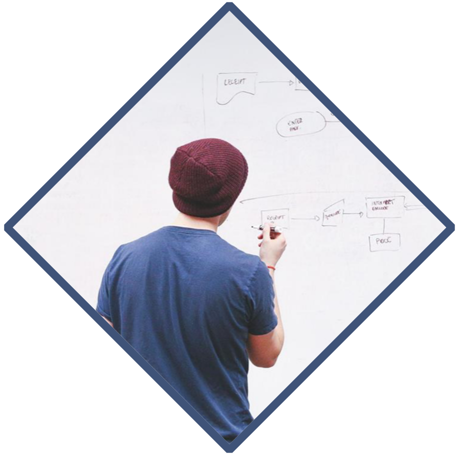
Building a cloud security monitoring and auditing framework



HELLO!

Prasoon Dwivedi and Nirali Shah

DISCLAIMER

The idea and concept presented in this talk is our own work.
It does not represent our employer in any way.

Why are we here?

- Background and Motivation
- Similar Projects/Solutions
- Features
- Design and Approach
  - Architecture
  - Data formats
- CIS benchmarks
- Results
  - Sample data
  - Stats
- Conclusion

Why Cloud Security?

First Thing First

> “By 2020
> 92% of global data-center traffic will come **from the cloud.**

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

Data Records Compromised In First Half Of 2018

3,353,172,708

3 BILLION Whoa! That's a big number, isn't it?

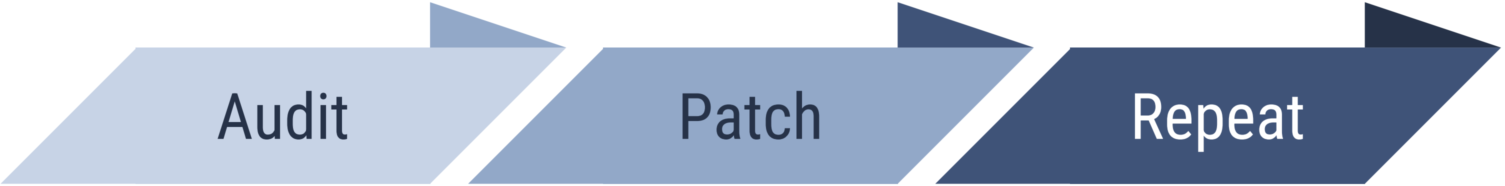
Source: Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper

THE BIG QUESTION

HOW TO SECURE CLOUD?

Image Credit : https://pixabay.com

THE PROCESS IS EASY



Audit

Patch

Repeat

KEY FEATURES

Cloud Agnostic

IaaS & PaaS

Extensible

Plugin Based Framework

Agentless

Written in Python

Uses open source public cloud Python SDKs

Fast

Multiprocessing and Multithreading

Rapid on-demand scans

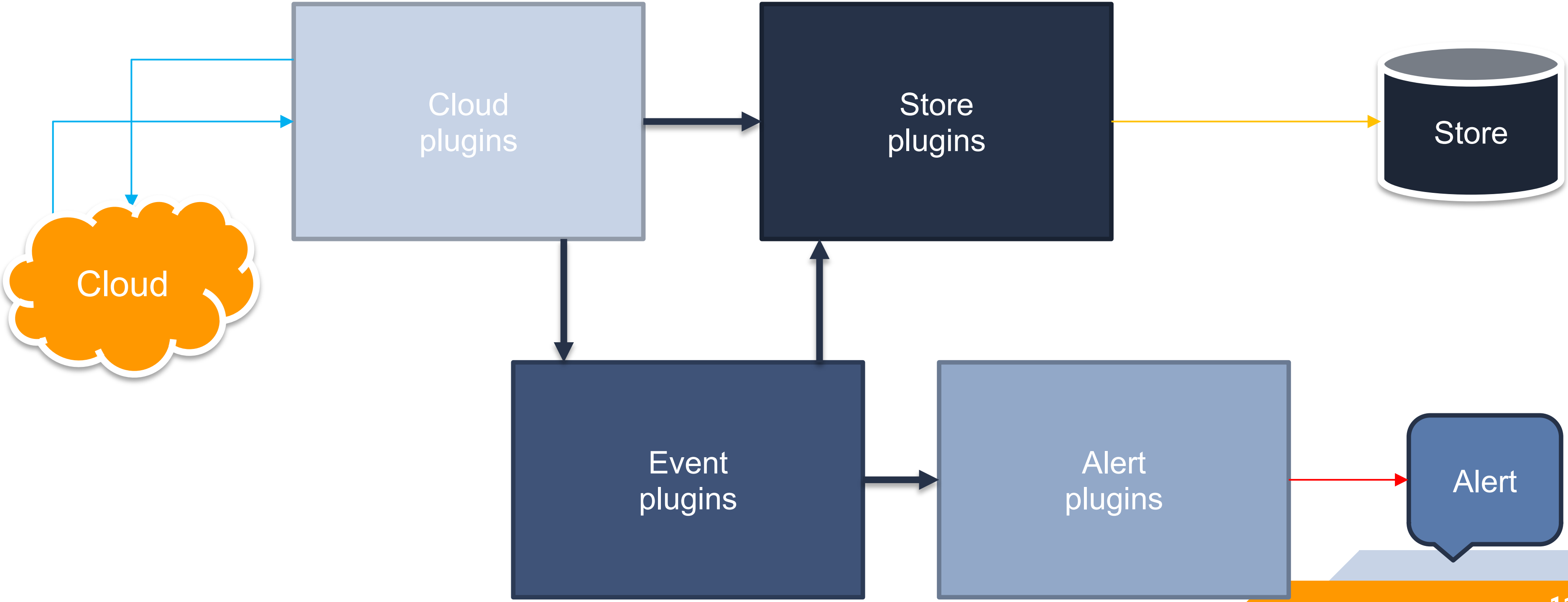
Reports

Normalized data

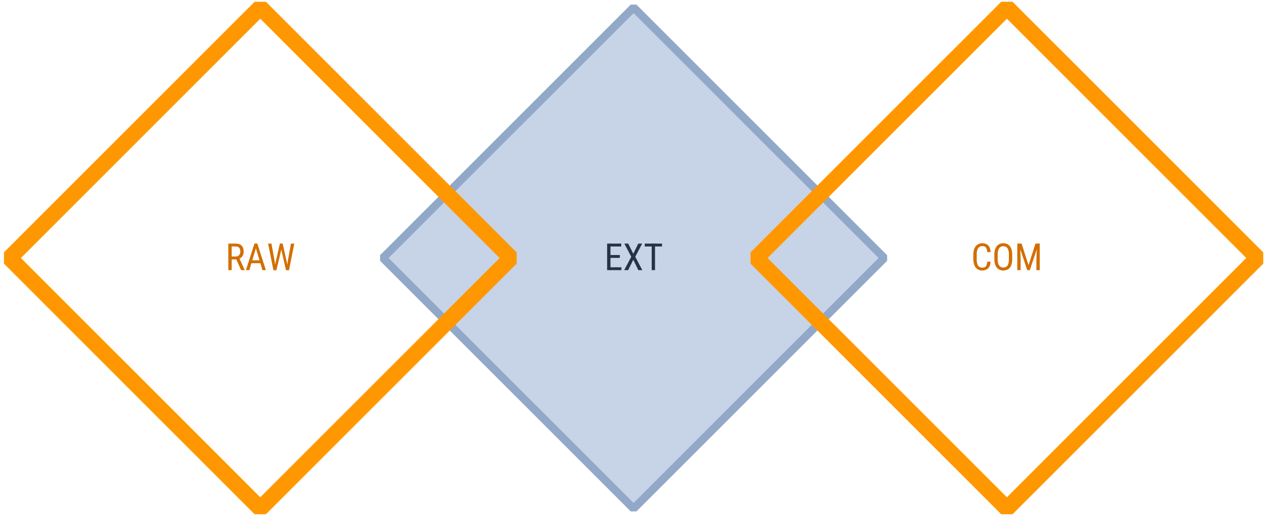
Configurable dashboards

CIS Benchmarks

Architecture



How the data looks?



Record JSON

```
{
        "raw": {…},
        "ext": {…},
        "com": {…}
}
```

RAW Bucket

Example

```
{
    "id": ”sample_subscription/sample_resource",
    "name": "myVM",
    "type": ”virtualmachine",
    "location": ”india",
  "hardware_profile": {
      "vm_size": ”standard"
    }
}
```

What it is?

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

EXT Bucket

Example

```
"ext": {
   "cloud_type": ”xyz",
   "record_type": "virtual_machine",
   "subscription_id": ”sample_subscription",
   "subscription_state": "Enabled",
   "power_state": "running",
   "os_disk_encrypted": false
 }
```

What it is?

Extended and derived data specific to a cloud

COM Bucket

Example

```
"com": {
    "cloud_type": ”xyz",
    "record_type": "compute",
    “description”: “Some security misconfiguration”,
    “recommendation”: “fix this !!!”,
    "reference": “sample_subscription/sample_resource",
    "audit_key": "mockaudit",
    "audit_version": "20190906_174513",
    "origin_key": ”cloudvm",
    "origin_class": ”CloudVM",
    "origin_worker": "mockaudit_cloudvm”
}
```

What it is?

This record bucket contains data common across all clouds

Where to **START** cloud auditing?

CIS Benchmarks for Cloud Audits

For Public Clouds

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
- Security Center

Audit Example

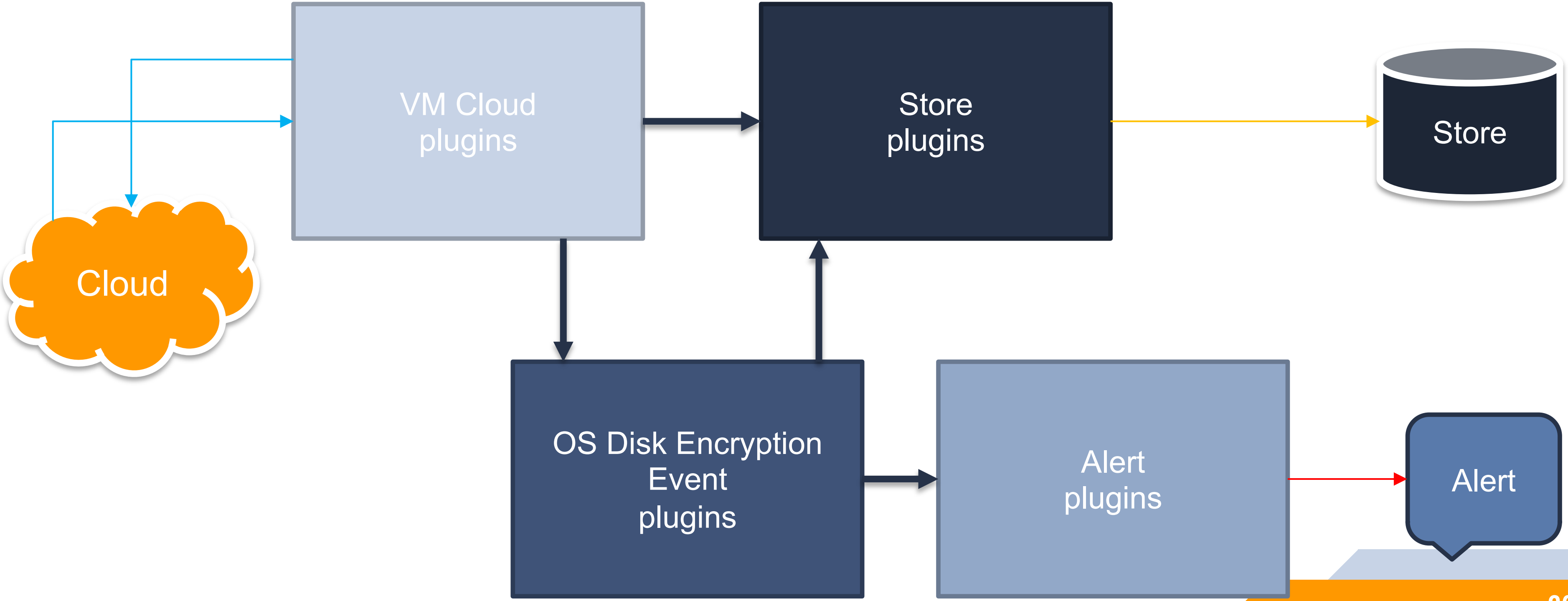
Ensure that ‘OS disk’ are encrypted

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.

Source: CIS Microsoft Azure Foundations Benchmark v1.1.0 - 02-15-2019 Section 7.1

How it works?


VM Cloud plugins
Store plugins
Store
Cloud
OS Disk Encryption Event plugins
Alert plugins
Alert

Event Record

```
"ext": {
                    "cloud_type": "public_cloud_xyz",
                    "record_type":
"vm_os_disk_encryption_event",
                    "subscription_id": "sample_sub",
                    "subscription_state": "Enabled",
                    "power_state": "running",
                    "os_disk_encrypted": false
}
```

```
"com": {
                    "cloud_type": "public_cloud_xyz",
                    "record_type": "vm_os_disk_encryption_event",
                    "description": "public_cloud_xyz virtual machine sample_sub/myVM has
unencrypted OS disk myVM_OsDisk_1",
                    "recommendation": "Check public_cloud_xyz virtual machine
sample_sub/myVM and encrypt OS disk
                    myVM_OsDisk_1",
                    "audit_key": "mockaudit",
                    "audit_version": "20190906_192006",
                    "origin_key": "vmosdiskencryptionevent",
                    "origin_class": "VMOSDiskEncryptionEvent",
                    "origin_worker": "mockaudit_vmosdiskencryptionevent",
                    "origin_type": "event",
}
```

Audit Example: Databases

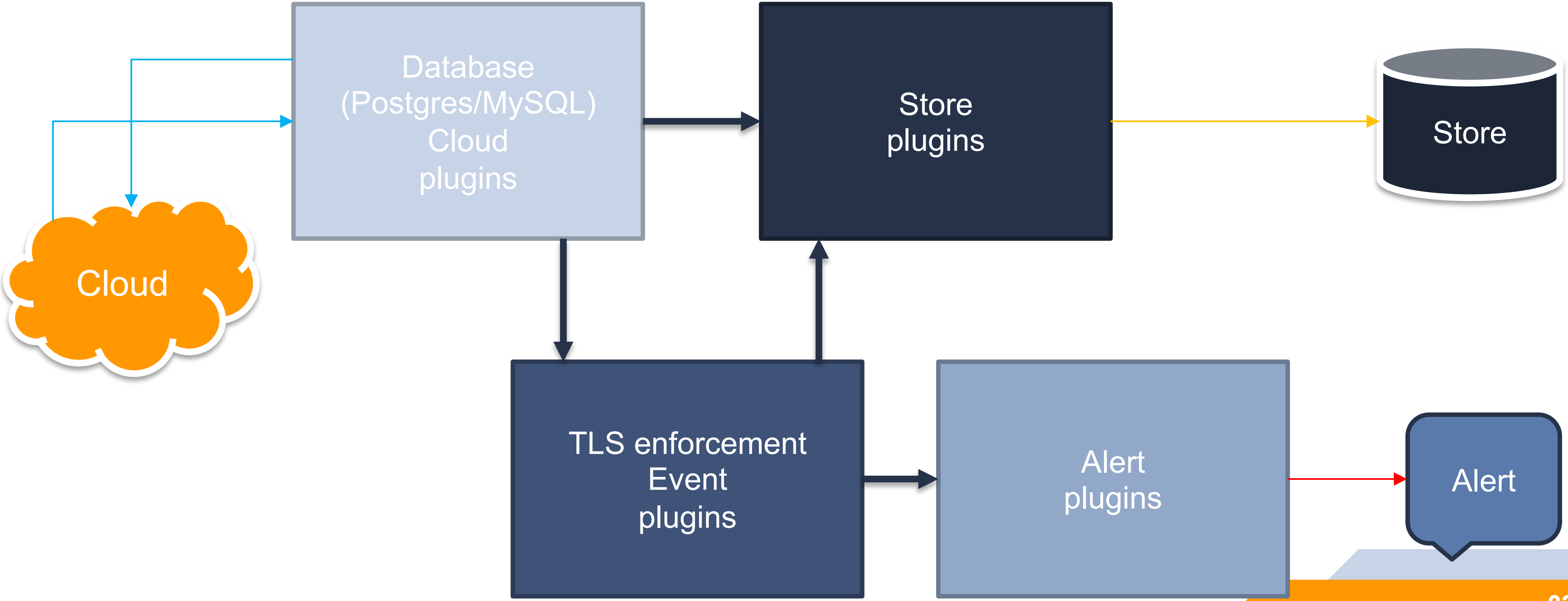
Ensure that DB servers have SSL enforced

Why?

Enforcing SSL connections between database server and client applications helps protect against "man in the middle" attacks by encrypting the data stream between the server and application.

Source: CIS Microsoft Azure Foundations Benchmark v1.1.0 - 02-15-2019 Section 4.13

How it works?


Database
(Postgres/MySQL)
Cloud
plugins
Store
plugins
Store
Cloud
TLS enforcement
Event
plugins
Alert
plugins
Alert

Audit Example: Logs

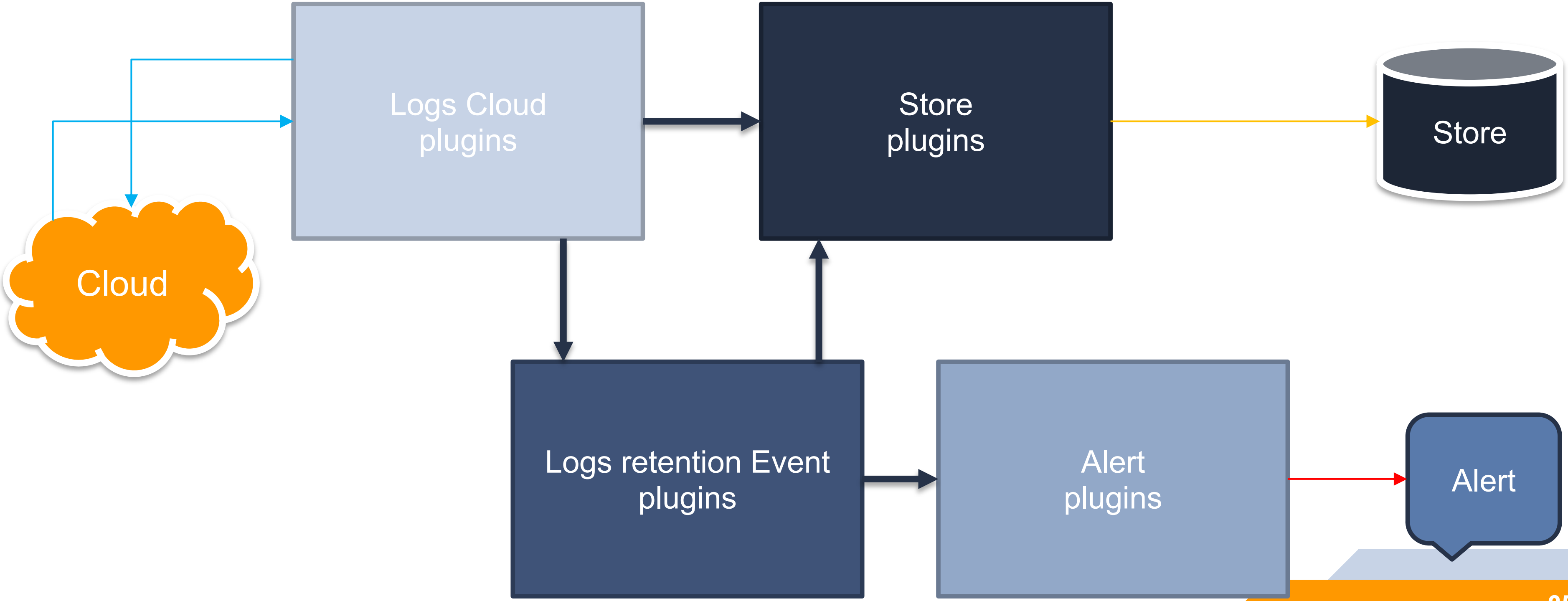
Ensure that logs are retained for atleast 365 days

Why?

Log should be retained for 365 days or more in order to have time to respond to any incidents.

Source: CIS Microsoft Azure Foundations Benchmark v1.1.0 - 02-15-2019 Section 5.12

How it works?


Logs Cloud plugins
Store plugins
Store
Cloud
Logs retention Event plugins
Alert plugins
Alert

Audit Example: Web Applications

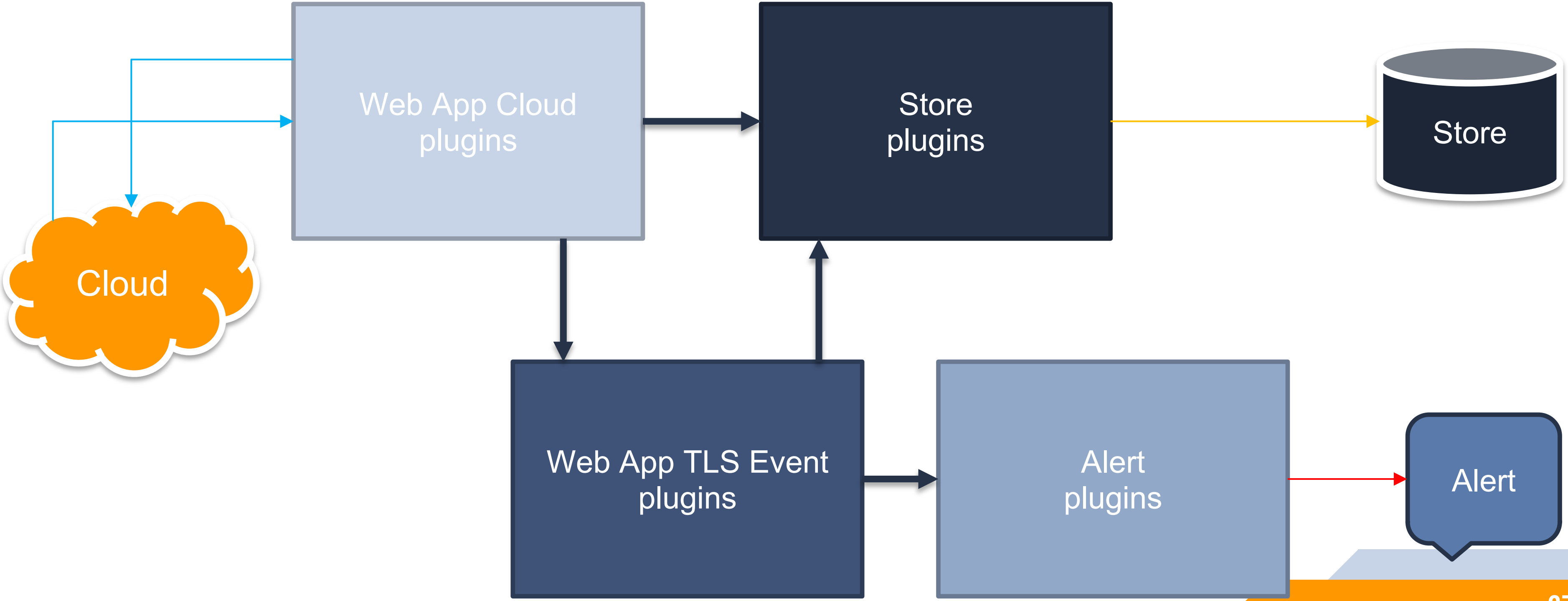
Ensure that Web Apps use latest version of TLS

Why?

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.

Source: CIS Microsoft Azure Foundations Benchmark v1.1.0 - 02-15-2019 Section 9.3

How it works?


Web App Cloud plugins
Store plugins
Store
Cloud
Web App TLS Event plugins
Alert plugins
Alert

THANKS!

Any questions?