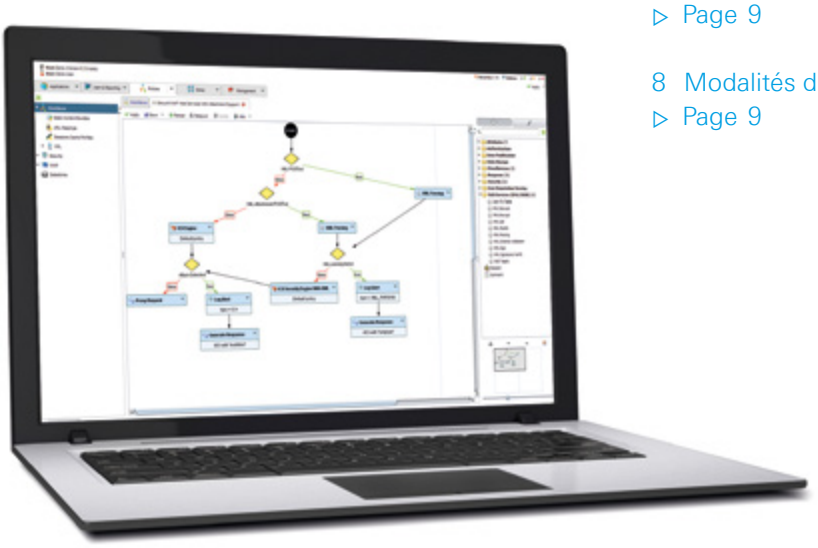
Application Security
Catalogue des formations 2019

ROHDE&SCHWARZ
Cybersecurity

Sommaire



1 Introduction

Rohde&Schwarz Cybersecurity propose à ses clients et partenaires un choix de formations certifiantes couvrant l'ensemble du cycle de mise en œuvre de ses produits Application Security. Les stagiaires peuvent également parfaire leur connaissance de la sécurité applicative, en suivant notamment un module portant sur le panorama des attaques Applicatives Web.

Que la mise œuvre soit assurée par le client lui-même, par un partenaire, ou par Rohde&Schwarz Cybersecurity, il est essentiel que les ingénieurs mettant en œuvre ou exploitant les solutions soient formés et disposent d'un niveau technique suffisant pour assurer une sécurité efficace des applications et services web. Les formations proposées s'adressent donc aux ingénieurs d'étude et d'exploitation, et dans une certaine mesure aux maîtrises d'ouvrage qui souhaitent s'impliquer dans la protection des applications qu'ils mettent à la disposition de leurs utilisateurs ou partenaires.

L'ensemble de ces formations sont délivrées par des experts techniques opérant au sein de Rohde&Schwarz Cybersecurity depuis de nombreuses années. Les dates indiquées se déroulent dans les locaux de Rohde&Schwarz Cybersecurity SAS à Meudon. Pour répondre aux besoins spécifiques de certains projets, nous proposons également des sessions de formation intra-entreprise personnalisées en fonction des contraintes. Enfin, il est possible, sous certaines conditions, de définir un programme dit « custom » sur un périmètre précis et un temps déterminé.

Les modules de formations décrits dans ce présent catalogue sont délivrés en français. Merci de vous référer aux versions anglaise ou allemande pour d'autres langages.

2 Planning

	R&S®Web Application Firewall	Web Access Manager	API Security
Durée	**3 jours**	**2 jours**	**2 jours**
Janvier	28-30	-	30-1st
Février	-	-	-
Mars	4-6	11-12	7-8
Avril	-	-	-
Mai	-	-	-
Juin	3-5	17-18	6-7
Juillet	-	-	-
Août	-	-	-
Septembre	9-11	16-17	12-13
Octobre	-	-	-
Novembre	-	-	-
Décembre	2-4	9-10	5-6

3 R&S®Web Application Firewall

3.1 Détails de la formation

Durée	3 jours
Price	3.000 €
Audience	Ingénieurs et Administrateurs Sécurité
Contenu	50 % théorie / 50 % pratique
Certification	oui

Cette formation se faisant avec la dernière version stable du produit R&S®Web Application Firewall, son contenu est par conséquent régulièrement mis à jour afin d'y intégrer les dernières fonctionnalités et innovations. En conséquence, l'agenda décrit ci-dessous peut être amené à être légèrement différent tout en gardant bien entendu les lignes directrices constituant les bases nécessaires à l'exploitation de la solution. Chaque module se compose d'une partie théorie dans un premier temps, suivie d'une seconde partie, pratique cette fois, à travers différents ateliers.

3.2 Agenda

- Introduction
  - Présentation globale
  - Produits et intégration
  - Support et espace client
- HTTP
  - Bases HTTP
  - Transactions importantes
  - Concepts SSL
  - Expressions régulières
- Installation
- Challenges

- Workflow
  - Concept et bases
  - Gestion
  - Modification des flux
  - Request limiter
- Politique de sécurité ICX
  - Concept
  - Mise à jour
- Sécurité avancée
  - IP Réputation
  - Réputation utilisateur
  - Sitemap et liste blanche
  - Scoring Lsite
  - Normalisation
  - Autres moteurs
- Authentification
- Introduction

- Gestion des faux positifs
  - Résolution automatique
  - Résolution custom
  - Rejeu des requêtes
- Haute-disponibilité
- Load-Balancing
- Gestion des logs
- Alertes et Reporting
- Actions programmées
- Monitoring
- Certification (1h)
- Challenges

4 Web Access Manager

4.1 Détails de la formation

Durée	2 jours
Price	2.000 €
Audience	Ingénieurs et Administrateurs Sécurité
Contenu	50 % théorie / 50 % pratique
Certification	non

L'objectif de cette formation est l'obtention des connaissances et de l'expérience nécessaires pour mettre en place, maintenir, et diagnostiquer une authentification de type Web SSO. Cette formation se faisant avec la dernière version stable du produit R&S®Web Application Firewall, son contenu est par conséquent régulièrement mis à jour afin d'y intégrer les dernières fonctionnalités et innovations. En conséquence, l'agenda décrit ci-dessous peut être amené à être légèrement différent tout en gardant bien entendu les lignes directrices constituant les bases nécessaires à l'exploitation de la solution. Chaque module se compose d'une partie théorie dans un premier temps, suivie d'une seconde partie, pratique cette fois, à travers différents ateliers.

4.2 Agenda

- Authentification périmétrique
- Web SSO
  - SQL
  - LDAP
  - RADIUS
  - Multi facteurs
- Politiques d'autorisation
- Gestion des logs
- Customisations possibles
- Dépannage et diagnostique
- Challenges

5 Sécurité API

5.1 Détails de la formation

Durée	2 jours
Price	2.000 €
Audience	Ingénieurs et Administrateurs Sécurité
Contenu	50 % théorie / 50 % pratique
Certification	non

L'objectif de cette formation est l'obtention des connaissances et de l'expérience nécessaires pour mettre en place, maintenir, et diagnostiquer une sécurité portée sur les Web Services. Cette formation se faisant avec la dernière version stable du produit R&S®Web Application Firewall, son contenu est par conséquent régulièrement mis à jour afin d'y intégrer les dernières fonctionnalités et innovations. En conséquence, l'agenda décrit ci-dessous peut être amené à être légèrement différent tout en gardant bien entendu les lignes directrices constituant les bases nécessaires à l'exploitation de la solution. Chaque module se compose d'une partie théorie dans un premier temps, suivie d'une seconde partie, pratique cette fois, à travers différents ateliers

5.2 Agenda

- Conformité de schémas
- Parsing XML/JSON
- Encription
- Signature
- Gestion des tokens JWT
- Utilisation d'un fichier Swagger
- Transformations XSLT
- Dépannage et diagnostique
- Challenges

6 Attaques Applicatives Web

6.1 Détails de la formation

Durée	3 jourss
Price	4.500 €
Audience	Equipes de Sécurité, SOC, pentesteurs
Contenu	50 % théorie / 50 % pratique
Certification	non

A la fin de cette formation, chaque participant sera capable de :

- Identifier les familles de vulnérabilités spécifiques aux applications Web (XSS, Injections SQL/XML/HTML, CSRF, SSRF, XXE)
- Exploiter les vulnérabilités précédemment identifiées
- Contourner des filtres de défenses basiques
- Manipuler les outils les plus courants
- Adapter ces outils à leurs besoins spécifiques

6.2 Agenda

- Rappels sur HTTP
  - Requêtes et réponses
  - Gestion des états et du cache
  - Redirection
  - Authentification
  - Chiffrement
  - Actions implicites du navigateur
- Attaques courantes
  - Introduction au top 10 de l'OWASP (injection HTML et SQL, IDOR, CSRF)
  - Exemples réels
- Outillage
  - Extensions des navigateurs
  - Proxy (ZAP, Burp Suite)
- Exercices pratiques (injection SQL, manipulation de données, cassage de mots de passe, extraction de données)
- Exploitation avancée
  - Accès au système de fichiers
  - Contournement de filtres de protection
  - Exploitation en masse
  - Enchaînement de techniques
- Vulnérabilités hors top 10 de l'OWASP
  - Théorie d'attaques modernes (injection JSONP, SSRF, XXE)
  - Pratique

7 Prérequis

7.1 Matériel

Un accès réseau adéquate est fourni à l'ensemble des participants. L'ensemble des formations se font à travers un environnement de lab virtualisé. Chaque stagiaire, afin d'accéder à cet environnement, devra se munir du matériel suivant :

- Un ordinateur portable 64-avec un minimum de 4 GB de RAM
- Un navigateur internet graphique récent, de type Firefox ou Chrome
- Une solution de virtualisation telle que VMware ou VirtualBox

7.2 Connaissances pour l'ensemble des formations

- Connaissances approfondies des protocoles HTTP/HTTPS et TCP/IP
- Connaissances des technologies reverse proxy
- Maîtrise des expressions régulières
- Connaissance du top10 de l'OWASP

7.3 Connaissances spécifiques pour la formation Web Access Manager

- Connaissances des différents types d'authentification applicatives
- Connaissances des protocoles LDAP / Active directory / PKI

7.4 Connaissances spécifiques pour la formation API Security

- Connaissances des standards XML et JSON
- Connaissances de la terminologie des Web Services

8 Modalités d'inscription et paiement

Tout enregistrement en ligne peut se faire à travers l'URL suivante

www.rohde-schwarz.com/cybersecurity/training

L'enregistrement peut également se faire directement en prenant contact avec votre responsable commercial au sein de Rohde&Schwarz Cybersecurity.

Tout paiement devra se faire par transfert bancaire et déclenchera systématiquement la réservation définitive de votre place, celle-ci n'étant que provisoirement assurée avant cela. Toute annulation doit se faire dans un délai de 15 jours minimum avant le premier jour de la formation. Passé ce délai, la formation sera due.

Service à valeur ajoutée

- Mondial
- Local et personnalisé
- Spécifique au client et flexible
- Qualité sans compromis
- Fiabilité à long term

Rohde&Schwarz Cybersecurity
Rohde&Schwarz Cybersecurity est une société de sécurité informatique qui protège les entreprises et les institutions publiques du monde entier contre les cyberattaques. Avec plus de 500 employés, la société développe et produit des solutions technologiques de pointe pour la sécurité des informations et des réseaux. Pour prévenir les cyberattaques de manière proactive, plutôt que réactive, nos solutions informatiques de confiance sont développées selon l'approche de la sécurité par design.

Rohde&Schwarz
Groupe spécialisé en électronique, Rohde & Schwarz offre des solutions innovantes dans les domaines d'activité suivants : test et mesure, broadcast et médias, communications sécurisées, cybersécurité, surveillance et test des réseaux. Fondée il y a plus de 80 ans, l'entreprise indépendante dont la maison mère est installée en Allemagne, à Munich, est présente dans plus de 70 pays avec un réseau étendu de vente et de service.

Rohde&Schwarz Cybersecurity SAS
Parc Tertiaire de Meudon
9-11 Rue Jeanne Braconnier | 92366 Meudon, France
Info: +33 (0)1 46 20 96 00
Email: sales-fr.cybersecurity@rohde-schwarz.com

Rohde&Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich, Allemagne
www.rohde-schwarz.com/cybersecurity

Rohde&Schwarz GmbH&Co. KG
www.rohde-schwarz.com

PD 5216.4479.63 | Version 01.00 | février 2019 (sch)
Application Security Catalogue des formations 2019
Données sans tolérance : sans obligation | Sous réserve de modification

5216447963

5216.4479.63 01.00 PDP 1 fr