1 Security Measure Summary Checklists

Table 1: Holistic Security Measure Checklist

Holistic Security Measure Checklist
Timely updates to latest versions and patches
Consistent Backups
Logging and Monitoring

Table 2: Users Asset Security Measure Checklist

Users asset Security Measure Checklist	
Insider threat	Non Disclosure Agreement Signing
	Strict Asset Access Control/Monitoring (UEBA,logging)
	Least Priviledge policies
	Segregation of duties
Lack of security awareness	Security Awareness Training, Briefing
	Social Engineering Attack Simulations
	AI On Social Engineering (Phishing, Malicious URL)
Management Strategy	Vulnerability Disclosure Programs
	Company-Wide Risk Asessments
	Security Incident Scenario Strategies In Place

Table 3: Devices Asset Security Measure Checklist

Devices asset Security Measure Checklist	
Physical Security	Inaccessibility To Devices, No Exposed Ports
	Biometrics Access Control
	Board Encapsulation/Coating
Hardware Security	Security Fuse Usage
	Tampering Detectors, Randomness Against Side Channel Attacks
	Jamming and DoS Avoidance through Secure Routing, Frequency Hopping, Spectrum Spreading
	TEE - Trusted Execution Environment
	Secure Booting, HRoT (Hardware Root of Trust)
	OTA Authenticated/Encrypted Firmware Updates
Software Security	Application Whitelisting
	Static Analysis Malware Detection (AI Classifiers)

Table 4: Communication Channels Asset Security Measure Checklist

Communication Channels asset Security Measure Checklist	
TLS Cryptography Usecase	Independent TCP over TLS, or Offloading to TLS gateway
TLS Characteristics	TLSv1.3 for Forward Secrecy, Efficient Cryptography, Else v.1.2
	Assymetric: Elliptic-Curve Diffie Hellman Ephemeral (ECDHE)
	Symmetric: AES-GCM, ChaCha20-Poly1305
	Hashing: Blake2, Photon, Quark
Authentication	2-Way TLS Authentication with X.509 Certificates
	AI-based Authentication (Proximity/Fingerprint Based)

Table 5: Message Brokers Asset Security Measure Checklist

Message Brokers asset Security Measure Checklist	
Authentication	Client TLS Certificates
	Authentication Tokens
Authorization	Access Control Lists (ACL)
	Role-Based Access (RBAC)
	Usage Control (UCON)
	Capability Based Access Control (CapBAC)

Table 6: Web Application Asset Security Measure Checklist

Web Application asset Security Measure Checklist	
Injection Attacks (SQL, OS etc.) (Applicable to XSS as well)	Input Validation
	Input Sanitization/Escape
	Trusted Modern Frameworks/Libraries (ORMs , Front-End frameworks that sanitize automatically)
Access Control	Access to authorized content only
Information-Disclosure	Non-Information Exposing Error Messages
	Non-Exposure of Sensitive Assets
Vulnerability Assessment	Web-Application Testing Tools
Intrusion Detection/Prevention	Hybrid Web Application Firewalls (WAFs)

Table 7: Databases Asset Security Measure Checklist

Databases asset Security Measure Checklist	
SQL Injection Protection	Stored Procedures
	Parameterized Queries
	Non-Root Database User for Queries
Database System Protection	Non-Exposure to the Internet
Data Protection	Hashed Sensitive Data Fields
	Encrypted Database (Optional - Tradeoff)
Key Management	No Key Storage where Data are stored
	Access Control where Keys are stored
	Hardware Security Modules (Optional - Tradeoff)

Table 8: Processing Services Asset Security Measure Checklist

Processing Services asset Security Measure Checklist	
Untrusted Code Execution	Inside Containers spawned in VM for Virtual Kernel
	Non-Root, Least Priviledge Container User
	Minimal Container Images
	Installed only needed Libraries/Binaries/Tools
	Restricted Programming Language Support
	Strict Resource Quotas

Table 9: Backend Server Asset Security Measure Checklist

Backend Server asset Security Measure Checklist	
API security	Encryption on API requests (HTTPS)
	Authentication with API tokens
	Authorization
	Rate Limiting in API requests
	API request Validation and Sanitization
	Intrusion Detection on API requests (Heuristic and AI based)

Table 10: Deployment Infrastructure Asset Security Measure Checklist

Deployment Infrastructure asset Security Measure Checklist	
Physical Security	Strict Access control to machines (Biometrics)
	Camera Surveillance
	Resilience to Natural Disasters
Machine Management	Secure/Authenticated Management Platforms
	Network and Device Monitoring
	Enforced Virtual Machine Quotas
	VM Isolation
Intrusion Detection	IDS, NIDS and IPS Usage (AI and Signature Based)