Functional Requirements

IEEE: 3.2 | ISO: Functionality

- Antivirus and Antimalware Tools should scan files and monitor activities to detect and neutralize threats like viruses, trojans, and ransomware
- Firewalls should enforce security policies by filtering incoming and outgoing traffic
- Intrusion Detection and Prevention Systems (IDPS) should monitor network traffic for suspicious activities and unauthorized access
- Encryption Tools should ensure data privacy by converting sensitive information into unreadable formats
- Vulnerability Scanners should identify weaknesses in systems, networks, and applications
- Penetration Testing Tools should simulate real-world cyberattacks to identify weaknesses in security measures
- Identity and Access Management (IAM) Tools should manage user identities and permissions effectively
- Security Information and Event Management (SIEM) Tools should provide comprehensive monitoring and response capabilities

Non-Functional Requirements

IEEE: 3.3 | ISO: Usability

- Usability: Tools should be intuitive and easy to deploy, minimizing the learning curve for security teams
- Cost-effectiveness: Budget constraints often dictate the choice of tools, making cost-benefit analysis crucial
- Scalability: Security tools must accommodate organizational growth and changing IT infrastructure
- Compatibility: Tools should integrate seamlessly with existing systems and workflows
- Automation and AI Integration: Automated features enhance efficiency in threat detection and response
- Compliance: Tools must 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

- None

Constraints

IEEE: 3.4 | ISO: Portability

- False Positives and Negatives: Excessive alerts can lead to alert fatigue, while undetected threats can cause significant damage
- High Costs: The acquisition, deployment, and maintenance of advanced tools can strain budgets, particularly for small and medium-sized enterprises (SMEs)
- Integration Complexity: Incorporating new tools into legacy systems can be time-consuming and requires specialized expertise
- User Resistance: Employees may resist adopting new tools or fail to follow security protocols, undermining the tools' effectiveness

Assumptions

IEEE: 3.5 | ISO: Maintainability

- None