3.3 Solution Requirement

Solution Requirements for Cybersecurity System

1. Functional Requirements:

These are the core features and functions the cybersecurity system must provide to ensure it can detect, prevent, and respond to security threats.

1.1 Threat Detection and Prevention:

Real-Time Threat Detection: The system should be capable of detecting cyber threats (e.g., malware, ransomware, phishing, data breaches) in real-time.

Vulnerability Scanning: The solution must include the ability to regularly scan systems, applications, and networks for vulnerabilities.

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS): The system must monitor network traffic and automatically block malicious activities.

1.2 Risk Assessment and Management:

Vulnerability Assessment: The solution should identify potential security risks and provide recommendations for mitigation.

Risk Rating: The ability to assign risk scores based on severity and likelihood to help prioritize mitigation efforts.

Compliance Management: The solution must help the organization adhere to relevant industry standards and regulations (e.g., GDPR, HIPAA, PCI-DSS).

1.3 Incident Response:

Automated Response to Threats: The system should be capable of automatically responding to certain predefined security incidents (e.g., quarantine suspicious files, block IP addresses).

Alerting and Reporting: The solution must provide real-time alerts and detailed reporting for security incidents to allow rapid investigation and resolution.

1.4 Access Control and Authentication:

Multi-Factor Authentication (MFA): The solution must support MFA for accessing critical systems, applications, and data.

Role-Based Access Control (RBAC): Users should only have access to the systems and data they need to perform their job functions.

Identity and Access Management (IAM): The solution should include the ability to manage and monitor user identities and their access rights.

1.5 Data Encryption and Integrity:

Data Encryption: The solution must support the encryption of data at rest and in transit to protect sensitive information from unauthorized access.

Data Integrity Checks: The system should regularly verify the integrity of data to ensure it hasn’t been altered or tampered with.

1.6 Network Security:

Firewall Integration: The solution must integrate with existing network firewalls to filter malicious traffic and enforce security policies.

Virtual Private Network (VPN) Support: The system must ensure secure remote access for employees via VPN connections.

Segmentation: The ability to segment networks to minimize the spread of attacks.

1.7 Security Monitoring and Auditing:

Centralized Security Monitoring: The solution must provide centralized monitoring of the security environment across all devices, networks, and applications.

Audit Trails and Logs: The system should create comprehensive logs of security-related events, which can be reviewed for auditing purposes.

2. Non-Functional Requirements:

These requirements relate to the system’s performance, usability, and other qualities that affect how the solution works in practice.

2.1 Performance and Scalability:

Scalability: The solution must scale to accommodate growing numbers of users, devices, and data without a significant performance loss.

Low Latency: The solution should have minimal impact on system performance, ensuring it does not slow down critical business operations during threat detection or incident response.

High Availability: The cybersecurity solution should be available 24/7 and have a high uptime rate, with failover capabilities in case of system failures.

2.2 Usability:

User-Friendly Interface: The solution should offer an intuitive, easy-to-use interface for both administrators and end-users to interact with the system effectively.

Training and Documentation: Clear documentation and training materials should be provided for IT staff to learn how to configure, use, and maintain the solution.

2.3 Security and Compliance:

Data Protection Standards: The solution must meet industry-standard data protection frameworks, ensuring that sensitive data is kept safe.

Regulatory Compliance: The solution should facilitate compliance with local and international regulations (e.g., GDPR, HIPAA, SOC 2) by implementing necessary security controls and audits.

Penetration Testing: The system should undergo regular penetration testing to ensure its security mechanisms are effective.

2.4 Integration:

Integration with Existing Systems: The cybersecurity solution should be able to integrate seamlessly with existing enterprise software (e.g., IT systems, databases, cloud environments).

API Availability: The solution should offer APIs for integration with third-party applications or other cybersecurity tools like SIEM (Security Information and Event Management) systems.

2.5 Availability and Reliability:

Disaster Recovery and Backup: The solution must provide a disaster recovery plan and automated backups for critical systems and data.

Redundancy: It should include failover mechanisms and redundancy to ensure minimal disruption in case of component failure.

2.6 Cost-Effectiveness:

Cost of Implementation: The solution should be cost-effective, considering the organization's budget for cybersecurity tools and solutions.

Ongoing Maintenance and Support: It should offer affordable and efficient support and maintenance plans.

Total Cost of Ownership (TCO): The solution should provide a balance of features, cost, and scalability over the long term.

2.7 Vendor Support and Maintenance:

Technical Support: The solution must provide comprehensive technical support, including helpdesk access and troubleshooting.

Software Updates: The vendor should regularly release patches and updates to address emerging threats and improve the solution.

Security Patches: Timely delivery of security patches is essential to protect against newly discovered vulnerabilities.

3. Stakeholder Requirements:

These are the expectations and needs of different stakeholders involved in the cybersecurity project (e.g., security officers, IT teams, business leaders).

3.1 IT Department Requirements:

Ease of Deployment and Management: The IT team needs the system to be easy to deploy, configure, and maintain.

Integration with Existing IT Infrastructure: The solution should integrate with existing enterprise tools such as firewalls, endpoint security, and SIEM systems.

3.2 Business and Executive Requirements:

Cost-Effectiveness: Business leaders expect a return on investment (ROI) in terms of reduced risk and cost-saving due to effective threat prevention.

Risk Mitigation: Executives want assurance that the cybersecurity solution reduces the business's exposure to cybersecurity threats.

3.3 End-User Requirements:

Minimal Disruption: End users should experience minimal disruption or slowdowns in their work due to cybersecurity systems.

User Training: End-users need to be trained on how to work securely within the system (e.g., safe handling of passwords, multi-factor authentication).

Summary of Solution Requirements for Cybersecurity System:

Functional Requirements:

Threat detection, vulnerability scanning, IDS/IPS, automated incident response, access control, data encryption, and security monitoring.

Non-Functional Requirements:

Scalability, low latency, usability, high availability, cost-effectiveness, compliance with regulations, and reliability.

Stakeholder Requirements:

IT teams require easy integration and management.

Business leaders require cost-effective risk mitigation.

End users need minimal disruption and adequate training.

By addressing these requirements, the cybersecurity solution will be able to meet both the technical and business needs of the organization while ensuring that the security posture remains strong and resilient.