Functional Requirements

IEEE: 3.2 | ISO: Functionality

- The system should detect and prevent cyber threats such as ransomware, phishing, DDoS, and APTs.
- The system should provide real-time protection and regular updates against evolving threats.
- The system should filter incoming and outgoing traffic based on predefined rules.
- The system should monitor network traffic for suspicious activities and unauthorized access.
- The system should encrypt sensitive information and ensure data privacy.
- The system should identify weaknesses in systems, networks, and applications.
- The system should simulate real-world cyberattacks to identify weaknesses in security measures.
- The system should manage user identities and permissions effectively.
- The system should provide comprehensive monitoring and response capabilities by collecting and analyzing logs from various systems.

Non-Functional Requirements

IEEE: 3.3 | ISO: Usability

- The system should be intuitive and easy to deploy, minimizing the learning curve for security teams.
- The system should be cost-effective, making cost-benefit analysis crucial.
- The system should accommodate organizational growth and changing IT infrastructure.
- The system should integrate seamlessly with existing systems and workflows.
- The system should have automated features to enhance efficiency in threat detection and response.
- The system should comply with industry regulations, such as GDPR, HIPAA, or PCI DSS, depending on the organization’s domain.

Business Rules

IEEE: N/A | ISO: N/A

- The selection of security tools depends on various factors to ensure they meet organizational needs.
- The system should ensure that only authenticated users can access sensitive resources, reducing the risk of insider threats and unauthorized access.

Constraints

IEEE: 3.4 | ISO: Portability

- Budget constraints often dictate the choice of tools, making cost-benefit analysis crucial.
- The system should accommodate organizational growth and changing IT infrastructure.

Assumptions

IEEE: 3.5 | ISO: Maintainability

- The system assumes that no user or device is inherently trustworthy, enforcing strict verification and access controls.