Montgomery IT Summit
Common Computing Environment (CCE) - Common Services, Automation Panel

Isobar, AIS, Mitre, Akamai
23 May 2018
Why CCE?

- **Common** Computing Environment: we provide the guardrails to the cloud in a standard manner so you can focus on your mission

- **Fully Automated**: All environmental stand-up is managed by automation scripts drastically speeding up deployment, reducing manual work and human error

- **Single, federated**, MFA Security Tier: there is one login across all logins with one user that all management applications leverage, no secondary logins, non elevated machine accounts. Fully audited for all management activities

- **SecDevOps** Focused: secure, mission driven deployments are built into the framework to ensure self-service and seamless deployments

- **Proactive** Scaling and System Monitoring: Mission Owners can see all operational metrics and provide rules and alerts to manager each mission their way

- **Accreditation Inheritance** and real time compliance monitoring: Using Xacta we have loaded the CCE level packages for the CSP, USAF and DoD, as well as CCE. All that’s left for the mission is the controls that are unique to them
CCE Access: Compliant, Federated Access Control for All Management Systems

Single Identity – Secure MFA Login – **Federated to ALL Systems**

"One Identify to rule them all, no secondary logins, no elevated machine accounts"
CCE Access: Video Demo
CCE Access: Redirect to Federation & CAC Prompt

Select a certificate

- [ ] SPURLOCK:HEALTH.Q.11180448071 (DOD ID CA-43)
- [ ] SPURLOCK:HEALTH.Q.11180448071 (DOD EMAIL CA-43)

[Show Certificate] [Cancel] [OK]
CCE Access: Role-Based Access to Resources

No recent connections.

All Connections:
- APORALRDPO1
- APORALRDPO2
- COMRDPPST01
- COMRDPTST02
- EESOHRDPO1
- EESOHRDPO2
- GWRMRRDP01
- GWRMRRDP02
- PRPSRDPO1
- PRPSRDPO2
- TBA-UPERDPO1
- TBA-UPERDPO2
- TBARDPO1
- TBARDPO2
- WSMISRDPO1
- WSMISRDPO2
CCE Access: Federated Bastion Host Access
CCE Access: Consent Agreement

NOTICE

You are accessing a U.S. Government Information System (IS) that is provided for USG-authorized use only.

By using this IS, you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using or data stored on this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access control) to protect USG interests—not for your personal benefit or privacy.

NOTICE: There is the potential that information presented and exported from the AF Portal contains FOUO or Controlled Unclassified Information (CCI). It is the responsibility of all users to ensure information extracted from the AF Portal is properly marked and properly safeguarded. If you are not sure of the safeguards necessary for the information, contact your local Information Security Officer.

Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychologists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

I Agree
CCE Access: Federated AWS Access

Developers

Incoming Artifacts

Approved for Test

CCE COMMON SERVICES INTEGRATION

Scanning

Deployable to Integration

INTEGRATION APPLICATION ACCOUNT

CCE COMMON SERVICES TEST

Deployable to Test

Approved for Prod

CCE COMMON SERVICES PROD

Deployable to Prod

TEST APPLICATION ACCT

Instances

Instances

Deployable to
Integration

DEPLOYMENT TOOL

DEPLOYMENT TOOL

PROD APPLICATION ACCT

Instances

Instances

DEPLOYMENT TOOL

Instances

Instances
CCE Release Process: CCE Deployments in Azure
<table>
<thead>
<tr>
<th>APPLICATION HOSTING</th>
<th>DATABASE PAAS</th>
<th>CLOUD MONITORING &amp; ALERTING</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCE Leverages AWS and Azure provided, fully managed platforms for application hosting.</td>
<td>CCE Leverages AWS and Azure provided, fully managed database platforms.</td>
<td>Logging, Monitoring, Alerting, and Audit all leverage AWS and Azure provided capabilities.</td>
</tr>
</tbody>
</table>
CCE Demo: Auto-Scaling & Monitoring in Azure
CCE Demo: Environment Self-Healing in AWS
Continuous Monitoring of controls allows for “perpetual ATOs” and real-time compliance status.

No more Periodic paper-drills!

The "common" in "Common Computing Environment" supports significant inheritance.
Automating RMF with Xacta 360

Xacta Assessment Engine
Automating the NIST RMF

Step 1: Categorize Systems
Data types (NIST and custom)

Step 2: Select Security Controls
Tailoring
Overlays
Custom requirements

Step 3: Implement Controls
Inherent controls
Import hardware and software
Integration with Nessus, Retina, and HostInfo

Step 4: Assess Security Controls
Test plan generation

Step 5: Authorize Systems
Automated risk analysis
POA&M management
Executive interface
Digital signing

Step 6: Monitor Security Controls
Workflow management
Automated change control
Automated escalation

Additional Xacta Assessment Engine Features:
Automated workflow
Automated and custom document generation
Role-based access control

Xacta Continuum
NIST SP 800-53 and other regulations

Xacta CCM
NIST SP 800-53 and other regulations

Automated Adaptive Mapping® and trending

HostInfo Agent & Other Tools
Data from: WASSP, Retina, Nessus, others
Frequency-based, automated control testing and automated tools

Asset Management

Campaigns
Based on Controls, questionnaires
Frequency-based control testing

Users

Step 3: Import assets:
Step 4 enhanced with automated test result updates with Xacta Continuum and Xacta CCM

Step 3: Import assets:
Continuous Monitoring and “real time” Compliance

### Compliance View for georgia-1 in Test Cycle 2017 Aug

#### Manage Remediation Plans

<table>
<thead>
<tr>
<th>Rule</th>
<th>Control Status</th>
<th>Aggregated Scanner Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-3</td>
<td>NOT MET</td>
<td>FAIL</td>
</tr>
<tr>
<td>AC-8</td>
<td>NOT MET</td>
<td>FAIL</td>
</tr>
<tr>
<td>AI-10</td>
<td>NOT MET</td>
<td>FAIL</td>
</tr>
</tbody>
</table>

**Tests for Control SC-13**

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Test name</th>
<th>Scanner Result</th>
<th>Analyzed Result</th>
<th>Confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe AIR</td>
<td>AIR 13.0.0.111 Multiple Vulnerabilities (APSB14-16)</td>
<td>FAIL</td>
<td>70%</td>
<td></td>
</tr>
<tr>
<td>Adobe AIR</td>
<td>AIR 3.6.0 Multiple Vulnerabilities (APSB14-06)</td>
<td>FAIL</td>
<td>70%</td>
<td></td>
</tr>
<tr>
<td>Cisco AnyConnect Secure Mobility Client 2.x / 3.x &lt; 3.1.5(170) Multiple OpenSSL Vulnerabilities</td>
<td>FAIL</td>
<td>70%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco AnyConnect Secure Mobility Client &lt; 3.1.1877 (POCOLE)</td>
<td>FAIL</td>
<td>70%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tenable</td>
<td>SSL 04-bit Block Size Cipher Suites Supported (DRAEET32)</td>
<td>FAIL</td>
<td>70%</td>
<td></td>
</tr>
<tr>
<td>Tenable</td>
<td>SSL Certificate Signed Using Weak Hashing Algorithm</td>
<td>FAIL</td>
<td>80%</td>
<td></td>
</tr>
<tr>
<td>Tenable</td>
<td>SSL RC4 Cipher Suites Supported (Bar Mifraah)</td>
<td>FAIL</td>
<td>70%</td>
<td></td>
</tr>
<tr>
<td>Tenable</td>
<td>SSL/TLS Diffie-Hellman Modulus &lt; 1024 Bits (Logjam)</td>
<td>FAIL</td>
<td>70%</td>
<td></td>
</tr>
<tr>
<td>Tenable</td>
<td>VMware vSphere Client Multiple Vulnerabilities (VMASA-2014-0033)</td>
<td>FAIL</td>
<td>70%</td>
<td></td>
</tr>
</tbody>
</table>