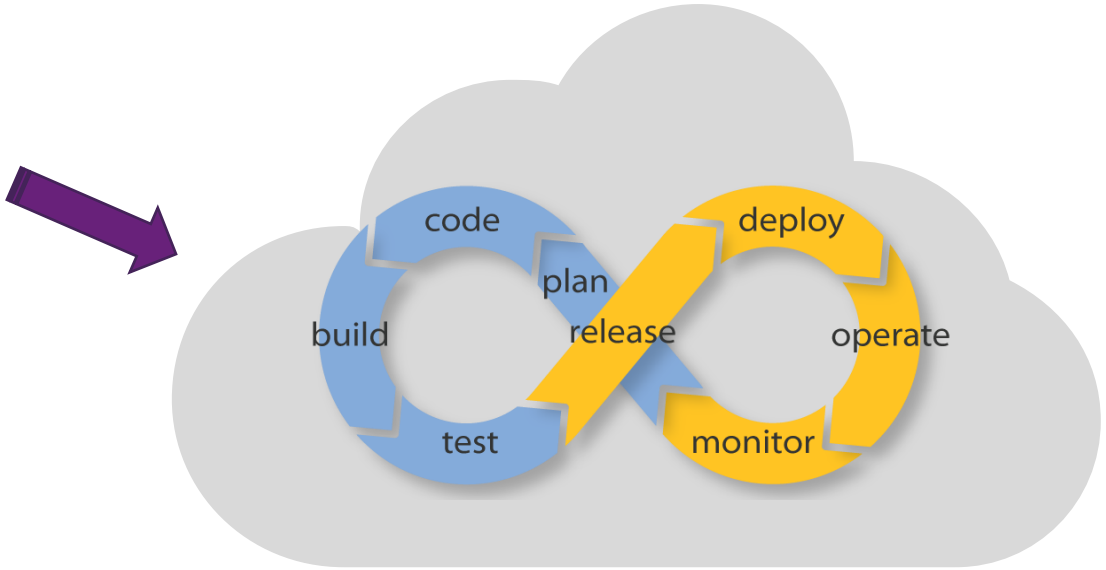
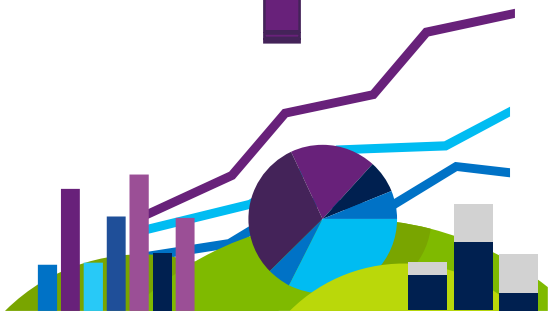
Building and operating cloud apps securely using the Secure DevOps Kit for Azure

Jonathan Trull

Microsoft

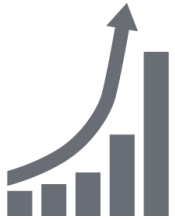
"Companies looking to digitally transform need a trusted cloud" – Satya Nadella





Onboarding	Configuration	Operational Practices and Hygiene
Pilot Onboarding	Get Secure Process	Incident Response Table Top
Subscription Procurement	Subscription Configuration	Backup and Recovery Table Top
Security Operations Onboarding	Azure Security Center Configuration	Audit Log Table Top
Configuration Insights Onboarding	Application Insights Configuration	Azure Security Center Table Top
OMS Onboarding	Deployment Template Use	Configuration Insights Table Top
MyApps Onboarding	PowerShell Library Use	Subscription User Access Reviews
Engage ISRM Onboarding	Network Configuration	RG/Resource Access Reviews
SAW Onboarding	Forensics Use	Key and Secret Rotation Table Top
Alternate Credentials – SC-backed	Key and Secret Management	Release Management/Change Control
ExpressRoute Onboarding	Key Escrow Process	Segregation of Duties & Environments
Identification of user roles within services	Tech Control Procedures and Validation	OSA Control Procedures
	ARM Policy and Resource Lock	Resource Utilization - MyBill
	Resource Group Configuration	
	OMS Configuration	

Learnings from pilot projects



> Automating security is a must!

- Challenging to maintain parity across "DevTest -> SIT -> UAT -> PROD". Too many environments to review!
- Need to strive for end-to-end validation – from a claim during a threat model to actual resource in the subscription
- HBI v/s other resources in a sub – tagging/organization can help. Need to track critical HBI artifacts (secure 'snapshot')
- Exception processes such as DRA causes lot of angst

> Need to push engineering team empowerment to the next level

- Make pre-configuration of security easier – e.g., miniature ARM-templates
- Integrate security tools such as CredScan into OneITVSO build workflow
- Expand the scope of automated security control verification (more services, more controls for each service)

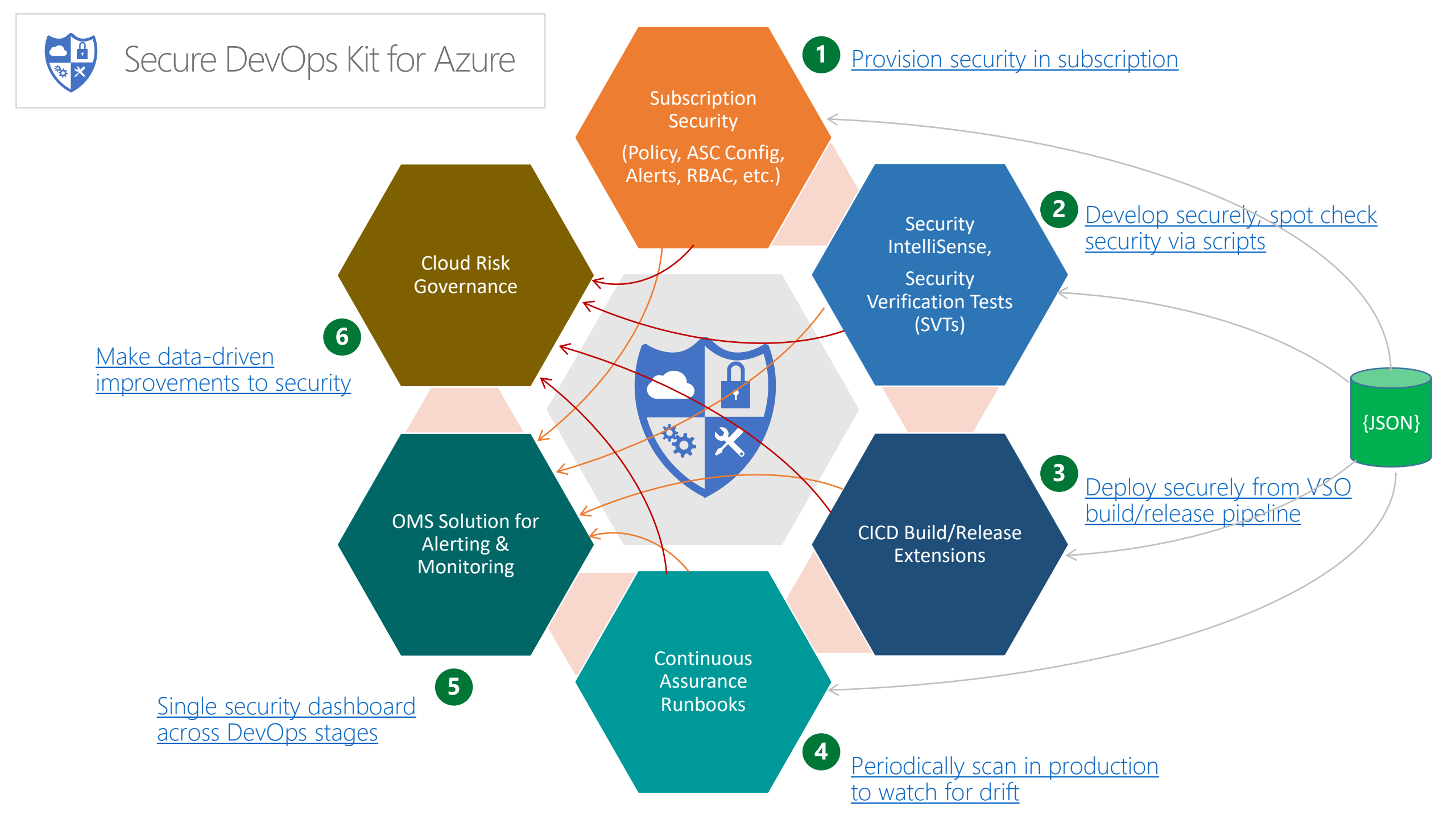
> Continuous change requires a shift towards continuous assurance!

- "Signed-off" designs and "point-in-time" assessments have a natural tension with CICD
- Need a capability to capture security snapshots and track 'drift' from a secure state

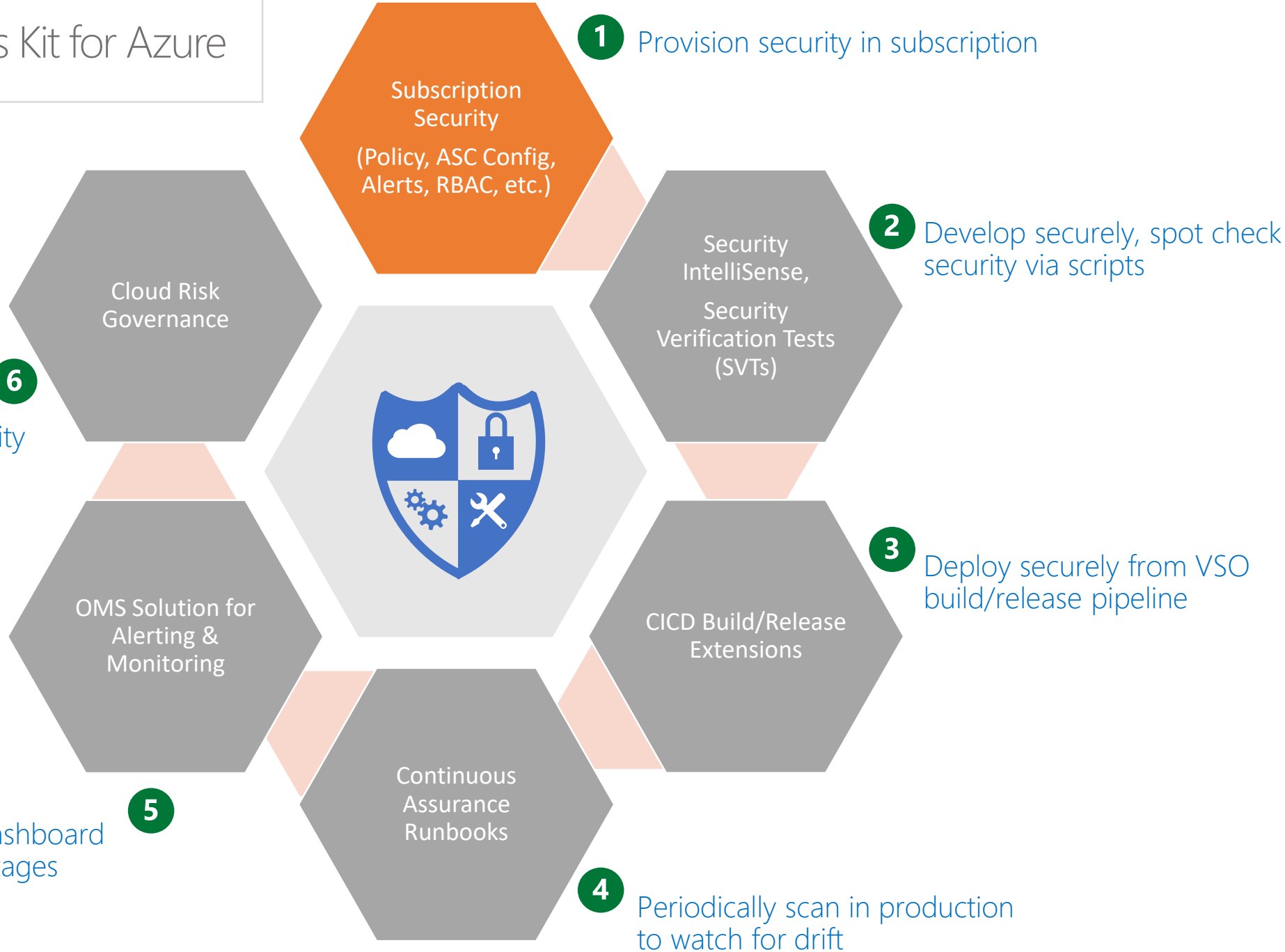
> Need to understand and establish operational security hygiene in Azure

- Subscription hygiene, access reviews, change management
- Resource configurations, firewalls, network (appliance) configuration reviews
- Key rotation, BC/DR, auditing/monitoring, incident response

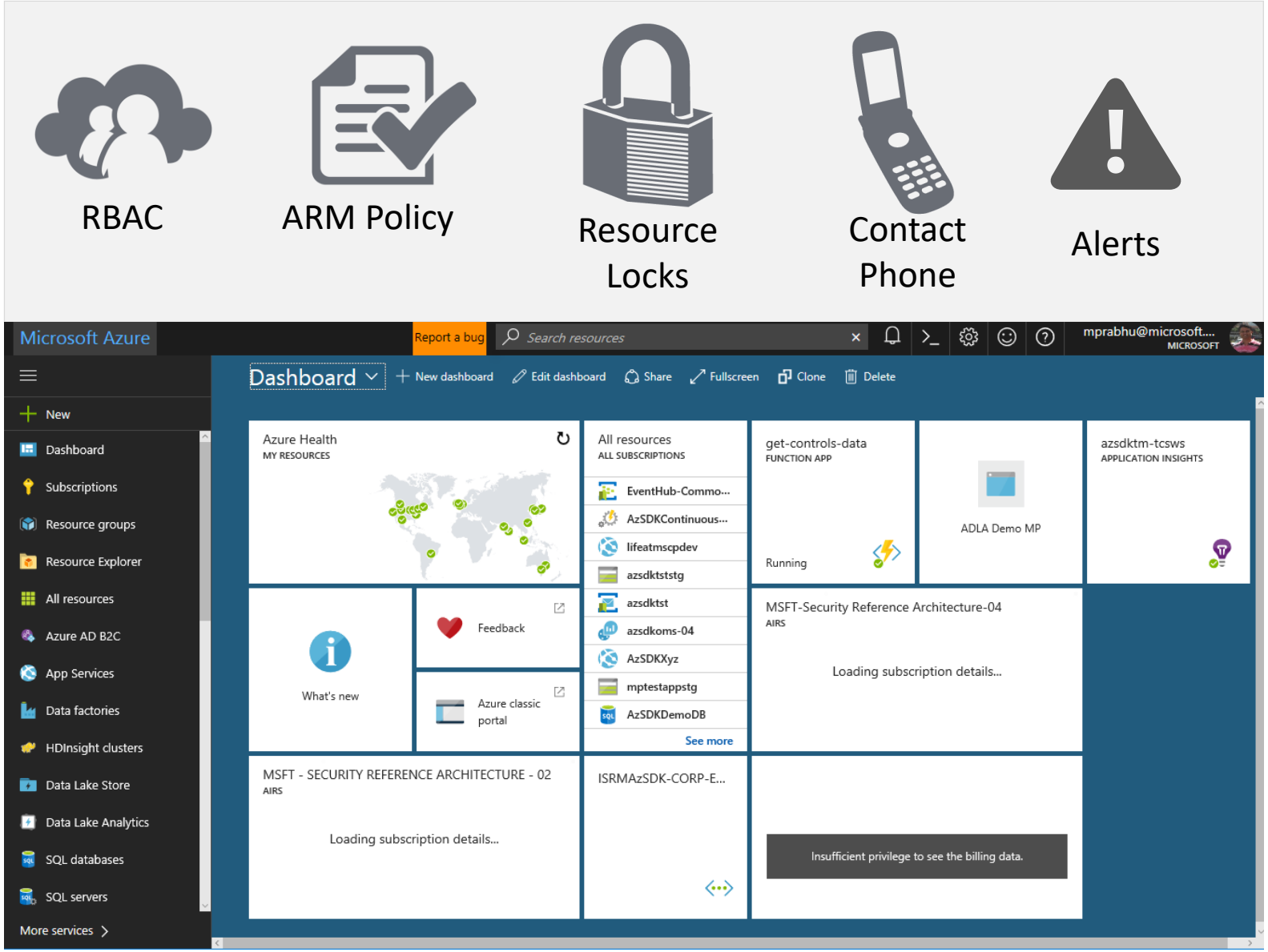
Secure DevOps Kit for Azure



Secure DevOps Kit for Azure



1- Secure your cloud subscription



Subscription security setup script…

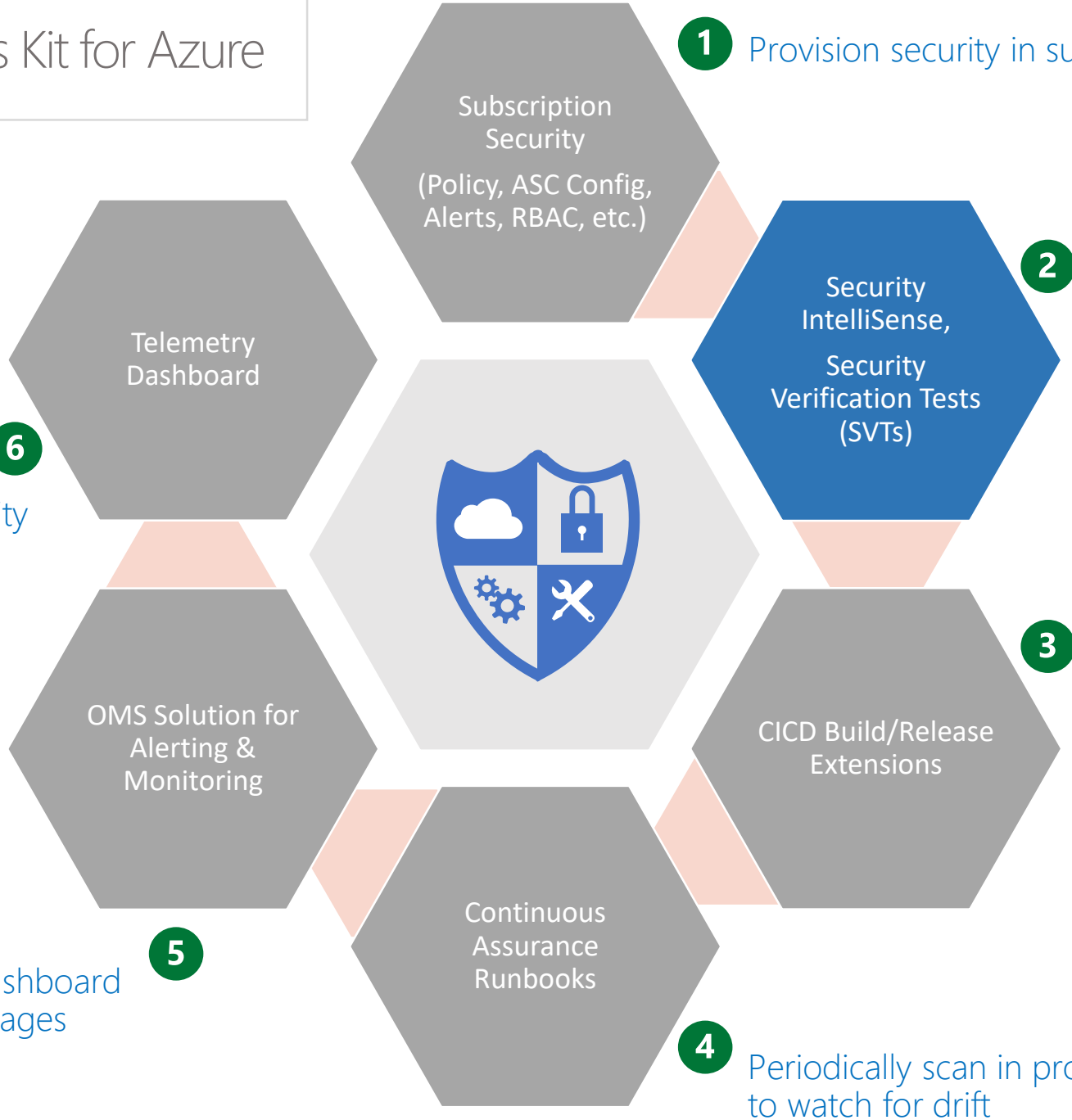
Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

```
Set-AzSKSubscriptionSecurity -SubscriptionId <sub_id> …
```

```
PS C:\> Set-AzSDKSubscriptionSecurity -SubscriptionId $subId -SecurityContactEmails 'mprabhu@microsoft.com, sbyna@microsoft.com' -SecurityPhoneNumber '425-882
================================================================================
AzSDK Version: 2.8.1
================================================================================
Method_Name: Set-AzSDKSubscriptionSecurity
================================================================================
Running AzSDK cmdlet using CSE policy...
================================================================================
Configuring Security Center
================================================================================
SecurityCenterPolicy configuration in your subscription is already up to date. If you would like to reconfigure, please rerun the command with
 '-Force' parameter.
================================================================================
Completed Security Center configuration
================================================================================
================================================================================
Setting up subscription RBAC
================================================================================
Processing RBAC rules for adding central accounts. Tags: [Mandatory]. Total accounts: 1
All required accounts are correctly configured
================================================================================
Completed subscription RBAC configuration
================================================================================
================================================================================
Setting up ARM policies
================================================================================
Processing AzSDK ARM policies. Total policies: 6
Note: Configuring ARM policies can take about 2-3 min...
33% Completed
67% Completed
100% Completed
All AzSDK ARM policies have been added to the subscription successfully
--------------------------------------------------------------------------------
================================================================================
Completed ARM policy configuration
================================================================================
================================================================================
Setting up Alerts
================================================================================
Processing AzSDK alerts. Total alerts: 7
Note: Configuring alerts can take about 4-5 min...
All AzSDK alerts have been configured successfully.
================================================================================
Completed Alerts configuration
================================================================================
================================================================================
```

Secure DevOps Kit for Azure



1. Provision security in subscription
2. Develop securely, spot check security via scripts
3. Deploy securely from VSO build/release pipeline
4. Periodically scan in production to watch for drift
5. Single security dashboard across DevOps stages
6. Make data-driven improvements to security

2- Empower developers – code, compile, prototype

1

```
public static void RandomData()
{
    // Insecure Random data generator
    var random = new Random();

    // Secure
    var rng = new RNGCryptoServiceProvider();

    // Insecure hashing algo
    var md5 = new MD5CryptoServiceProvider();

    // Insecure hashing algo
    var sha1 = new SHA1CryptoServiceProvider();

    // Secure
    var sha256 = new SHA256CryptoServiceProvider()

    //Insecure Encryption
    var rijndael = new RijndaelManaged();

    // Secure
    var aes = new AesCryptoServiceProvider();

    // Insecure AES config
    aes.KeySize = 128;
```

SecurityIntelliSenseCSCA — SecurityIntelliSenseCS The MD5 hash algorigthm is weak and must not be used.

```
...
var rng = new RNGCryptoServiceProvider();

// Insecure hashing algo
var md5 = new MD5CryptoServiceProvider();
SHA256CryptoServiceProvider md5 = new SHA256CryptoServiceProvider();

...
```

Preview changes

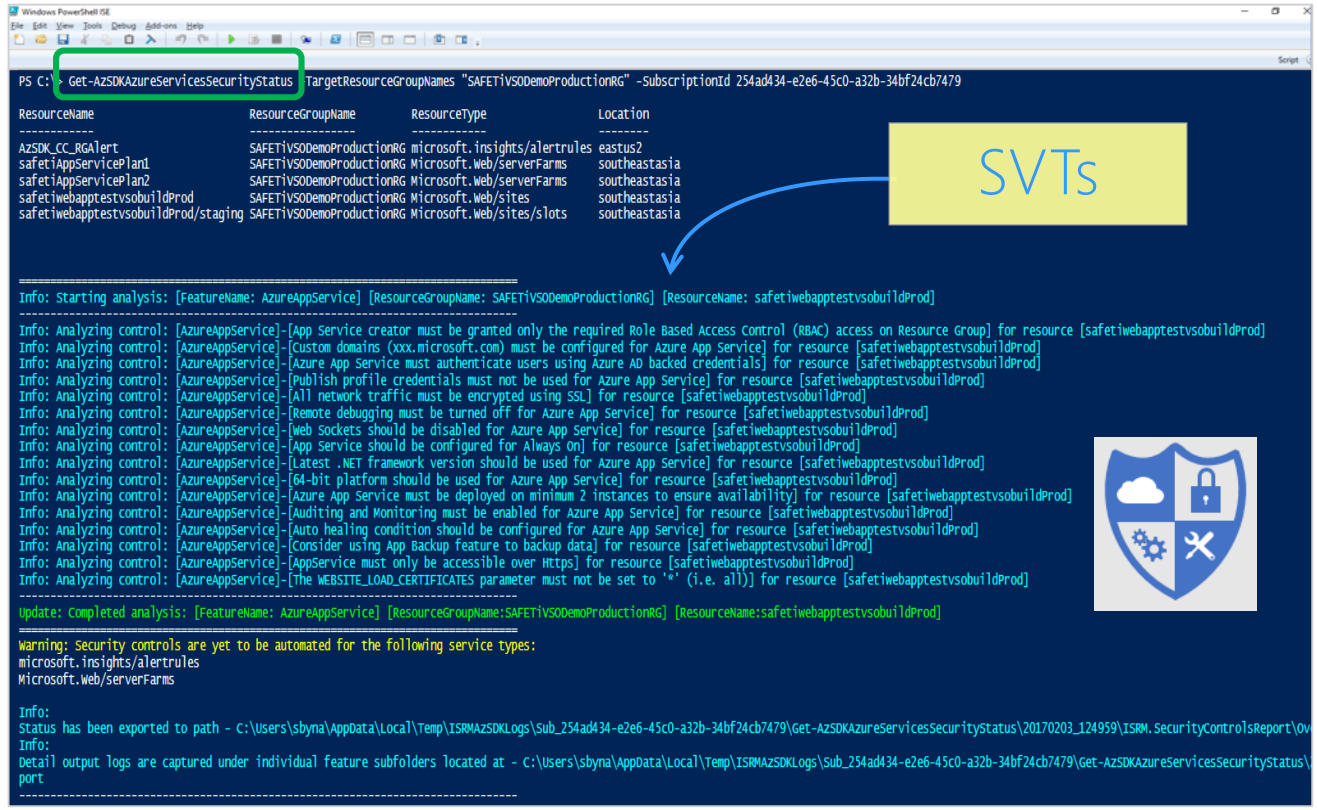
Fix all occurrences in: Document | Project | Solution

2

Along with the usual suspects…

- Static code analysis tools
- Traditional security checks
- Credentials in code, etc.

3



Write secure code with Security IntelliSense

```
public static void RandomData()
{
    // Insecure Random data generator
    var random = new Random();

    // Secure
    var rng = new RNGCryptoServiceProvider();

    // Insecure hashing algo
    var md5 = new MD5CryptoServiceProvider();

    // Insecure hashing algo
    var sha1 = new SHA1CryptoServiceProvider();

    // Secure
    var sha256 = new SHA256CryptoServiceProvider()

    //Insecure Encryption
    var rijndael = new RijndaelManaged();

    // Secure
    var aes = new AesCryptoServiceProvider();

    // Insecure AES config
    aes.KeySize = 128;
```

SecurityIntelliSenseCSCA

Suggested fix

SecurityIntelliSenseCS The MD5 hash algorigthm is weak and must not be used.

```
...
var rng = new RNGCryptoServiceProvider();

// Insecure hashing algo
var md5 = new MD5CryptoServiceProvider();
SHA256CryptoServiceProvider md5 = new SHA256CryptoServiceProvider();

...
```

Preview changes

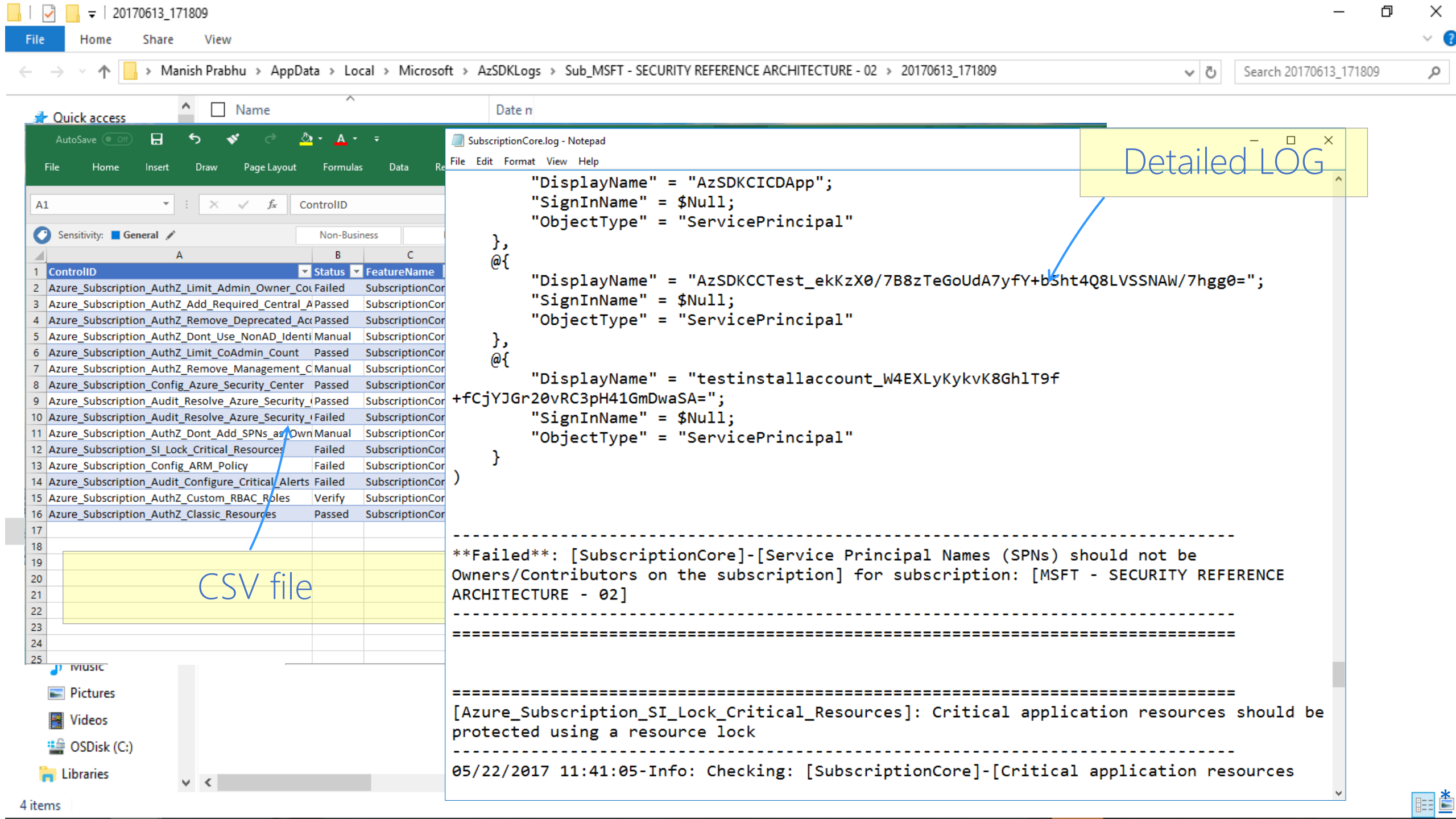
Fix all occurrences in: Document | Project | Solution

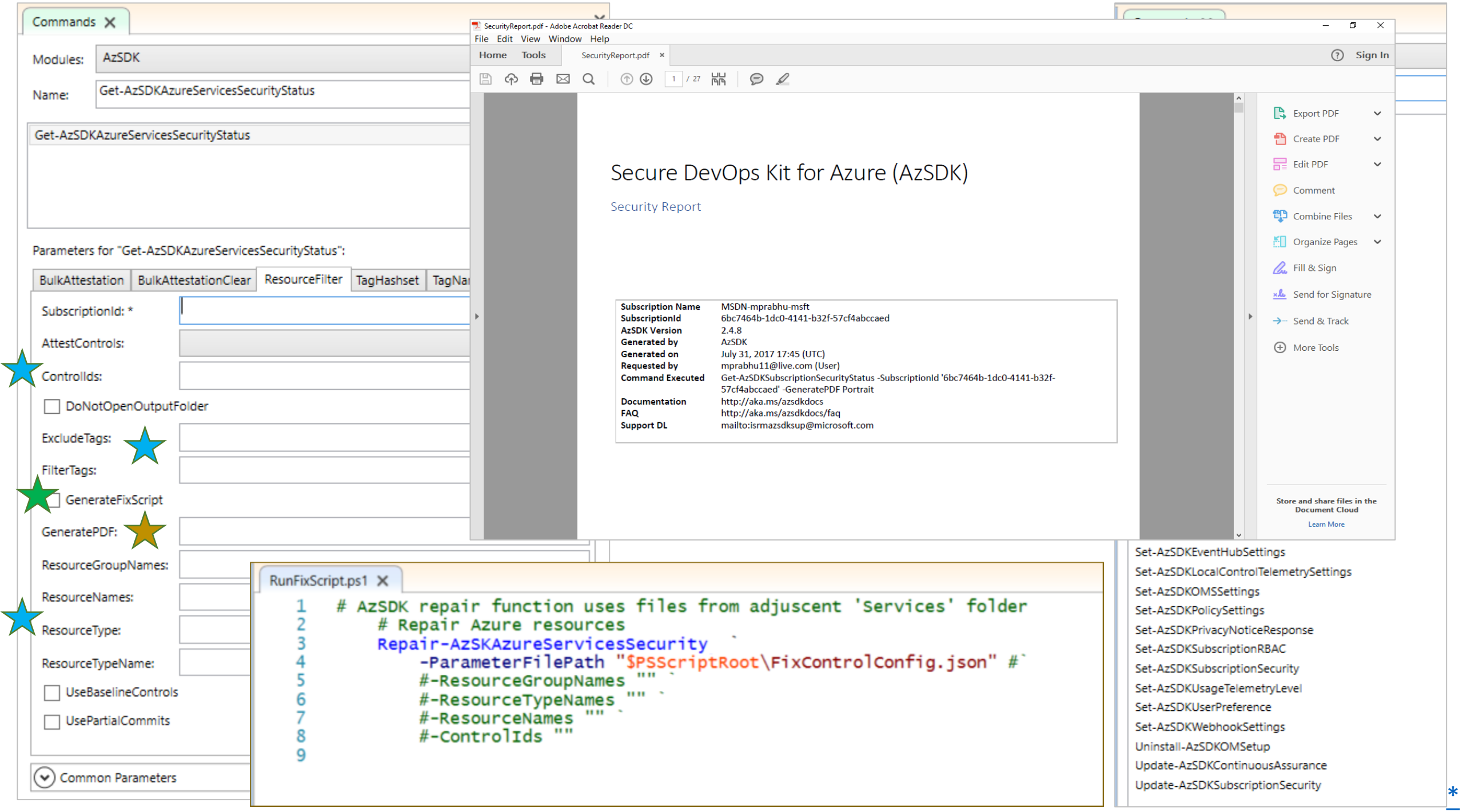
Security checks for subscription & services

```
Get-AzSKAzureServicesSecurityStatus -SubscriptionId <sub_id> -ResourceGroupNames <rg1, rg2>
```

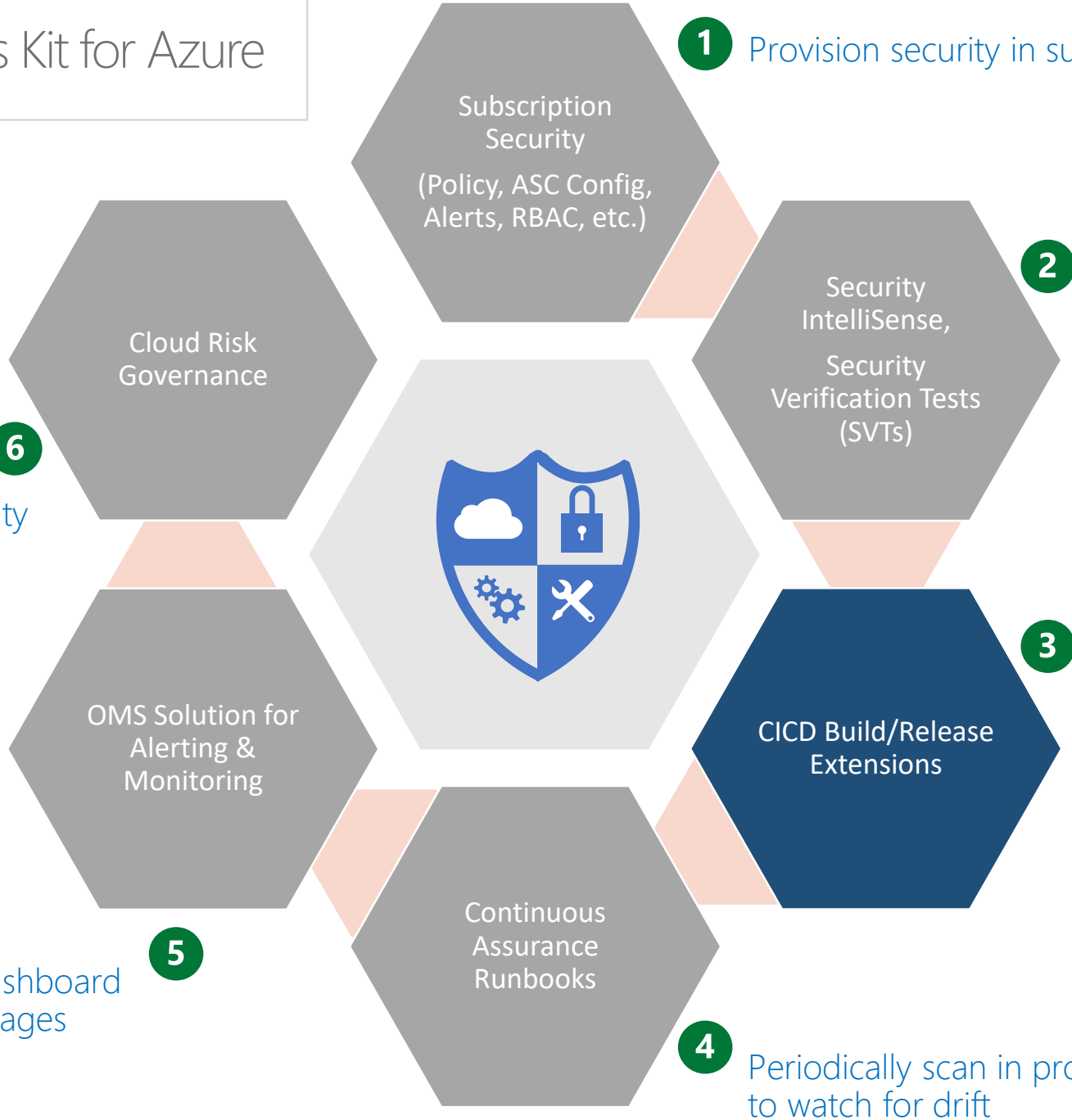
```
PS C:\> Get-AzSDKAzureServicesSecurityStatus -TargetResourceGroupNames "SAFETiVSODemoProductionRG" -SubscriptionId 254ad434-e2e6-45c0-a32b-34bf24cb7479

ResourceName                          ResourceGroupName          ResourceType                        Location
------------                          -----------------          ------------                        --------
AzSDK_CC_RGAlert                      SAFETiVSODemoProductionRG microsoft.insights/alertrules       eastus2
safetiAppServicePlan1                 SAFETiVSODemoProductionRG Microsoft.Web/serverFarms           southeastasia
safetiAppServicePlan2                 SAFETiVSODemoProductionRG Microsoft.Web/serverFarms           southeastasia
safetiwebapptestvsobuildProd          SAFETiVSODemoProductionRG Microsoft.Web/sites                 southeastasia
safetiwebapptestvsobuildProd/staging SAFETiVSODemoProductionRG Microsoft.Web/sites/slots           southeastasia


================================================================================
Info: Starting analysis: [FeatureName: AzureAppService] [ResourceGroupName: SAFETiVSODemoProductionRG] [ResourceName: safetiwebapptestvsobuildProd]
--------------------------------------------------------------------------------
Info: Analyzing control: [AzureAppService]-[App Service creator must be granted only the required Role Based Access Control (RBAC) access on Resource Group] for resource [safetiwebapptestvsobuildProd]
Info: Analyzing control: [AzureAppService]-[Custom domains (xxx.microsoft.com) must be configured for Azure App Service] for resource [safetiwebapptestvsobuildProd]
Info: Analyzing control: [AzureAppService]-[Azure App Service must authenticate users using Azure AD backed credentials] for resource [safetiwebapptestvsobuildProd]
Info: Analyzing control: [AzureAppService]-[Publish profile credentials must not be used for Azure App Service] for resource [safetiwebapptestvsobuildProd]
Info: Analyzing control: [AzureAppService]-[All network traffic must be encrypted using SSL] for resource [safetiwebapptestvsobuildProd]
Info: Analyzing control: [AzureAppService]-[Remote debugging must be turned off for Azure App Service] for resource [safetiwebapptestvsobuildProd]
Info: Analyzing control: [AzureAppService]-[Web Sockets should be disabled for Azure App Service] for resource [safetiwebapptestvsobuildProd]
Info: Analyzing control: [AzureAppService]-[App Service should be configured for Always On] for resource [safetiwebapptestvsobuildProd]
Info: Analyzing control: [AzureAppService]-[Latest .NET framework version should be used for Azure App Service] for resource [safetiwebapptestvsobuildProd]
Info: Analyzing control: [AzureAppService]-[64-bit platform should be used for Azure App Service] for resource [safetiwebapptestvsobuildProd]
Info: Analyzing control: [AzureAppService]-[Azure App Service must be deployed on minimum 2 instances to ensure availability] for resource [safetiwebapptestvsobuildProd]
Info: Analyzing control: [AzureAppService]-[Auditing and Monitoring must be enabled for Azure App Service] for resource [safetiwebapptestvsobuildProd]
Info: Analyzing control: [AzureAppService]-[Auto healing condition should be configured for Azure App Service] for resource [safetiwebapptestvsobuildProd]
Info: Analyzing control: [AzureAppService]-[Consider using App Backup feature to backup data] for resource [safetiwebapptestvsobuildProd]
Info: Analyzing control: [AzureAppService]-[AppService must only be accessible over Https] for resource [safetiwebapptestvsobuildProd]
Info: Analyzing control: [AzureAppService]-[The WEBSITE_LOAD_CERTIFICATES parameter must not be set to '*' (i.e. all)] for resource [safetiwebapptestvsobuildProd]
--------------------------------------------------------------------------------
Update: Completed analysis: [FeatureName: AzureAppService] [ResourceGroupName:SAFETiVSODemoProductionRG] [ResourceName:safetiwebapptestvsobuildProd]
================================================================================
Warning: Security controls are yet to be automated for the following service types:
microsoft.insights/alertrules
Microsoft.Web/serverFarms

Info:
Status has been exported to path - C:\Users\sbyna\AppData\Local\Temp\ISRMAzSDKLogs\Sub_254ad434-e2e6-45c0-a32b-34bf24cb7479\Get-AzSDKAzureServicesSecurityStatus\20170203_124959\ISRM.SecurityControlsReport\Ov
Info:
Detail output logs are captured under individual feature subfolders located at - C:\Users\sbyna\AppData\Local\Temp\ISRMAzSDKLogs\Sub_254ad434-e2e6-45c0-a32b-34bf24cb7479\Get-AzSDKAzureServicesSecurityStatus\
port
--------------------------------------------------------------------------------
```

Security test coverage for 25+ Azure services


20170613_171809
File
Home
Share
View
Manish Prabhu › AppData › Local › Microsoft › AzSDKLogs › Sub_MSFT - SECURITY REFERENCE ARCHITECTURE - 02 › 20170613_171809
Search 20170613_171809
Quick access
Name
Date m
AutoSave
File
Home
Insert
Draw
Page Layout
Formulas
Data
A1
ControlID
Sensitivity: General
Non-Business
ControlID
Status
FeatureName
Azure_Subscription_AuthZ_Limit_Admin_Owner_Co Failed SubscriptionCor
Azure_Subscription_AuthZ_Add_Required_Central_A Passed SubscriptionCor
Azure_Subscription_AuthZ_Remove_Deprecated_Ac Passed SubscriptionCor
Azure_Subscription_AuthZ_Dont_Use_NonAD_Identi Manual SubscriptionCor
Azure_Subscription_AuthZ_Limit_CoAdmin_Count Passed SubscriptionCor
Azure_Subscription_AuthZ_Remove_Management_C Manual SubscriptionCor
Azure_Subscription_Config_Azure_Security_Center Passed SubscriptionCor
Azure_Subscription_Audit_Resolve_Azure_Security_ Passed SubscriptionCor
Azure_Subscription_Audit_Resolve_Azure_Security_ Failed SubscriptionCor
Azure_Subscription_AuthZ_Dont_Add_SPNs_as_Own Manual SubscriptionCor
Azure_Subscription_SI_Lock_Critical_Resources Failed SubscriptionCor
Azure_Subscription_Config_ARM_Policy Failed SubscriptionCor
Azure_Subscription_Audit_Configure_Critical_Alerts Failed SubscriptionCor
Azure_Subscription_AuthZ_Custom_RBAC_Roles Verify SubscriptionCor
Azure_Subscription_AuthZ_Classic_Resources Passed SubscriptionCor
CSV file
Music
Pictures
Videos
OSDisk (C:)
Libraries
4 items
SubscriptionCore.log - Notepad
File Edit Format View Help
"DisplayName" = "AzSDKCICDApp";
"SignInName" = $Null;
"ObjectType" = "ServicePrincipal"
},
@{
"DisplayName" = "AzSDKCCTest_ekKzX0/7B8zTeGoUdA7yfY+b3ht4Q8LVSSNAW/7hgg0=";
"SignInName" = $Null;
"ObjectType" = "ServicePrincipal"
},
@{
"DisplayName" = "testinstallaccount_W4EXLyKykvK8Ghl T9f
+fCjYJGr20vRC3pH41GmDwaSA=";
"SignInName" = $Null;
"ObjectType" = "ServicePrincipal"
}
)
Failed: [SubscriptionCore]-[Service Principal Names (SPNs) should not be Owners/Contributors on the subscription] for subscription: [MSFT - SECURITY REFERENCE ARCHITECTURE - 02]
[Azure_Subscription_SI_Lock_Critical_Resources]: Critical application resources should be protected using a resource lock
05/22/2017 11:41:05-Info: Checking: [SubscriptionCore]-[Critical application resources
Detailed LOG

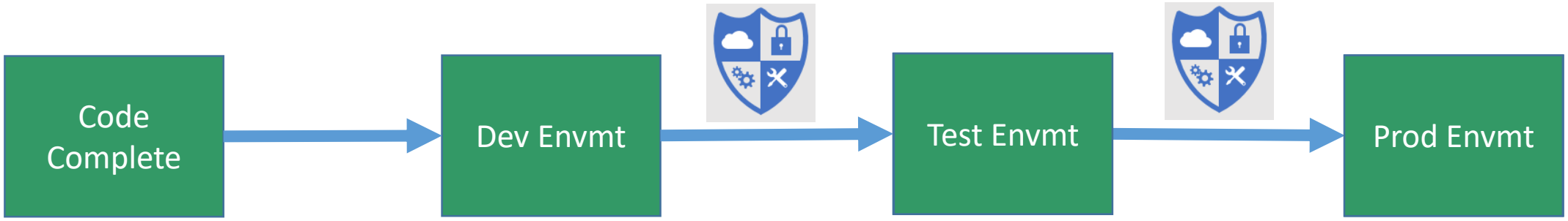

Commands
Modules: AzSDK
Name: Get-AzSDKAzureServicesSecurityStatus
Get-AzSDKAzureServicesSecurityStatus
Parameters for "Get-AzSDKAzureServicesSecurityStatus":
BulkAttestation
BulkAttestationClear
ResourceFilter
TagHashset
SubscriptionId: *
AttestControls:
ControlIds:
DoNotOpenOutputFolder
ExcludeTags:
FilterTags:
GenerateFixScript
GeneratePDF:
ResourceGroupNames:
ResourceNames:
ResourceType:
ResourceTypeName:
UseBaselineControls
UsePartialCommits
Common Parameters
SecurityReport.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools
SecurityReport.pdf
Sign In
Secure DevOps Kit for Azure (AzSDK)
Security Report
Subscription Name MSDN-mprabhu-msft
SubscriptionId 6bc7464b-1dc0-4141-b32f-57cf4abccaed
AzSDK Version 2.4.8
Generated by AzSDK
Generated on July 31, 2017 17:45 (UTC)
Requested by mprabhu11@live.com (User)
Command Executed Get-AzSDKSubscriptionSecurityStatus -SubscriptionId '6bc7464b-1dc0-4141-b32f-57cf4abccaed' -GeneratePDF Portrait
Documentation http://aka.ms/azsdkdocs
FAQ http://aka.ms/azsdkdocs/faq
Support DL mailto:isrmazsdksup@microsoft.com
Export PDF
Create PDF
Edit PDF
Comment
Combine Files
Organize Pages
Fill & Sign
Send for Signature
Send & Track
More Tools
Store and share files in the Document Cloud
Learn More
RunFixScript.ps1
1 # AzSDK repair function uses files from adjuscent 'Services' folder
2 # Repair Azure resources
3 Repair-AzSKAzureServicesSecurity `
4 -ParameterFilePath "$PSScriptRoot\FixControlConfig.json" #`
5 #-ResourceGroupNames "" `
6 #-ResourceTypeNames "" `
7 #-ResourceNames "" `
8 #-ControlIds ""
9
Set-AzSDKEventHubSettings
Set-AzSDKLocalControlTelemetrySettings
Set-AzSDKOMSSettings
Set-AzSDKPolicySettings
Set-AzSDKPrivacyNoticeResponse
Set-AzSDKSubscriptionRBAC
Set-AzSDKSubscriptionSecurity
Set-AzSDKUsageTelemetryLevel
Set-AzSDKUserPreference
Set-AzSDKWebhookSettings
Uninstall-AzSDKOMSetup
Update-AzSDKContinuousAssurance
Update-AzSDKSubscriptionSecurity

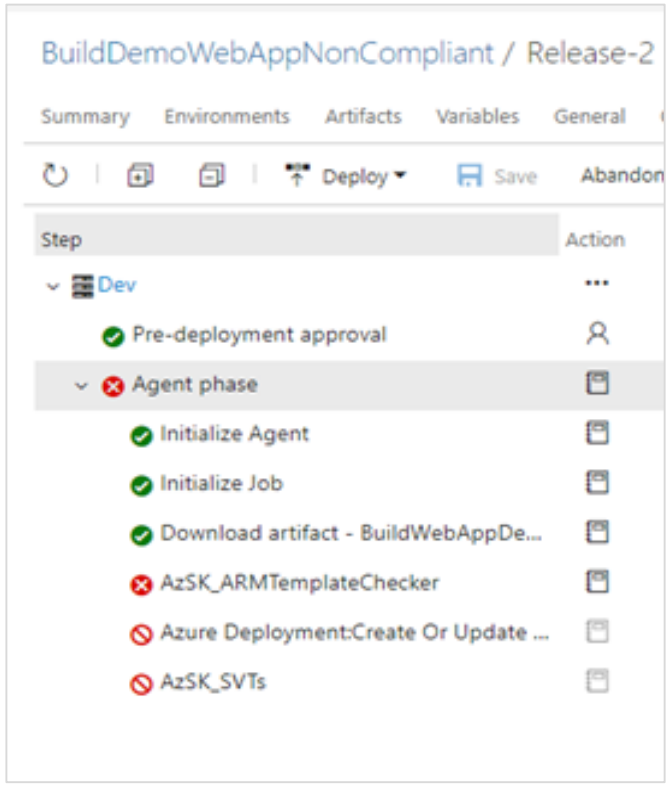
Secure DevOps Kit for Azure

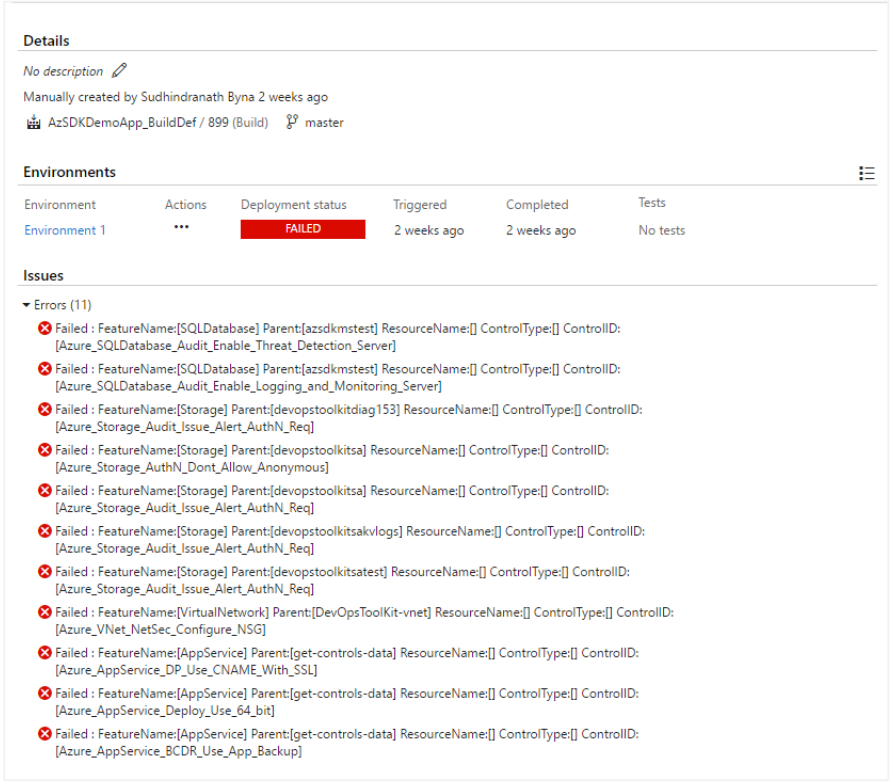


1. Provision security in subscription
2. Develop securely, spot check security via scripts
3. Deploy securely from VSO build/release pipeline
4. Periodically scan in production to watch for drift
5. Single security dashboard across DevOps stages
6. Make data-driven improvements to security

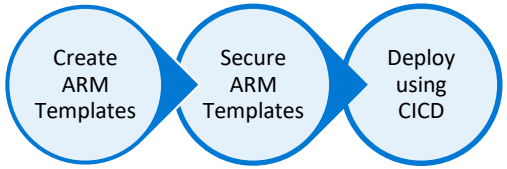
3- Bake security into cloud deployments (CICD)







Validate deployment templates



"Secure" Deploy

Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

BuildDemo.ps1

```
1  Import-Module AzSK
2  Get-AzSKARMTemplateSecurityStatus -ARMTemplatePath '.\azuredeploy_noncompliant.json' -Preview
3  Get-AzSKARMTemplateSecurityStatus -ARMTemplatePath '.\azuredeploy_compliant.json' -Preview
```

```
PS D:\Repos\BuildWebAppDemo\Build\BuildDemoApp\BuildAppARMTemplates> Get-AzSKARMTemplateSecurityStatus -ARMTemplatePath '.\azuredeploy_noncompliant.json' -Preview
================================================================================
AzSK Version: 3.1.0
================================================================================
Method Name: Get-AzSKARMTemplateSecurityStatus
Input Parameters:
Key             Value
---             -----
ARMTemplatePath .\azuredeploy_noncompliant.json
Preview         True
================================================================================
================================================================================
Starting analysis: [FileName: D:\Repos\BuildWebAppDemo\Build\BuildDemoApp\BuildAppARMTemplates\azuredeploy_noncompliantjson]
--------------------------------------------------------------------------------
Passed: [Azure_Storage_DP_Encrypt_At_Rest_Blob]
Failed: [Azure_Storage_DP_Encrypt_In_Transit]
Passed: [Azure_Storage_DP_Encrypt_At_Rest_File]
Failed: [Azure_AppService_BCDR_Use_Multiple_Instances]
Failed: [Azure_AppService_Config_Disable_Remote_Debugging]
Failed: [Azure_AppService_Config_Disable_Web_Sockets]
Failed: [Azure_AppService_BCDR_Use_AlwaysOn]
Failed: [Azure_AppService_Deploy_Use_Latest_Version]
Failed: [Azure_AppService_Audit_Enable_Logging_and_Monitoring]
Failed: [Azure_AppService_Audit_Enable_Logging_and_Monitoring]
Failed: [Azure_AppService_Audit_Enabl
Failed: [Azure_AppService_DP_Dont_All
Failed: [Azure_AppService_AuthN_Use_A
Failed: [Azure_AppService_AuthN_Use_A
--------------------------------------------------------------------------------
Summary  Total Passed Failed
-------  ----- ------ ------
High         6      2      4
Medium       7      0      7
Low          1      0      1
------   ------ ------ ------
Total       14      2     12
------   ------ ------ ------
================================================================================
Summary  Total Passed Failed
-------  ----- ------ ------
High         6      2      4
Medium       7      0      7
Low          1      0      1
------   ------ ------ ------
Total       14      2     12
------   ------ ------ ------
```

Completed

Ln 2 Col 1

Table Tools ARMCheckerResults_20180417_174139.csv - Excel

File Home Insert Draw Page Layout Formulas Data Review View Add-ins Help Team Design Search

Table Name: Table1 | Resize Table | Properties
Summarize with PivotTable | Remove Duplicates | Convert to Range | Tools
Insert Slicer | Export | Refresh | Properties | Open in Browser | Unlink | External Table Data
Header Row | Total Row | Banded Rows | First Column | Last Column | Banded Columns | Filter Button | Table Style Options
Table Styles

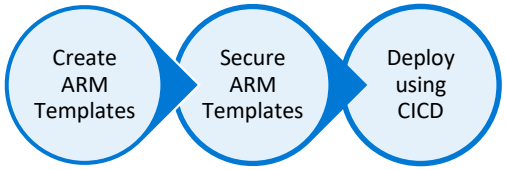
POSSIBLE DATA LOSS Some features might be lost if you save this workbook in the comma-delimited (.csv) format. To preserve these features, save it in an Excel file format. Don't show again Save As...

F15 -1

Sensitivity: General | Non-Business | Public | General | Confidential | Highly Confidential

	A	B	C	D	E	F	G	H	I	J
1	ControlId	Status	ResourceType	Severity	PropertyPath	LineNumber	CurrentValue	ExpectedValue	ResourcePath	Resou
2	Azure_Storage_DP_Encrypt_At_Rest_Blob	Passed	Microsoft.Storage/storageAcc	High	resources[1].properties.encryption.services.blob.enabled	126	TRUE	'True'	resources[1]	99
3	Azure_Storage_DP_Encrypt_In_Transit	Failed	Microsoft.Storage/storageAcc	Medium	resources[1].properties.supportsHttpsTrafficOnly	119	FALSE	'True'	resources[1]	99
4	Azure_Storage_DP_Encrypt_At_Rest_File	Passed	Microsoft.Storage/storageAcc	High	resources[1].properties.encryption.services.file.enabled	123	TRUE	'True'	resources[1]	99
5	Azure_AppService_BCDR_Use_Multiple_Instances	Failed	Microsoft.Web/serverfarms	Medium	resources[2].sku.capacity	142	1	GreaterThan 1	resources[2]	134

Fix deployment templates



"Secure" Deploy

Windows PowerShell ISE

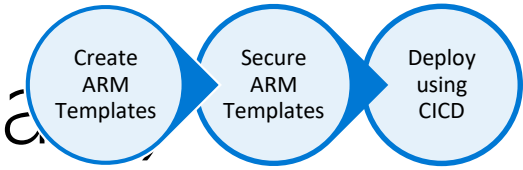
File Edit View Tools Debug Add-ons Help

BuildDemo.ps1

```
1  Import-Module AzSK
2  Get-AzSKARMTemplateSecurityStatus -ARMTemplatePath '.\azuredeploy_noncompliant.json' -Preview
3  Get-AzSKARMTemplateSecurityStatus -ARMTemplatePath '.\azuredeploy_compliant.json' -Preview
```

```
PS D:\Repos\BuildWebAppDemo\Build\BuildDemoApp\BuildAppARMTemplates> Get-AzSKARMTemplateSecurityStatus -ARMTemplatePath '.\azuredeploy_compliant.json' -Preview
================================================================================
AzSK Version: 3.1.0
================================================================================
Method Name: Get-AzSKARMTemplateSecurityStatus
Input Parameters:
Key              Value
---              -----
ARMTemplatePath .\azuredeploy_compliant.json
Preview          True
================================================================================
================================================================================
Starting analysis: [FileName: D:\Repos\BuildWebAppDemo\Build\BuildDemoApp\BuildAppARMTemplates\azuredeploy_compliantjson]
--------------------------------------------------------------------------------
Passed: [Azure_Storage_DP_Encrypt_At_Rest_Blob]
Passed: [Azure_Storage_DP_Encrypt_In_Transit]
Passed: [Azure_Storage_DP_Encrypt_At_Rest_File]
Passed: [Azure_AppService_BCDR_Use_Multiple_Instances]
Passed: [Azure_AppService_Config_Disable_Remote_Debugging]
Passed: [Azure_AppService_Config_Disable_Web_Sockets]
Passed: [Azure_AppService_BCDR_Use_AlwaysOn]
Passed: [Azure_AppService_Deploy_Use_Latest_Version]
Passed: [Azure_AppService_Audit_Enable_Logging_and_Monitoring]
Passed: [Azure_AppService_Audit_Enable_Logging_and_Monitoring]
Passed: [Azure_AppService_Audit_Enable_Logging_and_Monitoring]
Passed: [Azure_AppService_DP_Dont_Allow_HTTP_Access]
Passed: [Azure_AppService_AuthN_Use_AAD_for_Client_AuthN]
Passed: [Azure_AppService_AuthN_Use_AAD_for_Client_AuthN]
--------------------------------------------------------------------------------
Summary  Total Passed
-------  ----- ------
High         6      6
Medium       7      7
Low          1      1
------   ------ ------
Total       14     14
------   ------ ------
================================================================================
Summary  Total Passed
-------  ----- ------
High         6      6
Medium       7      7
Low          1      1
------   ------ ------
Total       14     14
------   ------ ------
```

Deploy through CICD pipeline (non-compliant)



"Secure" Deploy

BuildDemoWebAppNonCompliant / Release-2

Summary | Environments | Artifacts | Variables | General | Commits | Work items | Tests | Logs | History | View All

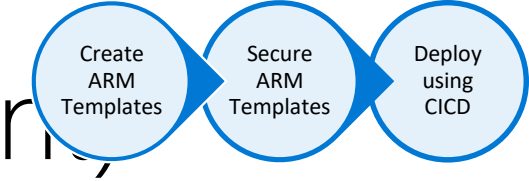
Deploy | Save | Abandon | Download all logs as zip | Send Email

Step	Action
Dev	
Pre-deployment approval	
Agent phase	
Initialize Agent	
Initialize Job	
Download artifact - BuildWebAppDe...	
AzSK_ARMTemplateChecker	
Azure Deployment:Create Or Update ...	
AzSK_SVTs	

Agent queue: Hosted VS2017 | Agent: Hosted Agent | Start Time: 4/17/2018 10:18 AM

```
2018-04-17T10:18:32.4023481Z Task         : AzSK ARM Template Checker
2018-04-17T10:18:32.4023703Z Description  : Scan ARM templates for security issues using AzSK.
2018-04-17T10:18:32.4023895Z Version      : 1.0.1
2018-04-17T10:18:32.4024085Z Author       : Microsoft Corporation
2018-04-17T10:18:32.4024285Z Help         : [More Information](http://aka.ms/azskossdocs)
2018-04-17T10:18:32.4024709Z ================================================================================
2018-04-17T10:18:49.6607753Z Installing Module AzSK...
2018-04-17T10:20:46.2288995Z ================================================================================
2018-04-17T10:20:46.2289714Z AzSK Version: 3.1.0
2018-04-17T10:20:46.2290143Z ================================================================================
2018-04-17T10:20:46.2941983Z Method Name: Get-AzSKARMTemplateSecurityStatus
2018-04-17T10:20:46.2942330Z Input Parameters:
2018-04-17T10:20:46.2942817Z Key             Value
2018-04-17T10:20:46.2944151Z ---             -----
2018-04-17T10:20:46.2944717Z ARMTemplatePath D:\a\r1\a\BuildWebAppDemo-CI\DemoBuildDrop\BuildAppARMTemplates\azuredeploy_noncompliant.json
2018-04-17T10:20:46.2945115Z Recurse         True
2018-04-17T10:20:46.2945459Z Preview         True
2018-04-17T10:20:46.2945798Z ================================================================================
2018-04-17T10:20:46.4049090Z ================================================================================
2018-04-17T10:20:46.4049482Z Starting analysis: [FileName: \azuredeploy_noncompliant.json]
2018-04-17T10:20:46.4051786Z --------------------------------------------------------------------------------
2018-04-17T10:20:46.6005716Z Passed: [Azure_Storage_DP_Encrypt_At_Rest_Blob]
2018-04-17T10:20:46.6119246Z Failed: [Azure_Storage_DP_Encrypt_In_Transit]
2018-04-17T10:20:46.6148811Z Passed: [Azure_Storage_DP_Encrypt_At_Rest_File]
2018-04-17T10:20:46.6176193Z Failed: [Azure_AppService_BCDR_Use_Multiple_Instances]
2018-04-17T10:20:46.6237927Z Failed: [Azure_AppService_Config_Disable_Remote_Debugging]
2018-04-17T10:20:46.6264926Z Failed: [Azure_AppService_Config_Disable_Web_Sockets]
2018-04-17T10:20:46.6290461Z Failed: [Azure_AppService_BCDR_Use_AlwaysOn]
2018-04-17T10:20:46.6315173Z Failed: [Azure_AppService_Deploy_Use_Latest_Version]
2018-04-17T10:20:46.6456212Z Failed: [Azure_AppService_Audit_Enable_Logging_and_Monitoring]
2018-04-17T10:20:46.6488389Z Failed: [Azure_AppService_Audit_Enable_Logging_and_Monitoring]
2018-04-17T10:20:46.6518820Z Failed: [Azure_AppService_Audit_Enable_Logging_and_Monitoring]
2018-04-17T10:20:46.6624335Z Failed: [Azure_AppService_DP_Dont_Allow_HTTP_Access]
2018-04-17T10:20:46.6650902Z Failed: [Azure_AppService_AuthN_Use_AAD_for_Client_AuthN]
2018-04-17T10:20:46.6677172Z Failed: [Azure_AppService_AuthN_Use_AAD_for_Client_AuthN]
2018-04-17T10:20:46.6733766Z --------------------------------------------------------------------------------
2018-04-17T10:20:46.8037398Z Summary  Total Passed Failed
2018-04-17T10:20:46.8037646Z -------  ----- ------ ------
2018-04-17T10:20:46.8038149Z High         6      2      4
2018-04-17T10:20:46.8038627Z Medium       7      0      7
2018-04-17T10:20:46.8039414Z Low          1      0      1
```

Deploy through CICD pipeline (compliant)



"Secure" Deploy

BuildDemoWebAppCompliant / Release-1

Summary | Environments | Artifacts | Variables | General | Commits | Work items | Tests | Logs | History | View All

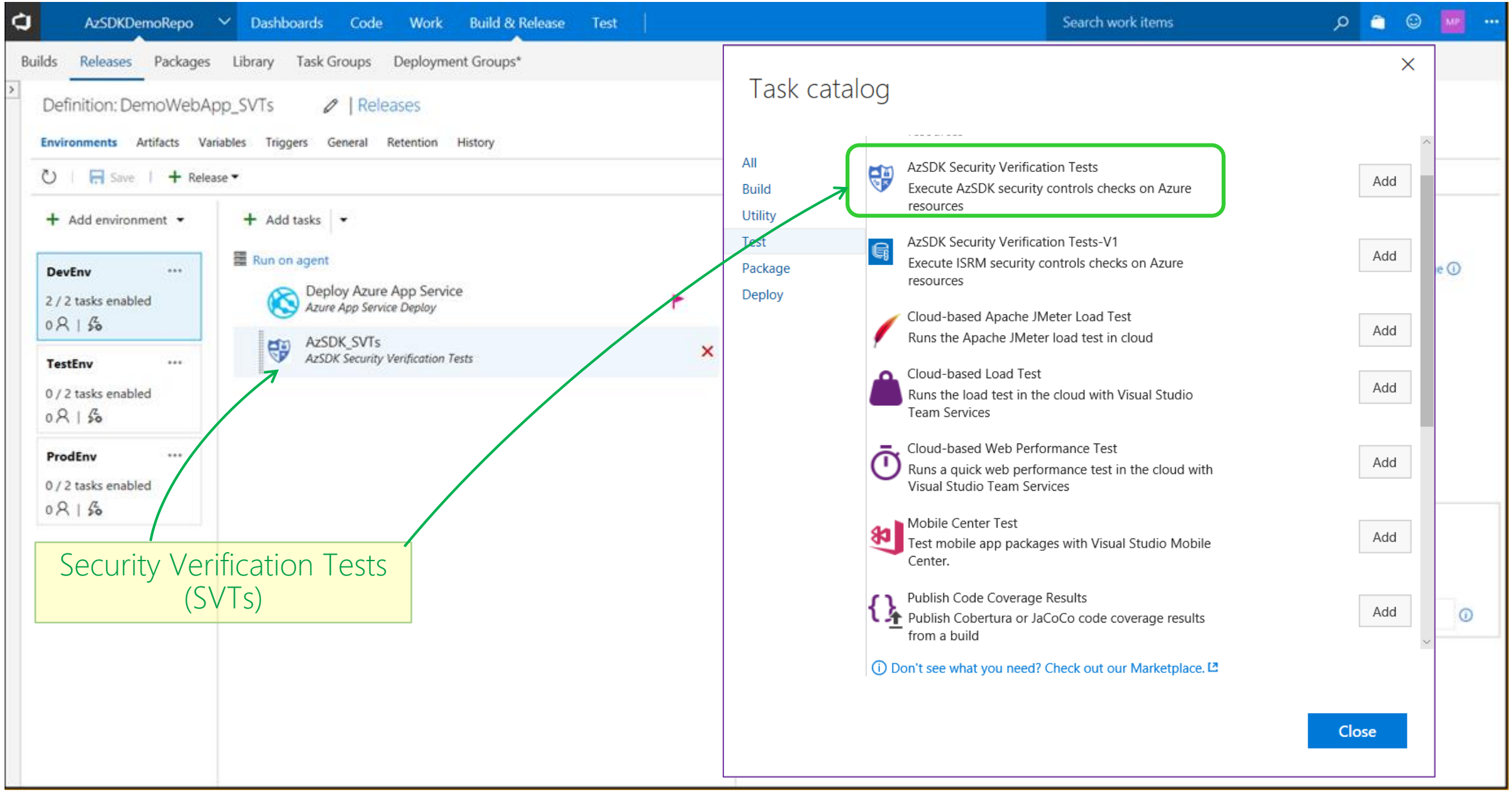
Deploy | Save | Abandon | Download all logs as zip | Send Email

Step	Action
Dev	...
Pre-deployment approval	
Agent phase	
Initialize Agent	
Initialize Job	
Download artifact - BuildWebAppDe...	
AzSK_ARMTemplateChecker	
Azure Deployment:Create Or Update ...	
AzSK_SVTs	

Agent queue: Hosted VS2017 | Agent: Hosted Agent — Start Time: 4/17/2018 11:02 AM

```
2018-04-17T11:02:53.6122280Z ##[section]Starting: AzSK_SVTs
2018-04-17T11:02:53.6129212Z ==============================================================================
2018-04-17T11:02:53.6129517Z Task         : AzSK Security Verification Tests
2018-04-17T11:02:53.6129791Z Description  : Scan Azure resources for security issues using AzSK.
2018-04-17T11:02:53.6130121Z Version      : 3.0.1
2018-04-17T11:02:53.6130353Z Author       : Microsoft Corporation
2018-04-17T11:02:53.6130598Z Help         : [More Information](http://aka.ms/azskossdocs)
2018-04-17T11:02:53.6130893Z ==============================================================================
2018-04-17T11:02:58.9654055Z Installing Module AzSK...
2018-04-17T11:04:05.4533432Z Successfully configured policy settings.
2018-04-17T11:04:05.4534041Z Start a fresh PS console/session to ensure any policy updates are (re-)loaded.
2018-04-17T11:04:11.7410016Z Successfully updated privacy settings.
2018-04-17T11:04:11.7841680Z Setting up OMS configuration...
2018-04-17T11:04:11.8464016Z ------------------------------------------------------------------------------
2018-04-17T11:04:11.8464690Z We have added new queries for the OMS solution. These will help reflect the aggregate control pass/fail status mor
2018-04-17T11:04:11.8487335Z Successfully changed policy settings
2018-04-17T11:04:28.3548141Z ==============================================================================
2018-04-17T11:04:28.3548445Z AzSK Version: 3.1.0
2018-04-17T11:04:28.3549037Z ==============================================================================
2018-04-17T11:04:28.3655569Z Method Name: Get-AzSKAzureServicesSecurityStatus
2018-04-17T11:04:28.3656053Z Input Parameters:
2018-04-17T11:04:28.3656366Z Key                  Value
2018-04-17T11:04:28.3656755Z ---                  -----
2018-04-17T11:04:28.3657073Z SubscriptionId       254ad434-e2e6-45c0-a32b-34bf24cb7479
2018-04-17T11:04:28.3657502Z DoNotOpenOutputFolder True
2018-04-17T11:04:28.3657811Z ResourceGroupNames   BuildDemoRG
2018-04-17T11:04:28.3658155Z ==============================================================================
2018-04-17T11:04:28.3711677Z Running AzSK cmdlet using CSE policy...
2018-04-17T11:04:28.4211078Z Number of resources: 4
2018-04-17T11:04:28.4399469Z Number of resources for which security controls will be evaluated: 4
2018-04-17T11:04:28.4652432Z
2018-04-17T11:04:28.4653000Z Checking resource [1/4]
2018-04-17T11:04:32.9092832Z ==============================================================================
2018-04-17T11:04:32.9093618Z Starting analysis: [FeatureName: Storage] [ResourceGroupName: BuildDemoRG] [ResourceName: builddemo1st]
2018-04-17T11:04:32.9094457Z ------------------------------------------------------------------------------
2018-04-17T11:04:33.0579158Z Checking: [Storage]-[The Access Type for containers must not be set to 'Anonymous']
2018-04-17T11:04:35.3167976Z Checking: [Storage]-[Alert rules must be configured for tracking anonymous activity]
2018-04-17T11:04:35.3264468Z **Disabled**: [Storage]-[Alert rules must be configured for tracking anonymous activity]
2018-04-17T11:04:35.3962325Z Checking: [Storage]-[Sensitive data in Storage Blob must be encrypted at rest]
2018-04-17T11:04:35.4123884Z Checking: [Storage]-[Storage Account must be configured to log and monitor authentication request data]
```

VSTS release task for 'AzSK SVTs'



AzSDKDemoRepo | Dashboards | Code | Work | Build & Release | Test | Search work items

Builds | Releases | Packages | Library | Task Groups | Deployment Groups*

DemoWebApp_SVTs / Release-4

Summary | Environments | Artifacts | Variables | General | Commits | Work items | Tests | Logs | History

Deploy | Save | Abandon | Send Email

Details

No description

Manually created by Sudhindranath Byna 4 weeks ago

AzSDKDemoRepo-Azure Web App-CI / 20170525.2 (Build) master

Work items

No associated work items found.

Tags

Add...

Environments

Environment	Actions	Deployment status	Triggered	Completed	Tests
DevEnv	...	FAILED	4 weeks ago	4 weeks ago	No tests
TestEnv	...	NOT DEPLOYED			No tests
ProdEnv	...	NOT DEPLOYED			No tests

Issues

Errors (7)

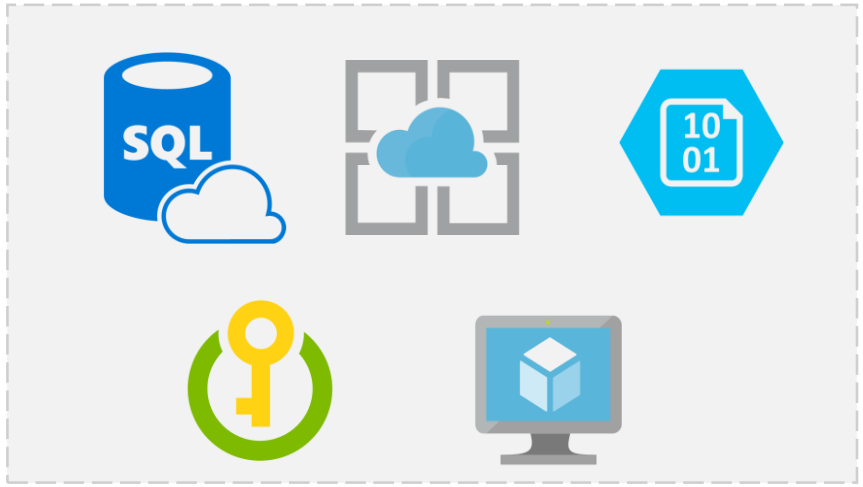
- Failed : FeatureName:[AppService] Parent:[DemoWebAppShell] ResourceName:[DemoWebAppShell] ControlType:[] ControlID:[Azure_AppService_DP_Use_CNAME_With_SSL]
- Failed : FeatureName:[AppService] Parent:[DemoWebAppShell] ResourceName:[DemoWebAppShell] ControlType:[] ControlID:[Azure_AppService_BCDR_Use_AlwaysOn]
- Failed : FeatureName:[AppService] Parent:[DemoWebAppShell] ResourceName:[DemoWebAppShell] ControlType:[] ControlID:[Azure_AppService_Deploy_Use_64_bit]
- Failed : FeatureName:[AppService] Parent:[DemoWebAppShell] ResourceName:[DemoWebAppShell] ControlType:[] ControlID:[Azure_AppService_BCDR_Use_App_Backup]
- Failed : FeatureName:[AppService] Parent:[DemoWebAppShell] ResourceName:[DemoWebAppShell] ControlType:[] ControlID:[Azure_AppService_Audit_Enable_Logging_and_Monitoring]
- Failed : FeatureName:[AppService] Parent:[DemoWebAppShell] ResourceName:[DemoWebAppShell] ControlType:[] ControlID:[Azure_AppService_DP_Dont_Allow_HTTP_Access]
- Windows PowerShell is in NonInteractive mode. Read and Prompt functionality is not available.

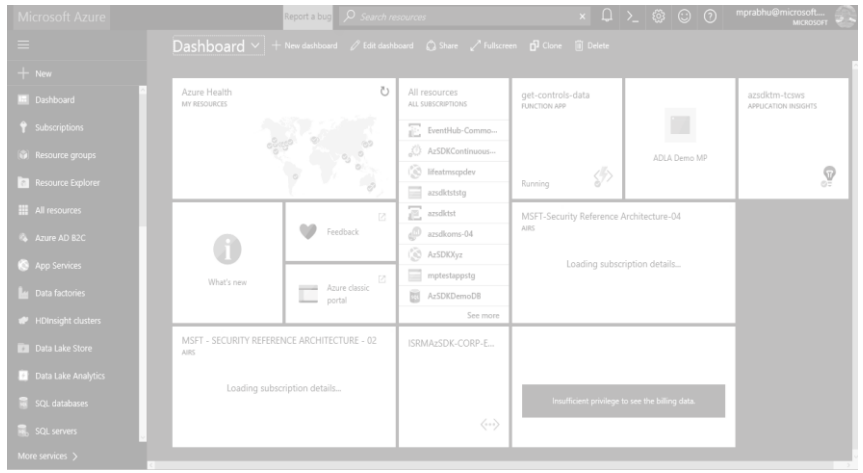
Release promoted (or not) based on outcome of AzSK SVT scan

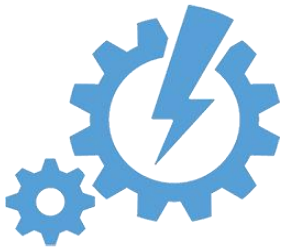
Secure DevOps Kit for Azure

1. Provision security in subscription
2. Develop securely, spot check security via scripts
3. Deploy securely from VSO build/release pipeline
4. Periodically scan in production to watch for drift
5. Single security dashboard across DevOps stages
6. Make data-driven improvements to security

4- Setup continuous security coverage



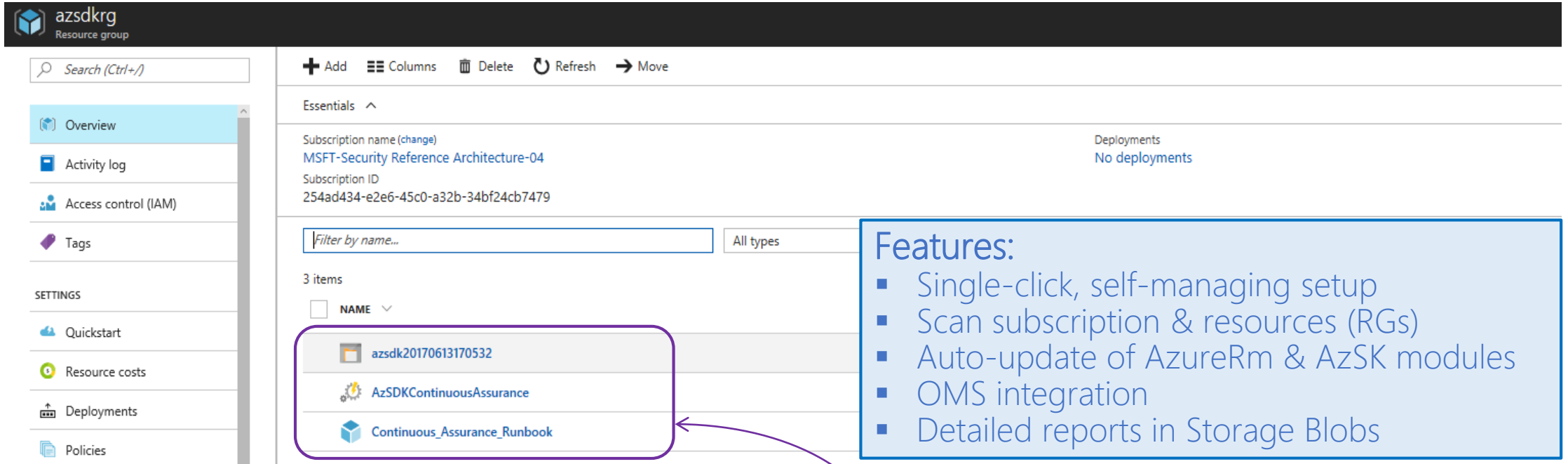




Azure Automation

Scan cloud resources in a scheduled fashion

4- Continuous assurance setup (a peek)

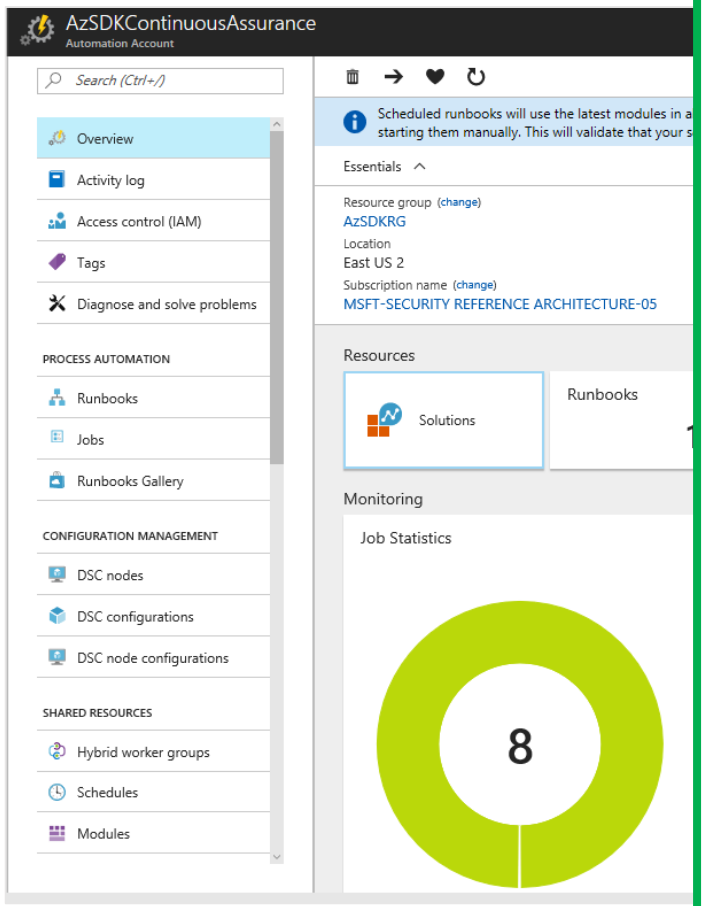


Features:

- Single-click, self-managing setup
- Scan subscription & resources (RGs)
- Auto-update of AzureRm & AzSK modules
- OMS integration
- Detailed reports in Storage Blobs

```
### Continuous Assurance setup

$omsWSId = '7b797.............................'
$omsShrKey = '40PXUi1hyMyPp.....................................=='

Install-AzSKContinuousAssurance `
            -ResourceGroupNames $appRGs `     #'RG1, RG2' or '*'
            -SubscriptionId $orgSub1 `
            -OMSWorkspaceId $omsWSId `
            -OMSSharedKey $omsShrKey
```

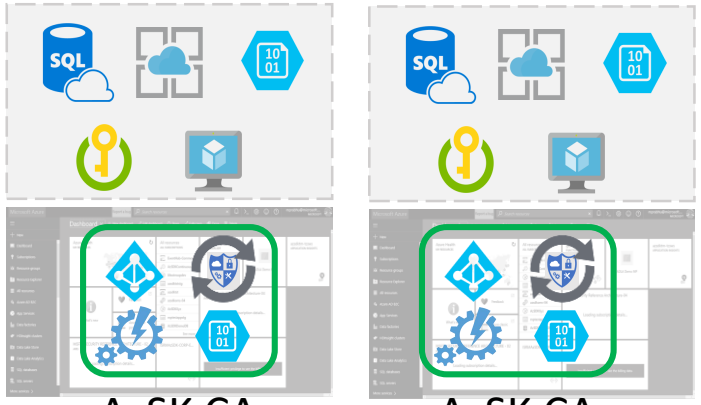
4- Continuous assurance setup (a peek)

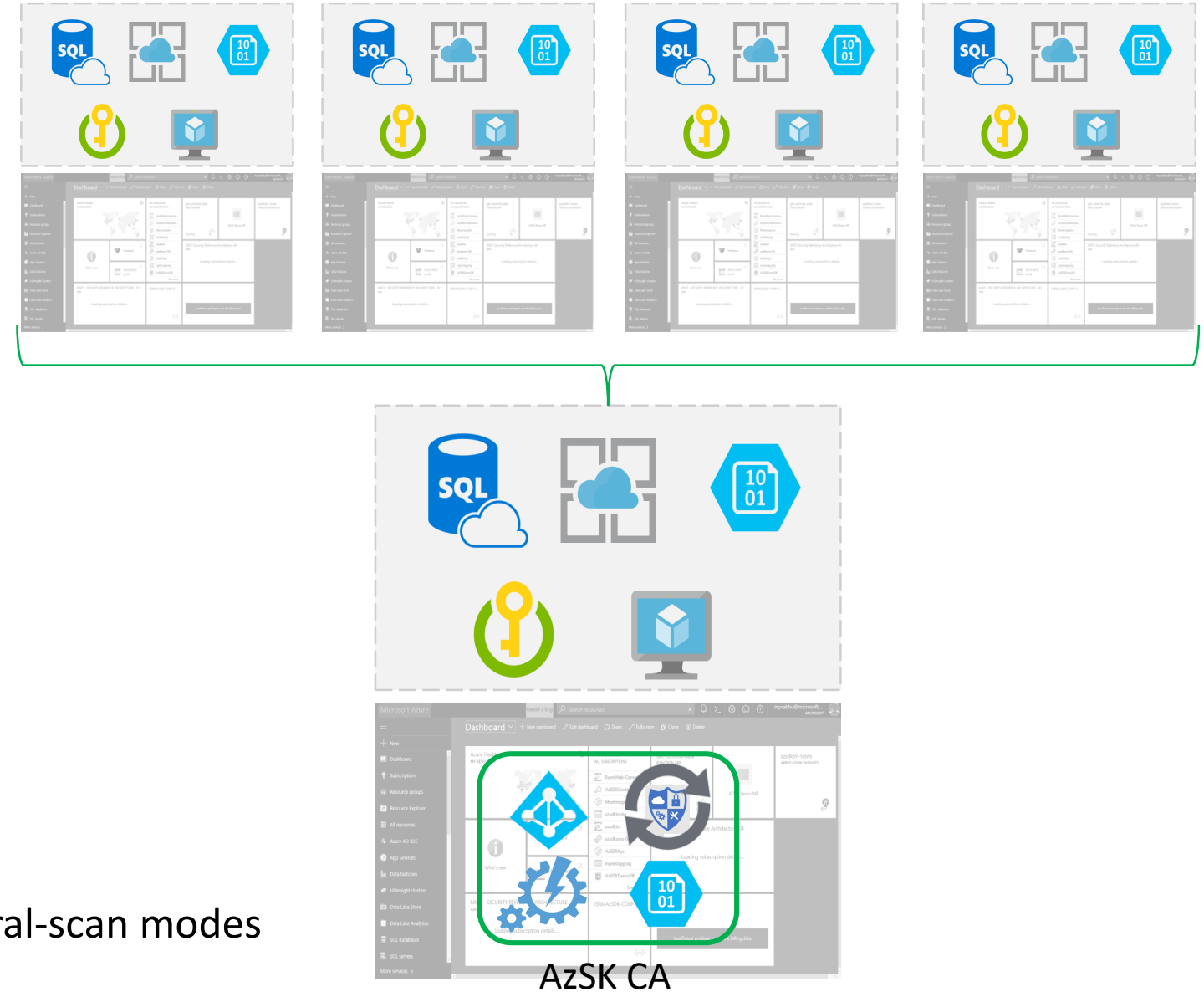


Org baseline mode (e.g.)

```
Azure_Subscription_AuthZ_Add_Required_Central_Accounts
Azure_Subscription_AuthZ_Remove_Deprecated_Accounts
Azure_Subscription_AuthZ_Dont_Use_NonAD_Identities
Azure_Subscription_AuthZ_Remove_Management_Certs
Azure_Subscription_Config_Azure_Security_Center
Azure_Subscription_Config_ARM_Policy
Azure_Subscription_Audit_Configure_Critical_Alerts

Azure_VirtualMachine_Deploy_Latest_OS_Version
Azure_VirtualMachine_Config_OS_Auto_Update_Windows
Azure_VirtualMachine_Config_Enable_Antimalware_Windows
Azure_VirtualMachine_NetSec_Dont_Open_Management_Ports

Azure_SQLDatabase_DP_Enable_TDE
Azure_SQLDatabase_Audit_Enable_Threat_Detection_Server
Azure_SQLDatabase_Audit_Enable_Threat_Detection_DB

Azure_AppService_DP_Dont_Allow_HTTP_Access

Azure_Storage_AuthN_Dont_Allow_Anonymous
Azure_Storage_DP_Encrypt_At_Rest_Blob
Azure_Storage_DP_Encrypt_At_Rest_File

Azure_CloudService_DP_DontAllow_HTTP_Access_InputEndpoints
Azure_CloudService_SI_Auto_OSUpdate
Azure_CloudService_SI_Enable_AntiMalware
Azure_CloudService_SI_Disable_RemoteDesktop_Access
```


CA – standalone v. central-scan modes

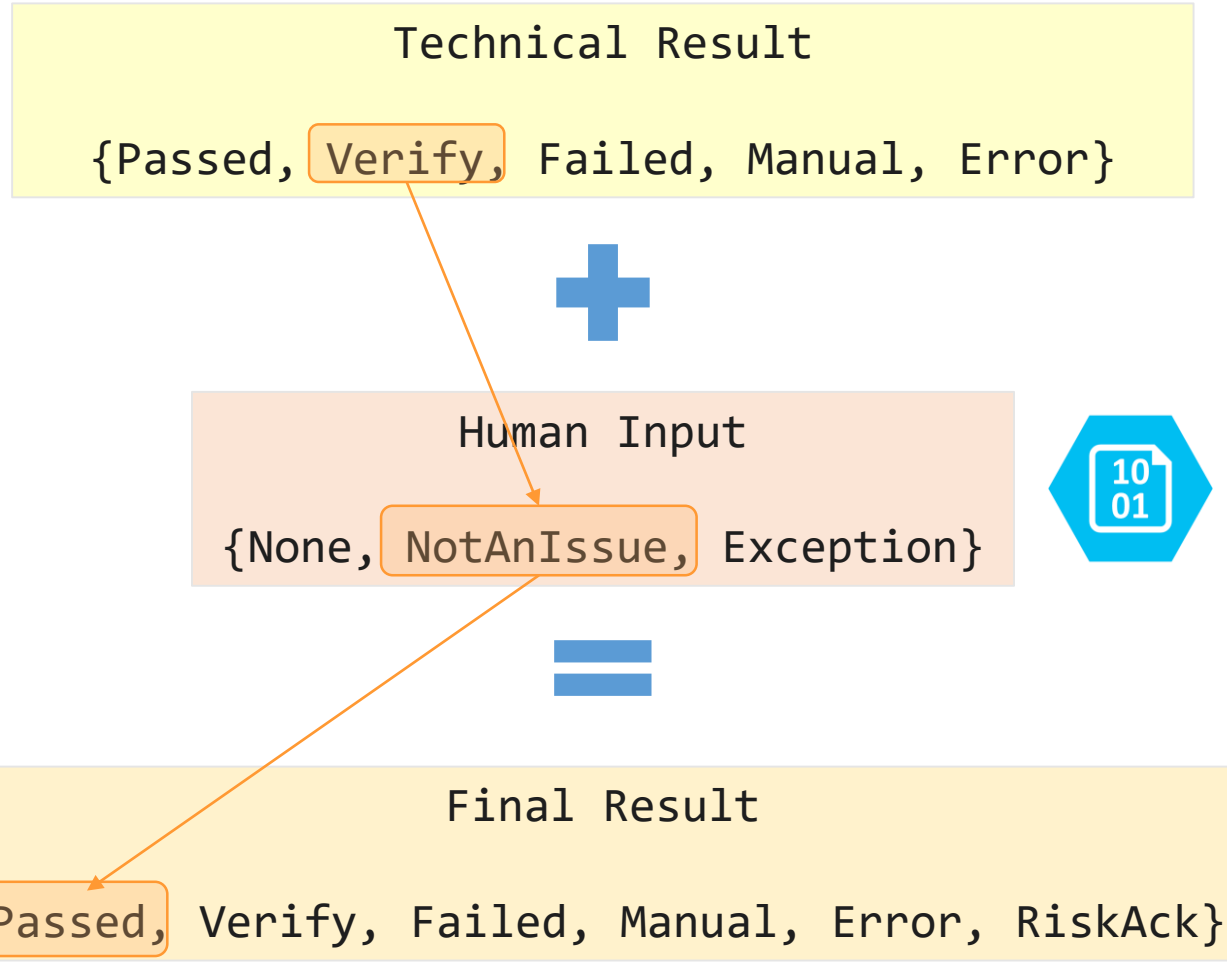




standalone v. central-scan modes

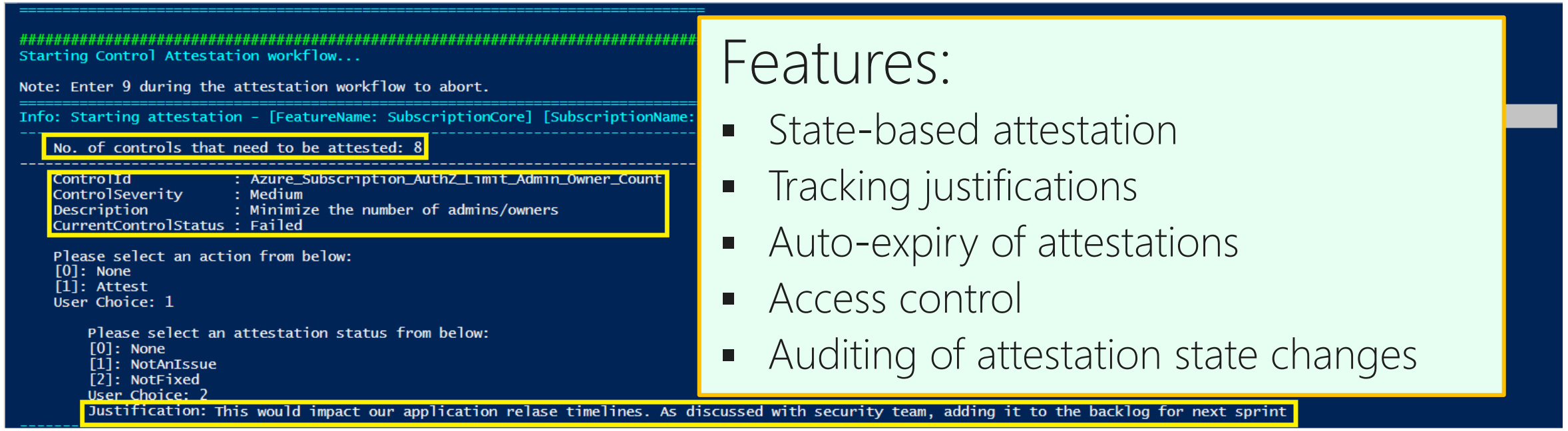
Control Attestation (overriding AzSK results)

AzSK Ctrl-Result	*Sub-status*	*Effective Ctrl-Result*	*Color*	*Notes*
Passed	None	Passed	G	
Verify	None	Verify	R	
Verify	NotAnIssue	Passed	G	Justification
Verify	NotFixed	Exception	Y	Justification
Failed	None	Failed	R	
Failed	NotAnIssue	Passed	G	Justification
Failed	NotFixed	Exception	Y	Justification
Error	None	Error	R	
Error	NotAnIssue	Passed	G	Justification
Error	NotFixed	Exception	Y	
Manual	None	Manual	R	
Manual	NotAnIssue	Passed	G	Justification
Manual	NotFixed	Exception	Y	Justification



Control Attestation – scenarios, workflow

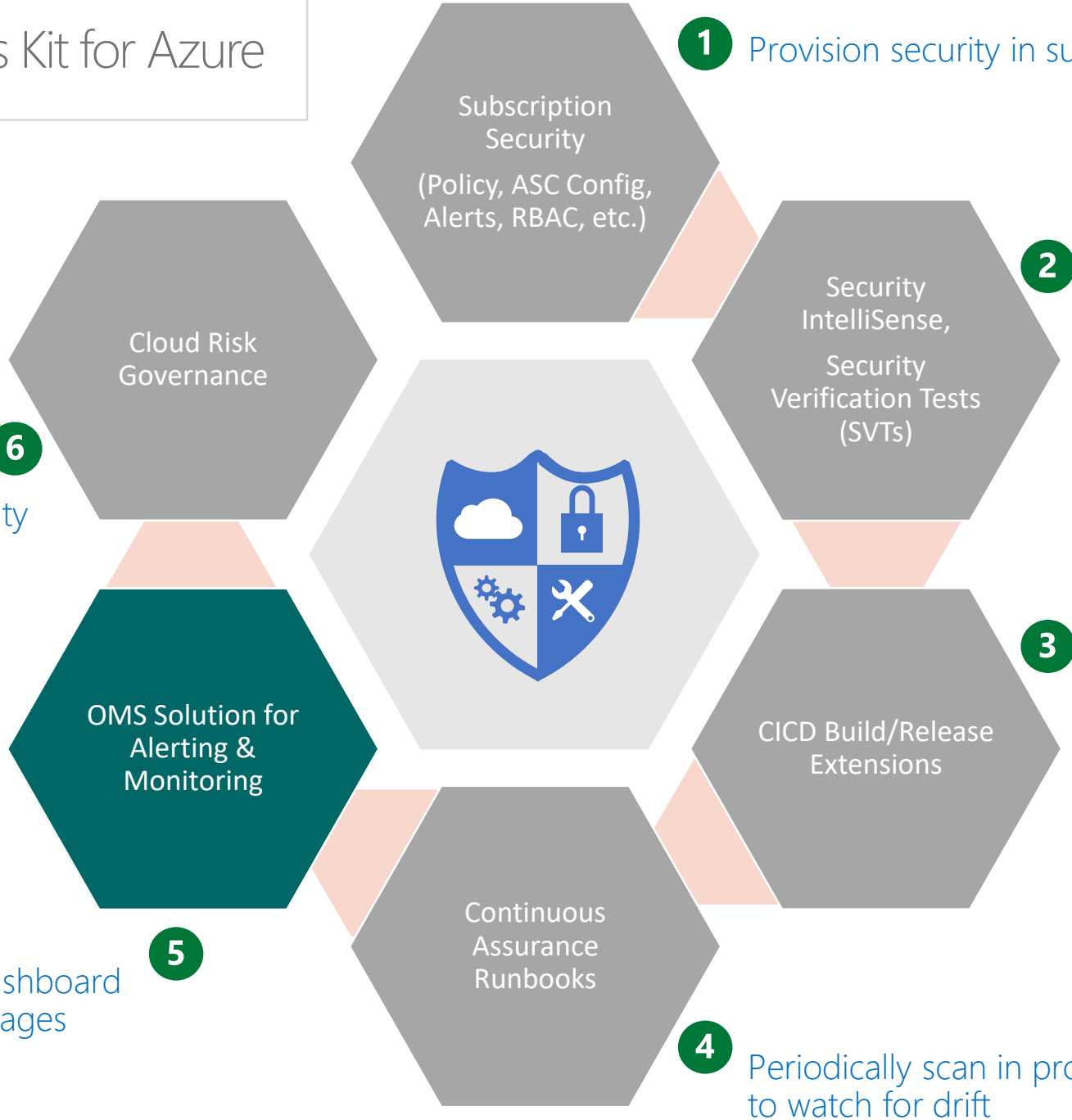
Control (e.g.,)	Technical Evaluation Result	User action/choice	Effective Result
RBAC grants	'Verify'	Reviewed log output, looks ok	'Passed'
SSE on Storage	'Failed'	Override based on contextual info	'Passed'
Use of WebSocket	'Failed'	Cannot fix at present, filing for risk ack	'Exception'



Features:

- State-based attestation
- Tracking justifications
- Auto-expiry of attestations
- Access control
- Auditing of attestation state changes

Secure DevOps Kit for Azure



1. Provision security in subscription
2. Develop securely, spot check security via scripts
3. Deploy securely from VSO build/release pipeline
4. Periodically scan in production to watch for drift
5. Single security dashboard across DevOps stages
6. Make data-driven improvements to security

5- Monitor security across dev ops stages

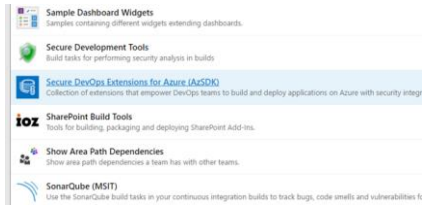
Gallery

AzSK

...

Individual developer

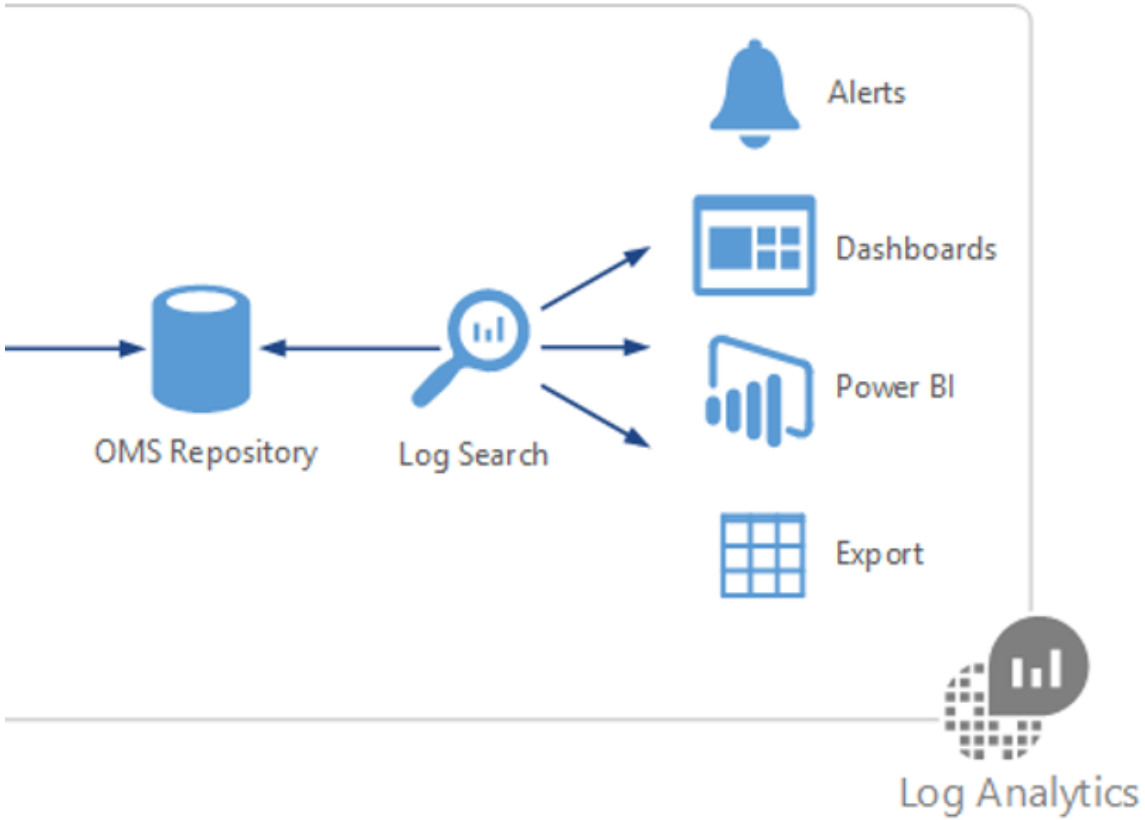
Security automation in CICD

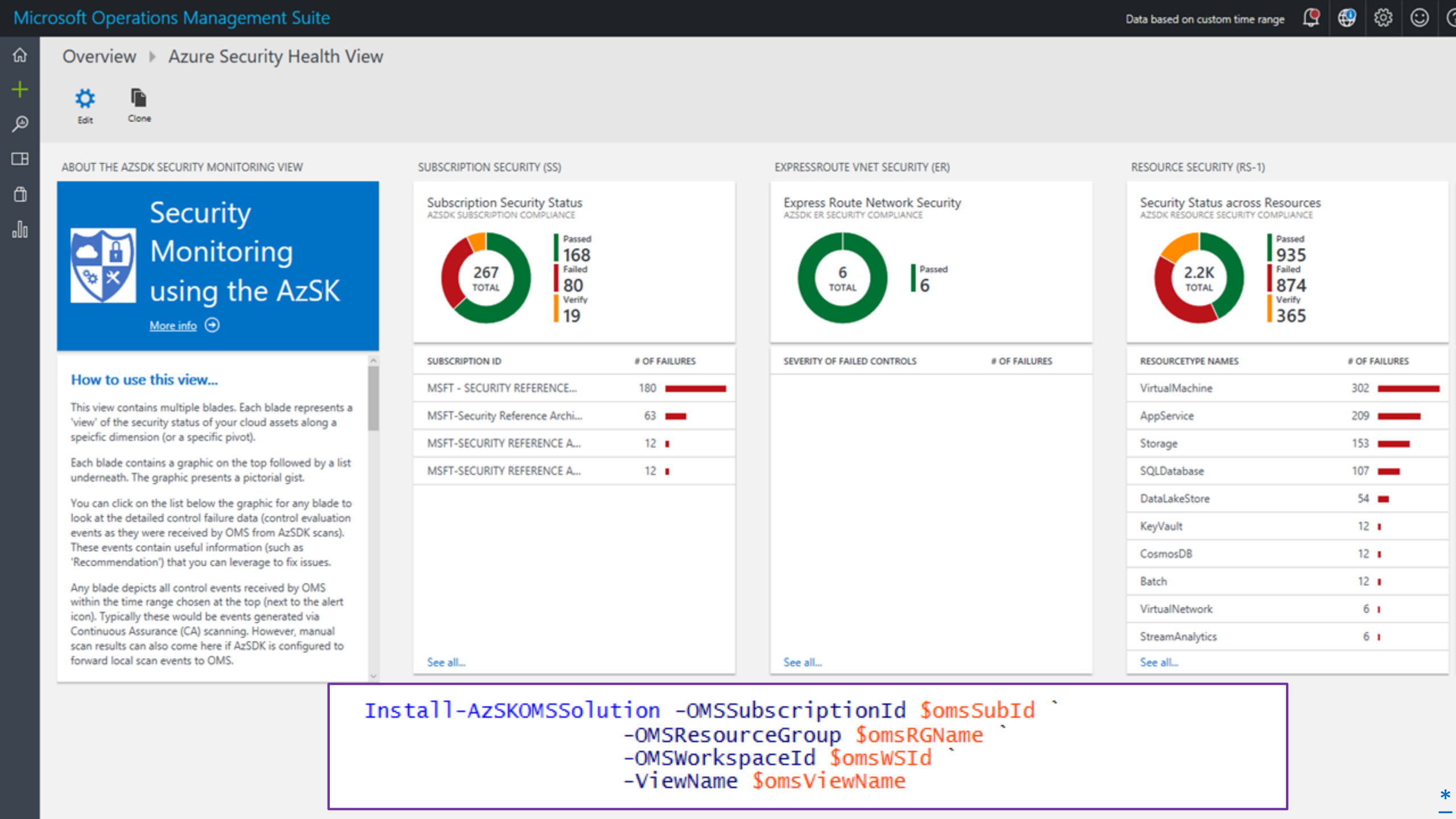


Continuous Assurance

x 1..N apps

Operations Management Suite (OMS) Repository



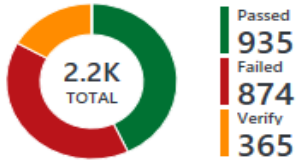

Microsoft Operations Management Suite
Data based on custom time range
Overview
Azure Security Health View
Edit
Clone
ABOUT THE AZSDK SECURITY MONITORING VIEW
Security Monitoring using the AzSK
More info
How to use this view...
This view contains multiple blades. Each blade represents a 'view' of the security status of your cloud assets along a speicfic dimension (or a specific pivot).
Each blade contains a graphic on the top followed by a list underneath. The graphic presents a pictorial gist.
You can click on the list below the graphic for any blade to look at the detailed control failure data (control evaluation events as they were received by OMS from AzSDK scans). These events contain useful information (such as 'Recommendation') that you can leverage to fix issues.
Any blade depicts all control events received by OMS within the time range chosen at the top (next to the alert icon). Typically these would be events generated via Continuous Assurance (CA) scanning. However, manual scan results can also come here if AzSDK is configured to forward local scan events to OMS.
SUBSCRIPTION SECURITY (SS)
Subscription Security Status
AZSDK SUBSCRIPTION COMPLIANCE
267 TOTAL
Passed 168
Failed 80
Verify 19
SUBSCRIPTION ID
OF FAILURES
MSFT - SECURITY REFERENCE... 180
MSFT-Security Reference Archi... 63
MSFT-SECURITY REFERENCE A... 12
MSFT-SECURITY REFERENCE A... 12
See all...
EXPRESSROUTE VNET SECURITY (ER)
Express Route Network Security
AZSDK ER SECURITY COMPLIANCE
6 TOTAL
Passed 6
SEVERITY OF FAILED CONTROLS
OF FAILURES
See all...
RESOURCE SECURITY (RS-1)
Security Status across Resources
AZSDK RESOURCE SECURITY COMPLIANCE
2.2K TOTAL
Passed 935
Failed 874
Verify 365
RESOURCETYPE NAMES
OF FAILURES
VirtualMachine 302
AppService 209
Storage 153
SQLDatabase 107
DataLakeStore 54
KeyVault 12
CosmosDB 12
Batch 12
VirtualNetwork 6
StreamAnalytics 6
See all...
Install-AzSKOMSSolution -OMSSubscriptionId $omsSubId `
-OMSResourceGroup $omsRGName `
-OMSWorkspaceId $omsWSId `
-ViewName $omsViewName

Overview ▸ Azure Security Health View

Edit Clone

RESOURCE SECURITY (RS-1)

Security Status across Resources
AZSDK RESOURCE SECURITY COMPLIANCE



Passed 935
Failed 874
Verify 365

RESOURCETYPE NAMES	# OF FAILURES
VirtualMachine	302
AppService	209
Storage	153
SQLDatabase	107
DataLakeStore	54
KeyVault	12
CosmosDB	12
Batch	12
VirtualNetwork	6
StreamAnalytics	6

See all...

RESOURCE SECURITY (RS-2)

Unique Resources with Security Issues

68

RESOURCE SECURITY (RS-3)

Unique ResourceGroups with Security Issues

33

RESOURCE SECURITY (RS-4)

Unique security failures across all resources

38

```
AzSDK_CL | where ControlStatus_s == "Failed" and FeatureName_s != "SubscriptionCore" and FeatureName_s == "Storage"
```

Advanced Analytics

19 Results List Table 00:00:00.001

8/22/2017 2:23:11.515 PM | AzSDK_CL

```
TimeGenerated : 8/22/2017 2:23:11.515 PM
ActualVerificationResult_s : Failed
ControlSeverity_s : High
Reference_s : aka.ms/azsdkosstcp/storage
ResourceName_s : azsdk20170816074206
ControlStatus_s : Failed
ControlId_s : Azure_Storage_DP_Encrypt_At_Rest_File
SubscriptionName_s : MSFT - SECURITY REFERENCE ARCHITECTURE - 02
FeatureName_s : Storage
Source_s : SDL
Recommendation_s : Run command 'Set-AzureRmStorageAccount -Name '<StorageAccountName>' -ResourceGroupName '<RGName>' -EnableEncryptionService 'File''. Run 'Get-Help Set-AzureRmStorageAccount -full' for more help.
Type : AzSDK_CL
```

[+] show more

Alerts from OMS (DevOps Kit control failures)

Wed 6/14/2017 8:07 PM

N

Microsoft Operations Management Suite Team <noreply@oms.microsoft.com>

AzSDKControlFailure_Sev_High

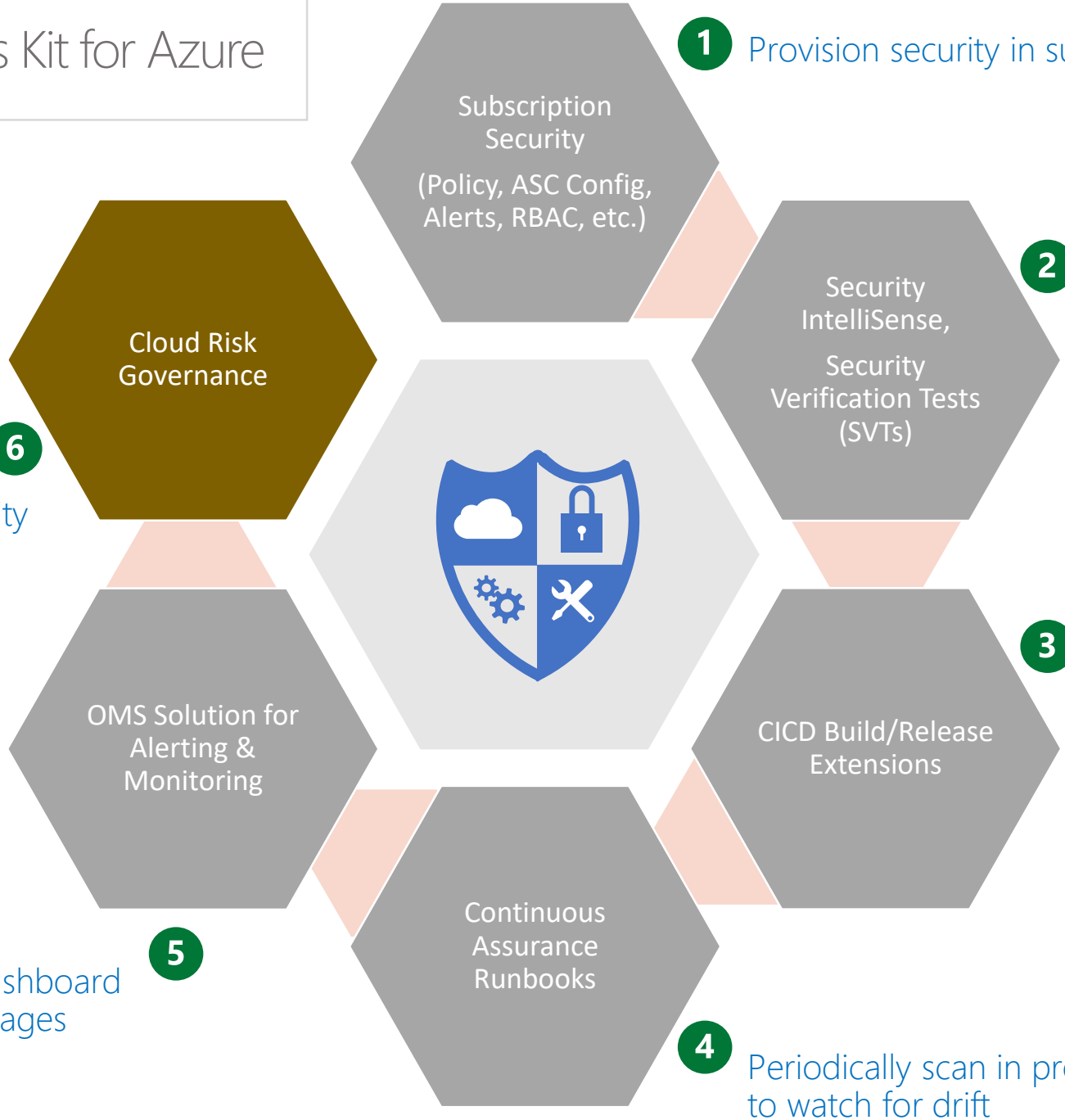
To Sudhindranath Byna

If there are problems with how this message is displayed, click here to view it in a web browser.

DESCRIPTION High severity control has failed in the recent scan

Top 10 result(s)	
SourceSystem	RestAPI
TimeGenerated	6/14/2017 2:31:14 PM
ActualVerificationResult_s	Failed
ControlSeverity_s	High
ResourceType	Microsoft.Storage/storageAccounts
ResourceGroup	AzSDK-Demo-RG
Reference_s	aka.ms/azsdkosstcp/storage
ResourceName_s	azsdkdemosaf07a8f9e
ControlStatus_s	Failed
ControlId_s	Azure_Storage_DP_Encrypt_At_Rest_Blob
SubscriptionName_s	MSFT-Security Reference Architecture-04
FeatureName_s	Storage
Source_s	CC
Recommendation_s	Run command 'Set-AzureRmStorageAccount -Name '<StorageAccountName>' -ResourceGroupName '<RGName>' -EnableEncryptionService 'Blob''. Run 'Get-Help Set-AzureRmStorageAccount -full' for more help.
SubscriptionId	254ad434-e2e6-45c0-a32b-34bf24cb7479
id	b4b9019e-874e-d316-3e81-8beac3ae8c32
Type	AzSDK_CL
MG	00000000-0000-0000-0000-000000000000

Secure DevOps Kit for Azure



1 Provision security in subscription

2 Develop securely, spot check security via scripts

3 Deploy securely from VSO build/release pipeline

4 Periodically scan in production to watch for drift

5 Single security dashboard across DevOps stages

6 Make data-driven improvements to security

Org

- Select All
- C… eering
- C… Engineering
- D… Risk Engineeri…
- Er… gineering
- Er… ure Services
- H…
- M…
- M…
- M…
- M…
- O…
- Sa…
- St… ering

Service Group

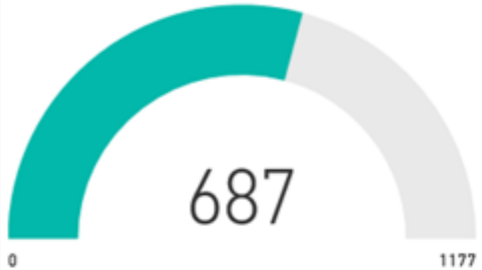
- Se…
- Bl…
- Ci…
- Cl…
- C… ement…
- C… l Affairs
- D…
- EA…
- EC…
- Er…
- Er… Social…

Service

- Select All
- Ac…
- An… igement
- An…
- An… gement
- Ap…

Subscriptions Scanned

Compliant Subscriptions

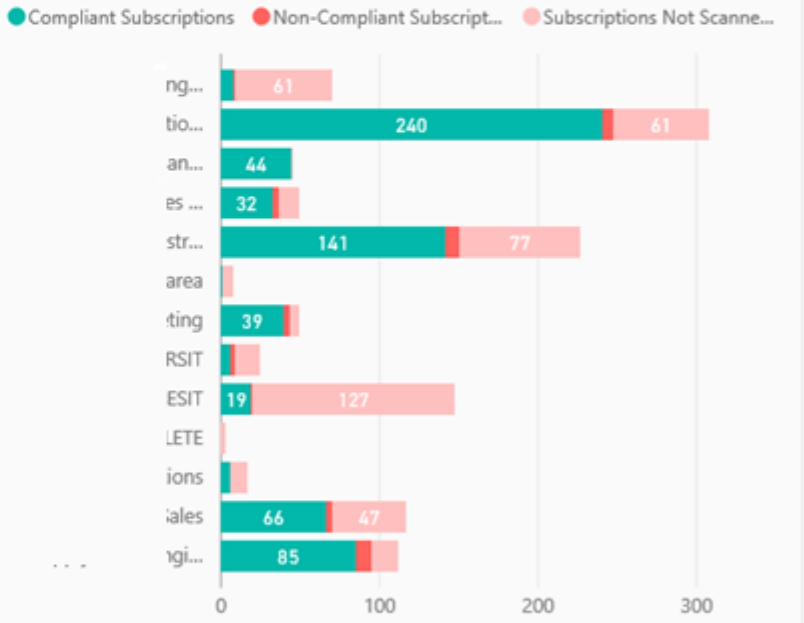


Subscription Security Controls

Drive

- Select All
- Wave 1
- Wave 2

Org View - Subscription Security



Subscription List - Subscription Security

Subscription…	Subscri…	IsSubSc…	IsSubCompliant	Alerts	ARM	ASC	CentralA…
D…	00 4…	Yes	Yes	Yes	Yes	Yes	Yes
C…	00 5…	Yes	Yes	Yes	Yes	Yes	Yes
M…	01 '3…	Yes	Yes	Yes	Yes	Yes	Yes
Sl…	01 9…	Yes	No	Yes	No	Yes	Yes
A…	01 8…	Yes	Yes	Yes	Yes	Yes	Yes
In…	01 i0…	Yes	Yes	Yes	Yes	Yes	Yes
M…	02 6…	Yes	Yes	Yes	Yes	Yes	Yes
A…	02 1…	Yes	Yes	Yes	Yes	Yes	Yes
M…	02 4…	Yes	Yes	Yes	Yes	Yes	Yes
M…	02 8…	Yes	Yes	Yes	Yes	Yes	Yes
M…	04 9…	Yes	Yes	Yes	Yes	Yes	Yes
N…	04 IF…	Yes	Yes	Yes	Yes	Yes	Yes
N…	04 :1…	Yes	Yes	Yes	Yes	Yes	Yes
O…	04 1…	Yes	Yes	Yes	Yes	Yes	Yes
G…	04 i8…	Yes	Yes	Yes	Yes	Yes	Yes
Pi…	05 A…	Yes	Yes	Yes	Yes	Yes	Yes
M…	05 '7…	Yes	Yes	Yes	Yes	Yes	Yes
C…	05 E…	Yes	Yes	Yes	Yes	Yes	Yes
Ei…	05 :5…	Yes	Yes	Yes	Yes	Yes	Yes
M…	05)B…	Yes	Yes	Yes	Yes	Yes	Yes
M…	05 :2…	Yes	Yes	Yes	Yes	Yes	Yes

NOTE: This SS status tab represents whether the security configurations of your subscriptions meet the current security baseline being driven for CSE. See the **Resource Security** tab to view the security state of resources in the subscription.
IsSubCompliant represents the cumulative status for the subscription controls applicable to the selected drive (Wave 1/Wave 2/etc.,). Individual status columns for Alerts, ARM, ASC, etc., will be removed soon. To determine the individual controls that need fixing, please utilize your OMS workspace.

Last Refresh (UTC)
2017-Aug-17 09:16

Next Refresh (UTC)
2017-Aug-17 12:16

Filters

Org

- Select All
- Cc ing
- Cc gineering
- Di c Engineeri...
- Er ieering
- Er e Services
- He
- M
- M
- M
- M
- Oj
- Sa
- Su ng

Service Group

- Select All
- BI
- Ca
- CI
- Cc gement...
- Cc gal Affairs
- De

Service

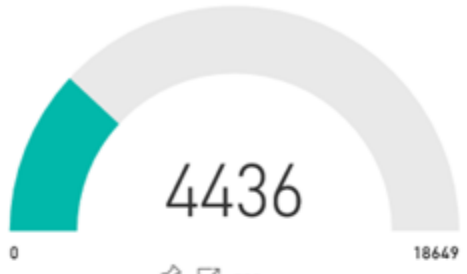
- Select All
- Ac
- Ar jement
- Ar
- Ar ement

Subscription Name

- Select All
- Al tion
- Ac
- Al ERVICE
- Al ROD
- Al

Resources Scanned

Compliant Resources



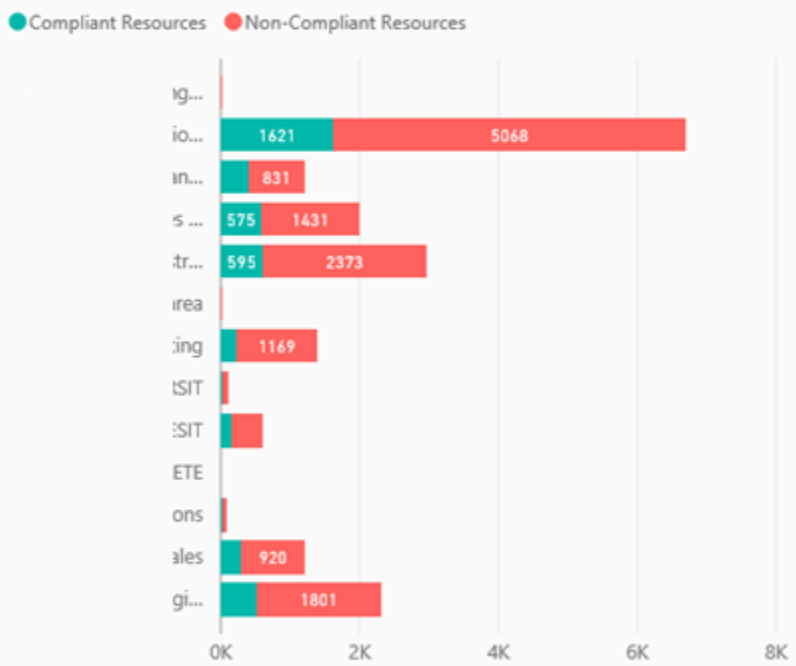
Drive

- Select All
- Wave 2

Top Failing Features

Feature	NonCompli...	CompliantR...
VirtualMachine	4352	37
Storage	4150	2819
AppService	3486	444
SQLDatabase	2203	1123
CloudService	22	13

Org View - Resource Security



Subscription List - Resource Security

SubscriptionName	Subscri...	CompliantRes...	NonCompliantRe...	OrgName	ServiceGroup
MS	58 55..	6	295	En ...	Nc ed
MS	D' 45..	23	244	Cc ...	Fir
MS	E6)D..	48	237	M ...	Sh t...
MS	4F 03..	3	230	En ...	En ...
PG	9E 50..	6	199	En ...	En ...
Cle	0C 35..	4	198	En ...	Nc ed
Cle	59 9F..	19	185	M ...	Cc ...
MS	4A 9F..	38	181	Cc ...	Hu s...
SEA	2C 40..	17	162	En ...	Nc ed
MS	BC CB..	5	160	Su ...	Sh ...
Pat	AI 22..	4	156	Cc ...	Hu s...
MS	21 5B..	11	154	Cc ...	Fir
MS	55 B7..	17	152	En ...	En ...
MS	17 10..	13	139	M ...	Mi ...
ME	1A D..	10	132	Su ...	Mi a...
MS	B5 99..	130	123	Cc ...	Fir
MS	3A F8..	5	122	Su ...	Mi a...
MS	8C C0..	16	122	Cc ...	Hu s...
MS	A(40..	5	120	En ...	En ...
MS	F7 F9..	6	120	Cc ...	Hu s...
MS	7F 07..	2	119	Su ...	OI ...
MS	BC 55..	1	118	Su ...	De ...

NOTE: This RS status tab represents whether the security configurations of your resources meet the current security baseline being driven for CSE.

Cumulative numbers by resource type are shown here. To determine the individual controls that need fixing, please utilize your OMS workspace.

Last Refresh (UTC)
2017-Aug-17 09:16

Next Refresh (UTC)
2017-Aug-17 12:16

Filters

Timeframe

- Select All
- 30 days (Last)
- 30+ to 60 days
- 60+ to 90 days
- 90+ days

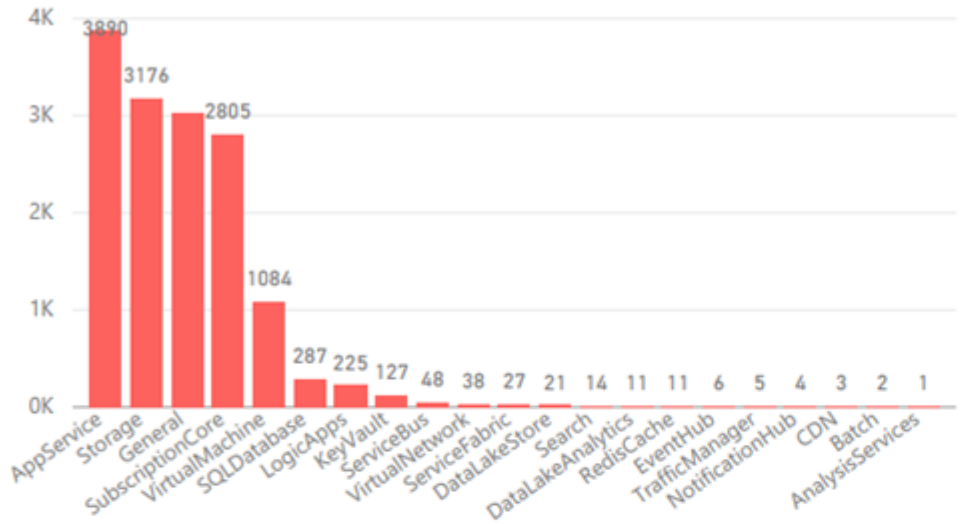
Feature filter

- Select All
- AnalysisServices
- AppService
- Batch
- CDN
- DataFactory
- DataLakeAnalyti...
- DataLakeStore
- ERvNet
- EventHub
- General
- KeyVault
- LogicApps
- NotificationHub
- ODG

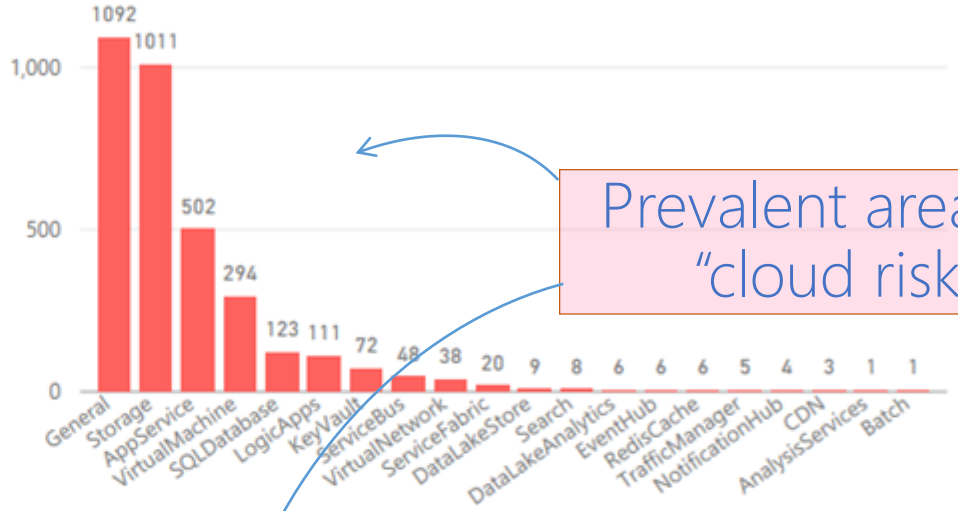
Severity

- Select All
- Critical
- High
- Information
- Low
- Medium

Failed Controls by Resource Type



Unhealthy Resources by Resource Type



Prevalent areas of "cloud risk"

DevOps Stage

- Select All
- Ad hoc
- CICD
- Cont. Assurance

Data Classification

- Select All
- Unknown

Org

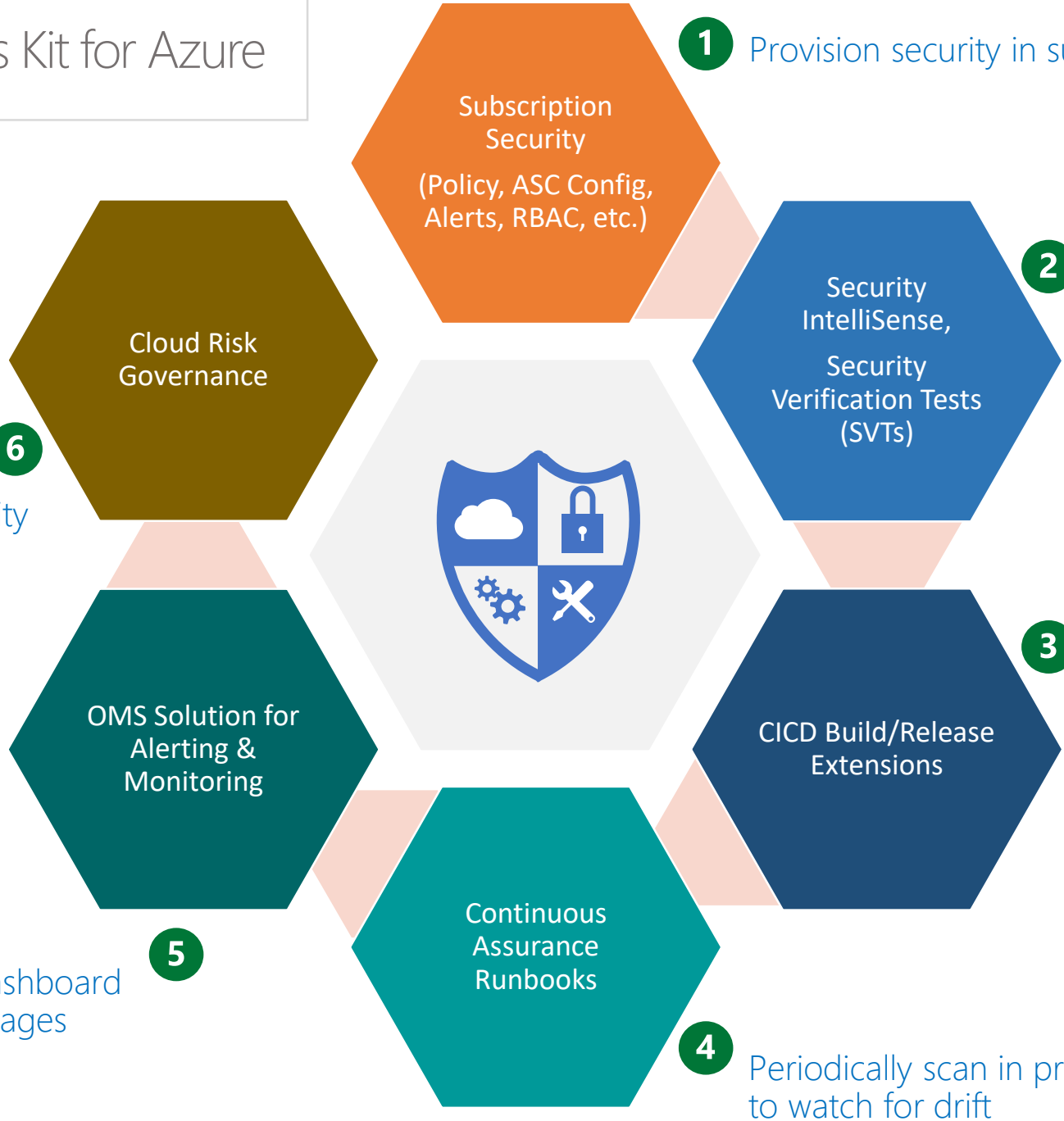
- Sel
- EIS
- FIF
- ISF
- MS
- MS
- Sal
- SE
- UE
- Un
- US

Scan Trend

Failed Controls Count

ControlStringId	Count of Result
Azure_Storage_Audit_Issue_Alert_AuthN_Req	1160
Azure_Storage_DP_Encrypt_at_Rest_Blob	864
Azure_Storage_Deploy_Use_Geo_Redundant	828
Azure_Storage_Audit_Config_Log_AuthN_Req	739
Azure_AppService_BCDR_Use_App_Backup	611
Azure_AppService_Audit_Enable_Logging_and_Monitoring	532
Azure_AppService_BCDR_Use_multiple_instances	520
Azure_AppService_Deploy_Use_64_bit	458
Azure_AppService_DP_Encrypt_in_Transit	408
Azure_Subscription_Audit_Resolve_Azure_Security_Center_Recommen...	390
Azure_Subscription_Audit_Configure_Critical_Alerts	387
Azure_Storage_Audit_AuthN_Requests	385
Azure_Subscription_Config_ARM_Policy	385

Secure DevOps Kit for Azure



1. Provision security in subscription
2. Develop securely, spot check security via scripts
3. Deploy securely from VSO build/release pipeline
4. Periodically scan in production to watch for drift
5. Single security dashboard across DevOps stages
6. Make data-driven improvements to security

Secure DevOps Kit – Impact at Microsoft IT

1000+ subscriptions scanned

35000 Azure resources secured

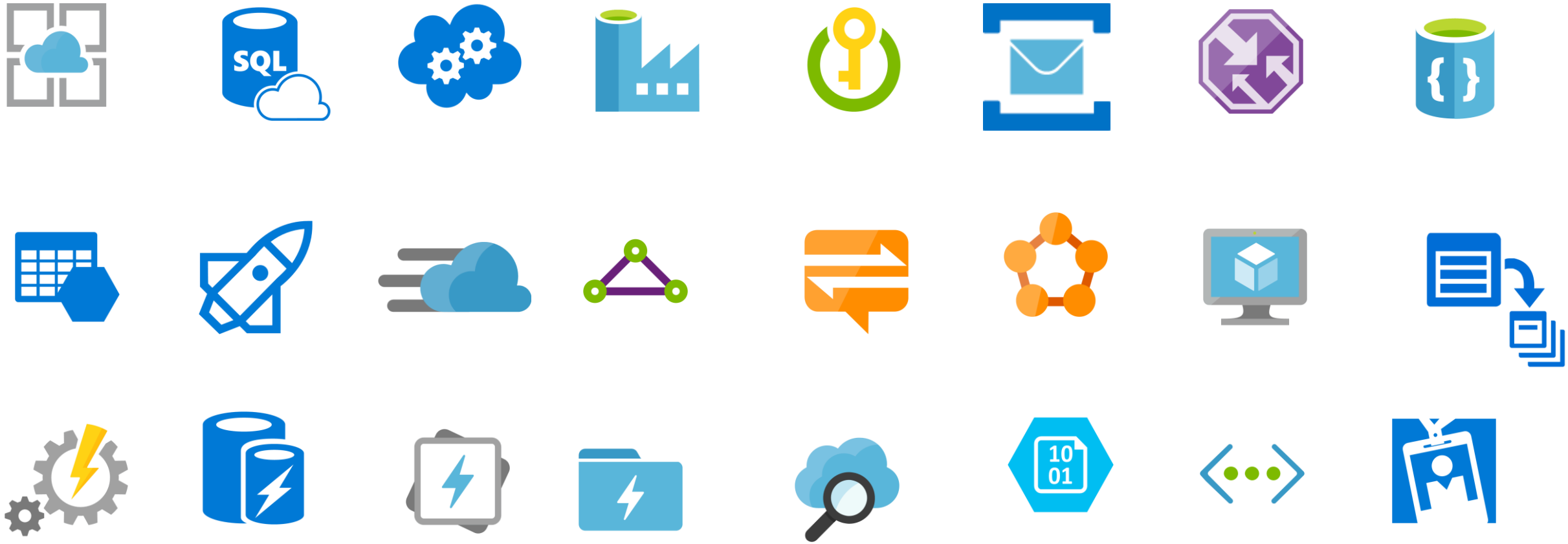
50+ enterprise LOB app SDLs across IT

25 million+ controls scanned till date

200k+ hours of manual effort saved

250+ security controls across 30 Azure PaaS/IaaS service types

Coverage of Azure Services in the DevOps Kit



Learnings from our DevOps Kit experience

Predominant motivation is *still* to seek 'Security sign-off'

Need to invest more in awareness about ownership of risk

Having 'Dev' and 'Ops' together is *not* 'Dev Ops'

Breaking down 'classic' team silos is going to be critical

Understanding of cloud security model is limited

Need more education/trainings in this area

Systemic gap in PowerShell/scripting expertise

Need to invest in scripting skills (DevOps == "Infrastructure as Code")

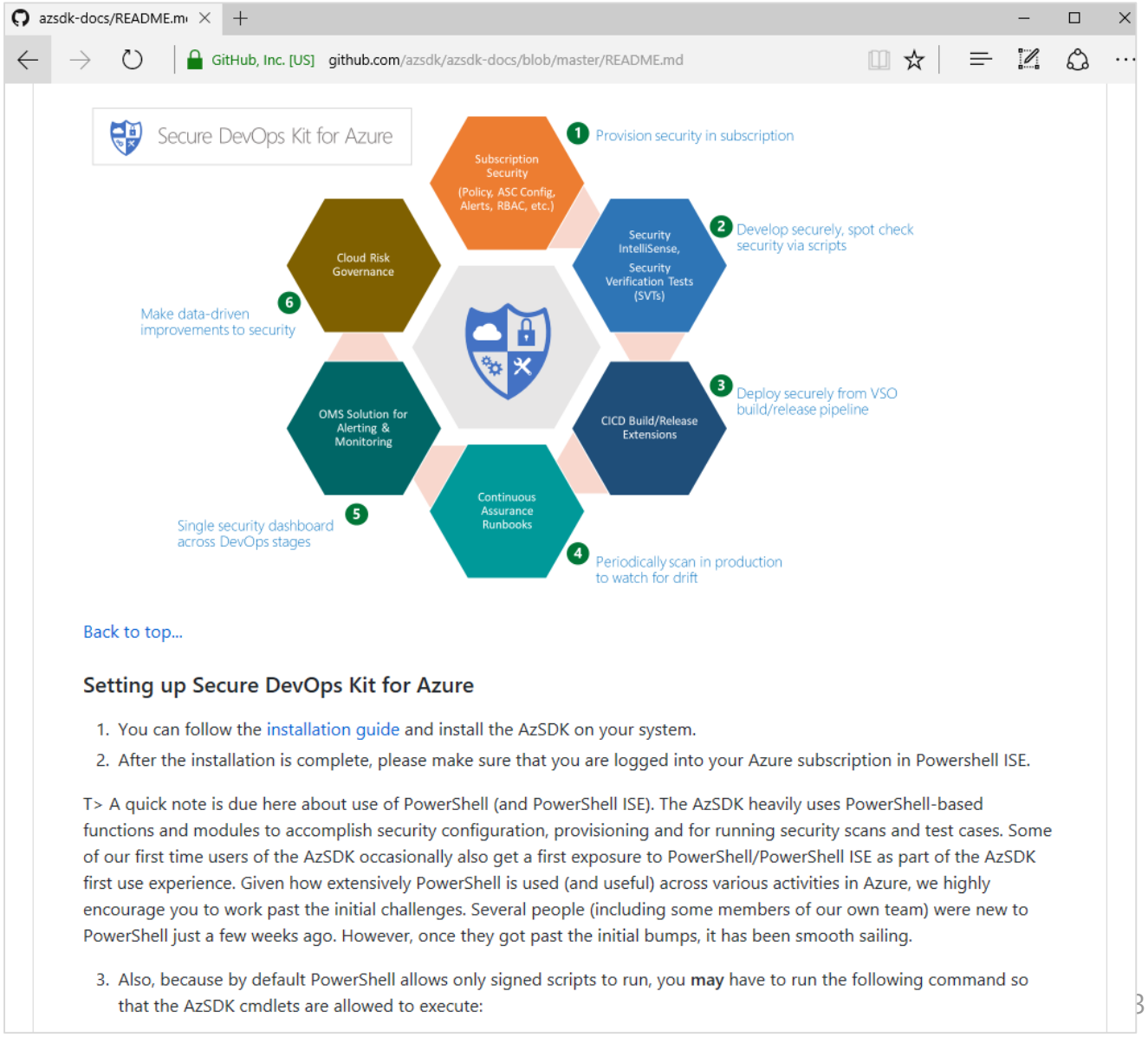
Engage uniformly with all stakeholders

We started with a 'dev heavy' approach, should have taken ops along

Next steps…

Try out the Secure DevOps Kit for Azure!

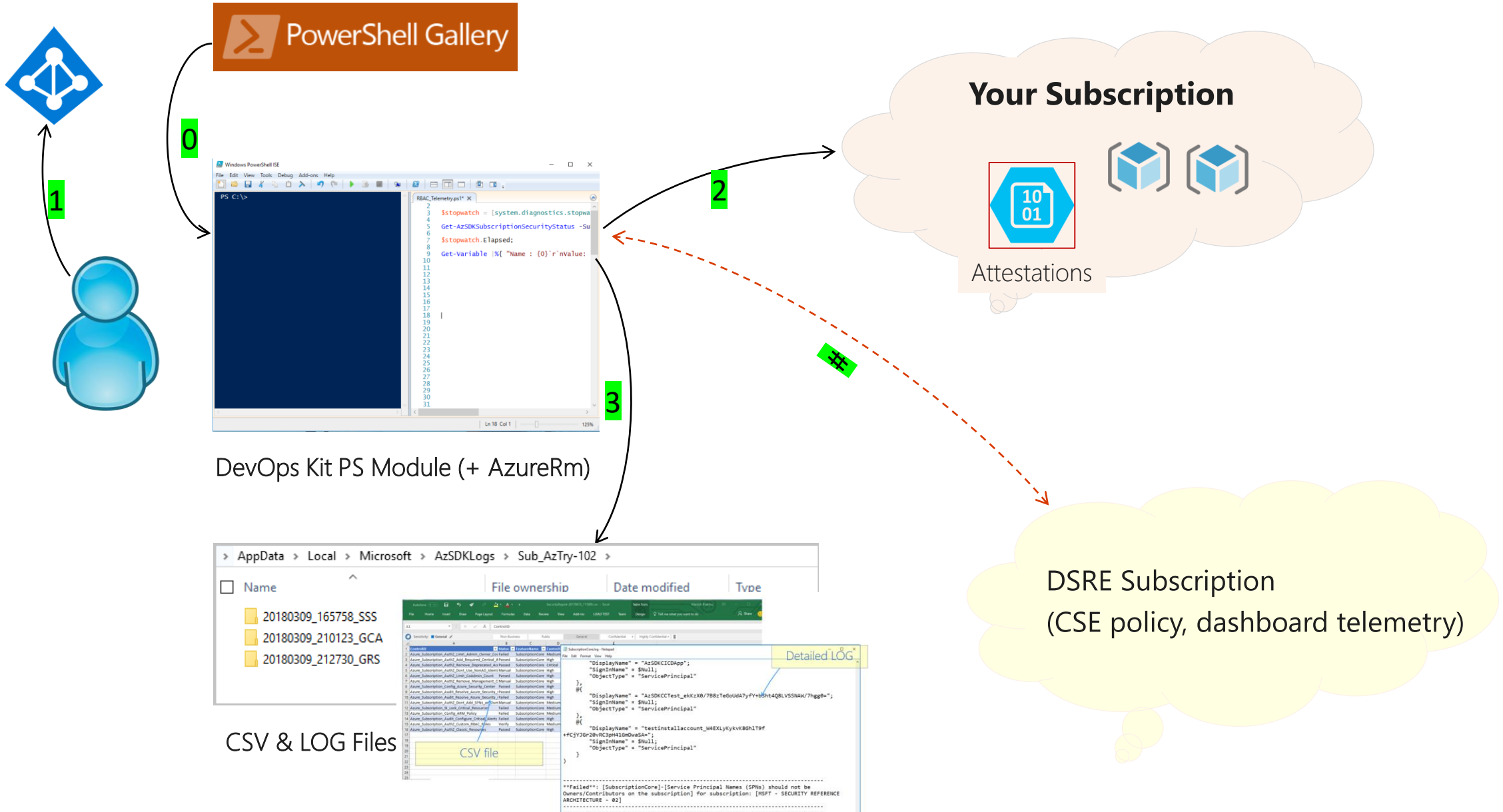
- GitHub src/docs: https://github.com/azsk
- Controls coverage: https://aka.ms/devopskit/tcp
- IT Showcase: https://aka.ms/devopskit/itshowcase
- Support: azsksup@microsoft.com



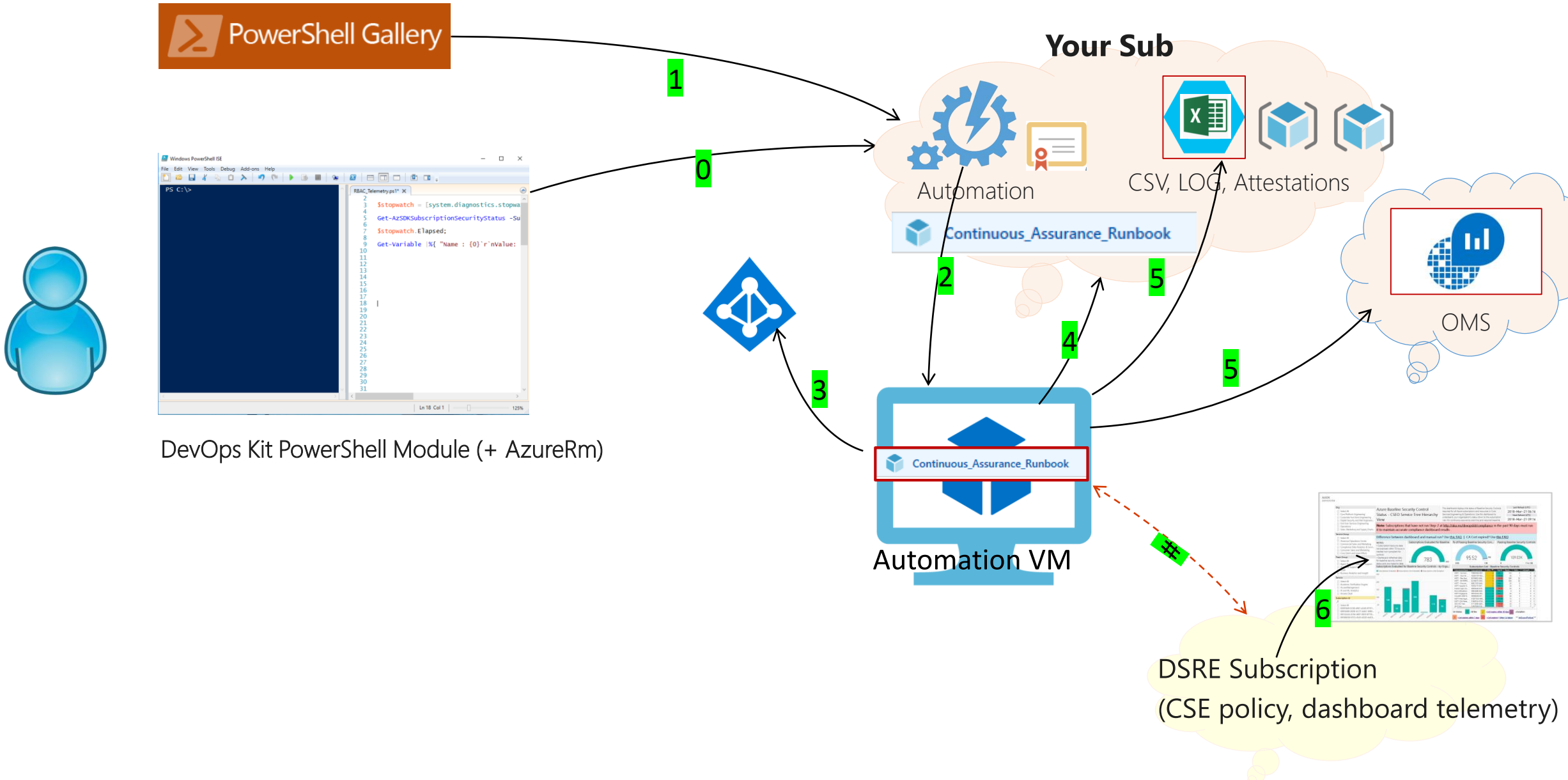
Thanks for attending!

References

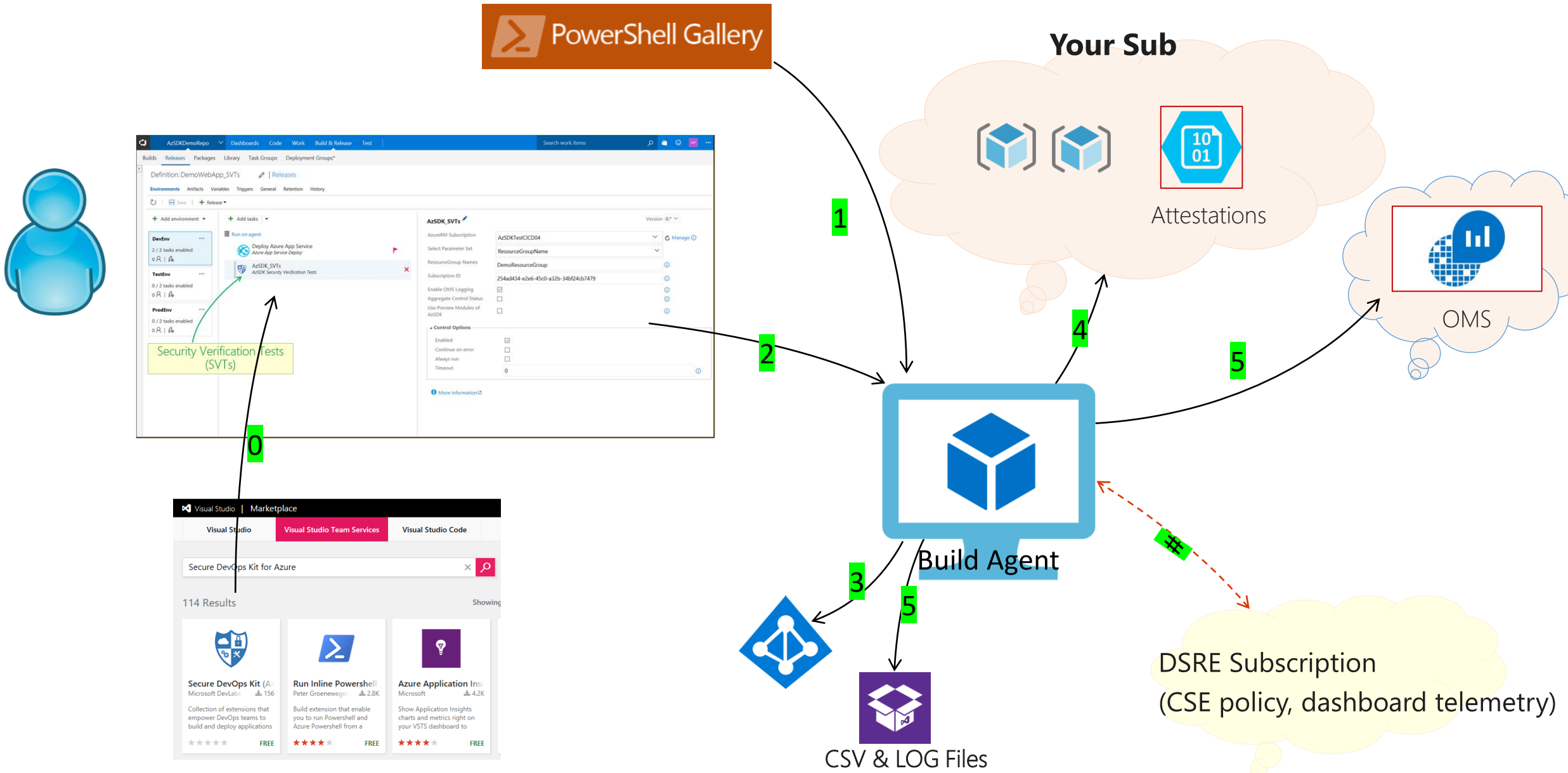
Core use cases – local scan



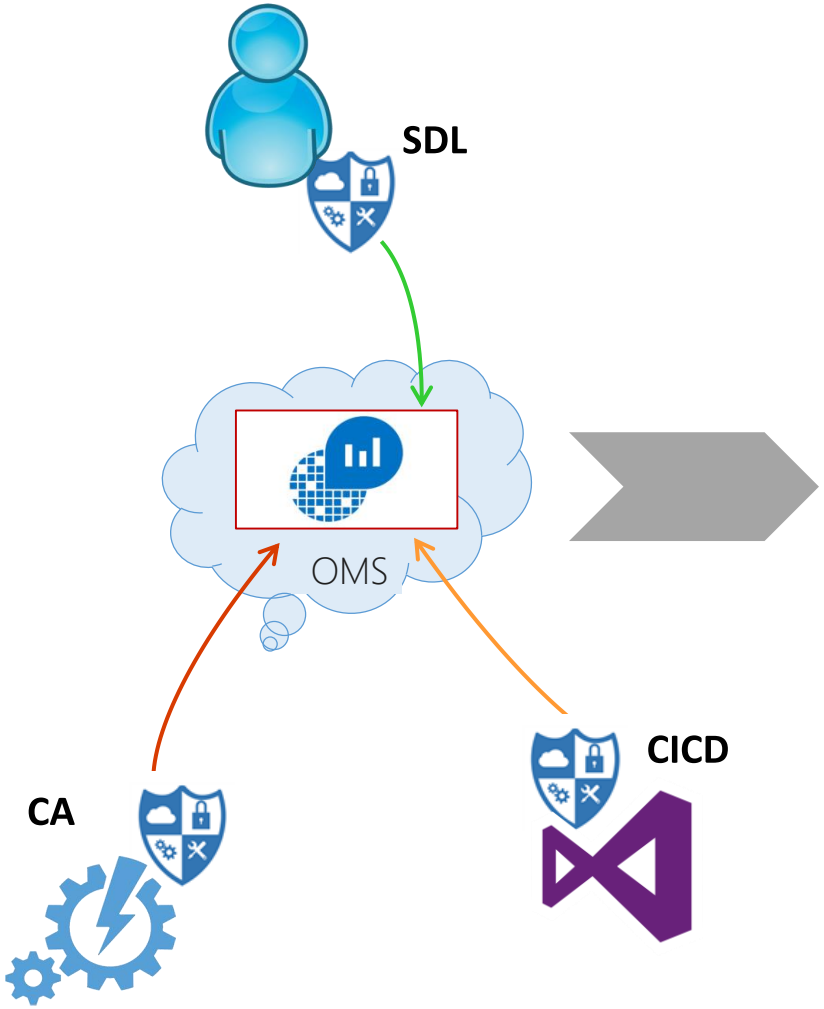
Core use cases – Continuous Assurance

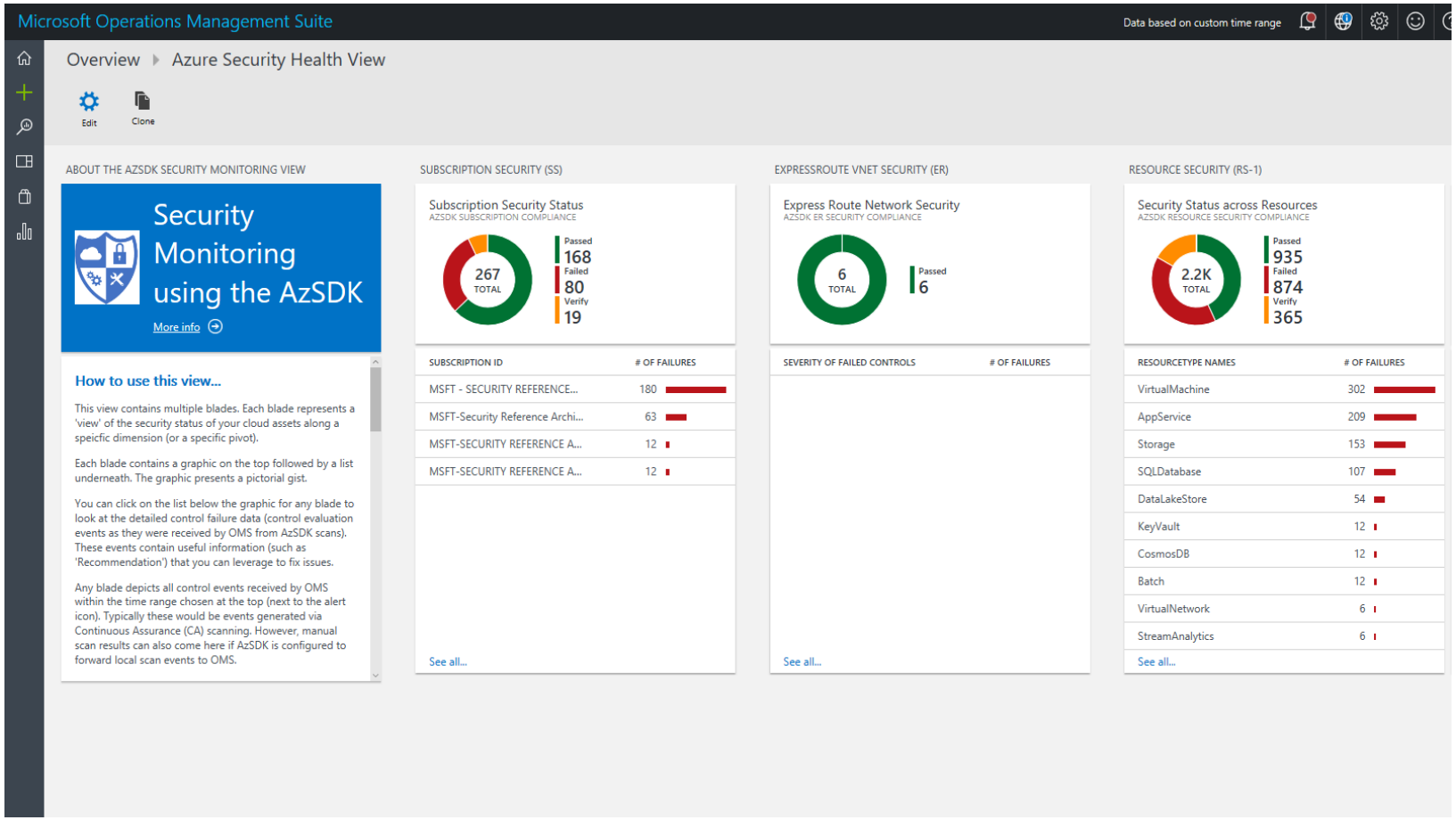


Core use cases – CICD Extension

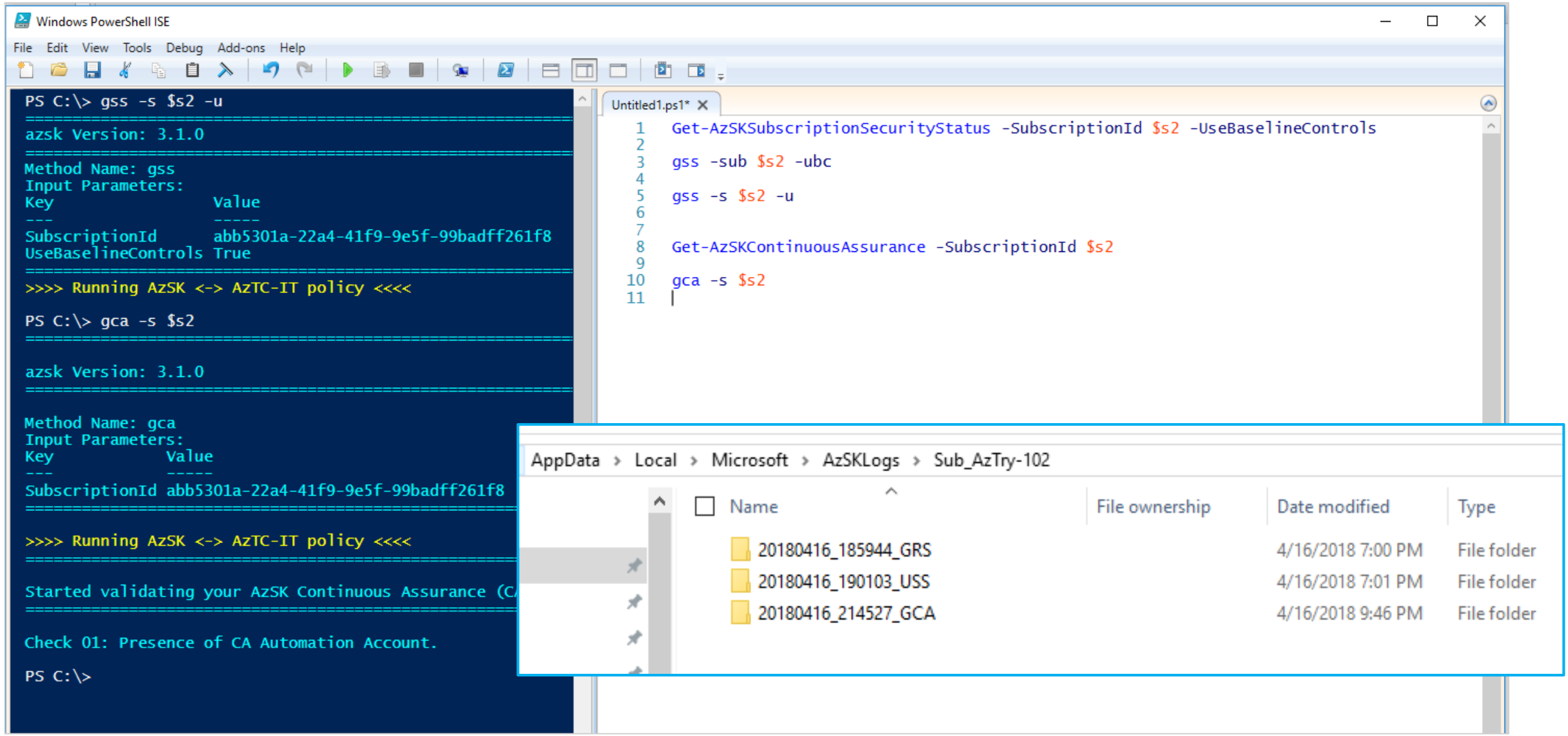


DevOps Kit OMS Solution





AzSK command acronyms



Customizing & extending AzSK

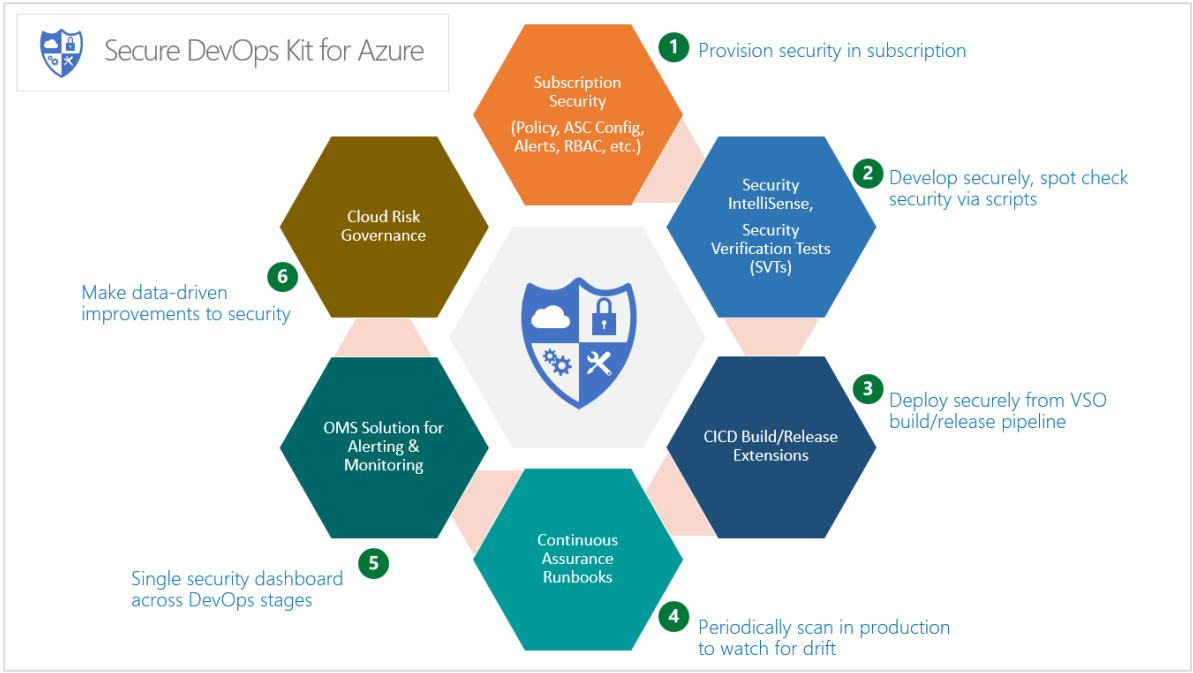
AzSK on a slide

Secure DevOps Kit for Azure (AzSK)

A toolkit for accelerating adoption of Azure at the enterprise by automating cloud resource configuration security for dev ops environments.

Areas of Focus

- ✓ Subscription security (ARM policies, RBAC, Alerts, ASC setup)
- ✓ Secure development (security baseline scans for ~30 Azure services)
- ✓ Security in deployment (AzSK CICD task for VSO)
- ✓ Continuous assurance in Ops (Azure Automation runbooks)
- ✓ Alerting & monitoring (single pane view in OMS across dev ops stages)
- ✓ Cloud risk governance (dashboards based on exhaustive security telemetry)



Key Benefits

- Accelerates cloud dev ops for the enterprise
- Empowers engineering teams to perform consistent cloud security configuration across dev ops stages
- Scale out security expertise through automation
- Facilitates risk governance in the cloud through security telemetry

Partners & Collaboration

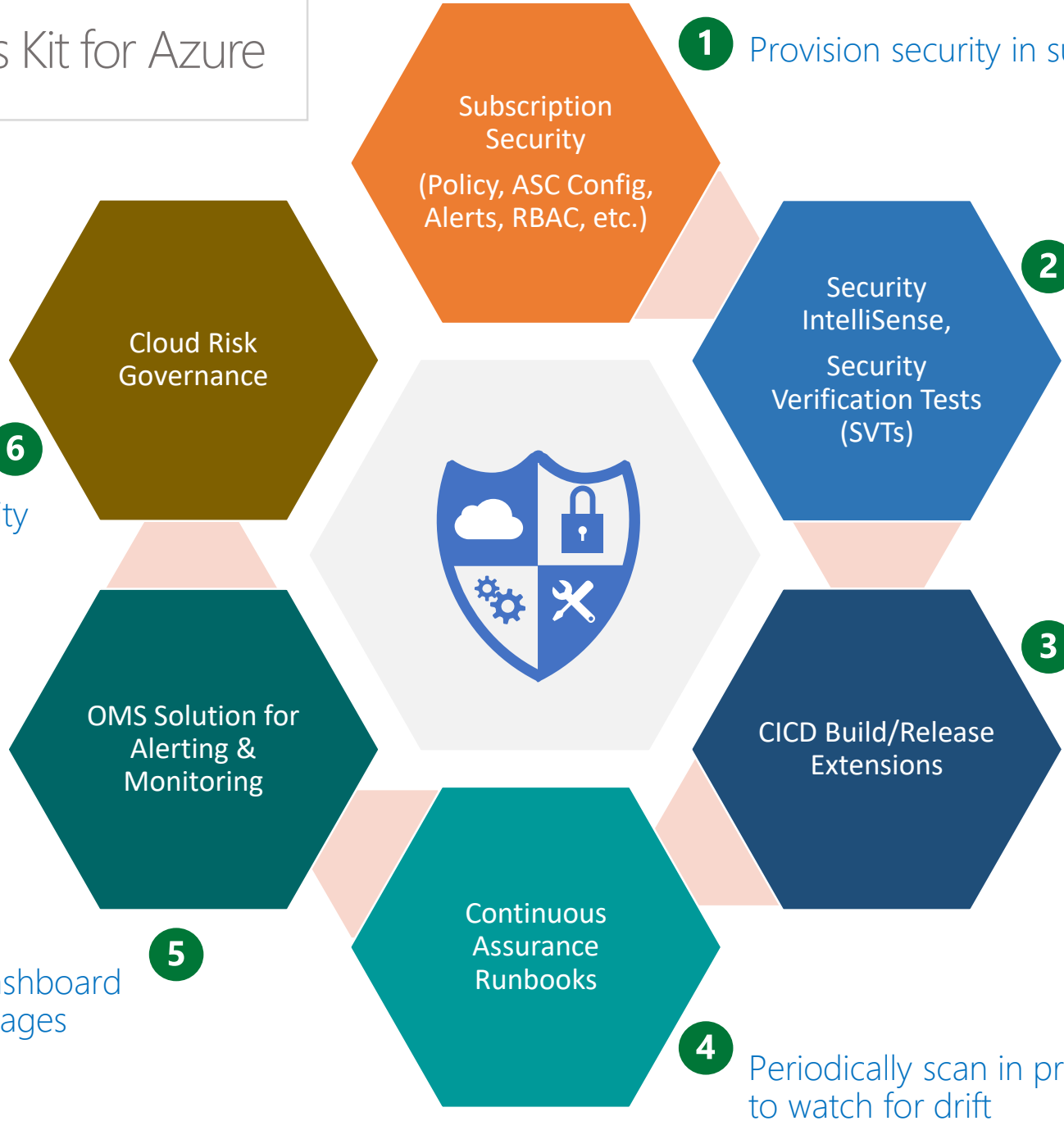
Built with contributions from multiple teams:

- **DSRE**: GRCC, ACE, SAFET, Tools, ISO, etc.
- **CSE**: CloudMS, NIS, E3, App Teams (EDDA, CELA BI, Incentive Comp, etc.)
- **PG**: ASC, OMS, Visual Studio, Key Vault, Azure Automation, etc.
- **Other:** Account Teams, CAT, GD, etc.

Showcase to Customers/Conferences

- Showcased to key enterprise customers (GEICO, Symantec, TCS, Infosys, DELL, Shell)
- Used by Global Delivery (GD) for their envt
- Presented at Inspire, RSA and Ready conferences, internal engineering forums.
- IT Showcase: Secure DevOps for Azure
- Built end to end on top of Microsoft Azure

Secure DevOps Kit for Azure



1. Provision security in subscription
2. Develop securely, spot check security via scripts
3. Deploy securely from VSO build/release pipeline
4. Periodically scan in production to watch for drift
5. Single security dashboard across DevOps stages
6. Make data-driven improvements to security

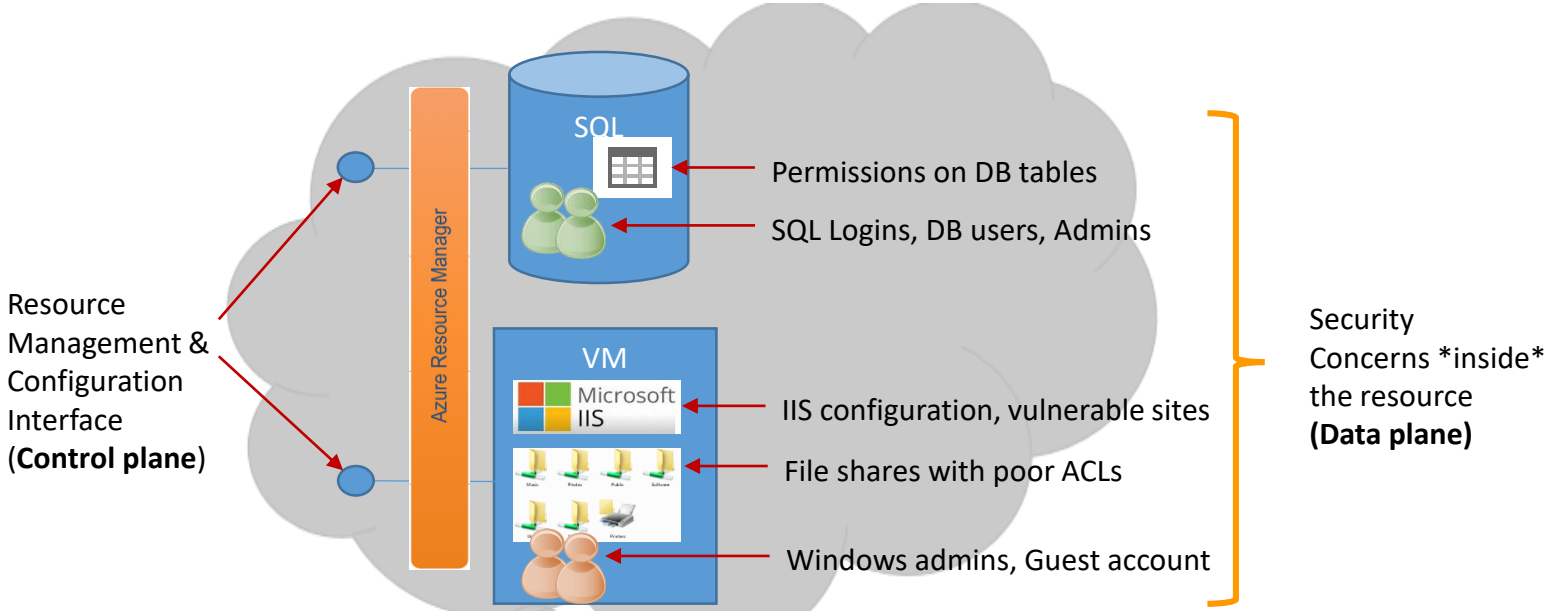
AzSK – what it covers v. does not cover

What it covers:

- Control plane (cloud resource configuration) security
- Drive uniform compliance for subscription and resources for cloud apps across all stages of dev ops
- Works in a decentralized manner
- Enable dev ops teams to do security monitoring of their own apps
- Visibility of security baseline state across the enterprise via extensive telemetry

What it does not cover:

- Data plane configuration checks (AzSK is not 'agent-based')
- v1/ASM resources (except Cloud Service). These are deprecated for use at CSE.
- SaaS/O365 security
- Replace SAST/DAST tools (these should carry over from on-prem solutions)
- Network layer things like DLP, IDS, FW, etc.
- Not all Azure services are covered (only top used ones)



Using AzSK at your organization

Level-0: Trying out the AzSK 'out-of-box' from aka.ms/devopskit/docs

Level-1: Setup 'org-specific' instance of AzSK

- Simple settings/config changes
- Pretty much mimic what we have at CSE

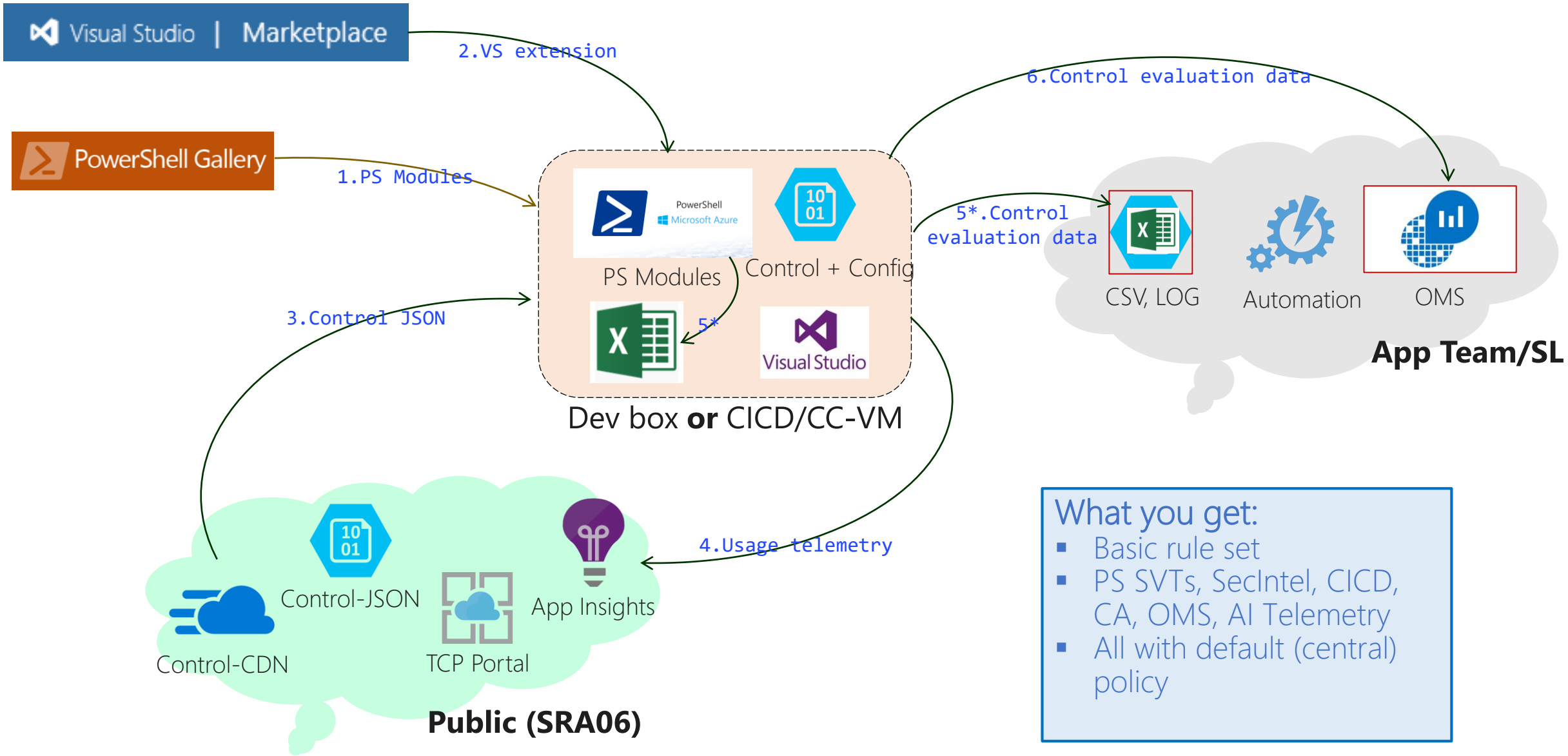
Level-2: Customizing AzSK for your environment

- Leverage integration points for other listeners, custom tags, telemetry, etc.

Level-3:

- Maintaining your own version (branch) of AzSK (e.g., cost optimization, inventory)

L0: AzSK dataflow ('preview'/'trial' use)



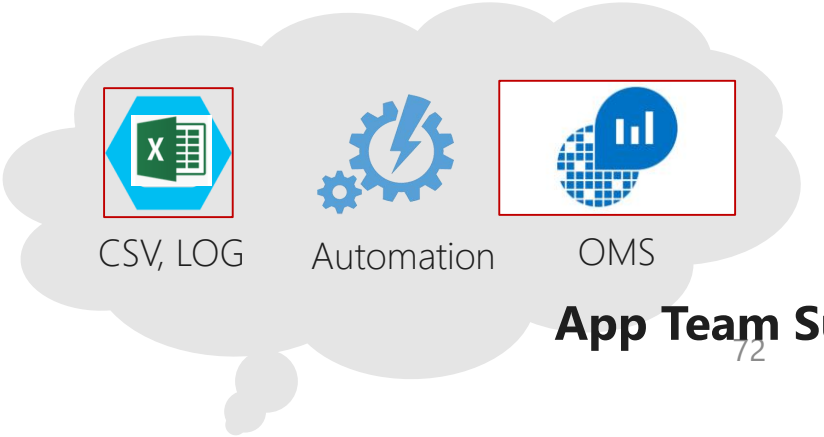
What you get:

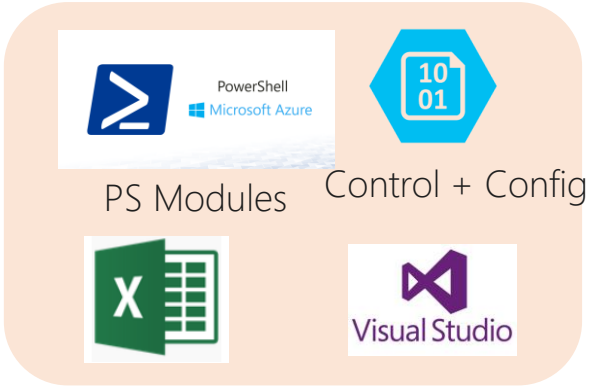
- Basic rule set
- PS SVTs, SecIntel, CICD, CA, OMS, AI Telemetry
- All with default (central) policy

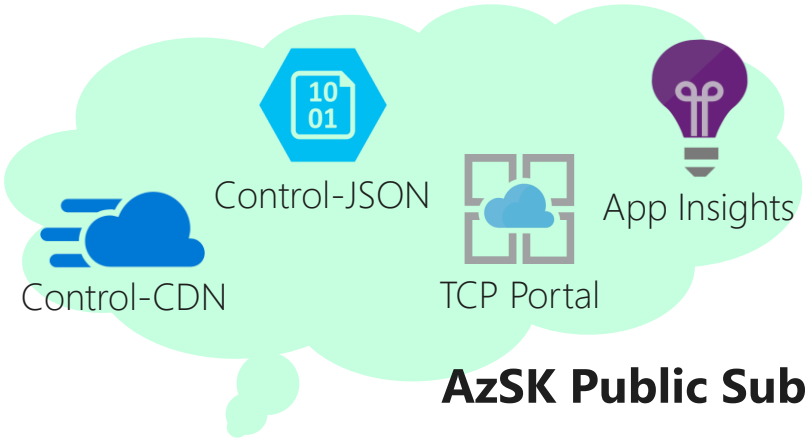
L1: AzSK – CDN v/s 'Org-specific' instance

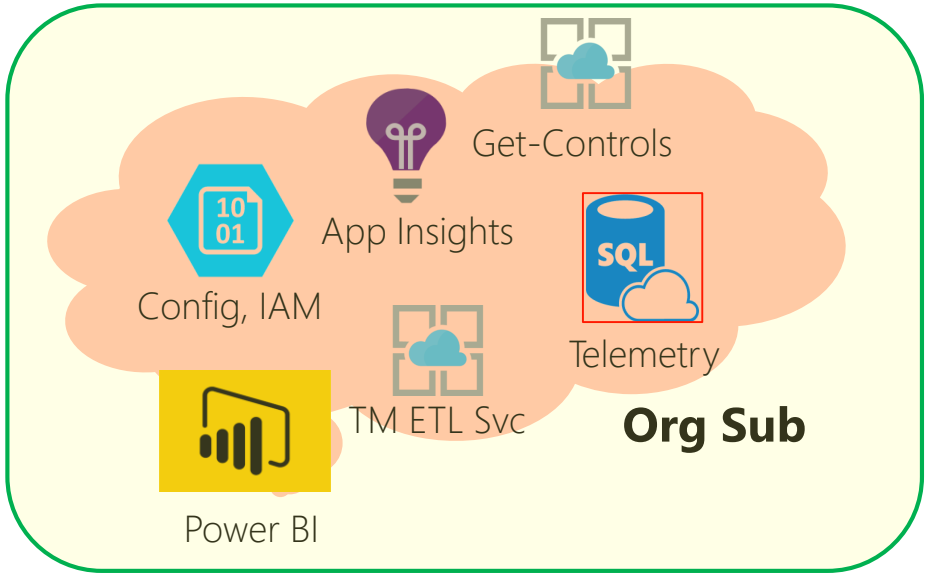
Visual Studio | Marketplace

PowerShell Gallery









Configurability & Extensibility

Configurability:

Org-specific settings (e.g., 5 admins, RBAC values, etc.)
Control settings (e.g., descriptions, severity, filters, etc.)
Custom report types (e.g., SOX, DR, etc.)
Other workflows (e.g., attestation expiry period)


```
{
  "Diagnostics_RetentionPeriod_Min": 365,
  "Diagnostics_RetentionPeriod_Forever": 0,
  "KeyVault": {
    "KeyRotationDuration_Days": 365,
    "SecretRotationDuration_Days": 180,
    "KeyType": "RSA-HSM",
    "ADAppCredentialTypeCrt": "AsymmetricX509Cert",
    "ADAppCredentialTypePwd": "Password"
  },
  "SqlServer": {
    "AuditRetentionPeriod_Days": 365
  },
  "AnalysisService": {
    "Max_Admin_Count": 2
  },
  "VirtualMachine": {
    "RDP_Port": 3389,
    "WinRM_Port": 5985
  },
  "NoOfApprovedAdmins": 5,
  "NoOfClassicAdminsLimit": 2,
  "WhitelistedMgmtCerts": ...,
  "UniversalIPRange": "0.0.0.0-255.255.255.255",
  "IPRangeStartIP": "0.0.0.0",
  "IPRangeEndIP": "255.255.255.255",
  "MetricAlert": ...,
  "StorageKindMapping": ...,
  "AppService": {
    "Backup_RetentionPeriod_Min": 365,
    "Backup_RetentionPeriod_Forever": 0,
    "LatestDotNetFrameworkVersionNumber": "v4.0",
    "Minimum_Instance_Count": 2,
    "AADAuthAPIVersion": "2016-08-01",
    "LoadCertAppSettings": "WEBSITE_LOAD_CERTIFICATES"
  },
  "StorageDiagnosticsSkuMapping": ...,
  "StorageGeoRedundantSku": ...,
  "RedisCache": ...
}
```

Configurability & Extensibility

Configurability:

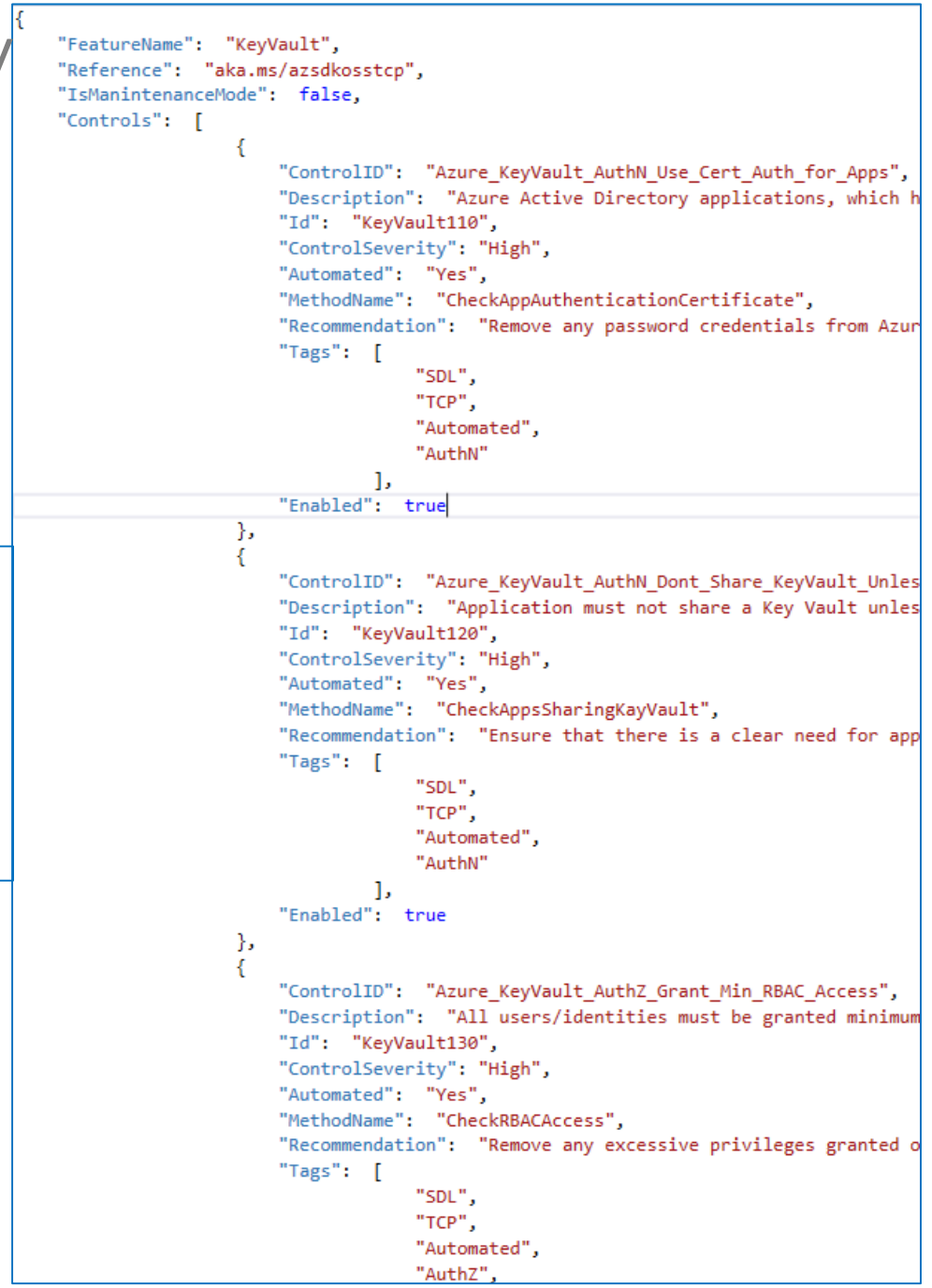
Org-specific settings (e.g., 5 admins, RBAC values, etc.)
Control settings (e.g., descriptions, severity, filters, etc.)
Custom report types (e.g., SOX, DR, etc.)
Other workflows (e.g., attestation expiry period)

Extensibility – Core Framework

Entirely new SVTs (e.g., new cloud service types)

New control for existing SVTs (e.g., org-specific policy)

CICD tasks for other engines



SecurityReport.pdf - Adobe Acrobat Reader DC

File Edit View Window Help

Home Tools SecurityReport.pdf Sign In

1 / 27

PDF format report

Secure DevOps Kit for Azure (AzSDK)

Security Report

Subscription Name	MSDN-mprabhu-msft
SubscriptionId	6bc7464b-1dc0-4141-b32f-57cf4abccaed
AzSDK Version	2.4.8
Generated by	AzSDK
Generated on	July 31, 2017 17:45 (UTC)
Requested by	mprabhu11@live.com (User)
Command Executed	Get-AzSDKSubscriptionSecurityStatus -SubscriptionId '6bc7464b-1dc0-4141-b32f-57cf4abccaed' -GeneratePDF Portrait
Documentation	http://aka.ms/azsdkdocs
FAQ	http://aka.ms/azsdkdocs/faq
Support DL	mailto:isrmazsdksup@microsoft.com

Export PDF

Create PDF

Edit PDF

Comment

Combine Files

Organize Pages

Fill & Sign

Send for Signature

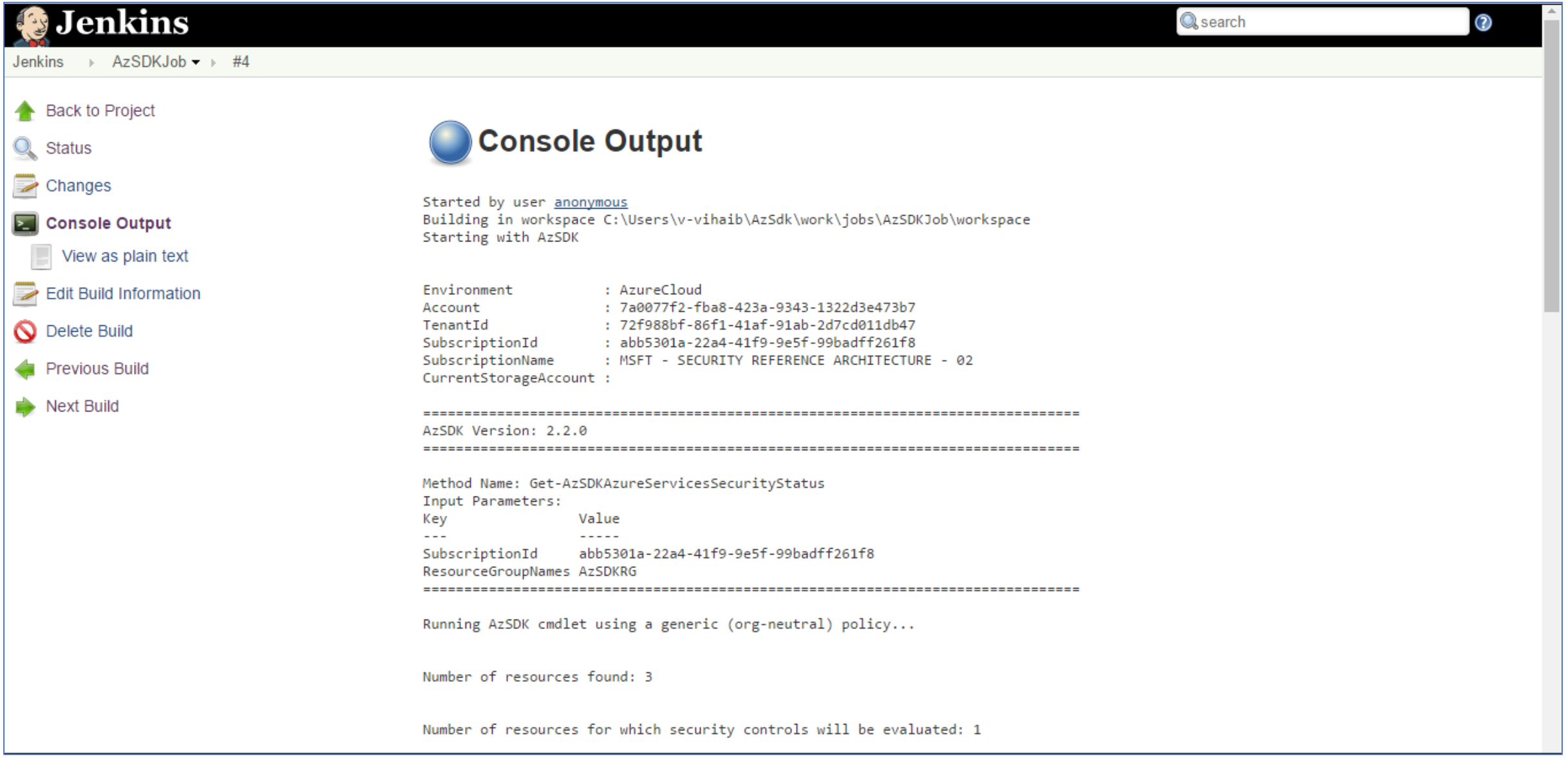
Send & Track

More Tools

Store and share files in the Document Cloud

Learn More

Security tests in CICD pipeline - Jenkins



Configurability & Extensibility

Configurability:

Org-specific settings (e.g., 5 admins, RBAC values, etc.)
Control settings (e.g., descriptions, severity, filters, etc.)
Custom report types (e.g., SOX, DR, etc.)
Other workflows (e.g., attestation expiry period)

Extensibility – Core Framework

Entirely new SVTs (e.g., new cloud service types)

New control for existing SVTs (e.g., org-specific policy)

CICD tasks for other engines

SecIntel rule templates

Extensibility – Downstream Integration

Event Hub

OMS

Webhook (e.g., Splunk)

Easy to extend SVT framework

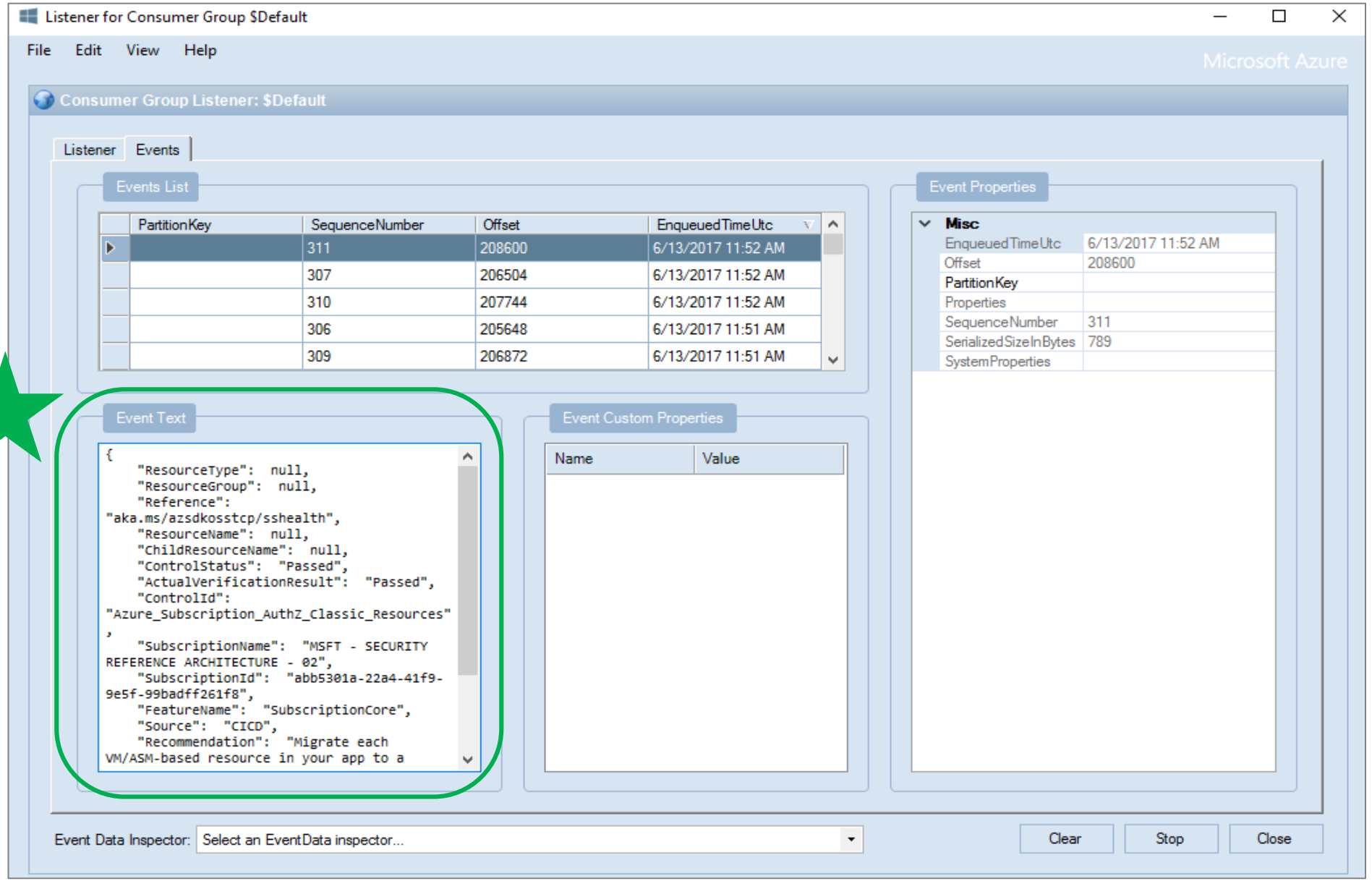
Downstream extensibility - connectors

```
$SubscriptionId = "abb5301a-xxxx-xxxx-9e5f-99baxxxx61f8"
#$SubscriptionId = (Get-AzureRmContext).Subscription.Id

Set-AzSDKEventHubSettings `
    -EventHubNameSpace "eventhub-common-01" `
    -EventHubName "common-eventhub" `
    -EventHubSendKeyName "ehSend" `
    -EventHubSendKey "VSQqIritI1fOVXXXXXXXXXXXXXXyufkq9WnKPSk8="


#Set-AzSDKEventHubSettings -Disable


Set-AzSDKWebhookSettings `
    -webHookurl $webHookUrl `
    -authZHeaderName $authZHeaderName `
    -authZHeaderValue $authZHeaderValue

Set-AzSDKWebhookSettings `
    -WebhookUrl $webhookUrl

#Set-AzSDKWebhookSettings -Disable

Get-AzSDKSubscriptionSecurityStatus -SubscriptionId $SubscriptionId
```

Event Hub

Webhook

Control results in EventHub



Controls results in Splunk (*via* Webhook)

Search | Splunk 6.6.0

splunk> Search & Reporting

New Search

source="http:azsdk_test"

Month to date

108 events (6/1/17 12:00:00.000 AM to 6/21/17 12:13:14.000 PM) No Event Sampling

Events (108) Patterns Statistics Visualization

Format Timeline — Zoom Out + Zoom to Selection × Deselect 1 day per column

List Format 20 Per Page

Prev 1 2 3 4 5 6 Next

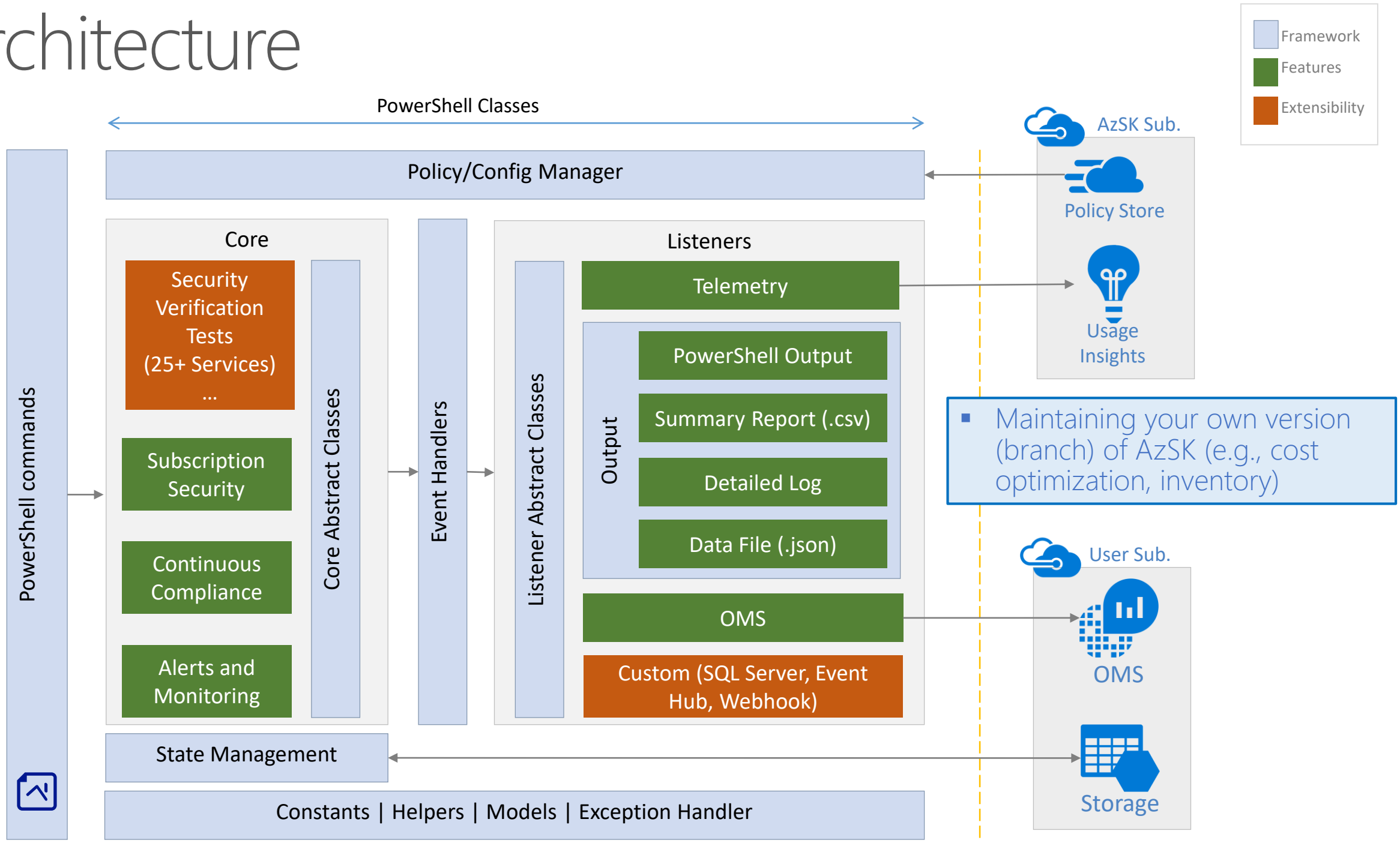
Hide Fields All Fields

Selected Fields
a host 1
a source 1
a sourcetype 1

Interesting Fields
a ActualVerificationResult 4
a AttestationStatus 1
a AttestedBy 1
a ChildResourceName 1
a ControlId 15
a ControlSeverity 3
a ControlStatus 4
a FeatureName 1
a index 1
a Justification 1
linecount 4
a punct 7
a Recommendation 14
a Reference 1

i	Time	Event
>	6/12/17 5:27:14.000 PM	{ "ResourceType": null, "ResourceGroup": null, "Reference": "aka.ms/azsdkosstcp/sshealth", "ResourceName": null, "ChildResourceName": null, "ControlStatus": "Passed", "ActualVerificationResult": "Passed", "ControlId": "Azure_Subscription_AuthZ_Classic_Resources", "SubscriptionName": "MSFT - SECURITY REFERENCE ARCHITECTURE - 02", "SubscriptionId": "abb5301a-22a4-41f9-9e5f-99badff261f8", "FeatureName": "SubscriptionCore", "Source": "CC", "Recommendation": "Migrate each VM/ASM-based resource in your app to a corresponding v2/ARM-based resource.", "ControlSeverity": "High", "TimeTakenInMs": null, "AttestationStatus": null, "AttestedBy": null, "Justification": null } Show syntax highlighted Collapse host = input-prd-p-9ns84q64sq2q.cloud.splunk.com:8088 source = http:AzSDK_Test sourcetype = httpevent
>	6/12/17 5:27:11.000 PM	{ "ResourceType": null, "ResourceGroup": null,

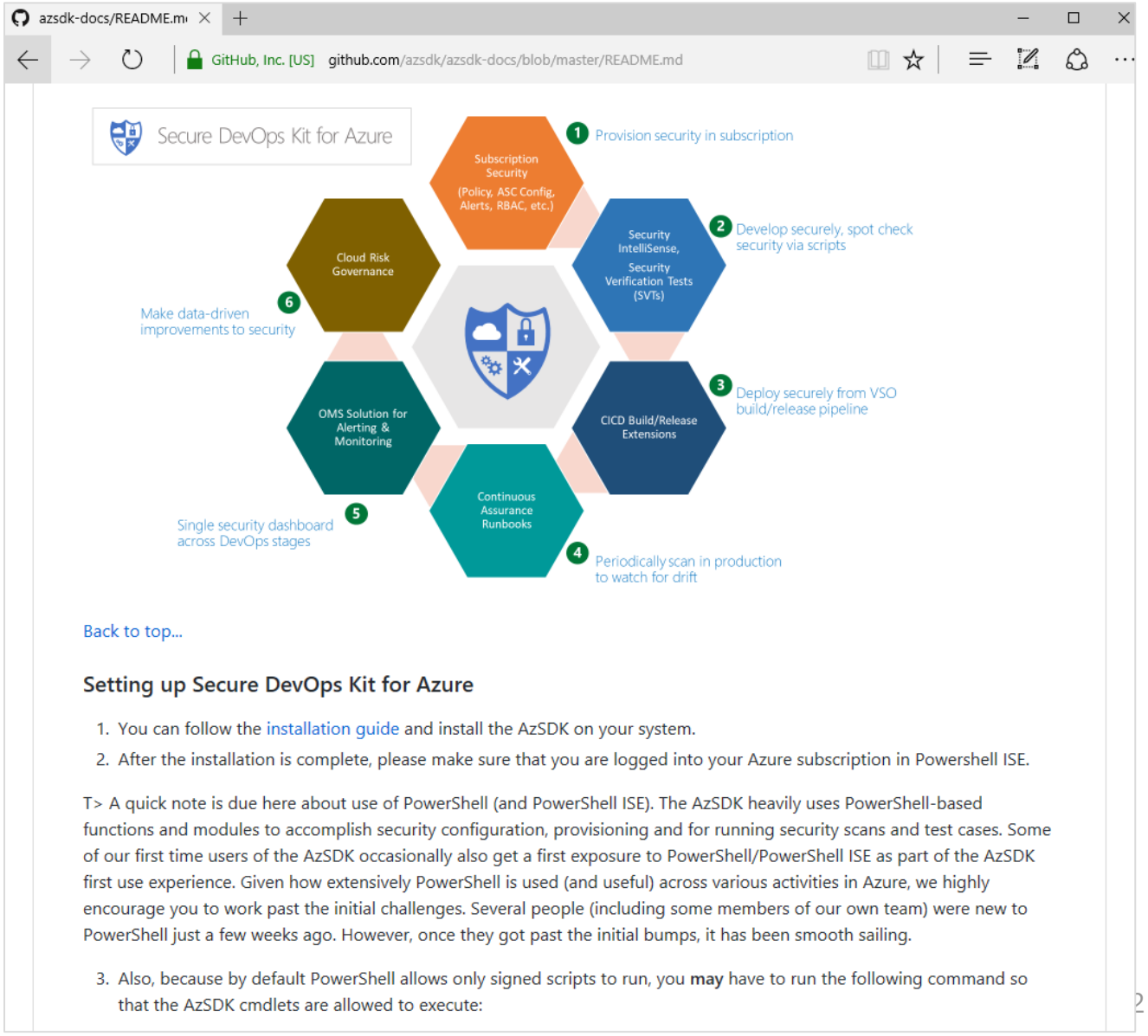
Architecture



Next steps…

Try out the Secure DevOps Kit for Azure!

- https://github.com/azsk
- Installation guide, docs: https://aka.ms/devopskit/docs
- Controls coverage: https://aka.ms/devopskit/tcp
- IT Showcase: https://aka.ms/devopskit/itshowcase
- Support: azsksup@microsoft.com



Questions?

Thanks for attending!

Outline of the workshop…

Session0 – Introduction (till here!)

Session1 – Getting Started with AzSK
- Setup & installation
- Subscription and application security scanning
- Understanding scan reports and fixing issues

Session2 – Exploring AzSK (dev-test workflows)
- Walkthrough of various AzSK cmdlets, artifacts
- Using Security IntelliSense to write secure code
- Integrating security into build/release (CICD) pipelines

Session3 – Exploring AzSK (production workflows)
- Customizing for enterprise environments
- Continuous assurance
- Integration with security dashboards for monitoring

Session4 – Close-out
- Next steps
- Validate action items for both teams

Learning objectives for the workshop

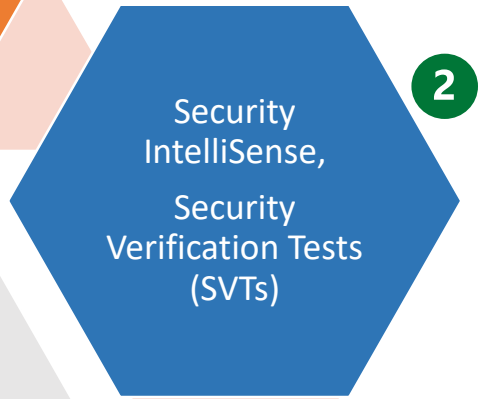
- Understand challenges and opportunities for Secure DevOps in Azure
- Hands-on introduction to the powerful capabilities of the Secure DevOps Kit for Azure (AzSK)
- Experience the speed/efficiency/simplicity of AzSK in a "hands on" manner
- Discuss key scenarios where AzSK can be readily used for your org
- Understand advanced use cases of AzSK and (possible) new requirements for AzSK team
- Identify follow-ups, action items and next steps for both teams

Session1 - Getting Started

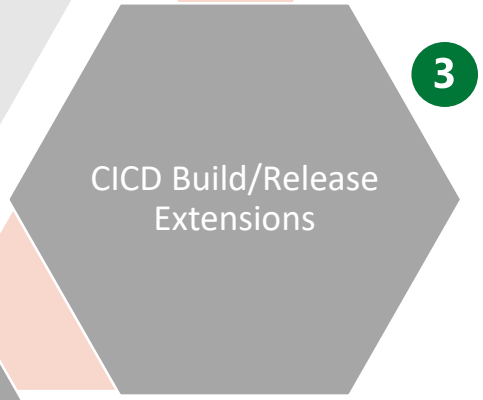
Setup & installation
Subscription and application security scanning
Understanding scan reports and fixing issues

Secure DevOps Kit for Azure

1 Provision security in subscription



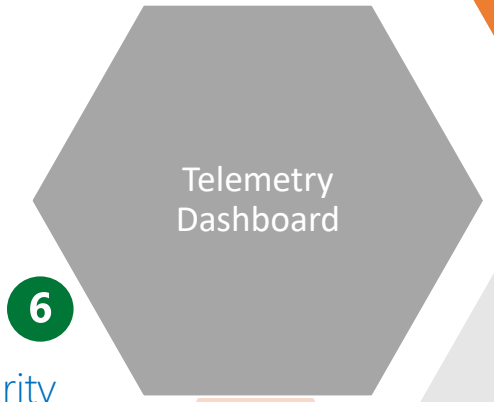
2 Develop securely, spot check security via scripts



3 Deploy securely from VSO build/release pipeline

4 Periodically scan in production to watch for drift

5 Single security dashboard across DevOps stages



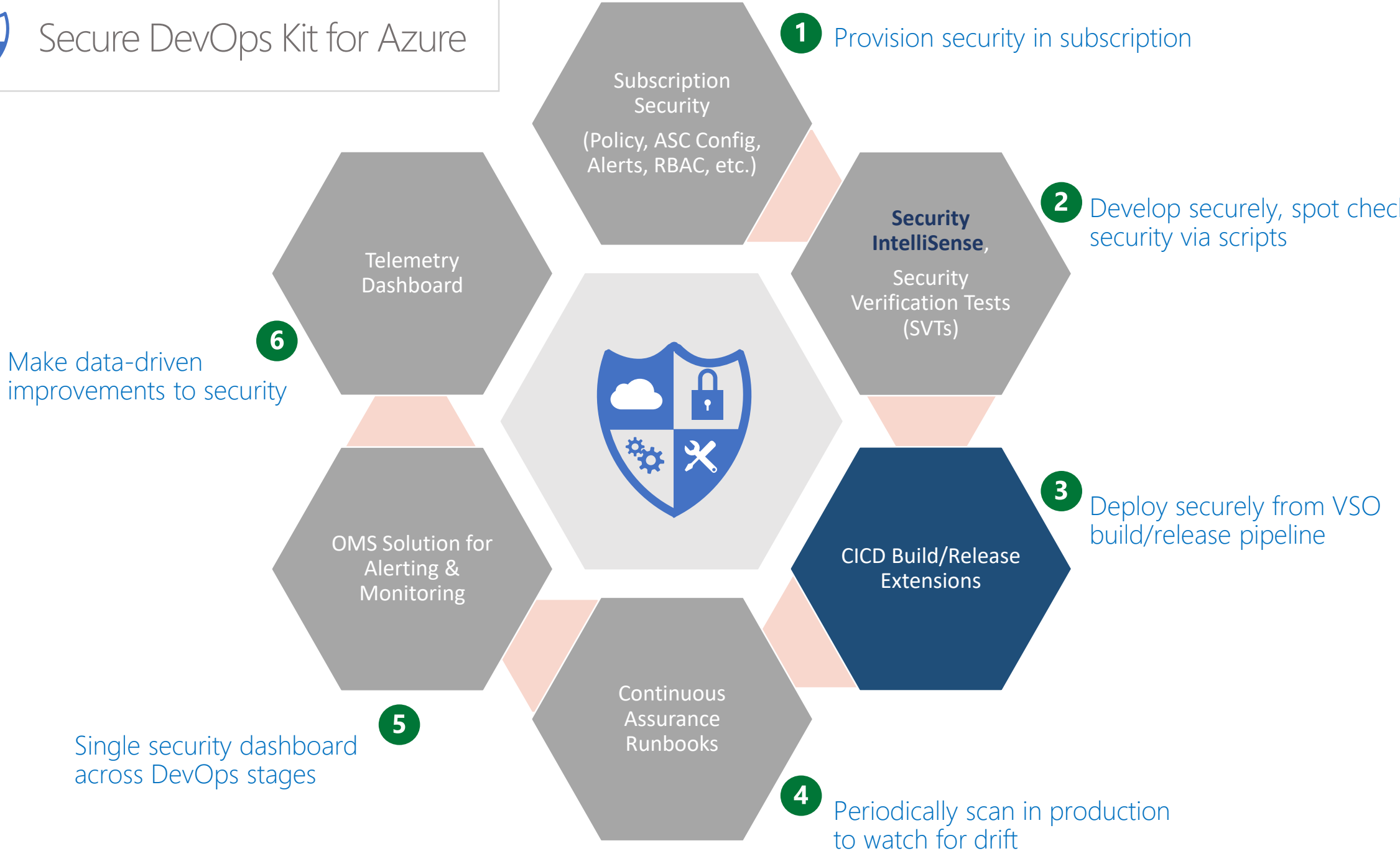
6 Make data-driven improvements to security

Session2 – Exploring AzSK

Dev-test workflows

Walkthrough of various AzSK cmdlets, artifacts
Using Security IntelliSense to write secure code
Integrating security into build/release (CICD) pipelines

Secure DevOps Kit for Azure

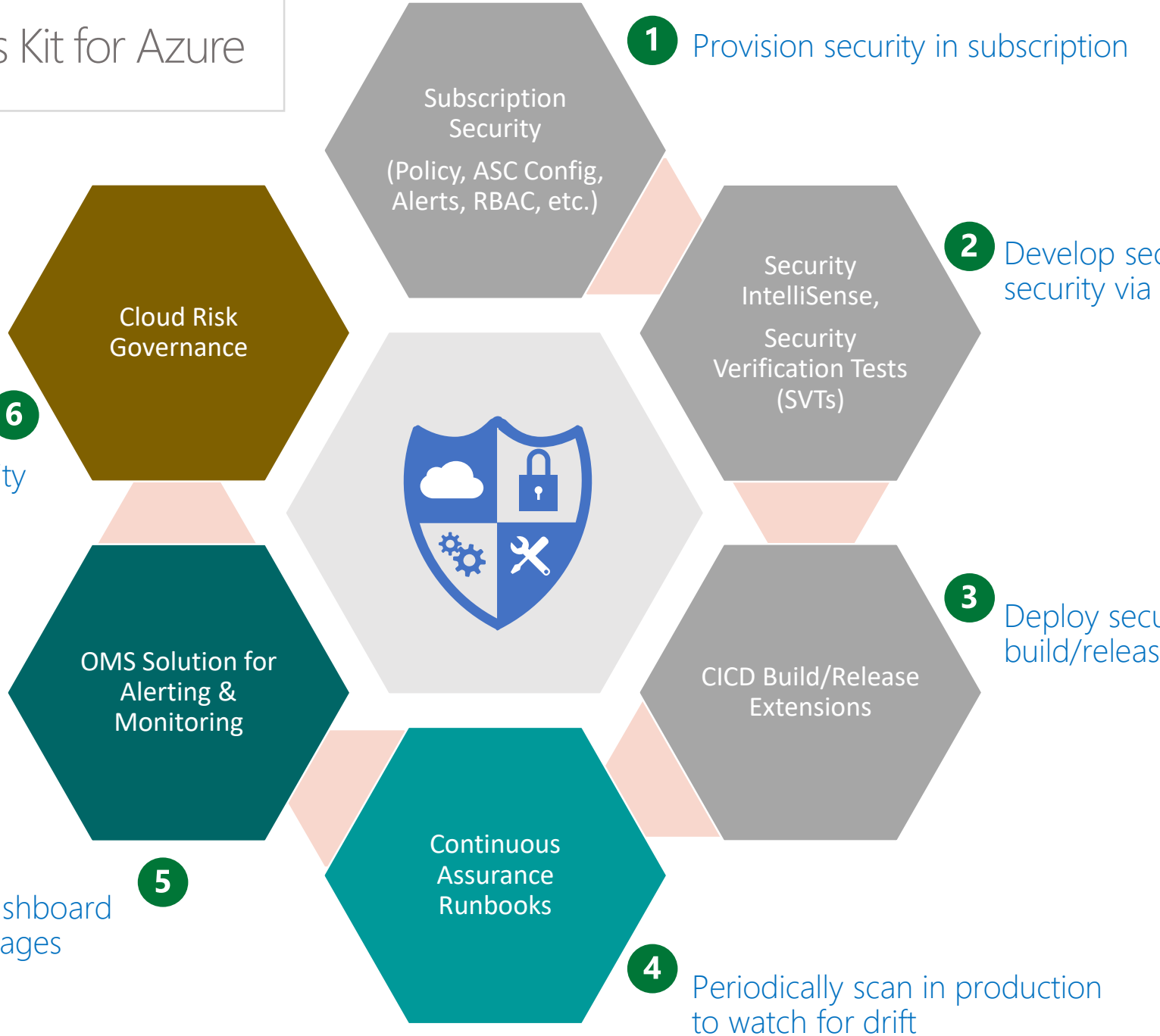


Session3 – Exploring AzSK

Production workflows

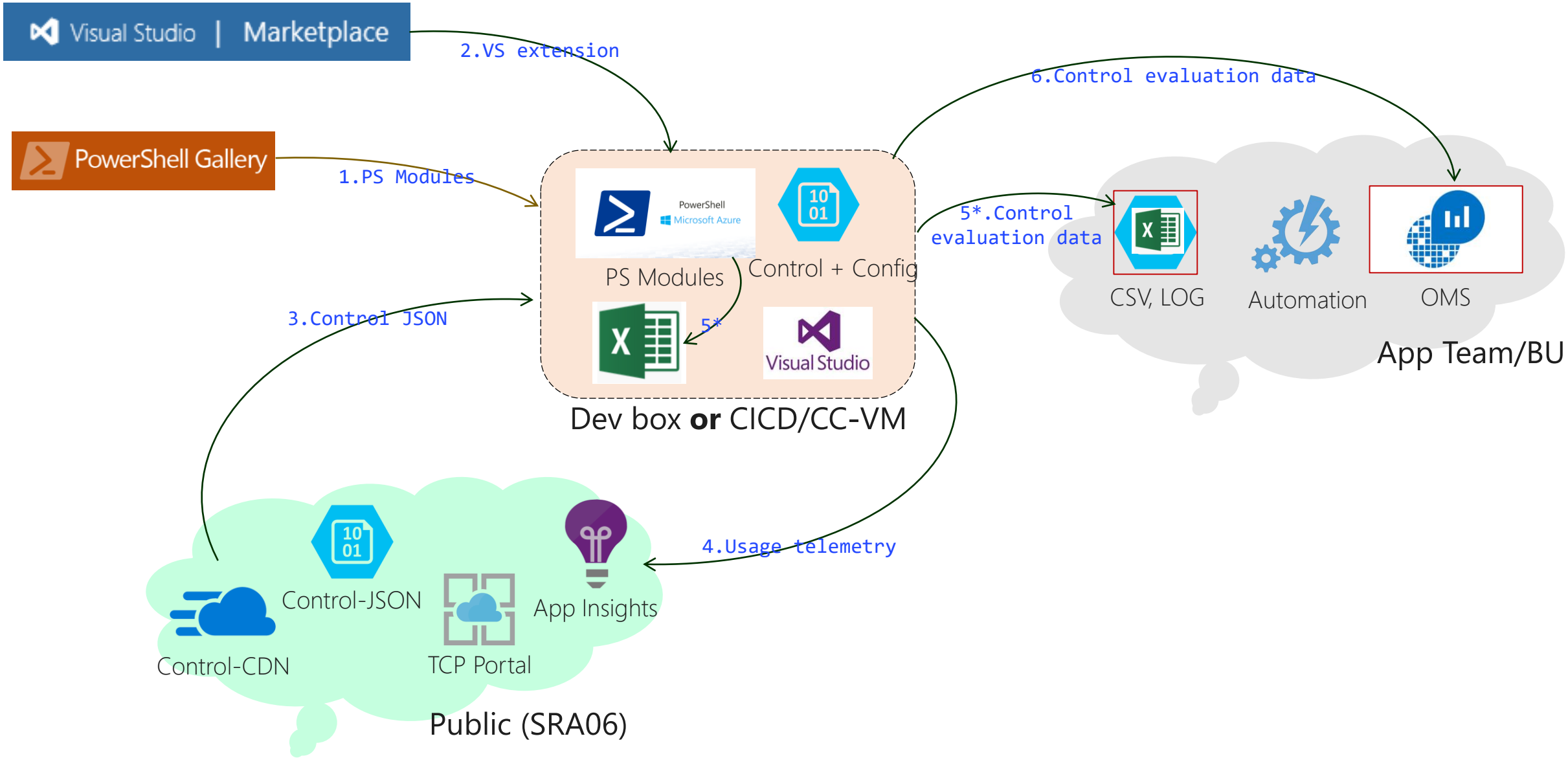
Customizing for enterprise environments
Continuous assurance
Integration with security dashboards for monitoring

Secure DevOps Kit for Azure



1. Provision security in subscription
2. Develop securely, spot check security via scripts
3. Deploy securely from VSO build/release pipeline
4. Periodically scan in production to watch for drift
5. Single security dashboard across DevOps stages
6. Make data-driven improvements to security

AzSK-OSS dataflow (for external users)



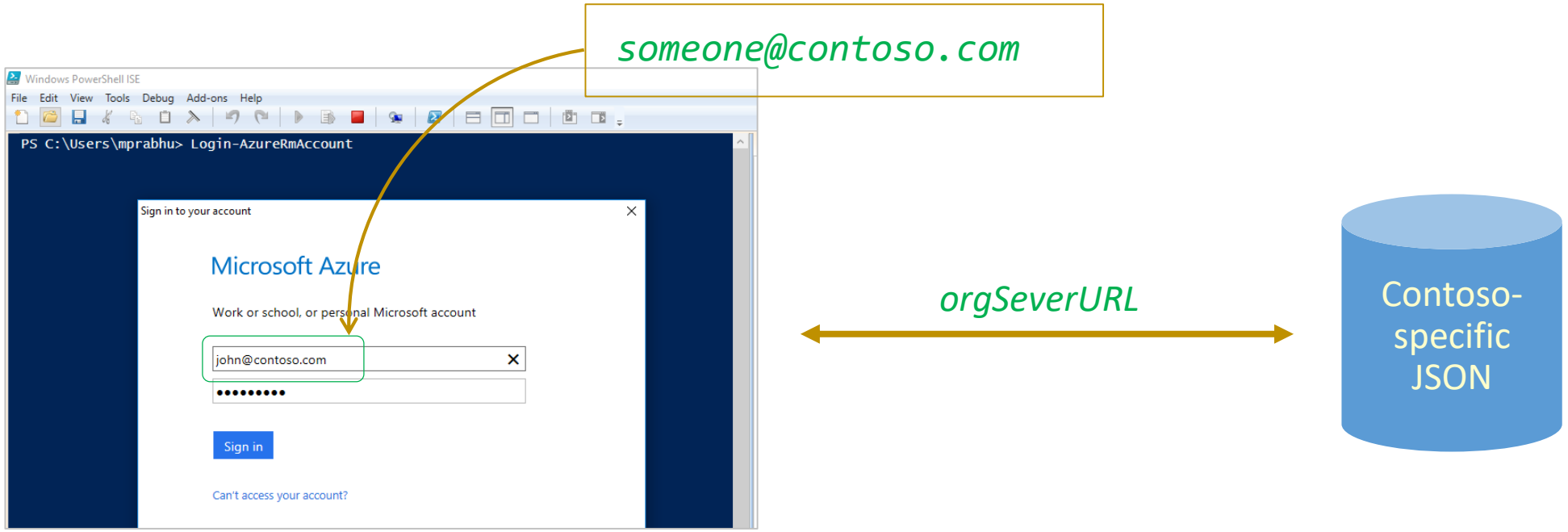
Bootstrapping architecture

Requirements & challenges

Need easy, seamless experience applicable to any enterprise

Cannot have a "consent UI" (must work in CICD, CC)

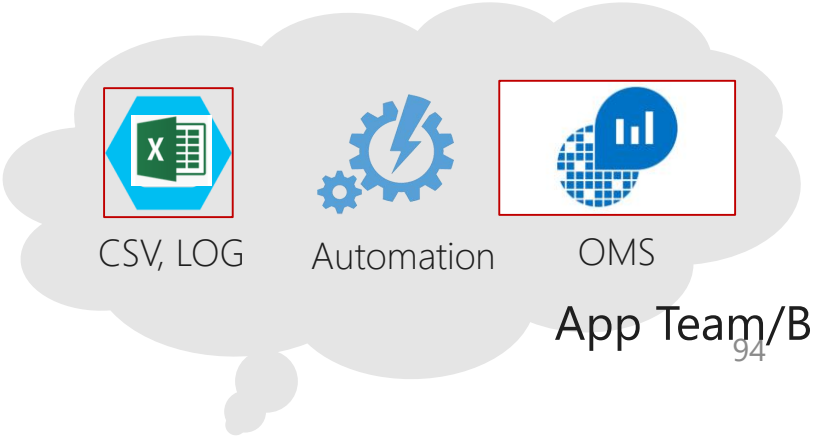
Possible options need AAD admin consent for app or Graph API permission

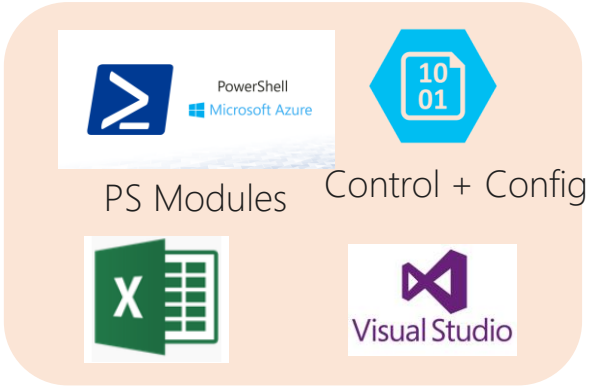


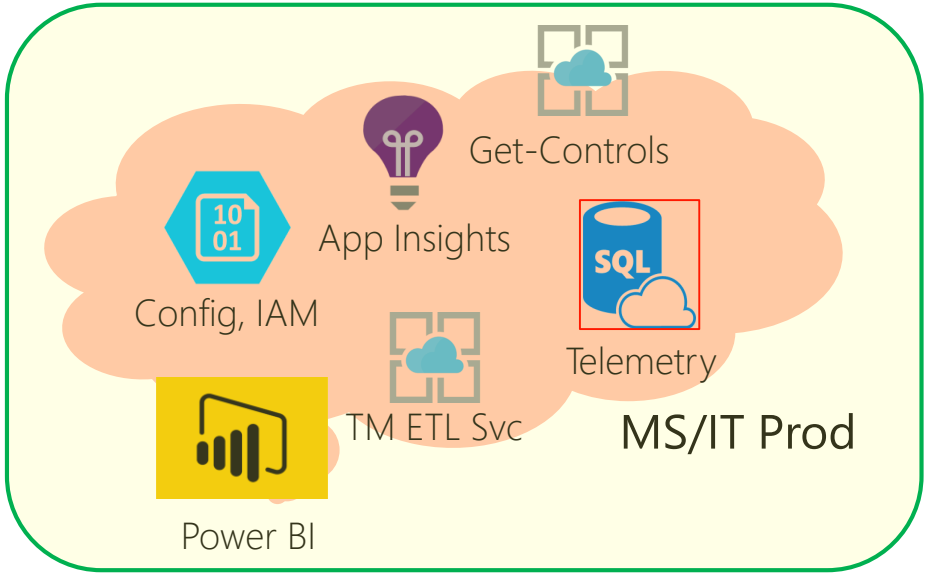
AzSK-OSS assets – runtime

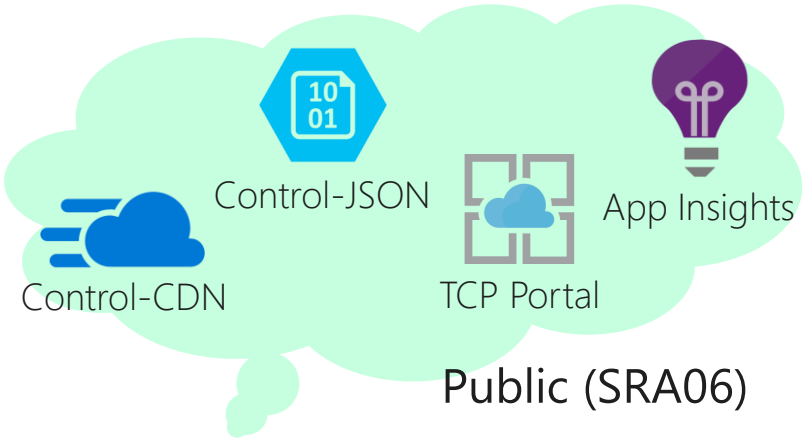
Visual Studio | Marketplace

PowerShell Gallery









Questions?

Thanks for attending!


1
Subscription Security
(Policy, ASC Config, Alerts, RBAC, etc.)
2
Security IntelliSense,
Security Verification Tests (SVTs)
3
CICD Build/Release Extensions
4
Continuous Assurance Runbooks
5
OMS Solution for Alerting & Monitoring
6
Telemetry Dashboard


1
Subscription Security
(Policy, ASC Config, Alerts, RBAC, etc.)
2
Security IntelliSense,
Security Verification Tests (SVTs)
3
CICD Build/Release Extensions
4
Continuous Assurance Runbooks
5
OMS Solution for Alerting & Monitoring
6
Telemetry Dashboard


1
Subscription Security
(Policy, ASC Config, Alerts, RBAC, etc.)
2
Security IntelliSense,
Security Verification Tests (SVTs)
3
CICD Build/Release Extensions
4
Continuous Assurance Runbooks
5
OMS Solution for Alerting & Monitoring
6
Telemetry Dashboard


1
Subscription Security
(Policy, ASC Config, Alerts, RBAC, etc.)
2
Security IntelliSense,
Security Verification Tests (SVTs)
3
CICD Build/Release Extensions
4
Continuous Assurance Runbooks
5
OMS Solution for Alerting & Monitoring
6
Telemetry Dashboard


1
Subscription Security
(Policy, ASC Config, Alerts, RBAC, etc.)
2
Security IntelliSense,
Security Verification Tests (SVTs)
3
CICD Build/Release Extensions
4
Continuous Assurance Runbooks
5
OMS Solution for Alerting & Monitoring
6
Telemetry Dashboard


1
Subscription Security
(Policy, ASC Config, Alerts, RBAC, etc.)
2
Security IntelliSense,
Security Verification Tests (SVTs)
3
CICD Build/Release Extensions
4
Continuous Assurance Runbooks
5
OMS Solution for Alerting & Monitoring
6
Telemetry Dashboard


Subscription Security
(Policy, ASC Config, Alerts, RBAC, etc.)
Security IntelliSense,
Security Verification Tests (SVTs)
CICD Build/Release Extensions
Continuous Assurance Runbooks
OMS Solution for Alerting & Monitoring
Telemetry Dashboard


Subscription Security
(Policy, ASC Config, Alerts, RBAC, etc.)
Security IntelliSense,
Security Verification Tests (SVTs)
CICD Build/Release Extensions
Continuous Assurance Runbooks
OMS Solution for Alerting & Monitoring
Telemetry Dashboard


Subscription Security
(Policy, ASC Config, Alerts, RBAC, etc.)
Security IntelliSense,
Security Verification Tests (SVTs)
CICD Build/Release Extensions
Continuous Assurance Runbooks
OMS Solution for Alerting & Monitoring
Telemetry Dashboard


Subscription Security
(Policy, ASC Config, Alerts, RBAC, etc.)
Security IntelliSense,
Security Verification Tests (SVTs)
CICD Build/Release Extensions
Continuous Assurance Runbooks
OMS Solution for Alerting & Monitoring
Telemetry Dashboard


Subscription Security
(Policy, ASC Config, Alerts, RBAC, etc.)
Security IntelliSense,
Security Verification Tests (SVTs)
CICD Build/Release Extensions
Continuous Assurance Runbooks
OMS Solution for Alerting & Monitoring
Telemetry Dashboard


Subscription Security
(Policy, ASC Config, Alerts, RBAC, etc.)
Security IntelliSense,
Security Verification Tests (SVTs)
CICD Build/Release Extensions
Continuous Assurance Runbooks
OMS Solution for Alerting & Monitoring
Telemetry Dashboard