به نام خدا

سند هدف امنیتی

[سیبتا – ۴,۰,۷]

[شرکت مهندسی پارتیان ابتکار پایدار]

[۰۵-۱۴۰۳]

[۱,۱]

فهرست مطالب

[شرکت مهندسی پارتیان ابتکار پایدار]

۱ معرفی

بروزرسانی اتوماتیک Signature های تجهیزات امنیتی FortiGate و FortiWeb توسط نرم افزار سیبتا

۱,۱ مشخصات سند و محصول

عنوان سند هدف امنیتی	سند هدف امنیتی سامانه یکپارچه بروزرسانی تجهیزات امنیتی (سیبتا)
نسخه	۱,۱
تاریخ	۱۴۰۳/۵/۳
نویسندگان	کارشناسان فنی و برنامه نویسی شرکت پارتیان ابتکار پایدار

نام شرکت	مهندسی پارتیان ابتکار پایدار
نام محصول	سامانه یکپارچه بروزرسانی تجهیزات امنیتی (سیبتا)
نوع محصول	نرم افزار تحت شبکه
نسخه‌ی محصول	۴,۰,۷

حداقل نیازمندی نرم‌افزاری/سخت‌افزاری/میان‌افزاری محصول

در جدول زیر سخت‌افزار، نرم افزار و میان افزارهای لازم برای کارکرد محصول بیان شده است:

سخت‌افزار/نرم-افزار/میان‌افزار	حداقل الزامات
پردازنده	2 Core CPU – Min 2Ghz
فضای ذخیره سازی	10 GB
حافظه	8 GB
سیستم عامل	Windows Server 2016
سایر نرم افزارها	VisualC++ & Dot.Net.Framework.4.8

۲ ادعای انطباق

۱،۲ انطباق با استاندارد ارزیابی امنیتی معیار مشترک

انطباق با استاندارد ارزیابی امنیتی معیار مشترک	ISO 15408 V3.1 R4
نام پروفایل حفاظتی	پروفایل حفاظتی سامانه سیبتا کلاینت سرور نسخه ۱.۰
سطح تضمین امنیتی	EAL1

۲،۲ شرح محصول

نرم افزار سیبتا با نصب بر روی یکی از سرورهای سازمان، از یک سو با سرور Core در ارتباط خواهد بود و از سوی دیگر به تجهیزات FortiGate و FortiWeb متصل می گردد. نرم افزار از طریق پروتکل امن HTTPS جهت احراز هویت و دریافت دسترسی های لازم برای کاربر، با سرور Core ارتباط برقرار میکند، سرور Core نیز با ارتباط با پایگاه داده (سرور Core و DB بر روی یک سیستم عامل نصب شده اند) و تحلیل اطلاعات ارسال شده از طرف کاربر، سطح دسترسی و اجازه ی لاگین به نرم افزار را به کاربر میدهد. سپس در صورت صحت اطلاعات جهت Login به تجهیزات فورتی گیت و فورتی وب، نرم افزار سیبتا، اطلاعات سیستم عامل و ورژن Signature های هر کدام از ماژول های فورتی گیت و فورتی وب را به سرور Core ارسال می نماید. سرور Core با توجه به اطلاعات دریافتی، فایل مناسب آن Firmware به همراه ورژن مناسب برای آن Signature خاص را در قالب یک فایل به نرم افزار سیبتا بر می گرداند، نرم افزار با دریافت لینک فایل مربوطه، آن را به وسیله ی پروتکل امن SSH به فورتی گیت و پروتکل امن HTTPS به فورتی وب تحویل می دهد. و به این طریق Signature های این دو دستگاه بروز رسانی می شوند.
در شبکه هایی که امکان دسترسی مستقیم فورتی گیت و فورتی وب به اینترنت میسر نباشد، نرم افزار سیبتا قادر خواهد بود تا فایل های مربوط به Signature ها را در یک Repository جداگانه در داخل شبکه ی کاربر ذخیره نماید تا فورتی گیت از آنجا نسبت به بروزرسانی Signature ها اقدام نماید.

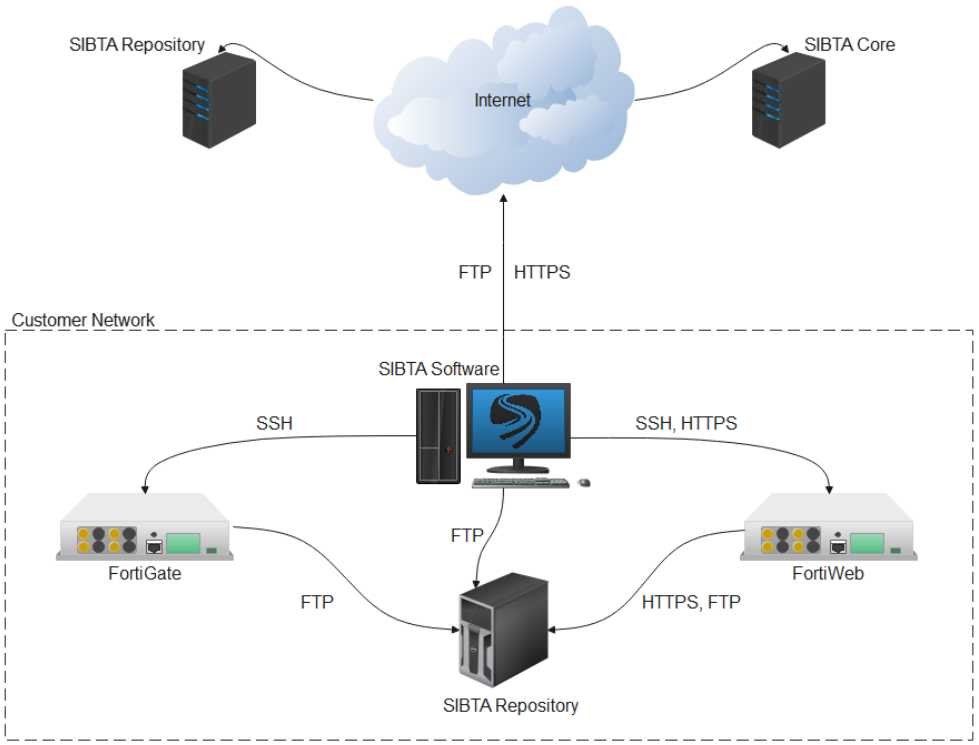
۱،۲،۲ حوزه فیزیکی

عناصر سخت‌افزاری و نرم‌افزاری مورد استفاده در جدول زیر مشخص گردیده است:

عناصر محصول	شماره مدل یا نسخه
Windows Server	2016 or Higher
SQL Server	2016 or Higher
Windows Client	Windows 10 or Higher
FortiGate	FortiOS 5.4 or Higher
FortiWeb	FortiWeb 6.3.6 or Higher

[شرکت مهندسی پارتیان ابتکار پایدار]

در این بخش قرار گیری محصول در محیط عملیاتی و پیکربندی آن در قالب تصویر آورده شود. لازم است محصول و محیط عملیاتی به تفکیک در تصویر مشخص گردند.

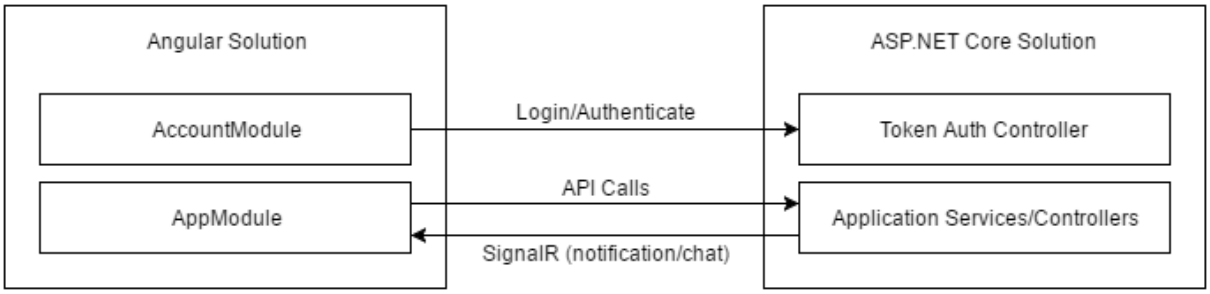


شکل ۱: حوزه فیزیکی محصول با تفکیک حوزه محصول و محیط عملیاتی آن

[شرکت مهندسی پارتیان ابتکار پایدار]

۲،۲،۲ حوزه منطقی

نمودار زیر معماری کلی سامانه را نشان می دهد:



تصویر ۱: معماری کلی سامانه

پروژه Angular به گونه ای طراحی شده است که می تواند به طور جداگانه از قسمت اصلیASP.NET Core ، با پورت متفاوت در همان سرور یا سرور دیگری مستقر شود و هنگامی که انتشار می‌یابد، در واقع یک برنامه ساده HTML + JS + CSSاست که می تواند در هر سیستم عامل و هر وب سروری ارائه شود.

قابل ذکر است که سیستم ASP.NET Core هیچ کد HTML، JS یا CSS ندارد. این به سادگی نقاط پایانی را برای احراز هویت مبتنی بر توکن و استفاده از سرویس‌های برنامه (REST API) فراهم می‌کند.

۳ مسائل امنیتی

۱،۳ خط مشی

خط مشی ها	توصیف
مسئولیت پذیری	تمام کاربران مجاز محصول باید مسئول اقداماتشان باشند.
اهداف مجاز	تمام داده های جمع آوری شده، ذخیره شده و تحلیل شده توسط محصول باید برای اهداف مجاز استفاده گردد.
تجزیه و تحلیل	پردازشهای تحلیلی و اطلاعاتی که از روند بروزرسانی به دست می آید باید به Syslog Server ارسال گردد تا به صورت آرشیو نگهداری گردد.
مدیریت	محصول باید توسط کاربران مجاز مدیریت گردد.
محافظت از تغییرات	داده های تحلیل شده و تولید شده توسط محصول باید از تغییرات محافظت گردند.
جلوگیری از ورود غیرمجاز	محصول باید از ورود غیرمجاز همچون قطع اجرای برنامه های معمولی محافظت نماید.

[شرکت مهندسی پارتیان ابتکار پایدار]

۲,۳ تهدیدات

تهدید	توصیف
خطای مدیر	مدیر سیستم ممکن است با پیکربندی نادرست محصول مکانیزم های امنیتی را تحت تأثیر قرار دهد.
مخاطرات محرمانگی و صحت	ممکن است موجودیت غیرمجازی با دور زدن مکانیزم های امنیتی، صحت و محرمانگی داده هایی که توسط نرم افزار جمع آوری، ذخیره یا تحلیل شده اند را به خطر اندازد.
دسترسی غیرمجاز	کاربر غیرمجاز ممکن است با دور زدن مکانیزم های امنیتی سعی در افشاء داده هایی که توسط محصول جمع آوری، ذخیره یا تحلیل شده اند، نماید.
مخاطرات دسترس پذیری	کاربر غیر مجاز ممکن است با متوقف نمودن سرویس محصول، سعی در به خطر انداختن پیوستگی عملکرد بروزرسانی تجهیزات نماید.
مخاطرات افزایش حق دسترسی	کاربر غیر مجاز ممکن است با دستیابی به محصول و با استفاده از مجوزهای سیستمی به عملکرد امنیتی محصول و داده های آن دستیابی پیدا نماید.
مخاطرات پیکربندی	محصول ممکن است توسط افراد مجاز یا غیرمجاز به صورت نامناسبی پیکربندی گردد و سبب عملکرد معیوب سامانه شود.
واکنش آسیب پذیری	

۳,۳ فرضیات

فرضیات	توصیف
دسترسی	محصول برای انجام عملکرد خود به تمام منابع موجود در زیرساخت IT که به آنها نیاز داشته، دسترسی دارد.
محافظت	محصول که به اجرای خط مشی های امنیتی حساس است، از هرگونه تغییرات نرم افزاری غیرمجاز محافظت میگردد.
محل استقرار	منابع پردازشی محصول در داخل فضایی قرار میگیرند که از نظر دسترسی کنترل شده هستند تا از دسترسی فیزیکی غیرمجاز جلوگیری شود.

[شرکت مهندسی پارتیان ابتکار پایدار]

مدیریت	یک یا بیش از یک فرد دارای صلاحیت برای مدیریت محصول و امنیت اطلاعات آن به محصول اختصاص داده میشود.
سرپرست مورد اعتماد	یک سرپرست مجاز فردی بی دقت یا متخاصم نیست و دستورات ارائه شده توسط مستندات محصول را دنبال می نماید.
دسترسی امن	محصول تنها توسط کاربران مجاز قابل دسترسی است.

۴ اهداف امنیتی

۱،۴ اهداف امنیتی برای محصول

هدف امنیتی	توضیحات
ممیزی	هر رخدادی که در زمینه امنیتی دارای ارزش باشد، در حوزه مالکیتش رکورد می گردد. این رکوردها در قبال تغییرات و حذف محافظت خواهند شد. کاربران مجاز امکان بررسی آسان و سریع رکوردها را دارند و مدیر سیستم به موقع از رخداد امنیتی بحرانی آگاه خواهد شد.
احراز هویت	هر کاربری که در سیستم تعریف گردد، به طور امن احراز هویت گشته و مطابق با نقش و مجوزهایشان اجازه فعالیت دارند. برای احراز هویت کاربر، قوانینی تعریف شده است به طوریکه کاربران را ملزم به استفاده از کلمه های عبور قدرتمند مینماید. اجازه طبقه بندی رکوردها و مستندات در دسترس است. ا توجه به طبقه بندی آنها قوانینی تعریف شده است. همچنین برای مستندات و رکوردهای شخصی امکان تعریف مجوز دسترسی نیز فراهم خواهد بود. کاربران به صورت انفرادی یا گروهی از کاربران سازوکار کنترل دسترسی به مستندات و رکوردها را خواهند داشت. مهاجم در تلاش است تا از تهدیدی چون رسیدن به سطح دسترسی بالاتر نهایت سود را ببرد.

[شرکت مهندسی پارتیان ابتکار پایدار]

هدف امنیتی	توضیحات
	برای جلوگیری از این تهدید، با استفاده از سازوکارهای قویتری مدیر سیستم احرازهویت می گردد. از جمله سازوکارها میتوان به محدود نمودن رنج IP ، محدود نمودن بازه زمانی، احرازهویت براساس توکن، احرازهویت چند فاکتوری و ترکیبی از این روشها اشاره نمود.
مدیریت خطا	به صورت امن و کارامد سازوکار مدیریت خطا فراهم است .خطاهای رخ داده در طول عملیات به کاربر به صورت امن و معنادار نشان داده میشود .برای مثال، اطلاعات کلی مربوط به احراز هویت ناموفق را ثبت خواهد کرد، همچنین برای کاربر عادی اطلاعات جزئی چون شماره خطا برگردانده میشود .از سوی دیگر مدیر سیستم سریعاً از شکست بحرانی که رخ داده مطلع می گردد.
مدیریت	مدیر سیستم تمام کارکردها را جهت مدیریت امن و کارامد سیستم فراهم می نماید. سازوکارهای کنترل دسترسی مناسب جهت حفاظت از واسطهای مدیریتی در نظر گرفته شده است. مدیر سیستم امکان تغییر مجوزها و نقشهای کاربران را فراهم می آورد و مدیر می تواند برای یک کاربر خاص و/یا گروهی از کاربران نقشها و مجوزهایی تنظیم نماید.

۲،۴ اهداف امنیتی برای محیط عملیاتی

هدف امنیتی	توضیحات
محیط امن	دسترسی غیرمجاز محدود گردیده و تمام مولفه ها در محیط عملیاتی امن هستند و تنها افراد مجاز اجازه دسترسی به مولفه های حساس را خواهند داشت. محیط عملیاتی به طور مناسب در قبال هر حمله DoS یا DDoS محافظت شده است. از جمله سازوکارهای حفاظتی جهت غیرفعال نمودن سرویسها، پورتها و دیگر موارد استفاده شده است.
ارتباطات	محیط عملیاتی به طور امن با سرویس های خارج از محدوده ی خود در ارتباط خواهد بود.
کاربران آموزش دیده	تمامی کاربران استفاده کننده از سامانه به طور خاص آموزش های لازم را دیده اند.
توسعه دهندگان آموزش دیده	تمامی تیم توسعه دهندگان آموزش های لازم را دیده اند.

[شرکت مهندسی پارتیان ابتکار پایدار]

هدف امنیتی	توضیحات
توسعه دهندگان مجرب	تمام کارمندان توسعه دهنده ی محصول در زمینه امنیت تجربه داشته و آنها اقدامات مقابله ای لازم برای تمام آسیب پذیری های امنیتی شناخته شده را در نظر میگیرند.
ممیزی کامل	هر رخداد مرتبط امنیتی برای مولفه های غیر از محصول نیز مورد ممیزی قرار میگیرند. این هدف امنیتی مکمل هدف ممیزی برای محیط عملیاتی محصول میباشد. رکورد های ممیزی محصول در صورت ترکیب با باقی رکورد های ممیزی بسیار معنادار خواهند بود.
تحویل امن	تحویل و نصب محصول بدون به خطر افتادن هرگونه محدودیت امنیتی انجام می شود. علاوه بر این، کارکرد ها و/یا پارامترهای استفاده شده به منظور تست پاک یا غیر قابل دسترس خواهد بود.
پشتیبان گیری مناسب	نسخه پشتیبان برای یک بازه زمانی منطقی تمام داده های باقیمانده در محیط عملیاتی خواهد بود. برای این منظور ممکن است از روالهای از پیش تعریف شده استفاده گردد. همچنین از واحدهای ذخیره سازی و دیگر مولفه های سخت افزاری نیز نسخه پشتیبان تهیه می گردد.

۵ الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با جدول زیر هستند. در ادامه هر یک از الزامات شرح و بسط داده شده‌اند.

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**تولید داده ممیزی ۱**	FAU_GEN.1.1
۲	**تولید داده ممیزی ۲**	FAU_GEN.1.2
۳	**تولید داده ممیزی ۳**	FAU_GEN.2.1
۴	**بازبینی داده ممیزی ۱**	FAU_SAR.1.1
۵	**بازبینی داده ممیزی ۲**	FAU_SAR.1.2
۶	**بازبینی داده ممیزی ۳**	FAU_SAR.2.1
۷	**بازبینی داده ممیزی ۴**	FAU_SAR.3.1
۸	**ذخیره سازی رویدادهای ممیزی ۱**	FAU_STG.1.1
۹	**ذخیره سازی رویدادهای ممیزی ۲**	FAU_STG.1.2

[شرکت مهندسی پارتیان ابتکار پایدار]

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۰	**ذخیره سازی رویدادهای ممیزی ۷**	FAU_STG.4.1
۱۱	انتخاب داده ممیزی ۱	FAU_SEL.1.1
۱۲	مدیریت کلید رمزنگاری ۱	FCS_CKM.1.1
۱۳	عملیات رمزنگاری ۱-رمزنگاری و رمزگشایی ۱	FCS_COP.1.1(1)
۱۴	عملیات رمزنگاری ۱	FCS_COP.1.1(2)
۱۵	مدیریت کلمه عبور	FIA_PMG_EXT.1.1
۱۶	مدیریت احراز هویت ناموفق ۱	FIA_AFL.1.1
۱۷	مدیریت احراز هویت ناموفق ۲	FIA_AFL.1.2
۱۸	تعریف مشخصات کاربر ۱	FIA_ATD.1.1
۱۹	شناسایی کاربر ۱	FIA_UID.1.1
۲۰	احراز هویت کاربر ۱	FIA_UAU.1.1
۲۱	احراز هویت کاربر ۲	FIA_UAU.1.2
۲۲	احرازهویت کاربر ۷	FIA_UAU.5.1

۱,۵ کلاس ممیزی امنیت

شماره الزام	نام الزام
۱	**تولید داده ممیزی ۱**

محصول می تواند براساس رخدادهای قابل ممیزی زیر، رکورد ممیزی تولید نماید:

- **ورود و خروج کاربر به/ از سیستم**
- **رویدادهای قابل ممیزی این رویدادها در جدول زیر آمده است**

مولفه	رویداد قابل ممیزی	جزئیات
بازبینی داده ممیزی	خواندن اطلاعات از رکوردهای ممیزی	
بازبینی داده ممیزی۳	تلاشهای ناموفق برای خواندن اطلاعات از رکوردهای ممیزی	
ذخیره سازی رویدادهای ممیزی	عملیات انجام شده به دلیل شکست ذخیره سازی ممیزی	در ممیزی های داده سازی ذخیره دلیل به پایگاه

		نمی پذیر امکان مشکلی چنین بروز داده .باشد پذیری آسیب چنین بروز احتمال اگر یعنی وجود ست درست داده پایگاه تنظیمات یعنی داشت افزار نرم کلی طور به صورت این در که نشده اجرا نخواهد شد.
عملیات کنترل دسترسی ۱	تمامی درخواستهای ناموفق برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول	
مدیریت کلمه عبور	تلاش موفق و ناموفق ورود کاربر	تمامی درخواست های ورود اعم از موفق یا ناموفق در سیستم ثبت می گردد.
مدیریت مشخصه های امنیتی ۱	تمامی تغییرات بر روی مقادیر مشخصه های امنیتی	تمامی فعالیت ها در داده های ممیزی ثبت می گردد.
مدیریت داده های محصول ۱-مدیر سیستم	تمامی تغییرات بر روی مقادیر داده های امنیتی	
مدیریت داده های محصول ۱-کاربرعادی، وارد کننده داده	تمامی تغییرات بر روی مقادیر داده های امنیتی	تمامی فعالیت ها در داده های ممیزی ثبت می گردد.
تغییرات روی موجودیت های غیر فعال	افزودن، ویرایش، حذف موجودیت های غیر فعال	
تغییرات روی موجودیت های فعال	افزودن، ویرایش، حذف موجودیت های فعال	
تعلیق ورود موجودیت فعال	جلوگیری از ورود کاربر پس از ۳ بار تلاش ورود ناموفق	

۲	**تولید داده ممیزی۲**

محصول می تواند برای هر رکورد ممیزی، حداقل اطلاعات زیر را ثبت نماید:

- **تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال و نتیجه (موفقیت یا شکست) رویداد**

[شرکت مهندسی پارتیان ابتکار پایدار]

• **نوع کاربری، IP کاربر، محل خدمت کاربر**	
۳	**تولید داده ممیزی ۳**
برای رویدادهای ممیزی حاصل از اقدامات کاربران شناسایی شده، محصول می تواند هویت کاربری که باعث ایجاد آن رویداد شده است، را شناسایی و ثبت نماید.	
۴	**بازبینی داده ممیزی ۱**
محصول می تواند امکان خواندن/مشاهده ورود موفق، ورود ناموفق، تعلیق ورود، ویرایش،حذف و ایجاد آیتم جدید،صدور مجوز و گواهینامه، تکمیل فرم و تصحیح اطلاعات از کل رکوردهای ممیزی را برای مدیر سیستم فراهم نماید.	
۵	**بازبینی داده ممیزی ۲**
محصول می تواند رکوردهای ممیزی را به شکل خوانا و قابل درک برای کاربر نمایش دهد.	
۶	**بازبینی داده ممیزی ۴**
محصول می تواند از دسترسی کلیه کاربران به جز کاربرانی که به آنها مجوز دسترسی خواندن داده شده باشد. (الزام شماره ۴)جهت خواندن رکوردهای ممیزی ممانعت نماید.	
۷	**بازبینی داده ممیزی ۴**
محصول می تواند امکان انجام مرتب سازی رکوردهای ممیزی را به نحوی فراهم نماید که کاربر مجاز بتواند آن رکوردها را براساس مرکز برگزار کننده، کاربر، نوع کاربری، تاریخ، موضوع و نوع رخداد(عملیات)مرتب نماید.	
۸	**ذخیره سازی رویدادهای ممیزی ۱**
محصول می تواند رکوردهای ممیزی ذخیره شده در محل ذخیره سازی را از حذف غیرمجاز حفاظت نماید. از طریق خود نرم افزار امکان حذف غیر مجاز داده ممیزی وجود ندارد .کاربر تنها در صورتی امکان حذف داده ممیزی را دارد که به صورت غیر مجاز به پایگاه داده دسترسی داشته باشد و از آنجا عملیات حذف را انجام دهد که در آن حالت عملیات پیش گفته در پایگاه داده به طور خودکار ممیزی می شود.	
۹	**ذخیره سازی رویدادهای ممیزی ۲**
محصول قادر به تشخیص تغییرات غیرمجاز در رکوردهای ممیزی ذخیره شده در محل ذخیره سازی آنها می باشد.	
۱۰	**ذخیره سازی رویدادهای ممیزی ۷**
محصول در صورت پر شدن محل ذخیره سازی رکورد ممیزی ذخیره رویدادهای قابل ممیزی، به جز آنهایی که توسط مدیر سیستم تعیین می گردد، جلوگیری نماید و هشدار لازم را با استفاده از **پیام کوتاه**، مدیر سیستم را مطلع می نماید.	
	انتخاب داده ممیزی ۱
محصول می تواند قادر به انتخاب مجموعهای از رخدادها جهت ممیزی شدن، از مجموعه تمام رخدادهای قابل ممیزی براساس مشخصه های زیر باشد:	

[شرکت مهندسی پارتیان ابتکار پایدار]

- هویت موجودیت فعال، نوع رخداد (عملیات)
- گروه کاربری
- محدوده زمانی
- موضوع، فرم، IP

۲,۵ کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام
۱۲	**تولید کلید رمزنگاری ۱**
رمزگذاری و رمزگشایی را بر اساس الگوریتم AES (تعریف‌شده ISO 18033-3) با توجه به مد عملیاتی GCM و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف‌شده در NIST SP 800-38D)	
۳	**عملیات رمزنگاری ۱ رمزنگاری و رمزگشایی ۱ – A**
محصول می تواند **رمزنگاری و رمزگشایی** را مطابق با الگوریتم رمزنگاری متقارن AES Key Warp مطابق سند-38F NIST SP 800، با اندازه کلید رمزنگاری ۱۱۸ و ۱۹۲ و یا ۲۵۶ بیتی را انجام دهد.	
۱۴	**عملیات رمزنگاری ۱ – B**
محصول مورد ارزیابی می تواند خدمات امضای رمزنگاری(تولید و تأیید)را بر اساس الگوریتم رمزنگاری زیر ارائه کند: الگوی : RSA اندازه کلیدهای ۱۰۴۸ بیتی و بر اساس FIPS PUB 186-4 استاندارد امضای دیجیتال ، DSS بخش ۴	

۳,۵ کلاس شناسایی و احرازهویت

شماره الزام	نام الزام
۱۵	**مدیریت کلمه عبور**
محصول می تواند قابلیتهای مدیریت رمزعبور را که در زیر ذکر شدهاند برای رمزهای عبور مدیریتی فراهم نماید: • رمزهای عبور باید بتوانند هرترکیبی ازحروف کوچک و بزرگ، اعداد و کاراکترهای خاص"!","@" ،"#","$" ،"٪" ، "*"، "("،")" ،"_" ،"+" ،"^"، "&" ،"{" ،"}" ،":" ،";" ،"?" ، "." باشند. • حداقل طول رمزعبور توسط مدیر سیستم قابل تنظیم می باشد.	

[شرکت مهندسی پارتیان ابتکار پایدار]

۱۶	**مدیریت احراز هویت ناموفق ۱**
محصول می تواند با استفاده از یک عدد مثبت قابل تنظیم از طرف مدیر سیستم تعداد تلاش های احراز هویت ناموفق را مدیریت نماید.	

۴,۵ کلاس

شماره الزام	نام الزام
۱۷	**مدیریت احراز هویت ناموفق ۲**
زمانی که تعداد تلاشهای ناموفق صورت گرفته برای احراز هویت به حد تعیین شده رسید و یا از آن بیشتر شد، محصول می تواند عملیات "جلوگیری از ورود کاربر به مدت تعیین شده توسط مدیر" اجرا نماید که باعث پیچیدهتر کردن عمل احراز هویت مجدد کاربر شود.	
۱۸	**تعریف مشخصات کاربر ۱**
محصول باید مشخصههای امنیتی زیر را برای هر کاربر نگهداری نماید: • شناسه کاربر داده های احراز هویت • نقش کاربر • وضعیت حساب کاربری(فعال، غیرفعال، بلوکه شده و غیره) • IP کاربر • رمز عبور کاربر	
۱۹	**شناسایی کاربر ۱**
محصول باید پیش از شناسایی کاربر اجازه اقدامات زیر را فراهم آورد: • مشاوره راهنمای نحوه ورود به سیستم،	
۲۰	**احراز هویت کاربر ۱**
محصول میواند پیش از احراز هویت کاربر، اجازه اقدامات زیر را به کاربر دهد: • بازیابی رمز عبور	
۲۱	**احراز هویت کاربر ۲**

[شرکت مهندسی پارتیان ابتکار پایدار]

شماره الزام	نام الزام
محصول می تواند هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، احراز هویت نماید.	
۲۲	**احراز هویت کاربر**
محصول باید اقدامات زیر را برای احرازهویت کاربر فراهم آورد: • نام کاربری و کلمه عبور	
۲۳	**انقیاد مشخصههای امنیتی کاربر با موجودیت فعال متناظر ۱**
محصول می تواند مشخصه های امنیتی زیر را برای کاربر فعال نگهداری نماید: • شناسه کاربر • نقش های کاربر • جزئیات واسط کلاینت مرورگر ، IP • پیشینه احرازهویت (زمان آخرین تلاش احرازهویت موفق و ناموفق) تا ۶۰ دقیقه گذشته • پیشینه دسترسی به سند/رکورد اخیر(ممیزی)	
۲۴	**انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۲**
محصول می تواند قوانین زیر را بر روی اتصال اولیه کاربر فعال اعمال نماید: • زمانیکه یک نشست جدید برقرار میشود، اطلاعات موجود از نشستهای قبلی حذف گردد. • اطلاعات پیشینه احراز هویت باید بروزرسانی گردد. • ثبت رکورد ممیزی برای ورود موفق/ناموفق کاربر در نشست جدید.	
۲۵	**انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۳**
محصول قوانین زیر را که حاکم بر تغییرات است به مشخصه های امنیتی کاربر فعال اعمال نماید: • هیچ تغییری در طول نشست فعال مجاز نمی باشد.	

۵,۵ کلاس حفاظت از داده های کاربری

شماره الزام	نام الزام
۲۶	**ورود داده های کاربری به محصول ۴**
محصول هنگام دریافت داده کاربری، خط مشی کنترل دسترسی، فرمتهای مجاز داده ها(PKG, TXT) را اعمال می نماید.	

[شرکت مهندسی پارتیان ابتکار پایدار]

شماره الزام	نام الزام
۲۷	**ورود داده های کاربری به محصول ۵**
محصول می تواند از مشخصه های امنیتی مرتبط با داده های کاربری را هنگام ورود داده ها استفاده نماید.	
۲۸	**ورود داده های کاربری به محصول ۶**
محصول می تواند اطمینان دهد که پروتکل مورد استفاده برای انتقال، ارتباط و همبستگی بین مشخصه های امنیتی و داده کاربری دریافت شده را فراهم می نماید.	
۲۹	**خروج داده های کاربری از محصول ۳**
محصول می تواند هنگام خروج داده کاربری به بیرون داده ها را در ۴ فرمت (PDF, Excel, PNG, JPG) نمایش داده و از خروج داده های حساس مانند نام کاربری و کلمه عبور و ایمیل کاربر جلوگیری کند.	
۳۰	**صحت داده های کاربری ذخیره شده ۲**
محصول می تواند داده کاربری حساس ذخیره شده در مکان تحت کنترل خود را براساس مشخصه های رمزنگاری امن نگهداری کرده و به منظور شناسایی خطای صحت داده رکورد و داده ممیزی، پایش نماید.	
۳۱	**صحت داده های کاربری ذخیره شده ۳**
هنگام تشخیص خطای صحت داده، محصول می تواند ثبت ممیزی را صورت دهد.	
۳۲	**خط مشی کنترل دسترسی ۱**
محصول می تواند دسترسی بر اساس نوع کاربری که هنگام ورود کاربر شناسایی می شود را بر روی موارد زیر اعمال نماید: موجودیت های فعال به تفکیک ماژول های سیستم • موجودیت غیرفعال: رکوردها، مستندات دادههای متعلق به کاربر داده احرازهویت داده با این معیارها: عکس کاربر با فرمت های BMP, PNG, JPG,GIF • عملیات: ایجاد موجودیت غیرفعال جدید انتقال موجودیت غیرفعال ویرایش و حذف موجودیت غیر فعال ایجاد موجودیت فعال جدید	

شماره الزام	نام الزام
انتقال موجودیت فعال ویرایش و حذف موجودیت فعال تغییر دسترسی ها به موجودیت غیرفعال عملیات بر روی فراداده های وابسته به موجودیت غیرفعال	
۳۳	**عملیات کنترل دسترسی ۱**
محصول می تواند سطح دسترسی را با توجه به موارد زیر بر روی موجودیتهای غیرفعال اعمال نماید: • هویت کاربر • نقشها و مجوزهای کاربر مجاز • اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده میشوند.	
۳۴	**عملیات کنترل دسترسی ۲**
محصول می تواند قوانین زیر را اجرا نمایند تا عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده را مجاز نمایند: عملیات تنها به شرطی مجاز است که در لیست کنترل دسترسی، رکوردی وجود داشته باشد که به کاربر با شناسه کاربری یا شناسه گروه مربوطه یا نقش کاربری تعریف شده حق دسترسی به موجودیت غیرفعال را بدهد.	
۳۵	**عملیات کنترل دسترسی ۳**
محصول می تواند براساس قوانین زیر، دسترسی مجازی از موجودیت فعال به موجودیت غیرفعال داشته باشد: • کاربران با مجوز مدیر سیستم به هر رکورد و روش ارائه شده توسط محصول دسترسی دارند. • کاربران غیر مجاز بدون نیاز به فرآیند احراز هویت، به اطلاعات قابل دسترس عموم، دسترسی دارند.	

۶,۵ کلاس مدیریت امنیت

شماره الزام	نام الزام
۳۶	**مدیریت کارکرد در محصول ۱**

[شرکت مهندسی پارتیان ابتکار پایدار]

شماره الزام	نام الزام
محصول می تواند توانایی تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار عملکرد تمام عملکردهای مدیریت امنیت سیستم را به مدیر سیستم محدود می نماید.	
۳۷	**مدیریت مشخصه های امنیتی ۱**
محصول می تواند با اعمال تعیین سطح دسترسی بر اساس نقش ، توانایی تغییر پیشفرض، پرس و جو، تغییر، حذف، ایجاد مشخصه های امنیتی نام کاربری و کلمه عبور را به مدیر سیستم محدود می نماید.	
۳۸	**مدیریت مشخصه های امنیتی ۳**
محصول برای مشخصه های امنیتی که برای اعمال خط مشی استفاده میشوند، می تواند مقادیر پیش فرض محدود شده ای درنظر بگیرد.	
۳۹	**مدیریت مشخصه های امنیتی ۴**
محصول برای تعیین مقادیر اولیه پیشنهادی می تواند به مدیر سیستم اجازه دهد تا هنگام ایجاد اطلاعات یا موجودیت غیر فعال، مقادیر پیشفرض را لغو و تغییر دهد.	
۴۰	**مدیریت داده های محصول ۱-مدیر سیستم**
محصول می تواند توانایی تغییر پیشفرض، پرسوجو، تغییر، حذف، پاک نمودن، ایجاد کاربر جدید، داده های ممیزی و داده های احراز هویت را به مدیر سیستم محدود نماید.	
۴۱	**مدیریت داده های محصول ۱-کاربرعادی، وارد کننده داده**
محصول می تواند توانایی تغییر پیشفرض، پرسوجو، تغییر پسورد به کاربر عادی محدود نماید.	
۴۲	**کارکردهای مدیریتی محصول ۲**
محصول می تواند قادر به انجام کارکردهای مدیریتی زیر باشد:	

[شرکت مهندسی پارتیان ابتکار پایدار]

شماره الزام	نام الزام

مولفه	عملیات مدیریتی
بازبینی داده ممیزی ۱	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی
انتخاب داده ممیزی ۱	پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی
ذخیره سازی رویدادهای ممیزی ۷	پشتیبانی از عملیات(حذف، ویرایش، اضافه)در زمان خرابی ذخیره سازی ممیزی
عملیات کنترل دسترسی۱	مدیریت مشخصه های مورد استفاده برای ایجاد دسترسی و یا منع
ورود داده های کاربری به محصول ۴	ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول
صحت داده های کاربری ذخیره شده ۲	عملیاتی برای تشخیص یک خطای صحت داده که میتواند قابل پیکربندی باشد.
مدیریت احراز هویت ناموفق۱	مدیریت حدآستانه برای تلاشهای ناموفق مدیریت عملیاتی که هنگام رویداد شکست احرازهویت باید صورت گیرد.
تعریف مشخصات کاربر۱	مدیر مجاز باید قادر به تعریف مشخصههای امنیتی بیشتر برای کاربران باشد.
مدیریت کلمه عبور	مدیریت معیارها برای بررسی کلمه عبورها
انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۱	مدیر مجاز میتواند مقادیر مشخصه های امنیتی موجودیت های فعال پیشفرض را تعریف و یا تغییر دهد.
مدیریت مشخصههای امنیتی ۱	مدیریت گروهی از نقشهایی که با مشخصه های امنیتی در تعامل هستند.
مدیریت مشخصه های امنیتی ۳	• مدیریت گروهی از نقش هایی که مقادیر اولیه را مشخص میکنند. • نقش مدیر سیستم توانایی مشخص نمودن مقادیر اولیه را داراست. • مدیریت مقادیر پیشفرض برای کنترل دسترسی محصول.
مدیریت داده های محصول ۱ مدیر سیستم	مدیریت گروهی از قوانین مرتبط با دادههای محصول

[شرکت مهندسی پارتیان ابتکار پایدار]

شماره الزام	نام الزام	
مدیریت داده های محصول ۱ کاربرعادی، وارد کننده داده	مدیریت گروهی از قوانین مرتبط با دادههای محصول توضیح: کاربر عادی نمی تواند قوانین مرتبط با داده های محصول را مدیریت کند. چون در فرآیند آموزش کاربرعادی نباید این امکان را داشته باشد.	
نقش های امنیتی ۱	مدیریت گروهی از کاربرانی که بخشی از یک نقش هستند.	
محدودیت بر روی چندین نشست همزمان ۱	مدیریت حداکثر نشست مجاز کاربران به طور همزمان توسط مدیر توضیح: با توجه به اینکه نشست های همزمان یک کاربر در آن واحد ممکن است موجب سوء استفاده گردد، نشست های فعال کاربر محدود به یک نشست می باشد.	
قفل کردن و خاتمه دادن به نشست ها ۹	تعیین زمان غیرفعال بودن کاربر که نشست آن کاربر خاتمه یابد. تعیین زمان پیشفرض غیرفعال بودن کاربر که نشست خاتمه یابد.	

۴۳	**نقش های امنیتی ۱**

نقش های کاربری به تفکیک ماژول های سیستم

داشبورد

- **Hangfire داشبورد**
- **آمار لحظه ای لایسنس ها**
- **کاربر**

گزارشات

- **SMTP Email**
- **ارسال دوره ای**
- **لاگ های بازرسی**
- **لاگ های بروز رسانی**
- **نگهداری**

مدیریت پلتفرم ها

- **سرورهای پیامک**
- **کنترل نسخه ها**

[شرکت مهندسی پارتیان ابتکار پایدار]

شماره الزام	نام الزام

مدیریت سیستم

- **Off Networks**
- **دسترسی اتمام یافته ها**
- **دسترسی فروش**
- **دسترسی فنی**
- **دسترسی کاربر**

تنظیمات

دستگاه ها

- **حذف لاگ های امروز**

زبان ها

- **ایجاد کردن زبان جدید**
- **تغییر دادن متون**
- **حذف کردن زبان**
- **ویرایش کردن زبان**

کاربران

- **ایجاد کردن کاربر جدید**
- **تغییر دادن مجوزها**
- **حذف کردن کاربر**
- **لاگین برای کاربران**
- **لایسنس های کاربر - افزودن یا ویرایش**
- **لایسنس های کاربر - فقط نمایش**
- **ویرایش کردن کاربر**

نقش ها

- **ایجاد کردن نقش جدید**
- **حذف کردن نقش**
- **ویرایش کردن نقش**

واحد های سازمان

شماره الزام	نام الزام
	• **مدیریت اعضا** • **مدیریت درخت سازمانی** • **مدیریت فورتی نت** • **IP List** • **آپدیت جدید** • **سیستم عامل ها** • **لیست فایل ها**
۴۴	**نقشهای امنیتی**
محصول، قادر به مرتبط نمودن کاربران با نقشهای مجاز تعریف شده می باشد.	
۴۵	**لغو مشخصه های امنیتی ۱**
محصول می تواند توانایی لغو نام کاربری مربوط به موجودیتهای فعال و لغو مشخصه امنیتی یک موجودیت غیر فعال تحت کنترل خود را به مدیر سیستم محدود نماید.	

۷,۵ کلاس حفاظت از توابع امنیتی محصول

شماره الزام	عنصر امنیتی
۴۶	حفظ وضعیت امن در زمان شکست ۱
محصول می تواند در زمان رخداد انواع شکست های زیر، وضعیت امن را حفظ نمایند. شکست های نرم افزاری، سخت افزاری و شبکه ای توضیح: در صورت رخ دادن هرگونه شکستی کاربر عادی خطای کلی را می بیند و مدیر از روی سرور جزئیات و منشأ پیغام را مشاهده می نماید. بنابراین در صورت شکست سیستم همواره در وضعیت امن باقی خواهد ماند.	
۴۷	**سازگاری داده های امنیتی بین محصول و موجودیت امن ۱**
محصول در صورت استفاده از محصولات امن، می تواند تفسیر سازگار ممیزی، شناسه کاربری و رمز عبور را در زمان اشتراکگذاری دادههای امنیتی بین خود و دیگر محصولات امن، فراهم آورد.	
۴۸	**انتقال داده امنیتی در داخل محصول ۱**
محصول می تواند هنگام انتقال داده ها بین بخشهای مجزای خود، در برابر افشاء یا تغییر محافظت نماید.	

[شرکت مهندسی پارتیان ابتکار پایدار]

شماره الزام	عنصر امنیتی
۴۹	**مهرهای زمانی ۱**
محصول، می تواند قادر به ایجاد مهر های زمانی قابل اطمینان باشند.	

۸،۵ کلاس دسترسی به محصول

شماره الزام	نام الزام
۵۰	**محدودیت بر روی چندین نشست همزمان ۱**
محصول می تواند حداکثر تعداد نشستهای همزمان متعلق به یک کاربر را محدود نماید.	
۵۱	**محدودیت بر روی چندین نشست همزمان ۲**
محصول می تواند به صورت پیشفرض، یک نشست برای هر کاربر در نظر بگیرد.	
۵۲	**قفل کردن و خاتمه دادن به نشست ها ۵**
محصول می تواند کلیه نشستهای تعاملی راه دور را پس از مدت زمان قابل تنظیم توسط مدیر غیرفعال بودن، خاتمه دهد.	
۵۳	**قفل کردن و خاتمه دادن به نشست ها ۶**
محصول می تواند اجازه خاتمه نشست، از سوی کاربری که خود آغازگر نشست بوده است را بدهد.	
۵۴	**سوابق دسترسی به محصول ۱**
در صورت برقراری نشست به طور موفقیت آمیز، محصول قادر به نمایش آخرین تلاش)موفق/ناموفق(برای ایجاد نشست براساس روز، زمان می باشد.	

۶ الزامات تضمین امنیت

الزامات عملکرد تضمین توصیف کننده چگونگی ارزیابی هدف ارزیابی است. در این بخش الزامات EAL1 آورده میشود که لیست الزامات آن در جدول زیر آمده است.

نام کلاس	نام الزام	توضیحات
Development	ADV_FSP.1	مشخصات کارکرد ابتدایی
Guidance Documents	AGD_OPE.1	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده سازی
Tests	ATE_IND.1	آزمون مستقل- منطبق

Vulnerability Assessment	AVA_VAN.1	تحلیل آسیب پذیری
Life cycle Support	ALC_CMC.1	برچسب گذاری هدف ارزیابی
	ALC_CMS.1	پوشش پیکربندی هدف ارزیابی

۱,۶ کلاس توسعه

اطلاعات محصول، از طریق از سند هدف « مشخصات امنیتی محصول » و بخش « مستندات راهنمای کاربر» امنیتی در اختیار کاربر نهایی قرار میگیرد .الزامی بر وجود بخش در سند هدف « مشخصات امنیتی محصول» امنیتی نمی باشد، اما در صورت وجود باید محتوای آن با الزامات کارکردی مرتبط بوده و مورد تائید توسعه دهندگان محصول باشد.

۲,۶ مشخصات کارکردی

مشخصات کارکردی، واسطهای کارکرد امنیتی محصول را توصیف مینماید اما نیازی به شرح مفصل و کاملی از این واسطها نمیباشد. فعالیتهای این خانواده باید بر روی شناخت واسطهای معرفی شده در بخش «مشخصات امنیتی محصول» از سند هدف امنیتی و «مستندات راهنما» متمرکز می گردد.

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی ADV_FSP	نام عنصر :مشخصات کارکرد ابتدایی۰ شماره مؤلفه(ADV_FSP.1.1D (: شرح مؤلفه: توسعه دهنده باید مشخصات کارکردی را ارائه نماید.
	نام عنصر :مشخصات کارکرد ابتدایی۱ شماره مؤلفه ADV_FSP.1.2D شرح مؤلفه: توسعه دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه نماید.
مؤلفههای اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
	نکته کاربردی: مشخصات کارکردی دربرگیرنده اطلاعات مستندات راهنمای کاربردی) AGD_OPE (و راهنمای آمادهسازی « AGD_PRE (خلاصه مشخصات محصول) » و اطلاعاتی که در بخش سند هدف امنیتی ارائه شده است، میباشند .با توجه به دلایلی که باید در مستندات و بخش وجود داشته باشند،

	الزامات کارکردی تضمین میگردند .از آنجا « خلاصه مشخصات محصول» که مشخصات کارکردی مستقیماً با الزامات کارکرد امنیتی مرتبط شدهاند، بنابراین ارتباط مطرح شده در این الزام صورت گرفته است و نیازی به مستندات بیشتر نمیباشد.
مؤلفه های محتوایی	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی (ADV_FSP)	نام عنصر :مشخصات کارکرد ابتدایی ۱ شماره مؤلفه ADV_FSP.1.1C شرح مؤلفه: مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجرا کننده کارکرد امنیتی SFR-enforcing TSFI و پشتیبان کنندهی الزام کارکرد امنیتیSFR-supporting TSFI توصیف نماید.
مؤلفههای محتوایی	
نام خانواده	**عنصر امنیتی**
	نام عنصر :مشخصات کارکرد ابتدایی ۱ شماره مؤلفه ADV_FSP.1.2C شرح مؤلفه: مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجرا کننده کارکرد امنیتی و پشتیبان کننده ی الزام کارکرد امنیتی را مشخص نماید.
	نام عنصر :مشخصات کارکرد ابتدایی شماره مؤلفهADV_FSP.1.3C شرح مؤلفه: مشخصات کارکردی باید برای دسته بندی ضمنی واسطهای غیر مداخله کننده ی الزام کارکرد امنیتی دلایلی را ارائه نماید.
	نام عنصر :مشخصات کارکرد ابتدایی ۱ شماره مؤلفهADV_FSP.1.4C شرح مؤلفه: ردیابی باید نشان دهنده مرتبط شدن الزامات کارکرد امنیتی به واسطه ای کارکرد امنیتی در سند مشخصات کارکردی باشد.
مؤلفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**

مشخصات کارکردی (ADV_FSP)	نام عنصر :مشخصات کارکرد ابتدایی ۱ شماره مؤلفهADV_FSP.1.1E شرح مؤلفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام الزامات مؤلفه های محتوایی را برآورده مینماید.
	نام عنصر :مشخصات کارکرد ابتدایی ۱ شماره مؤلفه ADV_FSP.1.2E شرح مؤلفه: ارزیاب باید مشخص نماید که مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی میباشند.

مستندات «مشخصات کارکردی» جهت پشتیبانی از ارزیابی الزامات کارکردی و اقدامات لازم در کلاس های زیر ارائه شده است. «آسیبپذیری» و «تست» و «راهنما»

۳,۶ کلاس راهنمای کاربر

مستندات راهنما همراه با سند هدف امنیتی برای استفاده کاربران ارائه خواهند شد .در این دسته از مستندات شرحی از مدل مدیریتی و نحوه بررسی محیط عملیاتی توسط مدیر(تا مشخص گردد که آیا میتواند نقش خود را برای کارکرد امنیتی ایفا نماید)ارائه میشود.

برای هر محیط عملیاتی که در سند هدف امنیتی ادعای پشتیبانی از آن شده باید مستند راهنما ارائه گردد .این راهنما شامل: دستورالعمل نصب موفقیت آمیز محصول در محیط، دستورالعمل مدیریت امنیت محصول به عنوان یک محصول و به عنوان بخشی از یک محیط عملیاتی بزرگتر، دستورالعمل هایی که ارائه دهنده قابلیت مدیریتی محافظت شده از طریق استفاده از قابلیتهای محصول، محیط عملیاتی یا هر دو میباشد.

۴,۶ راهنمای کاربردی

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی (AGD_OPE)	نام عنصر :راهنمای کاربردی ۱ شماره مؤلفهAGD_OPE.1.1D شرح مؤلفه: توسعه دهنده باید راهنمای کاربردی ارائه نماید.

مؤلفه های محتوایی

[شرکت مهندسی پارتیان ابتکار پایدار]

نام خانواده	عنصر امنیتی
راهنمای کاربردی (AGD_OPE)	نام عنصر :راهنمای کاربردی ۱ شماره مؤلفهAGD_OPE.1.1C شرح مؤلفه: سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی را که باید در یک محیط پردازشی امن کنترل شوند توصیف نماید، همانند هشدارهای مناسب.

مؤلفه های محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی (AGD_OPE)	سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسطه ای در دسترس ارائه شده توسط محصول به صورت امن استفاده میگردد.
	نام عنصر :راهنمای کاربردی۱ شماره مؤلفه AGD_OPE.1.3C شرح مؤلفه: سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسطهای دردسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین نماید.
	نام عنصر :راهنمای کاربردی ۱ شماره مؤلفهAGD_OPE.1.4C شرح مؤلفه: سند راهنمای کاربردی باید برای هر نقش کاربری، هرنوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط نماید، همانند تغییر مشخصات امنیتی وجودیت های تحت کنترل توابع امنیتی محصول.

۵,۶ راهنمای آماده سازی

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای آماده سازی (AGD_PRE)	نام عنصر :راهنمای آماده سازی ۱ شماره مؤلفه AGD_PRE.1.1D شرح مؤلفه:

[شرکت مهندسی پارتیان ابتکار پایدار]

	توسعه دهنده باید محصول را همراه با سند آماده سازی ارائه نماید.

مؤلفه های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	نام عنصر :راهنمای آماده سازی شماره مؤلفه AGD_PRE.1.1C شرح مؤلفه: مستندات آمادهسازی بایدتمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه های تحویل توسعه دهنده شرح دهند.
	نام عنصر :راهنمای آماده سازی ۱ شماره مؤلفهAGD_PRE.1.2C شرح مؤلفه: مستندات آماده سازی باید تمام مراحل لازم برای نصب امن محصول و آماده سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکر شده در سند هدف امنیتی شرح دهند.

مؤلفه های اقدامات ارزیاب	
راهنمای آماده-سازی (AGD_PRE)	نام عنصر :راهنمای آمادهسازی ۱ شماره مؤلفهAGD_PRE.1.1E شرح مؤلفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مؤلفه های محتوایی را برآورده می نماید.
	نام عنصر :راهنمای آماده سازی ۱ شماره مؤلفه AGD_PRE.1.2E شرح مؤلفه: ارزیاب باید رویه های آماده سازی شرح داده شده در سند را بکار ببرد تا تائید نماید، محصول میتواند به صورت امن برای عمل نمودن آماده شود.

۶,۶ کلاس تست

تست محصول برای بررسی بخشهای کارکردی سیستم و همچنین بخش هایی که طراحی و پیاده سازی آنها برای سیستم دارای آسیب های امنیتی است، در نظر گرفته میشود .تست بخشهای کارکردی سیستم از طریق خانواده ATE_IND ، و تست بخشهایی که طراحی و پیاده سازی آسیب زایی دارند از طریق خانواده AVA_VAN صورت میگیرد .در این سطح از ارزیابی

[شرکت مهندسی پارتیان ابتکار پایدار]

(سطح) EAL1 تست براساس کارکردی که برای محصول در نظر گرفته شده و واسط هایی که بر اساس اطلاعات طراحی در اختیار ارزیاب قرار میگیرد، انجام میگردد .نتایج تست و تحلیل آسیب پذیری باید در گزارش تست لحاظ شوند این مسئله در الزامات زیر در نظر گرفته شده است.

۷,۶ تست مستقل

«تست مستقل برای تائید کارکرد محصول که در بخش مشخصات امنیتی محصول از سند هدف امنیتی و مستندات « راهنمای مدیر»

ارائه شده، صورت میگیرند .هدف اصلی تست اطمینان از برآورده شدن الزامات کارکردی مشخص شده در سند هدف امنیتی میباشد .ارزیاب باید در سند گزارش تست، طرح تست و نتایج آن را مستند نماید.

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
آزمون مستقل (ATE_IND)	نام عنصر :آزمون مستقل ۱ شماره مؤلفهATE_IND.1.1D شرح مؤلفه: توسعه دهنده باید برای آزمودن، محصول را ارائه نماید.

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
آزمون مستقل (ATE_IND)	نام عنصر :آزمون مستقل ۱ شماره مؤلفهATE_IND.1.1C شرح مؤلفه: محصول باید مناسب آزمودن باشد.

مؤلفه های اقدامات محتوایی	
آزمون مستقل ATE_IND	نام عنصر :آزمون مستقل ۱ شماره مؤلفه ATE_IND.1.1E شرح مؤلفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده، مؤلفه های محتوایی را برآورده می نماید.

[شرکت مهندسی پارتیان ابتکار پایدار]

	نام عنصر :تست مستقل ۱ شماره مؤلفهATE_IND.1.2E شرح مؤلفه: ارزیاب باید زیرمجموعه ای از توابع امنیتی محصول را تست نماید تا تائید نماید که توابع امنیتی محصول به صورت مشخص شده عمل می نمایند.

۸,۶ کلاس آسیب پذیری

۸,۶,۱ تحلیل آسیب پذیری

مولفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
آسیب پذیری (AVA_VAN)	نام عنصر: آسیبپذیری ۱ شماره مولفه: AVA_VAN.1.1D شرح مولفه: توسعه دهنده باید برای آزمودن، محصول را ارئه نماید.

مولفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
آسیب پذیری (AVA_VAN)	نام عنصر: آسیبپذیری ۱ شماره مولفه: AVA_VAN.1.1C شرح مولفه: محصول باید مناسب آزمودن باشد.

مولفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
آسیب پذیری (AVA_VAN)	نام عنصر: آسیبپذیری ۱ شماره مولفه: AVA_VAN.1.1E شرح مولفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده، تمام مولفه های محتوایی را برآورده می نماید.

	نام عنصر: آسیبپذیری ۱ شماره مولفه: AVA_VAN.1.2E شرح مولفه: ارزیاب باید برای شناسایی آسیب پذیریهای بالقوه در محصول، در منابع عمومی جستجویی را انجام دهد.
	نام عنصر: آسیبپذیری ۱ شماره مولفه: AVA_VAN.1.3E شرح مولفه: ارزیاب باید براساس آسیب پذیری های بالقوه شناسایی شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت میگیرند، مشخص نماید.

۸,۷ کلاس پشتیبانی از چرخه حیات

۸,۷,۱ قابلیت های پیکربندی

مولفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
آسیب پذیری (AVA_VAN)	نام عنصر: برچسب گذاری محصول ۱ شماره مولفه: ALC_CMC.1.1D شرح مولفه: توسعه دهنده باید محصول و مرجع محصول را ارائه نماید.

مولفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
آسیب پذیری (ALC_CMC)	نام عنصر: برچسب گذاری محصول ۱ شماره مولفه: ALC_CMC.1.1C شرح مولفه: محصول باید با یک مرجع یکتا برچسب زده شود.

مولفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**

[شرکت مهندسی پارتیان ابتکار پایدار]

آسیب پذیری (ALC_CMC)	نام عنصر: برچسب گذاری محصول ۱ شماره مولفه: ALC_CMC.1.1E شرح مولفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه های محتوایی را برآورده می نماید.

۸,۷,۲ حوزه پیکربندی

مولفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
آسیب پذیری (ALC_CMC)	نام عنصر: برچسب گذاری محصول ۱ شماره مولفه: ALC_CMS.1.1D شرح مولفه: ارزیاب باید لیست پیکربندی محصول را ارائه نماید.

مولفه های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
آسیب پذیری (ALC_CMC)	نام عنصر: برچسب گذاری محصول ۱ شماره مولفه: ALC_CMS.1.1C شرح مولفه: لیست پیکربندی باید شامل خود محصول و مدارک مورد نیاز توسط الزامات تضمین امنیتی باشد.
	نام عنصر: برچسب گذاری محصول ۱ شماره مولفه: ALC_CMS.1.1C شرح مولفه: لیست پیکربندی باید موارد پیکربندی را به صورت یکتا معرفی نماید.

مولفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
آسیب پذیری (ALC_CMC)	نام عنصر: برچسب گذاری محصول ۱ شماره مولفه: ALC_CMC.1.1E شرح مولفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه های محتوایی را برآورده می نماید.

۹ شرح خلاصه محصول

- نسخه ۱,۱ سند هدف امنیتی سامانه بروزرسانی تجهیزات امنیتی (سیبتا) توسط تیم فنی و توسعه شرکت مهندسی پارتیان ابتکار پایدار تهیه و تدوین شده است و رعایت الزامات کارکرد امنیتی زیر در آن ادعا شده است.

- محصول می تواند برای تمام رویدادهای ورود و خروج کاربر به/ از سیستم، کنترل دسترسی، مشخصه های امنیتی و دیگر رویدادهای قابل ممیزی رکورد ممیزی تولید نماید و برای هر رکورد ممیزی، حداقل اطلاعات تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال و نتیجه موفقیت یا شکست رویداد، نوع کاربری، IP کاربر، محل خدمت کاربر زیر را ثبت نماید و کاربر عامل هر یک از رویدادهای سیستم را شناسایی و ثبت کند.

- محصول دارای قابلیت خواندن/مشاهده ورود موفق، ورود ناموفق، تعلیق ورود، ویرایش، حذف و ایجاد آیتم جدید، صدور مجوز و گواهینامه، تکمیل فرم و تصحیح اطلاعات از کل رکوردهای ممیزی را برای مدیر سیستم و دارای قابلیت نمایش رکوردهای ممیزی را به شکل خوانا و قابل درک برای کاربر میباشد و میتواند از خواندن رکوردهای ممیزی توسط کاربران غیر مجاز جلوگیری کرده و امکان انجام مرتب سازی رکوردهای ممیزی را به نحوی فراهم نماید که کاربر مجاز بتواند آن رکوردها را براساس مرکز برگزار کننده، کاربر، نوع کاربری، تاریخ، موضوع و نوع رخداد عملیات مرتب نماید.

- از طریق خود نرم افزار امکان حذف غیر مجاز داده ممیزی وجود ندارد. کاربر تنها در صورتی امکان حذف داده ممیزی را دارد که به صورت غیر مجاز به پایگاه داده دسترسی داشته باشد و از آنجا عملیات حذف را انجام دهد که در آن حالت عملیات پیش گفته در پایگاه داده به طور خودکار ممیزی می شود. در صورت تجاوز دنباله ممیزی از مقدار حجم تعریف شده اولیه میتواند حجم مورد نظر را به صورت خودکار و مقداری که از پیش تعیین شده افزایش دهد. در صورت درخواست سازمان طرف قرار داد می توان MailServer برای پایگاه داده تعریف کرد که اگر حجم درایو کمتر از ۱۰۰ مگابایت یا حجم مشخص دیگری باقیمانده بود ایمیلی مبنی بر عدم وجود حجم کافی برای ذخیره سازی داده ممیزی به مدیر سیستم ارسال شود.

- می توان بر اساس مشخصه های شعبه، گروه کاربری، محدوده زمانی، موضوع، فرم و IP مجموعه از رویدادها را جهت ممیزی نمودن انتخاب نمود.

- محصول می تواند کلیدهای رمزنگاری نامتقارن را مطابق با الگوریتمهای تولید کلید استاندارد " استفاده از طرح RSA با اندازه کلید ۱۰۴۸ بیت یا بیشتر که از اسناد FIPS PUB ۱۸۶-۴ "Digital Signature Standard (DSS)"، Appendix B. 3." پیروی میکند تولید کنند و رمزنگاری و رمزگشایی را مطابق با الگوریتم رمزنگاری متقارن AES Key Wrap with Padding KWP مطابق سند NIST SP 38-800 F ، با اندازه کلید رمزنگاری ۱۱۸ و ۱۹۶ بیتی را انجام دهد.

[۱,۱] [۰۵-۱۴۰۳]

- می توان با استفاده از یک عدد مثبت قابل تنظیم از طرف مدیر سیستم تعداد تلاش های احراز هویت ناموفق را مدیریت نموده و حداکثر تعداد ورود ناموفق نام کاربری و گذرواژه را در سیستم تعریف کرد.

- محصول میتواند مشخصه های امنیتی شناسه کاربر داده های احراز هویت، نقش کاربر، وضعیت حساب کاربری فعال، غیرفعال، بلوکه شده و غیره، IP کاربر، رمز عبور کاربر و ایمیل کاربر را برای هر کاربر نگهداری نماید.

- محصول می تواند مشخصه های امنیتی شناسه کاربر، نقش های کاربر، جزئیات واسط کلاینت مرورگر ، IP ، پیشینه احرازهویت زمان آخرین تلاش احرازهویت موفق و ناموفق(تا ۳۰ دقیقه گذشته، پیشینه دسترسی به سند/رکورد اخیر ممیزی، را برای کاربر فعال نگهداری نماید.

- زمانیکه یک نشست جدید برقرار می شود، اطلاعات موجود از نشست های قبلی حذف میگردد. اطلاعات پیشینه احراز هویت بروزرسانی میشود. رکورد ممیزی برای ورود موفق/ناموفق کاربر در نشست جدید ثبت میگردد.

- محصول می تواند هنگام دریافت داده کاربری حداکثر حجم، را اعمال کرده و از مشخصه های امنیتی مرتبط با داده های کاربری را هنگام ورود داده ها استفاده نماید.

- محصول میتواند هنگام خروج داده کاربری به بیرون داده ها را در سه فرمت (pdf,png, Excel نمایش داده و از خروج داده های حساس مانند نام کاربری و کلمه عبور و ایمیل کاربر جلوگیری کند. امکان نگهداری داده کاربری حساس ذخیره شده در مکان تحت کنترل براساس مشخصه های رمزنگاری امن نگهداری کرده و آنها را به منظور شناسایی خطای صحت داده رکورد و داده ممیزی پایش کند.

- سیستم می تواند هنگام تشخیص خطای صحت داده ممیزی مربوطه را ثبت نماید.

- محصول می تواند دسترسی بر اساس نوع کاربری که بر اساس نقش های کاربر مشخص می شود را بر روی عملیات های مانند ایجاد، تغییر، ویرایش و حذف موجودیت های فعال و غیرفعال اعمال نماید.

- محصول می تواند سطح دسترسی را با توجه به هویت کاربر، نقش ها و مجوزهای کاربر مجاز و اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می شوند، بر روی موجودیت های غیرفعال اعمال نماید.

- می توان با اعمال تعیین سطح دسترسی بر اساس نقش ، توانایی تغییر پیشفرض، پرس و جو، تغییر، حذف، ایجاد مشخصه های امنیتی نام کاربری و کلمه عبور را به مدیر سیستم محدود نمود و امکان در نظرگرفتن مقادیر پیش فرض محدود شده محصول برای مشخصه های امنیتی که برای اعمال خط مشی استفاده می شوند، وجود داشته و مدیر سیستم از طریق فایل Config می تواند هنگام ایجاد اطلاعات یا موجودیت غیر فعال، مقادیر پیشفرض را لغو و تغییر دهد.

- محصول می تواند توانایی تغییر پیشفرض، پرس و جو، تغییر، حذف، پاک نمودن، ایجاد کاربر جدید، داده های ممیزی و داده های احراز هویت را به مدیر سیستم و توانایی تغییر پیشفرض، پرس و جو، تغییر پسورد به کاربر عادی محدود نماید.

- سیستم می تواند کاربران را با نقش های مجاز تعریف شده مرتبط نماید و امکان لغو نام کاربری مربوط به موجودیت های فعال و لغو مشخصه امنیتی یک موجودیت غیر فعال تحت کنترل خود را به مدیر سیستم محدود کند.

- در صورت رخ دادن هرگونه شکستی کاربر عادی خطای کلی را می بیند و مدیر از روی سرور جزئیات و منشأ پیغام را مشاهده می نماید. بنابراین در صورت شکست سیستم همواره در وضعیت امن باقی خواهد ماند.

- محصول می تواند هنگام انتقال داده ها بین بخشهای مجزای خود، از آنها در برابر افشاء یا تغییر محافظت نماید.

- محصول، قادر به ایجاد مهرهای زمانی قابل اطمینان می باشد.

- محصول می تواند کلیه نشست های تعاملی راه دور را پس از مدت زمان قابل تنظیم توسط مدیر غیرفعال بودن، خاتمه دهد و اجازه خاتمه نشست، از سوی کاربری که خود آغازگر نشست بوده است را بدهد.

- در صورت برقراری نشست به طور موفقیت آمیز، محصول قادر به نمایش آخرین تلاش موفق/ناموفق برای ایجاد نشست براساس روز، زمان می باشد.

- محصول، می تواند مسیر ارتباطی امنی را با استفاده از پروتکل TLS, HTTPS میان خود و موجودیت IT معتبر همچون سامانه کاربر، سرور ممیزی و سرور احراز هویت که به طور منطقی از کانال های دیگر متمایز است فراهم نماید تا آنها را احرازهویت کرده و از داده های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد. همچنین محصول می تواند اجازه داشته باشد به موجودیتهای معتبر IT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند و تمامی بخش های سیستم. سازگاری کامل با پروتکل های امن SSL و غیره را دارند.