cyberguard 2

Owner: G03
Reviewer: Dr Mamoona Humayun & Dr Touseef Tahir
Contributors: David, Andrea, Daniel
Date Generated: Thu Oct 31 2024

Executive Summary

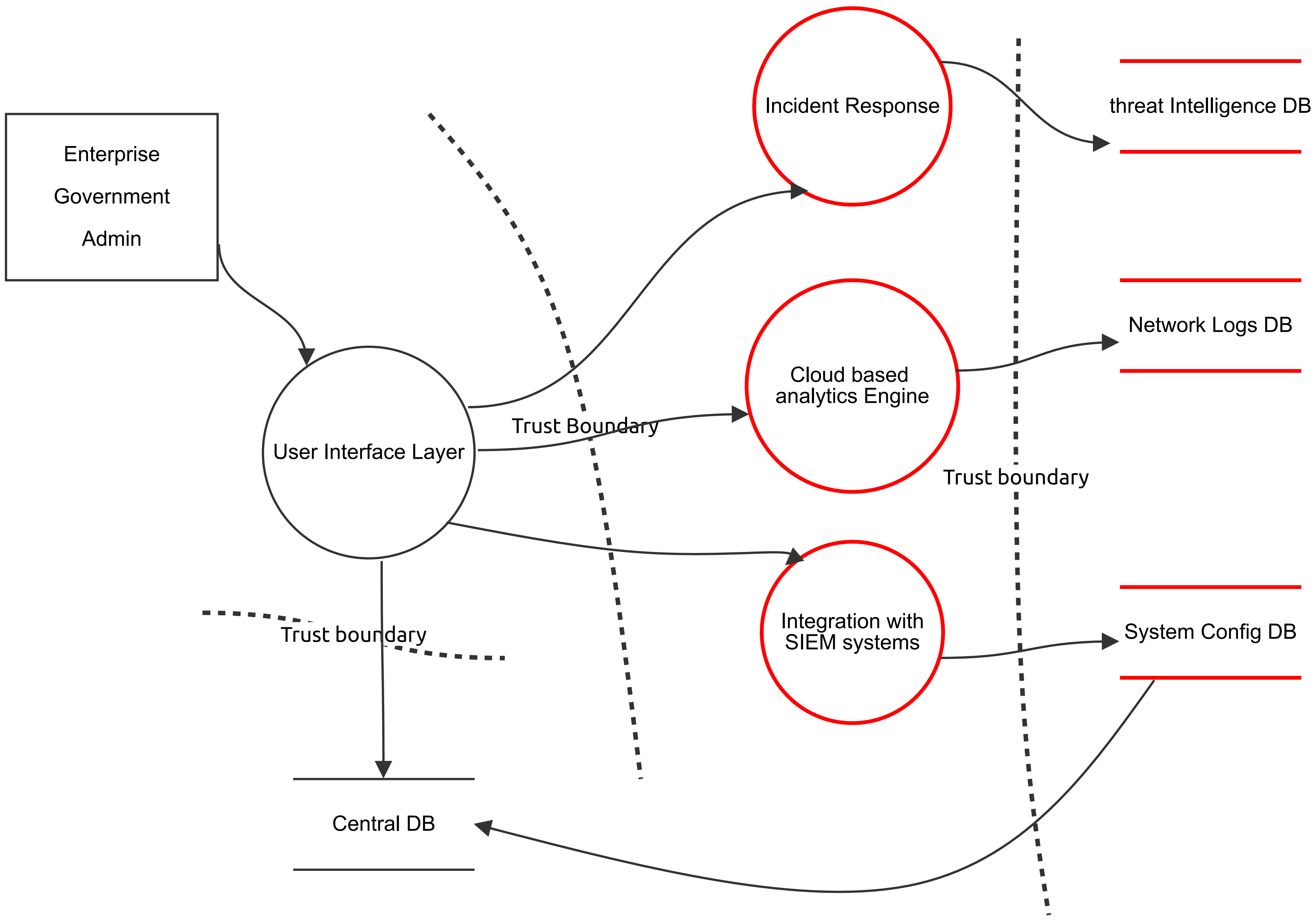
High level system description

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	24
Total Mitigated	18
Not Mitigated	6
Open / High Priority	6
Open / Medium Priority	0
Open / Low Priority	0
Open / Unknown Priority	0

Cyberguard 2 Diagram



Cyberguard 2 Diagram

Enterprise

Government

Admin (Actor)

those are the actors of the system

Number	Title	Type	Priority	Status	Score	Description	Mitigations

User Interface Layer (Process)

this comprises of the web-based dashboard, real-time visibility and Incident monitoring

Number	Title	Type	Priority	Status	Score	Description	Mitigations
16	New STRIDE threat	Spoofing	Low	Mitigated	4	An attacker might create a fake UI to capture user credentials	Enforce HTTPS and require strong authentication methods, such as MFA, for access.
17	New STRIDE threat	Tampering	Medium	Mitigated	6	The UI could be manipulated to display incorrect information to users	Regularly validate UI code integrity, implement secure coding practices, and conduct security audits.

threat Intelligence DB (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
21	New STRIDE threat	Information disclosure	Medium	Mitigated	7	Unauthorized access or exposure of sensitive data, such as network logs or threat intelligence data, could lead to a data breach.	Use encrypted storage, restrict access, and enforce automated updates to keep intelligence data secure.
22	New STRIDE threat	Tampering	High	Open	8	Malicious actors might attempt to alter data in transit or stored in databases, potentially corrupting critical logs or security configurations.	Validate data sources for threat intelligence, use checksum verification, and track data source authenticity.

Network Logs DB (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
18	New STRIDE threat	Information disclosure	High	Open	9	logs stored could be leaked to unauthorized entities.	Encrypt logs at rest and in transit; restrict access to authorized roles.
19	New STRIDE threat	Tampering	High	Mitigated	8	The DB could be manipulated to display incorrect information to users.	Enable immutability features for logs, implement logging integrity checks, and use secure storage locations.

System Config DB (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
20	New STRIDE threat	Tampering	High	Open	8	Malicious actors might attempt to alter data in transit or stored in databases, potentially corrupting critical logs or security configurations.	Set permission boundaries, enforce MFA, and restrict configurations to privileged roles only.

Central DB (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
23	New STRIDE threat	Tampering	High	Mitigated	8	Malicious actors might attempt to alter data in transit or stored in databases, potentially corrupting critical logs or security configurations.	Enable immutability features for logs, implement logging integrity checks, and use secure storage locations.
24	New STRIDE threat	Information disclosure	Medium	Mitigated	7	Unauthorized access or exposure of sensitive data, such as network logs or threat intelligence data, could lead to a data breach.	Use encrypted storage, restrict access, and enforce automated updates to keep intelligence data secure.

Incident Response (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
10	Repudiation	Repudiation	High	Mitigated	7	Lack of accountability for actions taken by the incident response module could obscure incident tracking.	Enable detailed logging and use secure timestamps to maintain a clear record of all actions performed.
11	New STRIDE threat	Elevation of privilege	High	Open	8	Unauthorized users may attempt to gain privileged access to initiate incident responses.	Use role-based access control (RBAC), requiring elevated privileges for specific actions within the module, and implement multi-factor authentication (MFA).

Cloud based analytics Engine (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
12	New STRIDE threat	Tampering	High	Open	9	Unauthorized access could lead to data manipulation, causing inaccurate analytics.	Use strong encryption for data in transit and rest, employ AWS IAM roles to restrict access, and ensure data integrity checks like hashing.
13	New STRIDE threat	Information disclosure	Medium	Mitigated	5	Data processed by the engine could be leaked to unauthorized entities.	Implement data encryption, access control policies, and secure logging practices with role-based access to sensitive information.

Integration with SIEM systems (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
14	New STRIDE threat	Tampering	Medium	Mitigated	7	Data transferred between CyberSentry and the SIEM could be altered by attackers.	Ensure data integrity through checksums, use TLS for encrypted connections, and set up audit logs.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
15	New STRIDE threat	Denial of service	High	Open	8	An overload of data could cause SIEM integration issues, potentially missing important events.	Implement data rate controls and create alert thresholds to prevent overloading the SIEM system.

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 threatData flow should use HTTP/S	Information disclosure	Medium	Mitigated	5	These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported.

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	Data flow should use HTTP/S	Information disclosure	Medium	Mitigated	5	These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported.

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
3	Data flow should use HTTP/S	Information disclosure	Medium	Mitigated	5	These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported.

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
5	Data flow should use HTTP/S	Information disclosure	Medium	Mitigated	5	These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported.

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
7	Data flow should use HTTP/S	Information disclosure	Medium	Mitigated	5	These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported.

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
8	Data flow should use HTTP/S	Information disclosure	Medium	Mitigated	5	These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported.

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	Data flow should use HTTP/S	Information disclosure	Medium	Mitigated	5	These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported.
9	Tampering with Claim Data	Tampering	Medium	Mitigated	5	Attackers could alter claims data, leading to fraudulent claims processing or unauthorised claims approvals.	Implement input validation, data integrity checks, and maintain an audit trail for all changes to claims data.

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	Data flow should use HTTP/S	Information disclosure	Medium	Mitigated	5	These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported.