Day 1: Introduction and Monitoring

09.00 – 09.15 Welcome and Expectations

09.15 – 10.45 **Introduction.** An introduction to the course. What is DPI and how does it work? Who are the typical customers and what are their needs? This module goes on to define key terms and to present the basic solution architecture. It finishes by presenting a number of case studies which will be used throughout the course to illustrate what is learnt

11.00 – 12.30 **Introducing NetEnforcer.** What is NetEnforcer? What are the differences between the NetEnforcer models? This module looks at the different factors involved in deciding where to place a NetEnforcer in the customer's network, before showing how to physically connect it to the network and how to perform initial configuration.

12.30 – 13.30 Lunch Break

13.30 – 14.30 **Introducing NetXplorer.** What is NetXplorer? We will learn how to install the NetXplorer server and the GUI client, and will then see how to get started working with the GUI.

14.45 – 16.15 **Monitoring and Reporting.** How can you use the NetXplorer to get full visibility of your network? In this module, we will learn how to use the real-time monitoring and long-term reporting functionalities of the NetXplorer. We will examine the different types of available graphs and will see how they are typically used. We will also look at some of the more advanced monitoring features, before seeing how to pre-define and schedule reports and how to use groups to enable reporting across different entities.

16:15 – 17:30 **Hands-on Monitoring Exercises**

Day 2: Policy Provisioning

09.00 – 10:30 **Condition Catalogs**. How to define different condition catalogs to classify the traffic running through your network. This module includes a thorough explanation of host, time, service, ToS and VLAN catalogs.

10.45 – 12.15 **Action Catalogs.** How to define the different action catalogs to enforce Quality of Service polices that you have defined for the traffic running through your network. This module includes a thorough explanation of QoS, ToS and DoS catalogs, as well as the NetEnforcer's access control mechanism.

12.15 – 13.15 Lunch Break

13.15 – 14:30 **Building a Policy.** How to use the building blocks you have defined in the catalog entries to build an effective policy to meet your business needs. This module includes explanations and case studies showing how to create rules using Lines, Pipes, VCs and Templates.

14:30 – 17.30 **Hands-On Provisioning Exercises**

Day 3: Alarms, Redundancy and Exam

09.00 – 10.30	**Events and Alarms.** How to ensure a proactive notification of changes in the status of your network. This module covers how to define alarms and alarm actions and how to assign them to different entities. In addition, we see how to configure events, and how to view events and alarms in the various logs. We end with several examples.
10.45 – 12.00	**Advanced Configurations.** How to ensure high availability and system redundancy. This module looks at the different redundancy configurations, the pro's and con's of each one, and how to connect and configure them.
12.00 – 13.00	**Theoretical Exam.** Summarizing the material learnt in the course.
13.00 – 14.00	Lunch Break
14.00 – 14.30	Reviewing the theoretical exam and answering questions
14:30 – 15.45	**Practical Exam**. Work in groups to build traffic policies on the basis of specific customer needs.
15.45 – 16.45	Presentation of practical exam results and feedback
16.45 – 17.00	Summary and Feedback