

إدارة وأمن جدار حماية تطبيقات الويب (WAF)

FortiWeb

UK Traininig

PARTNER



إدارة وأمن جدار حماية تطبيقات الويب (FortiWeb (WAF

مقدمة

أصبحت تطبيقات الويب تمثل ركيزة أساسية في تقديم الخدمات الرقمية داخل المؤسسات الحكومية والخاصة، حيث تعتمد عليها العمليات التشغيلية، والخدمات الإلكترونية، وإدارة البيانات، والمعاملات المالية. ومع التوسع المستمر في استخدام هذه التطبيقات، ازدادت التهديدات السيبرانية التي تستهدفها، مما جعل حماية تطبيقات الويب من الأولويات الإستراتيجية لضمان استمرارية الأعمال، والحفاظ على سرية المعلومات، وسلامة الأنظمة، وتوافر الخدمات.

وتعد منصة FortiWeb من الحلول المتخصصة في حماية تطبيقات الويب، حيث توفر إمكانيات متقدمة لمراقبة حركة البيانات، وتحليل الطلبات، واكتشاف الأنشطة الضارة، وتطبيق سياسات أمنية فعالة تسهم في التصدي للهجمات الإلكترونية، وتعزيز أمن التطبيقات، والحد من المخاطر الأمنية التي قد تؤثر في بيئات العمل الرقمية.

توفر هذه الدورة فهماً متكاملاً لمفاهيم جدار حماية تطبيقات الويب، وآليات عمل منصة FortiWeb، وأساليب نشرها وإدارتها داخل المؤسسات، مع التركيز على إعداد سياسات الحماية، وإدارة ملفات التعريف الأمنية، وتحليل حركة البيانات، ومراقبة الأحداث الأمنية، وإدارة السجلات، وتحسين الأداء، واستكشاف المشكلات الفنية، وتطبيق أفضل الممارسات في حماية تطبيقات الويب.

كما تستعرض الدورة أبرز المخاطر الأمنية التي تستهدف تطبيقات الويب، وأشهر الثغرات الأمنية، وأساليب الوقاية منها، بالإضافة إلى آليات التكامل مع منظومة الأمن السيبراني داخل المؤسسة، بما يعزز مستوى الحماية، ويرفع كفاءة إدارة أمن التطبيقات، ويدعم استمرارية الأعمال في بيئات العمل الحديثة.

أهداف الدورة

بنهاية هذه الدورة سيكون المشاركون قادرين على:

UK Training

PARTNER



- فهم المفاهيم الأساسية لجدران حماية تطبيقات الويب ودورها في حماية التطبيقات والخدمات الرقمية.
- التعرف على بنية منصة FortiWeb ومكوناتها وآلية عملها داخل بيئات العمل المؤسسية.
- نشر وتهيئة منصة FortiWeb وفق أفضل الممارسات الأمنية.
- التعرف على أبرز الثغرات الأمنية التي تستهدف تطبيقات الويب وسبل الحد من مخاطرها.
- إعداد سياسات حماية تطبيقات الويب بما يتوافق مع متطلبات المؤسسة.
- إنشاء وإدارة ملفات التعريف الأمنية الخاصة بحماية التطبيقات.
- مراقبة وتحليل حركة البيانات الواردة والصادرة واكتشاف الأنشطة غير الطبيعية.
- إدارة سياسات التحكم في الوصول وتعزيز أمن المستخدمين والتطبيقات.
- حماية تطبيقات الويب من هجمات حقن قواعد البيانات، وهجمات البرمجة النصية عبر المواقع، وغيرها من الهجمات الإلكترونية الشائعة.
- مراقبة السجلات والأحداث الأمنية وإعداد التقارير الداعمة لاتخاذ القرارات الأمنية.
- استكشاف المشكلات الفنية في منصة FortiWeb وتحسين كفاءتها التشغيلية.
- تطبيق أفضل الممارسات العالمية لإدارة أمن تطبيقات الويب وتعزيز مستوى الحماية داخل المؤسسات.

محاورة الدورة

اليوم الأول: أساسيات أمن تطبيقات الويب ومنصة FortiWeb

- المفاهيم الأساسية لأمن تطبيقات الويب وأهميته في الأمن السيبراني.
- أبرز التهديدات والثغرات الأمنية التي تستهدف تطبيقات الويب.
- أشهر المخاطر الأمنية التي تواجه تطبيقات الويب وطرق الحد منها.
- التعرف على بنية منصة FortiWeb ومكوناتها الرئيسية.
- أساليب نشر المنصة داخل بيئات العمل المختلفة.
- تثبيت النظام وإجراء الإعدادات الأولية.
- إدارة النظام والتعرف على أدوات الإدارة الرئيسية.

UK Training

PARTNER



اليوم الثاني: سياسات الحماية وإدارة ملفات التعريف الأمنية

- إنشاء وإدارة سياسات حماية تطبيقات الويب.
- إعداد ملفات التعريف الأمنية وتخصيصها وفق احتياجات المؤسسة.
- فحص وتحليل حركة البيانات الخاصة بتطبيقات الويب.
- إدارة سياسات التحكم في الوصول إلى الصفحات والخدمات.
- إدارة مصادقة المستخدمين وآليات التحكم في الصلاحيات.
- حماية جلسات المستخدمين وتعزيز أمن الوصول.
- مراجعة سياسات الحماية وتحسين كفاءتها.

اليوم الثالث: الحماية من الهجمات الإلكترونية

- الحماية من هجمات حقن قواعد البيانات.
- الحماية من هجمات البرمجة النصية عبر المواقع.
- الحماية من هجمات حقن الأوامر وإدراج الملفات الضارة.
- اكتشاف وإدارة البرمجيات الضارة.
- الحماية من هجمات حجب الخدمة وهجمات حجب الخدمة الموزعة.
- إدارة آليات اكتشاف الهجمات والاستجابة لها.
- تحليل الأحداث والتنبيهات الأمنية.

اليوم الرابع: المراقبة وإدارة السجلات وإعداد التقارير

- إدارة وتحليل سجلات النظام والأحداث الأمنية.
- مراقبة الأنشطة الأمنية بصورة مستمرة.
- إعداد وإدارة التنبيهات الأمنية.
- تصميم لوحات متابعة الأداء والمؤشرات الأمنية.
- إعداد التقارير الأمنية وتقارير الالتزام بالمتطلبات التنظيمية.
- التحقيق في الحوادث الأمنية وتحليل أسبابها.
- التكامل مع أنظمة إدارة معلومات وأحداث الأمن.



اليوم الخامس: تحسين الأداء والإدارة المتقدمة وأفضل الممارسات

- استكشاف المشكلات الشائعة في منصة FortiWeb ومعالجتها.
- تحسين الأداء ورفع الكفاءة التشغيلية.
- إدارة التوافر العالي لضمان استمرارية الخدمة.
- تنفيذ عمليات النسخ الاحتياطي واستعادة إعدادات النظام.
- صيانة المنصة وإدارة التحديثات الأمنية.
- أفضل الممارسات العالمية في إدارة وأمن جدار حماية تطبيقات الويب.
- تطوير إستراتيجية متكاملة لتعزيز أمن تطبيقات الويب داخل المؤسسة.

لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- اكتساب فهم شامل لمفاهيم جدار حماية تطبيقات الويب ودوره في حماية الخدمات الرقمية.
- التعرف على آلية عمل منصة FortiWeb وإمكاناتها في تأمين تطبيقات الويب.
- تطوير القدرة على إعداد سياسات الحماية وتثبيتها بما يتوافق مع احتياجات المؤسسة.
- تعزيز مهارات اكتشاف الهجمات الإلكترونية وتحليلها والاستجابة لها.
- تحسين القدرة على حماية تطبيقات الويب من أبرز الثغرات والهجمات الأمنية.
- رفع كفاءة مراقبة الأحداث الأمنية وتحليل السجلات وإعداد التقارير.
- التعرف على أفضل الممارسات في إدارة أمن تطبيقات الويب وتحسين مستوى الحماية.
- تحسين أداء منصة FortiWeb وضمان استمرارية الخدمات الرقمية.
- دعم الامتثال للسياسات الأمنية والمتطلبات التنظيمية الخاصة بحماية المعلومات.
- تعزيز قدرة المؤسسة على الحد من المخاطر الأمنية وتحسين جاهزيتها لمواجهة التهديدات السيبرانية.

الخاتمة

أصبحت حماية تطبيقات الويب عنصرًا أساسيًا في إستراتيجيات الأمن السيبراني، نظرًا لاعتماد المؤسسات المتزايد على الخدمات الرقمية والتطبيقات الإلكترونية في إدارة أعمالها وتقديم خدماتها. ويتطلب ذلك حلولًا متخصصة قادرة على حماية التطبيقات من التهديدات المتقدمة، وتعزيز أمن البيانات، وضمان استمرارية الخدمات، مع الحفاظ على الأداء والكفاءة التشغيلية.

توفر هذه الدورة فهمًا متكاملًا لمفاهيم إدارة وأمن جدار حماية تطبيقات الويب باستخدام منصة FortiWeb، بدءًا من التعرف على بنية النظام، وإعداد سياسات الحماية، وإدارة ملفات التعريف الأمنية، مرورًا بحماية التطبيقات من الهجمات الإلكترونية، ومراقبة الأحداث الأمنية، وتحليل السجلات، وصولًا إلى تحسين الأداء، وإدارة التوافر العالي، وتطبيق أفضل الممارسات في إدارة أمن تطبيقات الويب.

UK Training

PARTNER



ومن خلال الإلمام بالمفاهيم والمنهجيات الحديثة المستخدمة في حماية تطبيقات الويب، سيتمكن المشاركون من تعزيز قدراتهم في إدارة حلول الحماية، وتحسين كفاءة الاستجابة للتهديدات، ورفع مستوى أمن التطبيقات والخدمات الرقمية، ودعم الامتثال للمتطلبات التنظيمية، بما يساهم في بناء بيئة تقنية أكثر أماناً واستقراراً، وتعزيز جاهزية المؤسسات لمواجهة التحديات الأمنية المتزايدة في عالم التحول الرقمي.

الأسئلة الشائعة

ما هو FortiWeb، ولماذا يُعد مهماً لحماية تطبيقات الويب؟

يُعد FortiWeb أحد أبرز حلول جدار حماية تطبيقات الويب WAF، حيث يوفر حماية متقدمة ضد الهجمات الإلكترونية مثل حقن أوامر SQL، وهجمات البرمجة عبر المواقع XSS، وإدراج الملفات الضارة، وهجمات حجب الخدمة. توضح هذه الدورة مفهوم FortiWeb، وآلية عمل FortiWeb Web Application Firewall، ودوره في تعزيز أمن تطبيقات الويب ضمن بيئات الأمن السيبراني الحديثة.

ما هو جدار حماية تطبيقات الويب WAF، وكيف يعمل؟

جدار حماية تطبيقات الويب WAF هو نظام أمني يقوم بمراقبة حركة مرور بروتوكولي HTTP و HTTPS وتحليلها وتصنيفها قبل وصولها إلى التطبيقات. تشرح الدورة مفهوم Web Application Firewall، وآلية عمله، وكيفية استخدام قواعد جدار حماية تطبيقات الويب Web Application Firewall Rules للكشف عن الهجمات الإلكترونية ومنعها وحماية التطبيقات من التهديدات المختلفة.

هل تغطي الدورة حلول جدار حماية تطبيقات الويب السحابية؟

نعم، تستعرض الدورة حلول جدار حماية تطبيقات الويب السحابية، بما في ذلك AWS WAF و AWS Web Application Firewall و Azure Web Application Firewall، مع توضيح نماذج النشر المختلفة، ومزايا كل حل، وأفضل الممارسات لاختيار الحل الأنسب لحماية التطبيقات المستضافة في البيئات السحابية.

ما المهارات العملية التي سأكتسبها من دورة FortiWeb؟

سيكتسب المشاركون خبرة عملية في تثبيت وإعداد وإدارة FortiWeb، وإنشاء سياسات الحماية، وإعداد ملفات حماية التطبيقات، وتحليل حركة المرور، ومراقبة السجلات والأحداث الأمنية، وتحسين الأداء، وإعداد التوافر العالي HA، ومعالجة الأعطال، إضافة إلى حماية التطبيقات من أبرز مخاطر OWASP Top 10.

UK Training

PARTNER



من الفئة المستهدفة لهذه الدورة؟

طُفمت الدورة لمهندسي الأمن السيراني، ومهندسي الشبكات، ومسؤولي الأنظمة، ومتخصصي أمن السحابة، ومحلي مراكز العمليات الأمنية SOC، وجميع المتخصصين المسؤولين عن حماية تطبيقات الويب، وإدارة جدران حماية تطبيقات الويب، وتطبيق حلول أمنية متقدمة لحماية البنية التحتية الرقمية للمؤسسات.

UK Traininig

PARTNER

