
AWS
re:Invent

WPS214

Ransomware: Be prepared

Abhi Singh

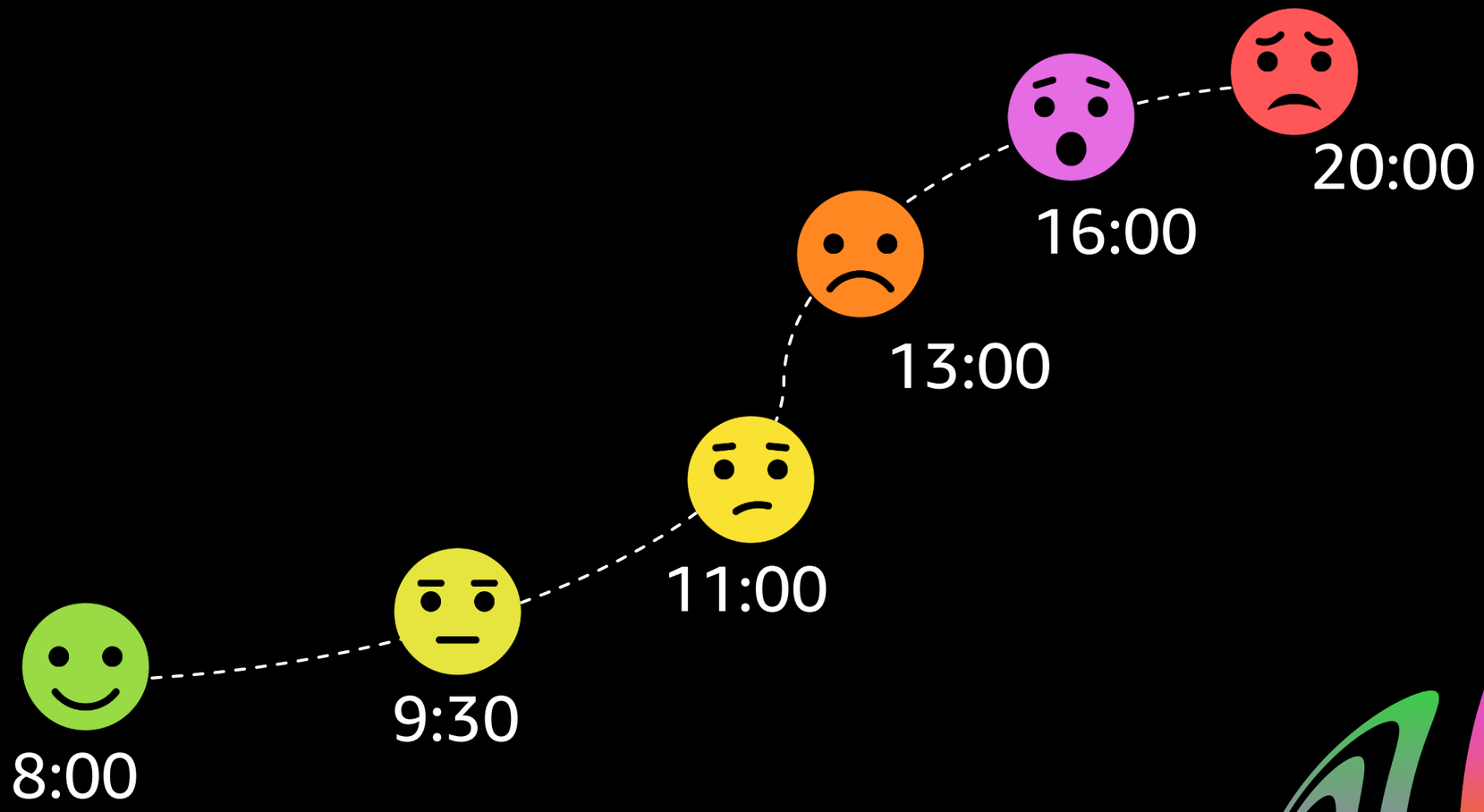
Specialist Solutions Architect

AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Once upon a time . . .



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Evolution of ransomware

Guidance from NIST 1800-25 and 1800-26

Adopting AWS guidance

Becoming proactive

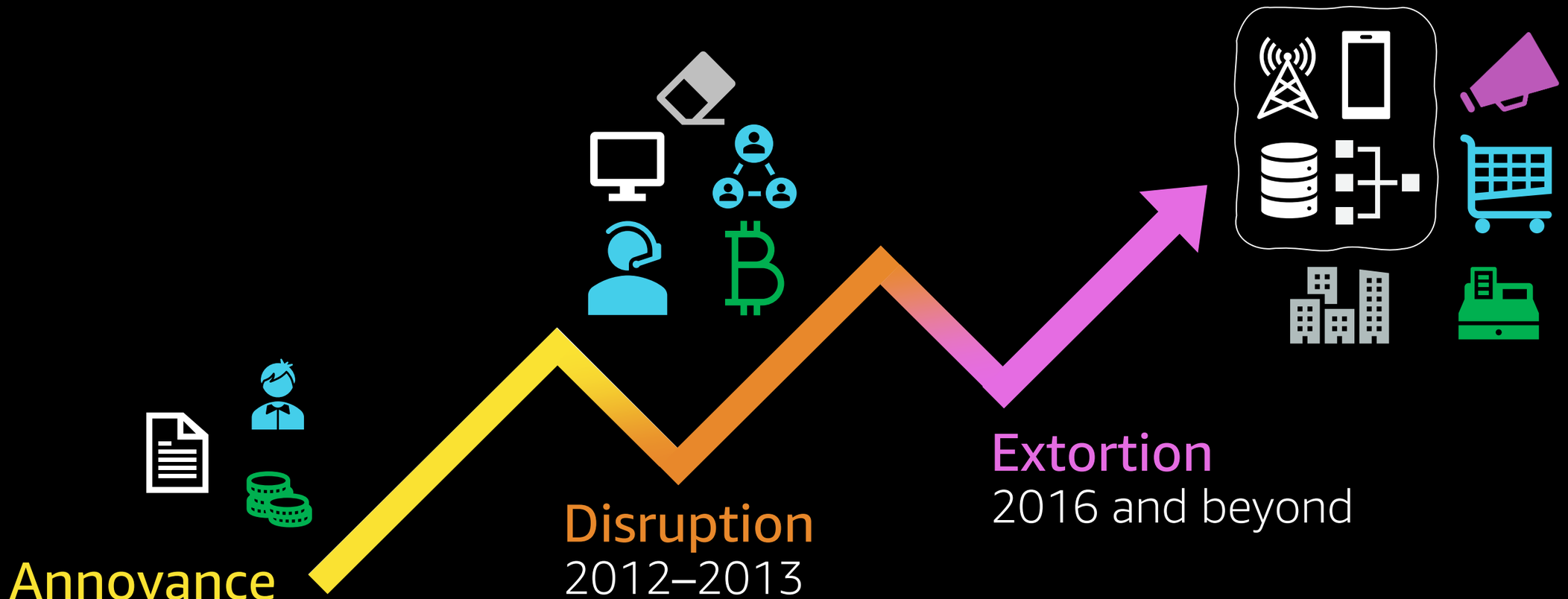
Improving detection and prevention coverage with AWS

Next steps



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ransomware –
From minor annoyance to BIG business



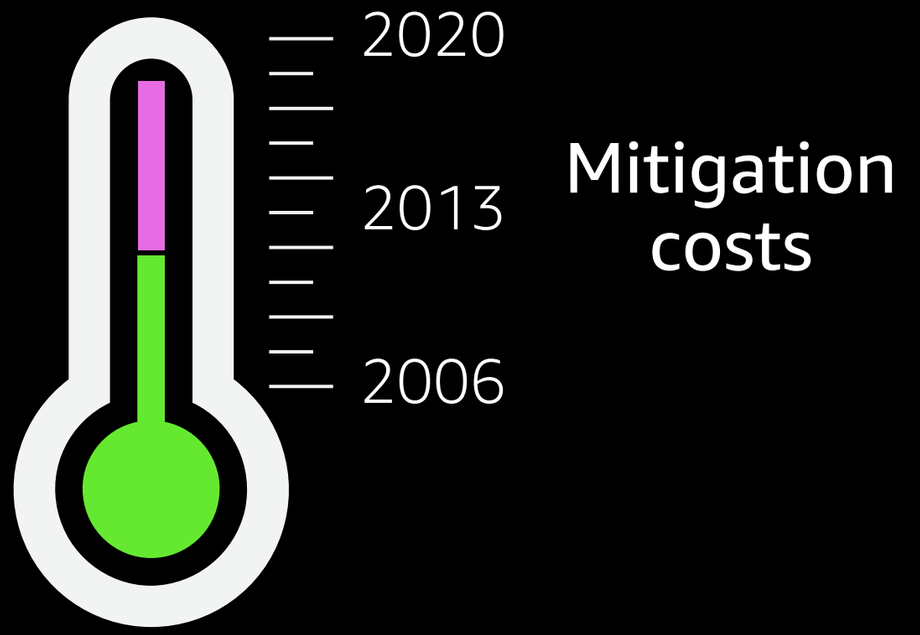
Evolution taught us a few key lessons

Early detection is the key

Prevention is better than cure

Automate assessments, recovery and response

Education and training become more important

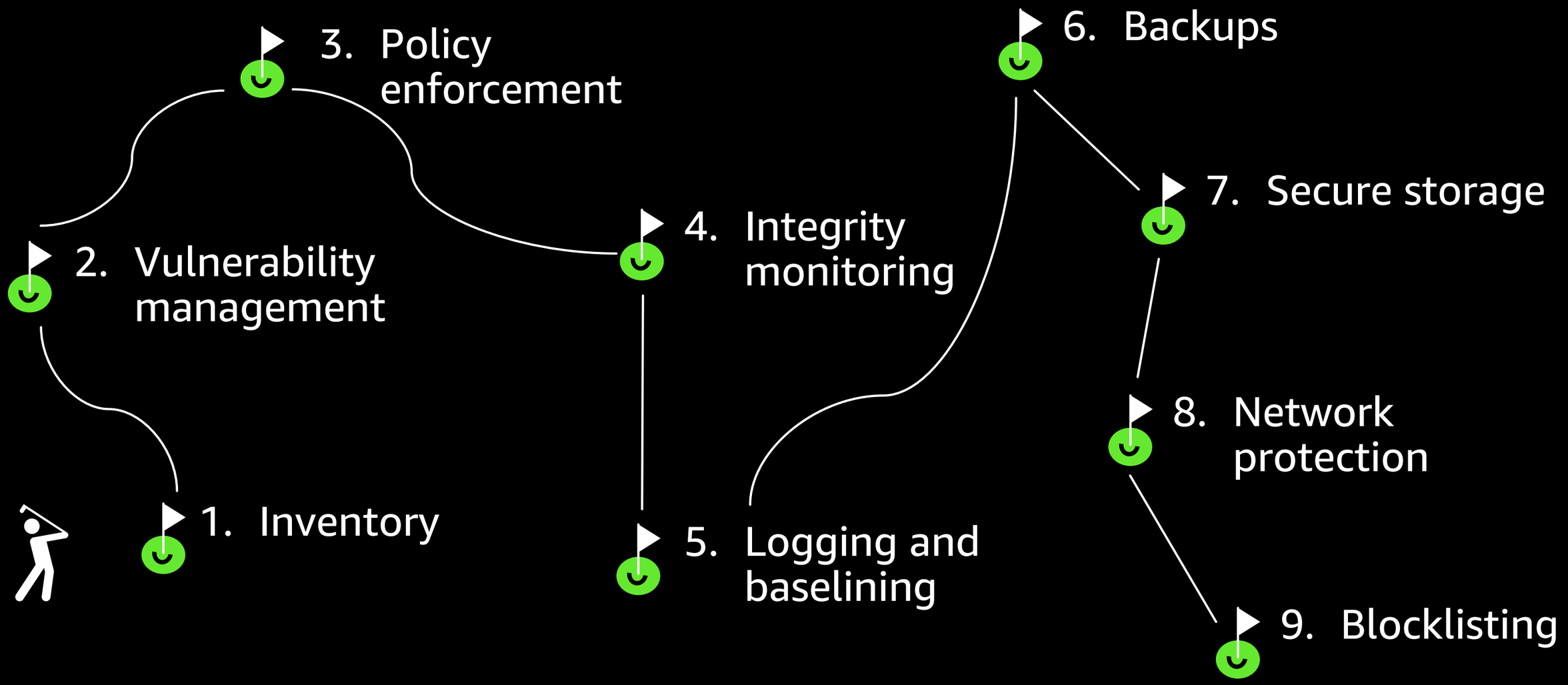




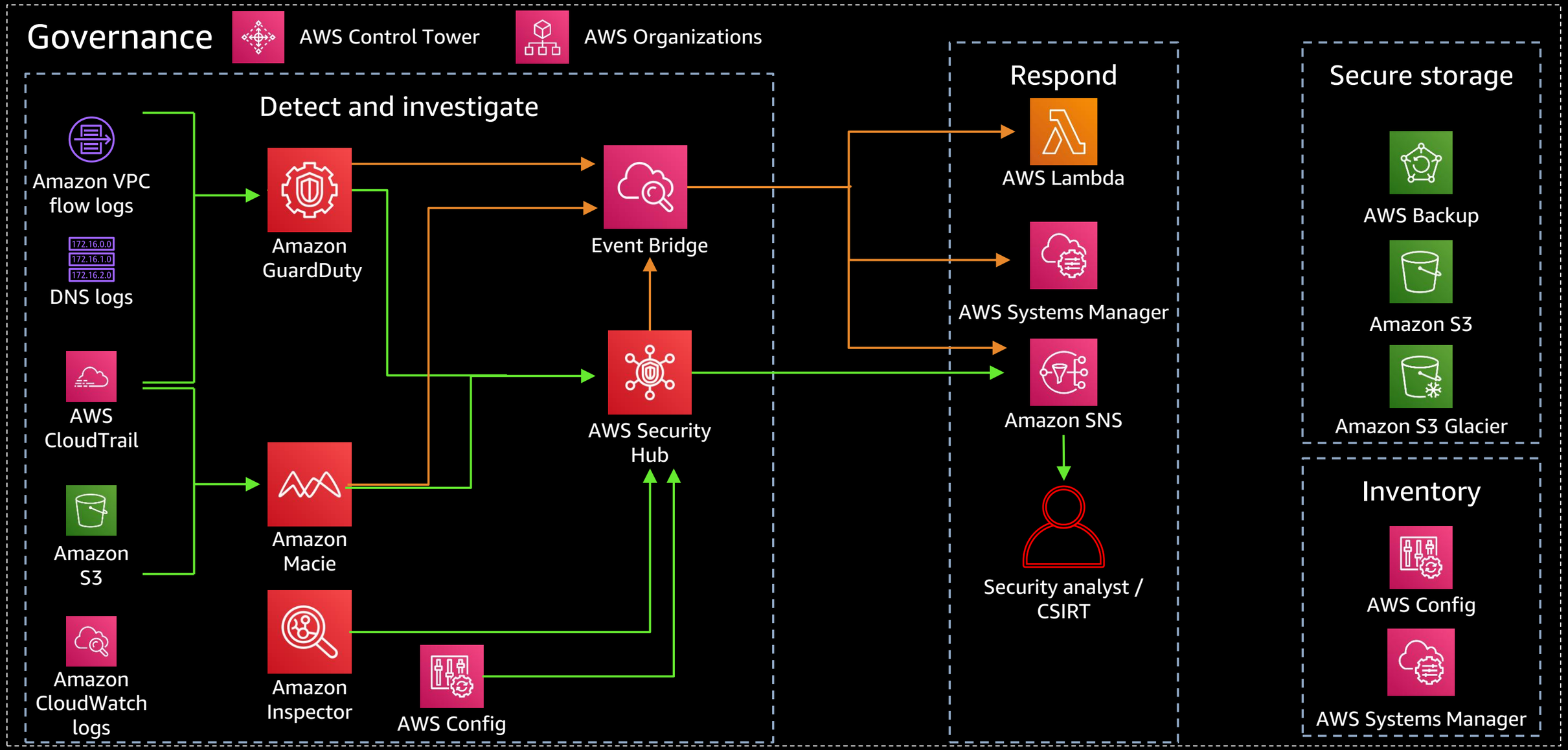
But how do you know **proactively** that you are prepared?

Not enough time, resources, money, or know-how . . .

NIST 1800-25 and 1800-26 reference framework



Putting the components into practice



Putting the components into practice



But how do you know **proactively** that you are prepared?

Identify exposures using AWS Self Assessment Toolkit (SAT)



Open source



Turnkey deployment



Less than $1 in most cases



Simple architecture



No AWS CloudFormation knowledge needed



Fully automated



Leverages reputable frameworks



https://github.com/awslabs/aws-security-assessment-solution

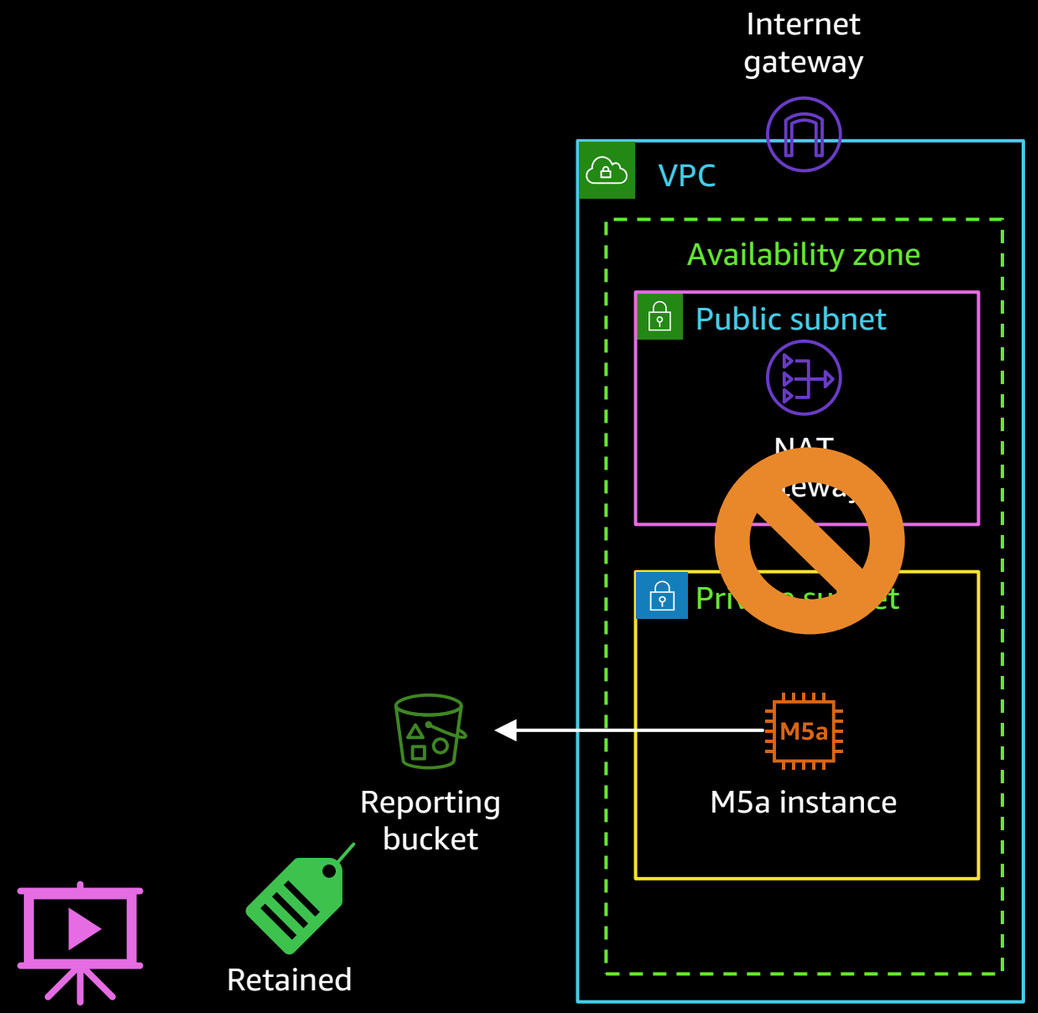
SAT ransomware modules – verify your AWS-powered defense capabilities



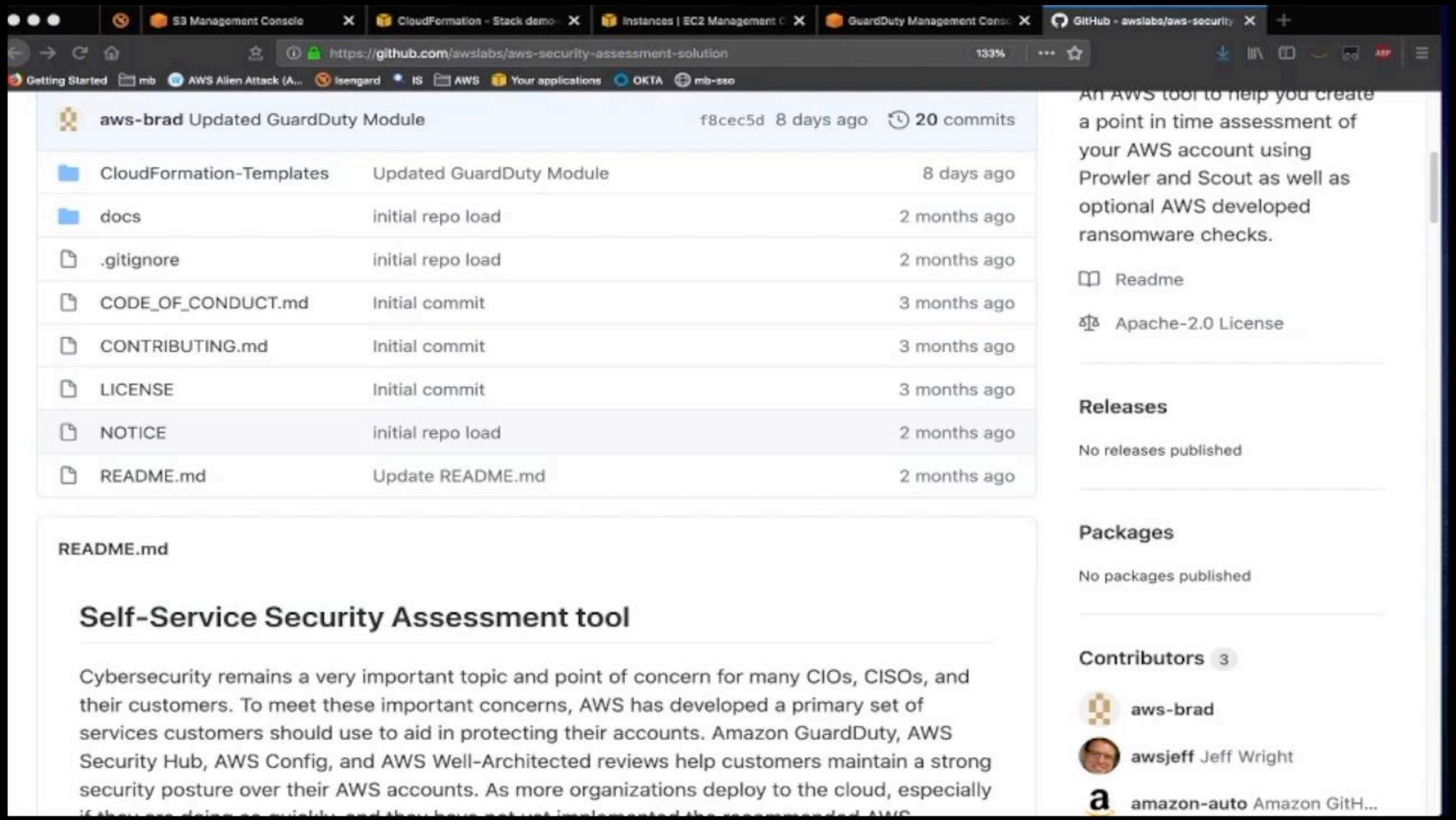
More are coming

Deployment

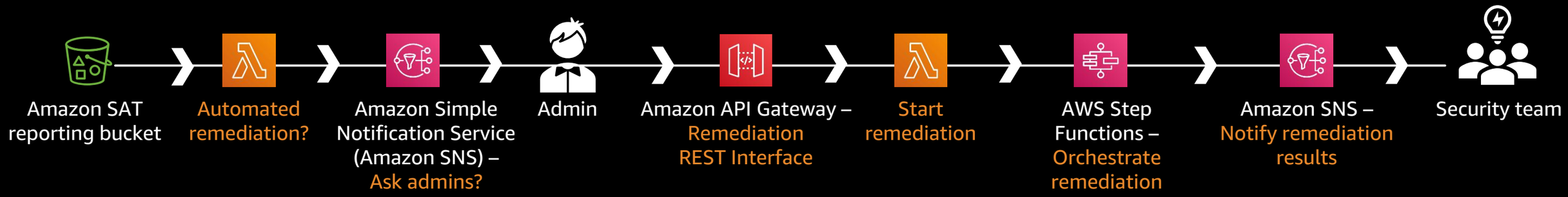
- Create an assessment VPC with public and private subnet
- Deploy NAT Gateway in public subnet
- Deploy an assessment Amazon Elastic Compute Cloud (Amazon EC2) instance in private subnet
- Create a reporting bucket



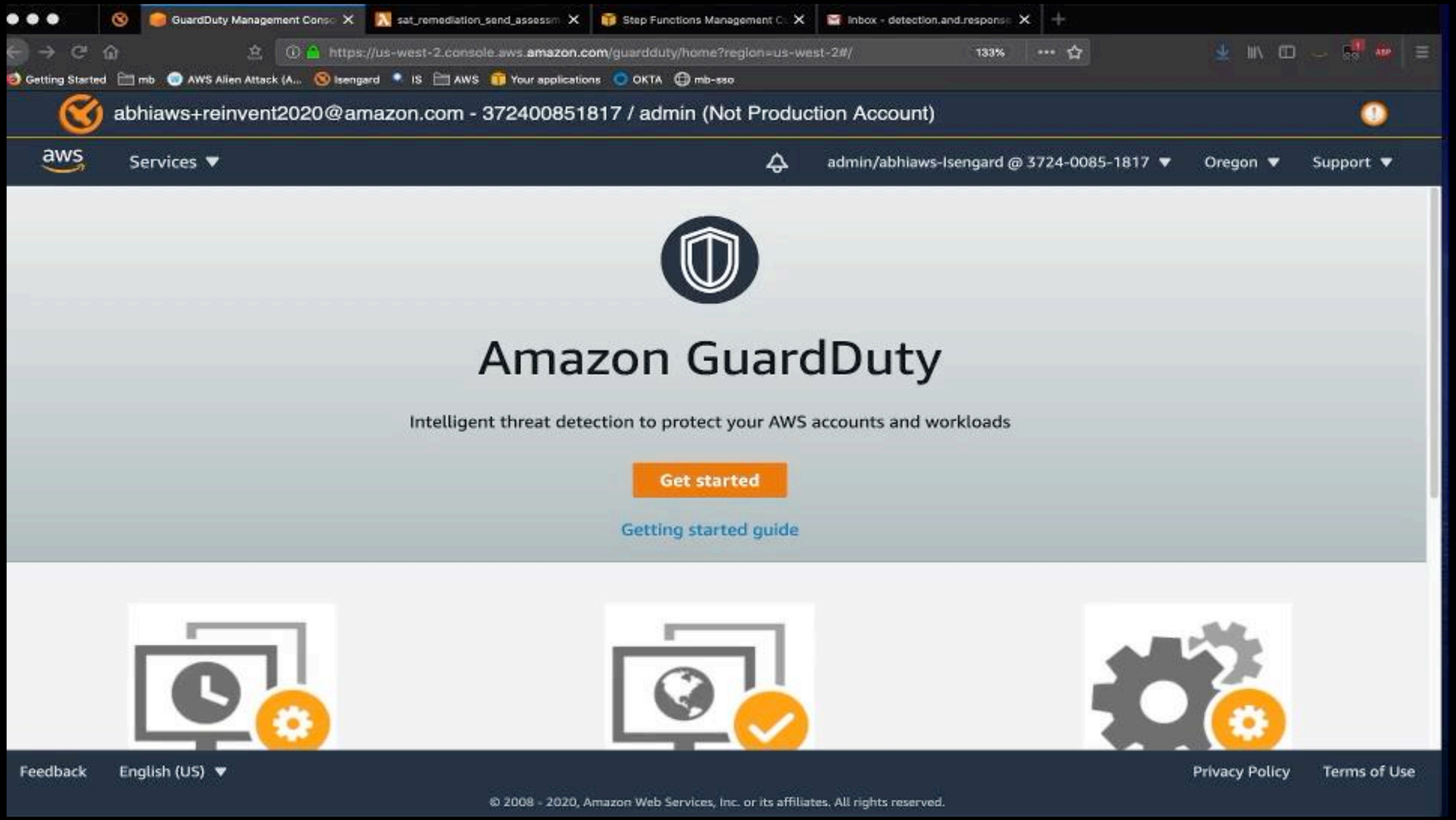
Deployment


S3 Management Console
CloudFormation - Stack demo
Instances | EC2 Management
GuardDuty Management Conso
GitHub - awslabs/aws-security
https://github.com/awslabs/aws-security-assessment-solution
133%
Getting Started
mb
AWS Alien Attack (A...
Isengard
IS
AWS
Your applications
OKTA
mb-sso
aws-brad Updated GuardDuty Module
f8cec5d 8 days ago
20 commits
CloudFormation-Templates Updated GuardDuty Module 8 days ago
docs initial repo load 2 months ago
.gitignore initial repo load 2 months ago
CODE_OF_CONDUCT.md Initial commit 3 months ago
CONTRIBUTING.md Initial commit 3 months ago
LICENSE Initial commit 3 months ago
NOTICE initial repo load 2 months ago
README.md Update README.md 2 months ago
README.md
Self-Service Security Assessment tool
Cybersecurity remains a very important topic and point of concern for many CIOs, CISOs, and their customers. To meet these important concerns, AWS has developed a primary set of services customers should use to aid in protecting their accounts. Amazon GuardDuty, AWS Security Hub, AWS Config, and AWS Well-Architected reviews help customers maintain a strong security posture over their AWS accounts. As more organizations deploy to the cloud, especially
a point in time assessment of your AWS account using Prowler and Scout as well as optional AWS developed ransomware checks.
Readme
Apache-2.0 License
Releases
No releases published
Packages
No packages published
Contributors 3
aws-brad
awsjeff Jeff Wright
amazon-auto Amazon GitH...

Extending the solution



Extending the solution



AWS has many services to strengthen your ransomware program

Ransomware response orchestration using Step Functions

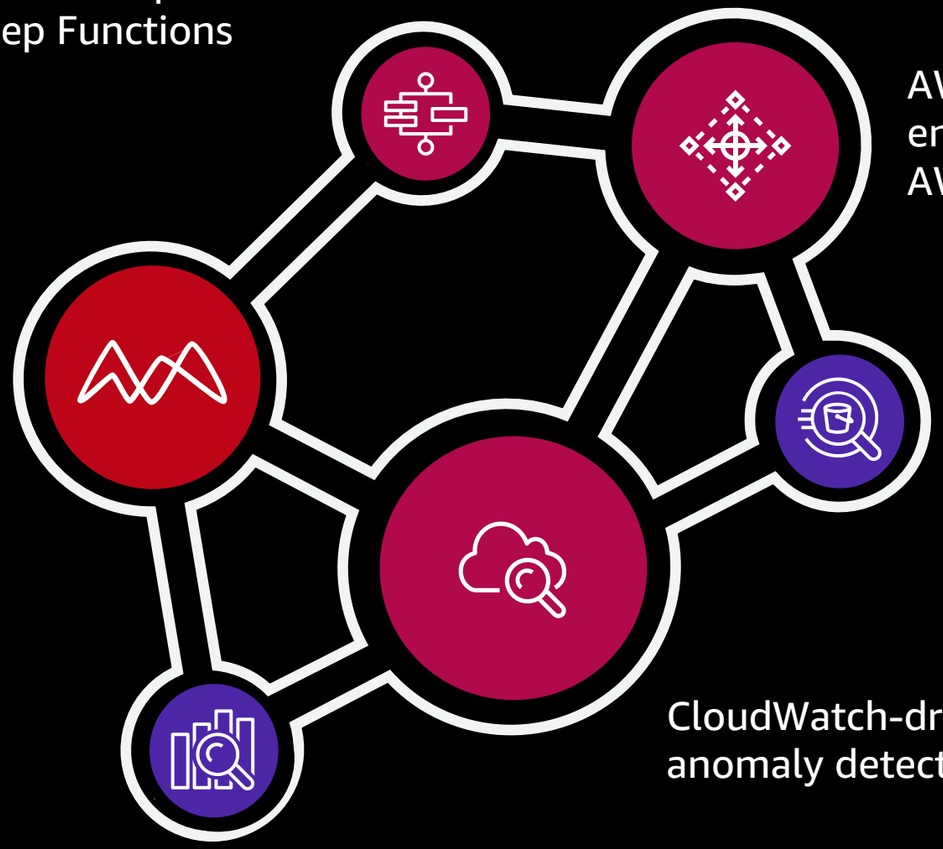
AWS best practices enforced using AWS Control Tower

Inventory business critical data assets using Amazon Macie

Detecting anomalies and trends using Amazon Athena

CloudWatch-driven anomaly detection

Detection rules and dashboards using Amazon Elasticsearch Service



For continuous assessment, leverage Security Hub

Next steps

- Deploy the Self Assessment Toolkit (SAT)
- Run a trial of the AWS services mentioned earlier
- Contribute, extend, fork, and help spread the word!

https://github.com/awslabs/aws-security-assessment-solution



The SAT is intended for point-in-time assessments – for continuous assessment (against best practices), leverage Security Hub

Your AWS SAT solution team



Stephen Alexander

Principal Specialist
Solutions Architect



Brad Dispensa

Principal Specialist
Solutions Architect



Abhi Singh

Specialist Solutions Architect



Jeff Wright

Senior Manager
Specialist Solutions Architect

Thank you!

Abhi Singh

Specialist Solutions Architect
AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.