Contents

Introduction

Multi-cloud environment offer businesses flexibility and scalability, but they also introduce complexity and security challenges. Managing multiple cloud providers with different security controls, data visibility across platforms, and consistent user access become major hurdles.

CNAPP

CNAPP (Cloud- Native Application Protection is a word coined by Gartner, to provide visibility around the cloud instances for security. The products consists of several key modules that work together to secure cloud-native applications:

1. Workload Security: This module safeguards containerized workloads by detecting and preventing vulnerabilities in container images and runtime environment.
2. Cloud Security Posture Management (CSPM): This module continuously monitors and assesses your cloud environment for security misconfigurations and ensures compliance with security best practices.
3. Cloud Workload Protection Platform (CWPP): This module provides runtime protection for cloud workloads by detecting and blocking malware, exploits, and other threats.
4. Kubernetes Security: This module secures your Kubernetes clusters by enforcing security policies, detecting vulnerabilities in deployments, and preventing unauthorized access.
5. Secrets Management: This module securely stores and manages sensitive data like API keys and passwords used by cloud-native applications.

Problem Statement

For an industry/organization having complex technology infrastructure and relying on cloud infrastructure; considering the Head counts, budget and skill set of the resources, the monitoring should be outsourced. In the region there is no Service providers who has established such Managed Service.

This document details an approach, scope and Standard Operating procedure, would help any professionals to onboard.

Solution

Cloud Security Risk Monitoring focuses on comprehensive and proactive approach to safeguarding our cloud environment against evolving security threats. The service will enable early detection of security risks in cloud and help to mitigate them. This will be playing a vital role considering Organisation's cloud adoption strategy and digital transformation journey.

Key goals of this service can be summarized as;

- To provide a centralized and consolidated picture of Bank's cloud/ multi-cloud environment pertaining to but not limited to user entitlements/ identities, service exposure, compliance status, misconfigurations, vulnerability detection and hardening status of cloud services, etc.
- To provide insight into any security and compliance issue related to SaaS providers engaged with Orgnisation.

1.1. Design

- Managed Service Provider has partnered with CNAPP Provider to provide Cloud security managed monitoring service. The platform designed to provide;
    a. CSPM – Cloud security posture management
    b. CWPP – Cloud workload protection platform
    c. CDR – Cloud threat detection and response
    d. DSPM – Data security posture management

- CNAPP Provider is a cloud based platform and hosted within AWS (Amazon Web Services) /Azure in Country.
- The platform is owned by CNAPP Provider and the service includes real time monitoring of cloud native applications and report back to the Bank for any anomalies.
- Platform leverages the native cloud API to establish a trust between the platform & Bank's cloud environment.
- The platform performs continuous scan on Orgnisation's cloud infrastructure to monitor, detect and alert anomalies or deviations.
-

Standard Operating Procedure

Cloud-Native Application Protection Platform - CNAPP

Definition

CNAPP stands for Cloud-Native Application Protection Platform. It refers to a specialized platform or framework designed to provide comprehensive security solutions specifically tailored for cloud-native applications. Cloud-native applications are built using cloud computing principles and technologies such as microservices architecture, containers, orchestration (e.g., Kubernetes), and DevOps practices. These applications are designed to be highly scalable, resilient, and portable across different cloud environments.

The primary goal of a CNAPP is to address the unique security challenges posed by cloud-native applications. This includes protecting against vulnerabilities, securing interactions between microservices, managing access controls and identities, ensuring data protection, and integrating security seamlessly into the continuous integration and continuous deployment (CI/CD) pipelines.

Key features and capabilities typically found in CNAPPs include:

Container Security: Ensuring the security of containers and containerized applications, including runtime protection and vulnerability management.

Microservices Security: Securing communication channels between microservices, managing service identities, and implementing policies for authentication and authorization.

Orchestration Platform Security: Securing orchestration platforms like Kubernetes, managing configurations, network policies, and access controls.

API Security: Protecting APIs used within cloud-native applications from attacks, ensuring API availability, and validating API requests for security.

Data Security: Implementing encryption, access controls, and data integrity checks to protect sensitive data within cloud-native environments.

Integration with DevOps: Integrating security controls into CI/CD pipelines for automated security testing, vulnerability scanning, and compliance checks throughout the application development lifecycle.

Compliance and Governance: Helping organizations meet regulatory and compliance requirements specific to cloud environments, such as GDPR, PCI-DSS, and HIPAA.

CNAPPs are essential for organizations adopting cloud-native architectures as they provide the necessary tools and frameworks to ensure that security is not compromised while leveraging the benefits of cloud computing. By implementing a CNAPP, organizations can enhance their overall security posture, reduce vulnerabilities, and effectively manage risks associated with modern cloud-native application deployments.

Methodology

Cloud-native applications are built to leverage cloud computing frameworks fully. They are typically designed using microservices architecture, containerization (e.g., Docker), orchestration (e.g., Kubernetes), and often employ DevOps practices for continuous integration and continuous deployment (CI/CD).

Key Characteristics: Scalability, resilience, portability, and agility are central to cloud-native applications, allowing them to operate efficiently in dynamic cloud environments.

Security Principles for CNAPP:

Adaptability: Security measures must adapt to the dynamic nature of cloud-native applications, where components may scale up/down or move across different cloud environments.

Integration: Integration with DevOps pipelines is crucial to embed security seamlessly throughout the application lifecycle.

Visibility: Comprehensive visibility into application components, interactions, and dependencies is essential for effective monitoring and threat detection.

Automation: Utilize automation for rapid response to security incidents and vulnerabilities, leveraging APIs and orchestration tools.

Components and Capabilities:

Container Security: Protecting containers and containerized applications from vulnerabilities and runtime threats.

Microservices Security: Ensuring security across distributed microservices, including secure communication and authentication.

Orchestration Security: Securing orchestration platforms (e.g., Kubernetes) and managing access controls, network policies, and configurations.

CI/CD Pipeline Security: Integrating security checks into CI/CD pipelines to detect and mitigate vulnerabilities early in the development process.

API Security: Safeguarding APIs used within and across cloud-native applications to prevent unauthorized access and data breaches.

Data Security: Implementing encryption, access controls, and data integrity checks to protect sensitive data within the cloud-native environment.

Process of Implementing CNAPP:

Assessment and Planning: Evaluate current application architecture, security posture, and compliance requirements. Develop a security strategy aligned with business goals.

Architecture Design: Design security controls tailored to the specific characteristics of cloud-native applications, including segmentation, encryption, and identity management.

Implementation: Deploy security tools and solutions across the application stack, integrating with existing DevOps workflows and ensuring minimal impact on performance and agility.

Monitoring and Response: Continuously monitor application and infrastructure health, performance metrics, and security events. Implement automated responses to anomalies and incidents.

Continuous Improvement: Regularly review and update security measures based on evolving threats, industry best practices, and lessons learned from incidents.

Benefits Of CNAPP:

Enhanced Security Posture: Provides comprehensive security coverage across all layers of cloud-native applications, reducing vulnerabilities and mitigating risks.

Operational Efficiency: Integrates security seamlessly into DevOps processes, fostering collaboration between development, operations, and security teams.

Scalability: Scales security measures alongside application growth and changes in cloud infrastructure.

Compliance: Helps organizations meet regulatory and compliance requirements specific to cloud environments.

In conclusion, CNAPP represents a strategic approach to securing cloud-native applications, emphasizing adaptability, integration, visibility, and automation. By implementing CNAPP methodologies and processes, organizations can effectively mitigate security risks and ensure the resilience and integrity of their cloud-native applications in today's dynamic digital landscape.

Standard Operating Procedures for SOC monitoring at XXXXXXX

Purpose:

The purpose of this document is to outline procedures for the Security Operations Center (SOC) to effectively monitor and respond to configuration changes in cloud-hosted applications for **Organization**. These procedures are designed to ensure compliance, security, and operational stability.

Scope:

These procedures apply to SOC personnel responsible for monitoring and responding to configuration changes in applications hosted in the Azure Environment for **xxxxxxxx**.

Roles and Responsibilities:

SOC Manager: Oversees SOC operations, ensures adherence to procedures, and escalates incidents as necessary.

SOC Analysts: Monitor configuration changes in cloud applications, investigate anomalies, and execute incident response procedures.

Incident Response Team: Respond to escalated incidents related to configuration changes and coordinate with xxxxx's IT team.

IT Operations: Collaborate with SOC for infrastructure support and incident containment related to cloud applications.

SOC Operations Procedures

Cloud Application Configuration Monitoring

Event Logging: Enable logging and monitoring of configuration changes in Azure environments

- **Cloud infrastructure entitlement management (CIEM)**
- **Cloud security posture management (CSPM)**

Change Detection: Continuously monitor for changes to Infrastructure configurations.

- Azure non-prod tenant
- Azure prod tenant

Incident Response

Incident Identification: Detect and verify unauthorized or suspicious configuration changes.

Analysis and Triage: Assess the impact and potential risk of detected changes.

Escalation: Notify appropriate stakeholders and escalate incidents according to severity levels.

Reporting and Communication

Internal Reporting: Document incident details, response actions, and outcomes.

Customer Communication: Communicate with xxxx's designated contacts regarding incident status and resolution.

Post-Incident Review: Conduct reviews to identify root causes and improve response procedures.

Compliance and Regulations

Regulatory Compliance: Ensure SOC operations comply with industry regulations.

Data Protection: Adhere to data protection requirements during incident handling and reporting.

Tools and Technologies

Cloud Monitoring Tools: Utilize tools for real-time monitoring and analysis of cloud application configurations.

Incident Severity Levels

Low: Minor changes or deviations with minimal impact.

Medium: Changes affecting operational efficiency or security posture.

High: Critical changes posing significant risk to data integrity or regulatory compliance.

Continuous Improvement

Process Review: Regularly review and update SOPs based on industry best practices and lessons learned.

Feedback Mechanism: Solicit feedback from SOC personnel and stakeholders for process improvement.