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

SUP309

AWS Well-Architected Framework security pillar: Cloud security at scale

Sarita Dharankar (she/her)

Security Pillar Lead,
AWS Well-Architected
AWS

Neel Sendas (he/him)

Principal Technical Account Manager
AWS

Jeff Henderson (he/him)

Manager, Security Engineering
Molex

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

Agenda



AWS Well-Architected



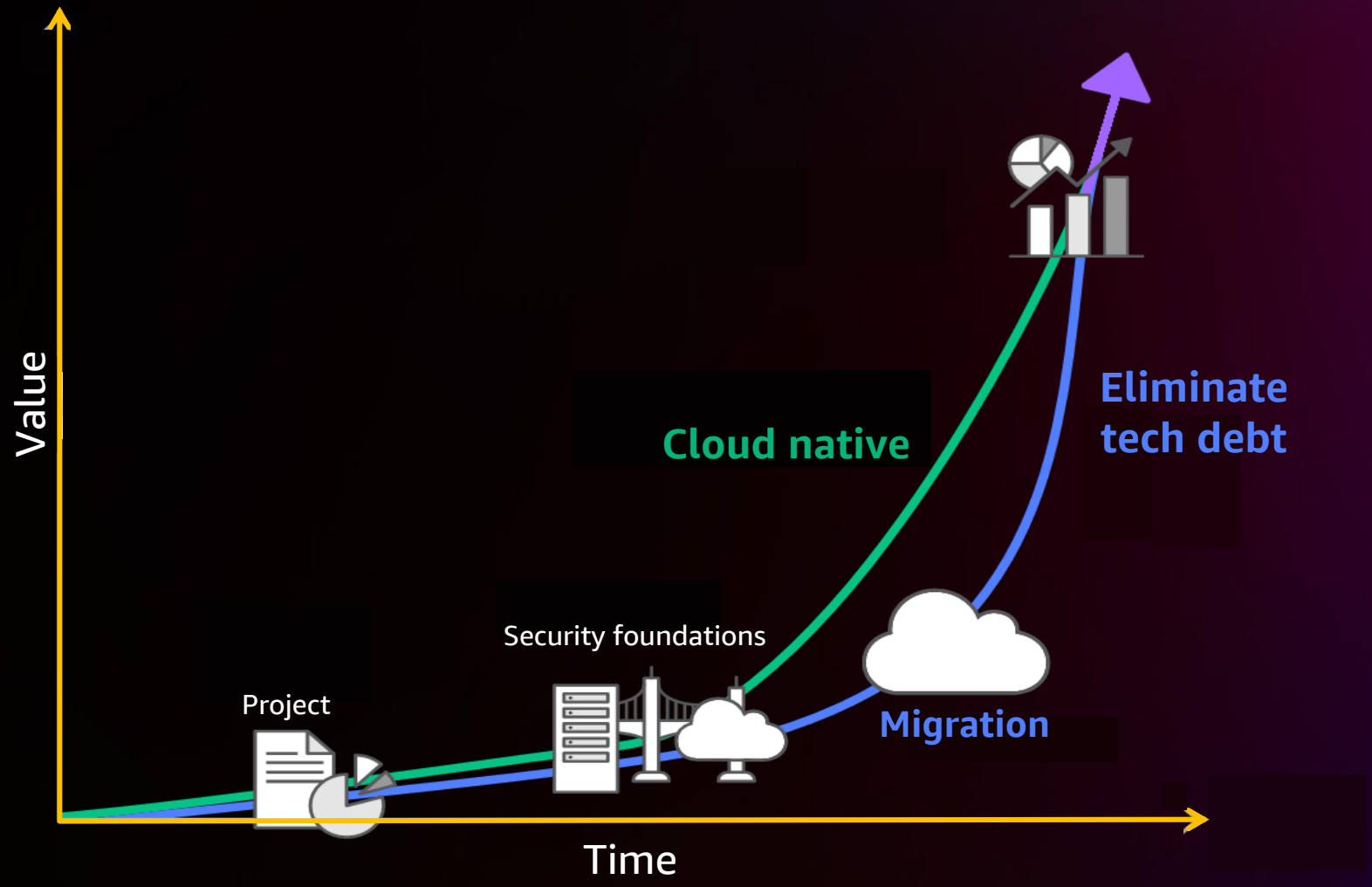
Security Improvement Program (SIP)



molex

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

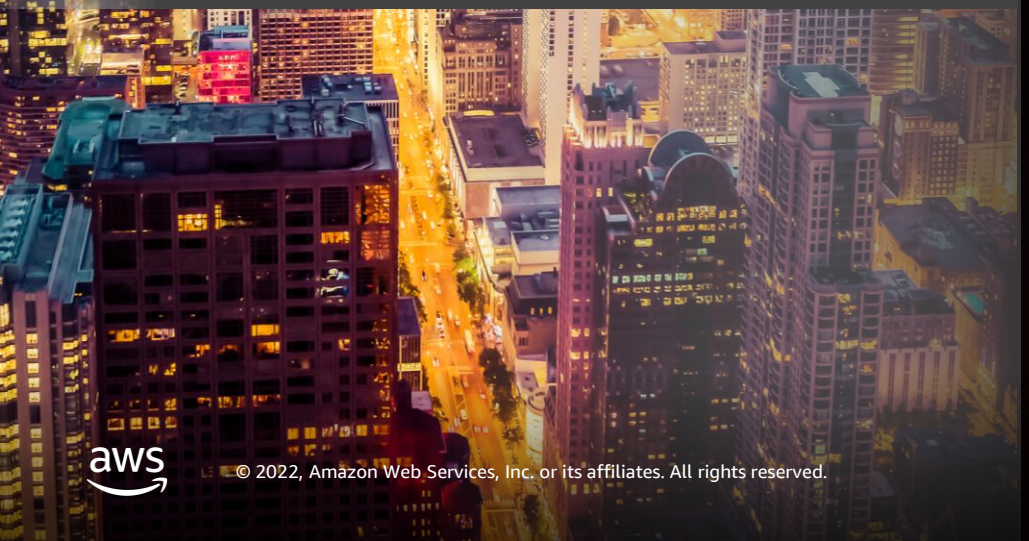
What are the cloud outcomes we want?



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

Why use the AWS Well-Architected Framework?





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



Build and deploy faster



Reduce or mitigate risks



Make informed decisions



Learn AWS best practices

Security design principles

- Implement a strong identity foundation
- Enable traceability
- Apply security at all layers
- Automate security best practices
- Protect data in transit and at rest
- Keep people away from data
- Prepare for security events



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

Top 5 security best practices for foundational security posture and secure scaling

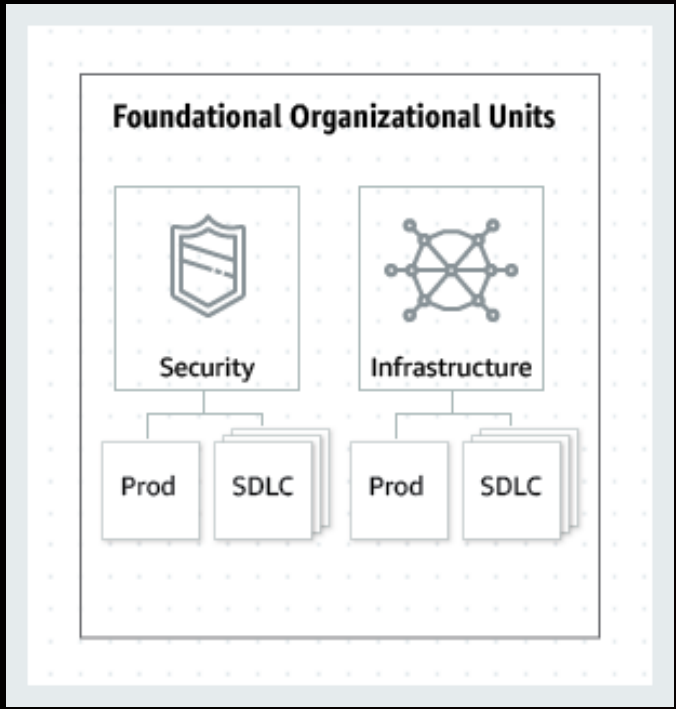
1. Use a multi-account strategy and segmentation to limit scope of impact and operational ease
2. Continuously strive for least privilege access
3. Have a plan for managing system vulnerabilities; regularly patch and harden systems
4. Develop and exercise an incident response plan
5. Protect data

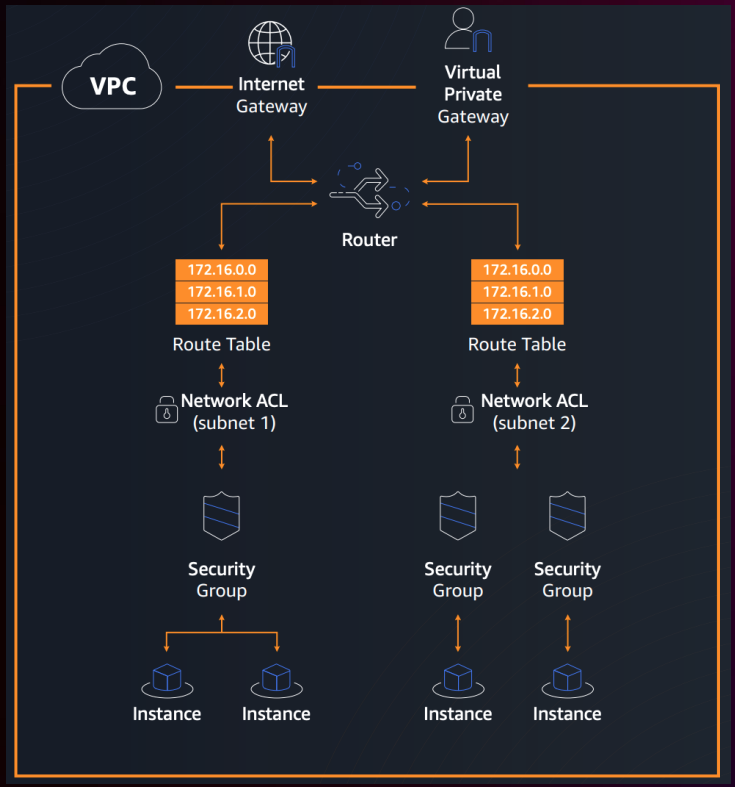
Perform continuous assessments



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

1. Use a multi-account strategy and network segmentation





AWS Security Reference Architecture
https://github.com/aws-samples/aws-security-reference-architecture-examples

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

2. Continuously strive for least privilege

STATIC CREDENTIALS AND OVERLY PERMISSIVE POLICIES REMAIN ONE OF THE TOP SECURITY RISKS

- **Eliminate** or minimize static IAM credentials
- **Federate** access using AWS IAM Identity Center (successor to AWS Single Sign-On) or existing federation provider
- Move to **least privilege** IAM roles and policies using **AWS Identity and Access Management Access Analyzer** to scope down permissions
- Utilize service control policies (SCPs) to **reduce access**

aws

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

3. Perform vulnerability management

UNPATCHED VULNERABILITIES OFTEN CAN CAUSE SECURITY ISSUES & INCREASE OPERATIONAL OVERHEAD

- Use **Amazon Inspector** to identity vulnerabilities and assess instances against security benchmarks
- Use **Amazon ECR image scanning** to identity vulnerabilities and assess your container images
- Use **Patch Manager, a capability of AWS Systems Manager,** to deploy OS and software patches automatically
- Use **endpoint workload protection software** on your instances in “Protect” mode

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

4. Develop & exercise an incident response plan

People

- Train security operations staff on AWS

Process

- Develop an incident response plan and strategy
- Run drills and automate simulations where possible

Technology

- Build dedicated AWS accounts for Security Operations, Log Management, and Forensics
- Create break-glass roles for emergency access to AWS accounts
- Set up security services like Amazon GuardDuty, AWS Security Hub to detect threats
- Use security services like Amazon Detective to help you investigate security findings

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

5. Protect data at rest and in motion

Encrypt **data at rest** (with occasional exceptions)



AWS KMS



Amazon S3

Enabling encryption at rest helps ensure the confidentiality and integrity of data; consider encrypting everything that is not public

0	7
CIS Foundation Benchmark	CIS Web-Tier Benchmark

Use **server-side encryption** with provider-managed keys



AWS KMS



Data encryption key

AWS Key Management Service (AWS KMS) is seamlessly integrated with multiple AWS services; you can use a default master key or select a custom master key, both managed by AWS

1	1
CIS Foundation Benchmark	CIS Web-Tier Benchmark

Encrypt **data in transit** (with no exceptions)



Amazon CloudFront



AWS Certificate Manager (ACM)



SSL/TLS/ HTTPS

Encryption of data in transit provides protection from accidental disclosure, verifies the integrity of the data, and can be used to validate the remote connection

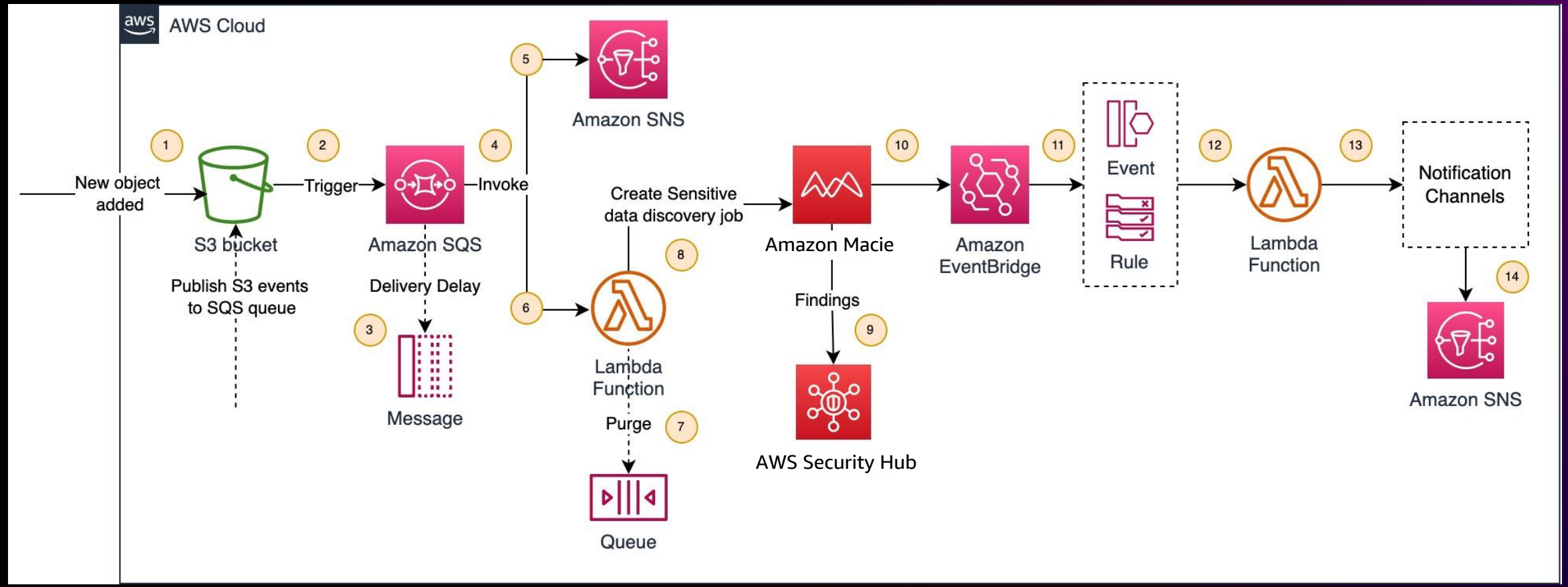
0	9
CIS Foundation Benchmark	CIS Web-Tier Benchmark

aws

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

Getting to the “How”

AWS WELL-ARCHITECTED LAB: DETECT AND SEND NOTIFICATIONS FOR SENSITIVE DATA IN AMAZON S3 BUCKETS USING AMAZON MACIE

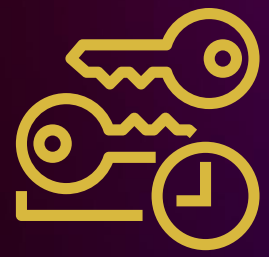


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Identify, improve, and evolve your security posture

Proactively identify risks, close security gaps, implement required controls, and be prepared for security events to **minimize and remediate future security events**

Building security improvement strategy and implementing the right controls

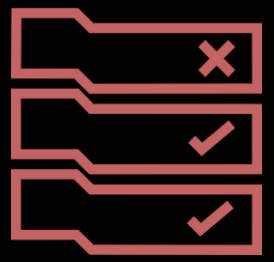


aws

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

Security improvement program (SIP)

- Proactive engagement for Enterprise Support (ES) customers that measures the maturity of a customer's AWS environment
- Automatically provides a weighted security score for identified security risks
- Prescriptive guidance on long-term security improvement strategies



Baseline review



Strategize



Prioritize



Continuous improvement

aws

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

Security improvement program phases



Baseline review

Baseline environment against security best practices

Proactive measurement

Identify risks and security gaps

Record existing processes

Generate weighted maturity score

aws

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

Security improvement program phases



Strategize

Build customized engagement model with guidance of AWS security experts

Deep dive to address your unique challenges

Identify different improvement use cases with TAMs and designated SMEs

Develop risk mitigation action plan

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

Security improvement program phases



Prioritize

Review security risks and corresponding impact

Provide targeted and prioritized recommendations

Do walkthrough of risk mitigation strategy

Define improvement strategy

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

Security improvement program phases



Continuous improvement

Training and enablement

Security workshops, hands-on demo

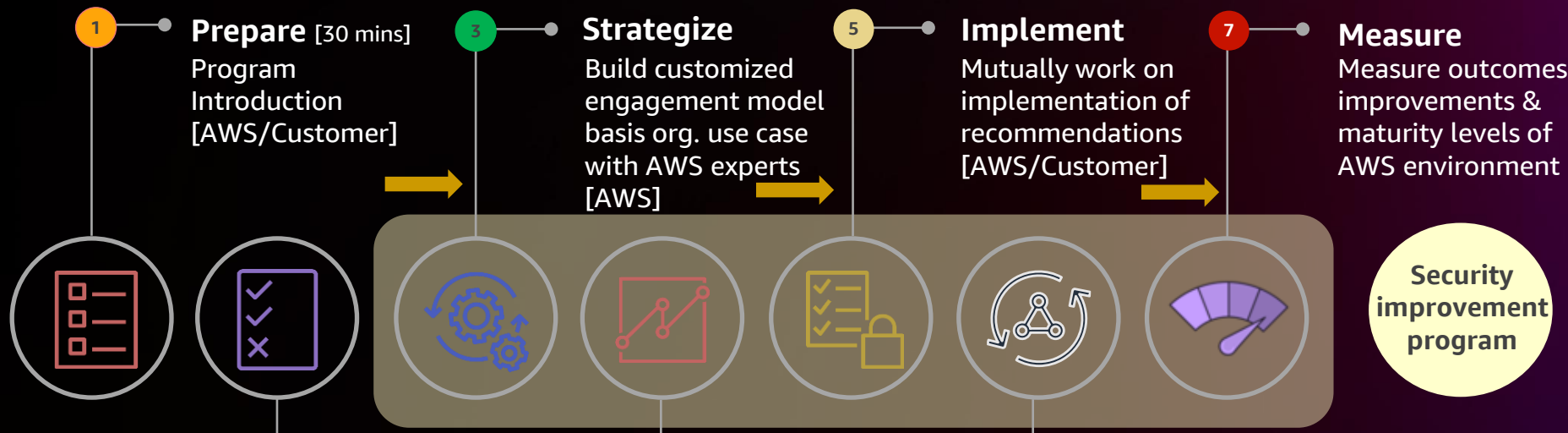
Security cadence with account TAMs, SAs, expert engagement

DevSecOps workshop – building secured solution

Security Gamedays

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

Security improvement program life cycle



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

SIP builds matured security model around the 5 security pillars



Identity & access management

Control access

- Multi-account strategy and governance
- Multi-account strategy and governance
- AWS identity configurations
- IAM policy strategy
- Access key and key pair management



Detection, auditing, and logging

Gain visibility

- Security monitoring and logging
- Centralized and continuous governance
- Data integrity checks
- Configuration change alerts
- Incident forensics



Infrastructure protection

Protect each layer

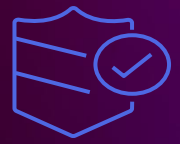
- Infrastructure vulnerability assessment
- Intrusion prevention and detection
- Threat detection mechanism
- Data audit mechanism



Data protection

Data security

- Tagging strategy
- Intrusion prevention and detection
- Threat detection mechanism
- Network protection



Incident response

Respond confidently

- Auto remediation strategy
- Risk assessment and remediation plan
- Benchmarking checks

aws

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

What SIP is not



Security audit



Service specific

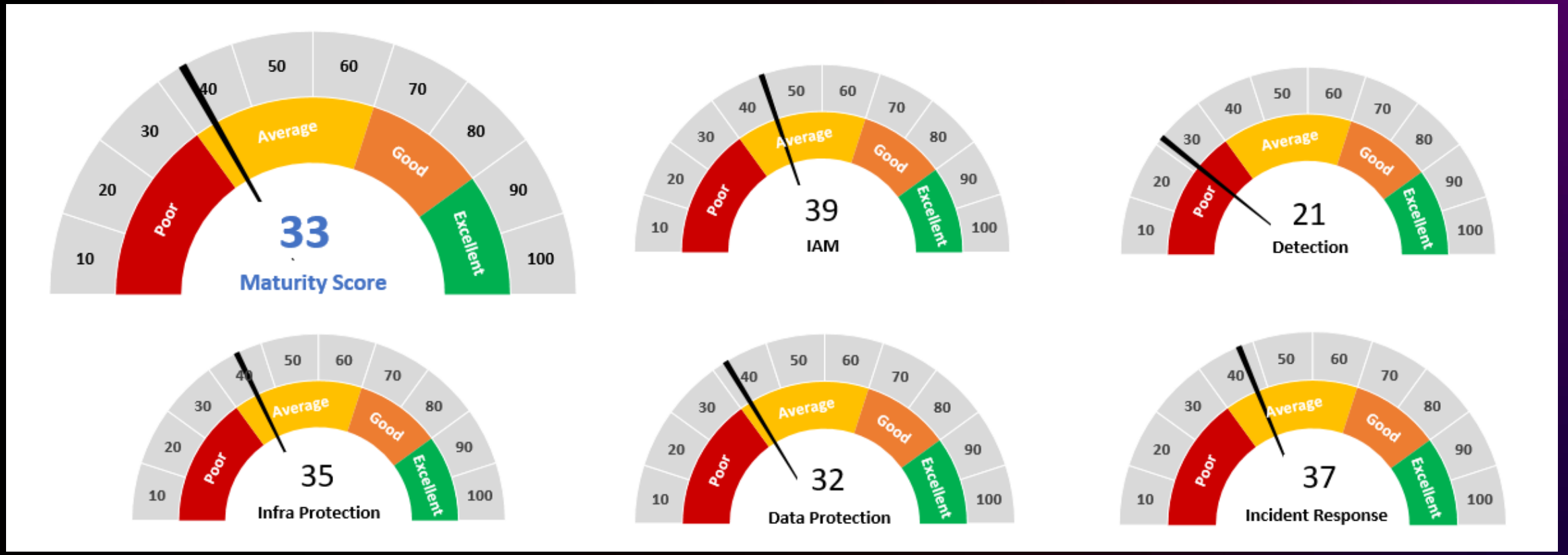


One-time review

aws

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

SIP deliverables – Security score



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

SIP deliverables – Weighted maturity model

TOTAL SECURITY MECHANISMS ACROSS DIFFERENT SECURITY PILLAR & SEVERITY						
Security Pillars & Severity	CRITICAL	HIGH	MEDIUM	LOW	Total Mechanisms	Pillar Weightage %
IAM	7	12	18	7	44	20%
Detection	6	8	22	9	45	20%
Infrastructure Protection	7	17	23	10	57	25%
Data Protection	9	13	29	16	67	30%
Incident Response	1	4	5	1	11	5%
Total Mechanisms	30	54	97	43	224	100%
Severity Weightage %	13%	24%	43%	19%	100%	

How Maturity Score is calculated?

Weighted Maturity Score Logic = Weighted average of mechanisms (Yes/Yes+No+In Progress) **multiplied** by total weightage of the severity **divided** by arithmetic mean of total weightage across each mechanisms and severities.

Weight: Critical 100, High 75, Medium 50, Low 25

CUSTOMER'S RESPONSE, MECHANISMS & MATURITY ACROSS DIFFERENT SECURITY PILLAR & SEVERITY												
Severity & Security Pillars	CRITICAL		HIGH		MEDIUM		LOW		Customer's Mechanisms		Process in place	Risks Identified
Customer's Response	Y	N	Y	N	Y	N	Y	N	Y	N		
IAM	6	1	10	2	11	7	6	1	33	11	80%	20%
Detection	2	4	1	7	12	10	3	6	18	27	31%	69%
Infrastructure Protection	5	2	9	8	12	11	7	3	33	24	62%	38%
Data Protection	7	2	9	4	11	18	8	8	35	32	64%	36%
IR & Automation	1	0	0	4	2	3	0	1	3	8	48%	52%
Customer's Mechanisms	21	9	29	25	48	49	24	19	122	102		
										Maturity Score	57%	43%

aws

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

SIP deliverables – Priority action plan

USE-CASE FOCUSED ACTION ITEMS						
Peculiar Use-case	**Next Steps**	**More Information**	**Priority**	**Customer Remarks**	**Completion Date**	**Status**
Best practices on protecting Sensitive Data on S3 and other storage like RDS, EBS	Targeted use-case focused discussion with Security Specialist		HIGH	Sensitive data on S3 - Identify PII data, Monitoring mechanisms, Infra - Detective Controls, More visibility, Principle of least privilege and access patterns by the organization		**Pending**
Deep Dive Session on AWS WAF	Targeted use-case focused discussion with Edge Specialist		CRITICAL	Multi- WAF strategy. Different workloads for each WAF.		**In Progress**
Check AWS Config service configuration & Readiness review	Review readiness of AWS Config by Security specialist to do configuration review and address best practices recommendations		HIGH	POC for Config was completed. Working on the Implementation.		**In Progress**
SSM Patch manager, Automation, Run document	Patch management and Hardening. SSM Automation for simplifying common maintenance and deployment tasks of Amazon EC2 instances and other AWS resources. Run command to remotely run commands on either AWS EC2 or on-premise instances. Sessions can be arranged for the same.		LOW			**Pending**

Dive deep on use-case-focused action items on your **particular use cases with security specialist engagement**

Prioritized recommendations for identified security risks and **prescriptive guidance on long-term security improvement strategy**

PRIORITY ACTION PLAN FOR IDENTIFIED SECURITY RISKS						
Best Practice	**Benefits & Recommendations**	**More Information**	**Severity**	**Customer Remarks**	**Completion Date**	**Status**
DETECTION						
Do you perform retrospective analysis and real time log analysis for security findings? Is there an automated way that detects anomalies from log aggregation?	**Retrospective analysis** of logs for any incident will help **automate common security best practices and improve MTTD & MTTR of incident.** It also helps updating your runbooks and playbook for **better incident management.** All logs should be collected centrally and **automatically analyzed to detect anomalies and indicators of malicious activity or compromise.**	Analyze Security, Compliance, and Operational Activity	MEDIUM	Guard Duty alerts for anomalies. Logs are not analyzed right now, POC for SIEM Tool (Sumo Logic).		**Pending**
Have you implemented mechanisms to disallow changes to Logging Configuration for critical S3 Buckets like that stores PII data, Log archive data etc or any critical bucket that matters to your business?	It is strongly recommended to apply Service Control Policies (SCPs) to **restrict advertent/inadvertent changes to Logging Configuration for critical S3 Buckets like that stores PII data, Log archive data etc or any critical bucket that matters to your business**	Disallow changes to Logging Configuration for critical S3 Buckets	MEDIUM	POC completed for AWS Config, implementation is pending yet. SCP's depend on migrating users to the master account, post that it will take effect.		**Pending**
What mechanisms you have in place for centralized and continuous governance of AWS Environment, resource chage history, inventory management?	Perform **compliance auditing, security analysis, resource change tracking, and troubleshooting of security incidents**. Maintain a configuration history of your AWS resources and **evaluates the configuration against best practices and your internal policies.** Trigger automated playbook in case of **change in resource compliance that deviates from your established governance standards**	30 Best Practices to strengthen your compliance	HIGH	Access Control Policies in place to stop users from changing the state of the env, no auto-remediation in place yet. Config POC. Waiting for implementation.		**Pending**

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

Security Improvement Program for Molex

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

About Molex

Our vision: We make a connected world possible by working together as a global team to enable technology that transforms the future and improves people's lives

- 7 billion in revenue
- 42K+ employees worldwide
- 100K+ products
- 80+ years of innovation
- Supplier to AWS with data networking products to support cloud and hyperscale applications
- Subsidiary of Koch Industries

aws

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

Why a security improvement program?

We had seen security incidents in some of our accounts and wanted to make sure we were covering all of our bases with prevention and response; we looked to our AWS account team to

- Improve security posture in our developer-managed accounts
- Know where to focus
- Help with metrics and reporting for management

Their response was, let’s start with SIP

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

How it worked

- Determined our focus (which accounts)
- Our AWS account team scheduled several calls with our security engineers and architects and the SMEs from the AWS account team
- Walked through questionnaire on the 5 pillars of security
- Four 1- to 2-hour calls
- Received a detailed report and metrics on security posture
- Scheduled follow-ups to review our progress

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

How SIP helped us improve our security posture

- Helped bridge some knowledge gaps between groups supporting the accounts
- Used metrics provided to report to management where we are at with security of these accounts
- Allowed us to focus in on the critical issues and make immediate progress
- Will allow us to continue to focus on needed improvements while leveraging our AWS account team for support

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

Our approach to using the results

Upon receiving the SIP report

- Focused on the critical items in the 5 security pillars
- Put each finding in our workflow (Agile Kanban) to track
- Focused on the findings we could quickly address
- Moved items that aligned with some of our current security initiatives into the story for those projects
- Schedule follow-ups to review our progress with AWS account team

I will highlight some of our progress in the next slides

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

IAM



One of the questions . . .

“Have you set up a security challenge question for each of your accounts?”

- Not one of those things you think of (at least I did not)
- Is there value in doing this?

This section focused a lot on improvements we are working on in our secrets management initiative

aws

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

Detection



One of the questions . . .

“Have you updated the right contact details for security incidents under Alternate Contacts in AWS account settings?”

- Another good one you would not think of
- Some of the others focused on log file protection

Able to address 100% of critical issues in this section!

aws

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

Infrastructure protection



This section includes

- WAFs, security groups, MFA on critical servers

One of this section’s questions was

- Is your CDN/CloudFront configured to return default root object to avoid exposing the contents of your web distribution?

This question helped us better understand how the firewall team was configuring the WAF

We made a 50% improvement in this pillar

aws

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

Data protection



Data protection presents a challenge where a group of accounts have fewer guardrails by design

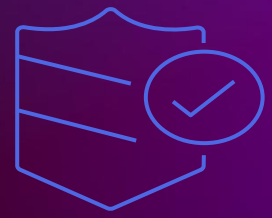
How did SIP help us with data protection?

- Helped us reinforce the need for encryption and data classification during architecture review meetings and account reviews
- Spotted areas we missed – Amazon RDS snapshots were not scrutinized like Amazon EBS; this reminded us of the importance of both
- Reduced our critical findings by 20%

aws

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

Incident response



Improved our score by 33%

One of the improvements centered around this finding:

- Have you implemented detection and auto remediation of common security incidents by doing retrospective analysis with existing tools or in-house tools?

While we were working on this presentation, we had an incident that was caught by GuardDuty, where a review of what happened prompted automation that can prevent the same incident in the future

aws

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

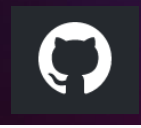
Going forward – Continuing to use SIP

We do not see SIP as a one-time event; we plan on continuing to improve our score by

- Setting up quarterly calls with our AWS account team to review our progress
- Expanding the scope of the review
- Planning on including more teams in future reviews

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

Call to action



awslabs / aws-security-assessment-solution

These security assessments are from the open-source projects “Prowler” and “ScoutSuite,” which include custom modules that **check for ransomware-specific findings**

AWS Well-Architected resources

Main: https://aws.amazon.com/well-architected/

Tool: https://aws.amazon.com/well-architected-tool/

Labs: https://www.wellarchitectedlabs.com/

Solutions: https://aws.amazon.com/solutions

To get started with a security improvement program (SIP), contact your technical account manager (TAM)

© 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.