resilient-six-threat-model

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
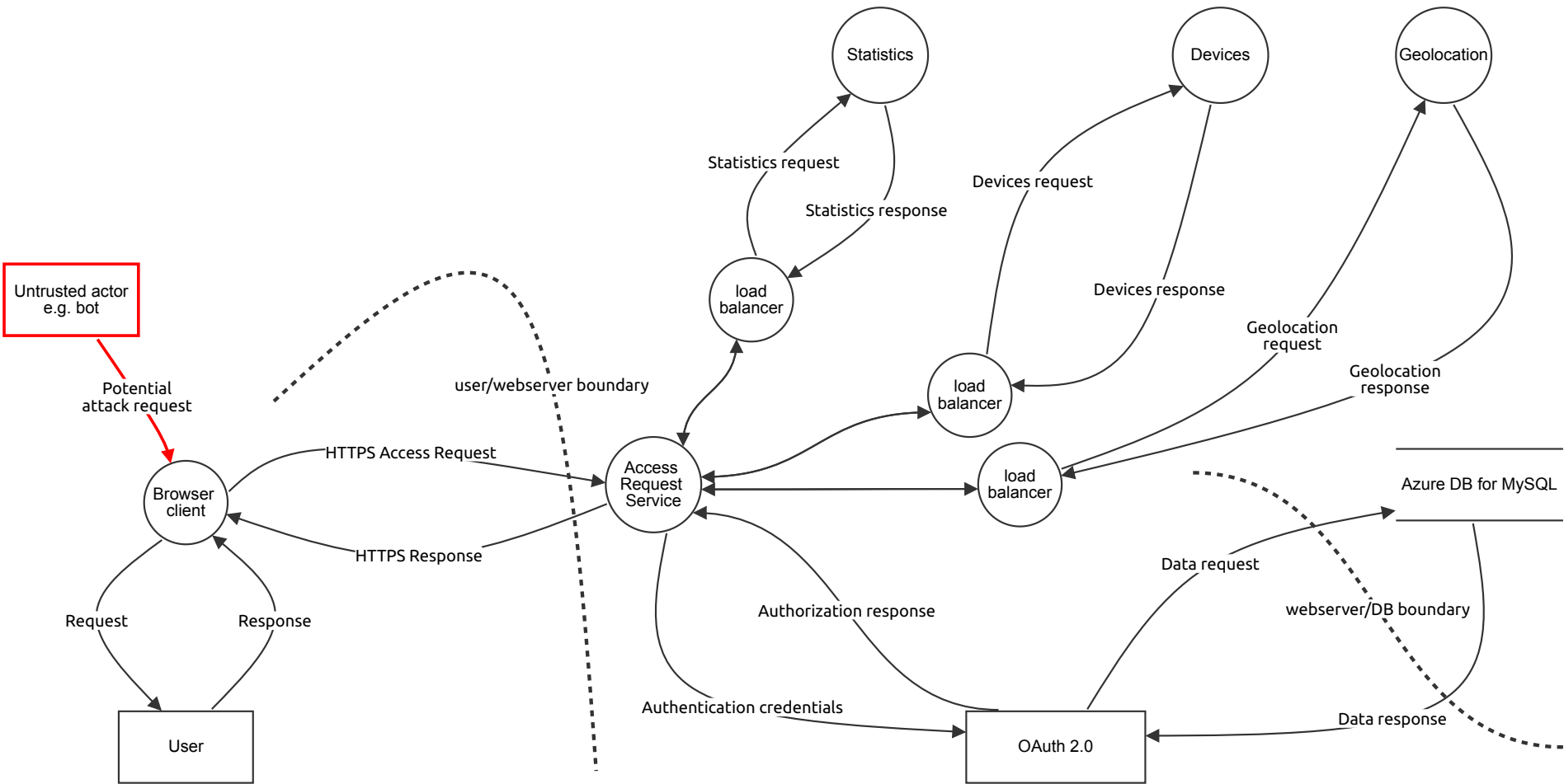
resilient-six-stride-model

User (Actor)

human client

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Browser client (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

OAuth 2.0 (Actor)

Authorization provider

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Access Request Service (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

HTTPS Access Request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Authorization response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Authentication credentials (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Statistics request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Devices response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Geolocation request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Geolocation response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Statistics response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Potential
attack request (Data Flow)

Number	Title	Type	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 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	Type	Priority	Status	Score	Description	Mitigations

HTTPS Response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Azure DB for MySQL (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Statistics (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Devices (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Geolocation (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

load balancer (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

load balancer (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

load balancer (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Untrusted actor e.g. bot (Actor)

Number	Title	Type	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