cyberguard 2

Owner: G03
Reviewer: Mamoona & Touseef
Contributors: David, Andrea, Daniel
Date Generated: Mon Oct 14 2024

Executive Summary

High level system description

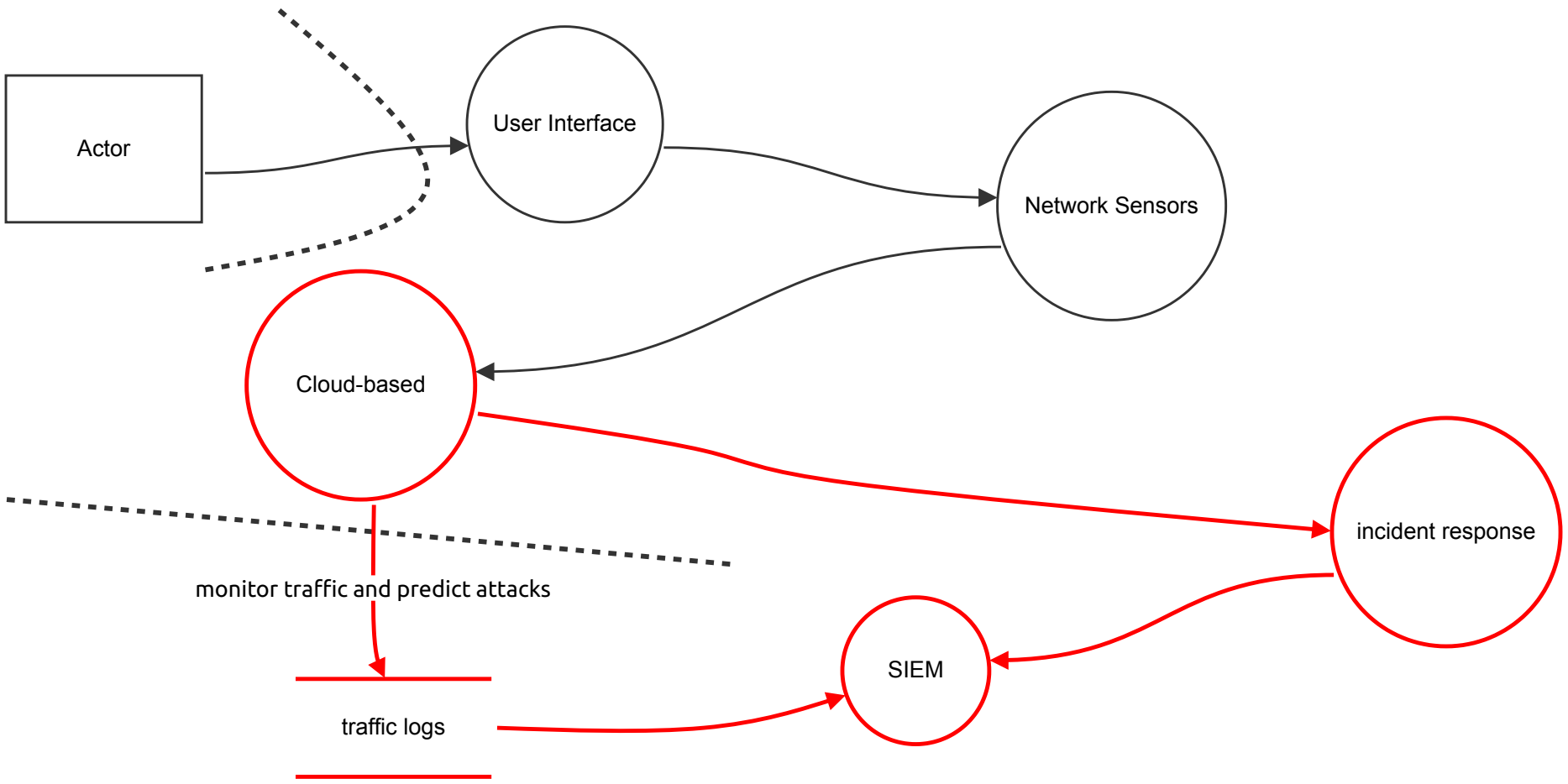
CyberGuard is a cutting-edge venture capital firm specializing in early-stage cyber security software investments. Founded by industry veterans, our mission is to empower innovative startups shaping the future of online protection. We invest in game-changing technologies addressing emerging threats and vulnerabilities in software and network connectivity. Our portfolio companies benefit from strategic guidance, access to top talent, and extensive networking opportunities within the cyber security ecosystem. With a keen eye for disruption and potential, we identify and support trailblazers poised to revolutionize the industry.

Summary

Total Threats	10
Total Mitigated	1
Not Mitigated	9
Open / High Priority	4
Open / Medium Priority	5
Open / Low Priority	0
Open / Unknown Priority	0

cyberguard 2

cyberguard 2



cyberguard 2

Actor (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Network Sensors (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Cloud-based (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
9	poison messages	Denial of service	Medium	Open		An attacker could generate a malicious message that the cloud cannot carry.	implement a poison message queue where messages are placed after a fixed number of tries.

User Interface (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

incident response (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
12	Poison messages	Denial of service	Medium	Open		An attacker could generate a malicious message that cannot be process.	Validate the content of all messages before processing.

SIEM (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	Poison Messages	Denial of service	Medium	Open		Provide a description for this threat	Implement a poison message queue where messages are placed after a fixed number of retries

Number	Title	Type	Priority	Status	Score	Description	Mitigations
7	poison messages 2	Denial of service	Medium	Open		An attacker could generate a Malicious message that the background worker cannot process	validate the content of all messages, before processing. reject any messages that have invalid content and log the rejection. do not log the malicious content - instead log a description of the error.

traffic logs (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
3	Unauthorised access	Information disclosure	High	Mitigated		an attacker can make a query call on the DB	All queries should be authenticated
5	data theft	Information disclosure	Medium	Open		An attacker could obtain DB data and use them for unauthorised purpose	use a firewall to restrict access to the database to only allow the worker IP address to access it.

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
2	New STRIDE threat	Tampering	High	Open		information provided by the database should not be tampered	strong access control mechanism

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
8	Data flow should use HTTP/S	Information disclosure	High	Open		these requests are made over the public internet and could be intercepted by an attacker.	the request should require HTTP/S. this will provide confidentiality and integrity. HTTP should not be supported.

monitor traffic and predict attacks (Data Flow)

sends in the captured network traffic to the database securely.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	Man in the middle attack	Information disclosure	High	Open	9	An attacker could intercept the DB queries in transit and obtain sensitive information, such as DB credentials, query parameters or query results (is unlikely since the data flow is over a private network).	Enforce an encrypted connection at the DB server.

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
14	Data flow should use HTTP/S	Information disclosure	High	Open		these responses are over the public internet and could be intercepted by an attacker.	the requests should require HTTP/S.