Architectural Diagram Threat Model & Risk Assessment

Executive Summary

This report presents a security analysis of the provided architectural diagram. A total of 3 components were identified, with 4 potential security threats and corresponding risk assessments.

Identified Components

Component 531 (database)
ID: comp_531

Component 900 (unknown)
ID: comp_900

Component 1164 (unknown)
ID: comp_1164

Identified Threats

High Severity Threats

SQL Injection (T003)
Type: Injection
Description: Databases may be vulnerable to SQL injection attacks
Risk: High likelihood, High impact (Score: 9)
Affected Components: Component 531
Mitigations:
- Use parameterized queries
- Implement input validation
- Apply principle of least privilege for database users

Sensitive Data Exposure (T004)
Type: Information Disclosure
Description: Databases may expose sensitive data if not properly secured
Risk: Medium likelihood, High impact (Score: 6)
Affected Components: Component 531
Mitigations:
- Encrypt sensitive data
- Implement proper access controls
- Use data masking for non-production environments

Medium Severity Threats

Insufficient Network Segmentation (T201)
Type: Lateral Movement
Description: Lack of network segmentation may allow lateral movement in case of breach
Risk: Medium likelihood, Medium impact (Score: 4)
Affected Components: Component 531, Component 900, Component 1164
Mitigations:
- Implement network segmentation
- Use firewalls between segments

- Apply zero trust principles

Single Point of Failure (T202)
Type: Availability
Description: Architecture may have single points of failure affecting availability
Risk: Medium likelihood, Medium impact (Score: 4)
Affected Components: Component 531, Component 900, Component 1164
Mitigations:
- Implement redundancy
- Use load balancing
- Design for fault tolerance

Risk Assessment

SQL Injection (T003)
Risk Score: 9 (High likelihood, High impact)
Recommendations:
- Use parameterized queries
- Implement input validation
- Apply principle of least privilege for database users
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

Sensitive Data Exposure (T004)
Risk Score: 6 (Medium likelihood, High impact)
Recommendations:
- Encrypt sensitive data
- Implement proper access controls
- Use data masking for non-production environments
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

Insufficient Network Segmentation (T201)
Risk Score: 4 (Medium likelihood, Medium impact)
Recommendations:
- Implement network segmentation
- Use firewalls between segments
- Apply zero trust principles
- Address within normal security improvement cycles
- Implement detection mechanisms

Single Point of Failure (T202)
Risk Score: 4 (Medium likelihood, Medium impact)
Recommendations:
- Implement redundancy
- Use load balancing
- Design for fault tolerance
- Address within normal security improvement cycles
- Implement detection mechanisms