

Trend Micro TippingPoint Certified Expert

Dieser fünftägige Kurs vermittelt den Teilnehmern Konzepte auf Expert-Level-Niveau und Best Practices für die Implementierungsplanung, Installation, Konfiguration, Sicherheitsverwaltung und Systemadministration der TippingPoint-Lösung. Durch interaktive Inhalte und praktische Übungen lernen sie die Implementierung des Intrusion Prevention System (IPS) und des Security Management System (SMS) mittels Standard Interface Modes. Weiterhin erwerben sie fundierte Fachkenntnisse darüber, wie ein TippingPoint IPS für optimale Leistung in ihrem Netzwerk optimiert und konfiguriert wird und wie ein Konfigurations-Management von mehreren IPS mit Hilfe der SMS funktioniert. Nach Abschluss des Kurses können die Teilnehmer eine Zertifizierungsprüfung ablegen. Die Prüfung ist im Kurspreis inkludiert.

Kursinhalt

- Device Setup und Konfiguration
- Policy Management
- SMS Setup und Konfiguration
- DV Filter und Policies
- Best Practices für die Administration
- SMS und Deep Discovery Interation

Jeder Teilnehmer erhält gedruckte Kursunterlagen von Trend Micro in englischer Sprache.

Zielgruppe

Der Kurs richtet sich an Ingenieure, Administratoren, Techniker und Architekten in den Bereichen Netzwerk, Security und Planung.

Voraussetzungen

Die Teilnehmer sollten vorab das web-basierte Tipping Point Essentials-Training absolvieren.

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.expertech.de/go/TMTI

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training		Preise zzgl. MwSt.
Classroom Training	5 Tage	€ 2.995,-
Termin/Kursort		
14.10.-18.10.19 Frankfurt		

Stand 16.03.2019



Inhaltsverzeichnis

Trend Micro TippingPoint Certified Expert

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

Device Configuration

SMS IPS communication
Layer 2 fallback
Link down synchronization
Zero power high availability
Device configuration
Network configuration

VLAN translation
TOS update
IPS system snapshots
IPS password recovery

Advanced Policy

Flow-based inspection filters vs. other techniques
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 & LSM Management
LSM navigation overview
Security profiles
Virtual ports
IPS preferences
Default IPS settings
LSM Filter configuration

Category settings
LSM 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
ADD oS platform support
ADD oS configuration
ADD oS events and reports

IPS Quarantine

IPS quarantine concepts
IPS quarantine considerations
IPS quarantine action set
IPS quarantine automatic timeout
IPS quarantine monitoring

Advanced Deployments

Policy by direction
Policy by VLAN
Policy by CIDR
Policy precedence and application

Architecture and Performance Optimization

N-Platform architecture
Optimizing performance
Transparent network high availability
Filter flow discussion
Deployment scenario

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



ExperTeach GmbH

Waldstraße 94 • 63128 Dietzenbach • Telefon: +49 6074 4868-0 • Fax: +49 6074 4868-109
info@exper teach.de • www.exper teach.de

