DataWorks Security Optimization Initiative Sprint Planning

11/15/2024

Sprint	Sprint 1	Sprint 2	Sprint 3	Sprint 4	Sprint 5	Sprint 6	Sprint 7
Dates	11/13/2024-11/19/2024	11/20/2024-11/26/2024	11/27/2024-12/03/2024	12/04/2024-12/10/2024	12/11/2024-12/17/2024	12/18/2024-12/24/2024	12/25/2024-12/31/2024
Goal	Finalize planning, documentation, and kickoff.	Complete initial configurations for identity and access management.	Implement network security configurations.	Complete compute, storage, and database security configurations.	Configure security operations and monitoring.	Conduct integration testing and User Acceptance Testing (UAT).	Finalize project documentation and close out the project.
Task 1	Conduct kickoff meeting and finalize project charter.	Configure Microsoft Entra ID for multi-factor authentication (MFA) and Conditional Access policies.	Configure Network Security Groups (NSGs) and Application Security Groups (ASGs).	Encrypt Azure virtual machines and enable just-in-time (JIT) access.	Set up Microsoft Defender for Cloud (Secure Score, workload protection).	Perform integration testing of all security configurations.	Complete compliance documentation and review.
Task 2	Complete scope statement and gain stakeholder approval.	Set up role-based access control (RBAC) for resource groups.	Set up Virtual Network peering and VPN gateway.	Configure access controls for storage accounts (Azure Blob Storage, Files, and Queues).	Configure Microsoft Sentinel with data connectors and analytics rules.	Conduct UAT with end-user representatives and gather feedback.	Finalize project handover materials and conduct lessons learned session.
Task 3	Document risk management plan and initial risk register.	Implement Privileged Identity Management (PIM).	Enable encryption for ExpressRoute connections.	Enable Transparent Data Encryption (TDE) for Azure SQL Database.	Test and validate automated threat response workflows.	Address issues identified during testing and make adjustments.	Archive project files and obtain final stakeholder sign-off.
Task 4	Create detailed project schedule and communication plan.						
Deliverable 1	Approved project charter and scope statement.	Configured MFA, Conditional Access, and RBAC.	Functional NSGs, ASGs, and VPN gateway.	Encrypted VMs and storage accounts.	Configured Microsoft Defender for Cloud and Sentinel.	Integration testing results.	Approved compliance documentation.
Deliverable 2	Completed risk management plan and communication plan.	Validated and tested Privileged Identity Management.	Validated encryption configurations for network traffic.	Secure database configurations with TDE enabled.	Validated threat response workflows.	Documented UAT feedback and resolutions.	Completed lessons learned and project closeout report.