گروه شرکت‌های افق اندیشه

مشاورین شبکه افق اندیشه

میتا وف

MITA WAF

آذر ۱۴۰۴

مشخصات شرکت تولید کننده:

نام شرکت:	مشاورین شبکه افق اندیشه
آیا شرکت دانش‌بنیان است؟ بله ■ خیر □	نوع: فناور
شناسه ملی :	۱۰۲۲۰۱۰۵۳۳۸
وب سایت:	www.oanc.ir www.mitautm.ir
آدرس پست الکترونیک :	info@oanc.ir
تلفن:	۰۲۱۸۸۶۲۵۰۰۷
فاکس:	۰۲۱۸۸۶۲۵۰۰۶

مشخصات پرسنل شامل:

تعداد کارکنان :	دفتر تهران ۳۴ نفر دفتر ارومیه ۱۶ نفر

استانداردها، گواهینامه ها و مجوزهای اخذ شده شرکت

نوع دستاورد	عنوان محصول	محل اخذ	شماره	
مجوز دانش بنیان	سیستم مدیریت یکپارچه تهدیدات امنیتی میتا	معاونت علمی		
کارت بازرگانی		اتاق بازرگانی صنایع معادن و کشاورزی	۱۰۲۲۰۱۰۵۳۳۸	
گواهی ارزیابی امنیتی محصول	سیستم مدیریت یکپارچه تهدیدات امنیتی میتا	مرکز مدیریت راهبردی افتا ریاست جمهوری	CBP-C108-0201	
گواهی ارزیابی امنیتی محصول	سیستم مدیریت یکپارچه تهدیدات امنیتی میتا	سازمان فناوری اطلاعات ایران	CBP-C108-0201	
گواهینامه ثبت علامت	سیستم مدیریت یکپارچه تهدیدات امنیتی میتا	سازمان ثبت اسناد و املاک کشور	۰۴۹۴۹۲	
گواهینامه تایید فنی نرم افزار	سیستم مدیریت یکپارچه تهدیدات امنیتی میتا	معاونت برنامه ریزی و نظارت راهبردی	۹۴۰۹ – ۲۷/۲۰	
گواهینامه ثبت اختراع	سیستم مدیریت یکپارچه تهدیدات امنیتی میتا	سازمان ثبت اسناد و املاک کشور	۰۰۷۵۳۵	
پروانه فعالیت در حوزه خدمات عملیاتی افتا	امن سازی و مقاوم سازی سامانه ها، زیرساختها و سرویس ها	سازمان فناوری اطلاعات ایران و افتای ریاست جمهوری	۱۰۲۰۱۲۳	
پروانه صلاحیت ارائه خدمات در حوزه پدافند سایبری	امنیت فناوری اطلاعات	سازمان پدافند غیر عامل کشور	۱۶۳/ق/س/۱۴۰۰/۱۲	
گواهینامه صلاحیت خدمات انفورماتیکی		سازمان برنامه و بودجه کشور	۲۵۳۳۱۷	

گروه شرکت‌های افق اندیشه

مشخصات محصول

عنوان فارسی: میتا وف
عنوان انگلیسی: Mita **WAF**
ماژول وف میتا تحت عنوان یک فایروال برنامه های کاربردی تحت وب بشکل یک دژ مستحکم با بررسی ترافیک HTTP و HTTPS با بهره گیری از قواعد پرمیوم OWASPو قابلیت پشتیبانی از بیش از ۴۰،۰۰۰ قاعده و بروزرسانی قواعد از سرورهای میتا از وب‌اپلیکیشن‌های سازمان محافظت می کند .

معرفی جامع محصول

WAF یا فایروال برنامه‌های تحت وب یک راهکار امنیتی پیشرفته است که برای محافظت از وب‌سایت‌ها و سرویس‌های آنلاین در برابر تهدیدات لایه کاربرد طراحی شده است. برخلاف فایروال‌های سنتی که روی لایه شبکه تمرکز دارند، WAF در لایه ۷ (Application Layer) فعالیت می‌کند و توانایی تحلیل عمیق درخواست‌های HTTP/HTTPS را دارد. این محصول با پایش و فیلتر کردن هوشمند ترافیک، حملات مخرب را در لحظه شناسایی و مسدود می‌کند.

هدف و ضرورت محصول	**شناسایی و بلاک کردن حملات برنامه های تحت وب**
کاربرد محصول	**امنیت سایبری، مقابله با حملات برنامه های تحت وب، محصول تخصصی در خصوص مقابله با حملات وب**
فعالیت‌ها و خروجی‌های اصلی	**کشف و شناسایی و بلاک کردن حملات برنامه های تحت وب**
بهره‌برداران	**تمام کاربرانی حقیقی و حقوقی که سرویس های مبتنی بر وب و درگاهای API را ارایه میدهند.** **حوزه پوشش** **B2C** **B2B** **B2Gاست.**
معماری، اجزای سیستم و ارتباطات	• **Traffic Entry Layer (Reverse Proxy / Edge Layer)** • **Core Inspection Engine (L7 Analysis Layer)** • **Policy Decision & Enforcement Layer** • **Threat Intelligence** • **Logging, Monitoring, and Analytics Layer** • **Management & Configuration Layer**
کارکردها و فرایندهای سیستم	**کشف و بلاک کردن حملات برنامه های تحت وب**

فازها و زمان‌بندی توسعه محصول

در این بخش فازهای پروژه و زمان برآورد شده برای انجام هر فاز ارائه شود. (فازها و زمان‌بندی ارائه شده در این بخش مبنای بازدید و ارزیابی محصول خواهد بود.)

برنامه توسعه محصول را به تفکیک و برای توسعه Component ها و بهمراه درصد وزنی اهمیت آن اعلام شود.

ردیف	شرح فعالیت‌ها	زمان (برحسب ماه)												شاخص‌های ارزیابی/خروجی‌ها
		۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	
1	Research & Requirements Analysis													تحلیل بازار، نیازمندی‌ها، استانداردها و رقبا
2	High-Level Architecture Design													طراحی معماری سیستم، اجزای اصلی، مدل استقرار
3	Core Engine Development													توسعه موتور HTTP/HTTPS، Parser، Rule Engine، Signature Detection
4	Security Modules Development													ساخت ماژول‌های امنیتی مانند: OWASP، Rate Limit، DDoS L7
5	Policy Management System													توسعه Rule Editor، مدیریت پروفایل‌ها، تنظیمات امنیتی
6	Dashboard & Monitoring													توسعه UI/UX، گزارش‌ها، نمودارها
7	QA, Security Testing & Performance Optimization													تست نفوذ، Load Test، کاهش False Positive و بهینه‌سازی سرعت
8	Documentation & knowledge base													مستندسازی و راهنمای کاربر

هزینه‌ها

مجمع هزینه مورد نیاز ۱۵۰.۰۰۰ میلیون ریال

تحلیل رقبا

هدف از این بخش ارائه تحلیلی شامل مزایا و معایب نسبت به رقبا می باشد.

ردیف	نام رقیب	نام کشور	لینک	مزایا محصول شما نسبت به محصول رقیب
				مزایا
۱	F5 Advanced WAF	آمریکا	https://f5.com	• امکان یکپارچه شدن با راهکار های امنیتی بومی • امکان ارایه خدمات و پوشش حداکثری شبکه ملی • عدم مشکل تامین لایسنس • عدم وابستگی در حوزه امنیت سایبری به کشورهای بیگانه
۲	Fortinet Fortiweb	آمریکا	https://fortinet.com	

استانداردها، مجوزها و گواهینامه‌های محصول

۱- توسعه محصول بر مبنای SSDLC و با رعایت حداکثری الزامات امنیتی شامل کدنویسی امن، معماری امن انجام شده است.

۲- تمامی الزامات و استانداردهای OWASP TOP 10 در وب و MITRE TOP 25 در هسته و ماژوهای محصول استفاده شده است.

۳- از تکنیکهای تست داینامیک همانند Fuzzing در تست محصول استفاده شده است.

۴- از استانداردها و راهکارهای متن باز و تجاری برای تحلیل استاتیک کد استفاده شده است.

موانع توسعه محصول:

هزینه R&D بالا است و لازم است حمایت معنوی و مادی برای تحقیق و توسعه محصول مهیا شود.

برنامه های پیشنهادی در توسعه آتی محصول

در این بخش برنامه پیشنهادی توسعه آتی محصول ، مورد بررسی قرار داده خواهد شد. پلن توسعه محصول در این فاز متمرکز بر AI و بکارگیری تکنولوژیهای لبه دانش در حوزه هوش مصنوعی برای کشف و بلاک کردن حملات مبتنی بر وب با استفاده از AI است.

ردیف	شرح فعالیت‌ها	زمان (برحسب ماه)												شاخص‌های ارزیابی/خروجی‌ها
		۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	
1	ML & Anomaly Detection Module													طراحی و توسعه مدل‌های رفتارشناسی و شناسایی حملات مبتنی بر یادگیری ماشین