MEDSHIELD

Slide 1

PRESENTER: ELINA HUANG

MedShield: Automated Cloud Compliance

Ensuring Security & Governance in MedTech

Security Automation AWS Serverless

Team: Elina Huang, Jiamin Cai, Yulin Xue

GitHub: `https://github.com/e1inahuang/medtech-compliance-checker`

PRESENTER: ELINA HUANG

The MedTech Challenge

Strict Regulations

HIPAA & GDPR require strict access control. Public DB ports are a massive violation.

Manual Audits are Slow

Weekly manual checks take 5-8 hours. Human error (e.g. missing shadow rules) is inevitable.

Dynamic Environments

Cloud resources spin up/down constantly. Snapshots get missed.

Our Goal

Continuous, Automated Compliance

Reduce audit time from Hours → Seconds

PRESENTER: ELINA HUANG

Problem Statement Summary

"How might we ensure that every EC2 instance and IAM User in our MedTech environment automatically adheres to security standards without slowing down development?"

Critical
Risk of Root/Admin compromise

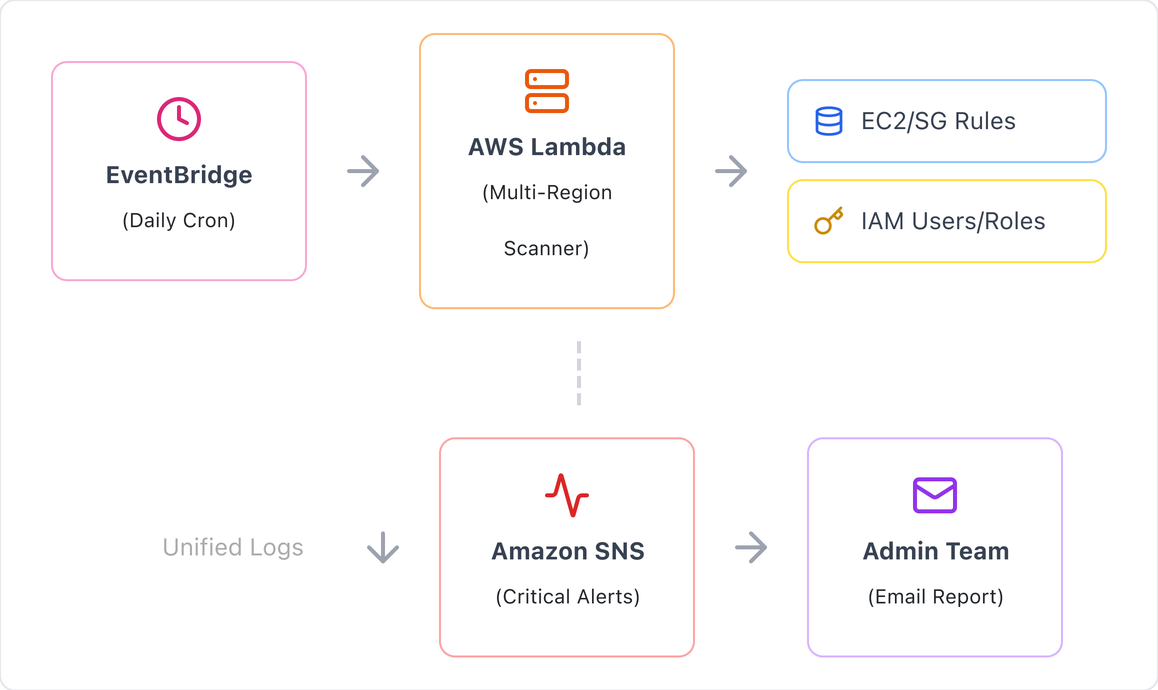
$2k+
Monthly waste on unused assets

High
Data Leak Potential

PRESENTER: YULIN XUE

High-Level Architecture

We utilized a **Serverless Event-Driven Architecture** to minimize cost and maintenance.



- **EventBridge:** Triggers the audit every 24 hours (Cron).
- **Lambda (Python):** Executes the compliance logic (Boto3) across multiple regions.
- **SNS:** Decouples the alert logic from the check logic.

PRESENTER: YULIN XUE

AWS Services & Data Flow

1. Trigger Phase

Amazon EventBridge Schedule invokes Lambda (Payload: ScanType: 'Full').

2. Execution Phase (Multi-Region)

Lambda assumes IAM Role → Iterates Regions (us-east-1, us-west-2) → Scans SGs & IAM Users.

3. Notification Phase

If `RiskLevel == CRITICAL/HIGH`, payload sent to SNS Topic → Subscribed Email receives detailed report.

PRESENTER: JIAMIN CAI

Implementation: Security Logic

1. Network Check (5 Dimensions)

- **Protocol:** TCP/UDP/All (is it too broad?)
- **Port Range:** Full (0-65535), SSH (22), DB (3306)
- **Source:** 0.0.0.0/0 (Danger) vs Internal CIDR
- **Intent:** Is a DB server accessible from Web?
- **Redundancy:** Are there shadow rules?

2. IAM Audit (Privilege)

- **Root Account:** MFA Enabled? (Must be Yes)
- **AdministratorAccess:** Direct attachment?
- **Stale Keys:** Active > 90 days?
- **Zombie Users:** Inactive users with permission?

Risk Classification Matrix

🔥 CRITICAL	⚠ HIGH	✓ SAFE
0.0.0.0/0 on 22/3389/DB	Stale Access Keys	Internal SG Ref
Root No MFA	AdminAccess on User	Least Privilege Role

PRESENTER: JIAMIN CAI

Code Structure

scanner.py (Enhanced)

```python
# Severity Definitions
CRITICAL = {22, 3389, 3306, 5432} # SSH, RDP, DBs
HIGH = {21, 25, 8080}

def classify_risk(port, source_cidr):
  if source_cidr == "0.0.0.0/0":
    if port in CRITICAL: return "CRITICAL"
    if port == "ALL": return "CRITICAL"
  return "LOW"

def scan_multi_region():
```

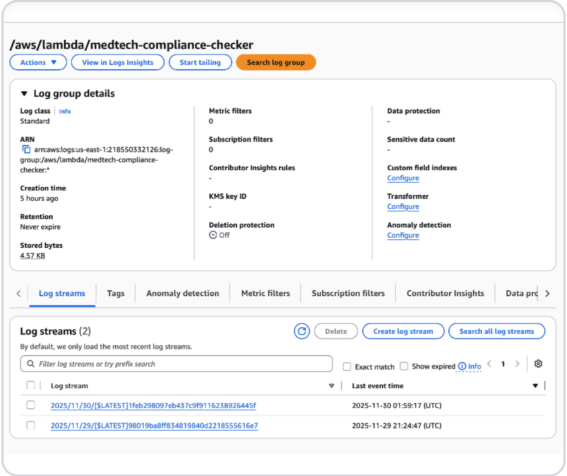
MEDSHIELD

Slide 8

PRESENTER: ELINA HUANG

Demo 1: Execution & Logs

>_ CloudWatch Logs



/aws/lambda/medtech-compliance-checker

▼ Log group details

Log class | Info
Standard

ARN
arn:aws:logs:us-east-1:218550332126:log-group:/aws/lambda/medtech-compliance-checker:*

Creation time
5 hours ago

Retention
Never expire

Stored bytes
4.57 KB

Metric filters
0

Subscription filters
0

Contributor Insights rules
-

KMS key ID
-

Deletion protection
⊖ Off

Data protection
-

Sensitive data count
-

Custom field indexes
Configure

Transformer
Configure

Anomaly detection
Configure

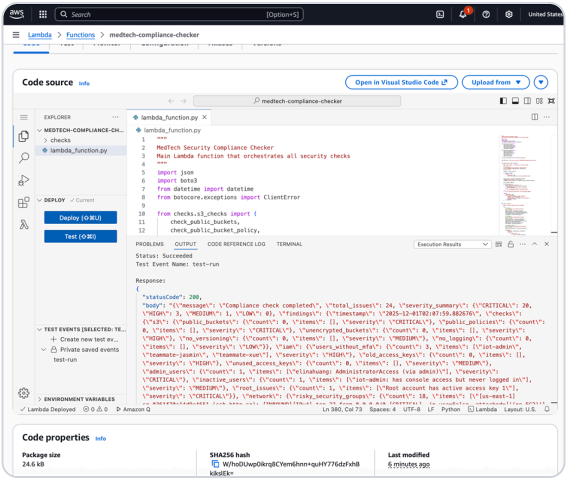
Log streams (2)

By default, we only load the most recent log streams.

Filter log streams or try prefix search
□ Exact match □ Show expired ⓘ Info
1

□	Log stream	Last event time
□	2025/11/30/[$LATEST]1feb298097eb437c9f9116238926445f	2025-11-30 01:59:17 (UTC)
□	2025/11/29/[$LATEST]98019ba8ff834819840d2218555616e7	2025-11-29 21:24:47 (UTC)

▷ Lambda Execution Result



```python
"""
MedTech Security Compliance Checker
Main Lambda function that orchestrates all security checks
"""
import json
import boto3
from datetime import datetime
from botocore.exceptions import ClientError

from checks.s3_checks import (
    check_public_buckets,
    check_public_bucket_policy,
```

```
Status: Succeeded
Test Event Name: test-run

Response:
{
  "statusCode": 200,
  "body": "{\"message\": \"Compliance check completed\", \"total_issues\": 24, \"severity_summary\": {\"CRITICAL\": 20,
  \"HIGH\": 3, \"MEDIUM\": 1, \"LOW\": 0}, \"findings\": {\"timestamp\": \"2025-12-01T02:07:59.882676\", \"checks\":
  {\"s3\": {\"public_buckets\": {\"count\": 0, \"items\": [], \"severity\": \"CRITICAL\"}, \"public_policies\": {\"count\":
  0, \"items\": [], \"severity\": \"CRITICAL\"}, \"unencrypted_buckets\": {\"count\": 0, \"items\": [], \"severity\":
  \"HIGH\"}, \"no_versioning\": {\"count\": 0, \"items\": [], \"severity\": \"MEDIUM\"}, \"no_logging\": {\"count\": 0,
  \"items\": [], \"severity\": \"LOW\"}}, \"iam\": {\"users_without_mfa\": {\"count\": 3, \"items\": [\"iot-admin\",
  \"teammate-jasmin\", \"teammate-xue\"], \"severity\": \"HIGH\"}, \"old_access_keys\": {\"count\": 0, \"items\": [],
  \"severity\": \"HIGH\"}, \"unused_access_keys\": {\"count\": 0, \"items\": [], \"severity\": \"MEDIUM\"},
  \"admin_users\": {\"count\": 1, \"items\": [\"elinahuang: AdministratorAccess (via admin)\"], \"severity\":
  \"CRITICAL\"}, \"inactive_users\": {\"count\": 1, \"items\": [\"iot-admin: has console access but never logged in\"],
  \"severity\": \"MEDIUM\"}, \"root_issues\": {\"count\": 1, \"items\": [\"Root account has active access key 1\"],
  \"severity\": \"CRITICAL\"}}, \"network\": {\"risky_security_groups\": {\"count\": 18, \"items\": [\"[us-east-1]
```

✓ Lambda Deployed ⊗ 0 ⚠ 0 ▷ Amazon Q
Ln 380, Col 73 Spaces: 4 UTF-8 LF Python Lambda Layout: U.S.

Code properties Info

Package size
24.6 kB

SHA256 hash
W/hoDUwp0ikrq8CYem6hnn+quHY776dzFxhBkikslEk=

Last modified
6 minutes ago

MEDSHIELD

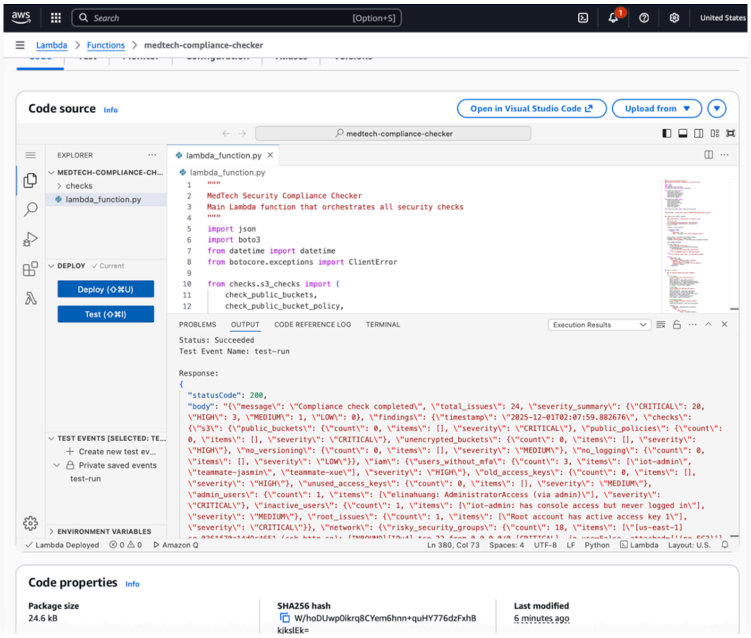
Slide 9

PRESENTER: ELINA HUANG

Demo 2: AWS Configuration

Interactive walkthrough of the deployed resources:

λ Function | Permissions | Trigger | SNS Topic | CloudWatch



lambda_function.py

```python
"""
MedTech Security Compliance Checker
Main Lambda function that orchestrates all security checks
"""

import json
import boto3
from datetime import datetime
from botocore.exceptions import ClientError

from checks.s3_checks import (
    check_public_buckets,
    check_public_bucket_policy,
```

```
Status: Succeeded
Test Event Name: test-run

Response:
{
  "statusCode": 200,
  "body": "{\"message\": \"Compliance check completed\", \"total_issues\": 24, \"severity_summary\": {\"CRITICAL\": 20,
  \"HIGH\": 3, \"MEDIUM\": 1, \"LOW\": 0}, \"findings\": {\"timestamp\": \"2025-12-01T02:07:59.882676\", \"checks\":
  {\"s3\": {\"public_buckets\": {\"count\": 0, \"items\": [], \"severity\": \"CRITICAL\"}, \"public_policies\": {\"count\":
  0, \"items\": [], \"severity\": \"CRITICAL\"}, \"unencrypted_buckets\": {\"count\": 0, \"items\": [], \"severity\":
  \"HIGH\"}, \"no_versioning\": {\"count\": 0, \"items\": [], \"severity\": \"MEDIUM\"}, \"no_logging\": {\"count\": 0,
  \"items\": [], \"severity\": \"LOW\"}}, \"iam\": {\"users_without_mfa\": {\"count\": 3, \"items\": [\"iot-admin\",
  \"teammate-jasmin\", \"teammate-xue\"], \"severity\": \"HIGH\"}, \"old_access_keys\": {\"count\": 0, \"items\": [],
  \"severity\": \"HIGH\"}, \"unused_access_keys\": {\"count\": 0, \"items\": [], \"severity\": \"MEDIUM\"},
  \"admin_users\": {\"count\": 1, \"items\": [\"elinahuang: AdministratorAccess (via admin)\"], \"severity\":
  \"CRITICAL\"}, \"inactive_users\": {\"count\": 1, \"items\": [\"iot-admin: has console access but never logged in\"],
  \"severity\": \"MEDIUM\"}, \"root_issues\": {\"count\": 1, \"items\": [\"Root account has active access key 1\"],
  \"severity\": \"CRITICAL\"}}, \"network\": {\"risky_security_groups\": {\"count\": 18, \"items\": [\"[us-east-1]
```

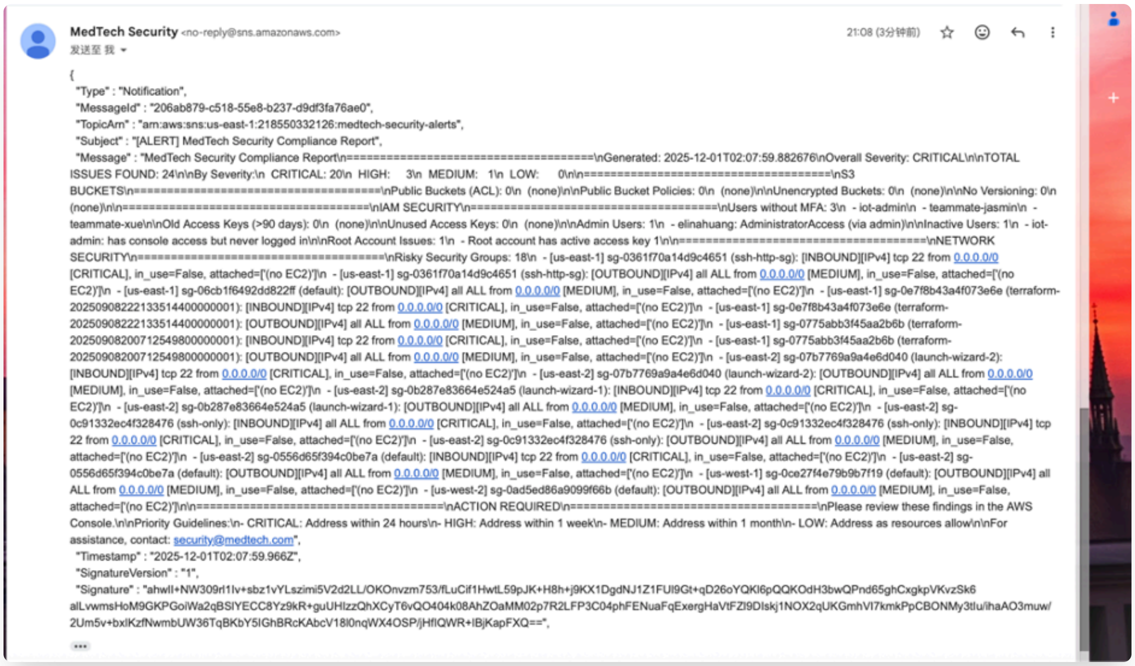
Code properties Info

Package size	SHA256 hash	Last modified
24.6 kB	W/hoDUwp0ikrq8CYem6hnn+quHY776dzFxhB kikslEk=	6 minutes ago

PRESENTER: ELINA HUANG

Demo 3: Notification Alert

Scenario: Admin receives email from SNS Topic `medtech-security-alerts`.



```
{
  "Type" : "Notification",
  "MessageId" : "206ab879-c518-55e8-b237-d9df3fa76ae0",
  "TopicArn" : "arn:aws:sns:us-east-1:218550332126:medtech-security-alerts",
  "Subject" : "[ALERT] MedTech Security Compliance Report",
  "Message" : "MedTech Security Compliance Report\n========================================\nGenerated: 2025-12-01T02:07:59.882676\nOverall Severity: CRITICAL\n\nTOTAL
ISSUES FOUND: 24\n\nBy Severity:\n  CRITICAL: 20\n  HIGH:     3\n  MEDIUM:   1\n  LOW:      0\n\n========================================\nS3
BUCKETS\n========================================\nPublic Buckets (ACL): 0\n  (none)\n\nPublic Bucket Policies: 0\n  (none)\n\nUnencrypted Buckets: 0\n  (none)\n\nNo Versioning: 0\n
(none)\n\n========================================\nIAM SECURITY\n========================================\nUsers without MFA: 3\n  - iot-admin\n  - teammate-jasmin\n  -
teammate-xue\n\nOld Access Keys (>90 days): 0\n  (none)\n\nUnused Access Keys: 0\n  (none)\n\nAdmin Users: 1\n  - elinahuang: AdministratorAccess (via admin)\n\nInactive Users: 1\n  - iot-
admin: has console access but never logged in\n\nRoot Account Issues: 1\n  - Root account has active access key 1\n\n========================================\nNETWORK
SECURITY\n========================================\nRisky Security Groups: 18\n  - [us-east-1] sg-0361f70a14d9c4651 (ssh-http-sg): [INBOUND][IPv4] tcp 22 from 0.0.0.0/0
[CRITICAL], in_use=False, attached=['(no EC2)']\n  - [us-east-1] sg-0361f70a14d9c4651 (ssh-http-sg): [OUTBOUND][IPv4] all ALL from 0.0.0.0/0 [MEDIUM], in_use=False, attached=['(no
EC2)']\n  - [us-east-1] sg-06cb1f6492dd822ff (default): [OUTBOUND][IPv4] all ALL from 0.0.0.0/0 [MEDIUM], in_use=False, attached=['(no EC2)']\n  - [us-east-1] sg-0e7f8b43a4f073e6e (terraform-
20250908222133514400000001): [INBOUND][IPv4] tcp 22 from 0.0.0.0/0 [CRITICAL], in_use=False, attached=['(no EC2)']\n  - [us-east-1] sg-0e7f8b43a4f073e6e (terraform-
20250908222133514400000001): [OUTBOUND][IPv4] all ALL from 0.0.0.0/0 [MEDIUM], in_use=False, attached=['(no EC2)']\n  - [us-east-1] sg-0775abb3f45aa2b6b (terraform-
20250908200712549800000001): [INBOUND][IPv4] tcp 22 from 0.0.0.0/0 [CRITICAL], in_use=False, attached=['(no EC2)']\n  - [us-east-1] sg-0775abb3f45aa2b6b (terraform-
20250908200712549800000001): [OUTBOUND][IPv4] all ALL from 0.0.0.0/0 [MEDIUM], in_use=False, attached=['(no EC2)']\n  - [us-east-2] sg-07b7769a9a4e6d040 (launch-wizard-2):
[INBOUND][IPv4] tcp 22 from 0.0.0.0/0 [CRITICAL], in_use=False, attached=['(no EC2)']\n  - [us-east-2] sg-07b7769a9a4e6d040 (launch-wizard-2): [OUTBOUND][IPv4] all ALL from 0.0.0.0/0
[MEDIUM], in_use=False, attached=['(no EC2)']\n  - [us-east-2] sg-0b287e83664e524a5 (launch-wizard-1): [INBOUND][IPv4] tcp 22 from 0.0.0.0/0 [CRITICAL], in_use=False, attached=['(no
EC2)']\n  - [us-east-2] sg-0b287e83664e524a5 (launch-wizard-1): [OUTBOUND][IPv4] all ALL from 0.0.0.0/0 [MEDIUM], in_use=False, attached=['(no EC2)']\n  - [us-east-2] sg-
0c91332ec4f328476 (ssh-only): [INBOUND][IPv4] all ALL from 0.0.0.0/0 [CRITICAL], in_use=False, attached=['(no EC2)']\n  - [us-east-2] sg-0c91332ec4f328476 (ssh-only): [INBOUND][IPv4] tcp
22 from 0.0.0.0/0 [CRITICAL], in_use=False, attached=['(no EC2)']\n  - [us-east-2] sg-0c91332ec4f328476 (ssh-only): [OUTBOUND][IPv4] all ALL from 0.0.0.0/0 [MEDIUM], in_use=False,
attached=['(no EC2)']\n  - [us-east-2] sg-0556d65f394c0be7a (default): [INBOUND][IPv4] tcp 22 from 0.0.0.0/0 [CRITICAL], in_use=False, attached=['(no EC2)']\n  - [us-east-2] sg-
0556d65f394c0be7a (default): [OUTBOUND][IPv4] all ALL from 0.0.0.0/0 [MEDIUM], in_use=False, attached=['(no EC2)']\n  - [us-west-1] sg-0ce27f4e79b9b7f19 (default): [OUTBOUND][IPv4] all
ALL from 0.0.0.0/0 [MEDIUM], in_use=False, attached=['(no EC2)']\n  - [us-west-2] sg-0ad5ed86a9099f66b (default): [OUTBOUND][IPv4] all ALL from 0.0.0.0/0 [MEDIUM], in_use=False,
attached=['(no EC2)']\n\n========================================\nACTION REQUIRED\n========================================\nPlease review these findings in the AWS
Console.\n\nPriority Guidelines:\n- CRITICAL: Address within 24 hours\n- HIGH: Address within 1 week\n- MEDIUM: Address within 1 month\n- LOW: Address as resources allow\n\nFor
assistance, contact: security@medtech.com",
  "Timestamp" : "2025-12-01T02:07:59.966Z",
  "SignatureVersion" : "1",
  "Signature" : "ahwlI+NW309rl1lv+sbz1vYLszimi5V2d2LL/OKOnvzm753/fLuCif1HwtL59pJK+H8h+j9KX1DgdNJ1Z1FUI9Gt+qD26oYQKl6pQQKOdH3bwQPnd65ghCxgkpVKvzSk6
alLvwmsHoM9GKPGoiWa2qBSIYECC8Yz9kR+guUHIzzQhXCyT6vQO404k08AhZOaMM02p7R2LFP3C04phFENuaFqExergHaVtFZI9Dlskj1NOX2qUKGmhVI7kmkPpCBONMy3tlu/ihaAO3muw/
2Um5v+bxlKzfNwmbUW36TqBKbY5IGhBRcKAbcV18l0nqWX4OSP/jHflQWR+IBjKapFXQ==",
```

PRESENTER: JIAMIN CAI

Metrics & Business Value

Time Savings

5 Hrs

2 Mins

Manual Audit vs. Automated Lambda

Compliance Coverage	**100% (IAM + EC2)**
Cost per Run	**< $0.01**
Human Error Rate	**0%**

PRESENTER: YULIN XUE

Future Enhancements

Auto-Remediation

Automatically close Port 22 or disable stale IAM Keys via Lambda.

QuickSight Dashboard

Visualizing compliance trends (e.g., "Open Ports over time").

S3 & RDS Scans

Expand scope to check S3 Public Access and RDS Encryption.

PRESENTER: ALL

Thank You

Questions?

Contact us regarding MedShield