# CRDQP
# Advanced and Quick Prevention

Duration: 1 Day

## Course Overview:

This Quick Prevention sales workshop is designed for Cisco partner customer-facing teams to confidently open up security conversations with prospects and customers and then clearly articulate the Cisco Ransomware Defense value propositions.

## Prerequisites:

The knowledge and skills that the learner should have before attending this course are as follows:

- Participants should have basic understanding of Cisco IOS Network Security

## Course Objectives:

This one-day Cisco Ransomware Defense seminar has been developed in two phases:

Quick prevention and Advanced Prevention + Containment Phase I – The Cisco Ransomware workshop covers the following:

- Quick Prevention Workshop

Advanced Prevention + Containment Phase II – The Cisco Ransomware workshop provides the following hands-on labs:

- Umbrella Roaming
- AMP for Endpoints (AMP4E)
- Cloud Email Security (CES)

# Course Outline:

**Module 1: Protect users wherever they work**
- Umbrella Roaming

**Module 2: Point-in-Time Blocking, Retrospective Security and Remediation**
- AMP for Endpoints (AMP4E)

**Module 3: Cloud-managed email security**
- Cloud Email Security (CES)
- AMP option for 24/7 protection from a growing set of inbound threats

**Module 4: Software Volume Purchase Option (SVP)**
- Advanced Starter Overview

**Module 5: Looking for Ransomware Defense Opportunities**
- Security to help differentiate
- Umbrella Romain
- NGFW Service
- AMP Deployment Service
- Security SEM Service Advanced Prevention + Containment Phase

**Module 6: Infecting Your System with Ransomware**
- In this module, the system will no longer protected by the Cisco Ransomware Defense Solution products. Without this protection, you can access all malicious websites and download and run ransomware executables. Observe how quickly one can encrypt the user files and present a ransom notification demand.
- Demonstrate: Infect Your System with Ransomware Executable.

**Module 7: Cisco Cloud Email Security**
- This scenario demonstrates how Cisco Cloud Email Security protects users against email-based ransomware attacks through a malicious website link embedded in the body of an email or a malicious file attachment.
- Overview of: Email Ransomware Protection by Cisco Cloud Email Security.

**Module 8: Cisco Umbrella**
- In this module, you will be shown how to access some malicious web links, which are blocked by the Cisco Umbrella solution.
- Discuss: DNS Ransomware Protection by Cisco Umbrella.

**Module 9: Cisco AMP for Endpoints**
- In this scenario, after successfully uninstalling Cisco Umbrella, access to malware sites are allowed. This site hosts authentic working Ransomware files. Observe how Cisco AMP for Endpoints detects the ransomware and blocks the application to be executed.
- Demonstrate: File Ransomware protection by Cisco AMP for Endpoints.