HLD

Feature Name

Document ID: AAA-BBB-12345

Revision History:

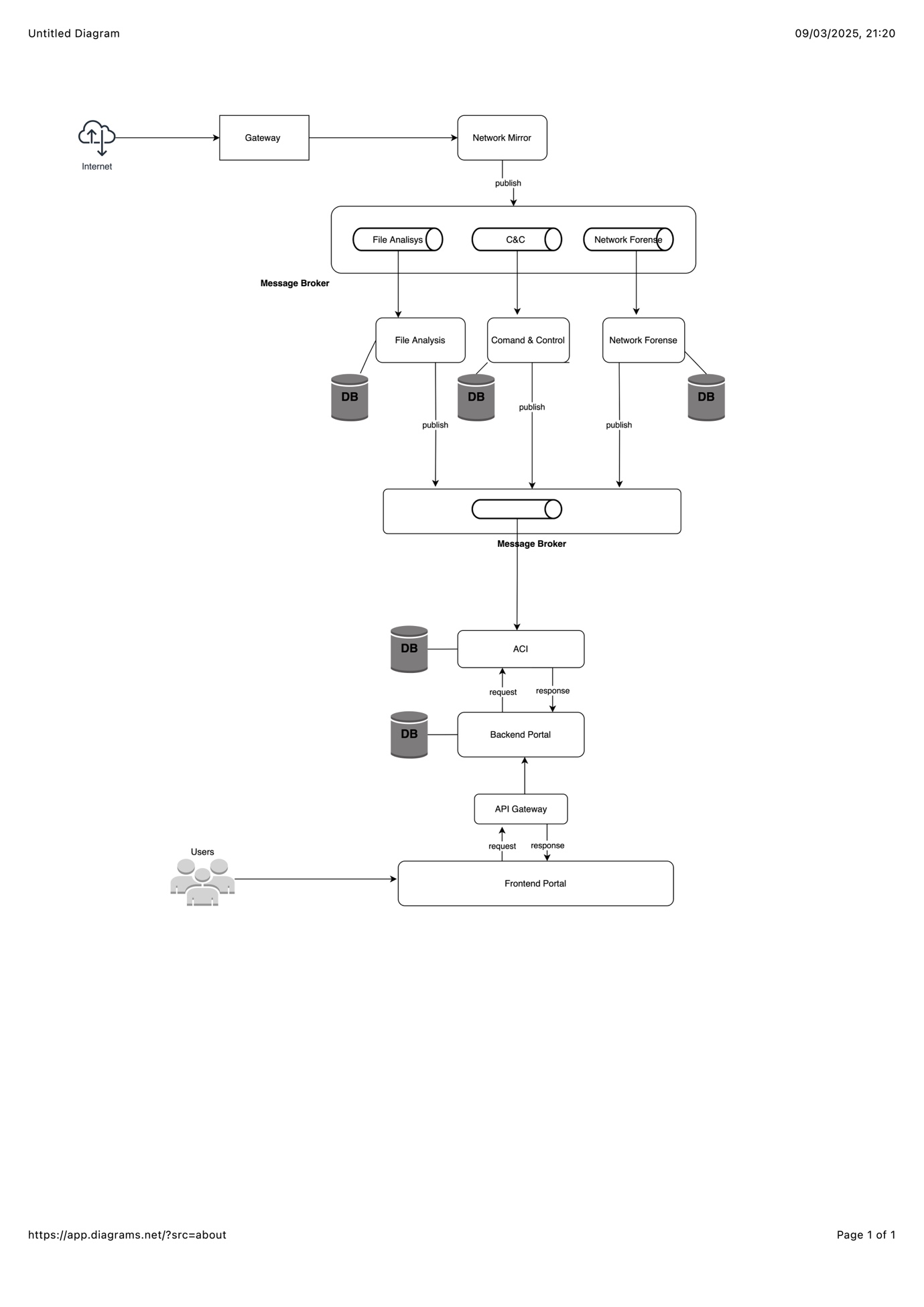
|  |  |  |  |
| --- | --- | --- | --- |
| Rev. | Date | Author | Details |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Abstract:

*{3-4 lines about what the feature is, which system/version it is for, which sub-systems it involves.}*

*CyberForNexus will collect information from the gateway of enterprise network to different sensors for investigation to protect against any cyber-attack. The sensors will provide information based on result of investigation to Central analysis Center and send alerts in casa of potential cyber-attack and allow the analysts carry out drill down to events and forensics.*

[Enter your writing here]



Contents

[1. General 3](#_Toc126490364)

[1.1 Introduction 3](#_Toc126490365)

[1.2 Glossary, references 3](#_Toc126490366)

[2. Requirements 3](#_Toc126490367)

[1.1 Logical (System Functionality) 4](#_Toc126490368)

[1.2 User Workflow 4](#_Toc126490369)

[1.3 Availability and Recovery 4](#_Toc126490370)

[1.4 Performance & Capacity Requirements 4](#_Toc126490371)

[1.5 Scalability 4](#_Toc126490372)

[1.6 Security 4](#_Toc126490373)

[1.7 Monitoring and Debugging 5](#_Toc126490374)

[1.8 Deployment 5](#_Toc126490375)

[1.9 Backward Compatibility 5](#_Toc126490376)

[3. High Level Design 5](#_Toc126490377)

[1.1 System Architecture 5](#_Toc126490378)

[1.2 Processes 5](#_Toc126490379)

[1.3 Design Rules and Principles 6](#_Toc126490380)

[1.4 Upgradability 6](#_Toc126490381)

[1.5 Assumptions and Dependencies 6](#_Toc126490382)

[4. Time Estimation 6](#_Toc126490383)

[5. Limitations and Reservations 6](#_Toc126490384)

[6. Risks 6](#_Toc126490385)

[7. Open Issues 7](#_Toc126490386)

1. General
   1. Introduction

*{In this section describe in high level the system's goals and objectives.}*

CyberForNexus is a system with intention to prevent cyber-attack and guarantee security of the enterprise network.

The following are some of the features CyberFoNexus provide:

* Capture all packet data from enterprise network.
* Examine all traffic to detect malware and vires in files, emails and C&C traffic.
* Save packet data captured during the examination.
* Index and save all connection (IP) metadata from the enterprise network.
* Ensure all captured data contain sufficient details to help for investigation.
* Provide automated and manual investigation.
* Send alerts in case of detection of malware, virus and suspicion of C&C traffic.
* Generate dashboard and report for investigations.
* Availability of user interface to allows users for management of open investigations.
* Availability of user interface to search the traffic and protocols (tcp/udp).
* Create user role, management permission and access levels for different users.

[Enter your writing here]

* 1. Glossary, references

*{It’s a good idea to create a glossary, dictionary with definitions of unusual phrases, product names etc. to create****ubiquitous language****. Moreover, it helps the reader to better understand not only documentation but also your business}*

[Enter your writing here]

1. Requirements

*{This chapter should NOT include any design constraints or ideas – only the requirements, as interpreted by dev teams. All design issues must be under “High Level Design”.*

*HLD Requirements are a transformation of Product requirements to technical domain.*

*Specific requirements should be crossed reference to other specifications (Product, Project etc.)*

*The breakdown below can be modified according to the specific subject of the HLD*

1. *Software requirements are the specific* ***needs, goals, and constraints*** *that a software product must meet to be successful.*
2. *These requirements typically describe* ***what the software should do****, how it should perform, and the conditions under which it should operate.*
3. *They also define the features and functionality that the software must provide, as well as any limitations or restrictions that must be considered.*
4. *Software requirements can come from various sources, such as customers, end users, stakeholders, and project team members.*
5. *The process of defining, documenting, and refining software requirements is a critical step in the software development lifecycle and is essential for creating a high-quality and successful software product.*
6. ***Functional requirements***
   1. *describe what a software system must do and define the specific features and capabilities that the system must provide.*
   2. *These requirements specify what the software should accomplish and how it should behave in response to specific inputs and actions.*
   3. *Examples of functional requirements include user authentication, data input and output, calculations, and reporting.*
7. ***Non-functional requirements***
   1. *describe* ***how well the software system must perform*** *and define the constraints and quality attributes that must be met.*
   2. *These requirements specify the* ***characteristics and qualities*** *that are expected of the system, such as reliability, scalability, security, and usability.*
   3. *Examples of non-functional requirements include response time, availability, and security standards.*
8. *Functional requirements are often described in terms of inputs, outputs, and specific user interactions with the software, while non-functional requirements are described in terms of performance and quality characteristics.*
9. *Both types of requirements are important for creating a software system that meets the needs and expectations of its users, and it's important to consider both functional and non-functional requirements when designing, building, and testing software.}*

*Mirro  
Ensure all information from enterprise network should be collected for further investigation.*

*Threat Detection Sensors  
All inbound, outbound, duplex traffic will be processed.*

*File Analysis  
Scan for malware and virus in inbound files and emails and send alert when something is detected.  
  
Command & Control  
Check malware outgoing C&C traffic on the metadata of raw packets and send notification when suspected C&C traffic is found.*

*Network Forensic  
Index and record all connection (IP) metadata from the enterprise network to search the traffic and protocols (tcp/udp). The information will be kept by 3 months.*

*Automatic Cyber Investigation*

*Collect all the data from Detection sensors and Network Forensic and performs automatic queries in order to send notification on cyber incident. Provide further details which can be helpful to allow manual investigation. Generate Automated cyber investigation to detect campaign.*

*Investigation Portal*

*The user interface that loads all relevant information from Automatic Cyber Information component to carry out cyber defense operation by the following actions:*

* *show notifications when malware/virus found from File analysis.*
* *show notifications when suspected C&C traffic is found from Command & Control sensor.*
* *Manage manual investigation which include a timeline of alerts and network recording.*
* *Manage automated investigated provided from Automatic Cyber Information component.*
* *Generate dashboard and reports of alerts and open investigation.*

*User management access should be defined to make sure users will be access only their own investigation*

[Enter your writing here]

* 1. Logical (System Functionality)

*{Several items (number each paragraph!) which describe the feature highlights from a user standpoint - should be very similar the feature description in the product requirements specification*

*If relevant and does not exists in Product Spec – include use cases, state machines }*

*All requirements should be uniquely identifiable (different section number)*

*Careful attention should be given to organizing the requirements to maximize readability (short sentences, sub-paragraphs, etc.)*

*System functionality will break into epics and user story. The dev teams eventually break the user story into tasks}*

[Enter your writing here]

* 1. User Workflow

*{If relevant and possible include sample of screen shots}*

[Enter your writing here]

* 1. Availability and Recovery

*{Defines the proportion of time that the system is functional and working. It can be measured as a percentage. It should also state the recovery measures for any relevant failure}*

[Enter your writing here]

* 1. Performance & Capacity Requirements

*{Performance & capacity requirements should be expressed in measurements, not terms like “very fast”. It should include responsiveness of a system to execute any action within a given time interval}*

[Enter your writing here]

* 1. Scalability

*{System ability to grow, by adding threads or HW. Address issues such as persistency and load balancing}*

[Enter your writing here]

* 1. Security

*{Address security in all relevant levels – OS, HW, Application level, interfaces (manly external), db}*

[Enter your writing here]

* 1. Monitoring and Debugging

*{define the monitoring capabilities of the feature. New Metrics, monitoring dashboards, log collection, and the ability of the system to provide any other information helpful for identifying and resolving issues when it fails to work correctly}*

[Enter your writing here]

* 1. Deployment

*{Describe the deployment environment - how this feature will be deployed, in the cloud native domain, how to deploy the container, what is the replica set, can this feature be deployed on any platforms}*

[Enter your writing here]

* 1. Backward Compatibility

*{Describe the required backward compatibility versions that should be supported}*

[Enter your writing here]

1. High Level Design
   1. System Architecture

*{This section should be filled for features which influence the system architecture: e.g. a new server / platform support, multi-site oriented features, etc.) Use the following views to describe your architecture:*

1. *Process – run time behavior – how components communicate, concurrency, distribution, performance and scalability – use sequence diagrams, state machine diagrams, communication and activity diagrams*
2. *Development – implementation view – component diagram*
3. *Physical – deployment view – topology of software components, the physical layer, networking}*

[Enter your writing here]

* 1. Processes

*{Define what the feature should do by identifying inputs, processes and outputs. Specify methods to be used. Interactions to other components & features should be specified or referred to.*

*This section will also identify the interfaces which will be elaborated in the detail design done by dev teams.*

*When writing this part, the following principles apply:*

*Break down the feature to user (or system) processes. Describe, for each process, the information flow between the user, and the subsystems involved. For each process, cover every aspect of the feature.*

[Enter your writing here]

* 1. Design Rules and Principles

*{Rules for constructing the architecture. Anything that the developers who will work on this feature need to keep in mind when they do low-level design that is not covered in the requirements or interfaces, in example – presentation layer should not direct access to persistency layer, all communication between components should be done over HTTPS. All data at reset should be encrypted.*

*This section can include guidance for the dev team – example – wherever possible, use asynch flows to improve parallelism}*

[Enter your writing here]

* 1. Upgradability

*{Describe how to upgrade older version of the system to support the deployment of this feature. What components needs to be upgrade, what kind of dependencies exits. Do we need to under go DB migration, or schema changes}*

[Enter your writing here]

* 1. Assumptions and Dependencies

[Enter your writing here]

1. Time Estimation

*{Insert the work plan time estimation for development after HLD writing }*

|  |  |
| --- | --- |
| Subsystem/team | Workdays |
|  |  |

*{Insert the work plan time estimation for development after this FRS review }*

1. Limitations and Reservations

*{This is a very important section. This is the place to put anything that the feature WON’T do that someone might easily think it SHOULD do. If this section is complete, there should be no surprises for the project manager or the client when they get the final product}*

[Enter your writing here]

1. Risks

*{For each risk, specify the resolution method (i.e., how to minimize the risk, and are there ways to minimize the “damage” of the risk if it materializes)}*

[Enter your writing here]

1. Open Issues

*{This section should list every item that is not 100% closed in the document. Looking at this section should be enough to know what still needs to be decided or investigated. In the final FRS, this section should not exist. Any time you write in the sections above “DBS will check that...” or “AMS will perform a benchmark that” or “the text of the message will be decided”, or “???”, or TBD - you MUST add a paragraph to this section!*

*The final revision of the document should NOT include this section!}*

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Description | Subsystem | Responsible |
|  |  |  |  |
|  |  |  |  |