Enterprise Computing Solutions - Education Services

# TRAINING OFFERING

**You can reach us at:**

Arrow ECS B.V., Kromme Schaft 5, 3991 AR Houten, The Netherlands

Email: education.ecs.nl@arrow.com
Phone: +31 20 582 6109

# TippingPoint IPS 5-day Technical Security Products with Certification

| CODE: | LENGTH: | PRICE: |
|---|---|---|
| TRM_TP IPS-SMS | 40 Hours (5 days) | €3,750.00 |

## Description

Tippingpoint Expert Technical Security products Training is a five-day course that teaches expert-level concepts and best practices necessary for implementation planning, installation, configuration, security management, and system administration of the Tippingpoint solution. Through interactive lectures and hands-on labs, students will learn to implement the intrusion prevention System (ipS) and the Security Management System (SMS) using the standard interface modes. Students will also acquire in-depth expert knowledge of how to tune and configure a Tippingpoint ipS for optimum performance on their network and learn advanced configuration management of multiple ipS's using the SMS.

## Objectives

upon completion of this course, students will acquire knowledge of the TippingPoint solution including:
• Fundamental security concepts
• IPS setup and configuration
• SMS setup and configuration
• deployment architecture and scenarios
• Administrative best practices

## Audience

Network engineers, network administrators, network technicians, security administrators, systems engineers, system administrators, and network security strategies, and planning architects.

## Prerequisites

TippingPoint Advanced Security Training or equivalent hands-on experience using the TippingPoint solution.

## Programme

**Device configuration**
- SMS <> IPS communication
- layer 2 fallback
- link down synchronization
- Zero power high availability
- device configuration
- network configuration
- VIAn translation
- ToS update
- IPS system snapshots
- IPS password recovery

**Advanced policy**
- Flow-based inspection filters vs. other techniques

**IPS Setup and configuration**
- TippingPoint product portfolio
- digital Vaccine
- Threat Management center (TMc)
- IPS and SMS initial setup at-a-glance
- IPS oBE
- IPS user account management
- Training lab overview

**SMS Setup and configuration**
- SMS oBE
- Adding IPS to SMS management
- SMS user administration
- SMS security preferences
- SMS named resources
- digital Vaccine management

**DV labs**
- digital Vaccine (Base)
- Basics of filters
- digital Vaccine contents
- category breakdown
- recommended settings
- Application digital Vaccine®
- Web Application digital Vaccine® Service
- digital Vaccine® Security Filter Service
- reputation digital Vaccine® Service
- TMc, ThreatlinQ
- The TippingPoint Solution

**Basic policy**
- Segment groups and policy
- Segment group management
- Filter categories
- rPc dcoM attack example
- TippingPoint Threat Suppression Engine
- TippingPoint Architecture
- TSE managed streams
- Security profiles
- Filter configuration best practices
- Filter search examples
- Shared settings: Action sets
- Shared settings: notification contacts
- notes on aggregation periods
- Shared settings: services
- Profile versioning
- Profile distribution schedules
- reviewing which profile is on a segment

**Digital Vaccine Toolkit**
- dV Toolkit (dVT)
- creating a new filter
- dVT filter payload
- dVT package management
- dVT testing
- dVT FTP PuT example

**SMS Management**
- SMS software updates
- SMS database administration
- SMS database backup
- SMS high availability
- SMS event handling architecture
- SMS events
- configuring SMS syslog
- SMS external database settings
- SMS API
- SMS reports
- SMS dashboard clI & ISM Management
- ISM navigation overview
- Security profiles
- Virtual ports
- IPS preferences
- default IPS settings
- ISM Filter configuration
- category settings
- ISM events
- re-managing with SMS
- Importing a profile
- Profile compare

**Non- DV Filters**
- non-DV filtering techniques (non-flow)
- Port scan/host sweeps
- Traffic threshold filters
- Traffic management filters
- IP/dnS reputation

**Advanced DDoS**
- Syn flood attacks
- connection based attacks
- AddoS platform support
- AddoS configuration
- AddoS events and reports

**IPS Quarantine**
- IPS quarantine concepts
- IPS quarantine considerations
- IPS quarantine action set
- IPS quarantine automatic timeout
- IPS quarantine monitoring

- recommended settings
- IPS profile management
- Editing filters
- Active vs distributed
- Security overview
- TippingPoint and Security

**Architecture and performance optimization**
- n-Platform architecture
- optimizing performance
- Transparent network high availability
- Filter flow discussion
- deployment scenario

**Advanced deployments**
- Policy by direction
- Policy by VlAn
- Policy by cldr
- Policy precedence and application

**SMS responder**
- SMS responder external initiation
- Manual initiation using the SMS event viewer
- External initiation using the SMS Web API
- External initiation from IPS quarantine
- SMS responder correlation and thresholding
- Post lab timing

## Options

**Certifications and Related Examinations**
- ASE - TippingPoint Security V2
- Implementing TippingPoint Solutions

## Session Dates

On request. Please contact us

## Additional Information

This training is also available as onsite training. Please contact us to find out more.