Defence Ventura DFD

Owner:
Reviewer:
Contributors:
Date Generated: Wed Oct 30 2024

Executive Summary

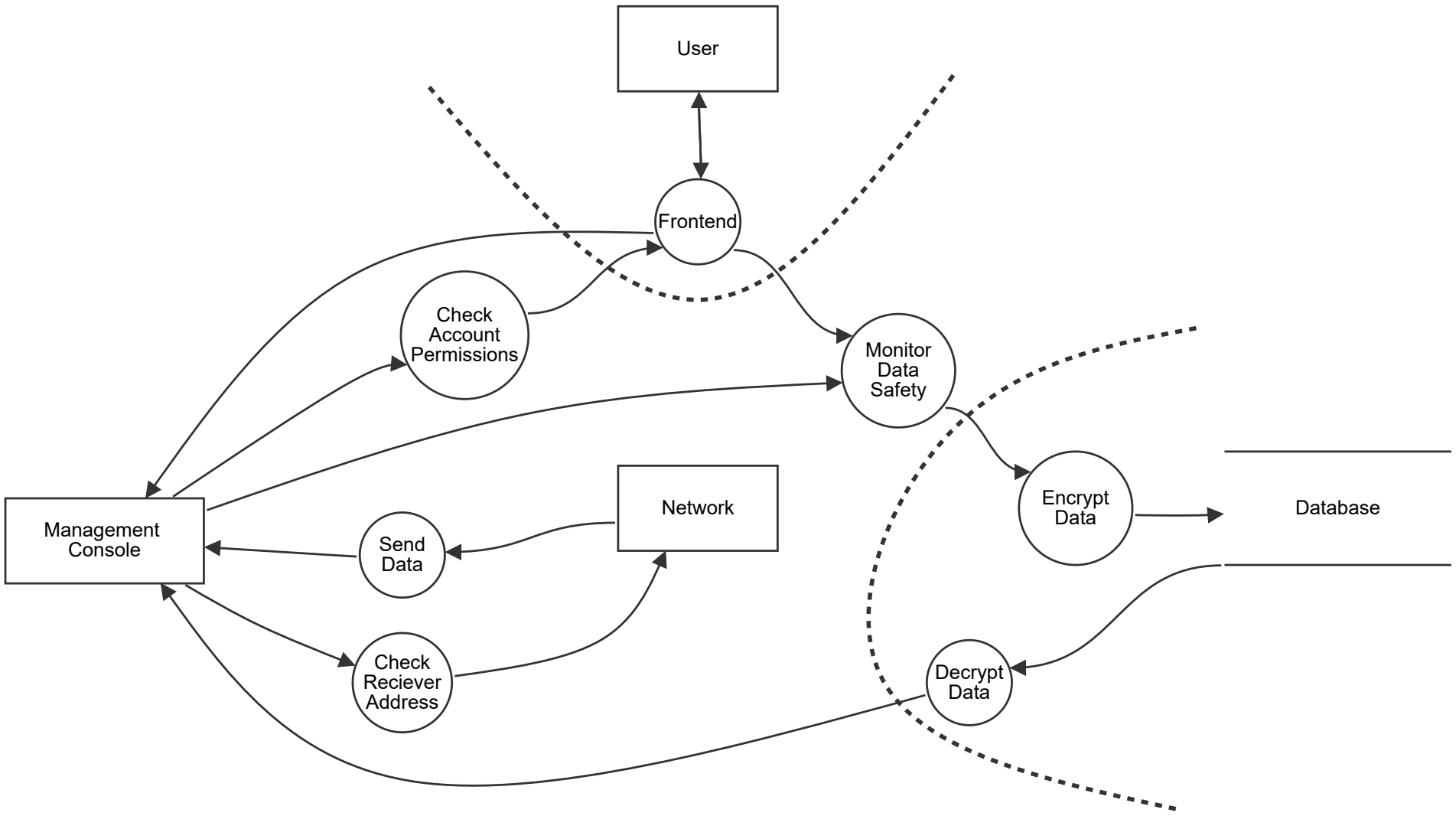
High level system description

Not provided

Summary

Total Threats	7
Total Mitigated	7
Not Mitigated	0
Open / High Priority	0
Open / Medium Priority	0
Open / Low Priority	0
Open / Unknown Priority	0

Defence Ventura DFD



Defence Ventura DFD

Frontend (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
105	Account breach	Spoofing	High	Mitigated		The user could possibly modify the system if they have enough privileges	Appropriately authorise the user and introduce integrity checks (such as Hashes and Digital Signatures)
110	DDOS attack	Denial of service	Low	Mitigated		Attacker launches a denial of service attack preventing the network from being used	Network monitoring to ensure packets are from an authorised user

Send Data (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
102	Spoofing attack	Spoofing	High	Mitigated		An attacker could send a phishing email or a spear phishing attack to try and gain access to the system	The management system will recognise this attack and filter it out sending a report to a user.
112	Repudiation attack	Repudiation	Medium	Mitigated		An attacker manipulates logs to cover their actions.	Ensure appropriate authorisation is put in place, check audit logs and timestamps

Monitor Data Safety (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
108	manipulation of data	Tampering	Medium	Mitigated		An attacker abuses the application to perform unintended updates to a database.	Implement appropriate authorisation measures and introduce integrity checks, such as Hashes

Check Account Permissions (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
104	Access to too much information	Elevation of privilege	Medium	Mitigated		A user may access more data than they need allowing them to have too much control over a system	Give a user the minimum amount of permissions to be able to do their job

Check Reciever

Address (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
103	Wrongful request of data	Information disclosure	Medium	Mitigated		An attacker may try and request data from the database when not having permissions to do so, to gain privileged information	Monitor where the user is requesting data from, if its not an approved IP cancel the request. Also ensure that it is from an employees account