## resilient-six-threat-model

Owner: Jakub Gorczynski

Contributors:

Date Generated: Mon May 27 2024

## **Executive Summary**

### High level system description

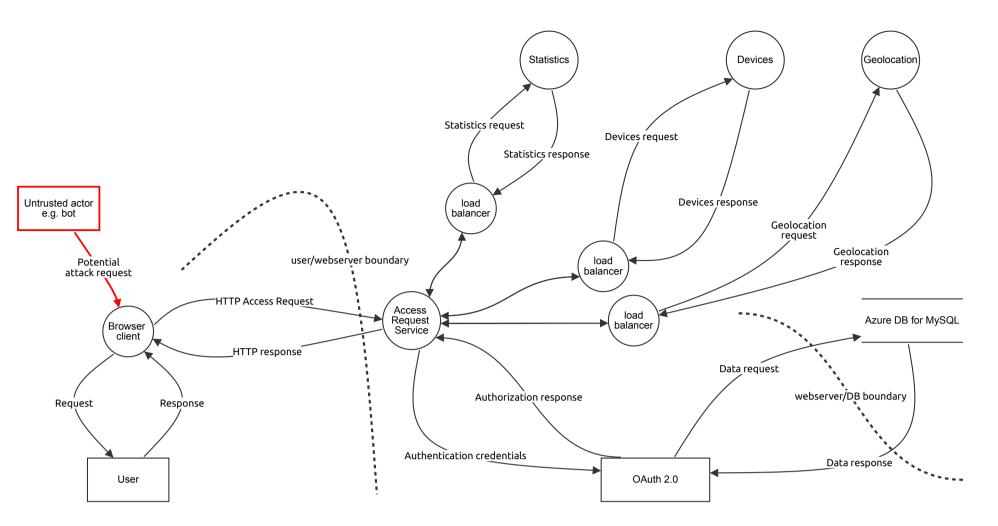
Not provided

### Summary

| Total Threats           | 4 |
|-------------------------|---|
| Total Mitigated         | 2 |
| Not Mitigated           | 2 |
| Open / High Priority    | 0 |
| Open / Medium Priority  | 2 |
| Open / Low Priority     | 0 |
| Open / Unknown Priority | 0 |

#### resilient-six-stride-model

STRIDE model for K8S high availability demo



### resilient-six-stride-model

| User (Acto           | r)        |       |            |        |       |              |                |
|----------------------|-----------|-------|------------|--------|-------|--------------|----------------|
|                      | •         |       |            |        |       |              |                |
| human client         |           |       |            |        |       |              |                |
| Number               | Title     | Туре  | Priority   | Status | Score | Description  | Mitigations    |
|                      |           |       |            |        |       |              |                |
|                      |           |       |            |        |       |              |                |
| Browser              |           |       |            |        |       |              |                |
| client (Pro          | cess)     |       |            |        |       |              |                |
|                      |           |       |            |        |       |              |                |
| Number               | Title     | Туре  | Priority   | Status | Score | Description  | Mitigations    |
|                      |           |       |            |        |       |              |                |
|                      |           |       |            |        |       |              |                |
| OAuth 2.0            | (Actor)   |       |            |        |       |              |                |
| Authorization provid | der       |       |            |        |       |              |                |
|                      |           |       |            |        |       |              |                |
| Number               | Title     | Туре  | Priority   | Status | Score | Description  | Mitigations    |
|                      |           |       |            |        |       |              |                |
| Access               |           |       |            |        |       |              |                |
| Request              |           |       |            |        |       |              |                |
| Service (Pr          | ocess)    |       |            |        |       |              |                |
|                      |           |       |            |        |       |              |                |
| Number               | Title     | Туре  | Priority   | Status | Score | Description  | Mitigations    |
| Training C           |           | .,,,, | · ···oricy | Julia  | 500.0 | Description. | - Integrations |
|                      |           |       |            |        |       |              |                |
| Request (D           | ata Flov  | v)    |            |        |       |              |                |
|                      |           |       |            |        |       |              |                |
|                      |           |       |            |        |       |              |                |
| Number               | Title     | Туре  | Priority   | Status | Score | Description  | Mitigations    |
|                      |           |       |            |        |       |              |                |
| Response             | (Data Flo | ow)   |            |        |       |              |                |
| •                    | •         | •     |            |        |       |              |                |
|                      |           |       |            |        |       |              |                |
| Number               | Title     | Туре  | Priority   | Status | Score | Description  | Mitigations    |

#### HTTP response (Data Flow)

| Number        | Title      | Туре        | Priority  | Status | Score | Description | Mitigations |
|---------------|------------|-------------|-----------|--------|-------|-------------|-------------|
|               |            |             |           |        |       |             |             |
| HTTP Acces    | s Reques   | t (Data Fl  | ow)       |        |       |             |             |
|               | •          | •           | ·         |        |       |             |             |
| Number        | Title      | Туре        | Priority  | Status | Score | Description | Mitigations |
| Number        | Titte      | Туре        | Filoney   | Status | Score | Descripcion | Micigations |
|               |            |             |           |        |       |             |             |
| Authorizati   | on respor  | ise (Data   | Flow)     |        |       |             |             |
|               |            |             |           |        |       |             |             |
| Number        | Title      | Туре        | Priority  | Status | Score | Description | Mitigations |
|               |            |             |           |        |       |             |             |
| Authentical   | tion crede | entials (Da | ata Flow) |        |       |             |             |
|               |            |             |           |        |       |             |             |
| Number        | Title      | Туре        | Priority  | Status | Score | Description | Mitigations |
|               |            |             |           |        |       |             |             |
|               |            |             |           |        |       |             |             |
| Data reques   | st (Data F | low)        |           |        |       |             |             |
|               |            |             |           |        |       |             |             |
| Number        | Title      | Туре        | Priority  | Status | Score | Description | Mitigations |
|               |            |             |           |        |       |             |             |
| Data respon   | ise (Data  | Flow)       |           |        |       |             |             |
|               |            |             |           |        |       |             |             |
| Number        | Title      | Туре        | Priority  | Status | Score | Description | Mitigations |
|               |            |             |           |        |       |             |             |
| Statistics re | anuest (D  | ata Flow)   |           |        |       |             |             |
| Statistics it | quest (D   | aca riow)   |           |        |       |             |             |
|               |            |             |           |        |       |             |             |
| Number        | Title      | Туре        | Priority  | Status | Score | Description | Mitigations |
|               |            |             |           |        |       |             |             |
| Devices res   | ponse (Da  | ata Flow)   |           |        |       |             |             |
|               |            |             |           |        |       |             |             |
| Number        | Title      | Туре        | Priority  | Status | Score | Description | Mitigations |
|               |            |             |           |        |       |             |             |

# Geolocation request (Data Flow)

| Number    | Title       | Туре | Priority | Status | Score | Description | Mitigations |
|-----------|-------------|------|----------|--------|-------|-------------|-------------|
|           |             |      |          |        |       |             |             |
| Geolocati | ion         |      |          |        |       |             |             |
| response  | (Data Flov  | w)   |          |        |       |             |             |
|           |             |      |          |        |       |             |             |
| Number    | Title       | Туре | Priority | Status | Score | Description | Mitigations |
|           |             |      |          |        |       |             |             |
| 1         | 451         |      |          |        |       |             |             |
| Data Flov | w (Data Flo | ow)  |          |        |       |             |             |
|           |             |      |          |        |       |             |             |
| Number    | Title       | Туре | Priority | Status | Score | Description | Mitigations |
|           |             |      |          |        |       |             |             |
| Data Flov | w (Data Flo | ow)  |          |        |       |             |             |
|           |             |      |          |        |       |             |             |
| Number    | Title       | Туре | Priority | Status | Score | Description | Mitigations |
|           |             |      |          |        |       |             |             |
| Data Flav | /Data El    |      |          |        |       |             |             |
| Data Flov | w (Data Flo | ow)  |          |        |       |             |             |
|           |             |      |          |        |       |             |             |
| Number    | Title       | Туре | Priority | Status | Score | Description | Mitigations |
|           |             |      |          |        |       |             |             |
| Data Flov | w (Data Fl  | ow)  |          |        |       |             |             |
|           |             |      |          |        |       |             |             |
| Number    | Title       | Туре | Priority | Status | Score | Description | Mitigations |
|           |             |      |          |        |       |             |             |
|           | <b>.</b>    | •    |          |        |       |             |             |
| Data Flov | w (Data Flo | ow)  |          |        |       |             |             |
|           |             |      |          |        |       |             |             |
| Number    | Title       | Туре | Priority | Status | Score | Description | Mitigations |

#### Data Flow (Data Flow)

| Number     | Title    | Туре      | Priority | Status | Score | Description | Mitigations |  |
|------------|----------|-----------|----------|--------|-------|-------------|-------------|--|
|            |          |           |          |        |       |             |             |  |
|            |          |           |          |        |       |             |             |  |
| Statistics | response | (Data Flo | ow)      |        |       |             |             |  |
|            |          |           |          |        |       |             |             |  |
| Number     | Title    | Туре      | Priority | Status | Score | Description | Mitigations |  |
|            |          |           |          |        |       |             |             |  |
|            |          |           |          |        |       |             |             |  |
|            |          |           |          |        |       |             |             |  |

# Potential attack request (Data Flow)

| Number | Title                                 | Туре                      | Priority | Status    | Score | Description   | Mitigations   |
|--------|---------------------------------------|---------------------------|----------|-----------|-------|---|---|
| 6      | Tampering                             | Tampering                 | Medium   | Open      |       | E.g. modification of frontend navigation in order to cause redirection to phishing page | Open - need to confirm whether there is any tampering/data validation mechanism implemented |
| 7      | Unauthorized access to sensitive data | Information<br>disclosure | Medium   | Mitigated |       | Compromise sensitive data due to faulty authorization process                           | Possible remedy - OAuth 2.0 + RBAC or ABAC (role-/attribute-based access control)           |
| 8      | DoS attempt                           | Denial of service         | High     | Mitigated |       | Overload and disruption of high availability system                                     | Each microservice is handled by separate load balancer                                      |

#### Devices request (Data Flow)

| Number | Title | Туре | Priority | Status | Score | Description | Mitigations |
|--------|-------|------|----------|--------|-------|-------------|-------------|
|        |       |      |          |        |       |             |             |

#### Azure DB for MySQL (Store)

| Number | Title | Туре | Priority | Status | Score | Description | Mitigations |
|--------|-------|------|----------|--------|-------|-------------|-------------|

#### **Statistics (Process)**

| Number   | Title | Туре | Priority | Status | Score | Description | Mitigations |
|----------|-------|------|----------|--------|-------|-------------|-------------|
| Hallibei | Titte | туре | Filolicy | Status | Score | Descripcion | Micigacions |

#### **Devices (Process)**

| Number | Title | Туре | Priority | Status | Score | Description | Mitigations |  |
|--------|-------|------|----------|--------|-------|-------------|-------------|--|
|        |       |      |          |        |       |             |             |  |

#### Geolocation (Process)

| Number | Title | Туре | Priority | Status | Score | Description | Mitigations |  |
|--------|-------|------|----------|--------|-------|-------------|-------------|--|
|        |       |      |          |        |       |             |             |  |

#### load balancer (Process)

| Number | Title | Туре | Priority | Status | Score | Description | Mitigations |
|--------|-------|------|----------|--------|-------|-------------|-------------|

#### load balancer (Process)

| Number | Title | Туре | Priority | Status | Score | Description | Mitigations |
|--------|-------|------|----------|--------|-------|-------------|-------------|

#### load balancer (Process)

| Number | Title | Туре | Priority | Status | Score | Description | Mitigations |  |
|--------|-------|------|----------|--------|-------|-------------|-------------|--|
|        |       |      |          |        |       |             |             |  |

# Untrusted actor e.g. bot (Actor)

| Number | Title             | Туре     | Priority | Status | Score | Description                           | Mitigations  |
|--------|-------------------|----------|----------|--------|-------|---------------------------------------|--|
| 0      | New STRIDE threat | Spoofing | Medium   | Open   |       | Provide a description for this threat | Provide remediation for this threat or a reason if status is N/A |