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

SEC201

Proactive security: Considerations and approaches

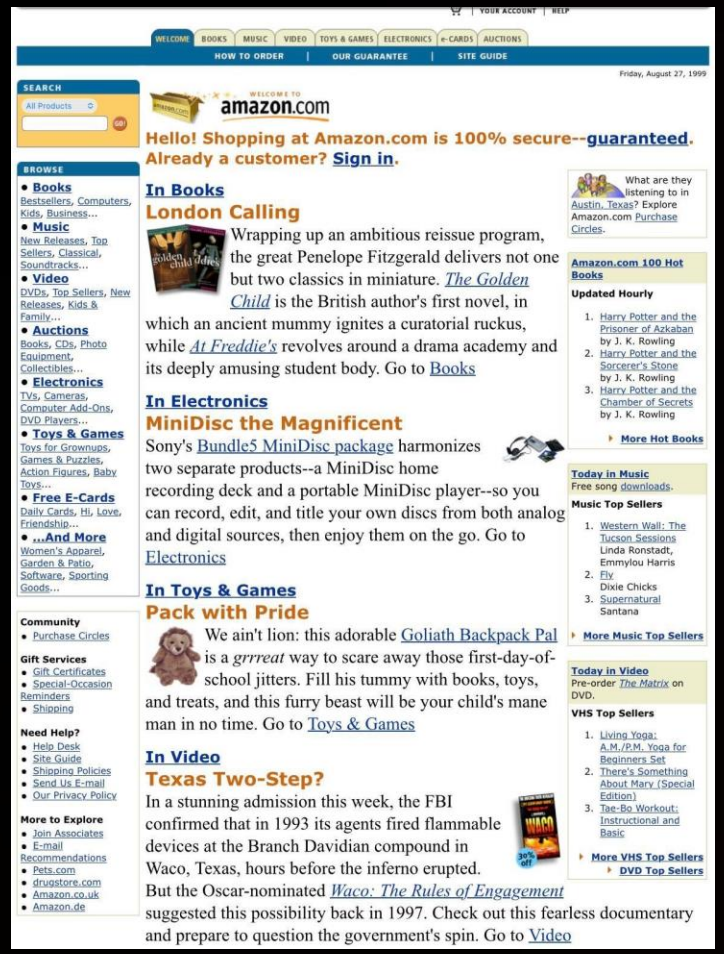
Eric Docktor

VP of Software Builder Experience
Amazon

Sarah Berry

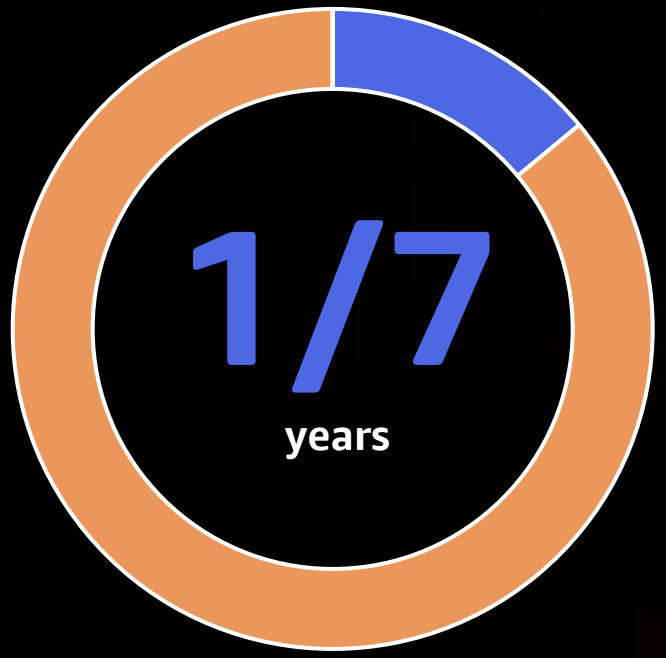
Security Manager, Proactive Security
Amazon

Eric Docktor



aws cryptography

Sarah Berry



aws security

What will you get out of this session?

COLLABORATION

BUILD DECISIONS

UNDIFFERENTIATED HEAVY LIFTING

MEASURING SUCCESS

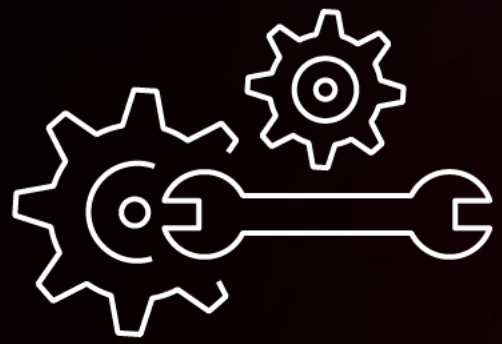
BUILDER EXPERIENCE MISSION

Make Amazon Earth's best employer for software builders

Every event is a learning opportunity

Focus areas of the builder experience

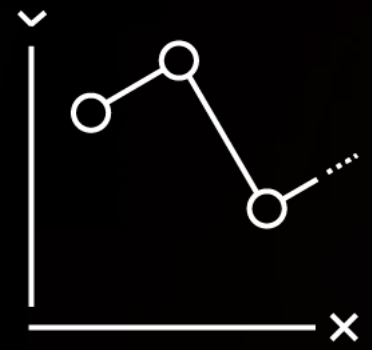
1. Radically reduce the cost of mandatory software updates



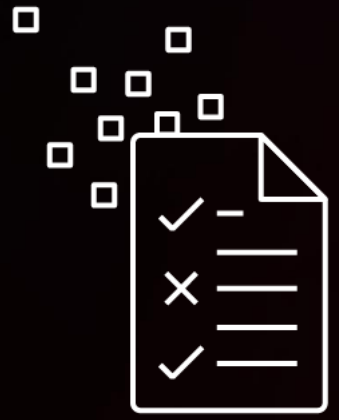
2. Eliminate routine maintenance and infrastructure build-out tasks

3. Build and adopt higher abstraction managed runtimes

Focus areas of the builder experience



4. Provide data to builders and leadership that guides investment in automation



5. Make managing work easier

6. Create learning and career development opportunities

"Service teams own the security of their service, AWS Security owns the security of AWS."

CJ Moses

Chief Information Security Officer
Amazon Web Services

Nourishing security ownership

“Two-pizza” teams

Own a service

Minimize social constraints (Conway’s Law)

Retain autonomy to make decisions

Proactive security mission

SHIP SECURELY

Security is a foundational part of the customer experience but isn’t the only thing that goes into delighting customers

A service with security issues doesn't satisfy customers, but a service that hasn't launched doesn't have the opportunity to serve customers in the first place

We empower service teams to launch on schedule, with the right customer experience and with an appropriately high security bar

Delivering for both customers and builders

SECURITY

BUILDER EXPERIENCE

CUSTOMER OBSESSION

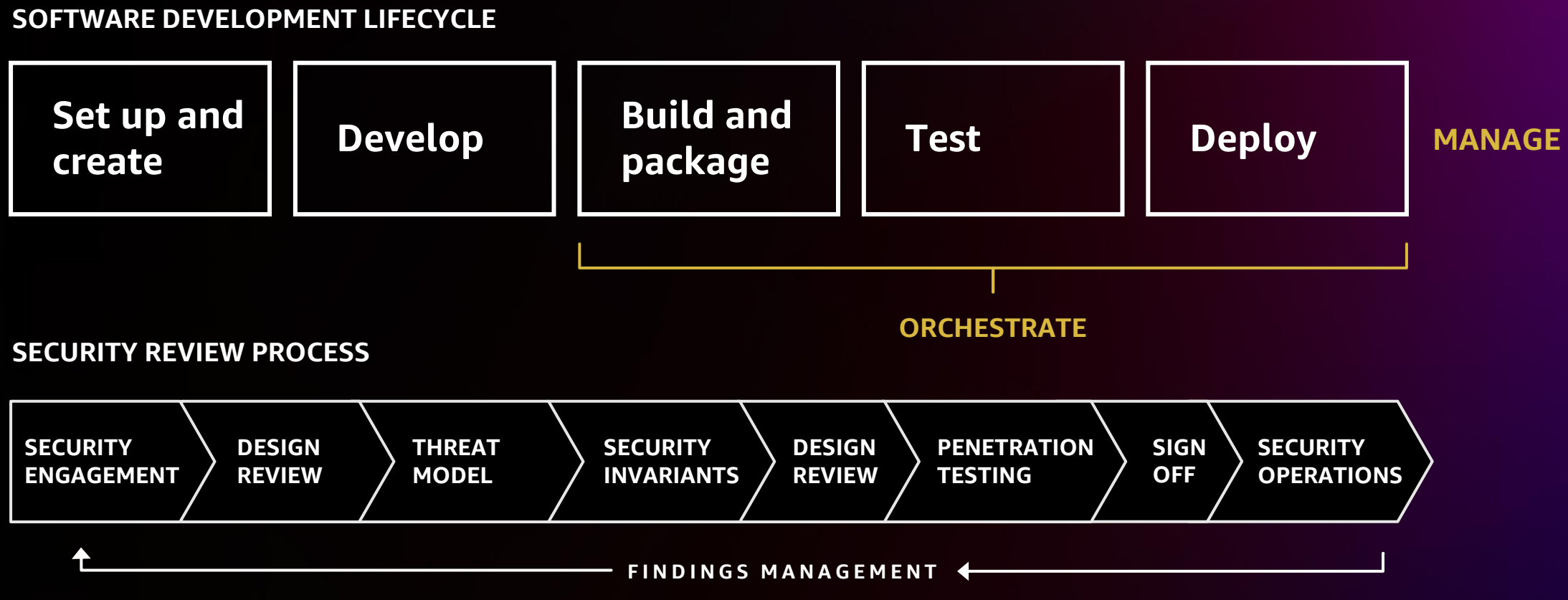
How we're improving the builder experience

Reducing the burden on builders requires first understanding where the friction is

We want to build tools that will have the biggest impact

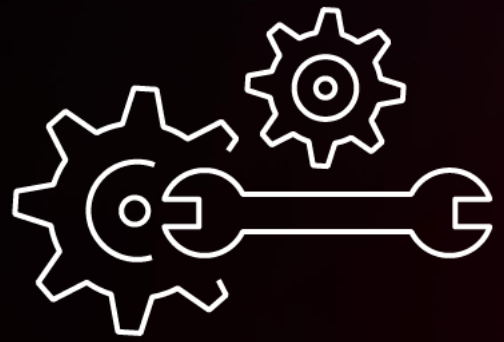
You need to measure whether you actually solved the problem

Builder experience



Broad goals

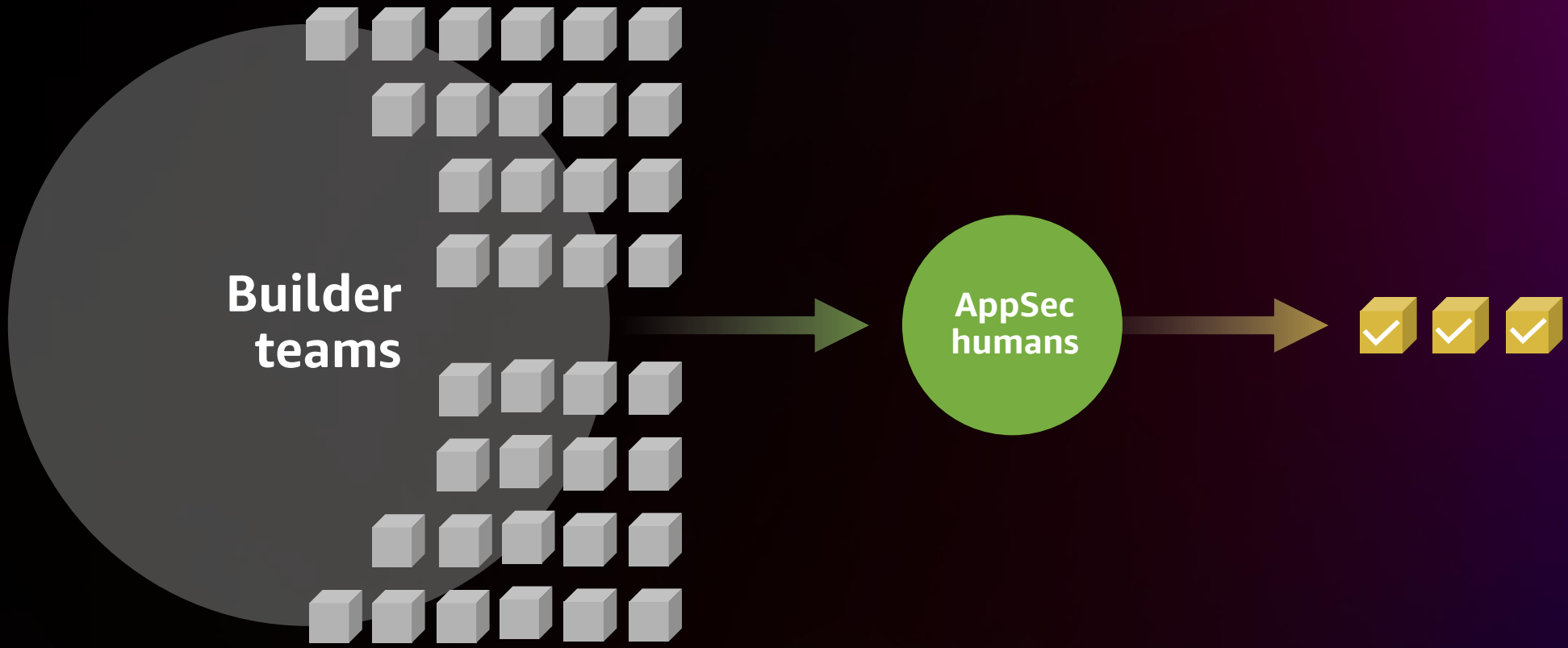
Launch on schedule, with an appropriately high security bar



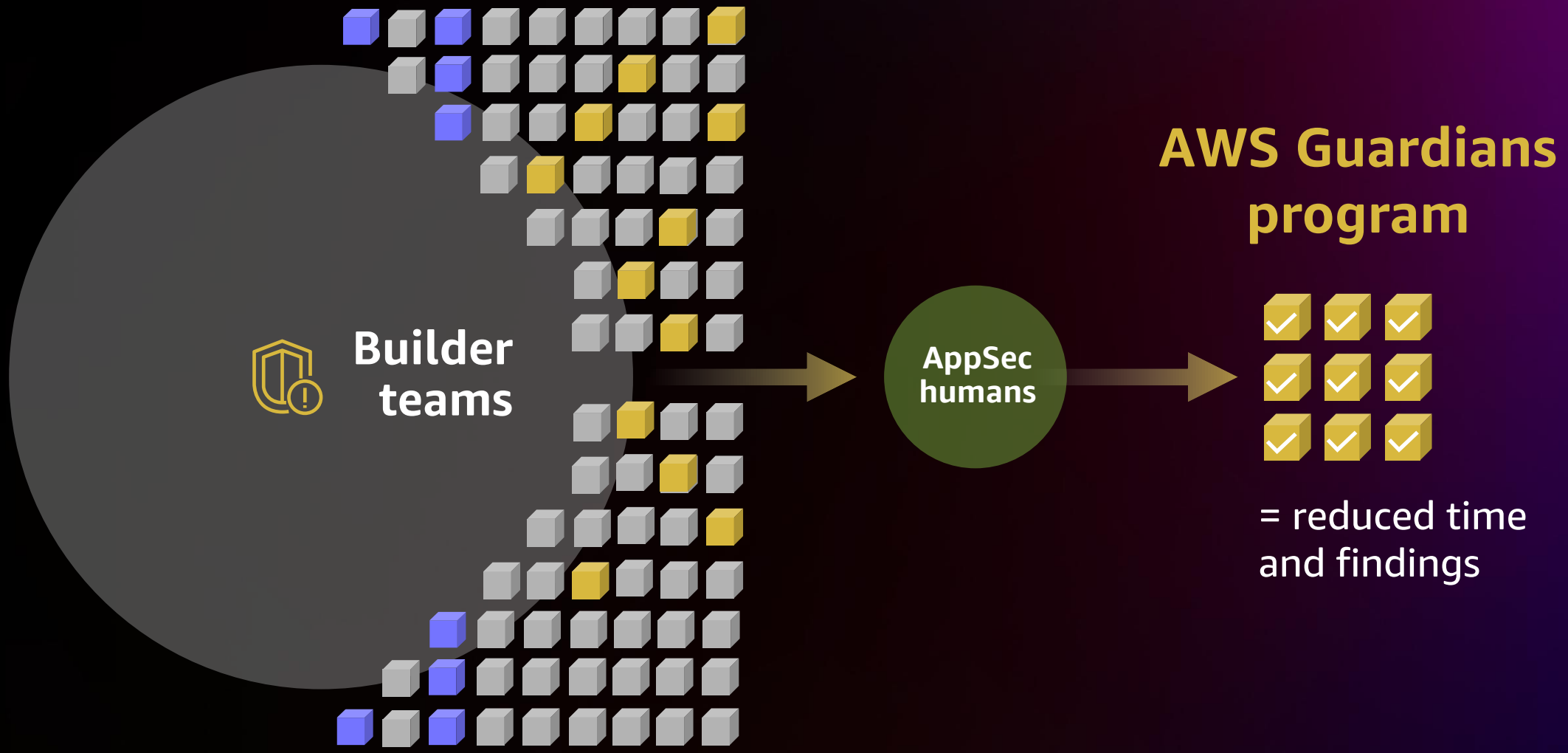
Identify risks and findings earlier in the development lifecycle

Reduce confusion and variation in the review process

Builders: Security ratio disparity



Embedding security into builder teams



Guardians vs. security engineers

The AWS Security Guardians' goal is to extend security ownership outside of AWS Security

Proactive security engineers are full-time security practitioners trained to understand and minimize risk posed by our builders to secure our customers and AWS

Impact of the Guardians program

- We've trained ~2,000 software development engineers **on how to think about security**
- Security reviews had **22.5% fewer medium- and high-severity findings** discovered during an AppSec review, representing 15,973 fewer findings
- Security reviews benefitted from **26.9% less time to complete a security review end to end**, yielding a savings of 210,216 total days

How can you get started?

Identify a diverse set of Guardians and **set an organizational goal**

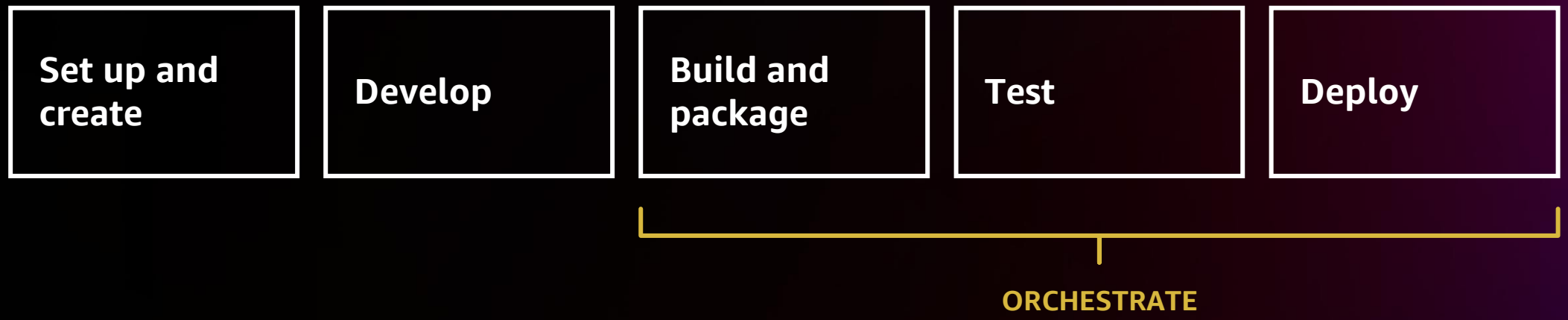
Ramp them up with skills and mentorship necessary to get them started

Build a community with continual **knowledge sharing**

Measure, report, and **recognize Guardian effectiveness**

Establish **continuous feedback mechanisms** with qualitative and quantitative data

Builder experience



Broad goals

Needed to meet our operational safety, security, and compliance requirements for securing customer data

Reduce human access to production systems and data across AWS

Build in standardization for monitoring, alarming, and auditing

What we built: Mechanic

Mechanic – unified operational tooling service that allows operators to run commands on production hosts without direct access

Builders can take action on production resources without having to access a production resource

Every action being taken has been reviewed, tested, and approved

Reporting UI shows which tools were run and by whom

How can you get started?

Start with identity – keep humans away from systems

Provide a request/approval mechanism to vend short-term credentials

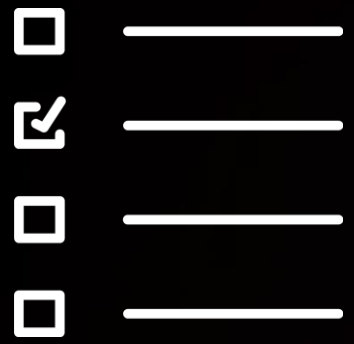
Automate your operations in your environment by authoring repeatable playbooks

Audit and review to find the friction and decide what to automate next

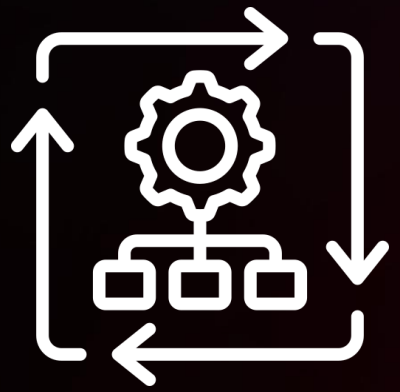
AWS Identity and Access Management (IAM)

AWS Systems Manager

Broad goals



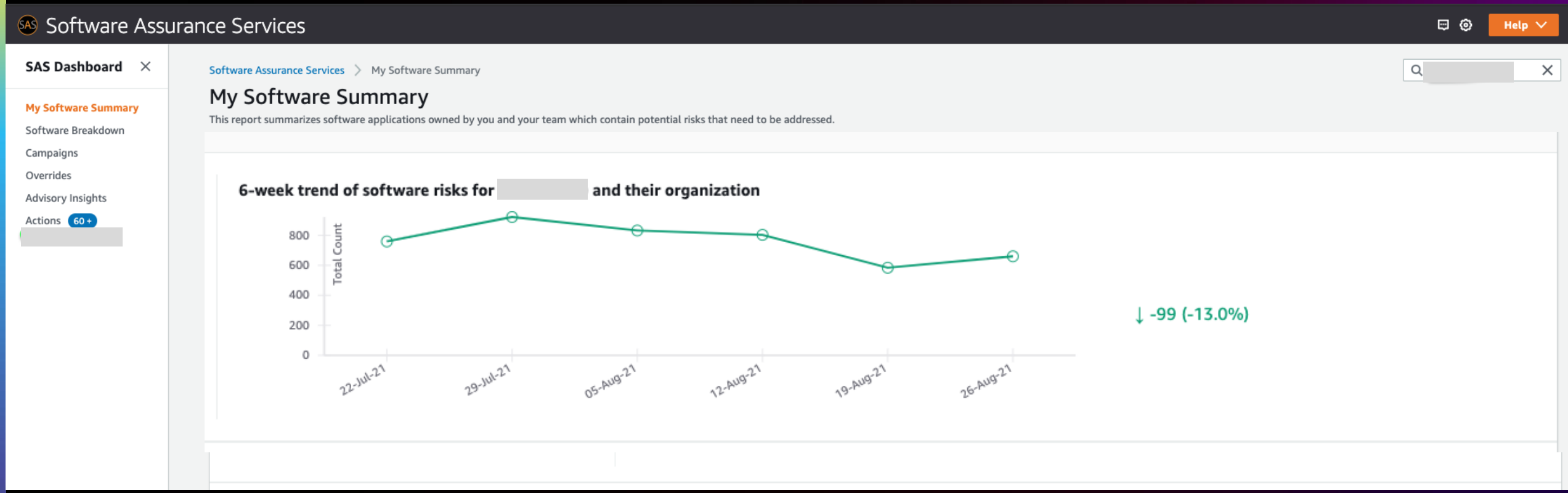
Provide builders prioritized actions to remediate issues



Automate remediation on builders' behalf

Alert builder teams that have out-of-date dependencies

What we built: Software assurance services



Software assurance services

```
@ -36,10 +36,11 @@
36          CoralClientBuilder = 1.1;
37
38          ClassicHeartbeat = 1.0;
39
40          SASQLMySQLSnapshotManager = 1.0;
```

```
@ -36,10 +36,11 @@
36          CoralClientBuilder = 1.1;
37
38          ClassicHeartbeat = 1.0;
39
40          SASQLMySQLSnapshotManager = 1.0;
41  +       Jackson-databind = 2.1;
```

RiskAggregationService | a few seconds ago

Rate this comment

Resolve comment

WARNING: Jackson-databind 2.1 is on the BLOCKED list and is part of 1 SAS run campaign(s):

- Blocked Software Campaign - Jul 2019

Update to use one of the versions with recommended vendor guidance

Reply

```
41          };
42      };
```

```
42          };
43      };
```

How can you get started?

Understand the components from which you build software

Combine AWS and AWS Partner tools depending on your developer environment

Use automation to provide visibility into what packages that are in use and when

Make it easy for builders to consume the right packages

AWS CodeArtifact

Third-party package manager

Amazon Inspector

“It is the goal of every security system to maximize the delivered customer value while minimizing the cost of that delivery.”

Eric Brandwine

AWS Security Distinguished Engineer and VP

Security Automation

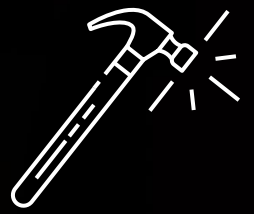
4

Scanners

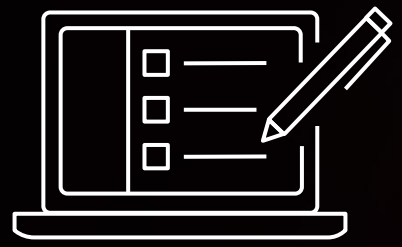
300+

Rules

Talos



Builder initiates Talos engagement



Talos engages builder to learn about the service and provide relevant guidance; builders implement guidance and review with Guardian

Builder submits for review

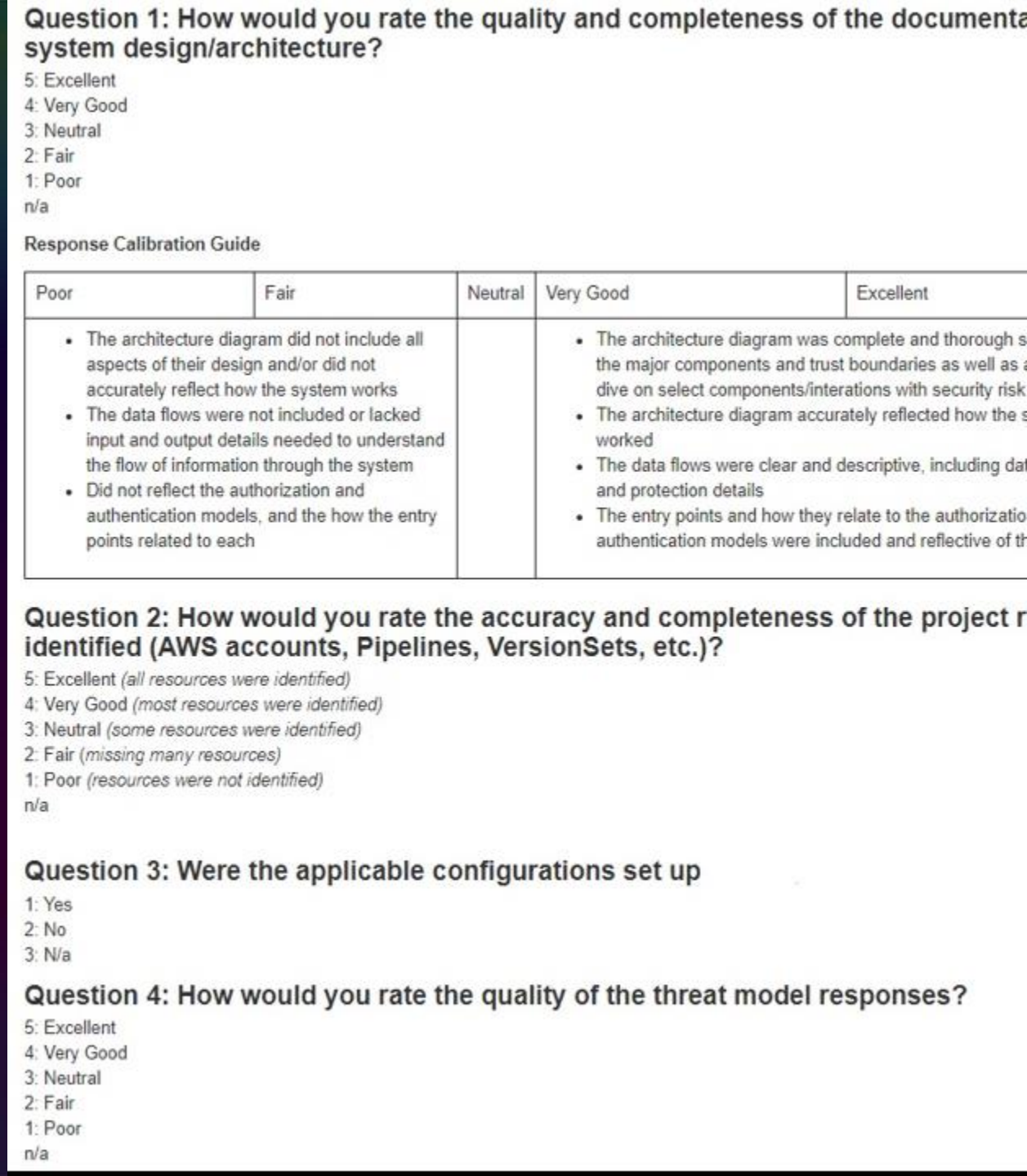
Review and pen testing

Approval

End of review survey

End of security review surveys to gauge **effectivity** of Security Guardians

1. Rates the quality of the security engagement submission
2. Provides feedback to the Guardian(s) if one was assigned



Question 1: How would you rate the quality and completeness of the documenta system design/architecture?

5: Excellent
4: Very Good
3: Neutral
2: Fair
1: Poor
n/a

Response Calibration Guide

Poor	Fair	Neutral	Very Good	Excellent
• The architecture diagram did not include all aspects of their design and/or did not accurately reflect how the system works • The data flows were not included or lacked input and output details needed to understand the flow of information through the system • Did not reflect the authorization and authentication models, and the how the entry points related to each			• The architecture diagram was complete and thorough s the major components and trust boundaries as well as a dive on select components/interations with security risk • The architecture diagram accurately reflected how the s worked • The data flows were clear and descriptive, including dat and protection details • The entry points and how they relate to the authorizatio authentication models were included and reflective of th	

Question 2: How would you rate the accuracy and completeness of the project r identified (AWS accounts, Pipelines, VersionSets, etc.)?

5: Excellent *(all resources were identified)*
4: Very Good *(most resources were identified)*
3: Neutral *(some resources were identified)*
2: Fair *(missing many resources)*
1: Poor *(resources were not identified)*
n/a

Question 3: Were the applicable configurations set up

1: Yes
2: No
3: N/a

Question 4: How would you rate the quality of the threat model responses?

5: Excellent
4: Very Good
3: Neutral
2: Fair
1: Poor
n/a

Builders' experience metrics

"People respect what you inspect"

Make it easy for builder teams and senior leaders to see how their team stacks up when it comes to eliminating manual, repetitive work across build, deployment, and production support

- Provide builder insights to teams in the tools they use
- Establish mechanisms to review common concerns raised by organizations and in surveys

How can you get started today?

What can you do next?

UNDIFFERENTIATED
HEAVY LIFTING

Identify where you have **undifferentiated heavy lifting** as you build and manage your services

Reduce interactive access to systems and measure the increase in automation

Build from known good and get visibility into potential issues using AWS CodeArtifact and Amazon Inspector

What can you do next?

COLLABORATION

How are you **developing** your builders to be informed security owners throughout the development lifecycle?

Identify a **diverse set of builders** to pilot a Guardians program

Train, measure, report on, and recognize **their impact**

Thank you!

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