DATA SHEET

Container Security Optimization Accelerator^{SM}

Increase application delivery. Securely.

STONE DOOR GROUP

ENGAGEMENT OVERVIEW

The purpose of this engagement is to perform an audit, gap analysis, and remediation of your current container implementation. Stone Door Group conducts a discovery of your cloud, DevOps, and container strategy, along with required regulatory controls. Our consultant then performs a gap analysis on the current container, orchestration, automation, and CI/CD configurations. You will be provided a gap analysis report (GAR) and container security blueprint (CSB) that identifies the gaps in container security and the required remediations. Finally, the consultant will work with your designated teams to implement the controls defined in the CSB and train teams on container security best practices.

KEY BENEFITS

- ✓ Identify previously unknown container security vulnerabilities due to lack of container controls
- ✓ Understand the key areas of container security
- ✓ Develop an integrated defense strategy for containers
- ✓ Integrate container security policies into existing infrastructure security policies
- ✓ Enable IT and developer teams to design applications and infrastructure with container security in mind

The following section describes the specific phases of the Cloud Container Security Optimization Assessment. Each phase builds on the previous phase, increasing the capability of the overall solution.

Phase 1 > Discovery

The goal of the discovery phase is to evaluate the existing customer cloud infrastructure for the purpose of creating a cost analysis report.

TASKS

- □ Review Regulatory and Compliance Requirements
- □ Review Container and DevOps strategies
- □ Review cloud IAM users and roles
    - Determine system vs user accounts
    - Identify job roles needing cloud resources
    - Determine if IAM permissions match job role requirements
- □ Review Application Workloads
    - Number of and purpose for applications
    - Required data access
    - Application requirements for Dev, QA, and Prod environments
- □ Review Application Lifecycle
    - Acquiring existing container content from public sources
- Secure registries for content storage and trustof public image content

WHAT FEATURES ARE INCLUDED?

Review current container strategy and regulatory requirements

Review container infrastructure configuration settings in key areas

Identify, prioritize, and assess risk of gaps in container configuration

Deliver gap analysis report (GAR) and container security blueprint (CSB) to key stakeholders

Guide IT teams through required configuration changes to implement CSB

Provide extensive security training

- Vulnerability scanning of content sources
- Practices for creating net new container content
- Runtime authorization of container content
- Access controls to data sources by users and container images

OUTPUTS

- □ Container Gap Analysis Report (CGAR): a 10 – 15 report that describes the current state of cloud consumption
- □ Review CGAR report with key executive stakeholders

Phase 2 > Analysis

The goal of the analysis phase is to synthesize the CGAR report into a Container Security Blueprint (CSB):

TASKS

- □ Synthesize data into an executable Container Security Blueprint (CSB)
- □ Generate container security blueprint for customer to implement:
  - Configuration of Identity and Access Management
  - Configuration Trusted Registries for container images
  - Implementation of container vulnerability scanning

OUTCOMES

✓ Bring container infrastructure into corporate and regulatory compliance

✓ Accelerate application and feature delivery through a secure container infrastructure

✓ Obtain full container and infrastructure security accountability

- Best practices for developing new container content
- Configuration of secure container and orchestration runtime environments
- Implementation of least privilege access to data from container based applications

OUTPUTS

- □ Container Security Blueprint: a 10 – 15 page report that describes the prescriptive actions required on the cloud platform to meet the Cost Reduction Goal.
- □ Container Security Blueprint Executive Deck: a 5 – 7 slide deck providing the executive highlights of the Cost Reduction Plan

Phase 3 > Review

The goal of the Review Phase is to review the Container Security Blueprint (CSB) with key executive stakeholders and discuss possible implementation of recommendations within the CSB to achieve the required corporate and regulatory compliance.

TASKS

- □ Conduct executive stakeholder review of Container Security Blueprint
- □ Review implementation options for the Container Security Blueprint
- □ Answer questions and ideate with executive stakeholders on future container implementation goals and how they interface with the Container Security Blueprint

OUTPUTS

- □ Meeting notes detailing executive stakeholder next steps

QUESTIONS?

Give us all call at 1-800-906-0102 or email us at letsdothis@stonedoorgroup.com.