CyberController Plus

Training Course Outline

Version 10.x

1 Introduction

Cyberattacks against networks of service providers can include multiple vectors with various characteristics, thereby threatening network infrastructure elements and requiring multiple methods of mitigation. **CyberController-Plus** (formally known as DefenseFlow) is a network detection and cybercontrol application designed to automate and orchestrate the detection and mitigation of network, multivector attacks.

Radware's CyberController-Plus supports out-of-path and always-on hosted customer protection use cases for service providers to provide the widest attack detection combined with real-time attack mitigation. Detection can be performed either by Radware security devices or 3rd party detectors. Mitigation is performed by Radware's award winning DDoS solution called DefensePro.

This document is protected by United States and International copyright laws. Neither this document nor any material contained within it may be duplicated, copied, or reproduced, in whole or part, without the expressed written consent of Radware, Inc.

2 Purpose and Scope

This course, **CyberController-Plus**, is a structured 2-day training.

It consists of a *practical* and a *theoretical* part.

In this course we will focus on the features used in all different CyberController-Plus deployments.

This comprehensive training course begins with an introduction to the key benefits and capabilities of CyberController-Plus, highlighting how it enhances network security and streamlines threat management. Participants will then learn how to set up CyberController-Plus from the ground up, including step-by-step guidance through the installation process and essential configuration tasks.

As the course progresses, we delve into advanced threat detection techniques using tools such as FlowDetector, DefensePro, and various external detection systems. You'll gain practical insights into how these components work together to identify and mitigate cyber threats in real time.

A dedicated module focuses on Cyber Controller Analytics, where we explore how to monitor attack patterns, interpret critical parameters, and respond effectively both before and during an attack. You'll learn how to leverage analytics for proactive defense and incident analysis.

We also introduce the Managed Security Service Providers (MSSP) portal, explaining its functionality and how it supports multi-tenant environments, centralized monitoring, and streamlined service delivery.

Finally, the course concludes with a hands-on troubleshooting session, where we cover essential diagnostic commands and options. You'll learn how to identify and correct misconfigurations, interpret system feedback, and maintain optimal performance.

3 Target Audience and Prerequisites

A prerequisite for this course is DefensePro-X Level 1 training.

This course is tailored for technical professionals with a strong foundation in networking, particularly in switching and routing concepts. A solid understanding of Border Gateway Protocol (BGP) is highly advantageous, as it enables participants to fully grasp the advanced configurations and integrations covered throughout the training.

The features and functions of Radware devices discussed in this document are based on the following firmware version.

Product	Version
CyberController-Plus	10.x
FlowDetector	2.x
DefensePro	10.x

4 Course Objectives

By the end of this course, participants will be able to:

- **Confidently install and deploy CyberController-Plus** following best practices and deployment guidelines tailored to various network environments.
- **Understand and configure a wide range of Attack Protection features**, including real-time threat detection, mitigation strategies, and integration with external security tools.
- **Grasp the core principles of AMS Analytics**, enabling effective monitoring, analysis, and interpretation of security events and performance metrics.
- **Navigate and operate the CyberController interface** with ease, utilizing its tools and dashboards to manage configurations, monitor activity, and respond to incidents efficiently

5 CyberController-Plus Presentations and Hands on Labs

5.1 Day 1

Presentations:

- **Getting Started with CyberController-Plus**
  Begin with a high-level introduction to CyberController-Plus, its purpose, and how it fits into modern cybersecurity infrastructures.
- **Technical Architecture and Capabilities**
  Explore the core components, system architecture, and operational flow of CyberController-Plus. Understand how it integrates with other security tools and supports scalable deployments.
- **Attack Simulation and Analysis**
  Walk through real-world attack scenarios using CyberController-Plus. Learn how threats are detected, analyzed, and mitigated using built-in and external detection mechanisms.
- **Security Templates and Policy Configuration**
  Discover how to use predefined security templates to streamline policy creation. Learn best practices for customizing templates to meet specific organizational needs and threat profiles.

Hands on Labs:

Administration and Initial Configuration:

- Configure Management IP and Gateway
- Configure NTP server and time zone
- Configure automatic updates for security modules
- Configure the first scrubbing center DefensePro (IP-mode)

Configure CyberController-Plus

- Check relevant licensing
- Adapt BDOS learning and attack grace period
- Configure IP settings to manage and control
- Add Router as Network Element
- Add DefensePro as Mitigation Device

Configure Use Case: DefensePro as Detector and IP-Mode DP as Scrubber

- Configure CyberController-Plus to use a DefensePro as detector
- Run an attack to see the delegation from DefensePro to DefensePro in IP-Mode

Configure Use Case: DefensePro as Detector and transparent DP as Scrubber

- Configure CyberController-Plus to use a DefensePro as detector
- Run an attack to see the delegation from DefensePro to DefensePro

5.2 Day 2

Presentations:

- **FlowDetector Deep Dive**
  Explore the functionality of FlowDetector, including how it identifies suspicious traffic patterns and contributes to proactive threat detection within the CyberController-Plus ecosystem.
- **Access Control and BGP Flowspec Integration**
  Learn how to configure and manage Access Lists and leverage BGP Flowspec for dynamic traffic filtering and mitigation. Understand how these tools enhance network security and responsiveness.
- **Managed Security Service Provider (MSSP) Portal**
  Gain hands-on experience with the MSSP Portal, including multi-tenant management, centralized monitoring, and service orchestration for distributed environments.
- **Troubleshooting and Diagnostics**
  Master essential troubleshooting techniques using diagnostic commands and tools. Learn how to identify root causes, resolve configuration issues, and maintain system health.
- **SmartTAP Best Practices**
  Discover how to implement SmartTAP effectively to optimize traffic visibility and data capture. Learn best practices for deployment, configuration, and integration with analytics platforms.

Hands on Labs:

Configure Use Case: FlowDetector as Detector and transparent DP as Scrubber

- Configure CyberController-Plus to use a FlowDetector as detector
- Run an attack to see the detection from FlowDetector

Configure Use Case: External Detector signaling an attack

- Configure CyberController-Plus to use an external device as detector
- Run an attack to see the traffic diversion to the DefensePro in the Scrubbing center based on the attack signaled from the external detector

Filter, Tuning during a live attack

- Change security policy during an attack
- Blacklist an IP address during an attack
- Use Filters to Blacklist/Whitelist traffic during an attack

MSSP Portal

Review the capabilities of the MSSP portal

Exercise configure multi step diversion

- Configure CyberController-Plus to use a DefensePro as detector and divert the traffic to different devices according to the attack bandwidth
- Run an attack to see the delegation from DefensePro to DefensePro

North America
Radware Inc.
575 Corporate Drive, Lobby 1
Mahwah, NJ 07430
Tel: +1-888-234-5763

International
Radware Ltd.
22 Raoul Wallenberg St.
Tel Aviv 69710, Israel
Tel: +972 3 766 8666