**DYNATRACE**

-> Dynatrace is an application performance monitoring tool that helps that their applications

are running optimally and delivering a great user experience.

-> Dynatrace uses a range of monitoring techniques to collect data from applications, infrastructure, and user interactions, and then analyses that data to identify issues and provide insights into performance and usage.

Dynatrace is a software intelligence platform used to monitor and optimize the performance of applications, services, and infrastructure. It is used by businesses and organizations of all sizes and across a wide range of industries to improve the performance, availability, and user experience of their digital assets.

**##Here are some of the common uses of Dynatrace:##**

->**Application Performance Monitoring (APM)**: Dynatrace provides real-time monitoring and end-to-end visibility of applications, including cloud environments, containers, and microservices. It can help businesses identify performance issues and optimize resources to improve the user experience and reduce downtime.

->**Infrastructure Monitoring**: Dynatrace provides comprehensive monitoring of infrastructure, including servers, networks, databases, and storage. It can help businesses identify bottlenecks and optimize resources to improve performance and reduce costs.

->**Digital Experience Management (DEM)**: Dynatrace provides monitoring and analysis of user behavior, enabling businesses to identify opportunities to improve the user experience and increase customer satisfaction.

->**Cloud Migration and Optimization**: Dynatrace can help businesses migrate their applications and infrastructure to the cloud and optimize resources to reduce costs and improve performance.

->**DevOps and Agile**: Dynatrace provides visibility and insights into the performance of applications throughout the software development lifecycle, enabling businesses to identify and resolve issues more quickly and deliver better-quality software.

**ActiveGate**

-> One of the key features of Dynatrace is its ActiveGate technology. ActiveGate is a lightweight component that is installed on the edge of the network, typically in a DMZ or other network boundary.

-> ActiveGate acts as a proxy between the monitored infrastructure and the Dynatrace monitoring server, and it collects and analyses monitoring data from a range of sources, including mobile devices, IoT devices, and cloud services.

-> ActiveGate is designed to be highly scalable and resilient, and it can handle large volumes of monitoring data from multiple sources simultaneously.

-> Overall, ActiveGate is a critical component of the Dynatrace monitoring platform, enabling organizations to gain deep insights into their application and infrastructure performance and make data-driven decisions to optimize their digital experiences.

**OneAgent**

-> OneAgent is a key component of the Dynatrace platform, responsible for collecting performance data from hosts, processes, containers, and services.

-> OneAgent is an agent software that is installed on the hosts and processes that are being monitored. It provides full-stack observability and auto-discovery capabilities, which means that it can automatically detect and monitor applications, services, and infrastructure components, without any manual configuration. OneAgent collects metrics, traces, logs, and events from the monitored components, and sends them to the Dynatrace platform for analysis and visualization.

-> Overall, OneAgent is a critical component of the Dynatrace platform, providing monitoring and analysis capabilities for software applications and infrastructure.

**Access Token**

-> Access tokens in Dynatrace are used to grant specific permissions to individuals or applications, which means they can be used to limit access to sensitive data or actions. These tokens can be revoked or deleted at any time, which is useful in case of security breaches or when access is no longer needed.

**dynakube.yaml**

-> The dynakube.yaml file in Dynatrace is a configuration file used to define and manage the deployment of the Dynatrace OneAgent on Kubernetes clusters. The file contains configuration parameters that define the behavior of the OneAgent, including which modules to install, which Kubernetes namespaces to monitor, and which custom configurations to apply.

**Types of Dashboards we can create in dynatrace**

-> **Application performance dashboards**: These dashboards provide insights into the performance of specific applications, including response times, error rates, and transaction volumes.

-> **Infrastructure monitoring dashboards**: These dashboards provide insights into the performance of infrastructure components such as servers, databases, and networks.

-> **User experience dashboards**: These dashboards provide insights into user behavior, including bounce rates, conversion rates, and session durations.

-> **Cloud monitoring dashboards**: These dashboards provide insights into the performance of cloud environments, including resource utilization, cost optimization, and security posture.

-> **Business impact dashboards**: These dashboards provide insights into how performance issues are impacting business metrics such as revenue, customer satisfaction, and employee productivity.

-> **Custom dashboards**: Dynatrace allows for the creation of fully custom dashboards, which can combine data from multiple sources and present it in a way that meets specific business needs.

**ECR Repo Vulnerability**

In I-exceed prod we are doing this task we want check the as per the requirement

So, that we are go through the crm and loans repository’s we check each and every repository and find the critical vulnerability’s and Akshaya prepared the documents regarding on this let me open that and check the data which we have.

Coming to crm we have total 13 repository’s and some have

Scan-eligibility expired it means as per the policy’s that image will delete after 30 days that’s why it’s showing the scan-eligibility expired, if they new deployed any particular services and push image to ECR then we can get the images her and check whether it’s critical or high.

And sometimes we can see the unsupported images it means the problem with docker file with the base image we have check it and update the docker file

Crm-ui repository

We can see here latest images under we get 4 the critical vulnerability’s go through and get why it’s happened like that and get the remediation for this and presume this issues from devops side or developer side as of now these all are from developer side only and we prode the remediation as well.

As per the status we have total 4 critical.

Coming to loans we have total 24 repository’s and same as if we go through the all the repository’s and check the vulnerability’s weather it’s critical or not high and check that we can fix from devops side or developer side.

As per the status we have total 33 critical issues are there. That we can see in the excel report