DataWorks Global Inc.

Compliance: Security Optimization Initiative

IT Security Department

Contents

Introduction

This compliance document serves as a summary of the DataWorks Security Initiative Project to ensure adherence to best practices and requirements for secure cloud infrastructure implementation. It outlines the compliance measures taken during each sprint and how they align with organizational and industry standards.

Compliance Goals

Identity & Access Management (IAM): Ensure proper authentication and authorization controls are implemented. Align IAM configurations with Zero Trust principles.

Data Protection: Protect sensitive data using encryption and access controls. Maintain compliance with relevant regulations (e.g., GDPR, HIPAA).

Network Security: Secure virtual network communications using modern practices (e.g., Network Security Groups, VPN gateways). Isolate critical resources from public exposure.

Operations Monitoring: Enable centralized monitoring to detect and respond to threats effectively. Automate incident responses to reduce response times.

Project Governance: Ensure transparency and proper documentation of all security operations. Align implementation with organizational objectives and compliance requirements.

Compliance Summary by Sprint

Sprint 1: Planning and Kickoff

Deliverables: Project Charter, Scope Statement, Risk Management Plan, Communication Plan.

Compliance Alignment: Defined governance structures and responsibilities for the project.

Sprint 2: Identity and Access Management

Deliverables: Configured Microsoft Entra ID for Multi-Factor Authentication (MFA). Implemented Role-Based Access Control (RBAC) for resource groups. Enabled Privileged Identity Management (PIM).

Compliance Alignment: Ensured secure user authentication and access control in line with Zero Trust principles.

Sprint 3: Network Security

Deliverables: Configured Network Security Groups (NSGs) and Application Security Groups (ASGs). Set up Virtual Network Peering and VPN Gateway. Enabled encryption for ExpressRoute connections.

Compliance Alignment: Secured network traffic and enforced encrypted connections for all critical communications.

Sprint 4: Compute, Storage, and Database Security

Deliverables: Encrypted Azure Virtual Machines and enabled Just-in-Time (JIT) access. Configured access controls for Azure Storage accounts (Blob, Files, Queues). Enabled Transparent Data Encryption (TDE) for Azure SQL databases.

Compliance Alignment: Protected sensitive data in transit and at rest using encryption.

Sprint 5: Operations Monitoring

Deliverables: Configured Microsoft Defender for Cloud (Secure Score and workload protection). Integrated Microsoft Sentinel with data connectors and analytics rules. Tested automated threat response workflows.

Compliance Alignment: Centralized monitoring and incident response ensured continuous protection.

Sprint 6: Final Security Testing

Deliverables: Performed integration testing for all security configurations. Conducted User Acceptance Testing (UAT) with feedback gathered. Resolved issues identified during testing and finalized adjustments.

Compliance Alignment: Validated security configurations to ensure full adherence to security and organizational requirements.

Monitoring and Reporting

Metrics Monitored

- Percentage of assets with complete data alignment between Tenable and ServiceNow.
- Week-over-week improvement in data completeness.
- Total count of detected incidents and automated responses.

Dashboard Features

- Real-time tracking of compliance status.
- Exportable reports highlighting gaps and action items.

Compliance Enhancements

Continuous Monitoring: Microsoft Sentinel provides real-time alerting and automated response capabilities.

Encryption Everywhere: Full implementation of encryption for data in transit and at rest across all Azure resources.

Access Governance: PIM and RBAC ensure only authorized users have access to critical resources.

Recommendation for Continuous Improvement

Incident Response Training: Ensure all stakeholders understand how to respond to Sentinel alerts.

Regular Audits: Schedule periodic reviews of compliance metrics and security configurations.

Documentation Updates: Maintain updated records of all security changes and configurations for audit purposes.

Project Closure

The project has met its compliance objectives, and all configurations have been implemented and validated. Final documentation has been uploaded to the project's GitHub repository for future reference.