Course Sequence and Topic Learning Objectives

**Module 1: Introduction To Machine Learning and BlackBerry Cylance Resources**
- Explain machine learning in the context of artificial intelligence
- Explain the difference between supervised and unsupervised ML
- Describe how BlackBerry Cylance uses ML as a solution that provides prevention to endpoints
- Explain how CylancePROTECT® identifies malware to those not familiar with AI and ML using analogies
- Describe how to obtain diagnostic and support-related information using the BlackBerry Cylance management console
- Identify support resources provided by BlackBerry Cylance

**Module 2: BlackBerry Cylance Technology Overview and Platform Solutions**
- Explain the main features of CylancePROTECT
- Describe how CylancePROTECT differs from traditional AV
- Describe the features of CylanceV™ and the use cases where it would be beneficial
- Explain the value proposition of CylanceOPTICS™ and how it integrates into a CylancePROTECT environment
- Describe the EDR capabilities of CylanceOPTICS, what data is collected, and where it is stored

**Module 3: Deployment and Installation**
- Define a zone and how zones apply to devices
- Explain how to use zones to manage a group of devices
- Create a zone rule and describe how devices can be automatically grouped
- Explain zone best practices
- Describe where to configure policy settings
- Explain how to find information about various policy options
- Identify important installation options during a deployment
- Describe uninstallation settings

**Target Audience**
- BlackBerry Cylance Customers / Administrators
- Solution Providers, Consulting Partners, and System Integrators

**Overall Course Objective**
Attendees will be able to explain BlackBerry Cylance technology in detail and install, configure, and deploy prevention-based endpoint security throughout their operating environments.

**Course Level: Introductory**
The instructor-led live session is two, eight-hour days and combines lecture, interactive exercises, group discussion, and hands-on labs.
Module 4: Administration and Threat Management
- Explain the different user roles, when they are used, and how they differ
- Construct the Syslog / SIEM settings for exporting venue console events
- Demonstrate how to access your account settings and view the audit log
- Explain the graphical data on the dashboard
- Prioritize threats found in the environment
- Explain the three threat priorities and how the priority is calculated
- Describe the BlackBerry Cylance Confidence Score and the difference between unsafe and abnormal
- Describe how a file is scored when offline vs. online
- Explain how to download the Threat Data Reports and understand their importance
- Explain how to sort threats by priority
- Explain how to conduct basic threat investigation utilizing the Threat Details page
- Explain what threat indicators are and why they are important
- Describe how to view, waive, and quarantine threats on a specific device
- Explain how to view devices and assigned zones and policies
- Describe how and when the device communicates with the console

Module 5: Troubleshooting and Support
- Describe how to troubleshoot basic application and performance issues
- Explain what settings in device policy can cause application and performance issues
- Explain the three places that verbose agent logging can be enabled and when it should be enabled
- Identify top support scenarios and basic troubleshooting steps for those issues
- Describe how to gather logs and use the support collection tool in preparation for contacting support