RSAConference2021

May 17 – 20 | Virtual Experience

SESSION ID: **CSV-M17**

Multi-Cloud Security Monitoring and CIS Benchmarks Evaluation at Scale

Prasoon Dwivedi

@mitprasoon

Susam Pal

@susam

Why are we here?

- Background and Motivation
- Features
- Design and Approach
- CIS Benchmarks
- Results
- Similar Projects and Solutions
- Conclusion

RSAConference2021

Why Cloud Security?

First Thing First

Why cloud is important?

> “Cloud data centers will process 94% of workloads in **2021**.

Source: Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper

Data records compromised in 2019

7, 953,172,708

Whoa! 7.9 Billion $. That's a big number

Source: https://selfkey.org/data-breaches-in-2019/

RSAConference2021

How to secure cloud?

The Big Question

The Process

- Audit
- Patch
- Repeat

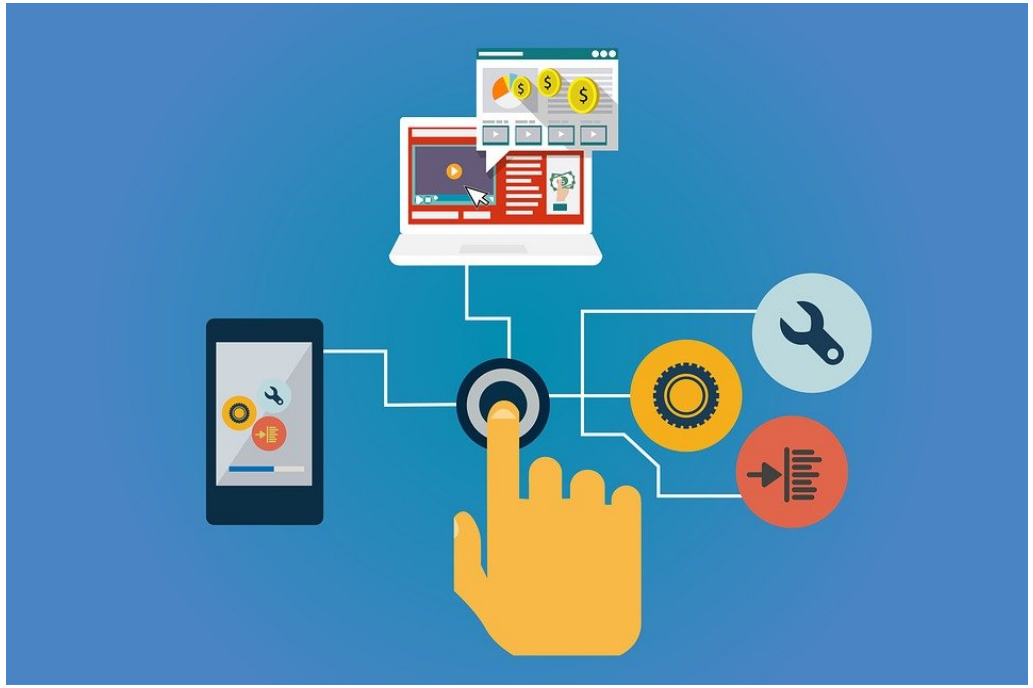
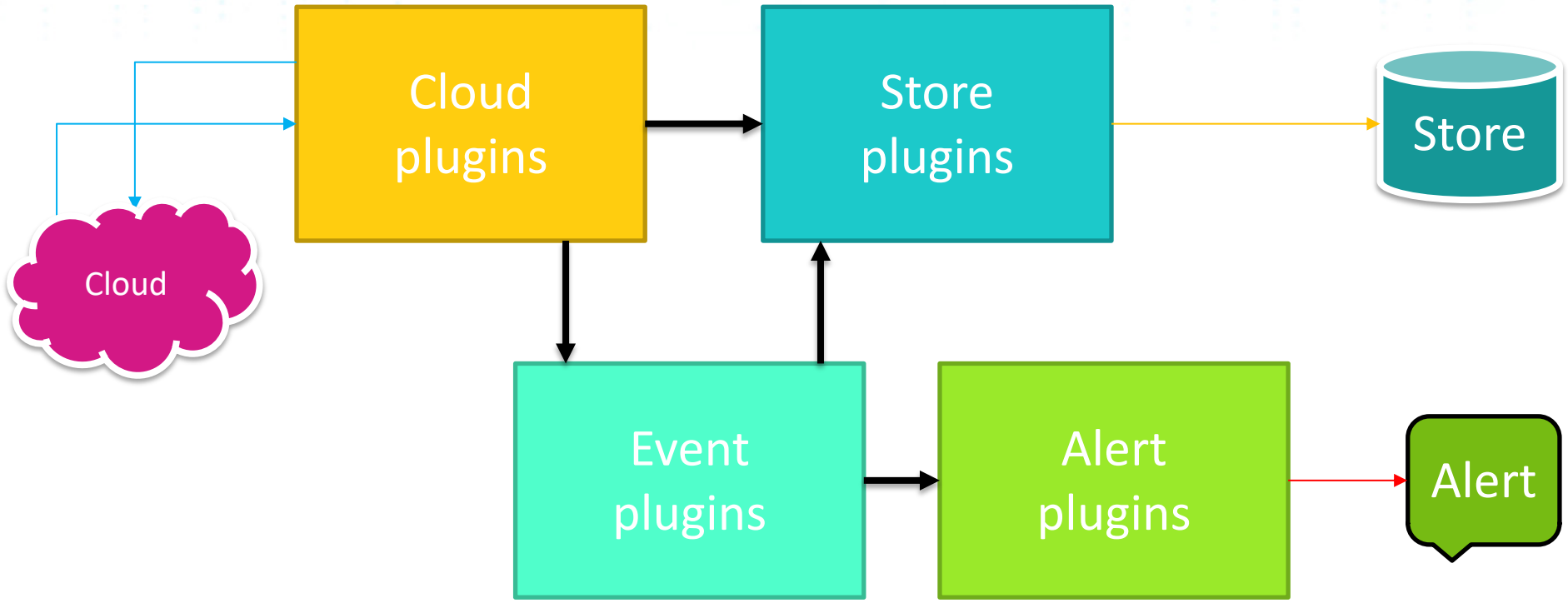


Image Credit : https://pixabay.com

Architecture



Architecture

Cloud Plugin

```
class AzCloud:
    def __init__(self, tenant, client, secret):
        # Connect to Azure Cloud with specified credentials.
        ...

    def read(self):
        # Return Azure cloud configuration records.
        ...
```

Architecture

Store Plugin

```
class SplunkStore:
    def __init__(self, uri, token, index_name):
        # Connect to Splunk with specified URI and token.
        ...

    def write(self, record):
        # Write the cloud record to Splunk.
        ...
```

Architecture

Event Plugin

```
class AzVMOSDiskEncryptionEvent:
    def eval(self, record):
        # Check if the OS disk is not encrypted.
        if not record['ext']['os_disk_encrypted']:
            return create_event_record(record)
            ...
```

Architecture

Alert Plugin

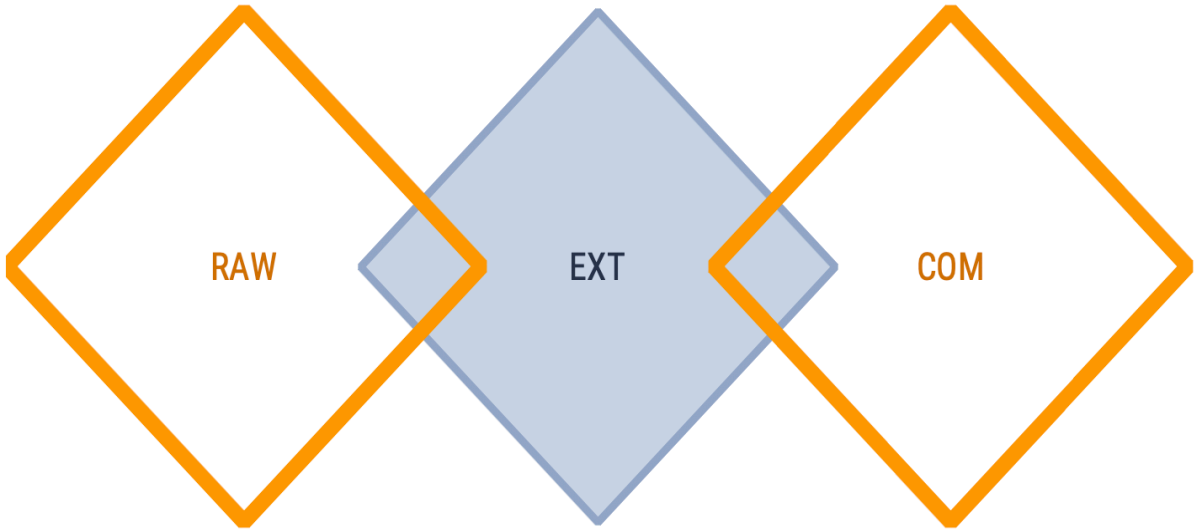
```
class SyslogAlert:
    def __init__(self, host, port):
        # Connect to a syslog receiver.
        ...

    def write(self, record):
        # Send the alert record to the syslog receiver.
        ...
```

Key Features

- Cloud Agnostic
- Extensible
- Agentless
- Fast
- Multiple Report Formats
- CIS Benchmarks

How the data looks like?



Record JSON

```
{
        “raw”: {…},
        “ext”: {…},
        “com”: {…}
}
```

The `RAW` Bucket

What is this?

It contains the data pulled by the cloud plugin in its original format.

Example

```
raw: {
     hardware_profile: { ...}
     id: /subscriptions/17f2cef0-e384-420d-8185-
498092d22111/resourceGroups/ALPHA_TEST/providers/Microsoft.Compu
te/virtualMachines/vm-alpha
     instance_view: { ...
       disks: [
         {
           name: vm-
alpha_OsDisk_1_dcbf97f9c508422a986b1766fc57d2ad
           statuses: [
             {
               code: ProvisioningState/succeeded
               display_status: Provisioning succeeded
               level: Info
               time: 2019-04-08T23:24:56.027235Z
             }
           ]
         }
       ]
       statuses: [
       ]
     }
     license_type: Windows_Server
     location: eastus2
     name: vm-win-jump-1
     network_profile: {...}
     os_profile: {...}
     provisioning_state: Succeeded
     storage_profile: {...}
     tags: {...}
     type: Microsoft.Compute/virtualMachines
     vm_id: 1def1935-dab8-40d7-a149-0126a4a56d8f
   }
}
```

The `EXT` Bucket

What is this?

Extended and derived data specific to a cloud

Example

```
"ext": {
    "cloud_type": "azure",
    "record_type": "virtual_machine",
    "subscription_id": "09d9d0a3-9e7a-4f32-8106-fd0db8763f83",
    "subscription_name": "Pay-As-You-Go",
    "subscription_state": "Enabled",
    "power_state": "running",
    "os_disk_encrypted": false
  }
```

The `COM` Bucket

What is this?

This record bucket contains data common across all clouds

Example


```
"com": {

    "cloud_type": "azure",

    "record_type": "compute",

    "reference": "/subscriptions/09d9d0a3-9e7a-4f32-8106-
fd0db8763f83/resourceGroups/MYRG/providers/Microsoft.Compute/vir
tualMachines/myVM",

    "audit_key": "mockaudit",

    "audit_version": "20190906_174513",

    "origin_key": "azvm",

    "origin_class": "AzVM",

    "origin_worker": "mockaudit_azvm",

    "origin_type": "cloud",

    "target_key": "filestore",

    "target_class": "FileStore",

    "target_worker": "mockaudit_filestore",

    "target_type": "store"

}
```

RSAConference2021

Where to start cloud auditing?

CIS Benchmarks for Cloud Audits

- Azure
- Google Cloud Computing Platform
- Others

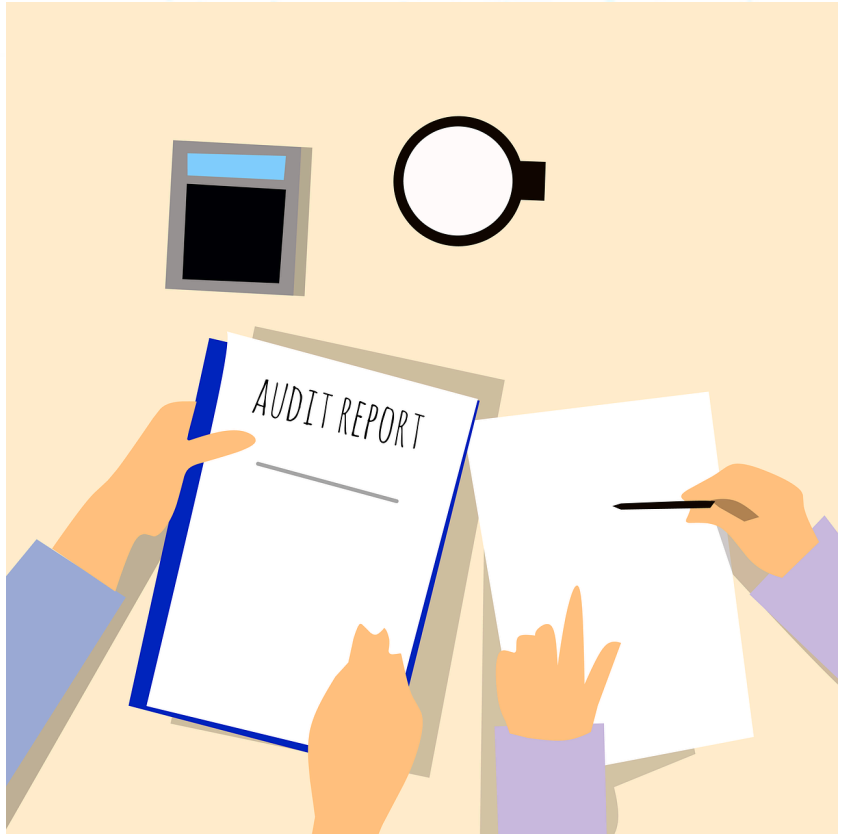


Image Credit : https://pixabay.com
Center for Internet Security https://www.cisecurity.org/

Resources Audited

- Identity and Access Management
- Storage Account
- Databases
- Logging and Monitoring
- Networking
- Virtual Machines
- Application Services

Image Credit : https://pixabay.com

RSAConference2021

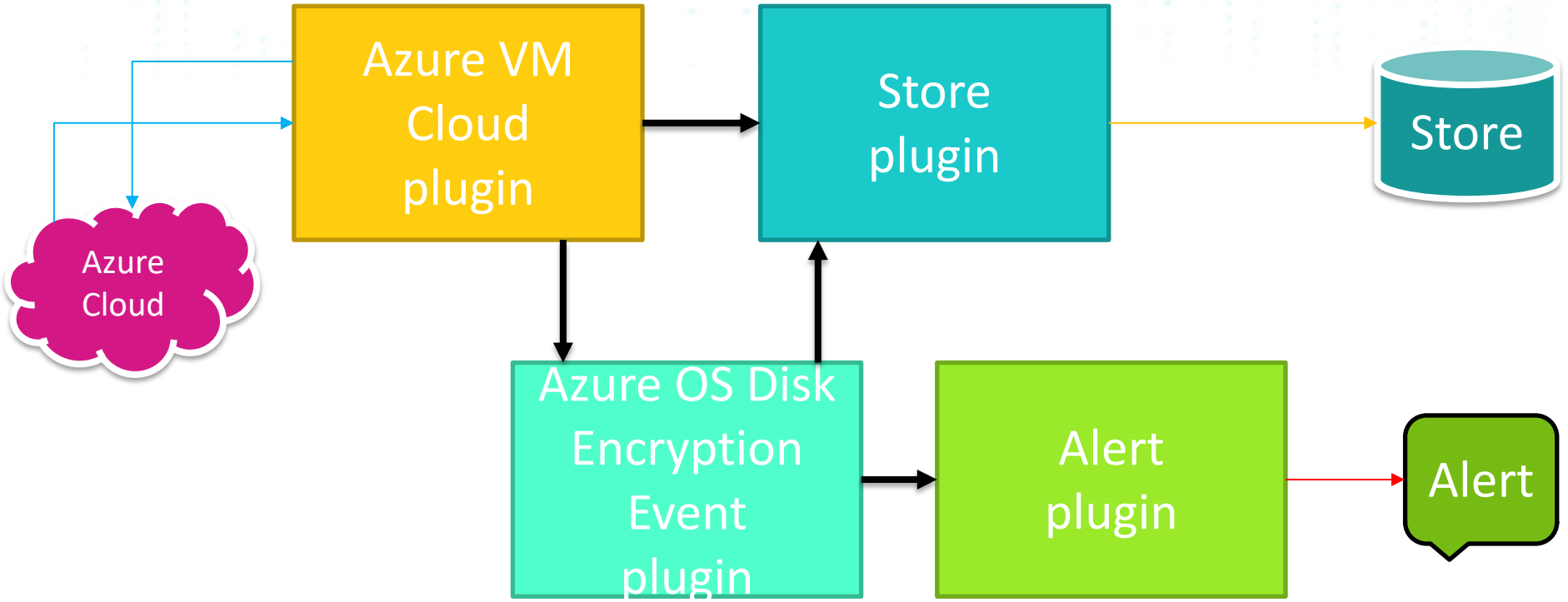
Ensure that `OS Disks` are encrypted
(CIS Microsoft Azure Foundations Benchmark v1.1.0 - 02-15-2019 Section 7.1)

AUDIT EXAMPLE

Why?

Encrypting the IaaS VM's OS disk (boot volume) ensures that its entire content is fully unrecoverable without a key and thus protects the volume from unwarranted reads.

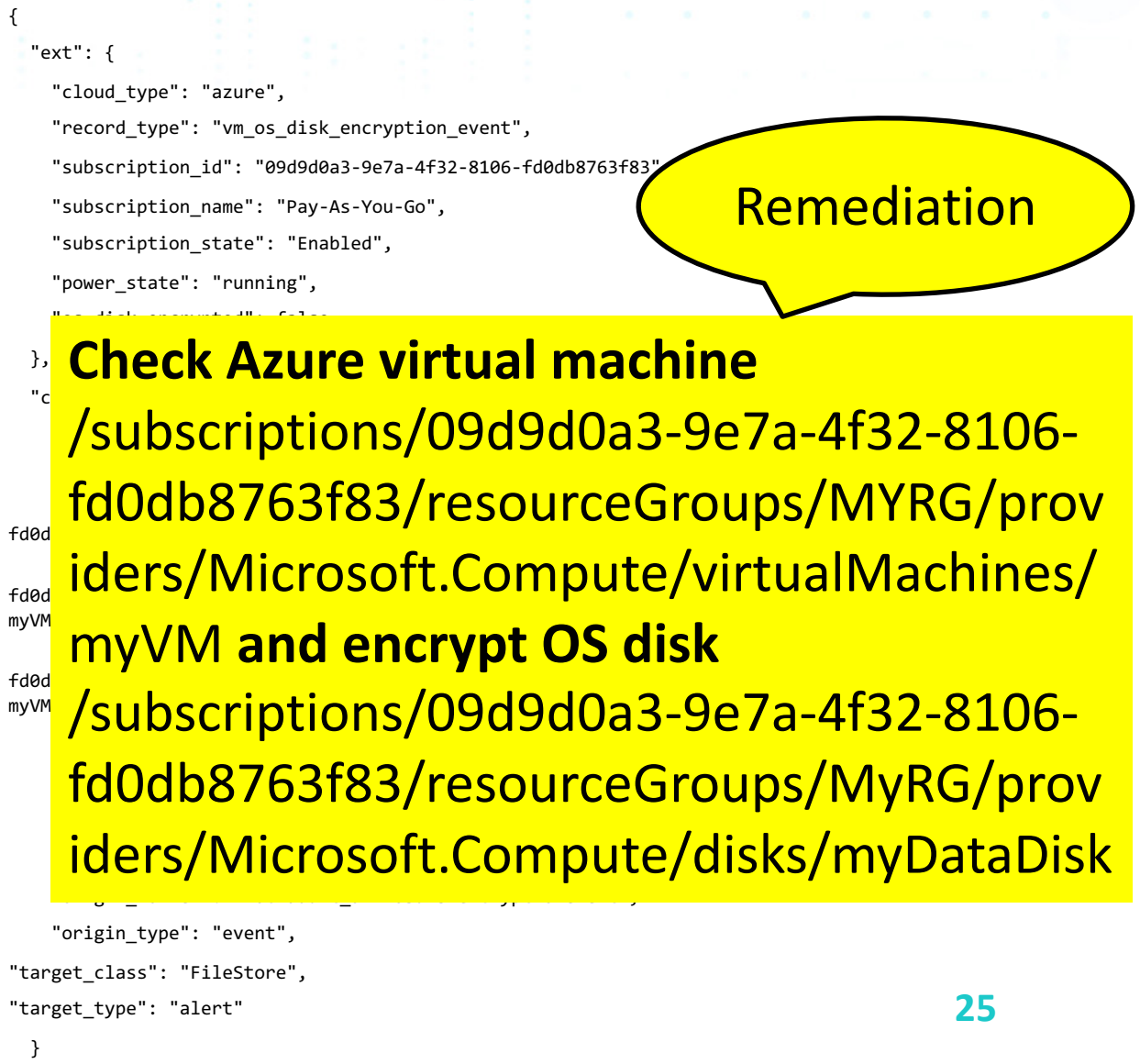
How it works?


Azure VM Cloud plugin
Store plugin
Store
Azure Cloud
Azure OS Disk Encryption Event plugin
Alert plugin
Alert

Event Example


```
{
  "ext": {
    "cloud_type": "azure",
    "record_type": "vm_os_disk_encryption_event",
    "subscription_id": "09d9d0a3-9e7a-4f32-8106-fd0db8763f83",
    "subscription_name": "Pay-As-You-Go",
    "subscription_state": "Enabled",
    "power_state": "running",
    "os_disk_encrypted": false
  },
  "com": {
    "cloud_type": "azure",
    "record_type": "vm_os_disk_encryption_event",
    "reference": "/subscriptions/09d9d0a3-9e7a-4f32-8106-
fd0db8763f83/resourceGroups/MYRG/providers/Microsoft.Compute/virtualMachines/myVM",
    "description": "Azure virtual machine /subscriptions/09d9d0a3-9e7a-4f32-8106-
fd0db8763f83/resourceGroups/MYRG/providers/Microsoft.Compute/virtualMachines/myVM has unencrypted OS disk
myVM_OsDisk_1_99622b8038e5482d9342a3bd9e44f7d9",
    "recommendation": "Check Azure virtual machine /subscriptions/09d9d0a3-9e7a-4f32-8106-
fd0db8763f83/resourceGroups/MYRG/providers/Microsoft.Compute/virtualMachines/myVM and encrypt OS disk
myVM_OsDisk_1_99622b8038e5482d9342a3bd9e44f7d9",
    "audit_key": "mockaudit",
    "audit_version": "20190906_192006",
    "origin_key": "azvmosdiskencryptionevent",
    "origin_class": "AzVMOSDiskEncryptionEvent",
    "origin_worker": "mockaudit_azvmosdiskencryptionevent",
    "origin_type": "event",
"target_class": "FileStore",
"target_type": "alert"
  }
```

Event Example



Remediation

Check Azure virtual machine /subscriptions/09d9d0a3-9e7a-4f32-8106-fd0db8763f83/resourceGroups/MYRG/providers/Microsoft.Compute/virtualMachines/myVM **and encrypt OS disk** /subscriptions/09d9d0a3-9e7a-4f32-8106-fd0db8763f83/resourceGroups/MyRG/providers/Microsoft.Compute/disks/myDataDisk

Misconfiguration Description

Azure virtual machine /subscriptions/09d9d0a3-9e7a-4f32-8106-fd0db8763f83/resourceGroups/MYRG/providers/Microsoft.Compute/virtualMachines/myVM **has unencrypted OS disk** /subscriptions/09d9d0a3-9e7a-4f32-8106-fd0db8763f83/resourceGroups/MyRG/providers/Microsoft.Compute/disks/myDataDisk

RSAConference2021

Ensure web app is using the latest version of TLS

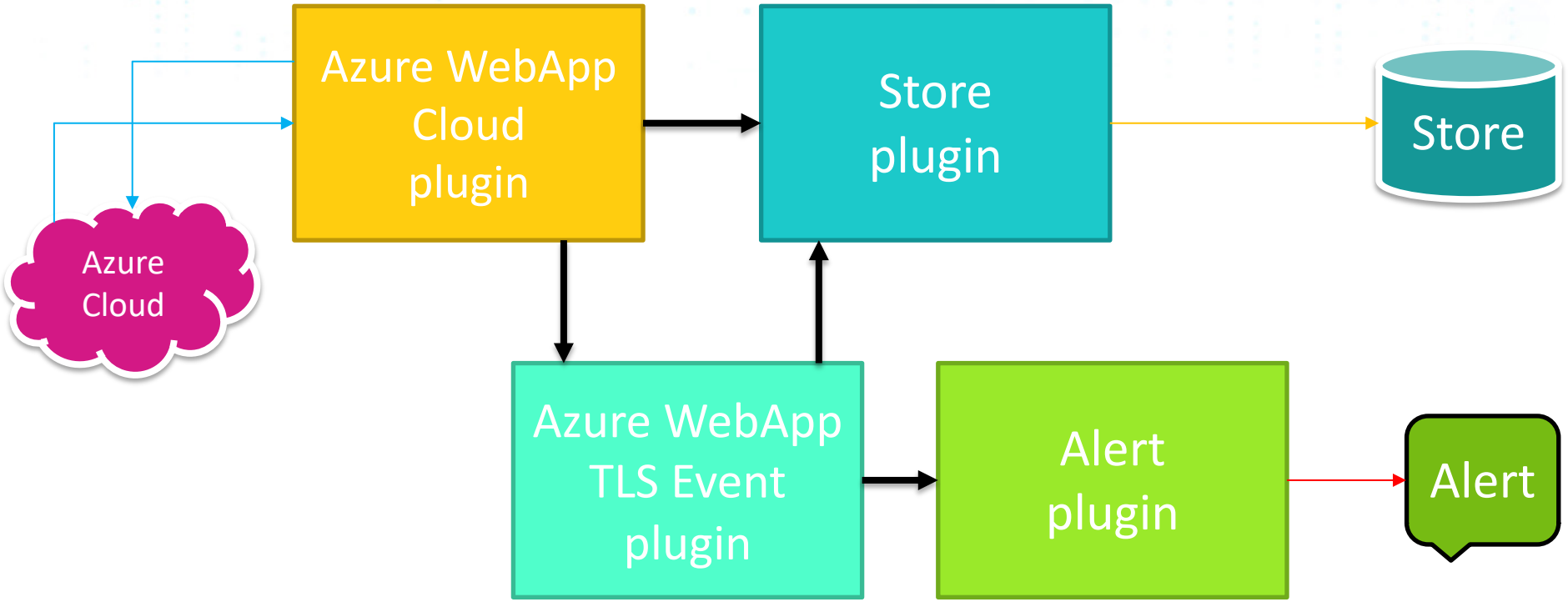
(CIS Microsoft Azure Foundations Benchmark v1.1.0 - 02-15-2019 Section 9.3)

AUDIT EXAMPLE

Why?

The TLS (Transport Layer Security) protocol secures transmission of data over the internet using standard encryption technology. Encryption should be set with the latest version of TLS. App service allows TLS 1.2 by default, which is the recommended TLS level by industry standards, such as PCI DSS.

How it works?


Azure WebApp Cloud plugin
Store plugin
Store
Azure Cloud
Azure WebApp TLS Event plugin
Alert plugin
Alert

Event Example


```
{
   com: {
     audit_key: wmazaudit
     audit_version: 20200227_030035
     cloud_type: azure
     description: Azure web app /subscriptions/fac5e9cf-9b05-9878-8e35-
824df62620b6/resourceGroups/loadmanager/providers/Microsoft.Web/sites/webapp-loadmanager has insecure minimum TLS version.
     origin_class: AzWebAppTLSEvent
     origin_key: azwebapptlsevent
     origin_type: event
     origin_worker: wmazaudit_azwebapptlsevent
     recommendation: Check Azure web app /subscriptions/fac5e9cf-9b05-9878-8e35-
824df62620b6/resourceGroups/loadmanager/providers/Microsoft.Web/sites/webapp-loadmanagerf and ensure the minimum TLS version is
set to 1.2.
     record_type: web_app_tls_event
     reference: /subscriptions/fac5e9cf-9b05-9878-8e35-
824df62620b6/resourceGroups/loadmanager/providers/Microsoft.Web/sites/webapp-loadmanager
     target_class: SplunkHECStore
     target_key: splunkstore
     target_type: alert
     target_worker: wmazaudit_splunkstore
   }
   ext: {
     cloud_type: azure
     min_tls_version: 1.0
     record_type: web_app_tls_event
     subscription_id: fac5e9cf-9b05-9878-8e35-824df62620b6
     subscription_name: Pay-As-You-Go
     subscription_state: Enabled
   }
}
```

Event Example


```
{
   com: {
     audit_key: wmazaudit
     audit_version: 20200227_030035
     cloud_type: azure
     description: Azure web app /subscriptions/fac5e9cf-9b05-9878-8
824df62620b6/resourceGroups/loadmanager/providers/Microsoft.W                    e minimum T
     origin_class: AzWebAppTLSEvent
     origin_key: azwebapptlsevent
     origin_type: event
     origin_worker: wmazaudit_azwebapptlsevent
     recommendation: Check Azure web app /subscriptions/fac5e9cf-98
824df62620b6/resourceGroups/loadmanager/providers/Microsoft.Web/sites/webapp-loadmanagerf and ensure the minimu
set to 1.2.
     record_type: web_app_tls_event
     reference: /subscriptions/fac5e
824df62620b6/resourceGroups/loadmana
     target_class: SplunkHECStore
     target_key: splunkstore
     target_type: alert
     target_worker: wmazaudit_splunk
   }
   ext: {
     cloud_type: azure
     min_tls_version: 1.0
     record_type: web_app_tls_event
     subscription_id: fac5e9cf-9b05-
     subscription_name: Pay-As-You-G
     subscription_state: Enabled
   }
}
```


Misconfiguration Description

Azure web /subscriptions/fac5e9cf-9b05-9878-8e35-824df62620b6/resourceGroups/loadmanager/providers/Microsoft.Web/sites/webapp-loadmanager **has insecure minimum TLS version.**

Remediation

Check Azure web app /subscriptions/fac5e9cf-9b05-9878-8e35-824df62620b6/resourceGroups/loadmanager/providers/Microsoft.Web/sites/webapp-loadmanagerf **and ensure the minimum TLS version is set to 1.2.**

Apply What You Have Learned Today

- Identify your cloud presence
- Identify controls and audit mechanisms already in place
- Go through the CIS Benchmarks and identify the benchmarks which are applicable to your deployment
- Check other standards (NIST, PCI, ISO-27001)
- Prepare an audit plan, define audit cycle, define roles and responsibilities to remediate findings
- Check https://github.com/cloudmarker/cloudmarker for reference implementation