Heinz College
Cloud Security
Fall 2025

MedTech AI Transformation Security Initiative

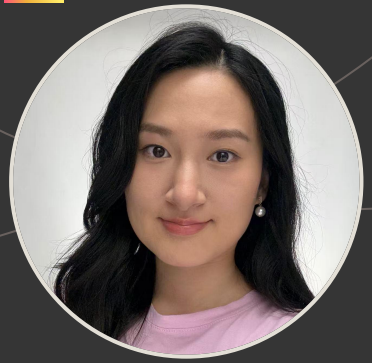
Cloud Security Engineer
Nicole Lyu, Alejandro Otero, Kelly Ta

Contents

1. Problem Statement
2. Solution Architecture
3. Implementation Design
4. Demo/Walkthrough
5. Metrics & Value
6. Future Enhancements

Cloud Security Engineer

Meet the Team



Nicole Lyu
Automation & Alert Engineer

Alejandro Otero
Infrastructure & Metrics Architect

Kelly Ta
Reporting & Visualization Lead

Carnegie Mellon University
Fall 2025

Problem Statement

MedTech lacks an automated, centralized system to continuously monitor and surface security risks across its AWS infrastructure.

Current Security Challenge

- No centralized view of security posture across IAM, EC2, S3, CloudTrail
- Configuration risks can go unnoticed
    - EX: Public resources, no MFA, unencrypted volumes

Problem Statement: Pain Points, Automation & Expected Benefits

Manual Process Pain Points

Security checks are ad hoc and very time consuming

No daily visibility

Inconsistent coverage/tracking and delayed detection

No unified reporting for leadership

Automation Opportunity

Automate daily collection of key security metrics

Real time issue detection

Centralize results into Cloudwatch dashboard

Standardize alerts and reporting

Expected Benefits

Continuous monitoring vs. periodic checks

Faster detection and response to misconfigurations

Reduced manual workload for engineers

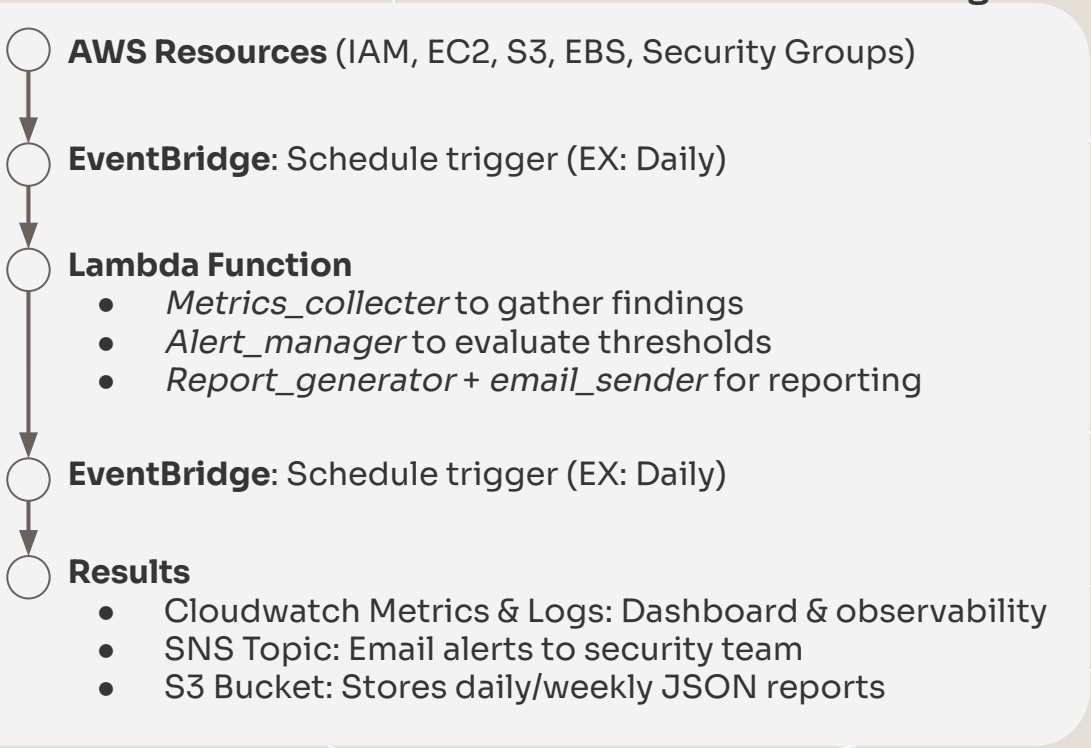
Clear, repeatable reporting for stakeholders

Solution Architecture

AWS Services Used

- **AWS Lambda**: Core automation & orchestration
- **Amazon EventBridge**: Scheduled execution
- **Amazon CloudWatch**: Metrics, logs, dashboard
- **Amazon SNS**: Alert notifications (email/integrations)
- **Amazon S3**: Report storage and retention
- **AWS IAM**: Secure access and least-privilege roles

Technical Architecture Diagram



Solution Architecture

Data Flow Visualization

1. **EventBridge** triggers the Lambda function on a schedule
2. **Lambda** calls *metric_collecter* to gather security metrics from IAM, EC2, S3, etc.
3. Metrics are published to **CloudWatch** for dashboard visualization
4. **Lambda** passes findings into *alert_manager* for threshold evaluation
    a. If thresholds are violated, **SNS** sends alerts to the security team
5. **Lambda** passes metrics to *report_generator* to build daily/weekly summaries
6. Reports saved to **S3** and summarized through **SNS** and *email_sender*
7. **CloudWatch Dashboard** visualizes current metrics for continuous monitoring

Integration Points

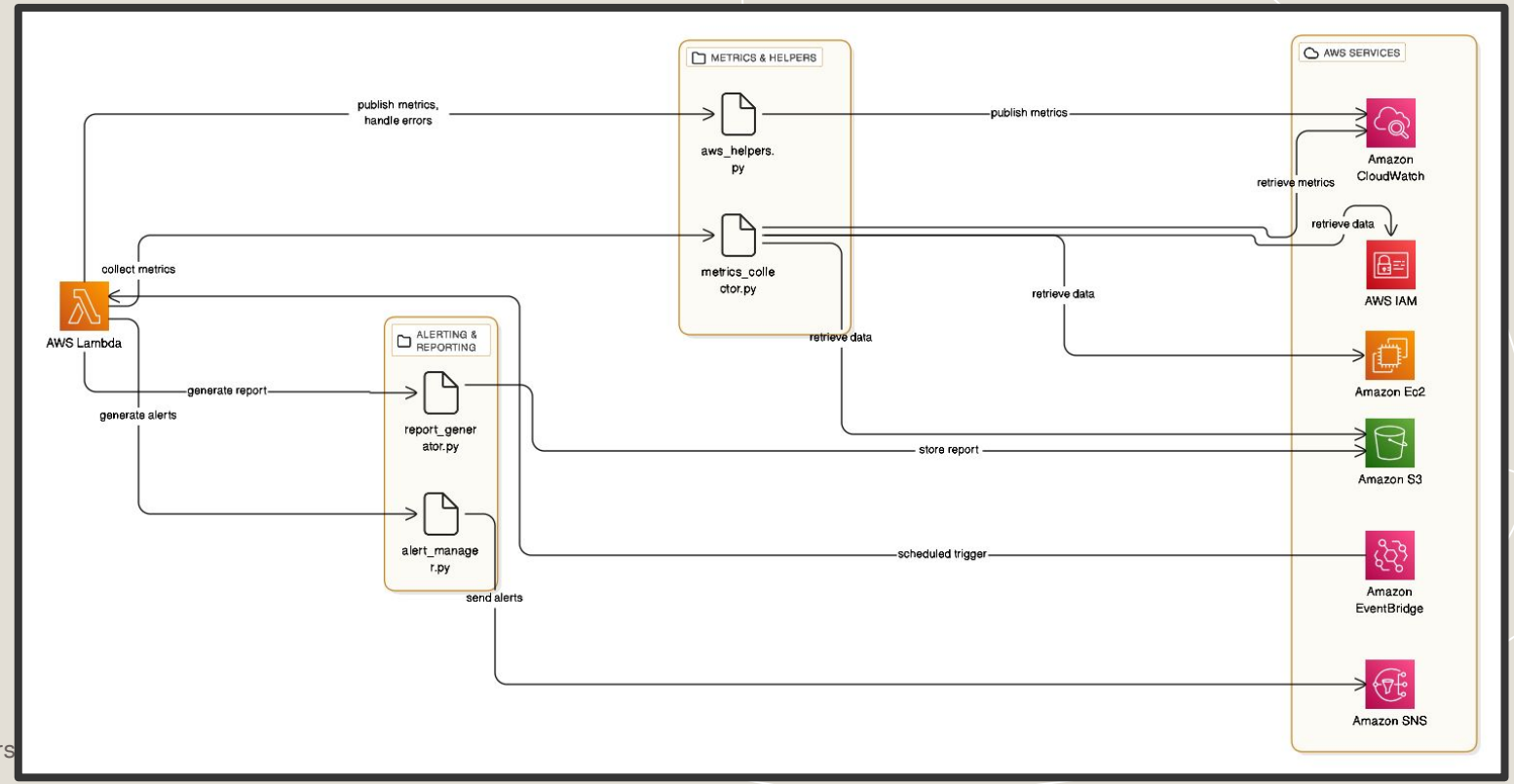
Lambda ↔ AWS Services
- Reads metrics (IAM/EC2/S3 API's)
- Publishes metric to CloudWatch
- Writes reports to S3

Lambda ↔ SNS
- Sends alerts and summary emails via SNS

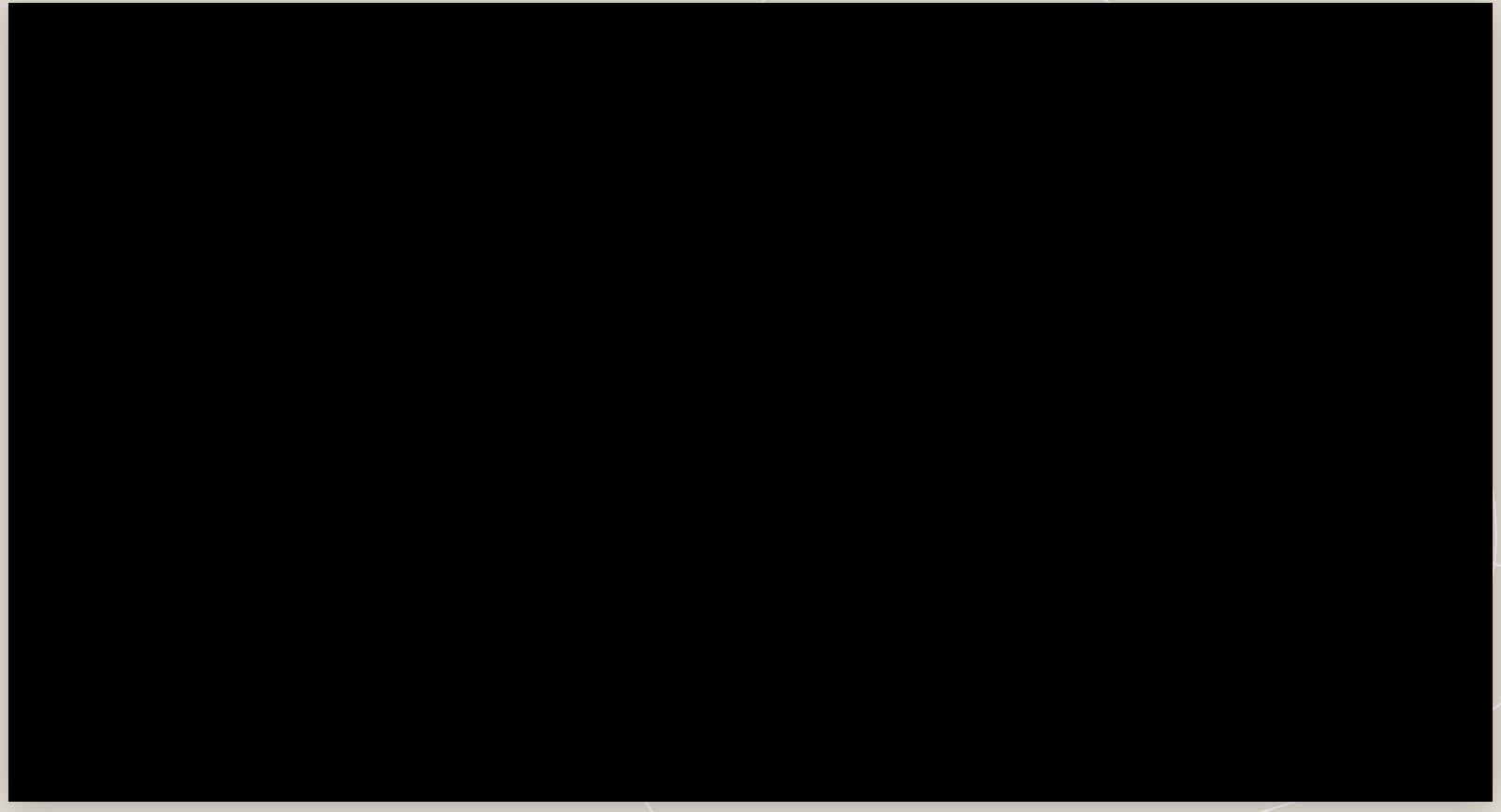
Lambda ↔ Reporting
- report_generator and email_sender for outputs

Cloudwatch ↔ Dashboard Users
- Consumed by security/engineering

Implementation Design



Demo



Metrics & Value

1

Time Saving

3 Hours/weekly (Manual checks)

vs.

1 Hour/weekly (Automatic report)

2

Security Improvements

Alert generation for rapid response:

- Unencrypted EBS volumes
- No MFA users
- Failed login attempts
- EC2/S3 exposure
- Cloudwatch status

3

Cost Implications

Less Hands, More Automation:

- Less labor cost
- Incident prevention cost

4

Success KPIs

% Accuracy

Mean detection time

% Usage of resources

Future Enhancements

Potential Improvements

- Expand security metrics
  - IAM roles
  - Permission analysis
- Reporting formats
  - CSV
  - PDF
  - Monthly rollups
- Improve visualization
  - Trend charts
  - Posture scoring

Scaling Considerations

- Support multi-account and multi-region monitoring
- Centralize metrics into “Security Monitoring” account
- Use cross-account IAM roles for scalable data collection
- Optimize Lambda for larger environments

Additional Features

- Machine learning-based anomaly detection
- Role-based dashboards
  - EX: Security, engineering, leadership
- Automated remediation for low-risk misconfigurations
- Integrations for real-time notifications

Thank you