



Designing and Implementing the Gigamon Inline Bypass Threat Prevention Solution

Price US\$ 1,995

Duration 2 days

DELIVERY METHODS



ILT – Instructor-Led Classroom Training

ILT sessions are conducted in a physical classroom environment.



ILO – Instructor-Led Online Training

ILO sessions are conducted via WebEx in a VoIP environment



FLEX Classroom™ – Combined ILT & ILO

FLEX Classroom sessions are delivered via ILT and ILO giving you the ultimate flexibility.

Singapore Office

60 Paya Lebar Road,
#07-17 Paya Lebar Square
Singapore 409501

Malaysia Office

No. A-1-16, Eve Suite Ara Damansara,
No. 1A, Jalan PJU 1A/41 Petaling Jaya
47301, Selangor Malaysia

Philippines Office

Unit 522 5th Floor,
Gateway Tower,
Araneta Center Cubao,
Quezon City Philippines 1109

Indonesia Office

Jl. Prof. Dr. Latumenten Raya # 7E,
Special Capital Region of Jakarta,
Indonesia

Taiwan Office

2F-15, No.12, Fuxing 4th Road
Qianzhen Dist
Kaohsiung City 806
Taiwan R.O.C.

Hong Kong Office

Suite 501, 5 Floor
The Hennessy, 256 Hennessy Road
Wan Chai
Hong Kong

Overview

The Gigamon® Inline Bypass Threat Prevention Solution is purpose-built to simultaneously maximize inline security tool performance and reliability, network resiliency and operational efficiency. The two-day Designing and Implementing Gigamon Inline Bypass Security Solution course will teach you how to best design and implement the Gigamon Inline Bypass Threat Prevention Solution to reduce costs, maximize security effectiveness and improve network resiliency.

You'll learn how to deliver the right data to the right tool at the right time, and how integrating advanced inline bypass functions helps maximize the effectiveness of security enhancement practices.

You'll learn how to deliver the right data to the right tool at the right time, and learn how integrating advanced inline bypass functions helps redistribute traffic when a tool fails and maximizes the effectiveness of the remaining security tools.

Course Description

After completing the course, you will be able to:

- Simplify architectures and enable security tools to do more, enabling faster onboarding of patches and new technology
- Help improve security posture and reduce network downtime when changing threat prevention tools
- Demonstrate competency in deploying solutions to maximize the effectiveness of your security stack

Audience

This program will appeal to:

- Professionals tasked with the implementation and support of network visibility for security, including administrators, security engineers and network engineers
- Security operations (SecOps) staff, whose priority is the security of the network
- Network operations (NetOps) staff, whose priority is network uptime

Prerequisites

Before taking the course, you should be familiar with:

- Gigamon solution fundamentals around network visibility
- Inline tools like ATP, IPS and WAF

- GigaSMART® software features, uses and configuration

Note: One way to get up to speed on these necessary skills is to complete the Gigamon Foundation course. See the Educational Services web page for details.

Course Delivery

This two-day course is delivered through a variety of methods, including:

- Instructor Led Training (ILT)
- Instructor Led Online (ILO)

Course Modules

This course includes approximately 12 hours of instruction time, including hands-on labs and several discrete, sequential modules that walk you through the materials covered:

1. GigaSECURE® Security Delivery Platform Overview
2. Inline Bypass Foundations
3. Design Considerations for the Inline Bypass Threat Prevention Solution
4. Flexible Inline Arrangements
5. Provisioning High Availability
6. Gigamon Inline SSL Decryption Design and Implementation

Course Goals

After completing this course, you will be able to understand:

- Data requirements for inline security and network analysis tools
- Approaches and considerations for packet access for inline tools
- Traffic sizing for inline security and network analysis tools
- How to filter traffic to meet the needs of security tools.
- Load sharing between inline security and network analysis tools
- How to implement tool groupings for inline processing
- Traffic management for inline processing
- How to replicate traffic to out-of-band tools for augmenting inline security

Overall, you'll gain the skills needed to design and implement solutions that scale inline threat prevention tools, stop tool sprawl and contain costs.