TRAINING OFFERING: ADM-471

HORTONWORKS CYBERSECURITY PLATFORM - METRON ADMINISTRATION

3 DAYS 

This course is designed for experienced HDP administrators who will be implementing an Apache Metron on a HDP cluster. Students will receive an overview of the Hortonworks Cybersecurity Platform (HCP) and Apache Metron. In addition, Data Sources, Telemetry Enrichment and an overview of Stellar will be discussed. Finally, participants will also work with Dashboards, Profiles and Threat Triage. Discussion topics and concepts will be further reinforced with hands-on lab activities.

PREREQUISITES

Students should have a strong understanding of system administration in a Linux environment and management of Hadoop clusters using Apache Ambari. Student must have completed Hortonworks University's ADM-221 HDP Operations: Hadoop Administration – Core, ADM-301 HDF Operations: Nifi Flow Management and ADM-351 HDP Operations: Hadoop Security training courses.

TARGET AUDIENCE

This class is for students who need to deploy Hortonworks Data Platform powered by Apache Metron on a HDP based cluster.

FORMAT

40% Lecture
60% Hands-on Labs

AGENDA SUMMARY

Day 1: An Overview of the Hortonworks Cybersecurity Platform, Platform Prerequisites, Deployment, and a Overview of Apache Metron
Day 2: Data Sources, Telemetry Enrichment and an Overview of Stellar
Day 3: Working with Dashboards, Profiles and Threat Triage

DAY 1 OBJECTIVES

- Describe the Hortonworks Cybersecurity Platform
- Summarize the Purpose of the Hortonworks Data Platform Software Frameworks
- Describe Apache Metron
- List Prerequisites for Hortonworks Cybersecurity Platform
- Deploy a Hortonworks Data Platform (HDP) Cluster
- Deploy Hortonworks Data Flow (HDF) to an Existing HDP Cluster
- Deploy Hortonworks Cybersecurity Package on an Existing HDP/HDF Cluster
- List the Steps for Planning HCP Cluster Deployment
- Deploy an HDP Cluster Using Apache Ambari
- Install HDF Mpack on Apache Ambari Server
- Perform an Interactive HDF Installation to an Existing HDP Cluster Using Apache Ambari
- Install Metron Mpack on Apache Ambari Server
- Perform an Interactive HCP Installation Using Apache Ambari

DAY 1 LABS

- Setting Up the Environment
- Installing HDP
- Installing HDF
- Installing Elasticsearch and Kibana
- Installing Apache Metron using Apache Ambari
- Installing the Hortonworks Cybersecurity Platform (HCP)

Contact

For further information visit www.hortonworks.com

+1 408 675-0983

+1 855 8-HORTON

INTL: +44 (0) 20 3826 1405

DAY 2 OBJECTIVES

- List and Describe Common Data Sources
- Describe Data Enrichment
- Describe Batchloaders
- Describe Stellar and How it Can be Used with Apache Metron
- Describe How to Use Stellar Shell Excel Functions for Cybersecurity

DAY 2 LABS

- Adding a Telemetry Data Source
- Transforming a Squid Message
- Enriching Telemetry Events
- Enriching Threat Intelligence Information

Contact

For further information visit www.hortonworks.com

+1 408 675-0983

+1 855 8-HORTON

INTL: +44 (0) 20 3826 1405

DAY 3 OBJECTIVES

- Describe How to Use Dashboards in the Metron UI
- Describe Zeppelin Metron Notebooks
- Describe the Kibana Metron Dashboard
- Describe Storm UI Metron Topologies
- Describe the Purpose of Profiles
- Define Model as a Service
- Define the Purpose of Data Sketches
- Define the Anatomy of a Profile
- Describe How to Create Profiles
- Describe the Implementation of Profiles
- Describe the Purpose of Threat Triage

DAY 3 LABS

- Adding a Telemetry Data Source
- Prioritizing Threat Intelligence
- Configuring Indexing
- Setting up a Profile
- End to End Metron Use Case

Revised 08/17/2018

Contact

For further information visit www.hortonworks.com

+1 408 675-0983

+1 855 8-HORTON

INTL: +44 (0) 20 3826 1405