Continuous Security Buddy (CSB) for OpenShift Kubernetes /OpenStack Platform

Mahesh Bang, Infosec Architect, Cisco Systems
Cloud & DevOps Security Summit, Denver 2019

Nov 2019
Agenda

1. Cloud NativeTransformation (CNT) and Security Needs
2. Tenant Security Assurance via Continuous Security Buddy (CSB)
3. CSB Story, Key Components and Features
4. CSB Core Building Blocks
5. Q&A
Cloud Native Transformation (CNT) Journey

Total Tenants: 12K +

Tenant-1
Cloud Application Environment (CAE)
OpenStack (P3)

Tenant-2
(Tenant-2 (Openshift))

Tenant-3

POD
Container

VM

CI/CD
DevSecOps
Cloud Native
Microservices
Containers
Security Need:

- Application Teams
- Platform Teams
- Infosec/PSA

Shared Responsibility

Multi-cloud security

Cloud Security: a SHARED Responsibility

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Continuous Security Buddy (CSB) provides templates, plugins, and capabilities to speed the secure deployment of cloud components via automating critical security requirements and delivers "Security as Code."
DevSecOps: Security Implementation as Code

Continuous Security Buddy (CSB)

Automate Security Controls & validation in CICD pipelines

Automate Security Controls & validation in Operating environments

CSB: Pipeline Edition

CSB: Platform Edition

Third Party Lib
Static Scan
Hardening Checks
Web and API Scanning
Credentials Management
PSB Validation and Reporting

IAM
Network
Logging & Monitoring
Compute
Storage
CSB Work-Flow

- Audit Test Capability Development
- Audit Test Execution
- Test Result Processing
- Reporting, Dashboard
- Known/Unknown Risks
- Scan Complete
  - Scan completed, Metadata Collected
- Risk Eliminated
  - Remediation of Vulnerabilities
CSB Journey
A DevSecOps way

- Agile Security (Security Hackathons)
- Security Guardrails
- Continuous Validation (Continuous Security Buddy)
- Automate Security (Security as code)
Agile Hackathons (Security)

You may think it’s this:

It’s more like this:

Agile Hackathon: Testing real use cases

Security requirements user stories

Analyze
Ready
Work in progress
Cross-team review
Done (definition of done)

Cross-team collaborators
Working outside of domain
Hands-on implementation
Live feedback exchange
Knowledge booster

Teams of 3
- Drives productivity
- Team stay focused
- Delivers tasks on time
Security Hackathons

Pre-Work Planning
- Identify Top Security use cases
- Team member Assignment

Event Logistics
- Run in sprints
- Sprint Readout, Reviews
- Definition of Done
- Documentation

Retrospective
- Worked /Didn’t work
- Improvements
- Next Steps

Output
- Publish Security Guardrails
- Automate Implementation via CSB

Security Guardrails are implementation steps for application teams against controls in specific environments to help satisfy security requirements.
Continuous Security Buddy (CSB) Platform Edition

A suite of security tools speed up compliance and security operations.
Secure & Trusted Base Images

- Approved sources only
- Any Image source
- My Dev VM
- Docker Push
- Containers.cisco.com
- Pull the image
- Is it scanned OK?
- Apply patches and Rebuild
- Scan report
- CAE/Openshift
- Enterprise Trusted Container Repository
- No known Vulnerabilities in Images
- Images must be hardened per CIS Benchmarks

CSB Components

- Tenant Management
- Scan Result Management
- Security Assurance Value
- Risk Impact Generation
- Scan Scheduler
- Risk Appetite Based Scanning
- Driving Remediation & Risk Management
- Vulnerability Reporting & Dashboard
- Analytics, Support, Operations

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
CSB Continuous Execution

Discovery

Execution

Results & Reporting

Remediation

CSB Tenants

Continuous Security Buddy

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
<table>
<thead>
<tr>
<th>Platform</th>
<th>Baseline</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAE</td>
<td>Identity Management</td>
<td>Audit for any unauthorized administrative roles that are not predefined platform provisioned roles</td>
</tr>
<tr>
<td></td>
<td>Security &amp; Trusted Base Container Images</td>
<td>Audit that user created service account token has been changed after 90 days</td>
</tr>
<tr>
<td></td>
<td>Network Security</td>
<td>Validate if the tenant container image was provisioned from a trusted registry</td>
</tr>
<tr>
<td></td>
<td>Privileged User and Service Account</td>
<td>Validate proper TLS termination type</td>
</tr>
<tr>
<td></td>
<td>Harden Base OS Images</td>
<td>Validate secure transport protocol is enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Validate known blacklisted vulnerable ports are not opened</td>
</tr>
<tr>
<td>Platform 3</td>
<td>Network Security</td>
<td>Audit for unauthorized administrative roles not predefined platform roles.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Validate tenant container VM image is provisioned from the C9 repository</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Validate least privilege network access is configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Validate icmp protocol not enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Validate secure transport protocol is enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Validate known blacklisted vulnerable ports are not opened</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Validate IPv6 is not configured</td>
</tr>
</tbody>
</table>
## CSB 1.0 : How to Understand Report

### CSB IT Security Health Report

**Application Name:** BCS Consulting Enablement Portal  
**Vulnerabilities:** 2  
**Data Classification:** Restricted  
**Tenant Contacts:**  
- Customer: john.doe@cisco.com  
- PSA: mark.smith@cisco.com  
- Prime: jill.williams@cisco.com  
**Key Compliance Failure Security-saught Areas:**  
1. Networking (3)

### Networking

<table>
<thead>
<tr>
<th>Vulnerability Name</th>
<th>Vulnerability Description</th>
<th>Additional Information</th>
<th>Identified Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSECURE Traffic is permitted</td>
<td>Insecure traffic should not be set to 'allow' Under TLS settings</td>
<td>hostName: bcs-stage.cisco.com tenantName: bcs-slb-instr-stage terminationType: edge insecureTraffic: Allow targetPort: web routeName: bcs-slb-instr-stage</td>
<td>2019-07-22 14:23:15</td>
</tr>
<tr>
<td>INSECURE Traffic is permitted</td>
<td>Insecure traffic should not be set to 'allow' Under TLS settings</td>
<td>hostName: bcs-stage.cisco.com tenantName: bcs-slb-instr-stage terminationType: edge insecureTraffic: Allow targetPort: web routeName: bcs-slb-instr-stage</td>
<td>2019-07-22 14:23:15</td>
</tr>
</tbody>
</table>

### Reference:

### Support Information:
- Web Team: [https://io2.cisco.com/2k-L7U](https://io2.cisco.com/2k-L7U)  
- Support Email: csb-cloud-security@cisco.com  
- CSB IT Community: [http://io2.cisco.com/csb-it](http://io2.cisco.com/csb-it)  

To change contact info such as PSA, Prime or other application attributes, please use ESP.
CSB 1.0 : Remediation Guidance

CSB – Vulnerabilities and Remediation Playbook
http://go2.cisco.com/CSBIT-REM

These next steps will show you to remediate through CLI

Warning - (Service level imapct) - At the end of these steps, the container will restart.

- a) OC login <cae-cluster-name> - login to CAE console
- b) OC project <your project name> - switch into the non compliant project
- c) OC get routes - Will list all the routes associated with the project, you can also to check whether you need modify the configuration for particular route
- d) OC edit routes/<your route name> - change to below

```bash
28     insecureEdgeTerminationPolicy: None
30     termination: edge
```

- Please look at step 2 to identify your route name
Questions?
Bonus Slides
Kubernetes Specific Test Cases – Configuration File Permission & Ownership

Permissions are set to 644 or more restrictive & ownership are set to root:root for following POD specification files

• admin.conf
• controller-manager.conf
• scheduler.conf
• etcd*
• Container Network Interface file

etcd data directory ownership is set to etcd:etc
Admission control policy is set to
- SecurityContextDeny
- NamespaceLifecycle
- AlwaysPullImages
- DenyEscalatingExec
- PodSecurityPolicy
- ServiceAccount
- NodeRestriction
- EventRateLimit

Admission control policy is NOT set to
- AlwaysAdmit
Kubernetes Specific Test Cases – Configuration checks

1. anonymous-auth argument is set to false
2. kubelet-https argument is set to true
3. insecure-port argument is set to 0
4. profiling argument is set to false
5. repair-malformed-updates argument is set to false
6. audit-log-maxage argument is set to 30
7. audit-log-maxbackup argument is set to 10
8. audit-log-maxsize argument is set to 100
9. service-account-lookup argument is set to true
10. authorization-mode argument is set to Node
11. use-service-account-credentials argument is set to true

Following Arguments are NOT set
• basic-auth-file
• insecure-allow-any-token
• insecure-bind-address
• token-auth-file parameter
• secure-port argument is NOT set to 0
• authorization-mode argument is NOT set to AlwaysAllow
• auto-tls argument is NOT set to true
• AdvancedAuditing argument is NOT set to false
• peer-auto-tls argument is NOT set to true
Kubernetes Specific Test Cases – Configuration checks Continue

1. RotateKubeletServerCertificate argument is set to true
2. encryption provider is set to aescbc
3. profiling argument is set to false
4. address argument is set to 127.0.0.1
5. client-cert-auth argument is set to true
6. peer-client-cert-auth argument is set to true
7. unique Certificate Authority is used for etcd
8. Do not admit privileged containers
9. Do not admit containers wishing to share the host process ID namespace
10. Do not admit containers wishing to share the host IPC namespace
11. Do not admit containers wishing to share the host network namespace
12. Do not admit containers with allowPrivilegeEscalation
13. Do not admit root containers
14. Do not admit containers with dangerous capabilities