به نام خدا

سندهدف امنیتی

APKSIEM-v7

فنی و مهندسی امن پردازان کویر

شهریور ۱۴۰۲

نسخه ۱,۶

فهرست

۱ معرفی سند هدف امنیتی

۱,۱ مرجع سند هدف امنیتی و محصول

عنوان سند هدف امنیتی	سند هدف امنیتی APKSIEM
نسخه	۱,۴
تاریخ	۱۴۰۱/۱۰/۰۱
نویسندگان	گروه توسعه APKSIEM شرکت امن پردازان کویر

نام تولید کننده (شرکت)	فنی مهندسی امن پردازان کویر
نام محصول	APKSIEM
نوع محصول	SIEM (Security information and event management)
نسخه	۷

۲,۱ نوع محصول

محصول مورد ارزیابی امکان اجرا هم بصورت ماشین‌مجازی و هم نصب مستقیم بروی سخت‌افزار را دارد؛ در هرکدام از حالت‌ها حداقل الزامات به شرح زیر است:

۳,۱ نرم‌افزار/سخت‌افزار/میان‌افزار پیش نیاز محصول

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

عناصر محصول	شماره مدل یا نسخه
نسخه نرم‌افزار/میان‌افزار	۷
سیستم عامل	Debian 11 (bullseye)
…	…

کامپوننت‌ها	حداقل الزامات
APKSIEM	دستگاه APKSIEM
مرورگر	Mozilla Firefox 40 or Higher Google Chrome 50.0 Safari 10 or Higher
SSH Client	کلاینت SSH (نظیر PUTTY) با قابلیت پشتیبانی از SSHv2

۴,۱ شرح محصول

در این قسمت محصول و کارکرد امنیتی آن به همراه کامپوننت‌های اصلی شرح داده می‌شود. در ادامه این بخش حوزه فیزیکی و حوزه منطقی محصول مطرح می‌شود. برای اطلاعات بیشتر جهت تکمیل این قسمت به بخش ۳,۶,۲ از سند «راهنمای نوشتن سند هدف امنیتی» مراجعه شود.

۵,۱ حوزه فیزیکی

عناصر سخت‌افزاری و نرم‌افزاری مورد استفاده با توجه به پیکربندی ارزیابی در جدول زیر معرفی می‌شود:

عناصر محصول	شماره مدل یا نسخه
نام ماژول	ILB
سیستم عامل	Debian 11 (bullseye)
پردازنده	Intel Core i7, 3.4 GHz
حافظه	8 GB RAM or Higher
اتصالات شبکه	100 Mbps Ethernet or Higher
فضای دیسک	100 GB or Higher

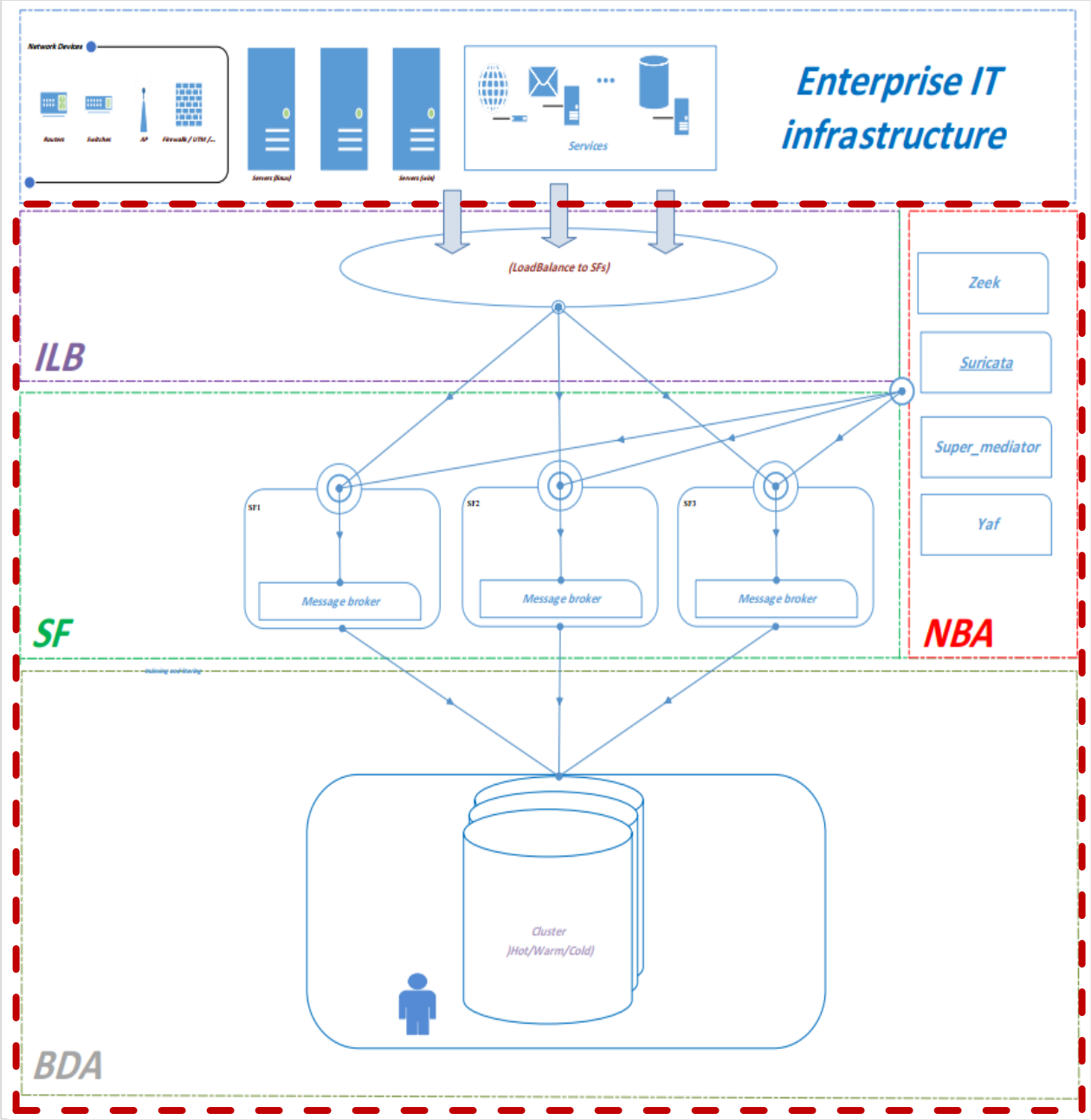
عناصر محصول	شماره مدل یا نسخه
نام ماژول	SF
سیستم عامل	Debian 11 (bullseye)
پردازنده	Intel Core i7, 3.4 GHz
حافظه	16 GB RAM or Higher

اتصالات شبکه	100 Mbps Ethernet or Higher
فضای دیسک	250 GB or Higher

عناصر محصول	شماره مدل یا نسخه
نام ماژول	NBA
سیستم عامل	Debian 11 (bullseye)
پردازنده	Intel Core i7, 3.4 GHz
حافظه	16 GB RAM or Higher
اتصالات شبکه	100 Mbps Ethernet or Higher 100 Mbps Ethernet or Higher which supports Promiscuous Mode (For IDS Service)
فضای دیسک	150 GB or Higher

عناصر محصول	شماره مدل یا نسخه
نام ماژول	BDA
سیستم عامل	Debian 11 (bullseye)
پردازنده	Intel Core i7, 3.4 GHz
حافظه	16 GB RAM or Higher
اتصالات شبکه	100 Mbps Ethernet or Higher
فضای دیسک	500 GB or Higher

در شکل زیر نحوه قرارگیری محصول APKSIEM در محیط عملیاتی آمده است. محصول مورد ارزیابی با علامت خط‌چین مشخص شده است.



۶,۱ حوزه منطقی

کارکردها	توصیف
احراز هویت	محصول مورد ارزیابی در سمت وب، در ماژول های مختلف مستقل از سیستم‌عامل مکانیزم احرازهویت را با استفاده از نام‌کاربری و گذرواژه و با ویژگی انتخاب قابلیت‌های Captcha و ارسال کدیکبارمصرف انجام می‌دهد.
کنترل دسترسی	سرپرست امنیتی می‌تواند سطح دسترسی هرکاربر به هرکدام از منوها و زیرمنوها را تعیین کند.
مدیریت ظرفیت ذخیره‌سازی	برای مدیریت ظرفیت ذخیره سازی دو سرویس با نام‌های retention-policy برای مدیریت فضای داده‌های دیتابیس و apk-resman برای داده‌های فایلی سامانه در نظرگرفته شده‌است. همچنین ویژگی ILM (Index lifecycle management) از قابلیت‌های داخلی سامانه برای مدیریت حجم و ایندکس‌ها می‌باشد که برای مدیریت چرخه حیات indexها به صورت اتوماتیک استفاده می‌شود تا لاگ‌های قدیمی‌تر که نیاز به جستجوی آن‌ها کاهش می‌یابد به منابع و سیستم‌های ارزان‌تر و کم‌سرعت‌تر منتقل شوند و لاگ‌های خیلی قدیمی‌تر که دیگر نیازی به نگهداری آن‌ها نمی‌باشد به طور کامل حذف شوند.

۲ ادعای انطباق

۱,۲ انطباق با استاندارد ارزیابی امنیتی معیار مشترک

انطباق با استاندارد ارزیابی امنیتی معیار مشترک	ISO/IEC 15408, version 3.1, revision 5, April 2017
نام پروفایل حفاظتی	SIEM Protection Profile 2.2
سطح تضمین امنیتی	EAL1

۳ تعریف مسائل امنیتی

۱,۳ خط‌مشی

خط مشی‌ها	توصیف
مسئولیت‌پذیری	تمام کاربران مجاز محصول باید مسئول اقداماتشان باشند.

اهداف مجاز	تمام داده‌های جمع‌آوری‌شده، ذخیره‌شده و تحلیل‌شده توسط محصول باید برای اهداف مجاز استفاده گردد.
تجزیه‌وتحلیل	پردازش‌های تحلیلی و اطلاعاتی که از استنتاج‌های صورت گرفته در رابطه بانفوذها (گذشته، حال، آینده) ناشی شده‌اند باید به داده SIEM اعمال گردد و اقدام مناسبی صورت گیرد.
تشخیص	اطلاعات پیکربندی ایستا باید جمع‌آوری گردد زیرا ممکن است از پتانسیل برای نفوذ در آینده یا رویداد مجدد نفوذ قبلی در یک سیستم IT حکایت نماید
مدیریت	محصول باید توسط کاربران مجاز مدیریت گردد.
محافظت از تغییرات	داده‌های تحلیل‌شده و تولیدشده توسط محصول باید از تغییرات محافظت گردند.
جلوگیری از ورود غیرمجاز	محصول باید از ورود غیرمجاز همچون قطع اجرای برنامه‌های معمولی محافظت نماید.

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 مکانیزم‌های امنیتی، صحت و محرمانگی داده‌هایی که توسط SIEM جمع‌آوری، ذخیره یا تحلیل‌شده‌اند را به خطر اندازد.
دسترسی غیرمجاز	کاربر غیرمجاز ممکن است با دور زدن مکانیزم‌های امنیتی سعی در افشاء داده‌هایی که توسط محصول جمع‌آوری، ذخیره یا تحلیل‌شده‌اند، نماید.
حذف غیرمجاز	کاربر غیرمجاز ممکن است داده‌هایی را که توسط محصول جمع‌آوری، ذخیره یا تحلیل‌شده‌اند را با دور زدن مکانیزم‌های امنیتی از بین ببرد.
تزریق لاگ	کاربر غیرمجاز ممکن است با وارد نمودن داده‌ای که محصول نتواند آن را بکار برد، سبب بدعمل نمودن محصول گردد.
مخاطرات دسترس‌پذیری	کاربر غیرمجاز ممکن است با متوقف نمودن اجرای محصول، سعی در به خطر انداختن پیوستگی عملکرد تحلیل محصول نماید.
مخاطرات افزایش حق دسترسی	کاربر غیرمجاز ممکن است با دستیابی به محصول و با استفاده از مجوزهای سیستمی به عملکرد امنیتی محصول و داده‌های آن دستیابی پیدا نماید.
مخاطرات پیکربندی	محصول ممکن است توسط افراد مجاز یا غیرمجاز به‌صورت نامناسبی پیکربندی گردد و سبب نفوذ بالقوه‌ای گردد که تشخیص داده نمی‌شود.
واکنش آسیب‌پذیری	محصول ممکن است در واکنش نشان دادن به آسیب‌پذیری‌های شناسایی‌شده یا مورد ظن یا فعالیت‌های نامناسب با شکست روبرو گردد.

تشخیص آسیب‌پذیری	محصول ممکن است در تشخیص آسیب‌پذیری‌ها یا فعالیت‌های نامناسب بر اساس داده‌هایی که SIEM دریافت نموده با شکست مواجه گردد.

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	سخت‌افزار و نرم‌افزار محصول که به اجرای خط‌مشی‌های امنیتی حساس هستند، از هرگونه تغییرات فیزیکی غیرمجاز محافظت می‌گردند.
محل استقرار	منابع پردازشی محصول در داخل فضایی قرار می‌گیرند که ازنظر دسترسی کنترل‌شده هستند تا از دسترسی فیزیکی غیرمجاز جلوگیری شود.
مدیریت	یک یا بیش از یک فرد دارای صلاحیت برای مدیریت محصول و امنیت اطلاعات آن به محصول اختصاص داده می‌شود.
سرپرست مورد اعتماد	سرپرست۱ مجاز فردی بی‌دقت یا متخاصم نیست و دستورات ارائه‌شده توسط مستندات محصول را دنبال می‌نماید.
دسترسی امن	محصول تنها توسط کاربران مجاز قابل‌دسترسی است.

۴ اهداف امنیتی

۱,۴ اهداف امنیتی برای هدف ارزیابی

هدف امنیتی	توصیف
محافظت	محصول باید خود را در برابر تغییرات غیرمجاز و دسترسی به عملکردهایش و داده‌هایش محافظت نماید.
تحلیل خروجی IDS	تحلیل‌گر باید از سنسورهای IDS و اسکنرهای IDS داده را بپذیرد و سپس پردازش‌های تحلیلی بر روی‌داده‌ها انجام دهد و اطلاعات ناشی از نتایج نفوذها (گذشته، حال، آینده) را بکار برد.
عکس‌العمل مناسب	محصول باید به‌طور مناسب به نتایج تحلیل عکس‌العمل نشان دهد.
مدیریت	محصول باید شامل مجموعه‌ای از کارکردها باشد که اجازه مدیریت مؤثر کارکردها و داده‌هایش را بدهد.

۱ Administrator

دسترسی مجاز	محصول باید بتواند کاربران مجاز را به کارکردها و/یا داده‌هایی محدود نماید که برای نقش آن‌ها یا سطح دسترسی‌شان مناسب است.
ممیزی	محصول باید برای داده‌های مورد دستیابی، رکوردهای ممیزی را ثبت کرده و از کارکردهای تحلیل‌گر استفاده نماید.
احراز هویت	محصول پیش از آنکه اجازه دسترسی به کارکردها و داده‌های محصول به کاربران مجاز داده شود باید قادر به شناسایی و احراز هویت آن‌ها باشند.
صحت	محصول باید از صحت تمام داده‌های ممیزی و تحلیل‌گر اطمینان حاصل نماید.
سرریزی	محصول باید به‌طور مناسب سرریزی که در ذخیره داده‌ی تحلیل‌گر و ممیزی رخ می‌دهد را بکار ببرد.

۲,۴ اهداف امنیتی برای محیط عملیاتی

هدف امنیتی	توصیف
محافظت از ممیزی	محیط IT قابلیتی برای محافظت از اطلاعات ممیزی ارائه خواهد داد.
مرتب‌سازی ممیزی	محیط IT قابلیتی برای مرتب‌سازی اطلاعات ممیزی ارائه خواهد داد.
کنترل دسترسی	افرادی که مسئول محصول هستند باید اطمینان یابند که تمام مجوزهای دسترسی توسط کاربران به صورتی که با امنیت IT سازگار باشد، محافظت‌شده است.
نصب	افرادی که مسئول محصول هستند باید اطمینان یابند که محصول به‌صورت سازگار با امنیت IT تحویل گرفته‌شده، نصب‌شده، مدیریت‌شده و عمل می-نماید.
مجتمع	محصول دارای قابلیت همکاری با سیستم IT که مانیتور می‌نماید و دیگر قسمت‌های IDS است.
کارکنان	کارکنانی که به‌عنوان سرپرستان مجاز کار می‌نمایند باید با دقت انتخاب شوند و در ارتباط باکار نمودن صحیح تحلیل‌گر آموزش ببینند.
امنیت فیزیکی	افرادی که مسئول محصول هستند باید از محافظت شدن بخش‌های مهم محصول از هرگونه حمله فیزیکی اطمینان یابند.

۵ الزامات کارکرد امنیتی

۱,۵ کلاس ممیزی امنیت

شماره الزام	عنصر امنیتی
۱	تولید داده ممیزی ۱
محصول مورد ارزیابی باید بتواند سوابق ممیزی را برای رویدادهای قابل ممیزی زیر تهیه کند:	

الف) آغاز و اتمام توابع ممیزی؛

ب) تمام اقدامات مدیریتی شامل موارد زیر:

- ورود و خروج مدیریتی به سیستم (درصورتی‌که مدیران سیستم نیاز به حساب کاربری شخصی داشته باشند، نام حساب کاربری آن‌ها نیز باید ثبت شود)
- تغییرات امنیتی در پیکربندی (علاوه بر اطلاعات حاکی از تغییرات رخداده ، باید ثبت شود که چه مواردی تغییر کرده‌اند)
- تولید، واردکردن، تغییر، یا پاک کردن کلیدهای رمزنگاری (علاوه بر این کار، نام کلید اختصاصی یا یک مرجع کلید نیز باید ثبت شود)
- تغییر کلمه عبور (نام حساب کاربری مربوطه نیز باید ثبت شود)
- هیچ اقدام دیگر

ت) اختصاصاً لیست رویدادهای قابل ممیزی تعریف شده در جدول زیر

- همه مواردی که از ساز و کار شناسایی و احراز هویت استفاده می کنند (ارائه کردن شناسه کاربری، مبدا تلاش)
- همه مواردی که از سازوکارهای احراز هویت استفاده می‌کنند. (مبدا تلاش)
- تلاش ناموفق برای اعتبارسنجی یک گواهینامه (دلیل ناموفق بودن و شکست خوردن)
- هر گونه تلاش برای شروع یک به روزرسانی دستی
- شروع به روز رسانی؛ نتیجه تلاش به روزرسانی (موفقیت یا شکست)
- تغییرات زمانی
- هرگونه تلاش در باز کردن یک نشست تعاملی
- پایان دادن به نشست راه دور تو سط ساز و کارهای قفل نمودن نشست
- پایان دادن یک نشست تعاملی
- راه اندازی یک کانال امن / پایان کانال امن / شکست در عملکرد کانال امن
- راه اندازی یک کانال امن / پایان کانال امن / شکست در عملکرد مسیر امن

۲	تولید داده ممیزی ۲

محصول مورد ارزیابی باید در هر یک از سوابق ممیزی، دست‌کم اطلاعات زیر را ثبت نماید:

الف) تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت۲ فعال و نتیجه رویداد (موفقیت یا شکست)؛ و

ب) در مورد هر یک از انواع رویدادهای ممیزی و بر اساس تعریف رویدادهای قابل ممیزی ارائه‌شده در پروفایل حفاظتی یا هدف امنیتی، اطلاعات در نکته کاربردی ۳ مشخص‌شده است.

برای الزام شماره ۱۶ و ۱۷ « مدیریت احرازهویت ناموفق» اطلاعات ممیزی تلاش‌های ناموفق که از تعداد مجاز بیشتر بوده است، ثبت می‌شود. این اطلاعات باید شامل منشأ تلاش صورت گرفته (مانند آدرس IP) باشد.

برای الزام شماره ۲۱ «سازوکار احرازهویت بر اساس رمز عبور» اطلاعات ممیزی تمام کاربردهای مکانیزم تعیین هویت و احرازهویت ثبت می‌شود. این اطلاعات باید شامل منشأ تلاش صورت گرفته (مانند آدرس IP) باشد.برای الزام شماره ۲۹ «مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی امن» اطلاعات ممیزی مربوط به هرگونه تلاش برای آغاز یک به‌روزرسانی، دستی ثبت می‌شود.

برای الزام شماره ۲۴ «مدیریت داده‌های محصول» اطلاعات ممیزی تمام فعالیت‌های مدیریتی داده‌های محصول ثبت می‌شود.

برای الزامات شماره ۳۳ الی ۳۵ «به‌روزرسانی امن» اطلاعات ممیزی مربوط به آغاز به‌روزرسانی، نتیجه تلاش‌های به‌روزرسانی (موفقیت یا شکست) ثبت می‌شود.

برای الزام شماره ۳۶ «مهرهای زمانی۳» اطلاعات ممیزی مربوط به تغییرات صورت گرفته در زمان ثبت می‌شود. این اطلاعات باید شامل زمان‌های جدید و قدیم، منشأ تلاش (مانند آدرس IP) برای تغییر زمان موفق یا ناموفق باشد.

برای الزام ۳۸ «قفل‌کردن و خاتمه دادن به نشست‌ها ۷» اگر "قفل کردن" انتخاب شود، اطلاعات ممیزی تمام تلاش‌های صورت گرفته برای باز کردن قفل یک نشست تعاملی ثبت می‌شود. در صورتی که "خاتمه دادن" انتخاب شود، اطلاعات ممیزی مربوط به خاتمه دادن یک نشست محلی از طریق یک مکانیزم قفل‌کردن نشست ثبت می‌شود.

برای الزام ۳۹ «قفل‌کردن و خاتمه دادن به نشست‌ها 5» اطلاعات ممیزی مربوط به خاتمه دادن یک نشست راه‌دور از طریق یک مکانیزم قفل‌کردن نشست ثبت می‌شود.

برای الزام ۴۰ « قفل‌کردن و خاتمه دادن به نشست‌ها ۶» اطلاعات ممیزی مربوط به خاتمه دادن یک نشست تعاملی ثبت می‌شود.

برای الزامات ۴۲ الی ۴۴ «کانال امن» اطلاعات ممیزی مربوط به آغاز کردن کانال امن / خاتمه دادن کانال امن / شکست توابع کانال امن ثبت می‌شود. این اطلاعات باید شامل شناسایی دلیل و هدف تلاش ناموفق برای ایجاد کانال امن باشد.

---

۲ Subject

۳ Time stamps

برای الزامات ۴۵ الی ۴۷ «مسیر امن» اطلاعات ممیزی مربوط به آغاز کردن مسیر امن / خاتمه دادن مسیر امن / شکست توابع مسیر امن ثبت می‌شود.	
۳	تولید داده ممیزی ۳
در مورد آن دسته از رویدادهای ممیزی که حاصل اقدامات کاربران احرازهویت‌شده هستند، محصول مورد ارزیابی باید بتواند هر رویداد قابل ممیزی را با هویت کاربری که مسبب آن رویداد شده است، مرتبط سازد.	
۴	محل ذخیره‌سازی داده‌های ممیزی ۱
محصول باید قادر به ارسال داده ممیزی تولید شده به یک موجودیت IT خارجی با استفاده از کانال امن مطابق با الزام FTP_ITC.1 باشد.	
۵	محل ذخیره‌سازی داده‌های ممیزی ۲
محصول مورد ارزیابی باید بتواند داده‌های ممیزی تولیدشده را در خود ذخیره کند. • هدف ارزیابی باید یک هدف ارزیابی توزیع شده باشد که داده‌های ممیزی را روی اجزاء هدف ارزیابی زیر ذخیره می‌کند: ▪ در ماژول BDA و در قسمت داشبوردها می‌توان نحوه نمایش لاگ ها را شخصی سازی کرد.	
۶	محل ذخیره‌سازی داده‌های ممیزی ۳
درصورتی که فضای حافظه محلی داده ممیزی پرشده باشد محصول مورد ارزیابی باید سوابق ممیزی گذشته را بر اساس قوانین بازنویسی سوابق ممیزی گذشته حذف کند.	

۲,۵ پشتیبانی رمزنگاری (FCS)

شماره الزام	عنصر امنیتی
۷	مدیریت کلید رمزنگاری ۱
محصول مورد ارزیابی باید بر اساس الگوریتم‌های تولید کلید رمزنگاری مشخص شده، کلیدهای رمزنگاری نامتقارن را تولید کند: • الگوهای RSA با استفاده از کلیدهای رمزنگاری با اندازه‌های ۲۰۴۸ بیت یا بزرگتر که این الزامات را رعایت کنند: FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS)، پیوست B.3. • الگوهای ECC با استفاده از <<منحنی های NIST>> P-256, P-384, P-521 بر اساس این الزامات: FIPS PUB 186-4،استاندارد امضای دیجیتال (DSS) پیوست B.4	
۸	مدیریت کلید رمزنگاری ۲

محصول مورد ارزیابی باید استقرار کلید رمزنگاری را بر اساس یک روش خاص استقرار کلید رمزنگاری انجام دهد:

- الگوهای استقرار کلید منحنی بیضوی که این الزامات را رعایت کنند: شماره ویژه NIST 800-56A، مرور۲
<<توصیه هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته>>

۹	مدیریت کلید رمزنگاری ۴

محصول مورد ارزیابی باید کلیدهای رمزنگاری را بر اساس یک روش خاص برای نابودی کلیدهای رمزنگاری، از بین ببرد :

- در مورد کلیدهای با متن ساده در ذخیره سازی فرار، نابودی باید از طریق یک بازنویسی ساده و مستقیم شامل از بین بردن ارجاع مستقیم به کلید پس از درخواست جمع آوری مقادیر باقی مانده انجام شود.
- در مورد کلیدهای با متن ساده در ذخیره سازی غیر فرار، نابودی باید از طریق فراخوانی یک رابط ارائه شده توسط بخشی از توابع امنیتی هدف امنیتی که آموزش بخشی از محصول برای تخریب انتزاعی که نشان دهنده کلید است باشد.

۱۰	عملیات رمزنگاری ۱ (۱)

محصول مورد ارزیابی باید رمزگذاری و رمزگشایی را بر اساس الگوریتم‌های رمزنگاری خاص AES که در حالت CTR و در اندازه‌های کلید ۱۲۸ و ۲۵۶ بیتی استفاده می‌شوند و با توجه به استاندارد AES که در ISO 18033-3 تعریف‌شده است، CTR مشخص شده در ISO 10116، GCM همانطور که در ISO 19772 مشخص شده است انجام دهد.

۱۱	عملیات رمزنگاری ۱ (۲)

توابع امنیتی مورد ارزیابی باید خدمات امضای رمزنگاری (تولید و تائید) را بر اساس الگوریتم‌های رمزنگاری خاص ارائه کند:

- الگوریتم امضای دیجیتال RSA و کلید رمزنگاری با اندازه‌های (ماژول‌ها) 2048 بیتی

با رعایت موارد زیر:

- در مورد الگوهای RSA: FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS)»، بخش 5.5، با استفاده از الگوی امضای RSASSA-PSS نسخه PKCS #1 v2.1 و/یا RSASSA-PKCS1v1_5؛ ISO/IEC 9796-2، الگوی امضای دیجیتال 2 یا الگوی امضای دیجیتال 3
- در مورد الگوهای ECDSA: FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS)»، بخش 6 و پیوست D با اجرای منحنی های P-256 NIST؛ ISO/IEC 14888-3 بخش ۶,۴

۱۲	عملیات رمزنگاری ۱ (۳)
توابع امنیتی مورد ارزیابی باید خدمات درهم‌سازی رمزنگاری را بر اساس یک الگوریتم رمزنگاری مشخص SHA-1، SHA-256 و اندازه‌پیام هشدار 160 ,256 بیت با رعایت استاندارد ISO/IEC 10118-3:2004، ارائه نماید.	
۱۳	عملیات رمزنگاری ۱ (۴)
محصول مورد ارزیابی باید احرازهویت پیام مبتنی بر کلید درهم‌سازی شده را بر اساس الگوریتم رمزنگاری خاص HMAC-SHA-1,HMAC-SHA-256, HMAC-SHA-512 و با استفاده از اندازه‌های کلید ۲۵۶ و ۵۱۲ و ۱۶۰ و اندازه‌های خلاصه پیام ۲۵۶ و ۵۱۲ و ۱۲۰ بیت و با توجه به موارد مطرح‌شده در بخش هفتم ISO/IEC 9797-2:2011 با نام «الگوریتم ۲ MAC» انجام دهد.	
۱۴	تولید بیت تصادفی ۱
محصول مورد ارزیابی باید تمامی خدمات تولید بیت تصادفی قطعی را بر اساسISO/IEC 18031:2011 و با استفاده از CTR_DRBG (AES) ارائه دهد.	
۱۵	تولید بیت تصادفی ۲
RGB قطعی باید دست کم توسط یک منبع آنتروپی تغذیه شود؛ و این منبع باید آنتروپی را از یک منبع نویز مبتنی بر نرم افزار (که این منبع خود نویز را از درایور های دستگاه جمع اوری میکند. /dev/random) گردآوری کند. این آنتروپی باید دست کم ۱۲۸بیت و حداقل معادل بالاترین قدرت امنیتی کلیدها و درهم سازهای تولیدشده مورد اشاره در ISO/IEC 18031:2011 از کلیدها و CSPهایی که تولید خواهد کرد، باشد.	

۳,۵ کلاس شناسایی و احرازهویت

شماره الزام	عنصر امنیتی
۱۶	مدیریت احرازهویت ناموفق ۱
محصول، باید هنگامی که یک عدد صحیح مثبت قابل تنظیم توسط سرپرست در بازه ۲ تا ۲۵۵ از تلاشهای ناموفق احراز هویت مربوط به تلاش سرپرست برای احراز هویت راه دور رخ داد، مشخص نمایند.	
۱۷	مدیریت احرازهویت ناموفق ۲
زمانی که تعداد تعیین شده از تلاشهای احراز هویت ناموفق صورت گرفت، محصول باید • احراز هویت موفق سرپرست راه دور متخلف را تا اتمام زمان تعیین شده توسط مدیر، محدود کند.	
۱۸	مدیریت رمز عبور ۱

توابع امنیتی مورد ارزیابی باید قابلیتهای مدیریت کلمه عبور زیر را برای کلمه عبور سرپرست محصول فراهم آورد: الف) گذرواژه را باید بتوان با هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای ویژه مطرح شده در این بخش ساخت: ["!", "@", "#","$", "٪", "^", "&", "*", "(", ")"،]; ب) حداقل طول کلمه عبور باید بین ۸ و حداکثر ۲۵۵ قابل پیکربندی باشد.

۱۹	شناسایی و احرازهویت کاربر ۱
محصول مورد ارزیابی پیش از آن که از دیگر موجودیت‌های خارج از محصول بخواهد که فرایند تعیین و احرازهویت را انجام دهد، باید اجازه انجام فعالیت‌های زیر را بدهد: • نمایش بنر اخطار با توجه به الزام FTA_TAB.1 • هیچ اقدام دیگری	
۲۰	شناسایی و احرازهویت کاربر ۲
پیش از آن که توابع امنیتی مورد ارزیابی امکان انجام هر اقدامات میانی دیگری از طرف کاربر مدیریتی سیستم را فراهم آورد، باید مدیر سیستم را با موفقیت شناسایی و احراز هویت نماید.	
۲۱	سازوکار احرازهویت بر اساس رمزعبور ۲
توابع امنیتی مورد ارزیابی باید یک مکانیسم احراز هویت مبتنی بر کلمه عبور محلی، هیچ مکانیسم احراز هویتی را برای احراز هویت کاربر مدیر محلی فراهم آورد.	
۲۲	احرازهویت کاربر ۱۰
هنگامی که فرایند احرازهویت بر روی کنسول محلی در حال جریان است، محصول مورد ارزیابی تنها باید بازخورد مبهم را در اختیار سرپرست محصول قرار دهد.	

۴,۵ کلاس مدیریت امنیت

شماره الزام	عنصر امنیتی
۲۳	مدیریت کارکرد در محصول ۱ (۱)/ به روزرسانی امن
توابع امنیتی مورد ارزیابی باید توانایی فعال کردن توابع به منظور به روزرسانی دستی را به سرپرست امنیتی محدود نماید.	
۲۴	مدیریت داده های محصول ۱
توابع امنیتی مورد ارزیابی باید امکان «مدیریت» داده‌های محصول را به سرپرست‌های امنیتی محدود کند.	
۲۵	کارکرد مدیریتی محصول ۱
محصول مورد ارزیابی باید قابلیت انجام کارکردهای مدیریتی زیر را داشته باشد:	

- توانایی مدیریت محصول به‌صورت محلی و از راه دور
- توانایی پیکربندی بنر دسترسی
- توانایی پیکربندی زمان غیرفعال بودن نشست پیش از قفل‌کردن یا خاتمه دادن آن
- توانایی به‌روزرسانی محصول مورد ارزیابی و تأیید به‌روزرسانی‌ها با استفاده از امضای دیجیتال پیش از نصب شدن این به‌روزرسانی‌ها
- توانایی پیکربندی پارامترهای شکست احرازهویت برای الزام FIA_AFL.1
- توانایی شروع و متوقف کردن سرویس‌ها
- توانایی پیکربندی رفتار ممیزی
- توانایی مدیریت کلیدهای رمزنگاری
- توانایی پیکربندی مدت زمان برای SA درIPsec
- توانایی تنظیم زمانی که برای مهرهای زمانی استفاده میشود.
- توانایی مدیریت انبار اطمینان هدف ارزیابی و تعیین گواهیهای v3.X509 به عنوان لنگر اطمینان
- توانایی وارد کردن گواهی v3.X509 به انبار اطمینان هدف ارزیابی
- توانایی تغییر رفتار انتقال داده ممیزی به یک موجودیت فناوری اطالعات خارجی، بررسی دادههای ممیزی، عملکرد ممیزی وقتی که فضای ذخیرهسازی محلی پر است.
- توانایی پیکربندی مرجع شناسایی همتا

۲۶	نقش‌های امنیتی ۳

محصول باید نقش‌های زیر را نگهداری کند.

- سرپرست امنیتی

۲۷	نقش‌های امنیتی ۴

در این الزام محصول مورد ارزیابی باید بتواند بین کاربران و نقش‌ها ارتباط برقرار نماید.

۲۸	نقش‌های امنیتی ۵

توابع امنیتی مورد ارزیابی باید از برقرار بودن شرایط زیر اطمینان حاصل کند:

- نقش سرپرست امنیتی باید بتواند محصول مورد ارزیابی را به صورت محلی مدیریت کند.
- نقش سرپرست امنیتی باید بتواند محصول مورد ارزیابی را از راه دور مدیریت کند.

۵,۵ کلاس حفاظت از محصول مورد ارزیابی

شماره الزام	عنصر امنیتی
۲۹	محافظت از داده‌های محصول (کلیدهای متقارن) ۱
محصول مورد ارزیابی باید از خواندن تمام کلیدهایی که از پیش به اشتراک گذاشته شده‌اند، کلیدهای متقارن و کلیدهای خصوصی جلوگیری به عمل آورد.	
۳۰	حفاظت از کلمه عبور سرپرست محصول ۱
محصول مورد ارزیابی نباید کلمه‌های عبور را به شکل متن ساده ذخیره کند.	
۳۱	حفاظت از کلمه عبور سرپرست محصول ۲
محصول مورد ارزیابی باید از خوانده شدن گذرواژه‌هایی که به‌صورت متن ساده هستند، جلوگیری کند.	

۶,۵ تست محصول مورد ارزیابی

شماره الزام	عنصر امنیتی
۳۲	خودآزمایی محصول ۱

محصول مورد ارزیابی باید مجموعه‌ای از این خودآزمایی‌ها را به طور دوره‌ای (دو دقیقه یکبار برای فعال‌بودن سرویس‌های حیاتی) در حین کارکرد دستگاه برای نشان دادن کارکرد صحیح محصول مورد ارزیابی انجام دهد:

- بررسی درحال‌اجرابودن سرویس‌های حیاتی و اجراکردن آن‌ها در صورتی که درحال‌اجرابودن نباشند.

- Kibana
- Elasticsearch
- Logstash
- Parser
- Zeek
- Yaf
- Suricata
- Syslog Server
- Kafka

۷,۵ به روز رسانی امن

۳۳	به روز رسانی امن ۱
محصول مورد ارزیابی باید این امکان را به سرپرستان امنیتی محصول بدهد که به نسخه فعلی نرم‌افزار/میان‌افزار محصول و هیچ نسخه دیگری از نرم‌افزار/میان‌افزار محصول دسترسی داشته باشد.	
۳۴	به روز رسانی امن ۲
محصول مورد ارزیابی باید این امکان را برای سرپرستان امنیتی محصول فراهم کند که به‌روزرسانی نرم‌افزار/میان‌افزار محصول مورد ارزیابی را به صورت دستی انجام دهد و از هیچ مکانیزم به‌روزرسانی دیگری پشتیبانی نکند.	
۳۵	به روز رسانی امن ۳
محصول مورد ارزیابی باید پیش از نصب به‌روزرسانی‌های نرم‌افزاری و میان‌افزاری، با استفاده ازمکانیسم امضای دیجیتال، ابزاری را برای احرازهویت میان‌افزار آن‌ها در اختیار محصول مورد ارزیابی قرار دهد.	
۳۶	مهرهای زمانی ۱
محصول مورد ارزیابی باید قابلیت ارائه مهرهای زمانی قابل‌اطمینان برای استفاده خودش، را داشته باشد.	
۳۷	مهرهای زمانی ۲
توابع امنیتی هدف ارزیابی باید به مدیر امنیتی اجازه تنظیم زمان بدهد.	

۸,۵ دسترسی به محصول

شماره الزام	عنصر امنیتی
۳۸	قفل‌کردن و خاتمه دادن به نشست‌ها ۷
در مورد نشست‌های تعاملی محلی۴، محصول مورد ارزیابی باید پس از اتمام زمان غیر فعال بودن که توسط سرپرست محصول تعیین شده است، نشست را خاتمه دهد.	
۳۹	قفل‌کردن و خاتمه دادن به نشست‌ها ۵

۴ Local interactive sessions

در مورد نشست‌های تعاملی راه‌دور۵، درصورتی که نشست تعاملی برای مدت معینی غیرفعال باشد، محصول مورد ارزیابی باید نشست تعاملی خاتمه دهد. مدت زمان مجاز برای غیرفعال بودن توسط سرپرست محصول تعیین می‌شود.	
۴۰	قفل‌کردن و خاتمه دادن به نشست‌ها ۶
محصول مورد ارزیابی باید به سرپرست محصول اجازه دهد که نشست تعاملی خود را خاتمه دهد.	
۴۱	پیغام‌های هشدار در رابطه با استفاده محصول ۱
قبل از ایجاد یک نشست کاربری سرپرست اجرایی۶، محصول مورد ارزیابی باید توصیه‌های مشخص شده توسط سرپرست امنیتی و همچنین تاییدیه استفاده از محصول مورد ارزیابی را نشان دهد.	

۹,۵ کلاس کانال ها / مسیرهای مورد اعتماد

شماره الزام	عنصر امنیتی
۴۲	کانال امن ۱
محصول، باید مسیر ارتباطی امنی را با استفاده از پروتکل IPsec میان خود و دیگر موجودیت‌های IT معتبر همچون سرور ممیزی، هیچ قابلیت های دیگری که به طور منطقی از کانال‌های دیگر متمایز است فراهم نماید تا آن‌ها را احرازهویت کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد.	
۴۳	کانال امن ۲
محصول مورد ارزیابی باید اجازه داشته باشد یا به موجودیت‌های معتبر IT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند.	
۴۴	کانال امن ۳
محصول مورد ارزیابی باید ارتباطات را از طریق کانال امن، برای ارسال امن لاگ به موجودیت IT خارجی راه‌اندازی نماید.	
۴۵	مسیر امن ۱
محصول، باید با استفاده از پروتکل SSH, HTTPS مسیر ارتباطی امنی را میان خود و سرپرست‌های راه‌دور مجاز که به طور منطقی از مسیرهای ارتباطی دیگر متمایز است را فراهم نماید و نقاط پایانی را به صورت مطمئن شناسایی کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات در داده کانال را تشخیص دهد.	
۴۶	مسیر امن ۲

۵ Remote

۶ Administrative user

محصول مورد ارزیابی باید به سرپرست‌های راه‌دور محصول اجازه دهد که ارتباطات را از طریق کانال امن آغاز کند.	
۴۷	مسیر امن ۳
محصول مورد ارزیابی باید استفاده از کانال امن را برای احرازهویت اولیه سرپرست محصول و تمام فعالیت‌های راه‌دور سرپرستی الزامی کند.	

۱۰,۵ کلاس مدیریت رویدادها

شماره الزام	عنصر امنیتی
۴۸	تجزیه‌وتحلیل تحلیل‌گر ۱
محصول باید عملکرد تجزیه و تحلیل همبستگی و فیلترینگ را بر روی تمام داده‌های دریافت شده اجرا نماید.	
۴۹	تجزیه‌وتحلیل تحلیل‌گر ۲
محصول باید عملکرد تجزیه‌وتحلیل زیر را بر روی تمام داده‌های دریافت شده‌ی SIEM، اجرا کند: • تحلیل های آماری، تطابق با امضا و جست و جو در لاگ های خام، فیلتر کردن بر روی پارامترهای خاص	
۵۰	تجزیه‌وتحلیل تحلیل‌گر ۳
محصول باید در درون هر یک از داده SIEM جمع‌آوری‌شده حداقل اطلاعات زیر را ثبت نماید: • زمان و تاریخ نتیجه، نوع نتیجه، شناسایی منبع داده • اطلاعات دیگری مانند آدرس و پورت مبدا و مقصد. وقتی هم که تحلیلی رخ دهد (آلارمی تولید شود) می‌تواند متوجه شد که چه لاگ‌هایی سبب این بوده و تاریخچه‌ای که منجر به تولید هشدار شده را می توان مشاهده کرد.	
۵۱	واکنش تحلیل‌گر ۱
محصول باید در زمان تشخیص هر هشدار یا حادثه عملیات مختلف مانند ارسال پیامک، ایمیل و ایجاد آگهی را برای کاربر دارای دسترسی هشدار انجام دهد.	
۵۲	بازبینی داده‌های محدودشده ۱ (۱)
محصول باید کاربران تحلیل گر امنیت، پشتیبان محصول و کارفرمای نهایی با قابلیت خواندن لاگ‌های امنیتی، تحلیلی و همچنین لاگ‌های چک کردن سلامت سیستم از داده‌های دریافت شده‌ی SIEM فراهم نماید.	
۵۳	بازبینی داده‌های محدودشده ۱ (۲)
توابع امنیتی هدف ارزیابی باید کاربران تحلیل گر امنیت و کارفرمای نهایی با قابلیت خواندن هشدارها و تیکت ها از داده‌های تحلیلگر فراهم نماید.	

۵۴	بازبینی داده‌های محدودشده ۲
محصول باید داده‌های جمع‌آوری‌شده‌ی SIEM را به شیوه‌ای مناسب ارائه نماید تا کاربر بتواند اطلاعات را تفسیر کند.	
۵۵	بازبینی داده‌های محدودشده ۳
محصول باید دسترسی خواندن داده‌های جمع‌آوری‌شده‌ی SIEM را برای تمام کاربران، به‌جز آن دسته از کاربرانی که مجوز دسترسی خواندن به آن‌ها اعطاشده، منع نماید.	
۵۶	تضمین در دسترس بودن داده‌های سیستم- حذف ۱ (۱)
محصول باید از حذف غیرمجاز داده‌های جمع‌آوری‌شده و ذخیره‌شده‌ی SIEM، محافظت نماید.	
۵۷	تضمین در دسترس بودن داده‌های سیستم-حذف ۱ (۲)
محصول باید از حذف غیرمجاز داده‌های ذخیره‌شده‌ی تحلیل‌گر، محافظت نماید.	
۵۸	تضمین در دسترس بودن داده‌های سیستم-تغییر ۱ (۱)
محصول باید از تغییر غیرمجاز داده‌های جمع‌آوری‌شده و ذخیره‌شده‌ی SIEM، محافظت نماید.	
۵۹	تضمین در دسترس بودن داده‌های سیستم-تغییر ۱ (۲)
محصول باید از تغییر غیرمجاز داده‌های ذخیره‌شده‌ی تحلیل‌گر، محافظت نماید.	
۶۰	تضمین در دسترس بودن داده‌های سیستم ۲
محصول باید درصورتی‌که ظرفیت ذخیره‌سازی به حد پر شدن رسید اقدام به بازنویسی بر روی قدیمی‌ترین داده‌های جمع‌آوری‌شده‌ی SIEM ذخیره شده نماید و یک هشدار ارسال نماید.	

۱۱,۵ الزامات کارکرد امنیتی برای پیاده سازی ارتباطات سلسه مراتبی

شماره الزام	عنصر امنیتی
۶۱	خروج داده‌های کاربری از محصول ۱
محصول باید در زمان صدور داده‌ی کاربری تحت کنترل خط مشی‌های کارکرد امنیتی به خارج از محصول خط مشی‌های کارکرد امنیتی کنترل دسترسی را اجرا نماید.	
۶۲	خروج داده‌های کاربری از محصول ۲
محصول باید اطمینان دهد که مشخصه‌های امنیتی زمانی که به خارج از محصول صادر می‌شود به‌صورت صریحی به داده‌های کاربری صادرشده، مرتبط شده‌اند.	
۶۳	خروج داده‌های کاربری از محصول ۳

محصول باید اطمینان دهد که مشخصه‌های امنیتی زمانی که به خارج از محصول صادر می‌شود به‌صورت صریحی به داده‌های کاربری صادرشده، مرتبط شده‌اند.	
۶۴	خروج داده‌های کاربری از محصول ۴
محصول باید ملزم نماید که قوانین زیر در زمان صدور داده از محصول اجرا گردند: • احراز هویت • کنترل سطح دسترسی	
۶۵	ورود داده‌های کاربری به محصول ۱
محصول باید خط مشی کارکرد امنیتی کنترل دسترسی و خط مشی کارکرد امنیتی کنترل جریان اطلاعات در زمان ورود داده ی کاربری تحت کنترل خط مشی از خارج به محصول اعمال نماید.	
۶۶	ورود داده‌های کاربری به محصول ۲
محصول باید از مشخصه‌های امنیتی همراه با داده‌های کاربری ورودی استفاده نماید.	
۶۷	ورود داده‌های کاربری به محصول ۳
محصول باید قوانین زیر را در زمان ورود داده کاربری تحت کنترل خط‌مشی کارکرد امنیتی از خارج محصول اجرا نماید: • احراز هویت • کنترل سطح دسترسی	

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 آماده‌سازی
Tests	ATE_IND.1	آزمون مستقل-منطبق
Vulnerability Assessment	AVA_VAN.1	تحلیل آسیب‌پذیری
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 «مستندات راهنمای کاربر» و بخش «مشخصات امنیتی محصول» از سند هدف امنیتی در اختیار کاربر نهایی قرار می‌گیرد. الزامی بر وجود بخش «مشخصات امنیتی محصول» در سند هدف امنیتی نمی‌باشد، 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 گردد.

مؤلفه‌های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
مشخصات کارکردی (ADV_FSP)	نام عنصر: مشخصات کارکرد ابتدایی ۱ شماره مؤلفه: (ADV_FSP.1.1D) شرح مؤلفه: توسعه دهنده باید مشخصات کارکردی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ 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) و اطلاعاتی که در بخش «خلاصه مشخصات محصول» سند هدف امنیتی ارائه شده است، می‌باشند. با توجه به دلایلی که باید در مستندات و بخش «خلاصه مشخصات محصول» وجود داشته باشند، الزامات کارکردی تضمین می‌گردند. از آنجا 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.

مؤلفه‌های 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 ۷و پشتیبان کننده‌ی الزام کارکرد امنیتی۸توصیف نماید.

۷ -SFR-enforcing TSFI

۸-SFR-supporting TSFI

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 کننده‌ی الزام کارکرد امنیتی را مشخص نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ شماره مؤلفه: (ADV_FSP.1.3C) شرح مؤلفه: مشخصات کارکردی باید برای دسته‌بندی ضمنی واسط‌های غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ شماره مؤلفه: (ADV_FSP.1.4C) شرح مؤلفه: ردیابی باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به واسط‌های کارکرد امنیتی در سند مشخصات کارکردی باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
مشخصات کارکردی (ADV_FSP)	نام عنصر: مشخصات کارکرد ابتدایی ۱ شماره مؤلفه: (ADV_FSP.1.1E) شرح مؤلفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام الزامات مؤلفه‌های 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 کلاس‌های «راهنما»، «تست» و «آسیب‌پذیری» ارائه شده است.

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 موفقیت‌آمیز محصول در محیط

دستورالعمل مدیریت امنیت محصول به عنوان یک محصول و به عنوان بخشی از یک محیط عملیاتی بزرگتر

دستورالعمل‌هایی که ارائه دهنده قابلیت مدیریتی محافظت شده از طریق استفاده از قابلیت‌های محصول، محیط عملیاتی یا هر دو می‌باشد.

۴,۶ راهنمای کاربردی

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

مؤلفه‌های محتوایی	
نام خانواده	عنصر امنیتی
راهنمای کاربردی (AGD_OPE)	نام عنصر: راهنمای کاربردی ۱ شماره مؤلفه: (AGD_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.
	نام عنصر: راهنمای کاربردی 1 شماره مؤلفه: (AGD_OPE.1.2C)

مؤلفه‌های محتوایی	
نام خانواده	عنصر امنیتی
	شرح مؤلفه: سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسطهای در دسترس ارائه شده توسط محصول به صورت امن استفاده می‌گردد.
	نام عنصر: راهنمای کاربردی ۱ 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 مؤلفه: (AGD_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 موجودیت‌های تحت کنترل توابع امنیتی محصول.
	نام عنصر: راهنمای کاربردی 1 شماره مؤلفه: (AGD_OPE.1.5C) شرح مؤلفه:

مؤلفه‌های محتوایی	
نام خانواده	عنصر امنیتی
	سند راهنمای کاربردی باید تمام مدهای عملیاتی محصول (مدهایی شامل شکست عملیات یا خطای عملیات)، آثار آنها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.
	نام عنصر: راهنمای کاربردی ۱ شماره مؤلفه: (AGD_OPE.1.6C) شرح مؤلفه: سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسط کاربر تبعیت می‌شوند توصیف نماید تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده‌اند، کاملاً اجرا گردند.
	نام عنصر: راهنمای کاربردی ۱ شماره مؤلفه: (AGD_OPE.1.7C) شرح مؤلفه: سند راهنمای کاربردی باید واضح و قابل فهم باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
راهنمای کاربردی	نام عنصر: راهنمای کاربردی ۱ شماره مؤلفه: (AGD_OPE.1.1E)

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
(AGD_OPE)	شرح مؤلفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده در سند راهنمای کاربردی تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۵,۶ راهنمای آماده‌سازی

مؤلفه‌های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
راهنمای آماده‌سازی (AGD_PRE)	نام عنصر: راهنمای آماده‌سازی ۱ شماره مؤلفه: (AGD_PRE.1.1D) شرح مؤلفه: توسعه دهنده باید محصول را همراه با سند آماده‌سازی ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
راهنمای آماده-سازی (AGD_PRE)	نام عنصر: راهنمای آماده‌سازی ۱ شماره مؤلفه: (AGD_PRE.1.1C) شرح مؤلفه:

مؤلفه‌های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
	مستندات آماده‌سازی بایدتمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه‌های تحویل توسعه دهنده شرح دهند.
	نام عنصر: راهنمای آماده‌سازی ۱ شماره مؤلفه: (AGD_PRE.1.2C) شرح مؤلفه: مستندات آماده‌سازی باید تمام مراحل لازم برای نصب امن محصول و آماده‌سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکر شده در سند هدف امنیتی، شرح دهند.

مؤلفه‌های اقدامات ارزیاب	
راهنمای آماده-سازی (AGD_PRE)	نام عنصر: راهنمای آماده‌سازی ۱ شماره مؤلفه: (AGD_PRE.1.1E) شرح مؤلفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: راهنمای آماده‌سازی 1 شماره مؤلفه: (AGD_PRE.1.2E) شرح مؤلفه:

مؤلفه‌های اقدامات ارزیاب	
	ارزیاب باید رویه‌های آماده‌سازی 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 بخش‌هایی که طراحی و پیاده‌سازی آنها برای سیستم دارای آسیب‌های امنیتی است، در نظر گرفته می‌شود. تست بخش‌های کارکردی سیستم از طریق خانواده ATE_IND، و تست بخش‌هایی که طراحی و پیاده‌سازی آسیب‌زایی دارند از طریق خانواده AVA_VAN صورت می‌گیرد. در این سطح از ارزیابی (سطح EAL1) تست براساس کارکردی که برای محصول در نظر گرفته شده و واسط‌هایی که بر اساس اطلاعات طراحی در اختیار ارزیاب قرار می‌گیرد، انجام می‌گردد. نتایج تست و تحلیل آسیب‌پذیری 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.

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

مؤلفه‌های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
آزمون مستقل (ATE_IND)	نام عنصر: آزمون مستقل ۱ شماره مؤلفه: (ATE_IND.1.1C) شرح مؤلفه: محصول باید مناسب آزمودن باشد.

مؤلفه‌های اقدامات ارزیاب	
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، مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: تست مستقل ۱ شماره مؤلفه: (ATE_IND.1.2E) شرح مؤلفه: ارزیاب باید زیرمجموعه‌ای از توابع امنیتی محصول را تست نماید تا تائید نماید که توابع امنیتی محصول به صورت مشخص شده عمل می‌نمایند.

۸,۶ کلاس آسیب‌پذیری

۹,۶ تحلیل آسیب پذیری

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	عنصر امنیتی
آسیب‌پذیری (AVA_VAN)	نام عنصر: آسیب‌پذیری ۱ شماره مؤلفه: (AVA_VAN.1.1D) شرح مؤلفه: توسعه دهنده باید برای آزمودن، محصول را ارئه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
آسیب‌پذیری (AVA_VAN)	نام عنصر: آسیب‌پذیری ۱ شماره مؤلفه: (AVA_VAN.1.1C) شرح مؤلفه: محصول باید مناسب آزمودن باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
آسیب‌پذیری	نام عنصر: آسیب‌پذیری ۱

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
(AVA_VAN)	شماره مؤلفه: (AVA_VAN.1.1E) شرح مؤلفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده، تمام مؤلفه‌های محتوایی را برآورده می-نماید.
	نام عنصر: آسیب‌پذیری ۱ شماره مؤلفه: (AVA_VAN.1.2E) شرح مؤلفه: ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در محصول، در منابع عمومی جستجویی را انجام دهد.
	نام عنصر: آسیب‌پذیری ۱ شماره مؤلفه: (AVA_VAN.1.3E) شرح مؤلفه: ارزیاب باید براساس آسیب‌پذیری‌های بالقوه شناسایی شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص نماید.

۱۰,۶ کلاس پشتیبانی از چرخه حیات

در سطح اطمینانی که این پروفایل حفاظتی ارائه شده است (EAL1) کلاس پشتیبانی از چرخه حیات به ویژگی‌هایی از چرخه حیات محدود می‌گردد که توسط کاربر نهایی قابل مشاهده باشد. این به معنی نیست که

سبک و سیاق توسعه دهنده نقش کمرنگی در قابل‌اعتماد بودن محصول دارد، بلکه در این سطح اطمینان(EAL1) تنها به این اطلاعات نیاز است.

۱۱,۶ قابلیت‌های پیکربندی

این مؤلفه جهت معرفی محصول به صورت مجزا از دیگر محصولات یا نسخه‌ای که توسط فروشنده ارائه شده، می‌باشد (بدین معنی که جدا ار برچسب گذاری محصول، محصول که ممکن است بخشی از یک محصول باشد به تنهایی، برچسب گذاری شود، نام محصول، نسخه آن و غیره). بدین ترتیب کاربر نهایی می‌تواند محصول که توسط مرکز گواهی تائید شده است را به آسانی تشخیص دهد.

مؤلفه‌های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
قابلیت‌های پیکربندی (ALC_CMC)	نام عنصر: برچسب گذاری محصول ۱ شماره مؤلفه: (ALC_CMC.1.1D) شرح مؤلفه: توسعه دهنده باید محصول و مرجع محصول را ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
قابلیت‌های پیکربندی (ALC_CMC)	نام عنصر: برچسب گذاری محصول ۱ شماره مؤلفه: (ALC_CMC.1.1C) شرح مؤلفه: محصول باید با یک مرجع یکتا برچسب زده شود.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
قابلیت‌های پیکربندی (ALC_CMC)	نام عنصر: برچسب گذاری محصول ۱ شماره مؤلفه: (ALC_CMC.1.1E) شرح مؤلفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می-نماید.

۱۲,۶ حوزه پیکربندی

مؤلفه‌های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
حوزه پیکربندی (ALC_CMS)	نام عنصر: پوشش پیکربندی محصول ۱ شماره مؤلفه: (ALC_CMS.1.1D) شرح مؤلفه: ارزیاب باید لیست پیکربندی محصول را ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
حوزه پیکربندی (ALC_CMS)	نام عنصر: پوشش پیکربندی محصول ۱ شماره مؤلفه: (ALC_CMS.1.1C)

مؤلفه‌های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
	شرح مؤلفه: لیست پیکربندی باید شامل خود محصول و مدارک مورد نیاز توسط الزامات تضمین امنیتی باشد.
	نام عنصر: پوشش پیکربندی محصول ۱ شماره مؤلفه: (ALC_CMS.1.1C) شرح مؤلفه: لیست پیکربندی باید موارد پیکربندی را به صورت یکتا معرفی نماید.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
حوزه پیکربندی (ALC_CMS)	نام عنصر: پوشش پیکربندی محصول ۱ شماره مؤلفه: (ALC_CMS.1.1E) شرح مؤلفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می-نماید.

۷ پیوست یک: الزامات اختیاری

۱,۷ کلاس ممیزی امنیت

شماره الزام	عنصر امنیتی
۶۸	ذخیره‌سازی داده‌های ممیزی محافظت شده ۱
توابع امنیتی مورد ارزیابی باید از پاک شدن غیرمجاز داده‌های ممیزی ذخیره شده در دنباله ممیزی محافظت نماید.	
۶۹	ذخیره‌سازی داده‌های ممیزی محافظت شده ۲
توابع امنیتی مورد ارزیابی باید قادر باشد از تغییرات غیرمجاز داده‌های ممیزی ذخیره شده در دنباله ممیزی جلوگیری نماید.	
۷۱	نمایش هشدار برای فضای ذخیره‌سازی محلی
توابع امنیتی هدف ارزیابی باید در صورتی که دنباله ممیزی بیش از ظرفیت ذخیره‌سازی دنباله ممیزی باشد، برای اطلاع‌رسانی به مدیر هشداری ایجاد نماید.	

۲,۷ کلاس مدیریت امنیت

شماره الزام	عنصر امنیتی
۷۴	مدیریت رفتار توابع امنیتی/خدمات ۱
توابع امنیتی هدف ارزیابی باید قابلیت شروع و متوقف کردن سرویس‌ها را به سرپرست امنیتی محدود سازد.	

۸ پیوست دو: الزامات مبتنی بر انتخاب

۱,۸ الزامات پروتکل HTTPS

شماره الزام	عنصر امنیتی
۱۰۳	الزامات پروتکل(۱) HTTPS
محصول مورد ارزیابی باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کنند.	
۱۰۴	الزامات پروتکل(۲) HTTPS
محصول مورد ارزیابی باید پروتکل HTTPS را با استفاده از TLS اجرا کند.	
۱۰۵	الزامات پروتکل(۳) HTTPS
درصورتی‌که گواهی‌نامه همتا ارائه شده باشد و نامعتبر باشد، محصول مورد ارزیابی باید اتصال را برقرار ننماید.	

۲,۸ الزامات پروتکل IPsec

شماره الزام	عنصر امنیتی
۱۰۶	الزامات پروتکل(۱) IPSEC
محصول مورد ارزیابی باید پروتکل IPsec را بر اساس آن چه در RFC 4301 مشخص شده است، پیاده‌سازی کند.	
۱۰۷	الزامات پروتکل(۲) IPSEC
محصول مورد ارزیابی باید مقدار/قانون در پایگاه دادهSPD ، برای تمام موارد غیر منطبق داشته باشد و آن‌ها را طبق آن مقدار/قانون دور بریزد.	
۱۰۸	الزامات پروتکل(۳) IPSEC

محصول مورد ارزیابی باید مد انتقال را پیاده‌سازی کند.	
۱۰۹	الزامات پروتکل(۴) IPSEC
محصول مورد ارزیابی باید بر اساس آنچه در RFC 4303 گفته شده است فریمورک ESP از پروتکل IPSEC را با استفاده از الگوریتم‌های رمزنگاری AES-CBC-256، به همراه الگوریتم درهم سازی امن HMAC مبتنی بر SHA، HMAC-SHA-256 پیاده سازی کند.	
۱۱۰	الزامات پروتکل(۵) IPSEC
توابع امنیتی هدف ارزیابی باید یکی از این پروتکل‌ها را پیاده‌سازی کند: IKEv2، مطابق با آنچه که در RFC 5996 و با پشتیبانی اجباری از پیمایش NAT چنان که در بخش 2,23 از RFC 5996 تشریح شده است و RFC 4868 برای توابع درهم ساز	
۱۱۱	الزامات پروتکل(۶) IPSEC
محصول مورد ارزیابی باید اطمینان حاصل کند که برای پی‌آیند رمزگذاری‌شده در پروتکل IKEv2 ، از الگوریتم‌های رمزنگاری AES-CBC-256 تشریح شده در RFC 5282 استفاده می‌شود .	
۱۱۲	الزامات پروتکل(۷) IPSEC
محصول مورد ارزیابی باید اطمینان حاصل کند که سرپرست محصول می‌تواند طول عمر IKEv2 SA را بر اساس مدت زمان که مقدار آن را می‌توان در بازه [1تا 24] ساعت قرارداد پیکربندی کند.	
۱۱۳	الزامات پروتکل(۸) IPSEC
محصول مورد ارزیابی باید اطمینان حاصل کند ک سرپرست محصول می‌تواند طول عمر IKEv2 Child SA را بر اساس مدت زمان که مقدار آن را می‌توان در بازه 1 تا 24 ساعت قرار دادپیکربندی کند	
۱۱۴	الزامات پروتکل(۹) IPSEC
توابع امنیتی هدف ارزیابی باید مقدار x را که در تبادل کلید IKE DiffieHellman به کار می‌رود، با استفاده از تولیدکننده بیت تصادفی که در الزام FCS_RBG_EXT.1 مشخص شده است و دست کم طول آن تعداد	

بیت های (یک یا بیش از یک) باشد که حداقل دو برابر قدرت امنیتی گروه Diffie-Hellman مذاکره شده باشد تولید نماید.	
۱۱۵	الزامات پروتکل(۱۰) IPSEC
توابع امنیتی هدف ارزیابی باید نانس‌های مورداستفاده در تبادلات IKEv2 را با طول حداقل 128 بیت اندازه و حداقل نصف اندازه خروجی تابع درهم‌سازی نیمه‌تصادفی مذاکره‌شده (PRF) تولید کند.	
۱۱۶	الزامات پروتکل(۱۱) IPSEC
محصول باید اطمینان حاصل نماید که پروتکل‌های IKE، همه گروه‌های DH (2048-bit MODP) را پشتیبانی می‌کنند.	
۱۱۷	الزامات پروتکل(۱۲) IPSEC
محصول باید به صورت پیش‌فرض بتواند اطمینان حاصل نماید که قدرت الگوریتم متقارن (از نظر تعداد بیت‌های کلید) که برای حفاظت از اتصال IKEv2 IKE_SA مذاکره شده است، بیشتر یا مساوی قدرت الگوریتم متقارنی(از نظر تعداد بیت‌های کلید) که برای حفاظت از اتصال IKEv2 CHILD_SA مذاکره شده است، باشد.	
۱۱۸	الزامات پروتکل(۱۳) IPSEC
محصول باید اطمینان حاصل نماید که همه پروتکل‌های IKE احرازهویت همتا را با استفاده از RSA که از گواهی‌های X.509v3 مطابق با RFC4945 و هیچ روش دیگری استفاده می‌کند، انجام می‌دهند.	
۱۱۹	الزامات پروتکل(۱۴) IPSEC
محصول باید کانال امن را فقط در صورتی که شناساننده موجود در گواهی‌نامه دریافتی با شناساننده مرجع پیکربندی شده انطباق داشته باشد، برقرار نماید .شناساننده مرجع و ارائه شده از انواع زیر می‌باشند : • آدرس IP و هیچ نوع شناساننده مرجع دیگری	

۳,۸ الزامات پروتکل SSH Client

شماره الزام	عنصر امنیتی
۱۲۴	الزامات پروتکل(۱) SSH Client
محصول باید پروتکل SSH را مطابق با RFC های ۴۲۵۱، ۴۲۵۲، ۴۲۵۳، ۴۲۵۴، ۴۲۵۶، ۵۶۵۶، ۶۶۶۸، ۸۳۰۸ و ۸۳۳۲ پیاده‌سازی نماید.	
۱۲۵	الزامات پروتکل(۲) SSH Client
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، روش‌های احرازهویت زیر مطابق با آنچه که در RFC 4252 توضیح داده‌شده است، پشتیبانی می‌شوند: احرازهویت مبتنی بر کلید عمومی، احرازهویت مبتنی بر گذرواژه.	
۱۲۶	الزامات پروتکل(۳) SSH Client
همان طور که در RFC 4253 توضیح داده‌شده است، محصول باید اطمینان حاصل نماید که بسته‌های دارای بایت‌های بیشتر از ۲۶۲۱۴۴ بایت در یک ارتباطات انتقال SSH، کنار گذاشته شوند.	
۱۲۷	الزامات پروتکل(۴) SSH Client
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، از الگوریتم‌های رمزنگاریAES128-CTR و AES256-CTR استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند.	
۱۲۸	الزامات پروتکل(۵) SSH Client
محصول باید اطمینان حاصل نماید که پیاده‌سازی پروتکل انتقال SSH، از ecdsa-sha2-nistp256، ecdsa-sha2-nistp384، ecdsa-sha2-nistp521، rsa-sha2-512، rsa-sha2-256 و ssh-ed25519 به عنوان الگوریتم(های) کلید عمومی خود استفاده کند و همه الگوریتم‌های دیگر را رد نماید.	
۱۲۹	الزامات پروتکل(۶) SSH Client

شماره الزام	عنصر امنیتی
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل انتقال SSH، از hmac-sha1, hmac-sha1-96 hmac-sha2-256, hmac-sha2-512به عنوان الگوریتم‌های MAC صحت داده‌ها استفاده می‌شود و سایر الگوریتم‌های MAC صحت داده‌ها رد می‌شوند.	
۱۳۰	الزامات پروتکل(۷) SSH Client
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که ecdh-sha2-nistp256، ecdh-sha2-nistp384،ecdh-sha2-nistp521 تنها روش‌های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می‌روند.	
۱۳۱	الزامات پروتکل(۸) SSH Client
محصول باید اطمینان پیدا کند که در یک ارتباط SSH، کلیدهای نشست یکسانی برای حدآستانه؛ طول نشست بیشتر از یک ساعت نباشد، و حجم داده مخابره شده بیشتر از 1 گیگابایت نباشد، استفاده می‌گردد. در صورت پر شدن حد آستانه هر کدام از موارد ذکر شده، مجددسازی کلید باید صورت بگیرد.	
۱۳۲	الزامات پروتکل(۹) SSH Client
محصول باید اطمینان حاصل نماید که کلاینت SSH، سرور SSH را احرازهویت می‌کند. سرور SSH از یک پایگاه داده محلی که نام هر میزبان را با کلید عمومی متناظر آن یا هیچ روش دیگری (تشریح شده در RFC 4251 بخش 4.1) همراه می‌کند، استفاده می‌نماید.	

۴,۸ الزامات پروتکل SSH Server

شماره الزام	عنصر امنیتی
۱۳۳	الزامات پروتکل(۱) SSH Server

محصول باید پروتکل SSH را مطابق با RFC های ۴۲۵۱، ۴۲۵۲، ۴۲۵۳، ۴۲۵۴، ۴۲۵۶، ۵۶۵۶، ۶۶۶۸، ۸۳۰۸ و ۸۳۳۲ پیاده‌سازی نماید.	
۱۳۴	الزامات پروتکل(۲) SSH Server
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، همان‌طور که در RFC 4252 توضیح داده‌شده است، روش‌های احرازهویت زیر پشتیبانی می‌شوند: احرازهویت مبتنی بر کلید عمومی، احرازهویت مبتنی بر گذرواژه.	
۱۳۵	الزامات پروتکل(۳) SSH Server
همان طور که در RFC 4253 توضیح داده‌شده است، محصول باید اطمینان حاصل نماید که بسته‌های بیشتر از 256KB در یک ارتباطات انتقال SSH، کنار گذاشته شوند.	
۱۳۶	الزامات پروتکل(۴) SSH Server
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، از الگوریتم‌های رمزنگاری AES128-CTR، AES256-CTR استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند.	
۱۳۷	الزامات پروتکل(۵) SSH Server
محصول باید اطمینان حاصل نماید که پیاده‌سازی پروتکل انتقال SSH، از rsa-sha2-256، rsa-sha2-512، ecdsa-sha2-nistp256، ssh-ed25519 به عنوان الگوریتم(های) کلید عمومی خود استفاده کند و همه الگوریتم‌های دیگر را رد نماید.	
۱۳۸	الزامات پروتکل(۶) SSH Server
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل انتقال SSH، از hmac-sha1، hmac-sha1-96، hmac-sha2-256، hmac-sha2-512 و هیچ الگوریتم MAC دیگری به عنوان الگوریتم‌های MAC صحت داده‌ها استفاده می‌شود و سایر الگوریتم‌های MAC صحت داده‌ها رد می‌شوند.	
۱۳۹	الزامات پروتکل(۷) SSH Server

محصول باید اطمینان حاصل نماید که ecdh-sha2-nistp256، ecdh-sha2-nistp384 و ecdh-sha2-nistp521 تنها روش‌های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می‌روند.	
۱۴۰	الزامات پروتکل(۸) SSH Server
محصول باید اطمینان پیدا کند که در یک ارتباط SSH، کلیدهای نشست یکسانی برای حدآستانه، طول نشست بیشتر از یک ساعت نباشد، و حجم داده مخابره شده بیشتر از 1 گیگابایت نباشد، استفاده می‌گردد. در صورت پر شدن حد آستانه هر کدام از موارد ذکر شده، مجددسازی کلید باید صورت بگیرد.	

۵,۸ الزامات پروتکل TLS Client

شماره الزام	عنصر امنیتی
۱۴۱	الزامات پروتکل TLS Client
توابع امنیتی هدف ارزیابی باید TLS 1.2 (RFC5246) را پیاده سازی کرده و تمامی نسخه‌های TLSو SSL را رد نماید. پیاده‌سازی توابع امنیتی هدف ارزیابی باید با پشتیبانی از مجموعه‌های رمز زیر باشد. • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 • TLS_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288 • TLS_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288	
شماره الزام	عنصر امنیتی
۱۴۲	الزامات پروتکل TLS Client

توابع امنیتی هدف ارزیابی باید تائید کند که شناسه ارائه شده با شناسه مرجع طبق RFC 6125 بخش ۶، آدرس IPv4 در CN یا SAN، IPv6 در CN یا SAN، آدرس IPv4 در SAN، آدرس IPv6 در SAN و نه انواع خصوصیات دیگر مطابقت داشته باشد.	
۱۴۳	الزامات پروتکلTLS Client
توابع امنیتی هدف ارزیابی باید فقط در صورتی که گواهینامه سرور معتبر باشد کانال امن را برقرار سازد. همچنین توابع امنیتی هدف ارزیابی باید - هیچ مکانیسم لغو سرپرستی پیادهسازی نشود.	
۱۴۴	الزامات پروتکلTLS Client
توابع امنیتی هدف ارزیابی باید در Client Hello، secp256r1، secp384r1، secp521r1، x448 و x25519 را ارائه دهد و هیچ منحنی دیگری.	

۶,۸ الزامات پروتکل TLS Client / احراز هویت

۱۴۵	الزامات پروتکل TLS Client / احراز هویت ۱
توابع امنیتی هدف ارزیابی باید با استفاده از گواهینامه X.509v3 از احراز هویت دوطرفه پشتیبانی نماید.	

۷,۸ الزامات پروتکل TLS Server

۱۴۶	الزامات پروتکل(۱) TLS Server
محصول باید TLS 1.2 (RFC 5246) را پیادهسازی کند و دیگر نسخههای TLS و SSL را رد نماید. همچنین TLS را با پشتیبانی از مجموعههای رمز زیر را پیادهسازی نماید. • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289	
۱۴۷	الزامات پروتکل(۲) TLS Server

توابع امنیتی هدف ارزیابی باید اتصال‌های کاربرانی را که درخواست SSL 2.0، SSL 3.0، TLS 1.0 و TLS 1.1 دارند، رد نماید.	
۱۴۸	الزامات پروتکل(۳) TLS Server
توابع امنیتی هدف ارزیابی باید پارامترهای EC Diffie-Hellman را بر روی منحنی‌های [secp521r1, NIST secp384rl, secp256r1] و هیچ منحنی دیگری تولید کند.	
۱۴۹	الزامات پروتکل(۴) TLS Server
توابع امنیتی هدف ارزیابی باید از بدون از سرگیری نشست یا بلیت نشست و از سرگیری نشست مبتنی بر بلیط های نشست با توجه به RFC 5077 پشتیبانی کنند.	

۸,۸ الزامات شناسایی و احرازهویت

شماره الزام	عنصر امنیتی
۱۵۳	اعتبارسنجی گواهینامه X509 (۱)
محصول مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند: • تأیید گواهی‌نامه RFC 5280 و تائید مسیر گواهینامه با پشتیبانی از حداقل طول مسیر از سه گواهینامه • مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد. • توابع امنیتی مورد ارزیابی باید برای تائید یک مسیر گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهینامه‌های CA به حالت «True» تنظیم شده است. • توابع امنیتی مورد ارزیابی باید وضعیت فسخ گواهی نامه را با استفاده از لیست فسخ گواهی نامه (CRL) چنان که در بخش ۶,۳ از RFC 5280 تعریف شده است را تایید کند. • توابع امنیتی مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تائید کند.	

○ گواهی‌نامه‌های مورداستفاده برای به‌روزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی، باید هدف «Code Signing» (id-kp 3 با OID 1.3.6.1.5.5.7.3.3) را در فیلد extendedKeyUsage خود داشته باشند. ○ گواهی‌نامه‌های سرور ارائه‌شده برای TLS باید هدف "Server Authentication" (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند. ○ گواهی‌نامه‌های کلاینت ارائه‌شده برای TLS باید هدف "Client Authentication" (id-kp2 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند. ○ گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ‌های OCSP باید هدف «OCSP Signing» (id-kp9 با OID 1.3.6.1.5.5.7.3.9) را در فیلد extendedKeyUsage خود داشته باشند.	
۱۵۴	اعتبارسنجی گواهینامه X509 (۲)
محصول مورد ارزیابی تنها درصورتی‌که افزونه مربوط به basicConstraints از پیش تنظیم‌شده باشد و پرچم CA به حالت «TRUE» تنظیم‌شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA می‌پذیرد.	
۱۵۵	احرازهویت گواهینامه X509 (۱)
توابع امنیتی مورد ارزیابی باید برای پشتیبانی از احراز هویت در SSH، HTTPS ، IPsecو همچنین برای امضای کد برای تایید اعتبار سنجی از گواهینامه‌های X.509v3تعریف شده در RFC 5280استفاده کند	
۱۵۶	احرازهویت گواهینامه X509 (۲)
اگر توابع امنیتی مورد ارزیابی نتواند اتصال مورد نیاز برای تعیین اعتبار یک گواهینامه را برقرار کند، توابع امنیتی هدف ارزیابی باید گواهینامه را نپذیرد.	
۱۵۷	درخواست‌های گواهینامه X509 (۱)
محصول مورد ارزیابی باید مطابق با آنچه که در RFC 2986 تشریح شده است، یک Certificate Request Message تولید کند و بتواند اطلاعات؛ کلید عمومی و Common Name ، Organization ، Organization Unit، Country را در درخواست فراهم کند.	

۱۵۸	درخواست‌های گواهینامه X509 (۲)
محصول مورد ارزیابی باید زنجیره گواهی‌نامه‌ها از Root CA را بر اساس پاسخ گواهینامه‌های CA دریافت شده اعتبارسنجی کند.	

۹,۸ الزامات مدیریت امنیت

شماره الزام	عنصر امنیتی
۱۶۴	مدیریت رفتار توابع امنیتی/ به روز رسانی خودکار ۲
توابع امنیتی هدف ارزیابی باید توانایی تعیین رفتار و تغییر رفتار توابع انتقال داده های ممیزی به موجودیت IT خارجی، مدیریت داده‌های ممیزی و عملکرد ممیزی زمانی که فضای حافظه محلی ممیزی پر شده باشد را به سرپرست امنیتی محدود کند.	