Threat Model and Risk Assessment Report

Executive Summary

This report presents the results of an automated threat modeling and risk assessment for the architecture diagram "LotsOGateways.png". The analysis identified 3 potential security threats that should be addressed.

Generated: 2025-07-22 11:54:47

Architecture Overview

The analyzed architecture consists of 1 components and 0 connections.

Components

ID	Name	Type
comp1	network 1	network

Threat Summary

Risk Level	Count	Percentage
High	1	33.3%
Medium	2	66.7%
Low	0	0.0%
Total	3	100%

Identified Threats

Detailed Threat Analysis

Repudiation Threats

Insufficient Logging (T005-comp1)

Description: Lack of proper logging makes it difficult to track security incidents

Category: Repudiation

Risk Level: MEDIUM

Impact: medium

Likelihood: possible

Affected Component: comp1

Recommended Mitigation:

1. Implement comprehensive logging and monitoring
2. Implement centralized logging with tamper-evident logs
3. Use a SIEM solution for log analysis
4. Ensure all security-relevant events are logged
5. Include unique request IDs in logs for traceability

Additional Information:

Repudiation threats involve users denying that they performed an action, and the system lacking the ability to prove otherwise. Proper logging and auditing are essential to mitigate repudiation threats.

References:

• OWASP Top 10 2021: A09 - Security Logging and Monitoring Failures

• CWE-778: Insufficient Logging

• NIST SP 800-53: AU-2 Audit Events

Insufficient Logging (T005-arch)

Description: Lack of proper logging makes it difficult to track security incidents

Category: Repudiation

Risk Level: MEDIUM

Impact: medium

Likelihood: possible

Affected Component: overall_architecture

Recommended Mitigation:

1. Implement comprehensive logging and monitoring
2. Implement centralized logging with tamper-evident logs
3. Use a SIEM solution for log analysis
4. Ensure all security-relevant events are logged
5. Include unique request IDs in logs for traceability

Additional Information:

Repudiation threats involve users denying that they performed an action, and the system lacking the ability to prove otherwise. Proper logging and auditing are essential to mitigate repudiation threats.

References:

• OWASP Top 10 2021: A09 - Security Logging and Monitoring Failures

• CWE-778: Insufficient Logging

• NIST SP 800-53: AU-2 Audit Events

Denial of Service Threats

Single Point of Failure (T006-arch)

Description: Architecture has components that represent single points of failure

Category: Denial of Service

Risk Level: HIGH

Impact: high

Likelihood: likely

Affected Component: overall_architecture

Recommended Mitigation:

1. Implement redundancy and high availability patterns

2. Implement rate limiting

3. Use a CDN for static content

4. Implement auto-scaling for dynamic resources

5. Use a DDoS protection service

Additional Information:

Denial of Service (DoS) attacks aim to make a system or resource unavailable to its intended users. This can be achieved by overwhelming the system with traffic, exploiting vulnerabilities, or exhausting system resources.

References:

• OWASP Top 10 2021: A05 - Security Misconfiguration

• CWE-400: Uncontrolled Resource Consumption

• NIST SP 800-53: SC-5 Denial of Service Protection