

Below is a detailed runbook covering all the mentioned topics, including cybersecurity best practices for web, app, debit/credit cards, online payments, scans, WiFi payments, ATM transactions, and relevant transactions between the bank and customers:

### **1. Azure WAF, SIEM, and SOAR Tool**

Azure Web Application Firewall (WAF):

Implement Azure WAF to protect web applications from OWASP Top Ten vulnerabilities.

Regularly update and customize WAF rules to adapt to emerging threats.

Configure rate limiting to prevent DDoS attacks.

SIEM (Security Information and Event Management):

Deploy a SIEM solution for centralized security event monitoring.

Configure alerts for suspicious activities and automate response actions.

Regularly review SIEM logs for anomalies.

SOAR (Security Orchestration, Automation, and Response):

Integrate SOAR tools to automate incident response workflows.

Create playbooks for common cybersecurity incidents like phishing and malware outbreaks.

Continuously improve SOAR processes based on incident learnings.

### **2. XDR and EDR Monitoring**

Extended Detection and Response (XDR):

Implement XDR solutions for cross-vector threat detection and response.

Continuously monitor endpoints, networks, and cloud environments for threats.

Develop incident response playbooks for XDR alerts.

Endpoint Detection and Response (EDR):

Deploy EDR agents on all endpoints, including ATMs and point-of-sale devices.

Conduct investigations and respond to endpoint security incidents promptly.

### **3. M365 Security**

Microsoft 365 Security:

Enable Multi-Factor Authentication (MFA) for all user accounts.

Regularly review and configure security settings in Microsoft 365, including email filtering and anti-phishing measures.

Educate users about email security and safe document handling practices.

### **4. Data Protection Implementation**

Data Classification:

Implement data classification policies to identify sensitive data.

Encrypt sensitive data at rest and in transit using industry-standard encryption algorithms.

Access Control:

Enforce strict access controls based on the principle of least privilege.

Regularly review and update access permissions, especially for databases containing customer financial data.

## **5. Sensitivity Label Implementation**

Sensitivity Labels:

Define sensitivity labels for data classification and apply them consistently to documents and emails.

Implement automated label-based data protection policies.

## **6. End User Guide for Phishing Email and Awareness**

Phishing Awareness:

Conduct regular phishing awareness training for all bank employees and customers.

Provide guidelines for recognizing and reporting phishing emails.

Simulate phishing attacks periodically to assess user readiness.

## **7. SOC Monitoring and Mitre Framework Implementation**

SOC Monitoring:

Establish a Security Operations Center (SOC) for continuous monitoring.

Implement the Mitre ATT&CK framework for advanced threat detection and response.

Develop incident response runbooks aligned with Mitre techniques.

## **8. SOC2 or Essential 8 Implementation**

Compliance Framework:

Assess the need for SOC2 or Essential Eight compliance based on regulatory requirements.

Develop and maintain documentation to meet compliance requirements.

## **9. Identity Protection**

Identity and Access Management (IAM):

Implement robust IAM controls with role-based access.

Enable User and Entity Behavior Analytics (UEBA) to detect unusual activities.

Monitor privileged accounts closely.

## **10. Threat Scan with Footprints**

Threat Intelligence:

Subscribe to threat intelligence feeds and stay informed about emerging threats.

Conduct regular threat scans with footprint analysis to identify potential threats targeting the bank.

### **11. Vulnerability Scan Real-time with Device Protection**

Vulnerability Management:

Perform real-time vulnerability scans on systems and devices, including ATMs.

Prioritize and remediate vulnerabilities promptly, considering the criticality of assets.

### **12. BYOD and MDM Protection**

BYOD Policies:

Establish BYOD policies and guidelines for bank employees.

Implement Mobile Device Management (MDM) solutions to control and secure mobile devices used within the bank's network.

### **Cybersecurity and Financial Vulnerabilities**

**User Education:**

Promote strong password practices and enforce Two-Factor Authentication (2FA) for all employee and customer accounts.

Educate customers about safe online behavior, including avoiding suspicious links and emails.

Encourage the use of Virtual Private Networks (VPNs) for secure connections, especially when accessing accounts remotely.

Monitor customer accounts for unusual activity and implement anomaly detection systems.

Educate customers about their rights and protections under relevant financial regulations.

Cybersecurity Management Plan

**Risk Assessment:**

Conduct regular risk assessments to identify and prioritize threats and vulnerabilities.

Develop and maintain risk mitigation strategies based on assessment results.

**Policies and Procedures:**

Develop and maintain comprehensive cybersecurity policies and procedures, covering everything from incident response to acceptable use of technology resources.

Ensure alignment with industry standards and best practices.

**Incident Response Plan:**

Establish a well-documented incident response plan that includes roles, responsibilities, and communication protocols.

Test the incident response plan through tabletop exercises and real-world simulations.

Continuously update the plan based on lessons learned.

#### Regular Testing and Updates:

Continuously test and update the risk management program to adapt to evolving threats and technologies.

Conduct penetration tests and security audits regularly to identify weaknesses in the system.

#### **Networking Security and Network Infrastructure Monitoring**

##### **Network Security:**

Implement network segmentation to isolate critical systems and sensitive data.

Regularly review and update firewall rules to block unnecessary traffic.

Use intrusion detection and prevention systems (IDPS) to detect and block malicious network activity.

Enforce network access control (NAC) to ensure only authorized devices can access the network.

##### **Network Infrastructure Monitoring:**

Continuously monitor network traffic patterns for anomalies and potential security breaches.

Maintain an up-to-date inventory of network assets and devices.

Centralize and analyze logs from network devices, servers, and applications.

Implement a patch management process to keep network devices up to date.

Develop specific incident response procedures for network-related incidents.

##### **Business Continuity and Disaster Recovery (BCDR):**

Develop and test a comprehensive BCDR plan to ensure the bank's operations can continue in the event of a cyber incident or natural disaster.

Regularly update and test the plan to maintain its effectiveness.

##### **Vendor Risk Management:**

Assess the cybersecurity posture of third-party vendors and partners.

Ensure vendors meet the bank's security standards and requirements.

##### **Information Sharing and Collaboration:**

Collaborate with industry peers, government agencies, and cybersecurity organizations to share threat intelligence and best practices.

Participate in information-sharing programs to stay informed about emerging threats.

##### **Cybersecurity Metrics and Key Performance Indicators (KPIs):**

Define and track cybersecurity metrics and KPIs to measure the effectiveness of security measures.

Use these metrics to drive continuous improvement in cybersecurity.

##### **Incident Post-Mortems:**

Conduct post-incident reviews to analyze and learn from security incidents.

Use the findings to enhance security controls and incident response procedures.

Red Teaming and Penetration Testing:

Regularly engage in red teaming exercises and penetration testing to assess the bank's security posture.

Address vulnerabilities identified during these exercises promptly.

By following this comprehensive runbook, a banking system can.