نام محصول/ خدمت	سامانه مدیریت دسترسی ممتاز (PAM)
حوزه محصول/خدمت	تولید نرم افزار امنیت سایبری
شماره یا نام نسخه	-
تاریخ انتشار/ ورود به بازار	۱۳۹۵/۰۷/۰۱
شیوه دستیابی (تحقیق و توسعه داخلی/مهندسی معکوس/انتقال فناوری)	تحقیق و توسعه
میزان فروش محصول/خدمت در سال اخیر(ریال)	۶.۳۳۵.۰۰۰.۰۰۰
مشتریان اصلی[1] (پنج مصرف‌کننده عمده)	- شرکت های دولتی - بانک ها، بیمه ها - اپراتورها، ISP ها و مراکز داده - شرکت های خصوصی بزرگ و متوسط - ...
وبگاه	demo.hamim.co
کاربرد محصول/خدمت (حداکثر در ۲۰۰ کلمه)	مدیریت دسترسی امن و کنترل شده به منابع سازمان و ضبط و حسابرسی نشست ها و کاربران ممتاز به منظور کاهش مخاطرات درون سازمانی و حملات

مشخصات طراحی محصول/خدمت Design Specification (حداکثر در ۲۰۰ کلمه)

- تحکیم دروازه دسترسی
- ممیزی بازپخش نشست‌ها
- فیلترینگ ورودی پروتکل شناسایی
- تزریق خودکار مشخصات کاربری و هویتی
- راه اندازی سریع
- ذخیره سازی ضد جعل
- انباره کلمه عبور
- نظارت ۴ چشم بر نشست‌ها
- فرمت های ذخیره سازی کارآمد و پیشرفته

تاییدیه، گواهینامه و استانداردهای کسب شده (در صورت وجود)

عنوان	تاریخ	مرجع صادرکننده	توضیحات

[1] در صورتیکه محصول/خدمت، فاقد مشتری خاص بوده و توسط عام مورد مصرف قرار می گیرد، می توانید، مشتریان اصلی خود را عام قید نمایید.

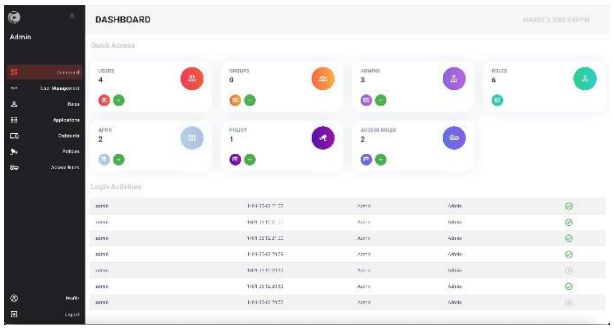
معرفی محصول/خدمت (حداقل در ۲۰۰ کلمه و حداکثر در ۳۵۰ کلمه)

سامانه مدیریت دسترسی ممتاز یا **Privileged Access Management** بنا بر گزارش هایی که در خصوص رخنه های امنیتی به صورت جدی وجود داشت در شرکت های امنیتی بزرگ دنیا پیشنهاد شده به عنوان مثال در تحقیقی مشخص شد هفت مورد از ده مورد نشست های اطلاعاتی بزرگ در قرن ۲۱ ناشی از سرقت هویت کاربران ممتاز و به خطر افتادن اعتبار حساب های کاربری مدیریتی بوده است.

سامانه مدیریت دسترسی ممتاز به صورت ویژه بر کاربران ممتاز یک سازمان تمرکز دارد یعنی کاربرانی که دسترسی سطح بالا به منابع اطلاعاتی اصلی سازمان دارند. این سامانه با قرارگرفتن میان کاربر ممتاز (یا هر کاربری که بخواهد به منابع سازمان به صورت دائمی یا موقت متصل شود) و منابع سازمان، دسترسی های کاربران ممتاز به سیستم ها را متناسب با مجوز دسترسی و حتی ساعت دسترسی مدیریت می کند تا کاربر امکان انجام اقداماتی را پس از اتصال به منابع سازمان داشته باشد که مجوز آن را دارد. و در صورت بروز رفتار خطرناک از صورت کاربر ممتاز گزارش آن به مدیران بالادست بنا بر تعریف هایی که از پیش تعیین شده است ارسال خواهد شد.

از مهمترین ویژگی های این سامانه ضبط نشست‌هاست که امکان بررسی ردپا در سیستم ها را در مواقع بحرانی فراهم می کند تا بتوان فهمید چه کسی چه کاری را انجام داده است.

نام محصول/ خدمت	پیشکار هویت آگاه (IAP)
حوزه محصول/خدمت	تولید نرم افزار امنیت سایبری
شماره یا نام نسخه	۱.۰
تاریخ انتشار/ ورود به بازار	۱۴۰۱/۰۹/۰۱
شیوه دستیابی (تحقیق و توسعه داخلی/مهندسی معکوس/انتقال فناوری)	تحقیق و توسعه
میزان فروش محصول/خدمت در سال اخیر(ریال)	۰
مشتریان اصلی[۲] (پنج مصرف‌کننده عمده)	- شرکت های دولتی - بانک ها، بیمه ها - اپراتورها، ISP ها و مراکز داده - شرکت های خصوصی بزرگ و متوسط - ...
وبگاه	Iap.hamimco.ir
کاربرد محصول/خدمت (حداکثر در ۲۰۰ کلمه)	مدیریت دسترسی کنترل شده به منابع وب سازمان با پیاده سازی معماری zero trust به منظور کاهش مخاطرات سازمانی و محدودسازی دسترسی باز کاربران درون سازمان



مشخصات طراحی محصول/خدمت Design Specification (حداکثر در ۲۰۰ کلمه)

- پیاده سازی معماری zero trust برای دسترسی کاربران به سرویس های وب درون سازمان
- تحکیم دروازه دسترسی
- دسترسی ایمن به برنامه ها از هرجا (داخل و خارج سازمان)
- سطوح متفاوت دسترسی به سرویس ها برای کاربران
- گزینه های احراز هویت متنوع
- راه اندازی سریع

تاییدیه، گواهینامه و استانداردهای کسب شده (در صورت وجود)

عنوان	تاریخ	مرجع صادرکننده	توضیحات

[۲] در صورتیکه محصول/خدمت، فاقد مشتری خاص بوده و توسط عام مورد مصرف قرار می گیرد، می توانید، مشتریان اصلی خود را عام قید نمایید.

سند ۶۰۴۱- مصوب ۹۸/۱۲/۲۰

معرفی محصول/خدمت (حداقل در ۲۰۰ کلمه و حداکثر در ۳۵۰ کلمه)

سرویس پیشکار هویت آگاه یا identity aware proxy یکی از به روز ترین سرویس‌ها در حوزه امنیت است که درخواست‌های وب ارسال شده به برنامه‌های سازمان را رهگیری می‌کند؛ این سرویس صرفا به کاربرانی اجازه دسترسی خواهد داد که احراز هویت شده باشند. با استفاده از این سرویس دسترسی به برنامه های کاربردی ابری یا داخلی و یا ماشین های مجازی به صورت کامل کنترل خواهد شد و نگرانی ای از بابت دسترسی غیرمجاز به این برنامه ها وجود نخواهد داشت چراکه پیش از صدور اجازه دسترسی هویت کاربر با استفاده از روش های مختلف شناسایی و تایید خواهد شد و صرفا در صورتی که هویت کاربر شناسایی شود اجازه دسترسی به او داده می شود. بسیاری از شرکت ها در حال حاضر از وی پی ان برای ایجاد دسترسی های محدود به برنامه های سازمان استفاده می کنند در حالیکه در استفاده از وی پی ان امکان ایجاد دسترسی های متفاوت برای کاربران را ندارند و هر کاربری که با وی پی ان به برنامه های سازمان متصل می شود امکان دسترسی به تمام برنامه ها را خواهد داشت اما در سرویس پیشکار هویت آگاه هر کاربر متناسب با مجوزی که برای او تعیین شده است به برنامه ها دسترسی دارد.

نام محصول/ خدمت	خدمت مرکز عملیات امنیت SOC
حوزه محصول/خدمت	خدمت مرکز عملیات امنیت
شماره یا نام نسخه	-
تاریخ انتشار/ ورود به بازار	۱۳۹۳/۰۴/۰۱
شیوه دستیابی (تحقیق و توسعه داخلی/مهندسی معکوس/انتقال فناوری)	تحقیق و توسعه
میزان فروش محصول/خدمت در سال اخیر(ریال)	۰
مشتریان اصلی[۳] (پنج مصرف‌کننده عمده)	- شرکت های دولتی - بانک ها، بیمه ها - اپراتورها، ISP ها و مراکز داده بزرگ - شرکت های خصوصی بزرگ - ...
وبگاه	www.hamimco.ir
کاربرد محصول/خدمت (حداکثر در ۲۰۰ کلمه)	ارائه خدمات مربوط به پیاده سازی و نگهداری مرکز عملیات امنیت (SOC)

مشخصات طراحی محصول/خدمت Design Specification (حداکثر در ۲۰۰ کلمه)

- ایجاد سیستم های زیربنایی امنیتی
- ایجاد قواعد مشخص و استاندارد در پاسخگویی به حوادث سایبری
- راه اندازی سامانه های امنیتی مورد نیاز سازمان
- ساختار سازمانی مسئول در رابطه با امنیت دارایی های سازمان

تاییدیه، گواهینامه و استانداردهای کسب شده (در صورت وجود)

عنوان	تاریخ	مرجع صادرکننده	توضیحات

[۳] در صورتیکه محصول/خدمت، فاقد مشتری خاص بوده و توسط عام مورد مصرف قرار می گیرد، می توانید، مشتریان اصلی خود را عام قید نمایید.

سند ۶۰۴۱- مصوب ۹۸/۱۲/۲۰

پروانه فعالیت در حوزه خدمات عملیاتی افتا	۱۴۰۰/۰۸/۲۹	سازمان فناوری اطلاعات ایران	پیاده سازی مرکز عملیات امنیت و تیم پاسخ به رخداد

معرفی محصول/خدمت (حداقل در ۲۰۰ کلمه و حداکثر در ۳۵۰ کلمه)

با توجه به بالا رفتن اهمیت اطلاعات در جامعه و سازمان ها حفاظت از این دارایی های مهم به یکی از چالش های بزرگ این قرن نیز تبدیل شده است به صورتی که حتی جنگ های آینده را جنگ های سایبری معرفی می کنند. خدمت **راه اندازی مرکز عملیات امنیت** به عنوان پایه ای ترین اقدام یک سازمان در راستای ایجاد سیستم امنیتی قوی در حوزه سایبری است. در این مرکز با چینش صحیح سیستم ها و تجهیزات یک سازمان و تربیت نیروی انسانی متخصص و مشخص کردن رتبه و میزان دسترسی مجاز برای هر یک و همچنین با استقرار صحیح سامانه های امنیتی گوناگون ، امکان اخلال در سازمان تا حد بالایی پایین می آید.

مجموعه ارتباط گستر حامی مسافت با در اختیار داشتن بهترین نیروهای تحصیل کرده و با تجربه در حوزه امنیت سایبری تاکنون به سازمان های متعددی در این حوزه کمک کرده است تا بتوانند مرکز عملیات امنیت سایبری خود را به شکل حرفه ای و درست راه اندازی نمایند.