Threat Modeling Report

Created on 11/13/2023 7:30:29 PM

Threat Model Name: HealthProvider-User DFD

Owner: Logan Stranglen, Daniel Kaseya

Reviewer:

Contributors:

Description: Cardea Mobile Agent is a phone app intended for end-users of Cardea. The app is like a digital wallet that holds legal and medical information of the user. The app's data store is the smartphone itself. All data saved by the app is stored on the phone itself; not external servers. The traveler is the end-user. They interact with Cardea Mobile Agent as an app on their phone. The internet boundary is interacting with the Enterprise Issuer Agent. This is a labority, healthcare provider, or state health agency who identifies a Cardea account with a medical release credential via a QR code, and then sends them the lab result.

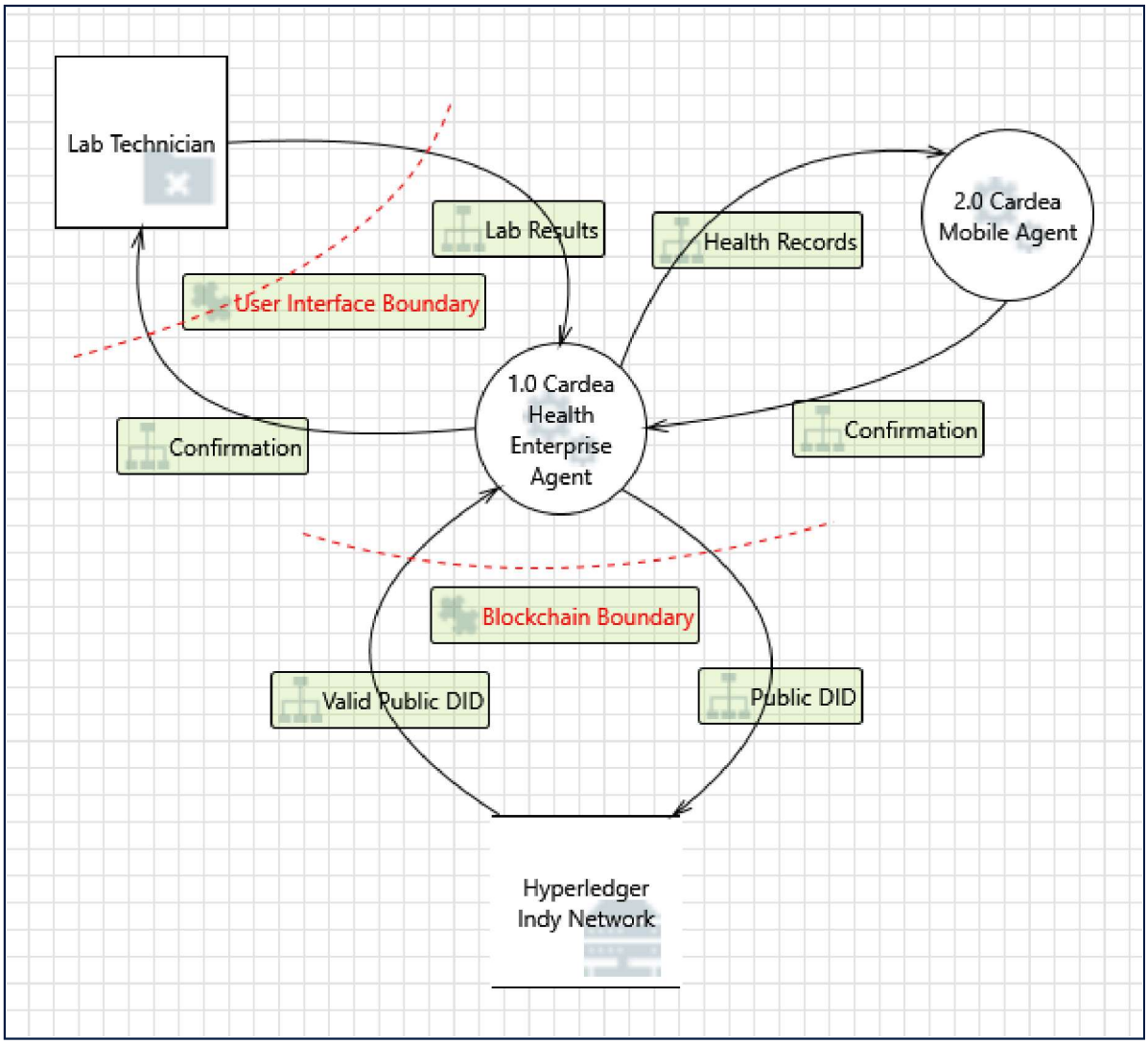
Assumptions: There are two other external entities of Cardea Mobile Agent: a verifier and a government enterprise agent. The threat boundary created by the verifier is better represented in the verifier DFD diagram by Cole. It was left out of here to avoid a superflous diagram. The government enterprise agent is only used on the Aruba version of Cardea. Aruba is a pacific island with a different legal jurisdiction that allows this external interactor. The Cardea team does not expect this entity to apply on a larger scale. In a level 2 DFD then this entity would be included. But it was decided that a level 1 DFD conveyed adequate information on threats for the system-of-interest.

External Dependencies: Cardea Mobile Agent is run on end-user smartphones. As such, the performance of the agent depends on the various software and hardware configurations of smartphones. For instance, a smartphone OS may prevent Cardea Mobile Agent from saving files, causing a DoS for the app.

Threat Model Summary:

Not Started	0
Not Applicable	13
Needs Investigation	1
Mitigation Implemented	19
Total	33
Total Migrated	0

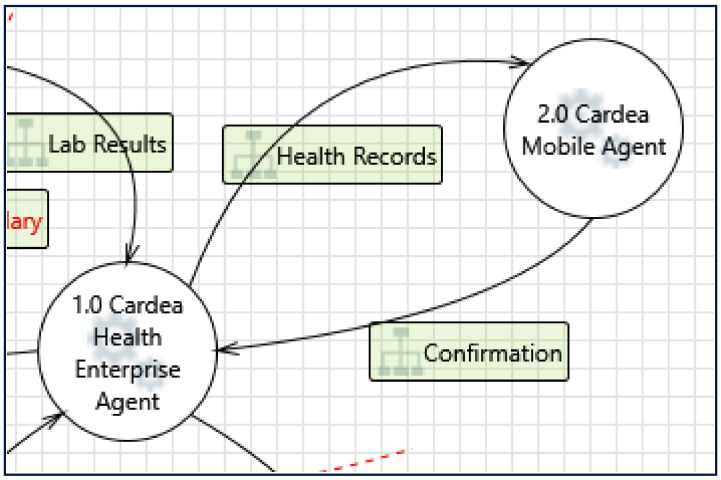
Diagram: HealthProvider-User DFD



HealthProvider-User DFD Diagram Summary:

Not Started	0
Not Applicable	13
Needs Investigation	1
Mitigation Implemented	19
Total	33
Total Migrated	0

Interaction: Confirmation



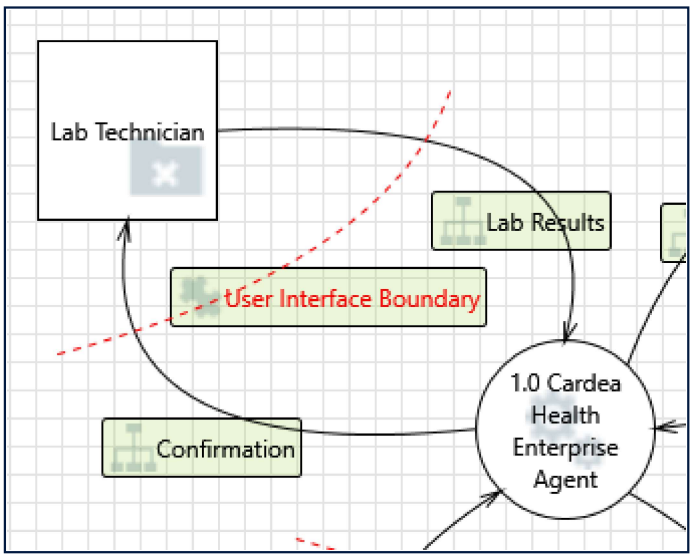
1. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: Low]

Category: Elevation Of Privilege

Description: 1.0 Cardea Health Enterprise Agent may be able to impersonate the context of 2.0 Cardea Mobile Agent in order to gain additional privilege.

Justification: This threat is considered low priority due to the unlikeliness of it occurring alongside there not being any additional privilege to gain (the health lab pulls results from blockchain).

Interaction: Confirmation



2. Spoofing of the Lab Technician External Destination Entity [State: Not Applicable] [Priority: Low]

Category: Spoofing

Description: Lab Technician may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Lab Technician. Consider using a standard authentication mechanism to identify the external entity.

Justification: This threat is considered invalid due to it not being possible. One would need credentials to upload information which requires authentication already.

3. External Entity Lab Technician Potentially Denies Receiving Data [State: Not Applicable] [Priority: Low]

Category: Repudiation

Description: Lab Technician claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: The threat is invalid as all the information the Cardea Health Enterprise Agent utilizes is going through and coming from the blockchain.
There would be a trail of both read and write edits logged from blockchain usage

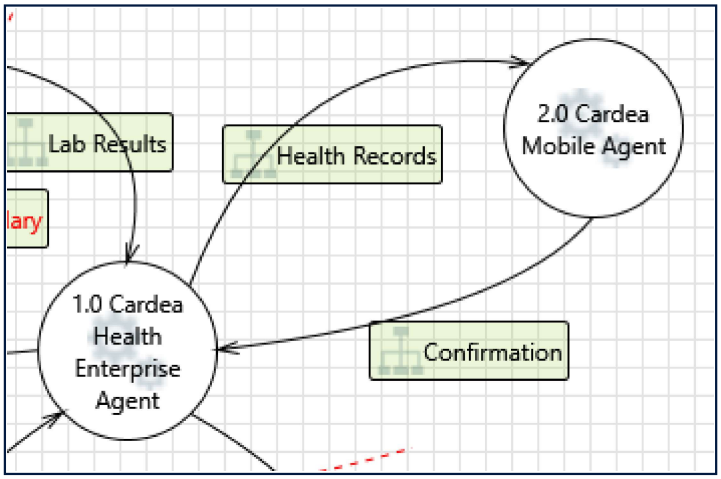
4. Data Flow Confirmation Is Potentially Interrupted [State: Mitigation Implemented] [Priority: Low]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: This threat is considered low priority due the unlikeliness of it occuring. Blockchain networks are resistant to traditional data interruptions because their decentralized design removes any single point of failure.

Interaction: Health Records



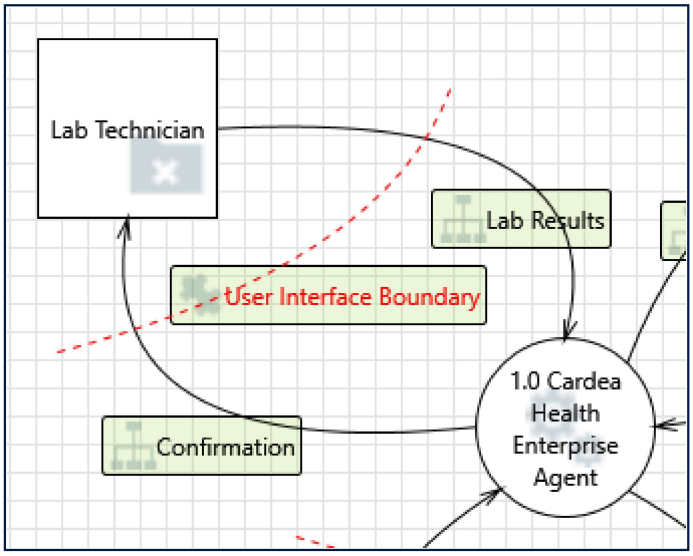
5. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: Low]

Category: Elevation Of Privilege

Description: 2.0 Cardea Mobile Agent may be able to impersonate the context of 1.0 Cardea Health Enterprise Agent in order to gain additional privilege.

Justification: This threat is considered low priority due to it not being possible. One would need credentials to upload information which requires authentication.

Interaction: Lab Results



6. Spoofing the Lab Technician External Entity [State: Needs Investigation] [Priority: High]

Category: Spoofing

Description: Lab Technician may be spoofed by an attacker and this may lead to unauthorized access to 1.0 Cardea Health Enterprise Agent. Consider using a standard authentication mechanism to identify the external entity.

Justification: MF2 can be implemented

7. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: Low]

Category: Elevation Of Privilege

Description: 1.0 Cardea Health Enterprise Agent may be able to impersonate the context of Lab Technician in order to gain additional privilege.

Justification: This threat is considered low priority due to the unlikeliness of it occurring alongside there not being any additional privilege to gain.

8. Spoofing the 1.0 Cardea Health Enterprise Agent Process [State: Mitigation Implemented] [Priority: Low]

Category: Spoofing

Description: 1.0 Cardea Health Enterprise Agent may be spoofed by an attacker and this may lead to information disclosure by Lab Technician. Consider using a standard authentication mechanism to identify the destination process.

Justification: This threat is considered invalid due to it not being possible. One would need credentials to upload information which requires authentication already.

9. Potential Lack of Input Validation for 1.0 Cardea Health Enterprise Agent [State: Mitigation Implemented] [Priority: Low]

Category: Tampering

Description: Data flowing across Lab Results may be tampered with by an attacker. This may lead to a denial of service attack against 1.0 Cardea Health Lab or an elevation of privilege attack against 1.0 Cardea Health Enterprise Agent or an information disclosure by 1.0 Cardea Health Enterprise Agent. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

Justification: This threat is considered low priority due the unlikeliness of it occuring. Blockchain networks are resistant to traditional DDoS (or consumption) attacks because their decentralized design removes any single point of failure. The only attack that would actually work in this case is a 51% attack toward the blockchain.

10. Potential Data Repudiation by 1.0 Cardea Health Enterprise Agent [State: Not Applicable] [Priority: Low]

Category: Repudiation

Description: 1.0 Cardea Health Enterprise Agent claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: The threat is invalid as all the information the Cardea Health Enterprise Agent utilizes is going through and coming from the blockchain.
There would be a trail of both read and write edits logged from blockchain usage

11. Data Flow Sniffing [State: Not Applicable] [Priority: Low]

Category: Information Disclosure

Description: Data flowing across Lab Results may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: This threat is invalid as information is wirtten directly to blockchain and requires authentication to read and write. All edits of read and write to the blockchain are logged

12. Potential Process Crash or Stop for 1.0 Cardea Health Enterprise Agent [State: Mitigation Implemented] [Priority: Low]

Category: Denial Of Service

Description: 1.0 Cardea Health Enterprise Agent crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Cardea Mobile Agent is open-sourced. So buggy behavior can be quickly fixed through contributions of the community.

13. Data Flow Lab Results Is Potentially Interrupted [State: Mitigation Implemented] [Priority: Low]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: This threat is considered low priority due the unlikeliness of it occuring. Blockchain networks are resistant to traditional data interruptions because their decentralized design removes any single point of failure.

14. 1.0 Cardea Health Enterprise Agent May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Applicable] [Priority: Low]

Category: Elevation Of Privilege

Description: Lab Technician may be able to remotely execute code for 1.0 Cardea Health Lab.

Justification: This threat is considered invalid as there is no option for code to be injected, there is no window for this to be done on the health providers end of the application when uploading health records.

15. Elevation by Changing the Execution Flow in 1.0 Cardea Health Enterprise Agent [State: Mitigation Implemented] [Priority: Low]

Category: Elevation Of Privilege

Description: An attacker may pass data into 1.0 Cardea Health Enterprise Agent in order to change the flow of program execution within 1.0 Cardea Health Enterprise Agent to the attacker's choosing.

Justification: Threat is valid due to the software being open source. However, a developer would validate code (through code review) to confirm authenticity of code and no changes/injections. Cardea developers do code review

16. Cross Site Request Forgery [State: Not Applicable] [Priority: Low]

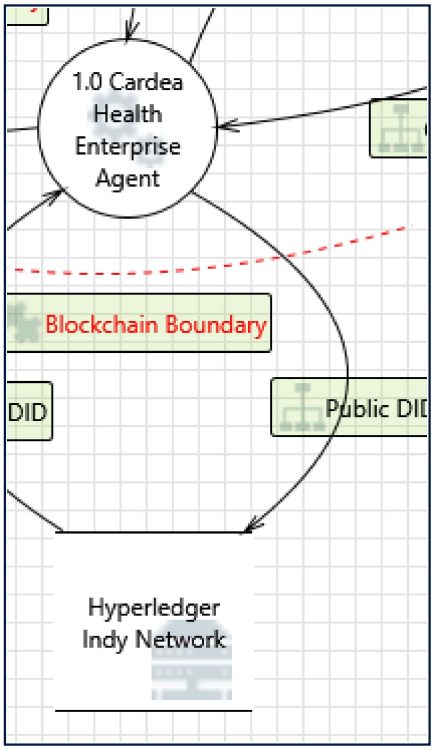
Category: Elevation Of Privilege

Description: Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting. The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the

browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.

Justification: This threat would be valid if Cardea utliized a browser for identification. However, Cardea runs solely on mobile devices where no requests or browser sessions are involved.

Interaction: Public DID



17. Spoofing of Destination Data Store Hyperledger Indy Network [State: Not Applicable] [Priority: Low]

Category: Spoofing

Description: Hyperledger Indy Network may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Hyperledger Indy Network. Consider using a standard authentication mechanism to identify the destination data store.

Justification: This threat is considered invalid due to it not being possible. One would need credentials to upload information which requires authentication.

18. Potential Excessive Resource Consumption for 1.0 Cardea Health Enterprise Agent or Hyperledger Indy Network [State: Mitigation Implemented] [Priority: Low]

Category: Denial Of Service

Description: Does 1.0 Cardea Health Enterprise Agent or Hyperledger Indy Network take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: This threat is considered low priority due the unlikeliness of it occuring. Blockchain networks are resistant to traditional DDoS (or consumption) attacks because their decentralized design removes any single point of failure.

19. Spoofing the 1.0 Cardea Health Enterprise Agent Process [State: Not Applicable] [Priority: Low]

Category: Spoofing

Description: 1.0 Cardea Health Enterprise Agent may be spoofed by an attacker and this may lead to unauthorized access to Hyperledger Indy Network. Consider using a standard authentication mechanism to identify the source process.

Justification: This threat is considered invalid due to it not being possible. One would need credentials to upload information which requires authentication already.

20. The Hyperledger Indy Network Data Store Could Be Corrupted [State: Mitigation Implemented] [Priority: Low]

Category: Tampering

Description: Data flowing across Public DID may be tampered with by an attacker. This may lead to corruption of Hyperledger Indy Network. Ensure the integrity of the data flow to the data store.

Justification: This threat is considered low priority due the unlikeliness of it occuring. Blockchain networks are resistant to tampering due to their decentralized design removing any single point of failure and logging all reads and writes. The only attack that would actually work in this case is a 51% attack toward the blockchain.

21. Data Store Denies Hyperledger Indy Network Potentially Writing Data [State: Not Applicable] [Priority: Low]

Category: Repudiation

Description: Hyperledger Indy Network claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: The threat is invalid as all the information the Cardea Health Lab utilizes is going through and coming from the blockchain.
There would be a trail of both read and write edits logged from blockchain usage

22. Data Flow Sniffing [State: Not Applicable] [Priority: Low]

Category: Information Disclosure

Description: Data flowing across Public DID may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: This threat is invalid as information is wirtten directly to blockchain and requires authentication to read and write. All edits of read and write to the blockchain are logged

23. Data Flow Public DID Is Potentially Interrupted [State: Mitigation Implemented] [Priority: Low]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: This threat is considered low priority due the unlikeliness of it occuring. Blockchain networks are resistant to traditional data interruptions because their decentralized design removes any single point of failure.

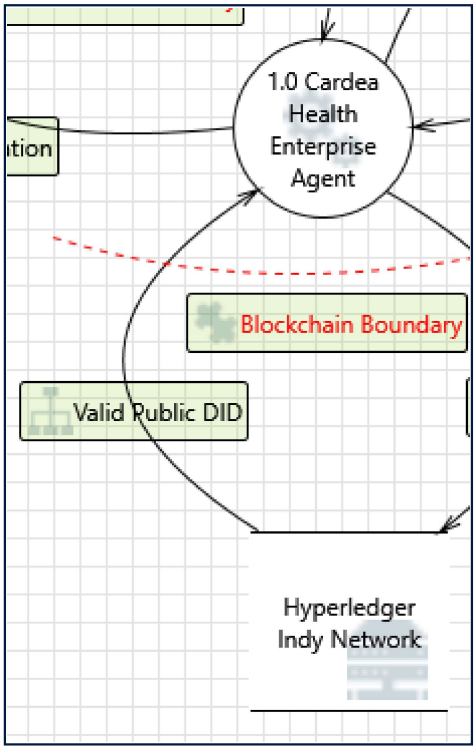
24. Data Store Inaccessible [State: Mitigation Implemented] [Priority: Low]

Category: Denial Of Service

Description: An external agent prevents access to a data store on the other side of the trust boundary.

Justification: This threat is considered low priority due the unlikeliness of it occuring. Blockchain networks are resistant to traditional data interruptions because their decentralized design removes any single point of failure.

Interaction: Valid Public DID



25. Spoofing of Source Data Store Hyperledger Indy Network [State: Mitigation Implemented] [Priority: Low]

Category: Spoofing

Description: Hyperledger Indy Network may be spoofed by an attacker and this may lead to incorrect data delivered to 1.0 Cardea Health Lab. Consider using a standard authentication mechanism to identify the source data store.

Justification: This threat is considered low priority due to the unlikeliness of it occurring. The only attack that would actually work in this case is a 51% attack toward the blockchain.

26. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: Low]

Category: Information Disclosure

Description: Improper data protection of Hyperledger Indy Network can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: This threat is considered low priority due to the unlikeliness of it occurring. The only attack that would actually work in this case is a 51% attack toward the blockchain.
All read and write toward the blockchain is logged.

27. Spoofing the 1.0 Cardea Health Enterprise Agent Process [State: Not Applicable] [Priority: Low]

Category: Spoofing

Description: 1.0 Cardea Health Enterprise Agent may be spoofed by an attacker and this may lead to information disclosure by Hyperledger Indy Network. Consider using a standard authentication mechanism to identify the destination process.

Justification: This threat is considered invalid due to it not being possible. One would need credentials to upload information which requires authentication already.

28. Potential Data Repudiation by 1.0 Cardea Health Enterprise Agent [State: Not Applicable] [Priority: Low]

Category: Repudiation

Description: 1.0 Cardea Health Enterprise Agent claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: The threat is invalid as all the information the Cardea Health Enterprise Agent utilizes is going through and coming from the blockchain.
There would be a trail of both read and write edits logged from blockchain usage.

29. Potential Process Crash or Stop for 1.0 Cardea Health Enterprise Agent [State: Mitigation Implemented] [Priority: Low]

Category: Denial Of Service

Description: 1.0 Cardea Health Enterprise Agent crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Cardea Mobile Agent is open-sourced. So buggy behavior can be quickly fixed through contributions of the community.

30. Data Flow Valid Public DID Is Potentially Interrupted [State: Mitigation Implemented] [Priority: Low]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: This threat is considered low priority due the unlikeliness of it occuring. Blockchain networks are resistant to traditional data interruptions because their decentralized design removes any single point of failure.

31. Data Store Inaccessible [State: Mitigation Implemented] [Priority: Low]

Category: Denial Of Service

Description: An external agent prevents access to a data store on the other side of the trust boundary.

Justification: This threat is considered low priority due the unlikeliness of it occuring. Blockchain networks are resistant to traditional data interruptions because their decentralized design removes any single point of failure.

32. 1.0 Cardea Health Enterprise Agent May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Applicable] [Priority: Low]

Category: Elevation Of Privilege

Description: Hyperledger Indy Network may be able to remotely execute code for 1.0 Cardea Health Enterprise Agent.

Justification: This threat is considered invalid as there is no option for code to be injected, there is no window for this to be done on the health providers end of the application when uploading health records.

33. Elevation by Changing the Execution Flow in 1.0 Cardea Health Enterprise Agent [State: Mitigation Implemented] [Priority: Low]

Category: Elevation Of Privilege

Description: An attacker may pass data into 1.0 Cardea Health Enterprise Agent in order to change the flow of program execution within 1.0 Cardea Health Enterprise Agent to the attacker's choosing.

Justification: Threat is valid due to the software being open source. However, a developer would validate code (through code review) to confirm authenticity of code and no changes/injections. Cardea developers do code review