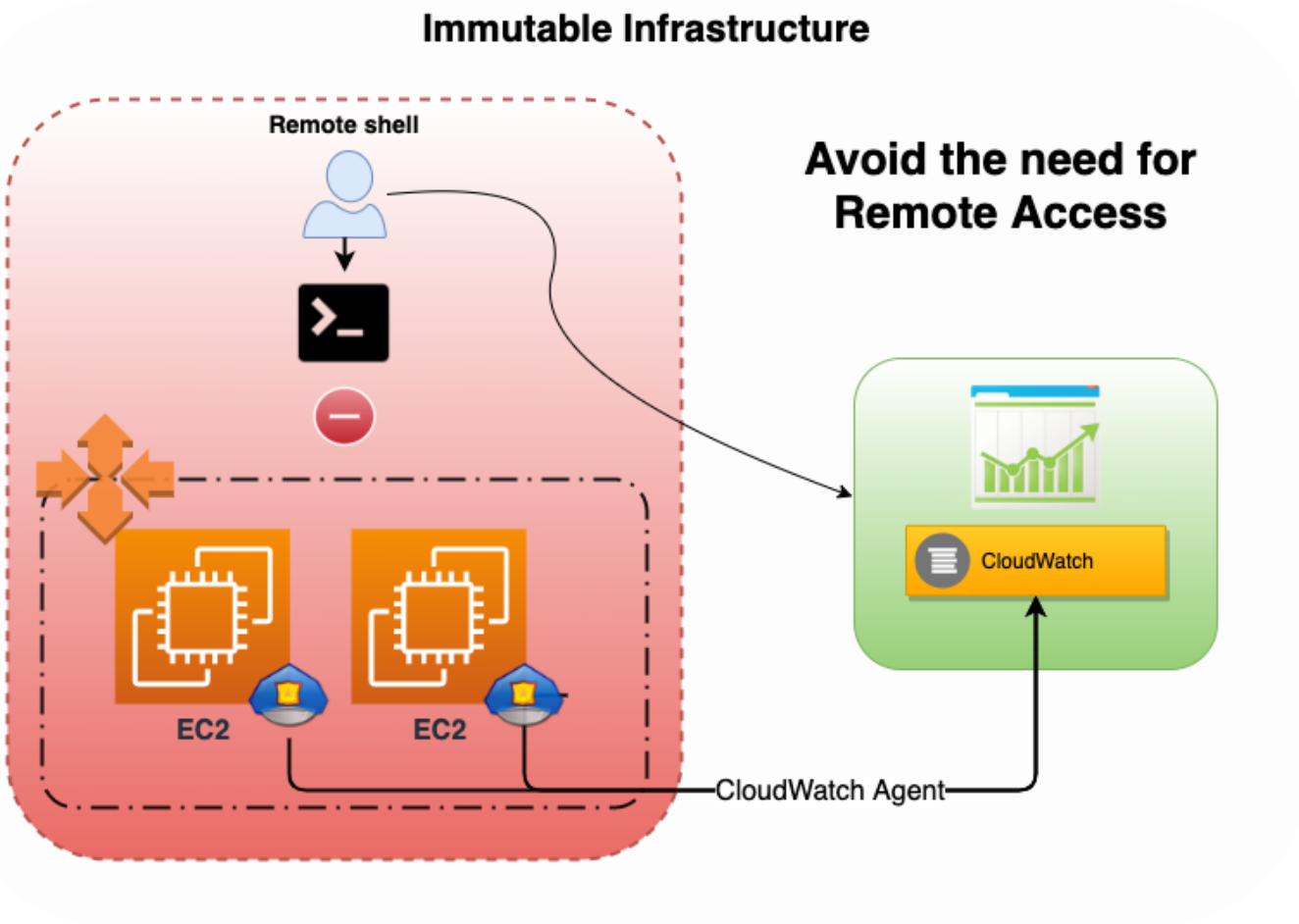
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon Inspector



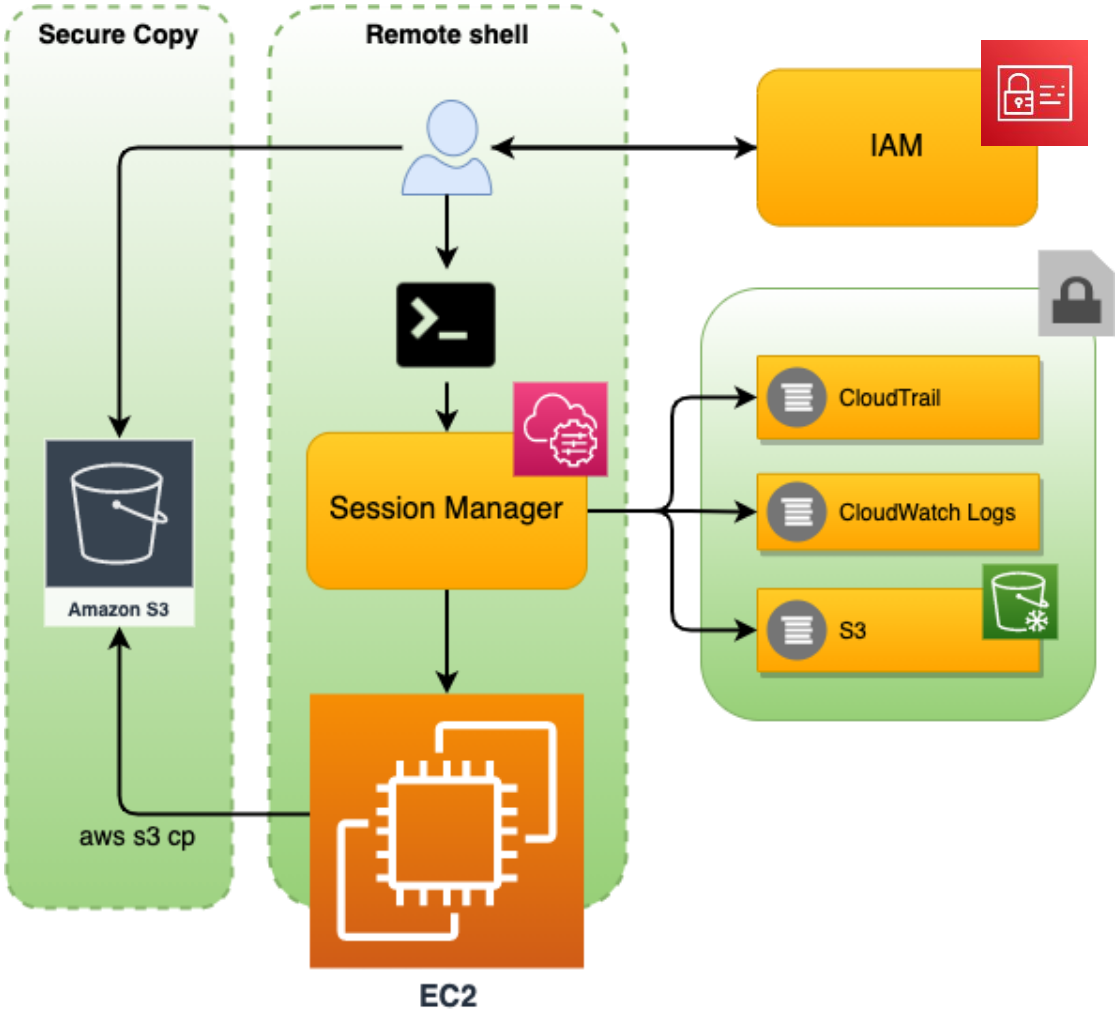
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Immutable infrastructure



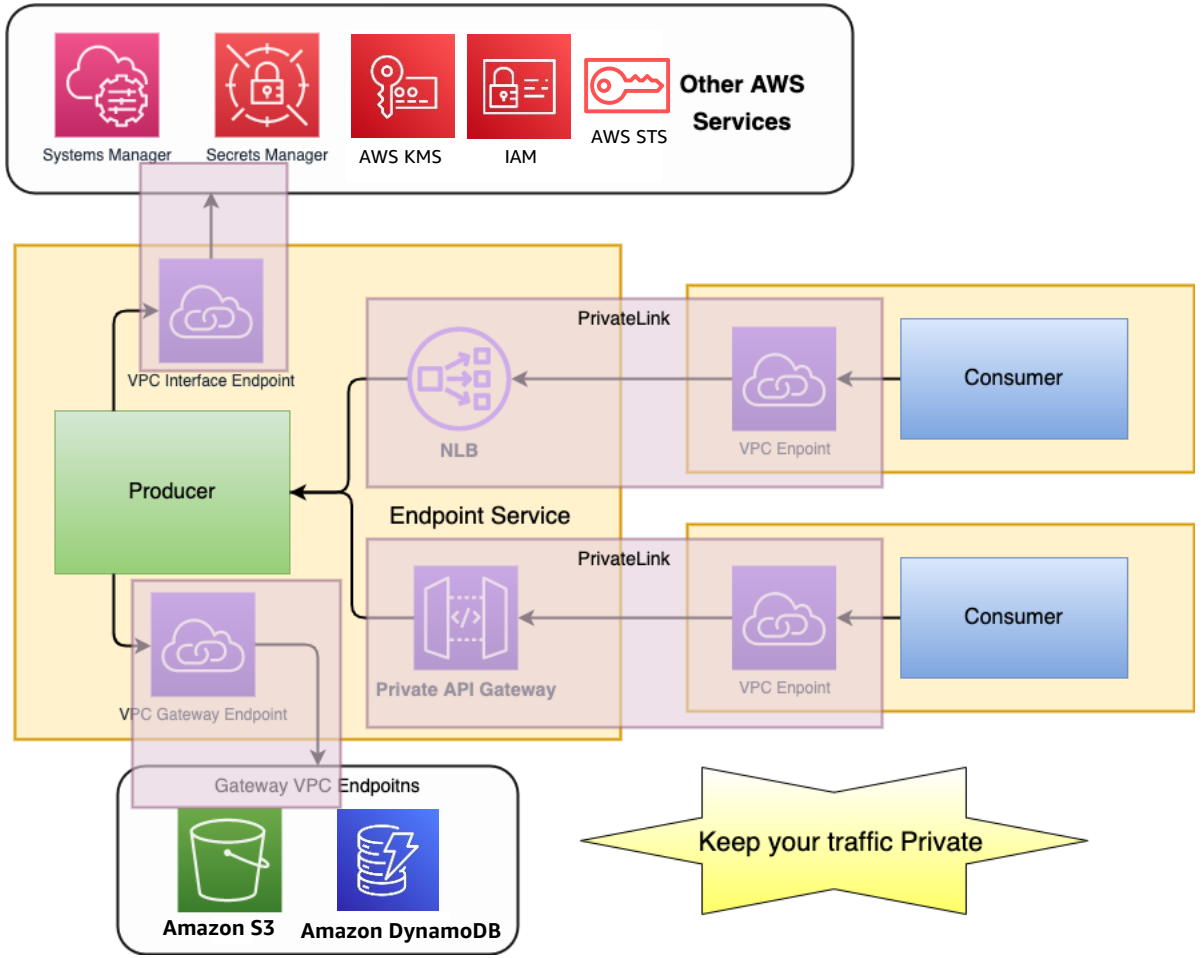
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Forget SSH, welcome Session Manager



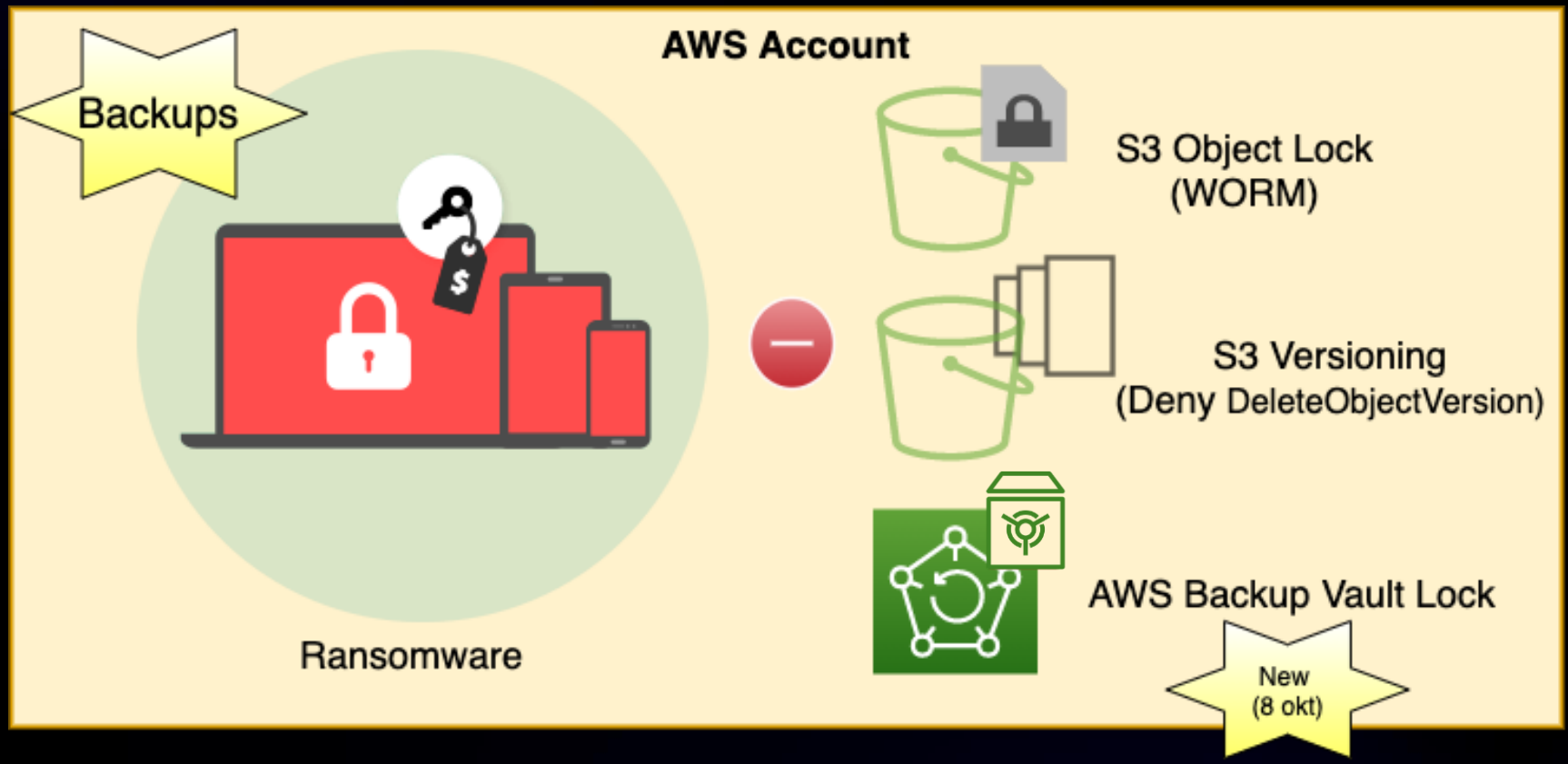
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS PrivateLink: Limit your attack surface



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Be prepared



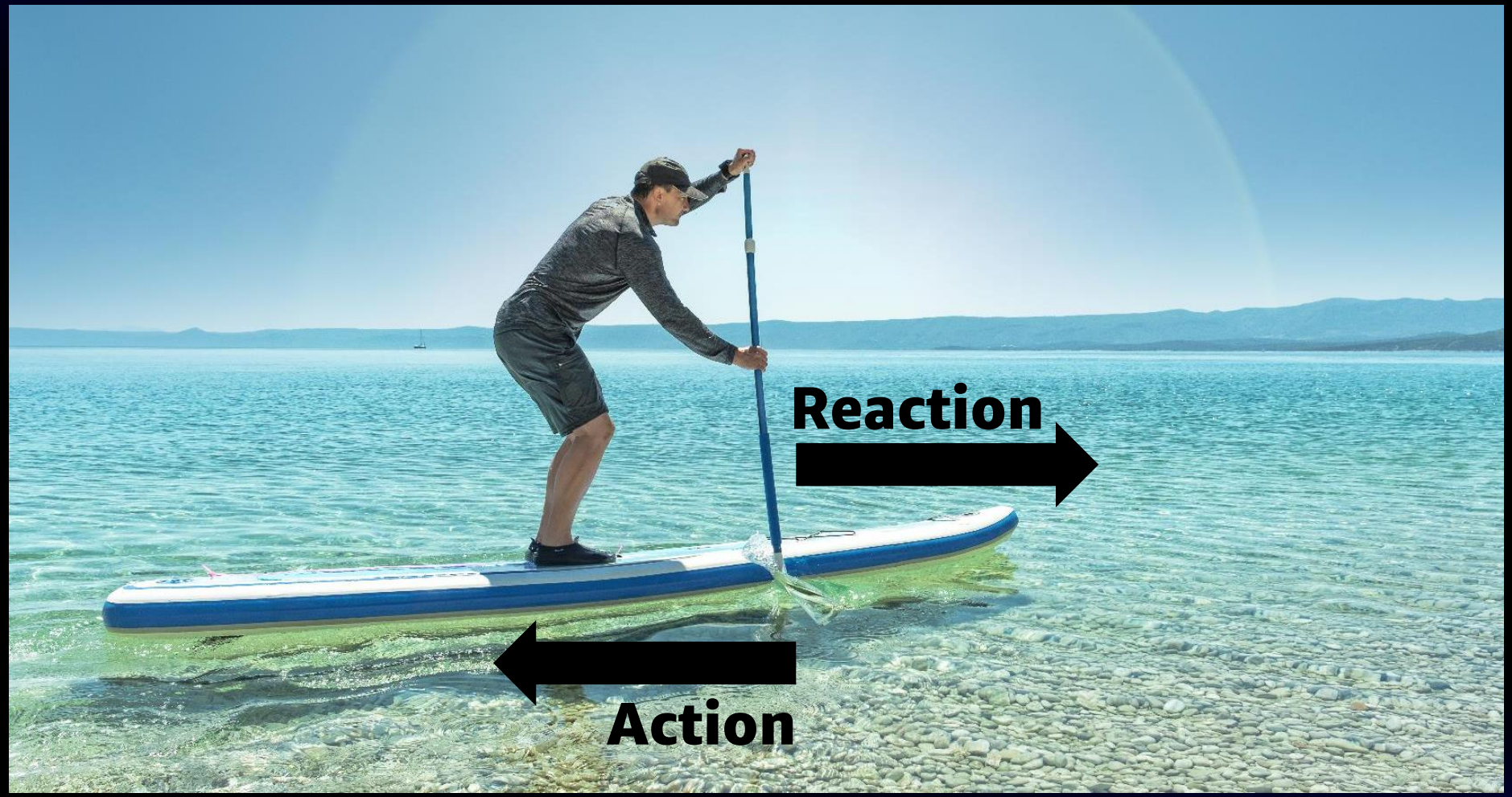
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- A word on security and shifting left
- Git
- CI/CD
- DTAP
- Day to day
- A word on architecture
- **How to respond**

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Respond



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Respond: Continuity planning

- Ensure you know the **recovery time and recovery point objective** for your service
- Have a business continuity plan (BCP) with a disaster recovery plan
- **Keep a regular fire drill for your BCP > “perfection by practice”**

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Respond: Collect (access) logs

Monitor the following activity

- Any kind of access logs
- Amazon CloudFront user requests
- Load balancer access logs
- AWS API Gateway access logs
- Amazon S3 access logs
- AWS VPC flow logs – Amazon Athena out-of-the-box integration available (https://go.aws/3EhOIyD)
- DNS query logs

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Respond: Retain access logs

Access log retention policy example using **intelligent tiering**

- First 14 days: log collector of choice (ELK, Amazon CloudWatch); easy to query
- First 6 months: Amazon S3, query capabilities with Amazon Athena; fairly easy to query
- 6 to 12 months: Amazon S3 Glacier, on-demand restore; log retrieval is harder







aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key takeaways

1. Be evergreen
2. Cover the full security cycle: prevent, detect, **respond**
3. Use AWS Security Hub (AWS CSPM)
4. Be prepared

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Any questions?

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

References

- Security, identity, and compliance on AWS: aws.amazon.com/products/security
- Protecting Amazon S3 data from ransomware: bit.ly/3nt6Yyd
- AWS security tools: github.com/toniblyx/my-arsenal-of-aws-security-tools
- Zero Trust architectures: an AWS perspective: go.aws/3Chnjw1
- Deploying CIS Level 1 hardened AMIs with Amazon EC2 Image Builder: go.aws/3Chv84V
- AWS API Gateway best practices in depth: www.element7.io/2021/06/aws-api-gateway-best-practices-in-depth
- The hidden Git backdoor in AWS CodePipeline and AWS CodeBuild: bit.ly/3bdX7Xu
- Keep up with the times: forget SSH, welcome AWS Session Manager: bit.ly/3meQLNF
- Keep up with the times: use AWS PrivateLink: bit.ly/3pGZpqu
- AWS SSM Session Manager port forwarding to RDS without SSH: bit.ly/3jGx7st
- Enhance the security posture of your backups with AWS Backup Vault Lock: go.aws/3vO6GpF

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Gert Leenders

Email: gert@element7.io
Twitter: @glnds
GitHub: https://github.com/glnds

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.