STRIDE Threat Model Analysis

Project: project-denali/ai-ml-workstream

Document Version:	1.0
Date:	2025-07-25
Environment:	AWS GovCloud (us-gov-west-1)
Generated:	2025-07-25 01:51:49 UTC

Executive Summary

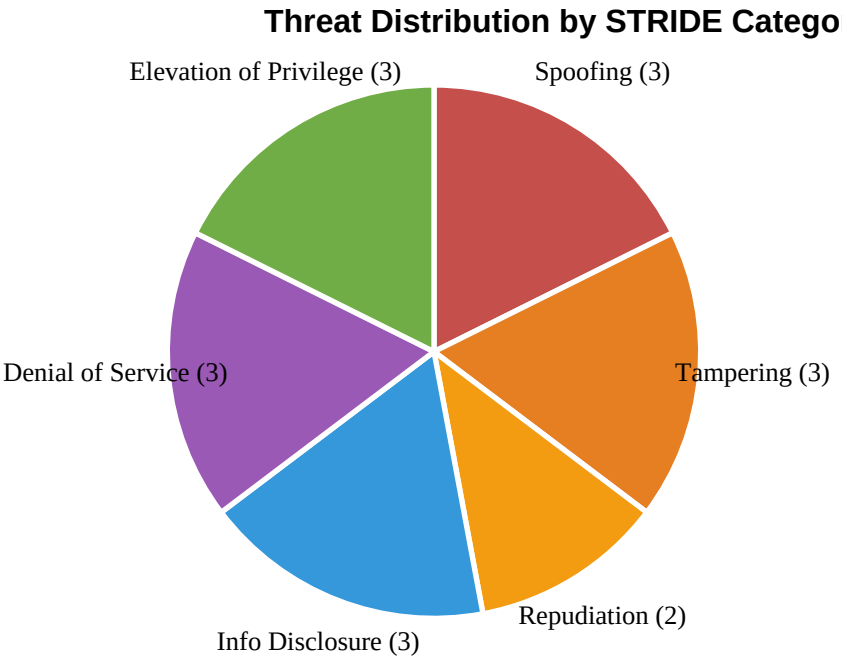
The AI-ML workstream implements an automated security vulnerability remediation system that leverages AWS Step Functions, Lambda, DynamoDB, and Amazon Bedrock to analyze code vulnerabilities from Fortify scans and automatically generate fixes using Large Language Models (LLM). The system integrates with Gitea for version control management and maintains a complete audit trail of remediation activities. **Overall Security Posture Assessment** - **Risk Level:** MEDIUM-HIGH - **Critical Gaps:** 7 identified - **Compliance Status:** Partial (requires additional controls for government standards) - **Immediate Actions Required:** 5 high-priority items **Key Security Concerns** 1. **AI/LLM Security Risks:** Potential for code injection through AI- generated fixes 2. **Secrets Management:** Hardcoded secret ARNs and insufficient rotation policies 3. **Network Security:** Limited network segmentation and monitoring 4. **Data Protection:** Sensitive code and vulnerability data handling 5. **Access Control:** Overly permissive IAM policies

Key Security Metrics

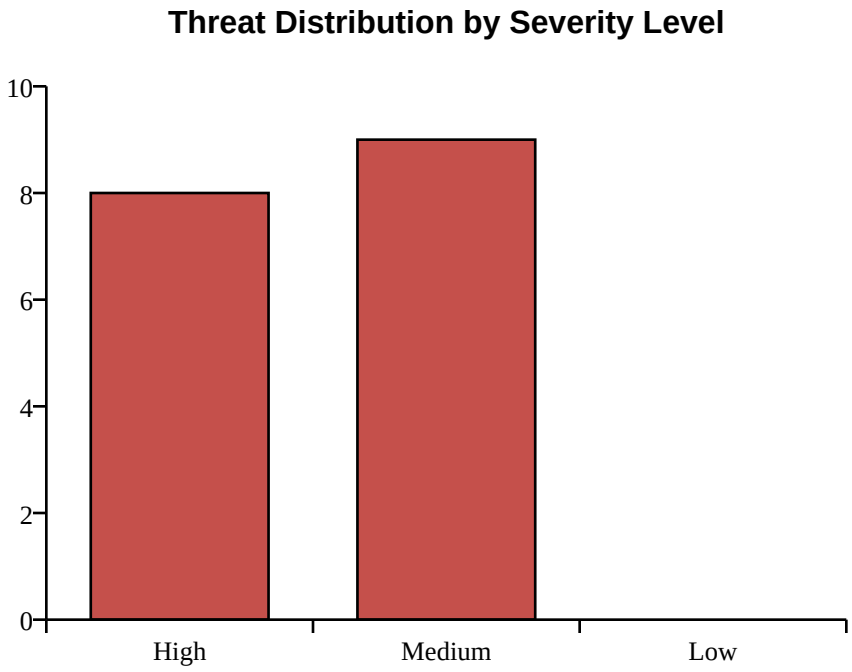
Metric	Value	Status
Total Threats Identified	17	Analyzed
High Severity Threats	8	Critical
Medium Severity Threats	9	Monitor
Low Severity Threats	0	Track
Overall Risk Level	MEDIUM-HIGH	Action Required

Visual Threat Analysis

STRIDE Category Distribution



Severity Level Distribution


Threat Distribution by Severity Level
10
8
6
4
2
0
High
Medium
Low

Detailed Threat Analysis

Spoofing Threats

S-001: Lambda Function Identity Spoofing

Severity:	HIGH
Likelihood:	MEDIUM
Description:	Malicious actors could potentially spoof Lambda function identities to access sensitive resources or execute unauthorized operations within the Step Functions workflow.
Impact:	Unauthorized access to code repositories, vulnerability data, or AI services could lead to data breaches or malicious code injection.

S-002: Gitea API Token Spoofing

Severity:	HIGH
Likelihood:	MEDIUM
Description:	Compromise of Gitea API tokens stored in Secrets Manager could allow attackers to impersonate the system and perform unauthorized repository operations.
Impact:	Malicious code commits, unauthorized access to source code, or manipulation of pull requests.

S-003: Step Functions Execution Spoofing

Severity:	MEDIUM
Likelihood:	LOW
Description:	Unauthorized execution of Step Functions workflows could trigger unintended remediation processes or bypass security controls.
Impact:	Unwanted code changes, resource consumption, or disruption of legitimate remediation processes.

Tampering Threats

T-001: AI-Generated Code Tampering

Severity:	HIGH

Likelihood:	HIGH
Description:	Malicious manipulation of prompts or responses to/from Amazon Bedrock could result in the injection of malicious code into the remediation process.
Impact:	Introduction of backdoors, vulnerabilities, or malicious functionality into production code.

T-002: DynamoDB Data Tampering

Severity:	MEDIUM
Likelihood:	MEDIUM
Description:	Unauthorized modification of vulnerability findings or remediation status in DynamoDB could lead to incomplete or incorrect remediation processes.
Impact:	False security posture reporting, missed vulnerabilities, or incorrect remediation tracking.

T-003: Git Repository Tampering

Severity:	HIGH
Likelihood:	MEDIUM
Description:	Unauthorized modification of source code in Git repositories could compromise the integrity of the remediation process or introduce malicious code.
Impact:	Compromised source code integrity, introduction of vulnerabilities, or bypass of security controls.

Repudiation Threats

R-001: Remediation Action Repudiation

Severity:	MEDIUM
Likelihood:	MEDIUM
Description:	Lack of comprehensive audit trails could make it difficult to prove or disprove specific remediation actions taken by the system.
Impact:	Inability to demonstrate compliance, investigate security incidents, or prove system integrity.

R-002: AI Decision Repudiation

Severity:	MEDIUM
Likelihood:	LOW
Description:	Inability to trace and verify AI-generated remediation decisions could lead to disputes about system behavior or effectiveness.
Impact:	Reduced trust in automated remediation, compliance issues, or inability to improve system performance.

Information Disclosure Threats

I-001: Source Code Exposure

Severity:	HIGH
Likelihood:	MEDIUM
Description:	Unauthorized access to source code through Lambda functions, DynamoDB, or network communications could expose sensitive intellectual property or security vulnerabilities.
Impact:	Loss of intellectual property, exposure of security vulnerabilities, or competitive disadvantage.

I-002: Vulnerability Data Exposure

Severity:	HIGH
Likelihood:	MEDIUM
Description:	Exposure of detailed vulnerability information could provide attackers with roadmaps for exploiting systems.
Impact:	Increased attack surface, targeted exploitation, or competitive intelligence gathering.

I-003: AI Model and Prompt Exposure

Severity:	MEDIUM
Likelihood:	LOW
Description:	Exposure of AI prompts, model configurations, or responses could reveal system capabilities and potentially enable prompt injection attacks.

Impact:	System manipulation, reduced effectiveness, or competitive intelligence gathering.

Denial of Service Threats

D-001: Lambda Function Resource Exhaustion

Severity:	MEDIUM
Likelihood:	MEDIUM
Description:	Excessive or malicious invocations could exhaust Lambda function resources, preventing legitimate remediation operations.
Impact:	System unavailability, delayed vulnerability remediation, or increased operational costs.

D-002: DynamoDB Throttling

Severity:	MEDIUM
Likelihood:	MEDIUM
Description:	High-volume operations could trigger DynamoDB throttling, causing workflow failures and system unavailability.
Impact:	System unavailability, data loss, or incomplete remediation processes.

D-003: Bedrock API Rate Limiting

Severity:	MEDIUM
Likelihood:	HIGH
Description:	Bedrock API rate limits could cause remediation workflows to fail or experience significant delays.
Impact:	Delayed vulnerability remediation, system unavailability, or incomplete processing.

Elevation of Privilege Threats

E-001: Lambda Function Privilege Escalation

Severity:	HIGH
Likelihood:	MEDIUM
Description:	Overly permissive IAM policies or vulnerabilities in Lambda functions could allow privilege escalation within the AWS environment.
Impact:	Unauthorized access to AWS resources, data breaches, or system compromise.

E-002: Cross-Service Privilege Escalation

Severity:	HIGH
Likelihood:	LOW
Description:	Compromise of one service could lead to unauthorized access to other connected services through service-to-service authentication.
Impact:	Lateral movement within the system, data breaches, or complete system compromise.

E-003: Gitea Integration Privilege Escalation

Severity:	MEDIUM
Likelihood:	MEDIUM
Description:	Compromise of Gitea integration could lead to unauthorized repository access or administrative privileges within the version control system.
Impact:	Unauthorized code access, malicious commits, or repository manipulation.

Priority Recommendations

■ HIGH Priority (Immediate Action Required)

- Implement AI Code Validation Pipeline
- Fix Secrets Management Hardcoding
- Apply Least Privilege IAM Policies
- Enable Network Security Monitoring
- Implement Data Integrity Validation

■■ MEDIUM Priority (Within 1 Month)

- Implement Comprehensive Audit Logging
- Add AI Decision Traceability
- Enable Advanced Threat Detection

■ LOW Priority (Within 3 Months)

- Implement Data Classification Framework
- Develop Disaster Recovery Procedures
- Add Performance Monitoring and Optimization