به نام خدا

پروفایل حفاظتی سیستم تشخیص نفوذ

نسخه ۱,۶

اردیبهشت ۱۳۹۳

پیش‌گفتار

این سند توسط مرکز مدیریت راهبردی افتا و سازمان فناوری اطلاعات ایران تهیه و نهایی شده است که معرفی کننده الزامات کارکرد امنیتی برای سیستم‌های تشخیص نفوذ[1]می‌باشد تا تولیدکنندگان این سیستم‌ها بتوانند بر مبنای این سند، کارکردهای امنیتی را در محصول خود لحاظ نموده و همچنین سند هدف امنیتی آن را ارائه نمایند.

در بخش اول، سیستم تشخیص نفوذ به صورت کلی معرفی شده است. سپس در بخشی تحت عنوان «مسائل امنیتی» تهدیدهایی که محصول با آنها روبرو است و فرضیاتی که در رابطه با امنیت محصول در نظر گرفته شده است و همچنین خط‌مشی‌های آن عنوان می‌گردد.

سپس در بخش «اهداف امنیتی» مواردی جهت مقابله با تهدیدها، اجرای خط‌مشی‌ها و بکاربردن فرضیات مطرح می‌گردد.

در بخش بعدی «الزامات کارکرد امنیتی» آورده شده است. براساس استاندارد ارزیابی معیار مشترک این قسمت از چندین کلاس تشکیل شده است که هریک از این کلاس-ها حوزه خاصی از امنیت را پوشش می‌دهد. کلاس‌هایی که برای سیستم تشخیص نفوذ در این سند مطرح شده است عبارتند از:

- کلاس ممیزی امنیت
- کلاس شناسایی و احراز هویت
- کلاس مدیریت امنیت
- کلاس حفاظت از توابع امنیتی هدف ارزیابی

[1]Intrusion Detection System (IDS)

- کلاس تشخیص نفوذ

هر کلاس مجموعه‌ای از خانواده و هر خانواده مجموعه‌ای از مولفه و هر مولفه مجموعه‌ای از عناصر می‌باشد. با استفاده از «الزامات کارکرد امنیتی» در واقع «اهداف امنیتی» بر مبنای استاندارد معیار مشترک بیان می‌گردد.

در بخش پایانی «الزامات تضمین امنیتی» که از ساختاری مشابه بخش قبلی برخوردار است مطرح گردیده است، این بخش الزامات لازم جهت ارزیابی محصول را عنوان می‌نماید.

فهرست

۱ هدف از ارائه سند

در راستای ارزیابی امنیتی محصولات مبتنی بر «استاندارد ارزیابی معیار مشترک» لازم است تا الزامات کارکرد امنیتی هر محصول بیان شود. بیان این الزامات برای توسعه دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی که در این سند برای برآورده نمودن الزامات ارائه شده‌اند را در محصول خود فراهم نمایند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد نمود.

۲ معرفی اصطلاحات

• هدف ارزیابی (TOE)

به سیستم مورد ارزیابی براساس «استاندارد ارزیابی معیار مشترک»، هدف ارزیابی گفته می‌شود.

• پروفایل حفاظتی (PP[1])

بیانیه‌ای از الزامات امنیتی برای یک نوع از هدف ارزیابی، که الزامات امنیتی را به صورت کلی بیان می‌دارد.

• هدف امنیتی (ST[2])

بیانیه‌ای از الزامات امنیتی برای هدف ارزیابی خاصی، که الزامات امنیتی را به صورت جزئی‌تر بیان می‌دارد. این بیانیه معمولاً توسط سازنده هدف ارزیابی نوشته می‌شود.

[1] Protection Profile

[2] Security Target

- **غیر هدف ارزیابی (Non-TOE[1])**

سخت‌افزار، نرم‌افزار و میان افزاری که هدف ارزیابی جهت اجرا به آن‌ها نیز نیاز دارد.

- **محیط عملیاتی (Operational Environment)**

محیطی که هدف ارزیابی در آن عمل می‌کند.

- **مسائل امنیتی (Security Problem)**

در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «مشکل امنیتی» وجود دارد که به طور رسمی ماهیت و حوزه امنیت در نظر گرفته شده توسط هدف ارزیابی را تعریف می‌نماید.

این بیانیه شامل موارد زیر است:

–«تهدیدهایی» که توسط هدف ارزیابی و محیط عملیاتی‌اش مقابله می‌گردد.

–«خط‌مشی امنیت سازمانی» که توسط هدف ارزیابی و محیط عملیاتی‌اش اجرا می‌گردد.

–«فرضیاتی» که برای محیط عملیاتی هدف ارزیابی تائید می‌گردند.

- **عامل تهدید (Threat Agent)**

موجودیت‌هایی که می‌توانند بر روی دارایی‌ها اقدام تهاجمی انجام دهند.

[1] Non-Target Of Evaluation

- **خط‌مشی امنیتی سازمانی (OSP[1])**

مجموعه‌ای از قوانین، که توصیف کننده رفتار امنیتی خاصی است که توسط «توابع امنیتی هدف ارزیابی» اجرا می‌گردند؛ این مجموعه قوانین به صورت یک مجموعه از «الزام‌های کارکرد امنیتی» قابل بیان است.

- **اهداف امنیتی (Security Objective)**

در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «اهداف امنیتی» وجود دارد که برای مقابله با تهدیدهای معرفی شده و/یا برای برآورده نمودن خط‌مشی‌های امنیت سازمان و یا فرضیات معرفی شده در بخش «مسائل امنیتی»، در نظر گرفته شده است.

- **الزام امنیتی (Security Requirement)**

الزاماتی که به زبان استاندارد بیان می‌گردند تا در حاصل شدن اهداف ارزیابی، برای هدف ارزیابی کمک نمایند.

- **الزام کارکرد امنیتی(SFR[2])**

بیان کننده کارکردهای امنیتی هدف ارزیابی در قالب کلاس می‌باشد. در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «الزام کارکرد امنیتی» وجود دارد.

- **الزامات تضمین امنیتی (SAR[3])**

[1] Organizational Security Policy

[2] Security Functional Requirement

[3] Security Assurance Requirement

این دسته از الزامات اطمینان می‌دهند که الزامات کارکرد امنیتی توسط هدف ارزیابی برآورده می‌گردند. در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «الزام تضمین امنیتی» وجود دارد.

- **بسته (Package)**

نام مجموعه‌ای از الزامات کارکرد امنیتی یا تضمین امنیتی می‌باشد. به عنوان مثال EAL3.

- **سطح تضمین ارزیابی (EAL[1])**

مجموعه‌ای از الزامات تضمین که از قسمت سوم از سندهای سه‌گانه «استاندارد ارزیابی معیار مشترک» برگرفته شده است و نشان دهنده سطح امنیتی محصول می‌باشد. سطوح تضمین از سطح ۱ تا سطح ۷ می‌باشند، لازم به ذکر است که «سطح تضمین امنیتی» یک نوع «بسته» می‌باشد.

- **توابع امنیتی هدف ارزیابی (TSFs[2])**

آن بخش از هدف ارزیابی که برای اجرای صحیح «الزامات کارکرد امنیتی» باید به آن تکیه نمود، به عنوان «توابع امنیتی هدف ارزیابی» نام برده می‌شود. «توابع امنیتی هدف ارزیابی» شامل تمام سخت‌افزار، نرم‌افزار و میان‌افزارهای هدف ارزیابی است که مستقیم و غیرمستقیم برای اجرا شدن امنیت باید به آنها تکیه نمود.

- **داده توابع امنیتی هدف ارزیابی (TSF data)**

داده‌هایی برای عملیات هدف ارزیابی هستند که اجرای الزامات کارکرد امنیتی وابسته به آنها می‌باشد. این داده‌ها اطلاعات استفاده شده توسط توابع امنیتی هدف ارزیابی هستند.

---

[1] Evaluation Assurance Level

[2] TOE Security Functions

- **داده کاربری (User data)**

داده‌های کاربری هستند که عملکرد توابع امنیتی هدف ارزیابی را تحت تاثیر قرار نمی‌دهند. این داده‌ها اطلاعاتی ذخیره شده در منابع هدف ارزیابی هستند که توسط کاربران مطابق با الزامات کارکرد امنیتی به کار برده می‌شود. محتویات یک پیام الکترونیک، نوعی داده کاربری می‌باشد.

- **کلاس (Class)**

مجموعه‌ای از خانواده‌های «استاندارد ارزیابی معیار مشترک» که روی یک موضوع متمرکز، اشتراک دارند.

- **خانواده (Family)**

مجموعه‌ای از عناصر که بر روی یک هدف اشتراک دارند اما در دقت و میزان تاکید، تفاوت دارند.

- **عنصر (Component)[۱]**

کوچکترین مجموعه از مولفه‌های قابل انتخاب، که الزامات ممکن است براساس آن‌ها باشد.

- **مولفه (Element)[۲]**

بیانی از نیاز امنیتی که غیر قابل تجزیه است.

---

[۱] در استاندارد ISO 15408 منتشر شده توسط سازمان استاندارد، Component مولفه ترجمه شده است.

[۲] در استاندارد ISO 15408 منتشر شده توسط سازمان استاندارد، Element عنصر ترجمه شده است.

- **اختصاص (Assignment)**

مشخص نمودن پارامترهای معرفی شده در یک مولفه (از استاندارد معیار مشترک) یا الزام می‌باشد.

- **انتخاب (Selection)**

انتخاب نمودن یک یا بیش از یک آیتم در لیستی که در مولفه یا الزام وجود دارد.

- **سرپرست (Administrator)**

موجودیتی که مسئولیت مدیریت و اعمال خط‌مشی‌ها را بر روی هدف ارزیابی بر عهده دارد و معمولا دارای بالاترین سطح مجوز است.

- **موجودیت فعال (Subject)**

موجودیت فعال، موجودیتی در سیستم مورد ارزیابی (هدف ارزیابی) است که عملیاتی را بر روی موجودیت‌های غیرفعال انجام می‌دهد. همانند نقش‌هایی همچون سرپرست، کاربر نهایی و غیره. به عبارت دیگر موجودیت فعال عامل انجام عملی بر روی هدف ارزیابی است.

- **موجودیت غیرفعال (Object)**

موجودیت غیرفعال، موجودیتی در سیستم مورد ارزیابی (هدف ارزیابی) می‌باشد که شامل اطلاعات است و یا اطلاعات را دریافت می‌نماید و روی آن توسط موجودیت‌های فعال، عملیاتی انجام می‌گیرد. همانند داده‌ها و اطلاعاتی همچون متن‌های رمز شده و کلیدها و غیره. به عبارت دیگر موجودیتی است که توسط موجودیت فعال بر روی آن رخدادی اتفاق می‌افتد، مانند لیست کردن رکوردها توسط سرپرست، حذف فایل‌ها توسط حمله کننده، که در این دو مثال رکوردها و فایل‌ها موجودیت‌های غیرفعال هستند.

- **راز (Secret)**

اطلاعاتی که باید تنها به کاربران مجاز و/یا توابع امنیتی هدف ارزیابی شناسانده شود، تا یک «خط‌مشی کارکرد امنیتی » اجرا گردد.

- **مشخصه امنیتی (Security Attribute)**

کاربران، موجودیت‌های فعال، اطلاعات، موجودیت‌های غیرفعال، نشست‌ها و منابع تحت کنترل قوانین «الزامات کارکرد امنیتی» ممکن است دارای اطلاعات خاصی باشند که جهت کارکرد صحیح هدف ارزیابی، مورد استفاده قرار گیرند. دسته‌ای از این اطلاعات حالت آگاهی‌دهنده دارند هم‌چون نام فایل که ممکن است برای معرفی منابع منحصر به فرد استفاده شود، اما دسته‌ی دیگر از این اطلاعات ممکن است به طور خاص برای اجرا شدن الزامات کارکرد امنیتی وجود داشته باشند، همانند اطلاعات کنترل دسترسی، این دسته از اطلاعات به طور کلی «مشخصه امنیتی» نامیده می‌شوند.

- **خط‌مشی کارکرد امنیتی (SFP[1])**

رفتار امنیتی که توسط «کارکرد امنیتی هدف ارزیابی» اجرا می‌گردد تحت مجموعه قوانینی در «الزامات کارکرد امنیتی» بیان می‌شوند، این مجموعه قوانین «خط مشی کارکرد امنیتی» نامیده می‌شوند. «الزامات کارکرد امنیتی» ممکن است چندین خط‌مشی جهت معرفی قوانینی که هدف ارزیابی باید اجرا نماید، تعریف کند. هر کدام از خط‌مشی‌ها باید حوزه کنترلی‌اش را توسط موجودیت‌های فعال، موجودیت‌های غیرفعال، منابع یا اطلاعات و عملکردهایی که بکار برده است، مشخص نماید. تمام این خط‌مشی‌ها توسط «توابع امنیتی هدف ارزیابی» پیاده‌سازی می‌شوند.

- **خط‌مشی کارکرد امنیتی کنترل دسترسی (Access Control SFP)**

چندین خط‌مشی کارکرد امنیتی وجود دارد که برای حفاظت از داده‌ها بکار برده می‌شوند، همچون «خط‌مشی کنترل دسترسی» و «خط مشی کنترل جریان اطلاعات». «خط‌مشی کنترل دسترسی» مکانیزم‌هایی هستند که براساس احکام خط‌مشی‌هایشان، بر روی مشخصه‌های امنیتی کاربران، منابع، موجودیت‌های فعال، موجودیت‌های غیرفعال، نشست‌ها، TSF status data و عملکردها در حوزه کنترلی‌شان پیاده‌سازی می‌شوند.

[1] Security Functionality Policy

این مشخصه‌های امنیتی در مجموعه قوانینی استفاده می‌شوند که حاکم بر عملیاتی است که موجودیت‌های فعال ممکن است بر روی موجودیت‌های غیرفعال اجرا نمایند.

- **خط‌مشی کنترل جریان اطلاعات (Information Flow Control SFP)**

«خط‌مشی کنترل جریان اطلاعات» مکانیزم‌هایی هستند که براساس احکام خط‌مشی‌هایشان، بر روی مشخصه‌های امنیتی موجودیت‌های فعال و اطلاعات در حوزه کنترلی‌شان و مجموعه قوانین حاکم بر عملیات که توسط موجودیت فعال بر روی اطلاعات صورت می‌گیرد، پیاده‌سازی می‌شوند.

۳ معرفی استاندارد ۱۵۴۰۸

استاندارد ISO/IEC 15408 که به عنوان استاندارد ارزیابی معیار مشترک[1]نیز شناخته می‌شود با هدف تعیین مبنایی جهت ارزیابی ویژگی‌های امنیتی محصولات فناوری اطلاعات و سیستم‌ها تدوین گردیده است. با ایجاد چنین مبنایی با معیار مشترک، نتایج ارزیابی امنیتی فناوری اطلاعات برای تعداد بیشتری از مخاطبین حائز اهمیت خواهد بود.

استاندارد ISO/IEC 15408 در برگیرنده مولفه‌های کارکرد امنیتی بوده که مبنایی برای ارزیابی الزامات کارکرد امنیتی موجود در پروفایل حفاظتی یا سند هدف امنیتی است. این الزامات به توضیح رفتارهای امنیتی مورد نظر هدف ارزیابی[2]یا محیط فناوری اطلاعات پرداخته و هدف آن برآورده نمودن اهداف امنیتی که در پروفایل حفاظتی یا سند هدف امنیتی تعیین شده، می‌باشد.

استاندارد ISO/IEC 15408 در سه بخش ارائه شده است :

بخش اول: مقدمه و مدل عمومی (اصطلاحات و واژگان)

بخش دوم: الزامات کارکرد امنیتی [3]

بخش سوم: الزامات تضمین امنیتی[4]

---

[1] Common Criteria (CC)

[2] Target Of Evaluation (TOE)

[3] Security Functional Requirement (SFR)

[4] Security Assurance Requirement (SAR)

۴ معرفی محصول سیستم تشخیص نفوذ[1]

این پروفایل حفاظتی، حداقل الزامات امنیتی را برای هدف ارزیابی (سیستم تشخیص نفوذ) مشخص می‌نماید. سیستم از یک یا بیش از یک سنسور و/یا اسکنر و تحلیل‌گر تشکیل شده است.

این سیستم ناظر فعالیت‌های یک سیستم IT می‌باشد که ممکن است بر روی دارایی‌های سیستم اثر نامطلوب بگذارد، داده‌های جمع‌آوری شده را تحلیل می‌نماید و همچنین عکس‌العمل مناسب انجام می‌دهد.

اطلاعات جمع‌آوری شده ممکن است از طیف گسترده‌ای از منابع که بر روی سیستم IT قرار گرفته است، جمع‌آوری گردد. همین‌طور، عملکرد پاسخ ممکن است یک یا بیش از یک هدف بر روی سیستم IT را تحت تاثیر قرار دهد.

سنسورها باید قادر باشند تا :

- داده‌هایی در ارتباط با تمام رویدادهایی که بر روی سیستم IT رخ داده است، جمع‌آوری نمایند. این رویدادها ممکن است شامل رویدادهای احراز هویت، رویداد دسترسی به داده، رویدادهای دسترسی پیکربندی، درخواست سرویس، ترافیک شبکه، معرفی داده، راه اندازی و متوقف نمودن عملکرد ممیزی باشند.

[1] Intrusion Detection System

- تمام داده‌های جمع‌آوری شده را به یک تحلیل‌گر مجاز برای تحلیل و داده کاهی[1] ارسال نمایند.

اسکنرها باید قادر باشند تا :

- اطلاعات پیکربندی ایستا در رابطه با یک سیستم IT را جمع‌آوری نمایند. اطلاعات پیکربندی ممکن است شامل، شناسایی کد مخرب، پیکربندی کنترل دسترسی، پیکربندی سرویس، پیکربندی احراز هویت، پیکربندی خط‌مشی پاسخگویی و تشخیص آسیب‌پذیری‌های شناخته شده باشد.
- تمام اطلاعات پیکربندی جمع‌آوری شده را به تحلیل‌گر مجاز برای تحلیل و داده کاهی ارسال نماید.

تحلیل‌گرها باید قادر باشند تا :

- داده را از اسکنرها و سنسورهای شناسایی شده، دریافت نماید.
- داده‌های مشخص شده را پردازش نمایند تا بتوانند آسیب‌پذیری/نفوذ را تعیین نمایند.
- به آسیب‌پذیری‌ها/نفوذ شناسایی شده واکنش نشان دهند، این عکس‌العمل ممکن است شامل، تولید گزارش، هشدارها/سیگنال‌های بصری، هشدارها/سیگنال‌های سمعی، تغییرات پیکربندی و/یا هشدار دادن از راه دور باشد.

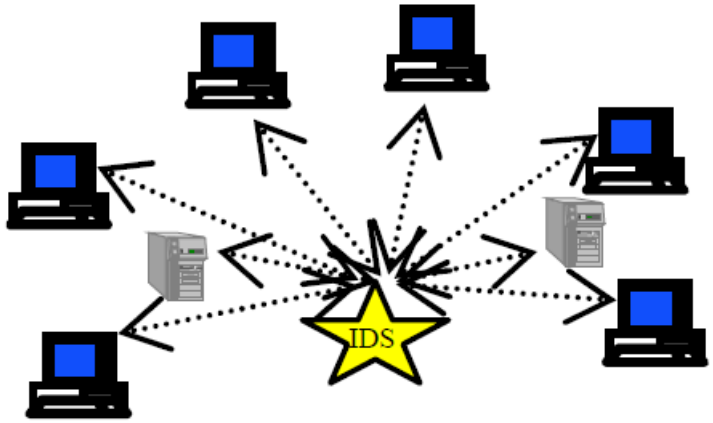
[1] Data reduction

تمام عناصر سیستم تشخیص نفوذ باید قادر باشند تا :

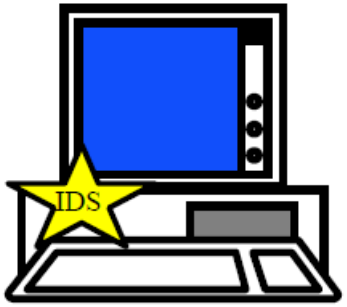
- خود و داده‌هایش را از دست‌کاری شدن، محافظت نماید.
- توسط کاربر مجاز پیکربندی گردد.
- یک دنباله ممیزی ایجاد نماید (همچون، تغییرات پیکربندی، دستیابی به داده و عناصر).

یک سیستم IT که نیاز دارد از آسیب‌پذیری‌ها و حملات سایبری مطلع گردد، باید از سیستم تشخیص نفوذ استفاده نماید. سیستم تشخیص نفوذ خودش و سیستم IT هدف را نظارت می‌نماید. از آنجائیکه سیستم تشخیص نفوذ در یک محیط غیر میزبان عمل می‌نماید، سیستم IT باید از سیستم تشخیص نفوذ به اندازه کافی محافظت نماید.

شکل زیر نشان دهنده نمونه‌ای از چگونه استفاده شده سیستم تشخیص نفوذ در سیستم‌های IT مختلف از یک سیستم کامپیوتری تا یک شبکه کامپیوتری می‌باشد. شکل ۲ نشان می‌دهد که سیستم تشخیص نفوذ می‌تواند در یک سیستم کامپیوتری وجود داشته باشد و نظارت نماید، که این سیستم کامپیوتری لزوماً بخشی از یک شبکه بزرگ نیست. شکل ۱ نشان می‌دهد که سیستم تشخیص نفوذ می‌تواند در داخل یک شبکه کامپیوتری وجود داشته باشد و نظارت نماید. فلش‌ها در این شکل معرف عملکرد نظارتی سیستم تشخیص نفوذ در قبال پیاده‌سازی شبکه کامپیوتری می‌باشند.



شکل ۱- شبکه کامپیوتری



شکل ۲- سیستم کامپیوتری

این پروفایل حفاظتی بین هدف ارزیابی و سیستم، تفاوت قائل شده است. اصطلاح سیستم زمانی استفاده می‌شود که پروفایل حفاظتی به نظارت نمودن ID، تحلیل و سازوکارهای عکس‌العمل همان‌گونه که توسط کلاس الزامات عملکرد امنیتی سیستم تشخیص نفوذ مشخص شده است، اشاره دارد.

زمانی از اصطلاح هدف ارزیابی استفاده می‌شود که این پروفایل حفاظتی به یک محصول IT کامل اشاره می‌نماید که تمام الزامات عملکرد امنیتی هدف ارزیابی که جهت تضمین نمودن پاسخگویی و حفاظت برای قابلیت‌های نظارت ID، تحلیل و عکس‌العمل لازم است را پیاده‌سازی می‌نماید.

۵ تعریف مسائل امنیتی

۵,۱ فرضیات

A.TYPE	توضیحات
A.ACCESS	هدف ارزیابی به تمام داده‌های سیستم IT که در اجرای عملکردش به آنها نیاز دارد، دسترسی دارد.
A.DYNMIC	هدف ارزیابی به صورتی مدیریت خواهد شد تا به صورت مناسبی تغییرات در سیستم IT که هدف ارزیابی مانیتور می‌نماید را آدرس‌دهی نماید.
A.ASCOPE	هدف ارزیابی به صورت مناسبی به سیستم IT که هدف ارزیابی مانیتور می‌نماید، قابل تنظیم [1] است.
A.PROTCT	سخت‌افزار و نرم‌افزار هدف ارزیابی که به اجرای خط‌مشی‌های امنیتی حساس هستند از تغییرات فیزیکی غیرمجاز، محافظت می‌گردند.
A.LOCATE	منابع پردازشی هدف ارزیابی در جاهایی قرار می‌گیرند که دسترسی کنترل شده‌ای داشته باشند، تا از

[1] scalable

A.TYPE	توضیحات
	دسترسی فیزیکی غیرمجاز جلوگیری گردد.
A.MANAGE	یک یا بیش از یک کامپوننت مجزا وجود خواهد داشت که اختصاص به مدیریت هدف ارزیابی و امنیت اطلاعات آن دارد.
A.NOEVIL	سرپرستان مجاز افراد بی‌دقت، عمداً مسامحه کار یا متخاصم نیستند، و دستورالعمل‌های ارائه شده در مستندات راهنما را دنبال می‌نمایند.
A.NOTRST	هدف ارزیابی تنها توسط کاربران مجاز می‌تواند دستیابی گردد.

۵,۲ تهدیدها

T.TYPE	توضیحات
T.COMINT	یک کاربر غیر مجاز ممکن است سعی نماید تا با دور زدن سازوکارهای امنیتی، صحت داده‌های جمع‌آوری شده و تولید شده توسط هدف ارزیابی را به خطر اندازد.
T.COMDIS	یک کاربر غیر مجاز ممکن است سعی نماید تا با دور زدن سازوکارهای امنیتی، داده‌های جمع‌آوری شده و تولید شده توسط هدف ارزیابی را افشاء نماید.
T.LOSSOF	یک کاربر غیر مجاز ممکن است سعی نماید تا داده‌های جمع‌آوری شده و تولید شده توسط هدف ارزیابی را از بین ببرد یا منتقل نماید.
T.NOHALT	یک کاربر غیر مجاز ممکن است سعی نماید تا با متوقف نمودن اجرای هدف ارزیابی، استمرار جمع‌آوری کننده سیستم و عملکرد تحلیل را به خطر اندازد.
T.PRIVIL	یک کاربر غیر مجاز ممکن است دستیابی به سیستم را به دست آورد و با استخراج نمودن مجوزهای سیستم

T.TYPE	توضیحات
	به داده و عملکرد امنیتی هدف ارزیابی، دستیابی پیدا نماید.
T.IMPCON	یک کاربر غیرمجاز ممکن است با تغییر دادن پیکربندی هدف ارزیابی سبب گردد نفوذهای بالقوه، تشخیص داده نشوند.
T.INFLUX	یک کاربر غیرمجاز ممکن است با نفوذ دادن داده‌هایی که هدف ارزیابی نمی‌تواند به کار ببرد[1]، سبب سوءعمل هدف ارزیابی گردد.
T.FACCNT	تلاش‌های غیرمجاز جهت دستیابی به داده هدف ارزیابی یا عملکرد امنیتی، ممکن است تشخیص داده نشود.
T.SCNCFG	ممکن است در سیستم IT که هدف ارزیابی آن را مانیتور می‌نماید، تنظیمات پیکربندی امنیتی نامناسبی وجود داشته باشد.
T.SCNMLC	کاربران می‌توانند با اجرای کدهای مخرب بر روی سیستم IT که هدف ارزیابی مانیتور می‌نماید، سبب تغییرات داده‌های محافظت شده سیستم IT یا تحلیل عملکرد امنیتی سیستم IT گردند.
T.SCNVUL	ممکن است در سیستم IT که توسط هدف ارزیابی مانیتور می‌گردد، آسیب‌پذیری‌هایی وجود داشته باشد.
T.FALACT	واکنش هدف ارزیابی به آسیب‌پذیری‌های شناسایی شده یا مورد ظن یا فعالیت‌های نامناسب، ممکن است با شکست مواجه گردد.
T.FALASC	هدف ارزیابی ممکن است در شناسایی آسیب‌پذیری‌ها یا فعالیت‌های نامناسب براساس تمام داده‌های سیستم تشخیص نفوذ [2]که از تمام منابع داده دریافت شده است، با شکست مواجه گردد.
T.MISUSE	دستیابی‌ها و فعالیت‌های غیرمجاز ممکن است ناشی از بدبکار بردن سیستم IT که توسط هدف ارزیابی مانیتور می‌گردد، باشد.

[1] Handle

[2] Intrusion Detection System

T.TYPE	توضیحات
T.INADVE	دستیابی‌ها و فعالیت‌های غیرعمدی ممکن است بر روی سیستم IT که توسط هدف ارزیابی مانیتور می-گردد، رخ دهد.
T.MISACT	فعالیت‌های مخربی، همچون منتشر نمودن اسب‌های تروجان و ویروس‌ها، ممکن است بر روی سیستم IT که توسط هدف ارزیابی مانیتور می‌گردد، رخ دهد.

۵,۳ خط‌مشی‌ها

P.TYPE	توضیحات
P.DETECT	اطلاعات پیکربندی ایستا که ممکن است نشان دهنده پتانسیلی برای نفوذ بعدی یا وقوع نفوذ قبلی سیستم IT باشد یا رویدادهایی که نشان دهنده فعالیت‌های نامناسب است که منجر به بدبکاربردن، دستیابی و فعالیت‌های مخربی از دارایی‌های سیستم IT می‌شوند، باید جمع‌آوری گردند.
P.ANALYZ	پروسه‌ها و اطلاعات تحلیلی منجر به نتایجی در ارتباط با نفوذها (قبلی، حال، بعدی) می‌گردند که این نتایج باید به داده سیستم تشخیص نفوذ اعمال گردد و اقدامات مناسبی در قبال آنها صورت گیرد.
P.MANAGE	هدف ارزیابی باید به تنهایی توسط کاربران مجاز مدیریت گردد.
P.ACCESS	تمام داده‌های جمع‌آوری شده و تولید شده توسط هدف ارزیابی باید تنها برای اهداف مجاز استفاده گردند.
P.ACCACT	کاربران هدف ارزیابی باید پاسخگوی اقداماتشان در داخل سیستم تشخیص نفوذ باشند.
P.INTGTY	داده‌های جمع‌آوری شده و تولید شده توسط هدف ارزیابی باید از تغییرات حفظ گردند.
P. PROTCT	هدف ارزیابی باید از دستیابی غیرمجاز و قطع شدن داده‌های هدف ارزیابی و عملکردشان محافظت نماید.

۶ اهداف امنیتی

۶,۱ اهداف امنیتی هدف ارزیابی

O.TYPE	توضیحات
O.PROTCT	هدف ارزیابی باید خود را از تغییرات غیرمجاز و دستیابی به عملکرد و داده‌اش حفظ نماید.
O.IDSCAN	اسکنر باید اطلاعات پیکربندی ایستا را که ممکن است حاکی از پتانسیلی برای نفوذ بعدی یا وقوع نفوذ قبلی از یک سیستم IT باشند را جمع‌آوری و ذخیره نماید.
O.IDSENS	سنسورها باید اطلاعات مرتبط با تمام رویدادهایی که نشان دهنده فعالیت نامناسبی هستند را جمع‌آوری و ذخیره نمایند این فعالیت‌ها ممکن است منجر به بد به کار بردن، دستیابی یا فعالیت‌های مخربی در رابطه با دارایی‌های سیستم IT و سیستم تشخیص نفوذ گردند.
O.IDANLZ	تحلیلگر باید داده را از سنسورها و اسکنرهای سیستم تشخیص نفوذ دریافت نماید و سپس با عمال پردازش‌ها و اطلاعات تحلیلی، نتایجی در ارتباط با نفوذها استنتاج نماید.
O.RESPON	هدف ارزیابی باید به نتایج تحلیلی پاسخ مناسبی بدهند.
O.EADMIN	هدف ارزیابی باید دارای عملکردهایی باشد که بتواند به صورت موثر عملکردها و داده‌هایش را مدیریت نماید.
O.ACCESS	هدف ارزیابی باید اجازه بدهد که کاربران مجاز تنها به عملکردها و داده‌های مناسب هدف ارزیابی دسترسی داشته باشند.
O.IDAUTH	هدف ارزیابی پیش از آنکه به کاربران اجازه دستیابی به عملکردها و داده‌های هدف ارزیابی را بدهد، باید قادر به شناسایی و احرازهویت آنها باشد.
O.OFLOWS	هدف ارزیابی باید به صورت مناسبی سرریز ذخیره داده سیستمی و ممیزی را مدیریت نماید.

O.TYPE	توضیحات
O.AUDITS	هدف ارزیابی باید رکوردهای ممیزی را برای دستیابی داده و استفاده از عملکرد سیستم ثبت نماید.
O.INTEGR	هدف ارزیابی باید نسبت به صحت تمام داده‌های ممیزی و سیستمی اطمینان حاصل نماید.
O.EXPORT	زمانی‌که هر کامپوننت سیستم تشخیص نفوذ سبب گردد داده‌اش در دسترس کامپوننت سیستم تشخیص نفوذ دیگری قرار گیرد، هدف ارزیابی اطمینان خواهد داد که داده سیسستمی محرمانه است.

۱۶,۲اهداف امنیتی محیط عملیاتی

OE.TYPE	توضیحات
OE.AUDIT_PROTECTION	محیط IT قابلیت محافظت از اطلاعات ممیزی را فراهم خواهد نمود.
OE.AUDIT_SORT	محیط IT قابلیت مرتب‌سازی اطلاعات ممیزی را فراهم خواهد نمود.
OE.TIME	محیط IT قابلیت مهرهای زمانی قابل اطمینانی را به هدف ارزیابی ارائه خواهد نمود.
OE.INSTAL	کسانی که مسئول هدف ارزیابی هستند باید اطمینان بدهند که هدف ارزیابی به صورتی دریافت، نصب، مدیریت شده و هم‌چنین عمل می‌نماید که با امنیت IT سازگار باشد.
OE. PHYCAL	کسانی که مسئول هدف ارزیابی هستند باید اطمینان بدهند که بخش‌هایی از هدف ارزیابی که به خط‌مشی امنیتی حساس هستند از هرگونه حمله فیزیکی محافظت می‌گردند
OE.CREDEN	کسانی که مسئول هدف ارزیابی هستند باید اطمینان بدهند که تمام گواهینامه‌های دستیابی توسط کاربران به صورتی محافظت می‌گردد که با امنیت IT سازگار باشد.
OE.PERSON	افرادی که به عنوان سرپرستان مجاز فعالیت می‌نمایند باید با دقت انتخاب شوند و از قبل آموزش ببینند.

OE.TYPE	توضیحات
OE.INTROP	هدف ارزیابی با سیستم IT که مانیتور می‌گردد، قابل تفسیر [1]است.

۷ الزامات کارکرد امنیتی سیستم تشخیص نفوذ

جدول ۱- الزامات کارکرد امنیتی هدف ارزیابی

نام کلاس	نام عنصر		توضیحات
کلاس ممیزی امنیت (FAU)	FAU_GEN.1	ما–ت‌ل.۱	تولید داده ممیزی
	FAU_SAR.1	ما-ب‌ز.۱	بازبینی ممیزی امنیت
	FAU_SAR.2	ما-ب‌ز. ۲	بازبینی ممیزی محدود
	FAU_SAR.3	ما-ب‌ز.۳	بازبینی ممیزی قابل انتخاب
	FAU_SEL.1	ما-اخ.۱	ممیزی انتخابی
	FAU_STG.2	ما-ذخ.۲	تضمین در دسترس بودن داده‌های ممیزی
	FAU_STG.4	ما-ذخ.۴	پیشگیری از اتلاف و از بین رفتن داده-های ممیزی
کلاس شناسایی و	FIA_UAU.1	اش-اه.۱	زمان بندی احراز هویت
	FIA_AFL.1	اش-ش‌ا.۱	اداره نمودن شکست در احراز هویت

[1] Interoperable

نام کلاس	نام عنصر		توضیحات
احرازهویت (FIA)	FIA_ATD.1	اش-م‌ک.۱	تعریف صفات کاربری
	FIA_UID.1	اش-ش‌ک.۱	زمان‌بندی شناسایی
کلاس مدیریت امن (FMT)	FMT_MOF.1	م‌د-م‌ت.۱	مدیریت رفتار توابع امنیتی
	FMT_MTD.1	م‌د-م‌د.۱	مدیریت داده های توابع امنیتی هدف ارزیابی
	FMT_SMR.1	م‌د-ن‌م.۱	نقش‌های مدیریت امنیت
کلاس حفاظت از توابع امنیتی هدف ارزیابی (FPT)	FPT_ITA.1	ح‌ت-م‌د.۱	محرمانگی داده‌های ارسال شده بین توابع امنیتی هدف ارزیابی
	FPT_ITI.1	ح‌ت-ی‌د.۱	یکپارچگی داده‌های ارسال شده توابع امنیتی هدف ارزیابی
	FPT_STM.1	ح‌ت-م‌ز.۱	مهرهای زمانی
کلاس سیستم تشخیص نفوذ (IDS)	IDS_SDC.1	ت‌ن-دس-(ت‌س).۱	مجموعه داده‌های سیستم
	IDS_ANL.1	ت‌ن-ت‌ا-(ت‌س).۱	تجزیه و تحلیل تحلیل‌گر
	IDS_RCT.1	ت‌ن-وا-(ت‌س).۱	واکنش تحلیل‌گر
	IDS_RDR.1	ت‌ن-ب‌د -(ت‌س).۱	بازبینی داده‌های محدود شده
	IDS_STG.1	ت‌ن-ت‌د-(ت‌س).۱	تضمین در دسترس بودن داده‌های سیستم
	DS_STG.2	ت‌ن-ت‌د-(ت‌س).۲	تضمین در دسترس بودن داده‌های سیستم

۷,۱ کلاس ممیزی امنیت

نام کلاس: ممیزی امنیت

شرح کلاس: سامانه‌های تشخیص نفوذ برای رخدادهای گوناگون اقدام به ایجاد گزارش‌هایی برای ممیزی می‌نمایند. کلاس ممیزی امنیت، الزاماتی پیرامون نحوه شناخت، ثبت و ذخیره و آنالیز اطلاعات ممیزی مربوط به فعالیت‌های امنیتی تعریف نموده است (فعالیت‌هایی که توسط توابع امنیتی هدف ارزیابی کنترل می‌گردند). با بررسی ممیزی‌های ثبت شده می‌توان تعیین کرد که کدام رخداد مرتبط با چه فعالیت امنیتی صورت گرفته و چه‌کسی (چه کاربری) مسوول آن است. این کلاس شامل شش خانواده است که عبارتند از:

- **خانواده پاسخ خودکار ممیزی امنیت[1]**

این خانواده تعریف کننده الزامات برای واکنش‌های سیستم نسبت به رویدادهایی است که به‌روز بودن آنها نشان‌دهنده نقض امنیتی بالقوه‌ای باشد.

- **خانواده تولید داده ممیزی[2]**

این خانواده الزاماتی برای ثبت رخدادهای امنیتی مربوط به رویدادهایی که تحت کنترل توابع امنیتی هدف ارزیابی صورت می‌گیرند را تعریف می‌نماید. این خانواده سطح ممیزی را تعیین می‌نماید، انواع رویدادهایی که باید توسط توابع امنیتی هدف ارزیابی قابل ممیزی باشند را بیان می‌نماید و یک مجموعه حداقلی از اطلاعات مرتبط با ممیزی را تعیین می‌کند که باید در داخل انواع ممیزی‌های امنیتی ثبت شده، ارائه گردند.

---

[1] Security audit automatic response (FAU_ARP)

[2] Security audit data generation (FAU_GEN)

➢ **خانواده تحلیل ممیزی امنیت**[1]

این خانواده الزاماتی برای ابزارهای خودکار، که فعالیت‌های سیستم را تحلیل می‌نماید و داده‌های ممیزی که نقض امنیتی واقعی یا ممکن را جستجو می‌کنند، تعریف می-نماید. این تحلیل ممکن است در پشتیبانی از تشخیص نفوذ، یا پاسخ خودکار به نقض امنیتی بالقوه کار نماید.

- **خانواده بازبینی ممیزی امنیت**[2]

این خانواده تعریف کننده الزاماتی برای ابزارهای ممیزی است که باید در دسترس کاربران مجاز قرار بگیرند تا به بازبینی داده‌های ممیزی کمک نماید.

- **خانواده انتخاب رویداد ممیزی امنیت**[3]

این خانواده تعریف کننده الزاماتی جهت انتخاب یک مجموعه رویدادهای ممیزی شده در طول عملکرد هدف ارزیابی، از بین تمام رویدادهای قابل ممیزی می‌باشد.

- **خانواده ذخیره‌سازی رویداد ممیزی امنیت**[4]

این خانواده تعریف کننده الزاماتی برای توابع امنیتی هدف ارزیابی است تا قادر به ایجاد و نگهداری از سوابق ممیزی بصورت امن باشد.

---

[1] Security audit analysis (FAU_SAA)

[2] Security audit review (FAU_SAR**)**

[3] Security audit event selection (FAU_SEL)

[4] Security audit event storage (FAU_STG)

شماره	نام خانواده	عنصر امنیتی
		الزام
۱	تولید داده ممیزی امنیت (FAU_GEN)	**نام عنصر: تولید داده ممیزی امنیت ۱** **شماره مولفه: م‌ا‌–ت‌ل.۱,۱(FAU_GEN.1.1))**

شرح مولفه:

توابع امنیتی هدف ارزیابی باید بتوانند از رویدادهای قابل ممیزی زیر یک رکورد ممیزی تولید نمایند:

الف-آغاز و پایان عملیات ممیزی

ب-کلیه رویدادهای قابل ممیزی برای سطح پایه ممیزی

پ-دسترسی به سیستم و دسترسی به هدف ارزیابی و داده‌های سیستم.

نکته کاربردی:

رویدادهای قابل ممیزی برای سطح پایه ممیزی در جدول زیر آمده‌اند.

جدول ۱- رویدادهای قابل ممیزی

عنصر	رویداد	جزئیات

شماره نام خانواده

عنصر امنیتی

الزام

ما-ت‌ل.۱	آغاز و پایان عملیات ممیزی	-
ما-ت‌ل.۱	دسترسی به سیستم	-
ما-ت‌ل.۱	دسترسی به هدف ارزیابی و داده سیستم	موجودیت غیرفعال سیستم تشخیص نفوذ، دسترسی درخواست شده
ما-ب‌ز.۱	خواندن اطلاعات رکورد ممیزی	-
ما-ب‌ز.۲	تلاش ناموفق جهت خواندن اطلاعات رکوردهای ممیزی	-
ما-اخ.۱	تمام تغییرات به تنظیمات ممیزی رخ می‌دهد، هنگامی که عملیات جمع‌آوری ممیزی صورت می‌گیرد	-
اش-اه.۱	تمام استفاده از سازوکار احراز هویت	هویت کاربر، موقعیت
اش-ش‌ک.۱	تمام استفاده از سازوکار شناسایی کاربر	هویت کاربر، موقعیت
مد-مت.۱	تمام تغییرات در رفتار عملیات‌های توابع امنیتی هدف ارزیابی	-

شماره	نام خانواده	عنصر امنیتی	الزام
		م‌د-م‌د.۱	تمام تغییرات مقادیر عملیات‌های توابع امنیتی هدف ارزیابی	-
		م‌د-ن‌م.۱	تغییرات به گروهی از کاربران که بخشی از یک نقش هستند.	-

نکته کاربردی:

الزامات خانواده (ت‌ن_ت‌ا[1]) و (ت‌ن_دس[2]) در این پروفایل حفاظتی به ثبت نتایج مربوط به پویش، سنجش و تجزیه و تحلیل وظایف سیستم تشخیص نفوذ اشاره می‌کنند.

۲ **نام عنصر: تولید داده ممیزی امنیت ۱**

شماره مولفه: م‌ا – ت‌ل.۲,۱(FAU_GEN.1.2)

شرح مولفه:

توابع امنیتی هدف ارزیابی باید در هر رکورد ممیزی، حداقل اطلاعات زیر را ثبت نمایند:

[1] IDS_ANL (Analyser analysis)
[22] IDS_SDC (System Data Collection)

شماره	نام خانواده	عنصر امنیتی	الزام
			الف - تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال و نتیجه (موفقیت یا شکست) رویداد ب- برای هر نوع رویداد ممیزی، بر اساس تعریف‌های رویداد قابل ممیزی عناصر عملیاتی موجود در پروفایل حفاظتی/هدف امنیتی، اطلاعات تکمیلی در ستون جزئیات جدول ۲ مشخص شده است.
۳	بازبینی ممیزی امنیت (FAU_SAR)	**نام عنصر: بازبینی ممیزی امنیت ۱** **شماره مولفه: م‌ا-ب‌ز.۱,۱(FAU_SAR.1.1)**	

شرح مولفه:

توابع امنیتی هدف ارزیابی باید [اختصاص: **کاربرانی مجاز**] را با قابلیت خواندن [اختصاص: **فهرستی از اطلاعات ممیزی**] از رکوردهای ممیزی ایجاد نماید.

نکته کاربردی:

این الزام به کاربران مجاز هدف ارزیابی اعمال می‌شود و برای نویسندگان هدف امنیتی این امکان را فراهم می‌آورد تا تعریف کند که کاربران مجاز به چه داده ممیزی می‌توانند دسترسی داشته باشند.

شماره	نام خانواده عنصر امنیتی الزام	
۴	**نام عنصر: بازبینی ممیزی امنیت ۱**	
	شماره مولفه: م‌ا-ب‌ز.۲,۱(FAU_SAR.1.2)	
	شرح مولفه:	
	توابع امنیتی هدف ارزیابی باید رکوردهای ممیزی را به شکل مناسبی برای کاربر، جهت تفسیر اطلاعات فراهم نمایند.	
۵	**نام عنصر: بازبینی ممیزی محدود ۲**	
	شماره مولفه: م‌ا-ب‌ز.۱,۲(FAU_SAR.2.1)	
	شرح مولفه:	
	توابع امنیتی هدف ارزیابی باید از قابلیت دسترسی کلیه کاربران جهت خواندن رکوردهای ممیزی ممانعت نمایند، بجز کاربرانی که به آنها مجوز دسترسی با قابلیت خواندن داده شده باشد.	
۶	**نام عنصر: بازبینی ممیزی قابل انتخاب ۳**	
	شماره مولفه: م‌ا-ب‌ز.۱,۳(FAU_SAR.3.1)	

شماره	نام خانواده	
ه		**عنصر امنیتی**
الزام		

شرح مولفه:

توابع امنیتی هدف ارزیابی باید قابلیت انجام مرتب‌سازی داده‌های ممیزی بر اساس تاریخ و زمان، هویت موجودیت فعال، نوع رویداد و موفقیت یا شکست رویداد مربوطه را فراهم نمایند.

۷	انتخاب رویداد ممیزی امنیت **(FAU_SEL)**	**نام عنصر: ممیزی انتخابی ۱** **شماره مولفه: ما-اخ.۱,۱(FAU_SEL.1.1)**

شرح مولفه:

توابع امنیتی هدف ارزیابی باید قابلیت انتخاب رویدادهای قابل ممیزی بر اساس دارا بودن/ نبودن ویژگی‌های زیر از مجموعه رویدادهای ممیزی را داشته باشند:

الف- نوع رویداد

ب- [اختصاص: **فهرستی از ویژگی‌های تکمیلی که انتخاب ممیزی بر اساس آن می‌باشد**].

۸	ذخیره سازی	**نام عنصر: تضمین در دسترس بودن داده‌های ممیزی ۲**

شماره	نام خانواده	عنصر امنیتی	الزام
	رویدادهای ممیزی امنیت (FAU_STG)	**شماره مولفه: م‌ا-ذخ.۲,۱(FAU_STG.2.1)** **شرح مولفه:**	

توابع امنیتی هدف ارزیابی باید رکوردهای ممیزی ذخیره شده را از حذف غیر مجاز محافظت نمایند.

۹		**نام عنصر: تضمین در دسترس بودن داده‌های ممیزی ۲** **شماره مولفه: م‌ا-ذخ.۲,۲(FAU_STG.2.2)** **شرح مولفه:**	

توابع امنیتی هدف ارزیابی باید قادر به تشخیص تغییرات در رکوردهای ممیزی باشند.

۱۰		**نام عنصر: تضمین در دسترس بودن داده‌های ممیزی ۲** **شماره مولفه: م‌ا-ذخ.۲,۳(FAU_STG.2.3)** **شرح مولفه:**	

توابع امنیتی هدف ارزیابی باید اطمینان بدهند هنگامی‌که [انتخاب: *ضعف در ذخیره نمودن ممیزی، خرابی، حمله*] رخ می‌دهد،

شماره	نام خانواده
ه	عنصر امنیتی
الزام	

[اختصاص: **معیار قابل سنجش برای ذخیره نمودن رکوردهای ممیزی**] رکوردهای ممیزی نگهداری خواهند شد.

۱۱ **نام عنصر: پیشگیری از اتلاف و از بین رفتن داده‌های ممیزی ۴**

شماره مولفه: م۱-ذخ.۴،۱(FAU_STG.4.1)

شرح مولفه:

توابع امنیتی هدف ارزیابی در صورت پر شدن دنباله ممیزی، باید [انتخاب:*«از ذخیره رویدادهای قابل ممیزی، بجز آنهایی که توسط کاربر مجاز و تحت حقوق خاص رخ می دهند، جلوگیری نماید»*، *«بر روی قدیمی ترین رکوردهای ممیزی ذخیره شده دوباره نویسی نماید»*] و یک هشدار ارسال نمایند.

۷،۲ کلاس شناسایی و احراز هویت

در ادامه المان‌های امنیتی مورد نیاز کلاس شناسایی و احرازهویت ارائه شده است.

نام کلاس: شناسایی و احراز هویت

شرح کلاس: خانواده‌های این کلاس بیان کننده الزامات مورد نیاز برای توابعی است تا بتوانند هویت کاربر ادعا شده را تصدیق و تائید نمایند. شناسایی و احراز هویت نمودن لازم و ضروری می‌باشد تا تضمین شود که کاربران همراه با صفات امنیتی مناسبی می‌باشند (به طور مثال، هویت، گروه‌ها، نقش‌ها، سطوح یکپارچگی یا امنیت)

شناسایی غیر مبهم کاربران مجاز و اختصاص صحیح صفات امنیتی به کاربران و موجودیت‌های فعال بسیار مهم و حساس است تا خط‌مشی‌های امنیتی در نظرگرفته شده در عمل پیاده سازی شوند. خانواده‌های این کلاس الزاماتی را فراهم می‌آورند تا هویت کاربران تعیین و احراز هویت شوند، صلاحیت آنهایی را که با هدف ارزیابی در تعامل هستند را تعیین نمایند، و برای هر کاربر مجاز مشخصه‌های امنیتی را به طور صحیح اختصاص داده شود. موثر اجرا شدن الزامات کلاس‌های دیگر (به طور مثال، محافظت داده کاربری، ممیزی امنیتی) به شناسایی و احراز هویت صحیح کاربران بستگی دارد. این کلاس از شش خانواده تشکیل شده است که در ادامه به صورت مختصر شرح داده شده‌اند.

- **خانواده شکست‌ها در احراز هویت[1]**

این خانواده حاوی الزاماتی است که تعریف کننده مقادیری برای تعداد تلاش‌های ناموفق صورت گرفته جهت احراز هویت می‌باشد، هم‌چنین اقداماتی که توابع امنیتی هدف ارزیابی در مواردی که تلاش جهت احراز هویت با شکست مواجه می‌گردد را تعریف می‌نماید. پارامترهایی هم‌چون تعداد تلاش‌های احراز هویت منجر به شکست و آستانه زمان در الزامات این خانواده تعیین می‌گردند.

- **خانواده تعریف مشخصه کاربر[2]**

تمام کاربران مجاز ممکن است دارای یک مجموعه از مشخصه‌های امنیتی، به غیر از هویت کاربر که در اجرای الزامات عملکرد امنیتی استفاده شده است، باشند. این خانواده الزاماتی برای مرتبط نمودن مشخصه‌های امنیتی کاربر به کاربران تعریف می‌نماید تا در صورت لزوم توابع امنیتی هدف ارزیابی را در تصمیم‌گیری های امنیتی پشتیبانی نماید.

---

[1] Authentication failures(FIA_AFL)

[2] User attribute definition (FIA_ATD)

- **خانواده خصوصیات رازها**[1]

این خانواده تعریف کننده الزاماتی برای سازوکارهایی است که معیارهای کیفی تعریف شده را، بر روی رازها اجرا می‌نمایند. الزامات بر روی ساختار کلمه عبور، نمونه‌ای از آن است.

- **خانواده احراز هویت کاربر**[2]

این خانواده تعریف کننده انواع سازوکارهای احراز هویت کاربر و الزامات مرتبط با آن است که توسط توابع امنیتی هدف ارزیابی پشتیبانی می‌گردد.

- **خانواده شناسایی کاربر**[3]

این خانواده تعریف کننده شرایطی است که تحت آن کاربران ملزم به شناسایی خود قبل از انجام هر اقدام دیگری توسط توابع امنیتی هدف ارزیابی می‌باشند.

- **خانواده اتصال موجودیت فعال- کاربر**[4]

یک کاربر احراز هویت شده، به منظور استفاده از توابع امنیتی هدف ارزیابی معمولاً به عنوان یک موجودیت فعال در سیستم عمل می‌کند. مشخصه‌های امنیتی کاربر به این موجودیت فعال نیز مرتبط می‌گردد(به طور کامل یا بخشی از آن). این خانواده الزاماتی را تعریف می‌نماید تا ایجاد و نگهداری ارتباط بین کاربر و موجودیت فعال متناظر با آن را فراهم آورد.

---

[1] Specification of secrets (FIA_SOS)

[2] User authentication (FIA_UAU)

[3] User identification (FIA_UID)

[4] User – subject binding (FIA_USB)

شماره	نام خانواده الزام	عنصر امنیتی
۱۲	احراز هویت کاربر (FIA_UAU)	**نام عنصر: زمان‌بندی احراز هویت ۱** **شماره مولفه: اش-اه.۱,۱ (FIA_UAU.1.1)** **شرح مولفه:** توابع امنیتی هدف ارزیابی، باید اجازه انجام [اختصاص: **لیستی از اقدامات میانی**] پیش از احراز هویت را به کاربر بدهند. **نکته کاربردی:** نویسنده هدف ارزیابی باید هرگونه اقدام میانی که مجاز است پیش از احراز هویت کاربر انجام بگیرد را مشخص نماید. این اقدامات باید کاربر را به صورت محدودی در دستیابی به هدف ارزیابی کمک نماید. از اقدامات قابل قبول، قبل از احراز هویت کاربر استفاده از امکانات راهنما است.
۱۳		**نام عنصر: زمان‌بندی احراز هویت ۱** **شماره مولفه:اش-اه ۲,۱ (FIA_UAU.1.2)** **شرح مولفه:** توابع امنیتی هدف ارزیابی، باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، با موفقیت

شماره	نام خانواده الزام	عنصر امنیتی
		احراز هویت نمایند.
۱۴	اداره نمودن شکست در احراز هویت (FIA_AFL)	**نام عنصر: ساماندهی شکست در احراز هویت ۱** **شماره مولفه: اش-ش ۱٫۱٫۱ (FIA_AFL.1.1)**

شرح مولفه:

توابع امنیتی هدف ارزیابی، باید [اختصاص: **یک عدد مثبت قابل تنظیم و غیر صفر]** از تلاش‌های ناموفق احراز هویت را نسبت به آخرین احراز هویت موفق، مشخص نمایند.

نکته کاربردی:

هدف ارزیابی ممکن است برای کاربران مختلف، روش‌های احراز هویت متفاوتی استفاده نماید، و از قوانین مختلفی براساس روش‌های احرازهویت/ یا کاربران، جهت ساماندهی احراز هویت‌های ناموفق بهره بگیرد. رفتاری که در قبال احراز هویت ناموفق، برای سیستم-های از راه دور و کاربران انسانی صورت می‌گیرد، به طور معمول متفاوت از هم می‌باشد. حتی برای کاربران انسانی ممکن است، عکس‌العمل در برابر احراز هویت ناموفق برای احراز هویتی که از طریق نام کاربری/رمزعبور صورت می‌گیرد نسبت به احراز هویتی که از طریق کارت هوشمند یا گواهینامه‌های دیجیتال انجام می‌گیرد، متفاوت باشد.

شماره	نام خانواده	عنصر امنیتی
		الزام

رویداد احراز هویت ناموفق با توجه به آخرین نشست موفق در ترمینال شمارش می‌گردد.

هرچند که لیستی از اقدامات می‌تواند توسط هدف ارزیابی، مشخص گردد. اما این مجموعه اقدامات باید اطمینان بدهند که، از حملات مبتنی بر جستجو در فضاهای ممکن جلوگیری می‌نمایند.

۱۵ **نام عنصر: ساماندهی شکست در احراز هویت ۱**

شماره مولفه: اش-ش ا ۲,۱ (FIA_AFL.1.2)

شرح مولفه:

زمانی‌که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین شده رسید یا از آن بیشتر شد، توابع امنیتی هدف ارزیابی باید اقداماتی را که بدین منظور در نظر گرفته شده است، انجام دهند. یکی از این اقدامات می‌تواند پیچیده تر کردن عمل احراز هویت مجدد کاربر باشد.

نکته کاربردی:

از آنجا که نیازی به قفل نمودن حساب کاربری سرپرست دیده نمی‌شود، این الزام برای سرپرستان محلی به کار برده نمی‌شود، بدین منظور حساب کاربری سرپرست محلی از سایر حساب‌های کاربری مجزا می‌گردد، جداسازی حساب کاربری سرپرست از کاربران می-

شماره	نام خانواده	عنصر امنیتی
		الزام
		تواند در سند مربوط به سرپرست بیان گردد یا سازوکار احراز هویت هدف ارزیابی، می‌تواند تلاش‌های ورود محلی به سیستم را از تلاش‌های ورود از راه دور به سیستم متمایز نماید.
۱۶	تعریف مشخصه کاربر (FIA_ATD)	**نام عنصر: تعریف مشخصه کاربر ۱** **شماره عنصر:اش-م‌ک .۱،۱ (FIA_ATD.1.1)** **شرح مولفه:** توابع امنیتی هدف ارزیابی، باید مشخصه‌های امنیتی زیر را برای هر کاربر نگهداری نماید: ۱- شناسه کاربر ۲- داده های احراز هویت ۳- مجوزهای کاربر ۴- [اختصاص: **هر مشخصه امنیتی دیگر**] **نکته کاربردی:** حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت باید وجود داشته باشد. این اطلاعات شامل نگهداری نمودن از هر

شماره	نام خانواده	عنصر امنیتی
الزام		
		مجوزی است که یک کاربر ممکن است دارا باشد.
۱۷	زمان‌بندی شناسایی (FIA_UID)	**نام عنصر: زمان‌بندی شناسایی ۱** **شماره عنصر:اش-ش‌ک.۱,۱ (FIA_UID.1.1)** **شرح مولفه:** توابع امنیتی هدف ارزیابی، باید اجازه انجام [اختصاص: **لیستی از اقدامات میانی**] را پیش از شناسایی کاربر به وی بدهند. **نکته کاربردی:** نویسنده هدف ارزیابی باید هرگونه اقدام میانی که پیش از شناسایی کاربر، مجاز است انجام بگیرد را مشخص نماید. این اقدامات باید کاربر را به صورت محدودی در دستیابی به هدف ارزیابی کمک نماید.
۱۸		**نام عنصر: زمان‌بندی شناسایی ۱** **شماره عنصر:اش-ش‌ک.۲,۱ (FIA_UID.1.2)** **شرح مولفه:** توابع امنیتی هدف ارزیابی، باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، با موفقیت

شماره	نام خانواده	عنصر امنیتی
الزام		
		شناسایی نماید.

۷,۳ کلاس مدیریت امنیت

نام کلاس: مدیریت امنیت

شرح کلاس: این کلاس جهت مشخص نمودن مدیریت ویژگی‌های مختلف توابع امنیتی هدف ارزیابی در نظر گرفته شده است. در این کلاس مشخصه‌های امنیتی، توابع و داده‌های توابع امنیتی هدف ارزیابی، نقش‌های مدیریتی مختلف و تعاملاتشان، هم‌چون جداسازی قابلیت‌ها ، می‌توانند مشخص گردند.

این کلاس دارای چندین هدف است:

- مدیریت داده توابع امنیتی هدف ارزیابی برای مثال علامت‌ها[1]
- مدیریت مشخصه‌های امنیتی، برای مثال لیست‌های کنترل دسترسی و لیست قابلیت‌ها
- مدیریت کارکرد توابع امنیتی هدف ارزیابی برای مثال، انتخاب توابع، نقش‌ها یا شرایطی که رفتار توابع امنیتی هدف ارزیابی را تحت تاثیر قرار می‌دهند.
- تعریف نقش‌های امنیتی

خانواده‌های آن در ادامه آمده است.

[1] Banner

- **خانواده مدیریت کارکرد توابع امنیتی هدف ارزیابی[1]**

این خانواده اجازه کنترل کاربران مجاز در حین مدیریت کارکرد توابع امنیتی هدف ارزیابی را می‌دهد. مثالی از عملکردها در توابع امنیتی هدف ارزیابی شامل ممیزی توابع و توابع احراز هویت چندگانه می‌باشد.

- **خانواده مدیریت مشخصه‌های امنیتی[2]**

این خانواده اجازه کنترل کاربران مجاز در حین مدیریت مجوزهای امنیتی را می‌دهد. این مدیریت می‌تواند شامل قابلیتی برای مشاهده و تغییر مجوزهای امنیتی باشد.

- **خانواده مدیریت داده‌های توابع امنیتی هدف ارزیابی[3]**

این خانواده اجازه کنترل کاربران (نقش‌ها) مجاز در حین مدیریت داده‌های توابع امنیتی هدف ارزیابی را می‌دهد. مثالی از داده توابع امنیتی هدف ارزیابی می‌تواند شامل ممیزی اطلاعات، ساعت و دیگر پارامترهای پیکربندی توابع امنیتی هدف ارزیابی باشد.

- **خانواده لغو[4]**

این خانواده لغو مشخصه‌های امنیتی انواع موجودیت‌ها در هدف ارزیابی را آدرس‌دهی می‌کند.

- **خانواده انقضای مشخصه امنیتی[1]**

---

[1] Management of functions in TSF (FMT_MOF)

[2] Management of security attributes (FMT_MSA)

[3] Management of TSF data (FMT_MTD)

[4] Revocation (FMT_REV)

این خانواده قادر به اعمال محدودیت زمانی برای اعتبار مشخصه‌های امنیتی می‌باشد.

➢ خانواده مشخصات کارکردهای مدیریت[۲]

این خانواده اجازه می‌دهد تا مشخصات عملکردهای مدیریتی توسط هدف ارزیابی ایجاد شوند. عملکردهای مدیریتی با استفاده از ایجاد رابط توابع امنیتی هدف ارزیابی، به سرپرستان اجازه می‌دهند تا پارامترهایی برای کنترل عملکرد ویژگی‌های مربوط به امنیت هدف ارزیابی تعریف نمایند، مانند مجوزها و صفات حفاظت از داده، مجوزها و صفات حفاظت از هدف ارزیابی، مجوزها و صفات ممیزی و مجوزها و صفات شناسایی و احراز هویت.

عملکردهای مدیریتی هم‌چنین شامل آن دسته از عملکردهایی است که توسط کاربر اجرا می‌گردد تا تداوم عملکرد هدف ارزیابی را تضمین نماید، مانند عملکردهای پشتیبانی و بازیابی. عملکرد این خانواده بر روی دیگر مولفه‌ها در کلاس مدیریت امنیت تاثیر دارد.

➢ خانواده نقش‌های مدیریت امنیتی[۳]

این خانواده برای کنترل اختصاص نقش‌های مختلف به کاربران در نظرگرفته شده است. توانایی این نقش‌ها با توجه به مدیریت امنیتی است که در دیگر خانواده‌های این کلاس توصیف شده است.

شماره	نام خانواده	عنصر امنیتی	الزام

[1] Security attribute expiration (FMT_SAE)

[2] Specification of Management Functions (FMT_SMF)

[3] Security management roles (FMT_SMR)

شماره	نام خانواده الزام	عنصر امنیتی
۱۹	مدیریت رفتار توابع امنیتی (FMT_MOF)	**نام عنصر: مدیریت رفتار توابع امنیتی ۱** **شماره عنصر: م‌د-م‌ت .۱,۱ (FMT_MOF.1.1)** **شرح مولفه:** توابع امنیتی هدف ارزیابی باید قابلیت تغییر رفتار توابع جمع‌آوری داده‌های سیستم، آنالیز و عکس‌العمل را فقط به سرپرستان مجاز سیستم محدود نمایند. **نکته کاربردی:** هدف ارزیابی ممکن است بر روی سیستم عامل دارای نقش‌های سرپرستی باشد که اجازه تغییر پیکربندی سیستم را نداشته باشند.
۲۰	مدیریت داده‌های توابع امنیتی هدف ارزیابی (FMT_MTD)	**نام عنصر: مدیریت داده‌های توابع امنیتی هدف ارزیابی ۱** **شماره عنصر:م‌د-م‌د.۱,۱ (FMT_MTD.1.1)** **شرح مولفه:** توابع امنیتی هدف ارزیابی باید قابلیت پرس و جو و اضافه نمودن داده‌های سیستم و ممیزی و هم‌چنین قابلیت پرس و جو و تغییر دیگر داده‌های هدف ارزیابی را به [اختصاص: **نقش‌های شناسایی شده مجاز**] محدود نماید.

شماره	نام خانواده الزام	عنصر امنیتی

نکته کاربردی:

نویسنده هدف امنیتی باید تعریف نماید که چه نقش‌هایی مجاز به دستیابی به داده‌های سیستم و دیگر داده‌های هدف ارزیابی هستند.

هدف امنیتی ممکن است چندین نقش را برای برآورده کردن این الزام تعریف نماید.

۲۱ نقش‌های امنیتی (FMT_SMR)

نام عنصر: نقش‌های امنیتی ۱

شماره عنصر:م‌د-ن‌م .۱,۱ (FMT_SMR.1.1)

شرح مولفه:

توابع امنیتی هدف ارزیابی باید نقش‌های زیر را ایجاد و نگهداری نمایند:

- سرپرست مجاز
- سرپرستان مجاز سیستم
- و [اختصاص: **دیگر نقش‌های شناسایی شده مجاز**]

۲۲

نام عنصر: نقش‌های امنیتی ۱

شماره عنصر:م‌د-ن‌م .۲,۱ (FMT_SMR.1.2)

شماره نام خانواده

الزام **عنصر امنیتی**

شرح مولفه:

توابع امنیتی هدف ارزیابی، باید قادر به مرتبط نمودن کاربران با نقش‌های مجاز تعریف شده باشند.

۷,۴ کلاس حفاظت از توابع امنیتی هدف ارزیابی

در ادامه المان‌های امنیتی مورد نیاز کلاس حفاظت از توابع امنیتی هدف ارزیابی ارائه شده است.

نام کلاس: حفاظت از توابع امنیتی هدف ارزیابی

شرح کلاس:

این کلاس خانواده‌هایی از الزامات عملیاتی را در برمی‌گیرد که در ارتباط با صحت و مدیریت ساز و کارهایی هستند که با توابع امنیتی هدف ارزیابی ترکیب می‌شوند و برای صحت و یکپارچگی داده توابع امنیتی هدف ارزیابی مورد استفاده قرار می‌گیرند. از بعضی جنبه‌ها، خانواده‌های این کلاس ممکن است به نظر بیاید که تکرار عناصر کلاس محافظت از داده کاربری است، حتی ممکن است هر دوی این کلاس‌ها با ساز و کاری مشابه پیاده‌سازی شده باشند. هرچند کلاس محافظت از داده کاربری بر روی محافظت از داده کاربری متمرکز شده است اما کلاس محافظت از توابع امنیتی هدف ارزیابی بر روی محافظت از داده‌های توابع امنیتی هدف ارزیابی متمرکز شده است. در حقیقت، عناصر کلاس محافظت از توابع امنیتی هدف ارزیابی لازم است الزاماتی را ارائه نمایند که خط‌مشی‌های توابع امنیتی هدف ارزیابی نتوانند مورد مداخله قرار بگیرند یا دور زده[1] شوند.

[1] Bypass

از دیدگاه این کلاس، باتوجه به توابع امنیتی هدف ارزیابی سه مولفه مهم وجود دارد:

- پیاده‌سازی توابع امنیتی هدف ارزیابی، که ساز و کارهای اجرا کننده توابع امنیتی هدف ارزیابی را اجرا و پیاده‌سازی می‌نمایند.
- داده توابع امنیتی هدف ارزیابی، که پایگاه داده‌های سرپرستی، راهنمایی کننده اجرای الزامات کارکرد امنیتی می‌باشند.
- موجودیت‌های خارجی که توابع امنیتی هدف ارزیابی، ممکن است جهت اجرای الزامات کارکرد امنیتی با آنها در تعامل باشند.

- **خانواده نقض امنیت[1]**

الزامات این خانواده اطمینان می‌دهد که هدف ارزیابی در هنگامی که مجموعه‌ای از شکست‌های مشخص در توابع امنیتی هدف ارزیابی روی می‌دهد، کارکرد امنیتی لازم اجرا می‌گردد.

- **خانواده در دسترس بودن داده‌های ارسال شده توابع امنیتی هدف ارزیابی[2]**

این خانواده قوانینی را تعریف می‌نماید که در هنگام انتقال داده توابع امنیتی هدف ارزیابی بین توابع امنیتی هدف ارزیابی و دیگر محصولات IT از نبود دسترسی به این داده-ها، جلوگیری می‌نماید. برای مثال این داده می‌تواند، داده‌های حساس توابع امنیتی هدف ارزیابی هم‌چون رمز عبور، کلیدها، داده ممیزی، یا کدهای اجرایی توابع امنیتی هدف ارزیابی باشند.

- **خانواده محرمانگی داده‌های ارسال شده توابع امنیتی هدف ارزیابی[3]**

[1] Fail secure (FPT_FLS)

[2] Availability of exported TSF data (FPT_ITA)

[3] Confidentiality of exported TSF data (FPT_ITC)

این خانواده تعریف کننده قوانینی برای محافظت از افشای غیرمجاز داده توابع امنیتی هدف ارزیابی در طول انتقال بین توابع امنیتی هدف ارزیابی و دیگر محصولات امن IT می‌باشد. برای مثال این داده می‌تواند، داده‌های حساس توابع امنیتی هدف ارزیابی هم‌چون رمز عبور، کلیدها، داده ممیزی، یا کُدهای اجرایی توابع امنیتی هدف ارزیابی باشد.

- **خانواده یکپارچگی داده‌های ارسال شده توابع امنیتی هدف ارزیابی[1]**

این خانواده تعریف کننده قوانینی برای حفاظت از تغییرات غیرمجاز داده‌های توابع امنیتی هدف ارزیابی است که بین توابع امنیتی هدف ارزیابی و دیگر محصولات امن IT منتقل می‌گردند. برای مثال این داده می‌تواند، داده‌های حساس توابع امنیتی هدف ارزیابی هم‌چون رمز عبور، کلیدها، داده ممیزی، یا کدهای اجرایی توابع امنیتی هدف ارزیابی باشد.

- **خانواده انتقال داده‌های داخلی توابع امنیتی هدف ارزیابی[2]**

این خانواده الزاماتی را ارائه می‌نماید که از داده توابع امنیتی هدف ارزیابی در زمان انتقال بین بخش‌های مجزای توابع امنیتی هدف ارزیابی در سراسر کانال داخلی محافظت می‌نماید.

- **خانواده محافظت فیزیکی از توابع امنیتی هدف ارزیابی[3]**

مولفه‌های حفاظت فیزیکی توابع امنیتی هدف ارزیابی به محدودیت‌هایی بر روی دستیابی فیزیکی غیرمجاز به توابع امنیتی هدف ارزیابی، بازدارندگی از، مقاومت در برابر، اصلاح فیزیکی غیرمجاز یا جایگزینی توابع امنیتی هدف ارزیابی اشاره دارند.

---

[1] Integrity of exported TSF data (FPT_ITI)

[2] Internal TOE TSF data transfer (FPT_ITT)

[3] TSF physical protection (FPT_PHP)

الزامات مولفه‌ها در این خانواده این اطمینان را می‌دهند که توابع امنیتی هدف ارزیابی از مداخله فیزیکی و تداخلات محافظت می‌گردد. ارضاء شدن این مولفه‌ها منجر به بسته‌بندی و استفاده توابع امنیتی هدف ارزیابی به صورتی گردد که مداخلات فیزیکی قابل تشخیص باشند یا مجبور به مقاومت در برابر تداخلات فیزیکی گردند. بدون این مولفه‌ها، عملکرد حفاظتی از توابع امنیتی هدف ارزیابی اثرشان را در محیط‌هایی که از آسیب فیزیکی نمی‌توان جلوگیری نمود، از دست می‌دهند این خانواده هم‌چنین الزاماتی را ارائه نموده است که چطور توابع امنیتی هدف ارزیابی باید به تلاش‌هایی که در ارتباط با تداخل فیزیکی صورت می‌گیرد، واکنش نشان دهد.

- **خانواده بازیابی مطمئن[1]**

الزامات این خانواده اطمینان می‌دهند که توابع امنیتی هدف ارزیابی می‌توانند تشخیص دهند که هدف ارزیابی بعد از قطع عملیات، بدون به خطر افتادن حفاظت راه‌اندازی می‌گردد و هم‌چنین می‌تواند بازیابی گردد. این خانواده بسیار مهم است زیرا وضعیت راه‌اندازی توابع امنیتی هدف ارزیابی تعیین کننده حفاظت از وضعیت‌های بعدی می‌باشد.

- **خانواده شناسایی مجدد[2]**

این خانواده انواع مختلف موجودیت‌ها (به طور مثال، پیغام‌ها، درخواست‌های سرویس، پاسخ‌های سرویس) و اقدامات بعدی را مجدداً شناسایی می‌نماید تا به طور صحیح انجام شده باشند. با توجه به این الزام از مواردی‌که ممکن است مجدداً شناسایی شوند به طور موثر جلوگیری می‌شود.

- **خانواده پروتکل همگامی حالت[3]**

هدف ارزیابی توزیع شده ممکن است نسبت به هدف ارزیابی واحد، به واسطه اختلاف حالت‌ها بین بخش‌های مختلف هدف ارزیابی و تاخیر در ارتباطات دارای پیچیدگی بیشتر باشد. در اغلب موارد هماهنگ سازی حالت‌ها بین عملکردهای توزیع یافته مستلزم یک پروتکل تبادلی است و یک عمل ساده نیست.

---

[1] Trusted recovery (FPT_RCV)

[2] Replay detection (FPT_RPL)

[3] State synchrony protocol (FPT_SSP)

در حالتی که عدم اعتماد به محیط توزیع وجود داشته باشد، به پروتکل همگام سازی پیچیده‌تری نیاز است.
پروتکل همگام‌سازی، الزاماتی را برای عملکردهای بحرانی مربوط به توابع امنیتی هدف ارزیابی ایجاد می‌کند تا از این پروتکل امن استفاده نمایند. پروتکل همگام‌سازی اطمینان می‌دهد که دو بخش توزیعی هدف ارزیابی (به طور مثال، میزبان‌ها) حالت‌هایشان را بعد از اقدامات مرتبط امنیتی همگام می‌نمایند.

- **خانواده مُهرهای زمانی[1]**

این خانواده، الزاماتی را برای یک مُهر زمانی معتبر در داخل هدف ارزیابی، آدرس دهی نموده است.

- **خانواده سازگاری داده‌های بین توابع امنیتی هدف ارزیابی[2]**

در یک محیط توزیعی، هدف ارزیابی ممکن است به تبادل داده توابع امنیتی هدف ارزیابی با دیگر محصولات امن IT نیاز داشته باشد. این خانواده الزاماتی برای به اشتراک گذاری و تفسیر سازگار صفات و مجوزها، بین توابع امنیتی هدف ارزیابی مربوط به هدف ارزیابی و یک محصول امن IT متفاوت را تعریف می‌نماید.

- **خانواده تست موجودیت‌های خارجی[3]**

این خانواده الزاماتی را برای توابع امنیتی هدف ارزیابی تعریف می‌نماید تا تست‌هایی را بر روی یک با بیش از یک موجودیت خارجی انجام دهد. عناصر مطرح شده در این خانواده برای اعمال به کاربران انسانی در نظر گرفته نشده‌اند.

موجودیت‌های خارجی، ممکن است شامل برنامه‌هایی باشد که بر روی هدف ارزیابی اجرا می‌گردند، سخت‌افزار و نرم‌افزاری که تحت هدف ارزیابی اجرا می‌گردند(پلتفرم‌ها، سیستم‌عامل و ...) یا برنامه‌ها و باکس‌های متصل شده به هدف ارزیابی (سیستم‌های تشخیص نفوذ، دیوارهای آتش، سرورهای ورود، سرورهای زمانی و غیره) باشد.

---

[1] Time stamps (FPT_STM)

[2] Inter-TSF TSF data consistency (FPT_TDC)

[3] Testing of external entities (FPT_TEE)

- **خانواده سازگاری در تکرار داده‌ها در توابع امنیتی هدف ارزیابی در داخل هدف ارزیابی[1]**

الزامات این خانواده از آن جهت لازم و ضروری می‌باشد، تا از سازگاری داده توابع امنیتی هدف ارزیابی زمانی‌که در داخل هدف ارزیابی تکرار می‌گردد، اطمینان حاصل نماید. منظور از سازگاری داده‌ها، یکسان بودن داده‌ها در محل‌ها و توابع مختلف است. داده توابع امنیتی هدف ارزیابی زمانی ناسازگار می‌شود که کانال داخلی بین بخش‌های مختلف هدف ارزیابی نامعتبر گردد. اگر اجزای هدف ارزیابی از نظر داخلی تشکیل یک شبکه بدهند، در صورت غیر فعال شدن ارتباطات شبکه‌ای، عدم سازگاری بین داده‌ها-ی تابع امنیتی می تواند رخ دهد.

- **خانواده خودآزمایی توابع امنیتی هدف ارزیابی[2]**

این خانواده الزاماتی را برای خودآزمایی توابع امنیتی هدف ارزیابی با توجه به عملکرد صحیح مورد انتظار تعریف می‌نماید. اجبار هدف ارزیابی به انجام تست بر روی بخش‌های حساس و مهم هدف ارزیابی با استفاده از نمونه عملیات‌های ریاضی مثالی از این الزام می‌باشد. این‌گونه تست‌ها می‌تواند در هنگام راه اندازی، به طور متناوب بنا به درخواست کاربر مجاز، یا در زمانی‌که شرایط خاصی ایجاد شود، انجام گیرد. عملی که باید به عنوان نتیجه خودآزمایی توسط هدف ارزیابی انجام شود در دیگر خانواده‌ها تعریف می‌گردد.

الزامات این خانواده هم‌چنین برای تشخیص عدم صحت داده توابع امنیتی هدف ارزیابی یا خود توابع امنیتی هدف ارزیابی (کُد اجرایی یا مولفه‌های سخت‌افزاری توابع امنیتی هدف ارزیابی) توسط خرابی‌های مختلفی که لزوماً عملکرد هدف ارزیابی (که توسط دیگر خانواده‌ها اداره شده‌اند) را متوقف نمی‌کنند، مورد نیاز است.
چنین خرابی‌هایی می‌توانند یا به دلیل حالت‌های پیش‌بینی نشده خرابی یا سهل‌انگاری‌های مرتبط در طراحی سخت‌افزار، میان‌افزار یا نرم افزار رخ دهند یا به دلیل تغییر مخرب توابع امنیتی هدف ارزیابی بر اثر حفاظت منطقی و/یا فیزیکی ناکافی صورت گیرند.

[1] Internal TOE TSF data replication consistency (FPT_TRC)

[2] TSF self test (FPT_TST)

شماره	نام خانواده	عنصر امنیتی
الزام		
۲۳	محرمانگی داده‌های ارسال شده بین توابع امنیتی هدف ارزیابی **(FPT_ITA)**	**نام عنصر: محرمانگی داده‌های ارسال شده بین توابع امنیتی هدف ارزیابی ۱** **شماره مولفه: ح‌ت-م‌د.۱،۱(FPT_ITA.1.1)** **شرح مولفه:** توابع امنیتی هدف ارزیابی باید از کلیه داده‌های انتقال یافته از خود به دیگر محصولات معتبرِ IT راه دور، در مقابل آشکارسازی و افشای غیرمجاز، در طول فرآیند انتقال، محافظت نمایند.
۲۴	یکپارچگی داده‌های ارسال شده توابع امنیتی هدف ارزیابی **(FPT_ITI)**	**نام عنصر: یکپارچگی داده‌های ارسال شده توابع امنیتی هدف ارزیابی ۱** **شماره مولفه: ح‌ت-ی‌د.۱،۱(FPT_ITI.1.1)** **شرح مولفه:** توابع امنیتی هدف ارزیابی باید بر اساس [اختصاص: **معیار تغییر تعریف شده**]، در هنگام نقل و انتقال داده‌ها بین خود و محصولات معتبر IT راه دور، قادر به شناسایی تغییرات در تمام داده‌ها باشند.
۲۵		**نام عنصر: یکپارچگی داده‌های ارسال شده توابع امنیتی هدف ارزیابی ۱** **شماره مولفه: ح‌ت-ی‌د.۲،۱(FPT_ITI.1.2)**

شماره	نام خانواده	عنصر امنیتی
	الزام	

شرح مولفه:

توابع امنیتی هدف ارزیابی باید توانایی بررسی یکپارچگی تمام داده‌های توابع امنیتی هدف ارزیابی که در حال انتقال بین توابع خود و محصولات معتبر IT راه دور، می‌باشند را فراهم نموده و در صورت تشخیص تغییرات، [اختصاص: **اقدامات مشخصی**] را انجام بدهند.

۲۶	مُهرهای زمانی (FPT_ITI)	**نام عنصر: مُهرهای زمانی ۱**

شماره مولفه: ح‌ت-م‌ز.۱,۱(FPT_STM.1.1)

شرح مولفه:

توابع امنیتی هدف ارزیابی، باید قادر به ایجاد مُهرهای زمانی قابل اطمینان برای استفاده **هدف ارزیابی** باشند.

۷,۵کلاس تشخیص نفوذ

شماره	نام خانواده	عنصر امنیتی
الزام		
۲۷	مجموعه داده‌های سیستم (IDS_SDC.1.1)	**نام عنصر: مجموعه داده‌های سیستم ۱** **شماره مولفه: ت‌ن-دس-(ت‌س).۱,۱ (IDS_SDC.1.1)**

شرح مولفه:

سیستم باید قادر باشد که اطلاعات زیر را از منابع سیستم فناوری اطلاعات مورد نظر، جمع‌آوری کند:

۱. [انتخاب: *راه‌اندازی و خاموش کردن سیستم، رویدادهای شناسایی و احراز هویت، دسترسی به داده‌ها، درخواست سرویس، ترافیک شبکه، تغییرات پیکربندی امنیت، شناسایی کد مخرب، تنظیمات کنترل دسترسی، پیکربندی سرویس، پیکربندی احراز هویت، پیکربندی خط‌مشی‌های قابل حسابرسی ، شناسایی آسیب‌پذیری‌های شناخته شده*] و

۲. [اختصاص: **سایر رویدادهای شناسایی‌شده خاص**].

نکته کاربردی:

با توجه به نیاز هدف ارزیابی به جمع‌آوری اطلاعات (دست کم یکی از موارد مطرح شده در قسمت «انتخاب») باید انتخاب گردد،

شماره نام خانواده

الزام

عنصر امنیتی

این الزام نشان می‌دهد که سیستم باید حداقل دارای یک حسگر یا اسکنر باشد. یک حسگر به طور کلی اطلاعات مربوط به رویدادهای مطرح شده زیر را جمع‌آوری می‌نماید:

راه‌اندازی و خاموش کردن سیستم، رویدادهای شناسایی و احراز هویت، دسترسی به داده‌ها، درخواست سرویس، ترافیک شبکه، تغییرات پیکربندی امنیت.

اسکنر نیز به طور کلی، اطلاعات پیکربندی ایستا را جمع‌آوری می‌کند که شامل رویدادهای زیر در قسمت اول الزام بالا می‌باشد: شناسایی کد مخرب، تنظیمات کنترل دسترسی، پیکربندی سرویس، پیکربندی احراز هویت، پیکربندی خط‌مشی‌های قابل حسابرسی، شناسایی آسیب‌پذیری‌های شناخته شده.

- **کد مخرب** شامل ویروس‌ها، کرم‌ها، اسب‌های تروجان ساده و غیره می‌باشد.
- **تنظیمات کنترل دستیابی** شامل لیست کنترل دستیابی، جستجوی فایل‌ها و دایرکتوری‌های دارای مجوز نوشتن و غیره می‌باشد.
- **پیکربندی سرویس** شامل، شناسایی سرویس‌های شبکه و/یا اختصاص پورت شبکه، سرویس‌های میزبان، نسخه سرویس‌ها، پروتکل‌های تصدیق شده توسط سرویس‌ها و غیره می‌باشد.

شماره نام خانواده

الزام

عنصر امنیتی

- **پیکربندی احراز هویت** شامل قفل شکنی[1]رمز عبور، تنظیمات پیکربندی (به عنوان مثال: حداقل طول رمز عبور و غیره)، توانایی احراز هویت قابل قبول (همانند NTLM، kerberos)، حساب میزبان تعریف شده، مجوز حساب و غیره می‌باشد.
- **پیکربندی خط‌مشی‌های قابل حسابرسی** شامل اندازه فضای در نظر گرفته شده برای ذخیره سازی اطلاعات ممیزی، در صورت فعال بودن ممیزی، در زمان پر شدن فضای در نظر گرفته شده چه عملی انجام شود و غیره.
- **آسیب‌پذیری‌های شناخته شده** که مبحث آن باز است و می تواند به طور مثال شامل نصب وصله‌های امنیتی، بررسی برای خطاهای پیکربندی پیش‌فرض و رایج باشد.

۲۸ **نام عنصر: مجموعه داده‌های سیستم ۱**

شماره مولفه: ت‌ن-دس-(ت‌س).۲,۱ (IDS_SDC.1.2)

شرح مولفه:

سیستم حداقل باید اطلاعات زیر را جمع‌آوری و ثبت کند:

[1] Cracking

شماره نام خانواده

الزام

عنصر امنیتی

- تاریخ و زمان رویداد، نوع رویداد، شناسه موجودیت فعال، و نتایج (موفقیت یا شکست) رویداد
- اطلاعات بیشتر در ستون سوم (جزئیات) جدول رویدادهای سیستم مشخص شده است.

جزئیات	رویداد	نام مولفه
هیچ	راه‌اندازی و خاموش کردن	ت‌ن-دس.۱
هویت کاربر، موقعیت، آدرس مبدا، آدرس مقصد	رویداد شناسایی و احراز هویت	ت‌ن-دس.۱
موجودیت[1] سیستم تشخیص نفوذ، دسترسی مورد تقاضا، آدرس مبدا، آدرس مقصد	دستیابی داده	ت‌ن-دس.۱
سرویس مشخص، آدرس مبدا، آدرس مقصد	درخواست سرویس	ت‌ن-دس.۱

[1] Object

شماره نام خانواده

الزام

عنصر امنیتی

پروتکل، آدرس مبدا، آدرس مقصد	ترافیک شبکه	ت‌ن-دس.۱
آدرس مبدا، آدرس مقصد	تغییر دادن تنظیمات امنیتی	ت‌ن-دس.۱
هیچ	راه‌اندازی و خاموش نمودن عملکرد حسابرسی	ت‌ن-دس.۱
موقعیت، شناسایی کُد	تشخیص کُد مخرب	ت‌ن-دس.۱
شناسایی سرویس(نام یا پورت)، واسطه، پروتکل‌ها	تنظیمات سرویس	ت‌ن-دس.۱
نام حساب برای قفل شکنی رمز عبور، پارامترهای مربوط به خط-مشی[1]حساب	تنظیمات احراز هویت	ت‌ن-دس.۱
پارامترهای تنظیمات خط‌مشی	تنظیمات خط‌مشی حسابرسی	ت‌ن-دس.۱

[1] Policy

شماره نام خانواده

الزام

عنصر امنیتی

حسابرسی		
شناسایی آسیب‌پذیری‌های شناخته شده	تشخیص آسیب‌پذیری‌های شناخته شده	ت‌ن-دس.۱

نکته کاربردی:

در مواردی که حسگر، رویدادهای مبتنی بر میزبان را جمع‌آوری می‌کند، برای رویدادهای شناسایی و احراز هویت، آدرس مبدا می‌تواند به صورت پیش‌فرض بر روی ماشین محلی و مقصد یک موجودیت سیستم تشخیص نفوذ تعریف گردد. برای رویدادهای دستیابی داده، آدرس مبدا می‌تواند نام فایل و آدرس مقصد می‌تواند موقعیت هدف برای آن فایل باشد.

۲۹ تجزیه و تحلیل تحلیل‌گر (IDS_ANL)

نام عنصر: تجزیه و تحلیل تحلیل‌گر ۱

شماره مولفه: ت‌ن-ت‌ا-(ت‌س).۱,۱ (IDS_ANL.1.1)

شرح مولفه:

شماره نام خانواده

الزام

عنصر امنیتی

سیستم باید توابع تجزیه و تحلیل زیر را بر روی تمام داده‌های دریافت‌شده سیستم تشخیص نفوذ، اجرا کند:

- [انتخاب: *تحلیل‌های آماری یا تطابق با امضا یا بررسی صحت*] و
- [اختصاص: **توابع تحلیلی دیگر]**

نکته کاربردی:

تحلیل‌های آماری، شامل شناسایی انحرافات از الگوی عملکرد طبیعی است. برای مثال، این تحلیل ممکن است شامل فرکانس‌های متوسط و اندازه‌گیری تغییرات جهت شناسایی استفاده‌های غیرطبیعی می‌باشد. تحلیل امضاء شامل، استفاده از الگوی متناظر با حملات شناخته شده یا سوء استفاده‌های یک سیستم است. برای مثال، الگوهایی از تنظیمات سیستم یا فعالیت کاربر می‌توانند با یک پایگاه داده از حملات شناخته شده، مقایسه گردند. تحلیل صحت شامل مقایسه تنظیمات سیستم یا فعالیت‌های کاربر در یک زمان با زمانی دیگر، جهت تشخیص دادن تفاوت‌ها است.

۳۰ **نام عنصر: تجزیه و تحلیل تحلیل‌گر ۱**

شماره مولفه: ت‌ن-ت‌ا-(ت‌س).۲,۱.۰ (IDS_ANL.1.2)

شرح مولفه:

شماره	نام خانواده	عنصر امنیتی
	الزام	

سیستم باید درون هر یک از نتایج تحلیلی حداقل اطلاعات زیر را ثبت نماید:

- زمان و تاریخ نتیجه، نوع نتیجه، شناسایی داده‌های منبع
- [اختصاص: **سایر اطلاعات مرتبط امنیتی درمورد نتیجه**]

نکته کاربردی:

نتایج تحلیلی بدست آمده توسط تحلیل‌گر، باید علاوه بر توصیف نتایج، تعیین نماید بر اساس چه اطلاعاتی به این نتایج رسیده است.

۳۱ واکنش تحلیل‌گر **(IDS_RCT)**

نام عنصر: واکنش تحلیل‌گر ۱

شماره مولفه: ت‌ن-وا-(ت‌س).۱,۱ (IDS_RCT.1.1)

شرح مولفه:

سیستم باید یک هشدار به [اختصاص: **مقصد هشدار**] ارسال نماید و [اختصاص: **اقدامات مناسب**] را در زمان تشخیص یک نفوذ، انجام دهد.

نکته کاربردی:

باید هشداری وجود داشته باشد که ماهیت آن و هدفش (به عنوان مثال کنسول سرپرستی و گزارش ممیزی) توسط نویسنده سند

شماره	نام خانواده الزام	عنصر امنیتی
		هدف امنیتی مشخص گردد. تحلیل‌گر ممکن است در زمان تشخیص نفوذ، اقدامات دیگری را به صورت اختیاری انجام دهد؛ این اقدامات باید در سند هدف امنیتی تعریف و مشخص گردد. هرگونه نفوذ در این الزام، به روی نتیجه‌گیری تحلیل‌گر در گذشته، حال و نفوذهای آینده و نفوذهای بالقوه، اثر می‌گذارد.
۳۲	بازبینی داده‌های محدود شده (IDS_RDR)	**نام عنصر: بازبینی داده‌های محدود شده ۱** **شماره مولفه: ت‌ن-ب‌د -(ت‌س).۱,۱ (IDS_RDR.1.1)** **شرح مولفه:** سیستم باید [اختصاص: **کاربرانی مجاز**] با قابلیت خواندن [اختصاص: **لیستی از داده‌های سیستم**] از داده‌های سیستم را فراهم نماید. **نکته کاربردی:** این الزام به کاربران مجاز سیستم اعمال می‌گردد. الزام برای نویسنده هدف امنیتی باز گذاشته شده است تا تعریف نماید که چه کاربران مجازی ممکن است به داده‌های سیستم دستیابی داشته باشند.
۳۳		**نام عنصر: بازبینی داده‌های محدود شده ۱**

شماره	نام خانواده	عنصر امنیتی
		الزام
		شماره مولفه: ت‌ن-ب‌د -(ت‌س).۲,۱.۲ (IDS_RDR.1.2)
		شرح مولفه:
		سیستم باید داده‌های خود را به شیوه‌ای مناسب فراهم نماید تا کاربر بتواند اطلاعات را تفسیر کند.
۳۴		**نام عنصر: بازبینی داده‌های محدود شده ۱**
		شماره مولفه: ت‌ن-ب‌د -(ت‌س).۳,۱.۳ (IDS_RDR.1.3)
		شرح مولفه:
		سیستم باید دسترسی خواندن داده‌های خود را برای تمام کاربران منع نماید، به جز آن دسته از کاربرانی که دسترسی خواندن به طور صریح و روشن، به آن‌ها اعطا شده است.
۳۵	تضمین در دسترس بودن داده‌های سیستم **(IDS_STG)**	**نام عنصر: تضمین در دسترس بودن داده‌های سیستم ۱**
		شماره مولفه: ت‌ن-ت‌د-(ت‌س).۱,۱.۱ (IDS_STG.1.1)
		شرح مولفه:
		سیستم باید از داده‌های ذخیره شده خود در برابر حذف غیر مجاز، محافظت نماید.

شماره الزام	نام خانواده عنصر امنیتی
۳۶	**نام عنصر: تضمین در دسترس بودن داده‌های سیستم ۱** **شماره مولفه: ت‌ن-ت‌د-(ت‌س).۲,۱.۱ (IDS_STG.1.2)** **شرح مولفه:** سیستم باید از داده‌های ذخیره شده خود در برابر دستکاری و تغییرات، محافظت نماید. **نکته کاربردی:** حذف مجاز داده، در این جا به عنوان تغییر در داده سیستم در نظر گرفته نمی‌شود. این الزام به محتوای حقیقی داده سیستمی که از هرگونه تغییر باید محافظت شود، اعمال می‌گردد.
۳۷	**نام عنصر: تضمین در دسترس بودن داده‌های سیستم ۱** **شماره مولفه: ت‌ن-ت‌د-(ت‌س).۳,۱.۱ (IDS_STG.1.3)** **شرح مولفه:** سیستم باید اطمینان یابد که بر اساس [اختصاص: **معیارهای ذخیره‌سازی داده‌های سیستم**]، از داده‌های خود در زمان [انتخاب: *پر شدن فضای ذخیره‌سازی داده سیستم، خرابی، حمله*] نگهداری می‌شود.

شماره	نام خانواده	عنصر امنیتی
	الزام	

نکته کاربردی:

لازم است هدف ارزیابی، میزان داده سیستمی که ممکن است تحت سناریوی معرفی شده، از بین رود را تعریف نماید.

۳۸ **نام عنصر: تضمین در دسترس بودن داده‌های سیستم ۲**

شماره مولفه: ت‌ن-ت‌د-(ت‌س).۱,۲ (IDS_STG.2.1)

شرح مولفه:

سیستم باید در صورتی که ظرفیت ذخیره‌سازی به حد پر شدن رسید [انتخاب: *اقدام به صرف نظر نمودن از داده‌های سیستم نماید، از ذخیره سازی داده‌های سیستم به جز داده‌هایی که توسط کاربر مجاز تعیین می‌کند جلوگیری نماید، یا اقدام به بازنویسی بر روی قدیمی‌ترین داده‌های ذخیره شده نماید*] و یک هشدار را ارسال نماید.

نکته کاربردی:

هدف ارزیابی باید تعریف نماید، سیستم در زمانی‌که ظرفیت ذخیره‌سازی به حد پر شدن رسید، چه اقداماتی انجام می‌دهد. هرچیزی که سبب متوقف شدن جمع‌آوری استاتیک اطلاعات گردد، راه‌حل خوبی نیست.

۸ الزامات تضمین امنیتی

جدول ۲- الزامات تضمین امنیتی

نام کلاس	نام کامپوننت	توضیحات
Development	ADV_FSP.2	مشخصات کارکرد ابتدایی
	ADV_ARC.1	معماری امنیتی
	ADV_TDS.1	طراحی اولیه
Guidance Documents	AGD_OPE.1	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی
Tests	ATE_IND.2	تست مستقل- منطبق
	ATE_FUN.1	تست کارکردی
	ATE_COV.1	پوشش
Vulnerability Assessment	AVA_VAN.2	آنالیز آسیب‌پذیری
Life cycle Support	ALC_CMC.2	استفاده از سیستم پیکربندی
	ALC_CMS.2	پوشش پیکربندی هدف ارزیابی
	ALC_DEL.1	رویه‌ها تحویل
	ALC_FLR.2	رویه‌های گزارش‌دهی نقص

۸,۱ کلاس توسعه

اطلاعات در رابطه با هدف‌های ارزیابی منطبق بر این پروفایل حفاظتی، در «مستندات راهنما» یا بخش «مشخصات امنیتی هدف ارزیابی[1] » سند هدف امنیتی لحاظ شده است و در اختیار کاربر نهایی قرار می‌گیرد. الزامی بر وجود بخش «مشخصات امنیتی هدف ارزیابی» در سند هدف امنیتی نمی‌باشد، اما در صورت وجود باید محتوای آن مرتبط با الزمات کارکردی و مورد تائید توسعه دهندگان هدف ارزیابی باشد.

فعالیت‌های تضمینی که در بخش «الزامات تضمین» آمده است باید به نویسندگان سند هدف امنیتی اطلاعات کافی بدهند تا آنها بتوانند برای بخش «مشخصات امنیتی هدف ارزیابی» محتوای مناسبی را در نظر بگیرند.

در زمینه درک و فهم واسط‌ها به هدف ارزیابی، مهم در نظر گرفتن تهدیدهایی است که با محرمانگی و صحت داده‌های کاربری که در میان شبکه منتقل می‌گردند یا داده‌های احراز هویتی که ممکن است پیمایش کننده اتصال باشند، مقابله می‌نمایند (از طریق اتصالات همتا به همتا هدف ارزیابی یا اتصال هدف ارزیابی به VPN Gateway). همچنین هدف ارزیابی با توجه به پیکربندی‌اش، ممکن است حفاظت از دسترسی غیرمجاز به شبکه پشت هدف ارزیابی را پیشنهاد نماید. علاوه بر واسط‌های شبکه لازم است که واسط‌های سرپرستی (چگونه هدف ارزیابی پیکربندی می‌شود) شرح داده شوند.

۸,۱,۱ معماری امنیتی

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱	معماری امنیتی	**نام عنصر: توصیف معماری امنیتی ۱**

[1] TOE Security Specification

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
	(ADV_ARC)	**شماره مولفه: (ADV_ARC.1.1D)** **شرح مولفه:** توسعه دهنده باید هدف ارزیابی را طوری پیاده‌سازی و طراحی نماید که نتوان ویژگی‌های امنیتی توابع امنیتی هدف ارزیابی را دور زد.
۲		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مولفه: (ADV_ARC.1.2D)** **شرح مولفه:** توسعه دهنده باید طوری توابع امنیتی هدف ارزیابی را طراحی و پیاده‌سازی نماید تا بتواند از خود در برابر مداخله توسط موجودیت‌های فعال ناامن، محافظت نماید.
۳		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مولفه: (ADV_ARC.1.3D)**

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مولفه: توسعه دهنده باید توصیفی از معماری امنیتی توابع امنیتی هدف ارزیابی را ارائه نماید.

مولفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۴	معماری امنیتی **(ADV_ARC)**	**نام عنصر: توصیف معماری امنیتی ۱** **شماره مولفه: (ADV_ARC.1.1C)** **شرح مولفه:** سطح جزئیات سند معماری امنیتی باید متناسب با توصیف واسط اجرا کننده کارکرد امنیتی باشد که در سند طراحی هدف ارزیابی ذکر شده است.
۵		**نام عنصر: مشخصات کارکرد ابتدایی۱**

مولفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شماره مولفه: (ADV_ARC.1.2C) **شرح مولفه:** سند معماری امنیتی باید دامنه امنیتی نگهداری شده توسط توابع امنیتی هدف ارزیابی سازگار با الزامات کارکرد امنیتی را توصیف نماید.
۶		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مولفه: (ADV_ARC.1.3C)** **شرح مولفه:** سند معماری امنیتی، باید چگونگی مقداردهی اولیه توابع امنیتی هدف ارزیابی را توصیف نماید.
۷		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مولفه: (ADV_ARC.1.4C)** **شرح مولفه:**

مولفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		سند معماری امنیتی باید نشان دهد که توابع امنیتی هدف ارزیابی از خود در برابر مداخله محافظت می‌نمایند.
۸		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مولفه: (ADV_ARC.1.5C)** **شرح مولفه:** سند معماری امنیتی باید نشان دهد، توابع امنیتی هدف ارزیابی از دور زدن عملکرد واسط اجرا کننده کارکرد امنیتی جلوگیری می‌نمایند.

مولفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۹	معماری امنیتی **(ADV_ARC)**	**نام عنصر: توصیف معماری امنیتی ۱** **شماره مولفه: (ADV_ARC.1.1E)**

مولفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مولفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده، تمام الزامات مولفه‌های محتوایی را برآورده می‌نماید.

۸,۱,۲ مشخصات کارکردی

مشخصات کارکردی، واسط‌های کارکرد امنیتی هدف ارزیابی را توصیف می‌نمایند اما نیازی به شرح مفصل و کاملی از این واسط‌ها نمی‌باشد. فعالیت‌های این خانواده باید بر روی درک پاسخ واسط‌های ارائه شده در دو بخش «مشخصات امنیتی هدف ارزیابی» و «مستندات راهنما» به الزامات کارکردی متمرکز گردند.

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۱۰	مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مولفه: (ADV_FSP.2.1D)**

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		شرح مولفه: توسعه دهنده باید مشخصات کارکردی را ارائه نماید.
۱۱		**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مولفه: (ADV_FSP.2.2D)** **شرح مولفه:** توسعه دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی را ارائه نماید.

مولفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱۲	مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مولفه: (ADV_FSP.2.1C)**

مولفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مولفه: مشخصات کارکردی باید توابع امنیتی هدف ارزیابی را به طور کامل نمایش دهند.
۱۳		**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مولفه: (ADV_FSP.2.1C)** **شرح مولفه:** مشخصات کارکردی باید اهداف و روش‌های مورد استفاده برای تمام واسط‌های توابع امنیتی هدف ارزیابی را توصیف نمایند.
۱۴		**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مولفه: (ADV_FSP.2.3C)** **شرح مولفه:**

مولفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		مشخصات کارکردی باید تمام پارامترهای مربوط به هر واسط توابع امنیتی هدف ارزیابی را معرفی و توصیف نمایند.
۱۵		**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مولفه: (ADV_FSP.2.4C)** **شرح مولفه:** برای هر واسط اجرا کننده کارکرد امنیتی، مشخصات کارکردی باید اقدامات آن واسط را توصیف نمایند.
۱۶		**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مولفه: (ADV_FSP.2.5C)** **شرح مولفه:** برای واسط اجرا کننده کارکرد امنیتی، سند مشخصات کارکردی باید پیغام خطاهایی را توصیف نماید که مستقیماً از پردازش اقدامات اجراکننده کارکرد امنیتی ناشی شده‌اند.

مولفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱۷		**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مولفه: (ADV_FSP.2.6C)** **شرح مولفه:** ردیابی‌ها باید نشان دهنده مرتبط شدن الزامات کارکرد امنیتی به واسط‌ها در سند مشخصات کارکردی باشند.

مولفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱۸	مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مولفه: (ADV_FSP.2.1E)** **شرح مولفه:**

مولفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
		ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام الزامات مولفه‌های محتوایی را برآورده می‌نمایند.
۱۹		**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مولفه: (ADV_FSP.2.2E)** **شرح مولفه:** ارزیاب باید مشخص نماید که سند مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی می‌باشد.

۸,۱,۳ طراحی

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۲۰	مشخصات کارکردی **(ADV_TDS)**	**نام عنصر: طراحی اولیه ۱** **شماره مولفه: (ADV_TDS.1.1D)**

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مولفه: توسعه دهنده باید طراحی هدف ارزیابی را ارائه نماید.
۲۱		**نام عنصر: طراحی اولیه ۱** **شماره مولفه: (ADV_TDS.1.2D)** **شرح مولفه:** توسعه دهنده باید نگاشتی از واسطهای سند مشخصات کارکردی به پائین‌ترین سطح از اجزای طراحی هدف ارزیابی را ارائه نماید.

مولفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی

مولفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۲۲	مشخصات کارکردی **(ADV_TDS)**	**نام عنصر: طراحی اولیه ۱** **شماره مولفه: (ADV_TDS.1.1C)** **شرح مولفه:** طراحی باید ساختار هدف ارزیابی را به صورت زیرمجموعه‌ای توصیف نماید.
۲۳		**نام عنصر: طراحی اولیه ۱** **شماره مولفه: (ADV_TDS.1.2C)** **شرح مولفه:** سند طراحی باید تمام زیرمجموعه‌های توابع امنیتی هدف ارزیابی را معرفی نماید.
۲۴		**نام عنصر: طراحی اولیه ۱** **شماره مولفه: (ADV_TDS.1.3C)** **شرح مولفه:**

مولفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		سند طراحی باید رفتار هر زیرمجموعه پشتیبان کننده الزام کارکرد امنیتی و غیر مداخله کننده الزام کارکرد امنیتی را با جزئیات کافی شرح داده تا نشان دهد که زیرمجموعه اجراکننده کارکرد امنیتی نمی‌باشد.
۲۵		**نام عنصر: طراحی اولیه ۱** **شماره مولفه: (ADV_TDS.1.4C)** **شرح مولفه:** طراحی باید به طور خلاصه رفتار اجرا کننده کارکرد امنیتی از زیرمجموعه‌های اجراکننده کارکرد امنیتی را بیان نماید.
۲۶		**نام عنصر: طراحی اولیه ۱** **شماره مولفه: (ADV_TDS.1.5C)** **شرح مولفه:**

مولفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		طراحی باید شرحی از تعاملات بین زیرمجموعه‌های اجرا کننده کارکرد امنیتی و هم‌چنین بین این زیرمجموعه‌ها و دیگر زیرمجموعه‌ها را بیان دارد.
۲۷		**نام عنصر: طراحی اولیه ۱** **شماره مولفه: (ADV_TDS.1.6C)** **شرح مولفه:** نگاشت باید نشان دهد، تمام رفتاری که در سند طراحی توصیف شده است به واسطه‌های درخواست کننده آنها نگاشت شده‌اند.

مولفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۲۸	مشخصات کارکردی **(ADV_TDS)**	**نام عنصر: طراحی اولیه ۱**

مولفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
		شماره مولفه: (ADV_TDS.1.1E) **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه‌های محتوایی را برآورده می‌نماید.

۸,۲ کلاس راهنمای کاربر

مستندات راهنما همراه با سند هدف امنیتی برای استفاده کاربران ارائه خواهند شد. در این دسته از مستندات شرحی از مدل سرپرستی و نحوه بررسی محیط عملیاتی توسط سرپرست (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 است باید مستند راهنما ارائه گردد. این راهنما شامل:

- دستورالعمل نصب موفقیت آمیز هدف ارزیابی در محیط
- دستورالعمل مدیریت امنیت هدف ارزیابی به عنوان یک محصول یا به عنوان بخشی از یک محیط عملیاتی بزرگتر
- دستورالعمل‌هایی که ارائه دهنده قابلیت سرپرستی محافظت شده از طریق استفاده از قابلیت‌های هدف ارزیابی، محیط عملیاتی یا هر دو می‌باشد.

۸,۲,۱ راهنمای کاربردی

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۲۹	راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مولفه: (AGD_OPE.1.1D)** **شرح مولفه:** توسعه دهنده باید راهنمای کاربردی را ارائه نماید.

مولفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۳۰	راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مولفه: (AGD_OPE.1.1C)** **شرح مولفه:**

مولفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی که باید در یک محیط پردازشی امن کنترل شوند را توصیف نماید، همانند هشدارهای مناسب.
۳۱		**نام عنصر: راهنمای کاربردی ۱** **شماره مولفه: (AGD_OPE.1.2C)** **شرح مولفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسط‌های در دسترس ارائه شده توسط هدف ارزیابی به صورت امن استفاده می‌گردد.
۳۲		**نام عنصر: راهنمای کاربردی ۱** **شماره مولفه: (AGD_OPE.1.3C)** **شرح مولفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسط‌های دردسترس، به خصوص تمام

مولفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین نماید.
۳۳		**نام عنصر: راهنمای کاربردی ۱** **شماره مولفه: (AGD_OPE.1.4C)** **شرح مولفه:** 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 هدف ارزیابی.
۳۴		**نام عنصر: راهنمای کاربردی ۱** **شماره مولفه: (AGD_OPE.1.5C)** **شرح مولفه:** سند راهنمای کاربردی باید تمام مودهای عملیاتی هدف ارزیابی (مودهایی شامل شکست عملیات یا

مولفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		خطای عملیات)، آثار آنها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.
۳۵		**نام عنصر: راهنمای کاربردی ۱** **شماره مولفه: (AGD_OPE.1.6C)** **شرح مولفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی که توسط کاربر تبعیت می‌شوند را توصیف نمایند تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده، کاملاً اجرا گردند.
۳۶		**نام عنصر: راهنمای کاربردی ۱** **شماره مولفه: (AGD_OPE.1.7C)** **شرح مولفه:** سند راهنمای کاربردی باید واضح و قابل فهم باشد.

مولفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۳۷	راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مولفه: (AGD_OPE.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده در سند راهنمای کاربردی تمام مولفه‌های محتوایی را برآورده می‌نماید.

۸,۲,۲ راهنمای آماده‌سازی

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۳۸	راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مولفه: (AGD_PRE.1.1D)**

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مولفه: توسعه دهنده باید هدف ارزیابی را همراه با سند آماده‌سازی ارائه نماید.

مولفه‌های اقدامات محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۳۹	راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مولفه: (AGD_PRE.1.1C)** **شرح مولفه:** مستندات آماده‌سازی باید تمام مراحل لازم برای پذیرش امن هدف ارزیابی توسط مشتری را مطابق با رویه‌های تحویل توسعه دهنده، شرح دهند.
۴۰		**نام عنصر: راهنمای آماده‌سازی ۱**

مولفه‌های اقدامات محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شماره مولفه: (AGD_PRE.1.2C) **شرح مولفه:** مستندات آماده‌سازی باید تمام مراحل لازم برای نصب امن هدف ارزیابی و آماده‌سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکر شده در سند هدف امنیتی، شرح دهند.

مولفه‌های اقدامات ارزیاب		
۴۱	راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مولفه: (AGD_PRE.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه‌های محتوایی را برآورده می‌نماید.
۴۲		**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مولفه: (AGD_PRE.1.2E)**

مولفه‌های اقدامات ارزیاب		
		شرح مولفه: ارزیاب باید رویه‌های آماده‌سازی شرح داده شده در سند را بکار ببرد تا تائید نماید، هدف ارزیابی می-تواند به صورت امن برای عمل نمودن آماده شود.

۸,۳ کلاس تست

تست هدف ارزیابی برای بررسی کارکرد سیستم و جنبه‌هایی که از ضعف طراحی و پیاده‌سازی سود می‌برند، در نظر گرفته می‌شود. تست کارکردی سیستم از طریق خانواده ATE_IND و تست جنبه‌هایی که از ضعف طراحی و پیاده‌سازی سود می‌برند از طریق خانواده AVA_VAN صورت می‌گیرد. در این سطح از ارزیابی (سطح EAL1) تست براساس کارکردی که برای هدف ارزیابی در نظر گرفته شده و واسطهایی که بر اساس اطلاعات طراحی در اختیار قرار می‌گیرند، انجام می‌گردد. یکی از خروجی‌های اولیه روال ارزیابی گزارش تست می‌باشد که در الزامات زیر مشخص شده است.

۸,۳,۱ تست پوشش

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۴۳	تست پوشش **(ATE_COV)**	**نام عنصر: تست پوشش ۱** **شماره مولفه: (ATE_COV.1.1D)** **شرح مولفه:** توسعه دهنده باید مدارک تست پوشش را ارائه نماید.

مولفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۴۴	تست پوشش **(ATE_COV)**	**نام عنصر: تست پوشش ۱** **شماره مولفه: (ATE_COV.1.1C)** **شرح مولفه:** مدارک ارائه شده برای تست پوشش باید نشان‌دهنده ارتباط بین تست‌های سند تست و واسط‌های توابع

مولفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		امنیتی هدف ارزیابی در سند مشخصات کارکردی باشند.

مولفه‌های قدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۴۵	تست پوشش **(ATE_COV)**	**نام عنصر: تست پوشش ۱** **شماره مولفه: (ATE_COV.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه‌های محتوایی را برآورده می‌نماید.

۸,۳,۲ تست کارکردی

مولفه‌های اقدامات توسعه دهنده

شماره الزام	نام خانواده	عنصر امنیتی
۴۶	تست کارکردی **(ATE_FUN)**	**نام عنصر: تست کارکردی ۱** **شماره مولفه: (ATE_FUN.1.1D)** **شرح مولفه:** توسعه دهنده باید توابع امنیتی هدف ارزیابی را تست نماید و نتایج آن را مستند کند.
۴۷		**نام عنصر: تست کارکردی ۱** **شماره مولفه: (ATE_FUN.1.2D)** **شرح مولفه:** توسعه دهنده باید سند تست را ارائه نماید.

مولفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۴۸	تست کارکردی	**نام عنصر: تست کارکردی ۱**

مولفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
	(ATE_FUN)	**شماره مولفه: (ATE_FUN.1.1C)** **شرح مولفه:** سند تست باید شامل طرح تست، نتایج مورد انتظار تست و نتایج واقعی تست باشد.
۴۹		**نام عنصر: تست کارکردی ۱** **شماره مولفه: (ATE_FUN.1.2C)** **شرح مولفه:** طرح تست باید تست‌های صورت گرفته را معرفی و انجام هر تست را توصیف نماید. این سناریو همچنین باید شامل ترتیب وابستگی به نتایج دیگر تست‌ها باشد.
۵۰		**نام عنصر: تست کارکردی ۱** **شماره مولفه: (ATE_FUN.1.3C)** **شرح مولفه:**

مولفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		نتایج تست باید نشان دهنده خروجی مورد انتظار از موفقیت آمیز تست باشد.
۵۱		**نام عنصر: تست کارکردی ۱** **شماره مولفه: (ATE_FUN.1.4C)** **شرح مولفه:** نتایج واقعی تست باید با نتایج مورد انتظار تست سازگار باشند.

مولفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۵۲	تست کارکردی **(ATE_FUN)**	**نام عنصر: تست کارکردی ۱** **شماره مولفه: (ATE_FUN.1.1E)** **شرح مولفه:**

مولفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
		ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام الزامات مولفه‌های محتوایی را برآورده می‌نماید.

۸,۳,۳تست مستقل

این دسته از تست‌ها برای تائید عملکردی که در بخش «مشخصات امنیتی هدف ارزیابی» و مستندات سرپرستی ارائه شده است، صورت می‌گیرند. تمرکز تست‌ها بر روی برآورده شدن الزامات کارکردی مشخص شده در سند هدف امنیتی می‌باشد. فعالیت‌های تضمین حداقل تست‌های مربوط به این بخش‌ها را معرفی می‌نماید و ارزیاب گزارشی از طرح تست و نتایج آن آماده می‌نماید.

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۵۳	تست مستقل **(ATE_IND)**	**نام عنصر: تست مستقل ۲** **شماره مولفه: (ATE_IND.2.1D)** **شرح مولفه:**

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		توسعه دهنده باید برای تست نمودن، هدف ارزیابی را ارائه نماید.

مولفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۵۴	تست مستقل **(ATE_IND)**	**نام عنصر: تست مستقل 2** **شماره مولفه: (ATE_IND.2.1C)** **شرح مولفه:** هدف ارزیابی باید مناسبِ تست نمودن باشد.
۵۵		**نام عنصر: تست مستقل ۲** **شماره مولفه: (ATE_IND.2.2C)** **شرح مولفه:**

مولفه‌های اقدامات محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		توسعه دهنده باید معادل مجموعه منابعی که در تست کارکردی توسعه دهنده استفاده شده‌اند را برای ارزیاب فراهم نماید.

مولفه‌های اقدامات ارزیاب		
۵۶	تست مستقل **(ATE_IND)**	**نام عنصر: تست مستقل ۲** **شماره مولفه: (ATE_IND.2.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده، تمام الزامات مولفه‌های محتوایی را برآورده می‌نماید.
۵۷		**نام عنصر: تست مستقل ۲** **شماره مولفه: (ATE_IND.2.2E)** **شرح مولفه:** ارزیاب باید نمونه‌ای از تست‌ها در سند تست را اجرا نماید تا از نتایج تست توسعه دهنده، اطمینان

مولفه‌های اقدامات ارزیاب		
		حاصل کند.
۵۸		**نام عنصر: تست مستقل ۲** **شماره مولفه: (ATE_IND.2.3E)** **شرح مولفه:** ارزیاب باید زیرمجموعه‌ای از توابع امنیتی هدف ارزیابی را تست نماید تا اطمینان حاصل کند که توابع امنیتی هدف ارزیابی به صورت مشخص شده، عمل می‌نماید.

۸,۴ کلاس آسیب‌پذیری

برای آماده نمودن اولیه این پروفایل حفاظتی، انتظار می‌رود آزمایشگاه‌های ارزیابی با تحلیل هدف ارزیابی آن دسته از آسیب‌پذیری‌هایی که در این نوع محصولات یافت شده-اند را بیابند. در اغلب مواقع سوء استفاده از این آسیب‌پذیری‌ها (یافتن آسیب‌پذیری‌های در آزمایشگاه) نیاز به مهارت و تخصص مهاجمان دارد.

تا زمانی‌که ابزارهای نفوذ در تمام آزمایشگاه‌ها توزیع می‌شوند و در دسترس هستند، انتظار نمی‌رود که ارزیاب‌ها برای این دسته از آسیب‌پذیری‌ها هدف ارزیابی را مورد تست قرار دهند. آزمایشگاه‌ها انتظار دارند توضیحاتی پیرامون احتمال کلی این دسته از آسیب‌پذیری‌ها در مستنداتی که توسط فروشنده به کاربران ارائه می‌شود لحظ گردد. اینگونه اطلاعات در توسعه ابزارهای تست نفوذ و همچنین نسخه‌های بعدی پروفایل‌های حفاظتی مورد استفاده قرار خواهند گرفت.

مولفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۵۹	آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۲** **شماره مولفه: (AVA_VAN.2.1D)** **شرح مولفه:** توسعه دهنده باید برای تست نمودن، هدف ارزیابی را ارائه نماید.

مولفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۶۰	آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۲** **شماره مولفه: (AVA_VAN.2.1C)** **شرح مولفه:** هدف ارزیابی باید مناسبِ تست نمودن باشد.

مولفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۶۱	آسیب‌پذیری (AVA_VAN)	**نام عنصر: آسیب‌پذیری ۲** **شماره مولفه: (AVA_VAN.2.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده، تمام مولفه‌های محتوایی را برآورده می‌نماید.
۶۲		**نام عنصر: آسیب‌پذیری ۲** **شماره مولفه: (AVA_VAN.2.2E)** **شرح مولفه:** ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در هدف ارزیابی، در منابع عمومی جستجویی را انجام دهد.
۶۳		**نام عنصر: آسیب‌پذیری ۲**

مولفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
		شماره مولفه: (AVA_VAN.2.3E) **شرح مولفه:** ارزیاب باید آنالیز آسیب‌پذیری هدف ارزیابی را با استفاده از مستندات راهنما، سند مشخصات کارکردی، طراحی هدف ارزیابی و توصیف معماری امنیتی انجام دهد تا آسیب‌پذیری‌های بالقوه در هدف ارزیابی را معرفی نماید.
۶۴		**نام عنصر: آسیب‌پذیری ۲** **شماره مولفه: (AVA_VAN.2.4E)** **شرح مولفه:** ارزیاب باید براساس آسیب‌پذیری‌های بالقوه شناسایی شده، تست نفوذ را انجام دهد تا مقاومت هدف ارزیابی در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند را مشخص نماید.

۸,۵کلاس 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 بدان معنی نیست که سبک و سیاق توسعه دهنده، نقش کمرنگی در قابل اعتماد بودن محصول دارد، بلکه در این سطح اطمینان(EAL1) تنها به این اطلاعات نیاز است.

۸,۵,۱ قابلیت‌های پیکربندی

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

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۶۵	قابلیت‌های	**نام عنصر: استفاده از یک سیستم پیکربندی۲**

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
	پیکربندی **(ALC_CMC)**	**شماره مولفه: (ALC_CMC.2.1D)** **شرح مولفه:** توسعه دهنده باید هدف ارزیابی و مرجع هدف ارزیابی را ارائه نماید.
۶۶		**نام عنصر: استفاده از یک سیستم پیکربندی۲** **شماره مولفه: (ALC_CMC.2.2D)** **شرح مولفه:** توسعه دهنده باید سند پیکربندی را ارائه نماید.
۶۷		**نام عنصر: استفاده از یک سیستم پیکربندی۲** **شماره مولفه: (ALC_CMC.2.3D)** **شرح مولفه:** توسعه دهنده باید از یک سیستم پیکربندی استفاده نماید.

مولفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۶۸	قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: استفاده از یک سیستم پیکربندی۲** **شماره مولفه: (ALC_CMC.2.1C)** **شرح مولفه:** هدف ارزیابی باید با یک مرجع یکتا برچسب زده شود.
۶۹		**نام عنصر: استفاده از یک سیستم پیکربندی۲** **شماره مولفه: (ALC_CMC.2.2C)** **شرح مولفه:** مستندات پیکربندی باید روش مورد استفاده برای معرفی یکتای موارد پیکربندی را معرفی نماید.
۷۰		**نام عنصر: استفاده از یک سیستم پیکربندی۲** **شماره مولفه: (ALC_CMC.2.3C)** **شرح مولفه:**

مولفه‌های اقدامات محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		سیستم پیکربندی باید تمام موارد پیکربندی را به صورت یکتا معرفی نماید.

مولفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۷۱	قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: استفاده از یک سیستم پیکربندی۲** **شماره مولفه: (ALC_CMC.2.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه‌های محتوایی را برآورده می‌نماید.

۸,۵,۲ حوزه پیکربندی

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۷۲	حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی بخشی از هدف ارزیابی ۲** **شماره مولفه: (ALC_CMS.2.1D)** **شرح مولفه:** ارزیاب باید لیست پیکربندی هدف ارزیابی را ارائه نماید.

مولفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۷۳	حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی بخشی از هدف ارزیابی ۲** **شماره مولفه: (ALC_CMS.2.1C)** **شرح مولفه:** لیست پیکربندی باید شامل خود هدف ارزیابی، مدارک مورد نیاز توسط الزامات تضمین امنیتی و بخش-هایی که شامل هدف ارزیابی هستند، باشد.

مولفه‌های اقدامات محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۷۴		**نام عنصر: پوشش پیکربندی بخشی از هدف ارزیابی ۲** **شماره مولفه: (ALC_CMS.2.2C)** **شرح مولفه:** لیست پیکربندی باید موارد پیکربندی را به صورت یکتا معرفی نماید.
۷۵		**نام عنصر: پوشش پیکربندی بخشی از هدف ارزیابی ۲** **شماره مولفه: (ALC_CMS.2.3C)** **شرح مولفه:** برای هر یک از موارد پیکربندی مربوط به توابع امنیتی هدف ارزیابی، لیست پیکربندی باید توسعه دهنده آن را نشان دهد.

مولفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی

مولفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۷۶	حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی بخشی از هدف ارزیابی ۱** **شماره مولفه: (ALC_CMS.2.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه‌های محتوایی را برآورده می‌نماید.

۸,۵,۳تحویل

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۷۷	تحویل **(ALC_DEL)**	**نام عنصر: رویه تحویل ۱** **شماره مولفه: (ALC_DEL.1.1D)** **شرح مولفه:**

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		توسعه دهنده باید رویه تحویل هدف ارزیابی یا بخشی از آن را به مشتری، مستند نماید.
۷۸		**نام عنصر: رویه تحویل ۱** **شماره مولفه: (ALC_DEL.1.2D)** **شرح مولفه:** توسعه دهنده باید از رویه‌های تحویل استفاده نماید.

مولفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۷۹	تحویل **(ALC_DEL)**	**نام عنصر: رویه تحویل ۱** **شماره مولفه: (ALC_DEL.1.1C)** **شرح مولفه:** مستندات تحویل باید تمام رویه‌هایی که برای حفظ امنیت در زمان توزیع نسخه‌های هدف ارزیابی لازم

مولفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		و ضروری هستند را شرح دهد.

مولفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۸۰	تحویل **(ALC_DEL)**	**نام عنصر: رویه تحویل ۱** **شماره مولفه: (ALC_DEL.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه‌های محتوایی را برآورده می‌نماید.

۸,۵,۴ اصلاح نقص

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۸۱	اصلاح نقص **(ALC_FLR)**	**نام عنصر: رویه گزارش نقص ۲** **شماره مولفه: (ALC_FLR.2.1D)** **شرح مولفه:** توسعه دهنده باید رویه‌های اصلاح نقص که به توسعه دهنده هدف ارزیابی داده می‌شوند را مستند نماید.
۸۲		**نام عنصر: رویه گزارش نقص ۲** **شماره مولفه: (ALC_FLR.2.2D)** **شرح مولفه:** توسعه دهنده باید رویه‌ای برای پذیرش تمام گزارشات نقص امنیتی و اقدام نمودن بر روی آنها، هم-چنین درخواست تصحیح نقص را ایجاد نماید.
۸۳		**نام عنصر: رویه گزارش نقص ۲** **شماره مولفه: (ALC_FLR.2.3D)**

مولفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		شرح مولفه: توسعه دهنده باید راهنمای اصلاح نقص را به کاربران هدف ارزیابی ارائه نماید.

مولفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۸۴	اصلاح نقص **(ALC_FLR)**	**نام عنصر: رویه گزارش نقص ۲** **شماره مولفه: (ALC_FLR.2.1C)** **شرح مولفه:** مستندات رویه‌های اصلاح نقص باید رویه‌هایی را توصیف نمایند که در هر هدف ارزیابی منتشر شده برای پیگیری نقص‌های امنیتی گزارش شده، مورد استفاده قرار می‌گیرند.
۸۵		**نام عنصر: رویه گزارش نقص ۲** **شماره مولفه: (ALC_FLR.2.2C)**

مولفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مولفه: رویه‌های اصلاح نقص باید ملزم به توصیف ماهیت و اثر هر نقص امنیتی ارائه شده، هم‌چنین وضعیت اصلاحیه یافته ، برای آن نقص باشند.
۸۶		**نام عنصر: رویه گزارش نقص ۲** **شماره مولفه: (ALC_FLR.2.3C)** **شرح مولفه:** رویه‌های اصلاح نقص باید ملزم به معرفی اقدامات اصلاحی برای هر نقص امنیتی باشند.
۸۷		**نام عنصر: رویه گزارش نقص ۲** **شماره مولفه: (ALC_FLR.2.4C)** **شرح مولفه:** مستندات رویه‌های اصلاح نقص باید روش‌هایی را توصیف نمایند که به کاربران هدف ارزیابی، اطلاعات

مولفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		نقص، اصلاحیه‌ها و راهنمایی در رابطه با اقدامات اصلاحی را ارائه می‌دهند.
۸۸		**نام عنصر: رویه گزارش نقص ۲** **شماره مولفه: (ALC_FLR.2.5C)** **شرح مولفه:** رویه‌های اصلاح نقص باید امکانی را فراهم نمایند تا توسعه دهنده بتواند گزارشات و درخواست‌های مربوط به نقص‌های امنیتی مشکوک در هدف ارزیابی را از کاربران آن دریافت نماید.
۸۹		**نام عنصر: رویه گزارش نقص ۲** **شماره مولفه: (ALC_FLR.2.6C)** **شرح مولفه:** رویه پردازش نقص امنیتی گزارش شده، باید اطمینان دهد که هر نقص گزارش شده اصلاح می‌گردد و هم‌چنین رویه اصلاح به کاربر هدف ارزیابی داده می‌شود.

مولفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۹۰		**نام عنصر: رویه گزارش نقص ۲** **شماره مولفه: (ALC_FLR.2.7C)** **شرح مولفه:** رَویه پردازش نقص امنیتی گزارش شده، باید هرگونه اصلاح نقص امنیتی را از مطرح نمودن نقص جدید در هدف ارزیابی حفاظت نماید.
۹۱		**نام عنصر: رویه گزارش نقص ۲** **شماره مولفه: (ALC_FLR.2.8C)** **شرح مولفه:** راهنمای اصلاح نقص باید امکانی را فراهم نماید که کاربران هدف ارزیابی بتوانند هرگونه نقص امنیتی مشکوک در هدف ارزیابی را به توسعه دهنده گزارش دهند.

مولفه‌های اقدامات ارزیاب

شماره الزام	نام خانواده	عنصر امنیتی
۹۲	اصلاح نقص **(ALC_FLR)**	**نام عنصر: رویه گزارش نقص ۲** **شماره مولفه: (ALC_FLR.2.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه‌های محتوایی را برآورده می‌نماید.