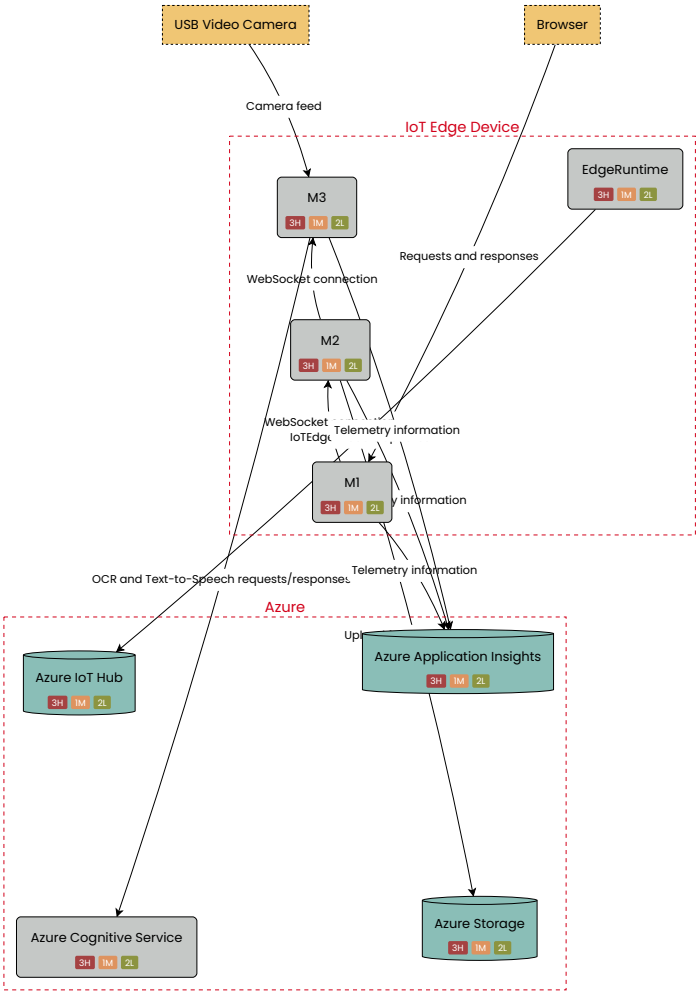
ThreatCanvas

by SecureFlag

My Threat Model

14/05/2025, 22:43:39

Diagram



Risk modifiers

Project type Application

Open risks

Threat	Node	Risk rating
Elevation of Privilege	Azure Application Insights	High
Spoofing	Azure Application Insights	High
Tampering	Azure Application Insights	High
Elevation of Privilege	Azure Cognitive Service	High
Spoofing	Azure Cognitive Service	High
Tampering	Azure Cognitive Service	High
Elevation of Privilege	Azure IoT Hub	High
Spoofing	Azure IoT Hub	High
Tampering	Azure IoT Hub	High
Elevation of Privilege	Azure Storage	High
Spoofing	Azure Storage	High
Tampering	Azure Storage	High
Elevation of Privilege	EdgeRuntime	High
Spoofing	EdgeRuntime	High
Tampering	EdgeRuntime	High
Elevation of Privilege	M1	High
Spoofing	M1	High
Tampering	M1	High
Elevation of Privilege	M2	High
Spoofing	M2	High
Tampering	M2	High
Elevation of Privilege	M3	High
Spoofing	M3	High

Threat	Node	Risk rating
Tampering	M3	High
Denial of Service	Azure Application Insights	Moderate
Denial of Service	Azure Cognitive Service	Moderate
Denial of Service	Azure IoT Hub	Moderate
Denial of Service	Azure Storage	Moderate
Denial of Service	EdgeRuntime	Moderate
Denial of Service	M1	Moderate
Denial of Service	M2	Moderate
Denial of Service	M3	Moderate
Information Disclosure	Azure Application Insights	Low
Repudiation	Azure Application Insights	Low
Information Disclosure	Azure Cognitive Service	Low
Repudiation	Azure Cognitive Service	Low
Information Disclosure	Azure IoT Hub	Low
Repudiation	Azure IoT Hub	Low
Information Disclosure	Azure Storage	Low
Repudiation	Azure Storage	Low
Information Disclosure	EdgeRuntime	Low
Repudiation	EdgeRuntime	Low
Information Disclosure	M1	Low
Repudiation	M1	Low
Information Disclosure	M2	Low
Repudiation	M2	Low
Information Disclosure	M3	Low
Repudiation	M3	Low

Node analysis

M1

Component	Generic Process
Trust boundary	IoT Edge Device

Denial of Service

Risk rating	Moderate
Status	Open

Firewall

Implemented	No

Mitigate Automated Attacks

Implemented	No

Elevation of Privilege

Risk rating	High
Status	Open

Apply Least Privilege

Implemented	No

Enforce Authorization

Implemented	No

Information Disclosure

Risk rating	Low
Status	Open

Encrypt Sensitive Information

Implemented	No

Redact Sensitive Data

Implemented	No

Secret Management

Implemented	No

Secure Connections with Strong Encryption

Implemented	No

Repudiation

Risk rating	Low
Status	Open

Enforce Authentication

Implemented	No

Enforce Authorization

Implemented	No

Logging and Monitoring

Implemented	No

Spoofing

Risk rating	High
Status	Open

Enforce Authorization

Implemented	No

Secure Connections with Strong Encryption

Implemented	No

Tampering

Risk rating	High
Status	Open

Encrypt Sensitive Information

Implemented	No

Input Sanitization

Implemented	No

Input Validation	
Implemented	No

Secure Connections with Strong Encryption	
Implemented	No

M2

Component	Generic Process
Trust boundary	IoT Edge Device

Denial of Service

Risk rating	Moderate
Status	Open

Firewall

Implemented	No

Mitigate Automated Attacks

Implemented	No

Elevation of Privilege

Risk rating	High
Status	Open

Apply Least Privilege

Implemented	No

Enforce Authorization

Implemented	No

Information Disclosure

Risk rating	Low
Status	Open

Encrypt Sensitive Information

Implemented	No

Redact Sensitive Data

Implemented	No

Secret Management

Implemented	No

Secure Connections with Strong Encryption

Implemented	No

Repudiation

Risk rating	Low
Status	Open

Enforce Authentication

Implemented	No

Enforce Authorization

Implemented	No

Logging and Monitoring

Implemented	No

Spoofing

Risk rating	High
Status	Open

Enforce Authorization

Implemented	No

Secure Connections with Strong Encryption

Implemented	No

Tampering

Risk rating	High
Status	Open

Encrypt Sensitive Information

Implemented	No

Input Sanitization

Implemented	No

Input Validation	
Implemented	No

Secure Connections with Strong Encryption	
Implemented	No

M3

Component	Generic Process
Trust boundary	IoT Edge Device

Denial of Service

Risk rating	Moderate
Status	Open

Firewall

Implemented	No

Mitigate Automated Attacks

Implemented	No

Elevation of Privilege

Risk rating	High
Status	Open

Apply Least Privilege

Implemented	No

Enforce Authorization

Implemented	No

Information Disclosure

Risk rating	Low
Status	Open

Encrypt Sensitive Information

Implemented	No

Redact Sensitive Data

Implemented	No

Secret Management

Implemented	No

Secure Connections with Strong Encryption

Implemented	No

Repudiation

Risk rating	Low
Status	Open

Enforce Authentication

Implemented	No

Enforce Authorization

Implemented	No

Logging and Monitoring

Implemented	No

Spoofing

Risk rating	High
Status	Open

Enforce Authorization

Implemented	No

Secure Connections with Strong Encryption

Implemented	No

Tampering

Risk rating	High
Status	Open

Encrypt Sensitive Information

Implemented	No

Input Sanitization

Implemented	No

Input Validation	
Implemented	No

Secure Connections with Strong Encryption	
Implemented	No

EdgeRuntime

Component	Generic Process
Trust boundary	IoT Edge Device

Denial of Service

Risk rating	Moderate
Status	Open

Firewall

Implemented	No

Mitigate Automated Attacks

Implemented	No

Elevation of Privilege

Risk rating	High
Status	Open

Apply Least Privilege

Implemented	No

Enforce Authorization

Implemented	No

Information Disclosure

Risk rating	Low
Status	Open

Encrypt Sensitive Information

Implemented	No

Redact Sensitive Data

Implemented	No

Secret Management

Implemented	No

Secure Connections with Strong Encryption

Implemented	No

Repudiation

Risk rating	Low
Status	Open

Enforce Authentication

Implemented	No

Enforce Authorization

Implemented	No

Logging and Monitoring

Implemented	No

Spoofing

Risk rating	High
Status	Open

Enforce Authorization

Implemented	No

Secure Connections with Strong Encryption

Implemented	No

Tampering

Risk rating	High
Status	Open

Encrypt Sensitive Information

Implemented	No

Input Sanitization

Implemented	No

Input Validation	
Implemented	No

Secure Connections with Strong Encryption	
Implemented	No

Azure IoT Hub

Component	Generic Data Store
Trust boundary	Azure

Denial of Service

Risk rating	Moderate
Status	Open

Firewall

Implemented	No

Mitigate Automated Attacks

Implemented	No

Elevation of Privilege

Risk rating	High
Status	Open

Apply Least Privilege

Implemented	No

Enforce Authorization

Implemented	No

Information Disclosure

Risk rating	Low
Status	Open

Encrypt Sensitive Information

Implemented	No

Redact Sensitive Data

Implemented	No

Secret Management

Implemented	No

Secure Connections with Strong Encryption

Implemented	No

Repudiation

Risk rating	Low
Status	Open

Enforce Authentication

Implemented	No

Enforce Authorization

Implemented	No

Logging and Monitoring

Implemented	No

Spoofing

Risk rating	High
Status	Open

Enforce Authorization

Implemented	No

Secure Connections with Strong Encryption

Implemented	No

Tampering

Risk rating	High
Status	Open

Encrypt Sensitive Information

Implemented	No

Input Sanitization

Implemented	No

Input Validation	
Implemented	No

Secure Connections with Strong Encryption	
Implemented	No

Azure Cognitive Service

Component	Generic Process
Trust boundary	Azure

Denial of Service

Risk rating	Moderate
Status	Open

Firewall

Implemented	No

Mitigate Automated Attacks

Implemented	No

Elevation of Privilege

Risk rating	High
Status	Open

Apply Least Privilege

Implemented	No

Enforce Authorization

Implemented	No

Information Disclosure

Risk rating	Low
Status	Open

Encrypt Sensitive Information

Implemented	No

Redact Sensitive Data

Implemented	No

Secret Management

Implemented	No

Secure Connections with Strong Encryption

Implemented	No

Repudiation

Risk rating	Low
Status	Open

Enforce Authentication

Implemented	No

Enforce Authorization

Implemented	No

Logging and Monitoring

Implemented	No

Spoofing

Risk rating	High
Status	Open

Enforce Authorization

Implemented	No

Secure Connections with Strong Encryption

Implemented	No

Tampering

Risk rating	High
Status	Open

Encrypt Sensitive Information

Implemented	No

Input Sanitization

Implemented	No

Input Validation	
Implemented	No

Secure Connections with Strong Encryption	
Implemented	No

Azure Application Insights

Component	Generic Data Store
Trust boundary	Azure

Denial of Service

Risk rating	Moderate
Status	Open

Firewall

Implemented	No

Mitigate Automated Attacks

Implemented	No

Elevation of Privilege

Risk rating	High
Status	Open

Apply Least Privilege

Implemented	No

Enforce Authorization

Implemented	No

Information Disclosure

Risk rating	Low
Status	Open

Encrypt Sensitive Information

Implemented	No

Redact Sensitive Data

Implemented	No

Secret Management

Implemented	No

Secure Connections with Strong Encryption

Implemented	No

Repudiation

Risk rating	Low
Status	Open

Enforce Authentication

Implemented	No

Enforce Authorization

Implemented	No

Logging and Monitoring

Implemented	No

Spoofing

Risk rating	High
Status	Open

Enforce Authorization

Implemented	No

Secure Connections with Strong Encryption

Implemented	No

Tampering

Risk rating	High
Status	Open

Encrypt Sensitive Information

Implemented	No

Input Sanitization

Implemented	No

Input Validation	
Implemented	No

Secure Connections with Strong Encryption	
Implemented	No

Azure Storage

Component	Generic Data Store
Trust boundary	Azure

Denial of Service

Risk rating	Moderate
Status	Open

Firewall

Implemented	No

Mitigate Automated Attacks

Implemented	No

Elevation of Privilege

Risk rating	High
Status	Open

Apply Least Privilege

Implemented	No

Enforce Authorization

Implemented	No

Information Disclosure

Risk rating	Low
Status	Open

Encrypt Sensitive Information

Implemented	No

Redact Sensitive Data

Implemented	No

Secret Management

Implemented	No

Secure Connections with Strong Encryption

Implemented	No

Repudiation

Risk rating	Low
Status	Open

Enforce Authentication

Implemented	No

Enforce Authorization

Implemented	No

Logging and Monitoring

Implemented	No

Spoofing

Risk rating	High
Status	Open

Enforce Authorization

Implemented	No

Secure Connections with Strong Encryption

Implemented	No

Tampering

Risk rating	High
Status	Open

Encrypt Sensitive Information

Implemented	No

Input Sanitization

Implemented	No

Input Validation	
Implemented	No

Secure Connections with Strong Encryption	
Implemented	No

Threat reference

Denial of Service

The node is susceptible to DoS attacks, which can render the node unavailable or unresponsive to legitimate users.

Elevation of Privilege

The node is vulnerable to elevation of privilege attacks, where an attacker gains higher- level permissions than intended.

Information Disclosure

The node leaks pieces of information, such as internal data or authentication material, which could be used to facilitate further attacks.

Repudiation

The node is prone to repudiation threats, where an attacker can deny their actions without the possibility of traceability.

Spoofing

The node is susceptible to identity spoofing, where an attacker may impersonate another user or entity.

Tampering

The node is vulnerable to data tampering, allowing unauthorized modification of data in transit or storage.

Control reference

Apply Least Privilege

Limit access privileges to those essential for performing the intended function.

Encrypt Sensitive Information

Ensure the sensitive information processed by the node is encrypted to comply with security and regulatory requirements.

Enforce Authentication

Enforce robust authentication mechanism to access the node's resources and functionalities, such as passwords, pre-shared tokens, or digital certificates.

Enforce Authorization

Ensure that the node uses strict access policies against unauthorized access.

Firewall

Use network appliances to filter ingress or egress traffic. Configure software on endpoints to filter network traffic.

Input Sanitization

Check untrusted input and remove anything that might be potentially dangerous.

Input Validation

Ensure that only properly formed data is entered into the system.

Logging and Monitoring

Keep detailed audit logs with timestamps for activities such as user logins, sensitive data access, access control changes, and administrative actions.

Mitigate Automated Attacks

Protect against automated attacks such as content scraping, password brute-force, or denial of service attacks.

Redact Sensitive Data

Redact, obfuscate, or tokenize sensitive information such as credit card numbers.

Secret Management

Securely encrypt, store, and manage access to secrets such as passwords, tokens, and encryption keys. This includes using centralized vaults, regular rotation, and auditing trails.

Secure Connections with Strong Encryption

Ensure that the node enforces network connections using protocols such as TLS or SSH, with approved versions and strong cipher suites to protect data in transit from exposure.