به نام خدا

پروفایل حفاظتی آنتی‌ویروس

نسخه ۱,۶

اردیبهشت ماه ۹۳

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 آنتی‌ویروس می‌باشد تا تولیدکنندگان آنتی‌ویروس‌ها بتوانند بر مبنای این سند، کارکردهای امنیتی را در محصول خود لحاظ و همچنین سند هدف امنیتی آن را ارائه کنند.

در بخش اول، آنتی‌ویروس به‌صورت 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 می‌شود.

سپس در بخش «اهداف امنیتی» مواردی جهت مقابله با تهدیدها، اجرای خط مشی‌ها و بکاربردن فرضیات مطرح می‌شود.

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

- کلاس ممیزی امنیت
- کلاس پشتیبانی از رمزنگاری
- کلاس حفاظت از داده‌های کاربری
- کلاس شناسایی و احراز هویت
- کلاس مدیریت امنیت
- کلاس حفاظت از توابع امنیتی هدف ارزیابی

- کلاس دسترسی به هدف ارزیابی
- کلاس آنتی‌ویروس

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 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 را که در این سند برای برآورده کردن الزامات ارائه شده‌اند در محصول خود فراهم کنند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد کرد.

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 می‌کند.

- **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 می‌کند.

این بیانیه شامل موارد زیر است:

- «تهدیدهایی» که توسط هدف ارزیابی و محیط عملیاتی‌اش مقابله می‌شود.
- «خط‌مشی امنیت سازمانی» که توسط هدف ارزیابی و محیط عملیاتی‌اش اجرا می‌شود.
- «فرضیاتی» که برای محیط عملیاتی هدف ارزیابی تائید می‌شوند.

- **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 می‌شوند؛ 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 کردن 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 می‌شود تا در حاصل شدن اهداف ارزیابی، برای هدف ارزیابی کمک کنند.

- **الزام کارکرد امنیتی (SFR[2])**

بیان کننده‌ی 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 می‌شوند. 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 است. 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 است. سطوح تضمین از سطح ۱ تا سطح ۷ هستند، لازم به ذکر است که «سطح تضمین امنیتی» یک نوع «بسته» است.

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

آن بخش از هدف ارزیابی که برای اجرای صحیح «الزامات کارکرد امنیتی» باید به آن تکیه کرد، 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 کرد.

1 Evaluation Assurance Level

2 TOE Security Functions

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

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

- **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 می‌شوند. محتویات یک پیام الکترونیک نوعی داده کاربری است.

- **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 مؤلفه‌های قابل انتخاب، که الزامات ممکن است براساس آن‌ها باشد.

- **مؤلفه (Element)[۲]**

۱ در استاندارد ملی ISO 15408 منتشر شده توسط سازمان ملی استاندارد ایران، Component مؤلفه ترجمه شده است.

۲ در استاندارد ملی ISO 15408 منتشر شده توسط سازمان ملی استاندارد ایران، Element عنصر ترجمه شده است.

بیانی از نیاز امنیتی که غیر قابل تجزیه است.

- **اختصاص (Assignment)**

مشخص کردن پارامترهای معرفی شده در یک مؤلفه (از استاندارد معیار مشترک) یا الزام است.

- **انتخاب (Selection)**

انتخاب کردن یک یا بیش از یک آیتم در لیستی که در مؤلفه 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) است که شامل اطلاعات است و یا اطلاعات را دریافت می‌کند، 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 حمله‌کننده، 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 «خط‌مشی کارکرد امنیتی » اجرا شود.

- **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 می‌شود تحت مجموعه قوانینی در «الزامات کارکرد امنیتی» بیان می‌شود، این مجموعه قوانین «خط مشی کارکرد امنیتی» نامیده می‌شوند. «الزامات کارکرد امنیتی» ممکن است چندین خط‌مشی جهت معرفی قوانینی که هدف ارزیابی باید اجرا کند، 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 کند. تمام این خط‌مشی‌ها توسط «توابع امنیتی هدف ارزیابی» پیاده‌سازی می‌شوند.

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

1 Security Functionality Policy

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

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

«خط‌مشی جریان اطلاعات» سازوکارهایی 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 عملکرد امنیتی بوده که مبنایی برای ارزیابی الزامات عملکرد امنیتی موجود در پروفایل حفاظتی[2]یا هدف امنیتی[3]است.

این الزامات به توضیح رفتارهای امنیتی مورد نظر هدف ارزیابی[4]یا محیط فناوری اطلاعات پرداخته و هدف آن برآورده نمودن اهداف امنیتی که در پروفایل حفاظتی یا هدف امنیتی تعیین شده است، 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 [5]

---

[1] Common Criteria (CC)

[2] Protection Profile (PP)

[3] Security Target (ST)

[4] Target Of Evaluation (TOE)

[5] Security Functional Requirement (SFR)

بخش سوم: الزامات تضمین امنیتی [1]

۴ معرفی آنتی‌ویروس

۱,۴ نوع محصول

هدف ارزیابی در این سند برنامه آنتی‌ویروس همراه با قسمت مدیریتی آن است که بر روی یک ایستگاه کاری اجرا می‌شود(به طور مثال لپ‌تاپ‌ها و رایانه‌های شخصی)، قسمت مدیریتی اجرا شدن برنامه آنتی‌ویروس را کنترل و نظارت می‌کند. هدف ارزیابی در این پروفایل حفاظتی می‌تواند منحصراً نرم‌افزاری باشد.

به طور عام اصطلاح «ویروس» به مجموعه‌ای اشاره دارد که از آسیب‌پذیری‌های امنیتی موجود در محصول بهره‌جویی می‌کند (همانند کرم‌ها و اسب‌های تروجان).

عبارت «آنتی‌ویروس» اغلب به اقداماتی اشاره دارد که در قبال مجموعه‌ای که از آسیب‌های امنیتی بهره‌جویی می‌کنند به‌کار می‌رود و فقط شامل تعریف خاصی از ویروس نمی‌شود. اصطلاح ویروس در این‌جا به مجموعه کاملی از بهره‌جویی‌ها اشاره دارد.

برنامه آنتی‌ویروس، محتویات موجود بر روی ایستگاه کاری را جهت یافتن ویروس‌ها اسکن می‌کند. این محتویات ممکن است از طریق رسانه قابل حملی(همانند CD) یا از طریق ترافیک شبکه دریافتی به ایستگاه کاری اضافه شوند.

قابلیت‌های برنامه آنتی‌ویروس:

- اسکن کردن بلادرنگ (برای تشخیص ویروس‌هایی که وارد سیستم شده‌اند)
- اسکن درخواستی (برای اسکن کردن رسانه قابل حمل مفید است)

[1] Security Assurance Requrement (SAR)

- اسکن زمان‌بندی شده (سازوکار پشتیبان، در مواردی که ویروس به‌صورتی وارد سیستم شده است که از کشف شدن فرار کرده باشد)

ویروس ممکن است در فایل یا در حافظه وجود داشته باشد. جهت تشخیص ویروس‌های حافظه، ممکن است آنتی‌ویروس، ترافیک شبکه دریافتی یا فضای حافظه و یا هردو را اسکن کند. همچنین آنتی‌ویروس با اسکن کردن فایل نیز باید قادر به تشخیص ویروس‌های موجود در فایل‌های فشرده باشد.

آنتی‌ویروس با توجه به امضاء ویروس‌های شناخته‌شده، عمل اسکن کردن را انجام می‌دهد. امضاءهایی که الگوی شناخته‌شده‌ای دارند، نشان‌دهنده ویروس هستند.

جهت برخورد با ویروس‌های جدید، فروشندگان فایل امضاء را (که اغلب به‌صورت فایل DAT است) پیوسته به‌روزرسانی می‌کنند و در دسترس قرار می‌دهند. برنامه آنتی ویروس باید بتواند در صورت لزوم امضاهای به‌روز شده را دریافت کند و با استفاده از خلاصه پیام، صحت و یکپارچگی فایل امضای دریافت شده را در ایستگاه‌های کاری که آنتی‌ویروس بر روی آن اجرا می‌شود، بررسی کند.

زمانی‌که آنتی‌ویروس، ویروس موجود در فایل را تشخیص داد، یک اقدام پیکره‌بندی شده (یا لیست مرتب شده‌ای از اقدامات) جهت ایزوله و/یا حذف کردن ویروس‌ها انجام می‌شود. اقدامات ممکن هنگام تشخیص ویروس موارد زیر هستند:

- پاک کردن ویروس از فایل
- قرنطینه کردن فایل
- تغییر نام فایل

- حذف فایل
- هیچ اقدامی (اجازه داده شود تا ویروس در داخل فایل باقی بماند)

زمانی‌که ویروس موجود در حافظه تشخیص داده شد، از اجرا شدن ویروس جلوگیری می‌شود. سازوکارهای استفاده شده برای جلوگیری از اجرای ویروس، به نوع اسکنی که صورت گرفته است بستگی دارد.

سازوکارهای ممکن برای جلوگیری از اجرای ویروس عبارتند از:

- مسدود کردن ترافیک شبکه دریافتی که شامل ویروس است
- یا پایان دادن به فرآیندی که در حافظه‌اش ویروس وجود دارد.

پیام هشداردهنده‌ای بر روی صفحه نمایش ایستگاه کاری نشان داده می‌شود، این پیام به کاربر ایستگاه کاری در ارتباط با ویروس و اقدامات انجام شده اطلاعاتی می‌دهد. این هشدار تا زمانی که کاربر تأیید نکرده است (یا به نشست پایان نداده است) بر روی صفحه نمایش باقی می‌ماند.

اهداف ارزیابی مطابق این پروفایل حفاظتی، در محیط‌های سازمانی استفاده خواهند شد. برای پشتیبانی از این نوع استفاده، کنترل و نظارت لازم است. سرپرست مرکزی باید در حوزه اختیارات خودش قادر به پیکره‌بندی از راه دور روی اهداف ارزیابی نصب شده بر روی تمام ایستگاه‌های کاری که به شبکه متصل هستند باشد.

حداقل موارد پیکره‌بندی که تنها در اختیار سرپرست مرکزی است، عبارتند از:

- پیکربندی اقداماتی که در زمان تشخیص ویروس موجود در فایل انجام می‌گیرد.
- تکرار اسکن زمان‌بندی‌شده
- عمق اسکن (برای فایل‌های فشرده)
- انواع فایل‌هایی که جهت اسکن کردن در نظر گرفته شده‌اند و/یا مستثنی شده‌اند.

کپی تمام ممیزی‌های ایستگاه‌های کاری متصل به شبکه به سیستم مدیریت مرکزی ارسال می‌شود، جایی که سرپرست مرکزی کپی ممیزی‌ها را بازبینی می‌کند. بافرهای ممیزی بر روی ایستگاه کاری ایجاد می‌شوند تا وقفه‌های موقتی ایجاد شده در اتصال بین ایستگاه کاری و سیستم جمع‌آوری مرکزی را به شمار آورند.

پیغام هشداری که به سرپرست مرکزی (اگر نشست در زمانی‌که اطلاعات ممیزی توسط سیستم جمع‌آوری ممیزی دریافت می‌شود، فعال باشد) نمایش داده می‌شود، اطلاعاتی در رابطه با ویروس و اقدامات انجام شده در قبال ویروس می‌دهد. این پیغام هشدار روی صفحه نمایش باقی می‌ماند تا زمانی‌که توسط سرپرست مرکزی اعلام دریافت شود (یا نشست خاتمه یابد).

در صورت متصل نبودن ایستگاه‌های کاری به شبکه (ایستگاه کاری مستقل باشد)، فرض می‌شود سرپرست محلی ایستگاه کاری، مجوز سرپرست مرکزی را برای آن ایستگاه کاری دارد.

در صورتی‌که ایستگاه‌های کاری در یک شبکه باشند، سرپرست مرکزی می‌تواند به‌صورت الکترونیکی فایل‌های امضاء شده را به دیگر ایستگاه‌های کاری درون شبکه منتقل کند. اما در صورت مستقل بودن ایستگاه‌های کاری، فایل‌های امضاء به‌صورت فیزیکی منتقل می‌شوند.

انتظار می‌رود فایل امضاء همواره به‌روزرسانی شود، به‌روزرسانی فایل امضاء از سوی فروشنده برنامه آنتی‌ویروس صورت می‌گیرد و توزیع این به‌روزرسانی در چندین مرحله انجام می‌شود.

در اولین مرحله، به‌روزرسانی‌ها به‌صورت امن از فروشنده به سازمان[1] منتقل می‌شوند (به طور مثال، DISA)، پیش‌بینی می‌شود که سازوکارهای استفاده شده در این مرحله با توجه به نیاز سازمان متفاوت باشد که پرداختن به این مسئله خارج از حوزه این پروفایل حفاظتی است. سازمان‌ها ترغیب می‌شوند تا از سازوکارهای قوی جهت بررسی محتوا و مبدا به‌روزرسانی استفاده کنند. هنگامی‌که به‌روزرسانی فایل امضاء از فروشنده دریافت شد، انتظار می‌رود سازمان این به‌روزرسانی را قبل از آنکه در اختیار مرحله‌ی دوم قرار بگیرد، اعتبارسنجی کند.

در مرحله‌ی دوم، به‌روزرسانی در اختیار سیستم‌های مدیریت مرکزی پشتیبان برنامه آنتی‌ویروس قرار می‌گیرد. سازوکاری که برای این توزیع توسط سازمان تعریف شده است، خارج از حوزه این پروفایل حفاظتی است. از آنجایی‌که این توزیع در داخل سازمان رخ می‌دهد، لزوماً نیاز به سازوکار قوی همانند مرحله‌ی اول نیست.

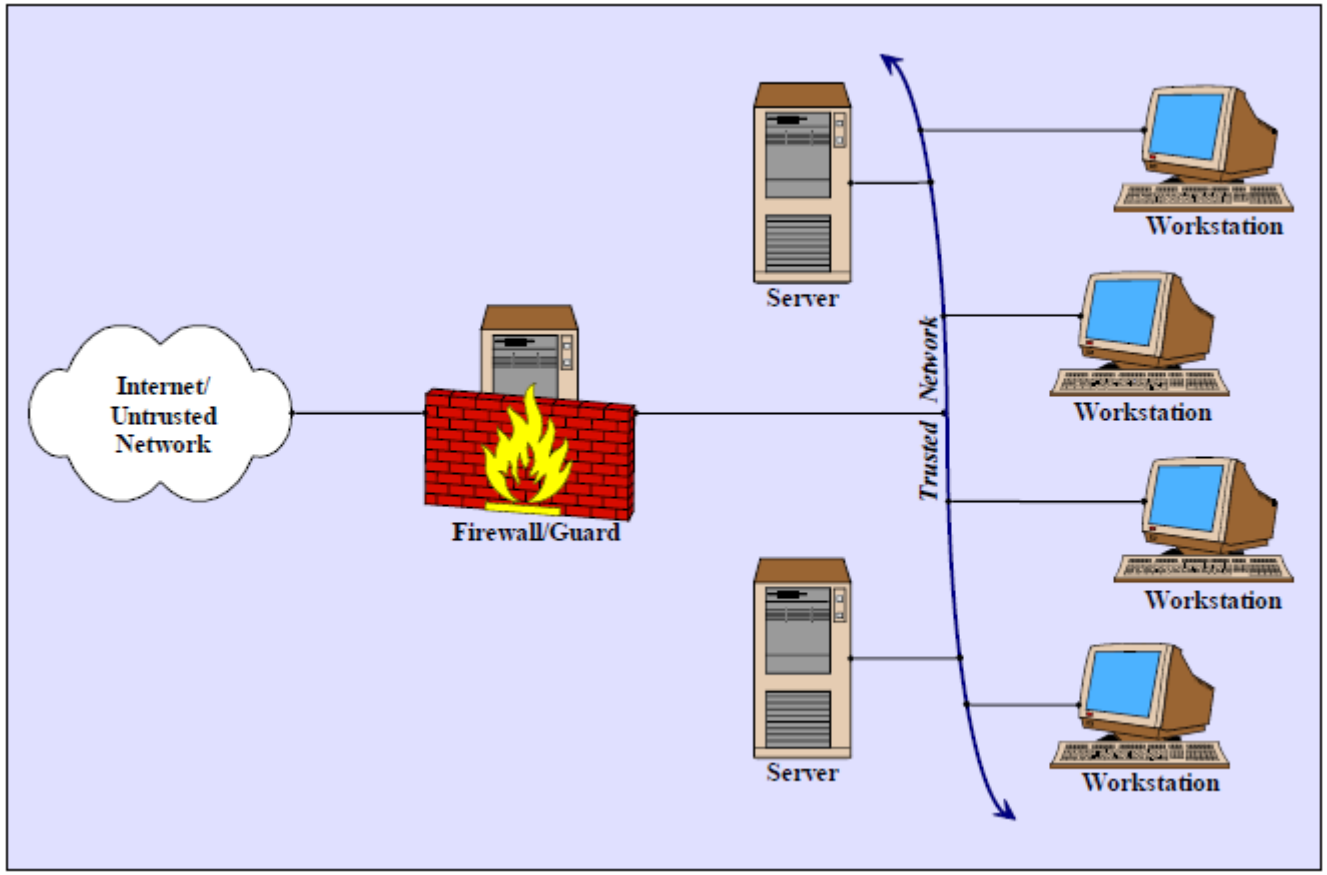
1 Enterprise

سومین مرحله در ارتباط با توزیع از سیستم مدیریت مرکزی به ایستگاه‌های کاری جداگانه است. فرض شده است که مسیر ارتباطی امنی بین قسمت‌های توزیع شده هدف ارزیابی وجود دارد. قدرت سازوکارهای استفاده شده برای مسیرهای ارتباطی امن توسط الزامات محیطی در هدف ارزیابی مورد استفاده، تعیین می‌شوند.

۲,۴ حدود هدف ارزیابی

در شکل ۱ هدف ارزیابی، بر روی ایستگاه‌های کاری شبکه‌ای که به‌صورت امن پیکربندی شده است، قرار دارند. دیوارآتش/گارد[1] در محدوده شبکه امن، نشان‌دهنده‌ی یک یا بیش از یک سامانه اجراکننده خدمات حفاظتی بر روی شبکه امن، می‌باشند. فرض براین است که پروتکل‌ها معمولاً جهت انتقال ویروس مورد استفاده قرار می‌گیرند، پروتکل‌هایی همانند SMTP، HTTP و FTP که این امر در عملکرد دیوارآتش/گارد در نظر گرفته شده است.

1 Firewall/guard



شکل ۱- محیط شبکه هدف ارزیابی

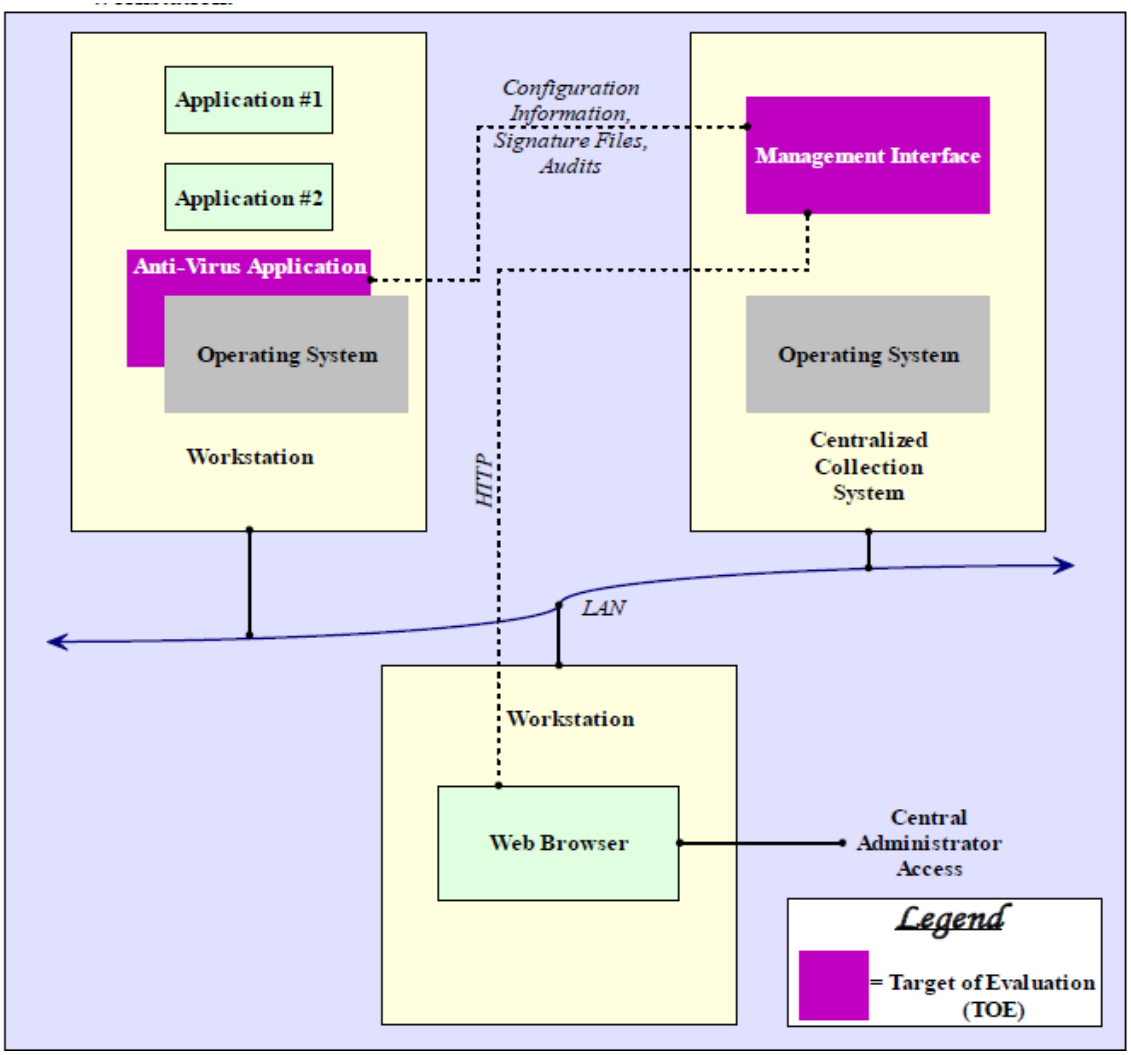
انتظار می‌رود که برنامه آنتی‌ویروس بتواند بر روی سرورها (ذخیره‌سازی‌های متصل به شبکه، سرورهای ایمیل، سرورهای وب) و ایستگاه‌های کاری در داخل شبکه امن اجرا شود. این پروفایل حفاظتی سرورها را پشتیبانی نمی‌کند و تنها بر روی ایستگاه‌های کاری متمرکز شده است. بنا به دلایلی که در ادامه مطرح شده، نیازی نیست که یک محصول از ایستگاه کاری و سرور باهم پشتیبانی کند:

- سرورها ممکن است از سیستم‌عامل‌های متفاوتی نسبت به ایستگاه کاری استفاده کنند.
- فروشندگان ممکن است برای ایستگاه کاری و سرورها محصولات متفاوتی ارائه کنند.
- سرورها معمولاً دارای کاربران محلی که مستقیماً به صفحه نمایش متصل ورود کنند، نیستند.

بر روی ایستگاه کاری که در شکل ۲ نشان داده شده است، برنامه آنتی‌ویروس بالاتر از سیستم عامل اجرا می‌شود تا بتواند عملیات زیر را انجام بدهد:

- اسکن کردن[1]
- اقدامات متقابل[2]
- ورود[1]

1 Scanning
2 Reaction


Application #1
Application #2
Anti-Virus Application
Operating System
Workstation
Configuration Information, Signature Files, Audits
HTTP
Management Interface
Operating System
Centralized Collection System
LAN
Workstation
Web Browser
Central Administrator Access
Legend
= Target of Evaluation (TOE)

1 logging

شکل ۲-حوزه هدف ارزیابی

واسط بین سیستم‌عامل، برنامه‌های کاربردی و برنامه آنتی‌ویروس، فروشنده آنتی‌ویروس و سیستم عامل خاص است، اما به‌طورکلی ممکن است شامل موارد زیر باشد:

- جداسازی فایل سامانه‌هایی که برای اسکن کردن فایل‌ها در زمانی‌که ایجاد می‌شوند، فراخوانی می‌شوند، تغییر می‌یابند و/یا باز می‌شوند.
- جداسازی ترافیک دریافتی شبکه جهت اسکن کردن حملات ویروس‌های موجود در حافظه
- دسترسی به برنامه پردازش حافظه جهت اسکن ویروس‌های موجود در حافظه
- جداسازی ترافیک خروجی شبکه تا منبع ترافیک SMTP ایستگاه کاری اعتبارسنجی شود.

۳,۴ خدمات امنیتی

الزامات عملکرد امنیتی می‌تواند به‌صورت زیر دسته‌بندی شوند:

- آنتی‌ویروس
- ممیزی
- عملیات رمزنگاری
- مدیریت
- حفاظت از هدف ارزیابی

۱,۳,۴ خدمات آنتی‌ویروس

خدمات آنتی‌ویروس در بخش‌های قبلی ۱,۴توصیف شده است.

۲,۳,۴ ممیزی

توصیف سطح بالایی از خدمات ممیزی در بخش ۱,۴ ارائه شده است. عملکرد ممیزی ملزم است زمانی‌که رویدادهای مرتبط امنیتی رخ می‌دهند، ممیزی‌هایی تولید کند و اطلاعات ممیزی را بر روی یک سیستم محلی ذخیره کند، اطلاعات ممیزی را به سیستم مدیریت مرکزی منتقل کند، هشدارهایی را برای رویدادهای طراحی شده تولید کند و همچنین ممیزی‌های تولید شده را بازبینی کند. حفاظت از داده ممیزی در دنباله ممیزی بر عهده‌ی هدف ارزیابی و سیستم‌عامل می‌باشد.

هدف ارزیابی اضافه شدن رویدادهای ممیزی در داخل گزارش ممیزی و همچنین حذف رویدادهای ممیزی از گزارش ممیزی را کنترل می‌کند. سیستم عامل نیز سرویس-های حفاظت از فایل ابتدایی را برای گزارش ممیزی فراهم می‌آورد.

۳,۳,۴ عملیات رمزنگاری

صحت فایل‌های امضاء توسط خلاصه پیام محاسبه شده برای فایل بررسی می‌شوند.

۴,۳,۴ مدیریت

خدمات مدیریت در بخش ۱,۴ و ۲,۴ توصیف شده‌اند.

۵,۳,۴ حفاظت از هدف ارزیابی

حفاظت از هدف ارزیابی لازم و ضروری است تا اطمینان حاصل شود که خدمات امنیتی هدف ارزیابی دور زده نمی‌شوند و یا تحریف نمی‌شوند. هدف ارزیابی و سیستم‌عامل همراه باهم ارائه دهنده این خدمات هستند.

بین بخش‌های جداگانه هدف ارزیابی، ارتباطات امنی توسط محیط IT ارائه شده است.

۴,۴ نقش‌ها

پروفایل حفاظتی تعریف کننده سه نقش زیر است:

۱,۴,۴ سرپرست مرکزی

سرپرست مرکزی عملکرد تمام نمونه‌های هدف ارزیابی تحت اختیارش را کنترل می‌کند. اختیارات این نقش عبارتند از:

- مدیریت عملکرد هدف ارزیابی بر روی ایستگاه کاری از راه دور
- اسکن زمان‌بندی شده‌ی فایل‌های موجود
- اسکن کردن دستی
- کنترل حداقل عمق اسکن
- به‌روزرسانی فایل امضاء ویروس

- دریافت پیام‌های هشدار از سیستم مدیریت مرکزی
- اعلام دریافت پیام هشدار از سیستم مدیریت مرکزی
- بازبینی اطلاعات ممیزی هدف ارزیابی در سیستم مدیریت مرکزی

۲,۴,۴ کاربر ایستگاه کاری

کاربری که از ایستگاه کاری استفاده می‌کند. این نقش دارای اختیارات زیر است:

- اسکن کردن دستی
- افزایش عمق اسکن در مورد اسکن‌هایی که به‌صورت دستی انجام می‌گیرد.
- دریافت پیام‌های هشدار برای رویدادهای ایستگاه کاری مورد استفاده
- بازبینی اطلاعات ممیزی هدف ارزیابی بر روی ایستگاه کاری مورد استفاده

۳,۴,۴ کاربر شبکه

کاربر یا فرآیند از راه دور که اطلاعات را به ایستگاه کاری از طریق پروتکل شبکه ارسال می‌کند. این نقش دارای اختیار زیر است:

- فرستادن اطلاعات به ایستگاه کاری

۵ تعریف مسائل امنیتی

در این بخش نیازهای امنیتی که توسط هدف ارزیابی پوشش داده شده است، در قالب سه بخش زیر تعریف می‌شوند:

- فرضیات
- تهدیدهای دارایی‌ها
- خط‌مشی‌های امنیت سازمانی[1]

در این بخش فرضیات به‌صورت A.assumption، تهدیدها به‌صورت T.threat و خط‌مشی‌ها به‌صورت P.policy معرفی شده‌اند.

۱,۵ تهدیدها

تهدیدهای توصیف شده در جدول زیر توسط هدف ارزیابی و محیط عملیاتی پوشش داده شده‌اند.

T.Type	توضیحات
T.ACCIDENTAL_ADMIN_ERROR	در صورت نصب و پیکربندی نامناسب هدف ارزیابی توسط سرپرست، ممکن است سازوکارهای امنیتی کارایی لازم را نداشته باشند.
T.AUDIT_COMPROMISE	یک کاربر یا فرآیند ممکن است به دنباله ممیزی[2] دستیابی غیرمجازی داشته باشد و سبب از دست رفتن یا تغییر یافتن رکورد ممیزی شود یا از ثبت رکوردهای ممیزی بعدی جلوگیری کند و بنابراین رویداد امنیتی مربوطه پنهان می‌شود.
T.MASQUERADE	یک کاربر یا فرآیند ممکن است به جای موجودیت دیگری خود را معرفی کند و به داده یا منابع هدف ارزیابی دستیابی غیرمجازی پیدا کند.
T.POOR_DESIGN	در طراحی هدف ارزیابی یا مشخصات آن ممکن است خطای غیرعمدی رخ دهد که منجر به نقصی شود که مورد سوءاستفاده کاربران یا

1 Organizational Security Policy

2 Audit trail

	برنامه‌های مخرب قرار گیرد.
T.POOR_IMPLIMENTATION	در پیاده‌سازی هدف ارزیابی ممکن است خطای غیرعمدی رخ دهد که منجر به نقصی شود که مورد سوءاستفاده کاربران یا برنامه‌های مخرب قرار گیرد.
T.POOR_TEST	عدم انجام آزمون یا آزمودن ناکافی که نشان می‌دهد عملکرد امنیتی هدف ارزیابی به درستی انجام می‌شود (پنهان ماندن مشکلات امنیتی از دید آزمون کننده) منجر به پنهان ماندن رفتار ناصحیح هدف ارزیابی می‌شود که سبب یک آسیب‌پذیری امنیتی بالقوه می‌شود.
T.RESIDUAL_DATA	یک کاربر یا فرآیند ممکن است با تخصیص مجدد حافظه‌ی استفاده شده توسط هدف ارزیابی به اسکن فایل‌ها یا فرآیندهای درخواست شده از سوی سرپرست، به‌صورت غیرمجاز به داده‌ها دسترسی پیدا کند.
T.TSF_COMPROMISE	یک کاربر یا فرآیند ممکن است باعث شود با استفاده از یک حمله ساده[1]، داده‌های توابع امنیتی هدف ارزیابی یا کدهای اجرایی به‌صورت نامناسبی در دسترس قرار گیرد(مشاهده شود، تغییر داده شود و حذف شود).
T.UNATTENDED_SESSION	یک کاربر ممکن است به نشستی که مراقبتی از آن صورت نمی‌گیرد، به‌صورت غیر مجاز دسترسی پیدا کند.
T.IDENTIFIED_ACTION	شکست سرپرست مجاز در شناسایی و اقدام بر روی فعالیت‌های غیرمجازی که ممکن است رخ دهد.
T.VIRUS	یک عامل مخرب ممکن است تلاش کند تا ویروسی را از طریق ترافیک شبکه یا رسانه قابل حمل[2] در ایستگاه کاری منتشر کند و داده های ایستگاه کاری را به خطر اندازد یا از آن ایستگاه کاری برای حمله به دیگر سیستم‌ها استفاده کند.

جدول ۱- تهدیدها

۲,۵ خط‌مشی‌ها

خط‌مشی‌های توصیف شده در جدول زیر توسط هدف ارزیابی و محیط عملیاتی پوشش داده شده‌اند.

1 Unsophisticate attack

2 Removable media

P.Type	توضیحات
P.ACCESS_BANNER	سیستم باید یک پرچم ابتدایی را به کاربران نشان دهد که بیان کننده محدودیت‌های استفاده، توافقات قانونی یا هر اطلاعات مناسب دیگری است که کاربران برای دستیابی به سیستم با آنها موافقت می‌کنند.
P.ACCOUNTABILITY	کاربران مجاز هدف ارزیابی باید پاسخگوی اقداماتشان در هدف ارزیابی باشند.
P.CRYPTOGRAPHY	تنها رمزنگاری معتبر NIST FIPS (متدها و پیاده‌سازی‌ها) برای مدیریت کلید (تولید کلید، دستیابی کلید، توزیع، از بین بردن و ذخیره کلید) و خدمات رمزنگاری (رمزنگاری، رمزگشایی، امضاء، درهم‌سازی، تبادل کلید، سرویس‌های تولید عدد تصادفی) قابل پذیرش است.
P.MANUAL_SCAN	کاربران مجاز ایستگاه‌های کاری باید پیش از آنکه هرگونه داده‌ای بر روی رسانه قابل حمل مورد دستیابی قرار گیرد، اسکن آنتی‌ویروس را به‌صورت دستی از رسانه قابل حمل (فلاپی، CD) معرفی شده به ایستگاه کاری شروع کنند.

جدول ۲: خط‌مشی‌ها

۳,۵ فرضیات

فرضیات توصیف شده در جدول زیر توسط محیط عملیاتی پوشش داده شده‌اند.

A.Type	توضیحات
A.AUDIT_BACKUP	سرپرستان از فایل‌های ممیزی نسخه پشتیبان تهیه و فضای دیسک مورد استفاده را بازبینی می‌کنند تا اطمینان حاصل کنند که اطلاعات ممیزی از دست نرفته است.
A.NO_EVIL	سرپرستان افراد متخاصمی نیستند و آموزش مناسب دیده‌اند و از تمام مستندات راهنمای مربوط به سرپرست پیروی می‌کنند.
A.PHYSICAL	فرض می‌شود که برای حفظ ارزش دارایی‌های فناوری اطلاعات که توسط هدف ارزیابی محافظت می‌شوند و همچنین حفظ ارزش اطلاعاتی که توسط هدف ارزیابی ذخیره، پردازش و منتقل می‌شود، امنیت فیزیکی در حوزه فناوری اطلاعات ارائه می‌شود.
A.SECURE_COMMS	فرض می‌شود که محیط فناوری اطلاعات یک خط ارتباطی امن بین بخش‌های توزیع یافته هدف ارزیابی و همچنین بین هدف ارزیابی و

	سرپرستان از راه دور ارائه خواهد داد.
A.SECURE_UPDATES	سرپرستان سازوکارهای امنی برای دریافت و تائید اعتبار فایل‌های امضاء به روز شده از فروشندگان و همچنین توزیع این فایل‌ها به سیستم‌های مدیریت مرکزی اجرا خواهند کرد.

جدول ۳: فرضیات

۶ اهداف امنیتی

در این بخش اهداف امنیتی برای هدف ارزیابی و محیط عملیاتی آن معرفی شده است. اهداف امنیتی مسئولیت هدف ارزیابی و محیط عملیاتی را در برابر نیازهای امنیتی عنوان کرده است. اهداف امنیتی برای هدف ارزیابی به‌صورت O.objective و برای محیط عملیاتی به‌صورت OE.objective نشان داده شده است.

۱,۶ اهداف امنیتی هدف ارزیابی

هدف ارزیابی باید اهداف زیر را برآورده کند.

O.Type	توضیحات
O.ADMIN_GUIDANCE	هدف ارزیابی به سرپرستان اطلاعات لازم جهت مدیریت امن را خواهد داد.
O.ADMIN_ROLE	هدف ارزیابی نقشی برای سرپرست مجاز در نظر خواهد گرفت تا اقدام‌های مربوط به سرپرست ایزوله شود.
O.AUDIT_GENERATION	هدف ارزیابی قابلیتی ارائه خواهد کرد تا رکوردهای امنیتی مربوط به رویدادها را شناسایی و ایجاد کنند.
O.AUDIT_PROTECT	هدف ارزیابی قابلیت حفاظت از اطلاعات ممیزی را ارائه خواهد کرد.
O.AUDIT_REVIEW	هدف ارزیابی قابلیت مشاهده انتخابی اطلاعات ممیزی را ارائه خواهد داد.
O.CONFIGURATION_IDENTIFICATION	پیکربندی هدف ارزیابی به طور کامل مشخص می‌شود به گونه‌ای که اجازه خواهد داد خطاهای پیاده‌سازی، شناخته شوند.
O.CORRECT_TSF_OPER	هدف ارزیابی قابلیت آزمودن عملکرد امنیتی را ارائه خواهد داد تا اطمینان دهند که عملکرد امنیتی از سوی کاربر به درستی عمل می-

ATION	کند.
O.CRYPTOGRAPHY	هدف ارزیابی باید از خدمات رمزنگاری معتبر NIST FIPS 140-2 استفاده کند.
O.DOCUMENTED_DESIGN	طراحی هدف ارزیابی باید به طور دقیق و کامل مستند شود.
O.MANAGE	هدف ارزیابی تمام امکانات و کارکردهای لازم، جهت پشتیبانی کردن از کاربران مجاز در مدیریت هدف ارزیابی ارائه خواهد کرد.
O.PARTIAL_FUNCTIONAL_TEST	هدف ارزیابی تحت برخی آزمون‌های کارکرد امنیتی قرار خواهد گرفت تا نشان داده شود که عملکرد امنیتی هدف ارزیابی برخی از الزامات کارکرد امنیتی‌اش را برآورده می‌کند.
O.PARTIAL_SELF_PROTECTION	عملکرد امنیتی هدف ارزیابی از یک دامنه[۱] برای اجرای خود استفاده می‌کند تا خود و منابعش را از تداخل خارجی، دست‌کاری[۲] یا افشای غیرمجاز از طریق واسطهایش حفظ کند.
O.VIRUS	هدف ارزیابی ویروس‌های شناخته شده‌ای را که از طریق ترافیک شبکه یا رسانه قابل حمل در شبکه منتشر شده‌اند، شناسایی و در قبال آن‌ها اقدامی صورت می‌دهد.
O.VULNARABILITY_ANALYSIS	هدف ارزیابی تحت برخی از آنالیزهای آسیب‌پذیری قرار می‌گیرد تا نشان دهد که طراحی و پیاده‌سازی هدف ارزیابی شامل هیچ نقص آشکاری نیست.

جدول ۴: اهداف امنیتی هدف ارزیابی

۲,۶ اهداف امنیتی محیط عملیاتی

محیط عملیاتی هدف ارزیابی باید اهداف زیر را برآورده کند.

OE.Type	توضیحات

[۱] Domain

[۲] Tampering

OE.AUDIT_BACKUP	از فایل‌های گزارش ممیزی نسخه پشتیبان گرفته می‌شود و می‌تواند بازیابی شود، فایل گزارش ممیزی خارج از فضای دیسک اجرا نخواهد شد.
OE.AUDIT_STORAGE	محیط فناوری اطلاعات امکانی را برای ذخیره امن فایل‌های گزارش ممیزی هدف ارزیابی ارائه خواهد کرد.
OE.DISPLAY_BANNER	محیط فناوری اطلاعات با توجه به استفاده‌ای که از سیستم می‌شود، پیغام هشداری را نمایش خواهد داد.
OE.DOMAIN_SEPERATION	محیط فناوری اطلاعات یک حوزه ایزوله شده برای اجرای هدف ارزیابی ارائه خواهد کرد.
OE.NO_BYPASS	محیط فناوری اطلاعات باید اطمینان بدهد که سازوکارهای امنیتی هدف ارزیابی جهت دستیابی به منابع هدف ارزیابی نمی‌تواند دور زده شوند.
OE.NO_EVIL	استفاده‌کنندگان هدف ارزیابی باید اطمینان دهند که سرپرستان مجاز، متخاصم نمی‌باشند، آموزش مناسب دیده‌اند و از تمام مستندات راهنمایی سرپرست پیروی می‌کنند.
OE.PHYSICAL	برای حفظ ارزش دارایی‌های فناوری اطلاعات که توسط هدف ارزیابی محافظت می‌شوند و همچنین حفظ ارزش اطلاعات ذخیره‌شده، پردازش‌شده و منتقل‌شده در داخل دامنه، امنیت فیزیکی ارائه خواهد شد.
OE.RESIDUAL_INFORMATION	محیط فناوری اطلاعات اطمینان خواهد داد در زمان تخصیص مجدد یک منبع، هیچ اطلاعاتی از منابع محافظت‌شده در حوزه کنترلی هدف ارزیابی آزاد نخواهد شد.
OE.SECURE_COMMS	محیط فناوری اطلاعات خط ارتباطی امنی را بین بخش‌های توزیع‌شده هدف ارزیابی و همچنین بین هدف ارزیابی و سرپرستان از راه دور[1] فراهم خواهد نمود.
OE.SECURE_UPDATES	شرکت‌های استفاده کننده از هدف ارزیابی باید مطمئن شوند که از طریق یک سازوکار امن به‌روزرسانی فایل‌های امضا، از فروشندگان دریافت خواهد شد و پیش از استفاده معتبر می‌شوند، همچنین این فایل‌های به روز شده از طریق یک سازوکار امن بین سامانه‌های مدیریت مرکزی توزیع می‌شوند.

1 Remote administrator

OE.TIME_STAMPS	محیط فناوری اطلاعات مهرهای زمانی قابل اطمینان[1] ارائه خواهد داد.
OE.TOE_ACCESS	محیط فناوری اطلاعات سازوکارهایی جهت کنترل دسترسی منطقی کاربر به هدف ارزیابی ارائه خواهد داد.

جدول ۵: اهداف امنیتی محیط عملیاتی

۷ الزامات کارکرد امنیتی

نام کلاس	نام خانواده	نام عنصر	
کلاس ممیزی امنیت	تولید داده ممیزی امنیت	ما–ت‌ل.۱	FAU_GEN.1
		ما–ت‌ل.۲	FAU_GEN.2
	بازبینی ممیزی امنیتی	ما–ب‌ز.۱	FAU_SAR.1
		ما–ب‌ز.۲	FAU_SAR.2
		ما–ب‌ز.۳	FAU_SAR.3
	ذخیره‌سازی رویدادهای ممیزی امنیتی	ما-ذخ.۱	FAU_STG.1
کلاس پشتیبانی از رمزنگاری	عملیات رمزنگاری	رز-ع‌ر.۱	FCS_COP.1
	تولید عدد تصادفی	رز-ب‌ت(ت‌س).۱	FCS_RBG_EXT.1
کلاس حفاظت از داده کاربری	حفاظت از اطلاعات باقیمانده	ح‌ف-اب.۱	FDP_RIP.1
	عملیات عقب‌گرد به‌منظور بازگرداندن حالت/حالت‌های	ح‌ف-ع‌گ.۱	FDP_ROL.1

1 Reliable

	قبل		
کلاس شناسایی و احراز هویت	مدیریت رمز عبور	اش-مع.۱	FIA_PMG_EXT.1
	شکست‌ها در احراز هویت	اش-ش‌ا.۱	FIA_AFL.1
	شناسایی احراز هویت	اش-ش‌ه.۱	FIA_UIA-EXT.1
	احراز هویت کاربر	اش-اه.۲	FIA_UAU.2
	شناسایی کاربر	اش-اه.۶	FIA_UID.6
		اش-اه.۲	FIA_UID.2
کلاس مدیریت امنیت	مدیریت توابع در توابع امنیتی هدف ارزیابی	مد-مت.۱	FMT_MOF.1
	نقش‌های امنیتی	مد-ن‌م.۱	FMT_SMR.1
	تعیین عملیات مدیریتی	مد-ع‌م.۱	FMT_SMF.1
کلاس توابع امنیتی هدف ارزیابی	انتقال داده‌های داخلی توابع امنیتی هدف ارزیابی	حت-اد.۱	FPT_ITT.1
	مهرهای زمانی	حت-مز.۱	FPT_STM.1
	محافظت از داده های توابع امنیتی هدف ارزیابی	حت-مح-(ت س).۱	FPT_SKP_EXT.1
	حفاظت از کلمه عبور سرپرست	حت-مپ-(ت س).۱	FPT_APW_EXT.1
	به‌روزرسانی امن	حت-رم-(ت س).۱	FPT_TUD_EXT.1
	یکپارچگی داده‌های ارسال شده	حت-ی‌د.۱	FPT_ITI.1

	توابع امنیتی هدف ارزیابی		
کلاس دسترسی به هدف ارزیابی	قفل‌گذاری بر روی نشست‌ها و پایان دادن به آنها	دس-ق‌ن-(ت-س).۱	FTA_SSL.(EXT).1
	علائم دسترسی هدف ارزیابی	دس-ع‌د.۱	FTA_TAB.1
کلاس آنتی‌ویروس	عملیات آنتی‌ویروس	آو-ع‌ا-(ت‌س).۱	FAV_ACT_(EXT).1
	هشدارهای آنتی‌ویروس	آو-ه‌ا-(ت‌س).۱	FAV_ALR_(EXT).1
	انجام اسکن توسط آنتی‌ویروس	آو-اس-(ت‌س).۱	FAV_SCN_(EXT).1

جدول ۶: الزامات کارکرد امنیتی آنتی‌ویروس

۱,۷ کلاس ممیزی امنیت

در ادامه مؤلفه‌های امنیتی مورد نیاز کلاس ممیزی امنیت ارائه شده است.

نام کلاس: ممیزی امنیت

شرح کلاس: آنتی‌ویروس‌ها برای رخدادهای گوناگون اقدام به ایجاد گزارشهایی برای ممیزی می‌کنند. کلاس ممیزی امنیت، الزاماتی پیرامون نحوه شناخت، ثبت و ذخیره و آنالیز اطلاعات ممیزی مربوط به فعالیت‌های امنیتی تعریف کرده است (فعالیت‌هایی که توسط توابع امنیتی هدف ارزیابی کنترل می‌شوند). 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 پاسخ خودکار ممیزی امنیتی[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 را برای ثبت رخدادهای امنیتی مربوط به رویدادهایی که تحت کنترل توابع امنیتی هدف ارزیابی صورت می‌گیرند تعریف می‌کند. این خانواده سطح ممیزی را تعیین می‌کند، انواع رویدادهایی را که باید توسط توابع امنیتی هدف ارزیابی قابل ممیزی باشند بیان می‌کند و یک مجموعه حداقلی از اطلاعات مرتبط با ممیزی را تعیین می‌کند که باید در داخل انواع ممیزی‌های امنیتی ثبت شده، ارائه شوند.

- **خانواده تحلیل ممیزی امنیت[3]**

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

- **خانواده بازبینی ممیزی امنیت[4]**

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

---

1 Security audit automatic response (FAU_ARP)

2 Security audit data generation (FAU_GEN)

3 Security audit analysis (FAU_SAA)

4 Security audit review (FAU_SAR)

- **خانواده انتخاب رویداد ممیزی امنیت[1]**

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

- **خانواده ذخیره‌سازی رویداد ممیزی امنیت[2]**

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

شماره الزام	نام خانواده	عنصر امنیتی
۱	تولید داده ممیزی امنیت **(FAU_GEN)**	**نام عنصر: تولید داده ممیزی امنیت ۱** **شماره مؤلفه: م‌ا – ت‌ل.۱٫۱(FAU_GEN.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید بتوانند از رویدادهای قابل ممیزی زیر یک رکورد ممیزی تولید کنند: الف- آغاز و پایان عملیات ممیزی ب- کلیه رویدادهای قابل ممیزی برای کمترین سطح ممیزی

1 Security audit event selection (FAU_SEL)

2 Security audit event storage (FAU_STG)

شماره الزام نام خانواده **عنصر امنیتی**

پ- رویدادهایی که در جدول زیر تعریف شده‌اند.

مولفه	رویداد	جزئیات
FAU_GEN.1	هرگونه دسترسی به آنتی ویروس و داده‌های آن	-
FAU_SAR.1	خواندن اطلاعات از رکوردهای ممیزی	-
FAU_SAR.2	تلاش ناموفق جهت خواندن اطلاعات از رکوردهای ممیزی	-
FAU_STG.NIAP_0414	انتخاب عمل	عمل انتخاب شده
FAV_ACT_(EXT)	عمل رخ داده در پاسخ به تشخیص ویروس	تشخیص دادن ویروس صورت گرفتن اقدام لازم در برابر ویروس مشخص نمودن فایل یا فرایندی که ویروس در آن تشخیص داده شده
FCS_COP.1	شکست در عملیات رمزنگاری	-
FCS_RBG_EXT.1	شکست در تولید بیت تصادفی	-
FIA_AFL.1	احرازهویت‌های ناموفق	-

شماره الزام نام خانواده **عنصر امنیتی**

FIA_UAU.2	تمام احراز هویت‌هایی که رخ می-دهد.	شناسه کاربری، موقعیت آن (به عنوان مثال آدرس IP)
FIA_UID.6	تمام شناسایی‌هایی که رخ می‌دهند.	شناسه کاربری، موقعیت آن (به عنوان مثال آدرس IP)
FIA_UID.2	تمام شناسایی‌هایی که رخ می‌دهند.	شناسه کاربری، موقعیت آن (به عنوان مثال آدرس IP)
FMT_MOF.1	هرگونه تغییر در کارکرد توابع امنیتی هدف ارزیابی	-
FMT_MTD.1	تمام تغییرات اعمال شده به مقادیر داده‌های توابع امنیتی هدف ارزیابی	-
FMT_SMF.1	هرگونه عملکرد مدیریتی: پیکربندی عملکرد، بروزرسانی امضاءهای اسکن، پاسخ‌دهی به هشدارها	-
FPT_STM.1	تغییرات زمانی	مقادیر جدید و قدیمی زمان مبدا تلاش (به عنوان مثال آدرس IP)
FPT_TUD_EXT.1	بروزرسانی نمودن	-
FTA_SSL.(EXT).1	هرگونه تلاشی که سعی می‌نماید نشست غیرفعال، قفل نشود.	-

عنصر امنیتی		
FAV_ACT_(EXT).1	پاک نمودن ویروس از فایل قرنطینه نمودن فایل حذف نمودن فایل	-
FAV_SCN_(EXT).1	انجام اسکن	-

شماره الزام نام خانواده

۲

نام عنصر: تولید داده ممیزی امنیت ۱

شماره مؤلفه: ما–ت‌ل.۲,۱(FAU_GEN.1.2)

شرح مؤلفه:

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

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 بالا مشخص شده است.

۳

نام عنصر: وابستگی هویت کاربر

شماره مؤلفه: ما–ت‌ل.۲,۱(FAU_GEN.2.1-NIAP-410)

شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه:
		برای رویدادهای ممیزی حاصل از اقدامات کاربران شناسایی شده، توابع امنیتی هدف ارزیابی باید قادر به مرتبط ساختن هر رویداد ممیزی با هویت کاربری که باعث ایجاد آن رویداد شده است، باشند.
۴	بازبینی ممیزی امنیت (FAU_SAR)	**نام عنصر: بازبینی ممیزی امنیت ۱**
		شماره مؤلفه: م‌ا-ب‌ز.۱،۱(FAU_SAR.1.1)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید کاربر سرپرست مرکزی را با قابلیت خواندن همه اطلاعات ممیزی از رکوردهای ممیزی، بر روی سامانه مدیریت مرکزی ایجاد کند.
۵		**نام عنصر: بازبینی ممیزی امنیت ۱**
		شماره مؤلفه: م‌ا-ب‌ز.۲،۱ (۱) ((1) FAU_SAR.1.2)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید رکوردهای ممیزی را به شکل مناسبی برای کاربر، جهت تفسیر اطلاعات فراهم کند.

شماره الزام	نام خانواده	عنصر امنیتی
۶		**نام عنصر: بازبینی ممیزی امنیت ۱** **شماره مؤلفه: ما-ب‌ز.۱,۱ (۲)((2) (FAU_SAR.1.1** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید کاربر سرپرست مرکزی و کاربر ایستگاه کاری را با قابلیت خواندن همه اطلاعات ممیزی از رکوردهای ممیزی بر روی ایستگاه کاری مورد استفاده ایجاد کند.
۷		**نام عنصر: بازبینی ممیزی امنیت ۱** **شماره مؤلفه: ما-ب‌ز.۲,۱ (۲) ((2) (FAU_SAR.1.2** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید رکوردهای ممیزی را به شکل مناسبی برای کاربر، جهت تفسیر اطلاعات فراهم کند. **نکته کاربردی:** کاربر ایستگاه کاری مجاز است تمام رکوردهای ممیزی ذخیره شده بر روی ایستگاه های کاری را که توسط آن کاربر مورد استفاده قرار می‌گیرد بازنگری کند. سرپرست مرکزی مجاز است تمام سوابق ممیزی را بر روی یک

شماره الزام	نام خانواده	عنصر امنیتی

ایستگاه کاری مشخص (که فقط به آن ایستگاه کاری اعمال می‌شود) یا بر روی سیستم مدیریت مرکزی (که به ایستگاه های کاری در آن دامنه اعمال میشود) بازنگری کند.

۸ **نام عنصر: بازبینی ممیزی محدود ۲**

شماره مؤلفه: م‌ا-ب‌ز.۱,۲(FAU_SAR.2.1)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید از قابلیت دسترسی کلیه کاربران جهت خواندن رکوردهای ممیزی ممانعت کند، به‌جز کاربرانی که به آن‌ها مجوز دسترسی با قابلیت خواندن داده شده باشد.

نکته کاربردی:

این الزامات به دسترسی خواندن رکوردهای ممیزی از طریق رابط توابع امنیتی هدف ارزیابی اعمال می‌شود. محیط فناوری اطلاعات (سیتم‌عامل) مسئول ممنوعیت دسترسی خواندن فایل ممیزی از طریق واسطه‌های سیستم‌عامل است.

۹ **نام عنصر: بازبینی ممیزی قابل انتخاب ۳**

شماره مؤلفه: م‌ا-ب‌ز.۱,۳(FAU_SAR.3.1)

شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید قابلیت انجام مرتب‌سازی داده‌های ممیزی را بر اساس تاریخ و زمان، نوع رویداد و هویت موجودیت فعال فراهم کند.
۱۰	تضمین در دسترس بودن داده‌های ممیزی **(FAU_STG)**	**نام عنصر: تضمین در دسترس بودن داده‌های ممیزی ۱**
		شماره مؤلفه: م‌ا-ذخ.۱(۱).۱(۱).۱(FAU_STG.1(1).1)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید از رکوردهای ممیزی ذخیره شده در دنباله ممیزی در مقابل حذف غیر مجاز از طریق رابط توابع امنیتی هدف ارزیابی جلوگیری کند.
		نکته کاربردی :
		این الزام در هر دو مورد سیستم مرکزی و ایستگاههای کاری منحصربه‌فرد اعمال می‌شود.
		این الزام در مورد حفاظت از رکوردهای ممیزی از طریق رابط توابع امنیتی هدف ارزیابی اعمال می‌شود و محیط فناوری اطلاعات (سیستم‌عامل) برای جلوگیری از حذف فایل ممیزی از طریق واسط سیستم عامل پاسخگو است.

شماره الزام	نام خانواده	عنصر امنیتی
۱۱		**نام عنصر: تضمین در دسترس بودن داده‌های ممیزی ۱** **شماره مؤلفه: م‌ا–ذخ.۱(۲).۱(FAU_STG.1(2).1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید از رکوردهای ممیزی ذخیره شده در دنباله ممیزی در مقابل تغییر غیر مجاز از طریق رابط توابع امنیتی هدف ارزیابی جلوگیری کند. **نکته کاربردی:** این الزام در هر دو مورد سیستم مرکزی و ایستگاههای کاری منحصر بفرد اعمال می‌شود. این الزام در مورد حفاظت از رکوردهای ممیزی از طریق رابط توابع امنیتی هدف ارزیابی اعمال می‌شود و محیط فناوری اطلاعات (سیستم عامل) برای جلوگیری از حذف فایل ممیزی از طریق واسط سیستم عامل پاسخگو می‌باشد.
۱۲		**نام عنصر: قابلیت پیکربندی در محل برای جلوگیری از عدم ممیزی** **شماره مؤلفه: م‌ا–ذخ.۴۱۴–۱ (FAU_STG.NIAP-0414-1-NIAP-429)**

شماره الزام **نام خانواده** **عنصر امنیتی**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید برای سرپرست قابلیتی ایجاد کنند تا بتواند در زمان پر شدن دنباله ممیزی اقدام/اقدامات زیر را صورت دهند:

[انتخاب: نادیده گرفتن رویدادهای ممیزی، جلوگیری از رویدادهای قابل ممیزی به‌جز آن‌ها که توسط کاربر مجاز شده با حق خاص رخ می‌دهند، بازنویسی بر روی قدیمی‌ترین رکوردهای ممیزی ذخیره شده]

[اختصاص: **اعمال دیگری که در زمان بروز خرابی در حافظه ممیزی باید انجام شوند**]

۱۳ **نام عنصر: قابلیت پیکربندی در محل برای جلوگیری از عدم ممیزی**

شماره مؤلفه: ما-ذخ.۴۱۴-۲ (FAU_ STG.NIAP-0414-2-NIAP-429)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید عمل [انتخاب: نادیده گرفتن رویدادهای ممیزی، جلوگیری از رویدادهای قابل ممیزی بجز آنها که توسط کاربر مجاز شده با حق خاص رخ می‌دهند، بازنویسی بر روی قدیمی‌ترین رکوردهای ممیزی ذخیره شده، [اختصاص: **اعمال دیگری که در زمان بروز خرابی در حافظه ممیزی باید انجام شوند**]] را در زمان پر شدن دنباله ممیزی انجام دهند و هیچ اقدام دیگری برای انتخاب وجود ندارد.

شماره الزام	نام خانواده	عنصر امنیتی
۱۴		**نام عنصر: قابلیت پیکربندی در محل برای جلوگیری از عدم ممیزی**

شماره مؤلفه: م‌ا-ذخ.۴۱۴-۳ (FAU_ STG.NIAP-0414-3-NIAP-429)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قبل از رسیدن حافظه ممیزی به ظرفیتش به‌صورت [انتخاب: اعلام زمان تا پر شدن شدن، اعلام تعداد رکوردها تا پر شدن، درصد فضای حافظه در دسترس آزاد برای ذخیره سازی ممیزی] به سرپرست هشدار دهند.

نکته کابردی:

هدف ارزیابی باید پیش از پر شدن حافظه ممیزی به سرپرست هشدار دهد. هدف از این هشدار، دادن زمان مناسب به سرپرست برای حل مشکل حافظه پیش از رخ دادن حذف رکوردهای ممیزی است. زمانی که حافظه پر شد و حذف اطلاعات ممیزی رخ داد، باید هشداری حاوی جزئیات حذف در محل ذخیره سازی ممیزی دیگری ثبت شود.

نویسنده هدف امنیتی باید رفتار هدف ارزیابی را در زمان بروز پرشدن حافظه ممیزی مشخص کند. بطور کلی از دست رفتن حداقل اطلاعات ممیزی مورد نظر است. هدف ارزیابی ممکن است از یک سازوکار برای حذف

شماره الزام	نام خانواده	عنصر امنیتی

رکوردهای ممیزی بر اساس پارامترهای خاصی استفاده کند که باید آن را اعلام کند. هدف امنیتی باید حاوی ارتباط بین خط‌مشی حذف از حافظه ممیزی و کمیت حذف باشد.

هشدارهای قبل از پر شدن حافظه ممیزی می تواند به عنوان نمونه به‌صورتهای زیر باشد:

- ۱۰ دقیقه تا پر شدن حافظه ممیزی زمان باقی است.
- ۱۰ رکورد تا پر شدن حافظه ممیزی زمان باقی است.
- ۳ درصد از فضای حافظه ممیزی آزاد است.

۲,۷ کلاس پشتیبانی از رمزنگاری

در ادامه مؤلفه‌های امنیتی مورد نیاز کلاس پشتیبانی از رمزنگاری ارائه شده است.

نام کلاس: پشتیبانی از رمزنگاری

شرح کلاس: توابع امنیتی هدف ارزیابی ممکن است با به کار بردن قابلیت‌های رمزنگاری، به برآورده‌شدن چندین هدف امنیتی سطح بالا کمک کنند. این اهداف می‌توانند شامل موارد زیر باشند، اما تنها به این دسته نیز محدود نمی‌شوند:

- شناسایی و احراز هویت

- عدم انکار
- مسیر امن
- کانال امن
- مجزاسازی داده

این کلاس زمانی که هدف ارزیابی، عملکرد رمزنگاری را پیاده‌سازی می‌کند، استفاده می‌شود این پیاده‌سازی می‌تواند در نرم‌افزار، سخت‌افزار و میان افزار صورت گیرد.

- **خانواده مدیریت کلید رمزنگاری[1]**

کلیدهای رمزنگاری باید از طریق دوره حیاتشان مدیریت شوند. این خانواده برای پشتیانی از دوره حیات کلید در نظر گرفته می‌شود و درنتیجه الزاماتی را برای فعالیت‌های زیر تعریف می‌کند:

- تولید کلید رمزنگاری
- توزیع کلید رمزنگاری
- دستیابی به کلید رمزنگاری
- تخریب کلید رمزنگاری

در صورت وجود الزامات عملیاتی برای مدیریت کلیدهای رمزنگاری، این خانواده نیز باید در نظر گرفته شود.

- **خانواده عملیات رمزنگاری [2]**

---

1 Cryptographic key management(FCS_CKM)

2 Cryptographic operation(FCS_COP)

به منظور عملکرد صحیح عملیات رمزنگاری، این عملیات باید مطابق با الگوریتم خاص و کلید رمزنگاری با اندازه مشخص انجام گیرد. در صورت وجود الزامات عملیاتی برای مدیریت کلیدهای رمزنگاری، این خانواده نیز باید در نظر گرفته شود.

معمولاً عملیات رمزنگاری شامل رمزنگاری و رمزگشایی داده، تائید و/یا تولید امضای دیجیتال، تولید کنترل [1]رمزنگاری برای یکپارچگی و صحت و یا تائید کنترل، درهم-سازی امن (خلاصه پیام)، رمزنگاری و/یا رمزگشایی کلید رمزنگاری و توافق کلید رمزنگاری می‌باشد.

شماره الزام	نام خانواده	عنصر امنیتی
۱۵	عملیات رمزنگاری (FCS_COP)	**نام عنصر: عملیات رمزنگاری ۱(۲)** **شماره مؤلفه: رز-ع‌ر.۱،۱(۲) ((FCS_COP.1.1(2))**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید خدمات رمزنگاری امضا را مطابق با موارد زیر انجام دهد:

[انتخاب :

- الگوریتم امضای دیجیتال (DSA) با کلید ۲۰۴۸ بیتی یا بیشتر مطابق با استاندارد FIPS PUB 186-3،

[1] Checksum

شماره الزام	نام خانواده	عنصر امنیتی

« استاندارد امضای دیجیتال»

- الگوریتم امضای دیجیتال RSA (rDSA) با کلید ۲۰۴۸ بیتی یا بیشتر مطابق با استاندارد FIPS PUB 186-2 یا FIPS PUB 186-3،«استاندارد امضای دیجیتال»
- الگوریتم امضای دیجیتال منحنی بیضوی (ECDSA[1]) با کلید ۲۵۶ بیتی یا بیشتر مطابق با
  - FIPS PUB 186-3 ، «استاندارد امضای دیجیتال»
  - تابع ارزیابی امنیتی باید «منحنی‌های استاندارد "NIST curves" ، P-256، P384 و [انتخاب: P251 ، نه سایر منحنی‌ها] (هم‌چنان‌که در FIPS PUB 186-3، «استاندارد امضای دیجیتال» تعریف شده‌است)] را پیاده‌سازی کند.

نکته کاربردی:

نویسنده سند هدف امنیتی باید الگوریتم پیاده‌سازی شده برای انجام امضای دیجیتال را انتخاب کند، اگر بیش از یک الگوریتم موجود است، این الزام(و الزام مرتبط با رز–م‌ک.۱ FCS_CKM.1) برای مشخص کردن قابلیت باید تکرار

1 Elliptic Curve Digital Signature Algorithm

شماره الزام	نام خانواده

عنصر امنیتی

شوند. برای الگوریتم انتخاب‌شده، نویسنده سند هدف امنیتی باید انتخاب‌ها/اختصاص‌های مناسب را برای مشخص‌کردن پارامترهایی که برای آن الگوریتم پیاده‌سازی شده‌اند، انجام دهند.

برای طرح‌های منحنی مبنای بیضوی، اندازه کلید به لگاریتم مبنای ۲ نقطه مبنا اشاره دارد. به عنوان یک راهکار برتر، برای امضاهای دیجیتال، الگوریتم امضای دیجیتال منحنی‌های بیضوی برای نسخه‌های بعدی این پروفایل حفاظتی موردنیاز هستند.

۱۶ **نام عنصر: عملیات رمزنگاری ۱(۴)**

شماره مؤلفه: رز-ع‌ر.۱٫۱(۴) ((FCS_COP.1.1(4))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید [**احراز هویت پیام مبتنی بر درهم‌سازی-کلید**] را در تطابق با یک الگوریتم رمزنگاری مشخص HMAC -[انتخاب:SHA-1, SHA-224, SHA-256, SHA-384, SHA-512]، با اندازه کلید [اختصاص: **اندازه کلید (بیت) استفاده شده در HMAC**]، و اندازه‌های خلاصه پیام [انتخاب: ۱۶۰ ،۲۲۴، ۲۵۶، ۳۸۴ و ۵۱۲ بیت] که مطابق با استاندارد FIPS 198-1، «کد احراز هویت پیام مبتنی بر درهم‌سازی-کلید» و

شماره	نام خانواده	عنصر امنیتی
الزام		

استاندارد FIPS 180-3، «استاندارد درهم‌ساز امن» باشد، انجام دهند.

نکته کاربردی:

در نسخه‌های بعدی این پروفایل حفاظتی، الگوریتم درهم‌سازی SHA-1 ممکن است به عنوان یک الگوریتم درهم‌ساز قابل قبول، حذف شود و توسعه‌دهندگان راغب به استفاده از الگوریتم‌های درهم‌ساز دیگر شوند.

۱۷	تولید بیت تصادفی (FCS_RBG_EXT)	**نام عنصر: تولید بیت تصادفی ۱** **شماره مؤلفه: رز-بت(ت‌س).۱,۱ (FCS_RBG_EXT.1.1)**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید تمام خدمات تولید بیت تصادفی را مطابق با [انتخاب: یکی از: NIST 800-90 با استفاده از [انتخاب: Hash_DRBG (هرکدام), HMAC_DRBG(هرکدام)، CTR_DRBG (AES)، Dual_EC_DRBG(هرکدام)]، پیوست C: X9.31 ضمیمه ۲,۴ از FIPS 140-2 با استفاده از AES] انجام دهد که توسط یک منبع آنتروپی انباشته از آنتروپی [انتخاب: یکی یا هر دو: منبع نویز مبتنی بر نرم‌افزار یا منبع نویز مبتنی بر سخت‌افزار توابع امنیتی هدف ارزیابی] جایگذاری شده است.

شماره	نام خانواده	عنصر امنیتی
الزام		

۳,۷ کلاس حفاظت از داده‌های کاربری

در ادامه مؤلفه‌های امنیتی مورد نیاز کلاس حفاظت از داده‌های کاربری ارائه شده است.

نام کلاس: حفاظت از داده کاربری

شرح کلاس: این کلاس شامل خانواده‌هایی است که الزامات مربوط به محافظت از داده کاربر را مشخص می‌کنند. خانواده‌های محافظت از داده کاربر در چهار گروه زیر دسته بندی شده‌اند که علاوه بر مشخصه‌های امنیتی مربوط به داده کاربری، داده‌های کاربری در داخل هدف ارزیابی را در طول ورود، خروج و ذخیره سازی نیز نشان می-دهند.

خانواده‌های این کلاس در چهار گروه زیر دسته بندی شده‌اند:

۱) سیاست‌های امنیتی مربوط به محافظت از داده کاربری

- سیاست‌های کنترل دسترسی (حف-س‌ک)[1]
- سیاست‌های مرتبط با کنترل جریان اطلاعات (حف-خج)[2]

1 Access control policy(FDP_ACC)

2 Information flow control policy(FDP_IFC)

در این دو خانواده، به نویسنده هدف امنیتی/پروفایل حفاظتی اجازه داده می‌شود تا سیاست‌های امنیتی که برای حفاظت از داده‌کاربری در نظر گرفته شده، و همچنین حوزه کنترلی این سیاست‌ها نام برده شود.
سیاست‌های امنیتی نام برده شده در این دو خانواده

- سیاست‌های امنیتی در نظر گرفته شده برای کنترل دسترسی
- سیاست‌های امنیتی در نظر گرفته شده برای کنترل جریان اطلاعات

توسط مؤلفه‌های دیگر خانواده‌ها با استفاده از بخش«انتخاب» یا «اختصاص» فراخوانی می‌شوند.
در دو خانواده‌ی توابع کنترل دسترسی (ح‌ف-ت‌ک)[1] و توابع کنترل جریان اطلاعات (ح‌ف-ک‌ج)[2] قوانینی که تعریف کننده‌ی «سیاست‌های امنیتی کنترل دسترسی» و «سیاست‌های امنیتی کنترل جریان اطلاعات» هستند، آورده شده است.

۲) فرم‌های مختلف محافظت از داده کاربری

- توابع کنترل دسترسی (ح‌ف-ت‌ک)
- توابع کنترل جریان اطلاعات (ح‌ف-ک‌ج)
- انتقال داخلی در هدف ارزیابی (ح‌ف-اد)[3]
- حفاظت از اطلاعات باقیمانده (ح‌ف-اب)[1]

1 Access control functions(FDP_ACF)
2 Information flow control functions(FDP_IFF)
3 Internal TOE transfer(FDP_ITT)

- عملیات عقب‌گرد به منظور بازگرداندن حالت/حالت‌های قبل (حف-ع‌گ)[۲]
- یکپارچگی داده‌های ذخیره شده (حف-ی‌د)[۳]

۳) ورود و خروج، ذخیره‌سازی برون‌خطی[۴]

- احراز هویت[۵] داده (حف-ت‌د)
- صادر شده از هدف ارزیابی (حف-ص‌ا)[۶]
- ورود داده‌ها از بیرون به هدف ارزیابی (حف-وب)[۷]

مؤلفه‌های این خانواده، انتقال قابل اعتماد به داخل یا خارج از هدف ارزیابی را نشان می‌دهند.

۴) ارتباطات میان توابع امنیتی هدف ارزیابی

- محافظت از انتقال محرمانگی داده کاربر توابع امنیتی هدف ارزیابی داخلی(حف-م‌د)[۸]
- محافظت از انتقال یکپارچگی داده کاربر توابع امنیتی هدف ارزیابی داخلی(حف-ی‌ا)[۱]

---

1 Residual information protection(FDP_RIP)
2 Rollback(FDP_ROL)
3 Stored data integrity(FDP_SDI)
4 Offline
5 Data authentication(FDP_DAU)
6 Export from the TOE(FDP_ETC)
7 Import from outside of the TOE(FDP_ITC)
8 Inter-TSF user data confidentiality transfer protection(FDP_UCT)

مؤلفه‌های این خانواده ارتباطات بین توابع امنیتی هدف ارزیابی و دیگر محصولات امن فناوری اطلاعات را نشان می‌دهد.

- **خانواده سیاست‌های کنترل دسترسی**

این خانواده سیاست‌های امنیتی مربوط به کنترل دسترسی را نام می‌برد و حوزه کنترلی سیاست‌گذاری‌ها را تعریف می‌کند. این حوزه کنترلی توسط سه مجموعه زیر مشخص می‌شود:

- موجودیت‌های فعال[۲] تحت کنترل سیاست‌گذاری‌ها
- موجودیت‌های غیرفعال[۳] تحت کنترل سیاست‌گذاری‌ها
- عملیات بین موجودیت‌های فعال کنترل شده و موجودیت‌های غیرفعال کنترل شده که توسط سیاست‌های امنیتی پوشش داده می‌شود.

بنابراین در مؤلفه‌های این خانواده، سیاست امنیتی نامبرده می‌شود و برای هریک از سیاست‌های امنیتی نام‌برده شده، موجودیت فعال و غیرفعال تحت کنترل آن سیاست و عملیات بین موجودیت فعال و غیرفعال نیز نام‌برده می‌شود.
در این خانواده می‌توان سیاست‌های امنیتی مختلفی برای کنترل دسترسی داشت، و هریک نام منحصر به فرد خود را داسته باشند تنها باید مؤلفه‌های این خانواده برای هر یک از سیاست‌های امنیتی به صورت جداگانه تکرار شود (به طور مثال حف-س‌ک.۱,۱(۱)، حف-س‌ک.۱,۱(۲)).
قوانینی که عملکرد سیاست‌های امنیتی را برای کنترل دسترسی تعریف می‌کنند، در خانواده‌های توابع کنترل دسترسی (حف-ت‌ک) و صادر شده از هدف ارزیابی (حف-ص‌ا) تعریف می‌شوند.
سیاست‌های نام برده شده در این خانواده توسط مؤلفه‌های دیگر خانواده‌ها با استفاده از بخش«انتخاب» یا «اختصاص» فراخوانی می‌شوند.

---

1 Inter-TSF user data integrity transfer protection(FDP_UIT)

2 Subject

3 Object

➢ خانواده توابع کنترل دسترسی

در خانواده سیاست‌های امنیتی کنترلی دسترسی (حف-س‌ک)، تنها این سیاست‌ها نام برده می‌شوند، اما در این خانواده قوانینی برای اجرای سیاست امنیتی بر روی عملیات بین موجودیت‌های فعال و غیرفعال (نام برده شده در خانواده (حف-س‌ک)) وضع می‌شود. هم‌چنین در این خانواده موجودیت‌های فعال و غیرفعال تحت کنترل سیاست‌های امنیتی و مشخصه‌های امنیتی مربوط به آنها نام‌برده می‌شوند.

➢ خانواده احراز هویت داده

احراز هویت داده به هر نهادی، اجازه‌ی پذیرش مسوولیت احراز صحت اطلاعات را می‌دهد (با دیجیتالی امضاء کردن اطلاعات). این خانواده روشی را مشروط بر تضمین اعتبار یک بخش خاص از داده ارائه می‌کند که می‌تواند به منظور بررسی محتوای اطلاعات از لحاظ جعل نشدن یا تغییر یافتن مکرر مورد استفاده قرار گیرد.

➢ خانواده صادرشده از هدف ارزیابی

در دو خانواده (حف-س‌ک) و (حف-خج)، سیاست‌های امنیتی بر روی کنترل دسترسی و جریان اطلاعات نام‌برده شده‌اند. در این خانواده این سیاست‌های امنیتی بر روی داده تحت کنترل این سیاست‌ها هنگام خروج از هدف ارزیابی اعمال می‌شود، مشخصه‌های امنیتی داده‌ها هنگام صدور می‌تواند حفظ گردیده یا نادیده گرفته شود. در واقع در این خانواده محدودیت‌هایی برای صدور داده از هدف ارزیابی اعمال می‌شود.

➢ سیاست‌های کنترل جریان اطلاعات

این خانواده سیاست‌گذاری‌های عملکرد امنیتی مربوط به کنترل جریان اطلاعات را نام می‌برد و برای هریک از آنها، حوزه کنترلی را تعریف می‌کند. این حوزه کنترلی توسط سه مجموعه زیر مشخص می‌شود:

- موجودیت‌های فعال تحت کنترل سیاست‌گذاری‌ها
- اطلاعات تحت کنترل سیاست‌گذاری‌ها

- عملیاتی که سبب کنترل اطلاعات جریان یافته به/از موجودیت‌های فعال کنترل شده تحت پوشش این سیاست‌ها هستند.

بنابراین در مؤلفه‌های این خانواده، سیاست امنیتی نام‌برده می‌شوند و برای هریک از سیاست‌های امنیتی نام‌برده شده، موجودیت فعال و غیرفعال تحت کنترل آن سیاست و عملیات بین موجودیت فعال و غیرفعال نیز نامبرده می‌شوند.
در این خانواده می‌توان سیاست‌های امنیتی مختلفی برای کنترل دسترسی داشت و هریک نام منحصر به فرد خود را داشته باشند تنها باید مؤلفه‌های این خانواده برای هر یک از سیاست‌های امنیتی به صورت جداگانه تکرار شود (به طور مثال حف-خج.۱,۱(۱)، حف-خج.۱,۱(۲)).
قوانینی که عملکرد سیاست‌های امنیتی را برای کنترل دسترسی تعریف می‌کنند، در خانواده‌های توابع کنترل دسترسی (حف-کج) و صادر شده از هدف ارزیابی (حف-ص-ا) تعریف می‌شوند.
سیاست‌های نام برده شده در این خانواده توسط مؤلفه‌های دیگر خانواده‌ها با استفاده از بخش«انتخاب» یا «اختصاص» فراخوانی می‌شوند.

- **خانواده توابع کنترل جریان اطلاعات**

در خانواده سیاست‌های امنیتی کنترلی دسترسی (حف-خج)، تنها این سیاست‌ها نام برده می‌شوند، اما در این خانواده قوانینی برای اجرای سیاست امنیتی بر روی عملیات بین موجودیت‌های فعال و غیرفعال (نام برده شده در خانواده (حف-خج)) وضع می‌شود. هم‌چنین در این خانواده موجودیت‌های فعال و غیرفعال تحت کنترل سیاست‌های امنیتی و مشخصه‌های امنیتی مربوط به آنها نام‌برده می‌شوند.این خانواده شامل دو الزام است:

- یکی پرداختن به مسائل عملکرد جریان اطلاعات رایج
- پرداختن به جریان اطلاعات غیرمجاز

این تقسیم‌بندی به این دلیل مطرح شده است که مسائل مربوط به جریان اطلاعات غیرمجاز، در برخی موارد با باقی سیاست‌گذاری‌های امنیتی مربوط به کنترل جریان اطلاعات در تعامد است. با توجه به طبیعتشان سرپیچی کردن آنها از سیاست‌گذاری‌های امنیتی مربوط به کنترل جریان اطلاعات، منجر به نقص در سیاست‌ها می‌شود. بنابراین، باید عملیات خاصی را برای جلوگیری یا محدود کردن جریان اطلاعات غیرمجاز در نظر گرفت.

- **خانواده ورود داده‌ها از بیرون به هدف ارزیابی**

این خانواده تعریف کننده سازوکارهایی برای ورود داده‌های کاربری تحت کنترل سیاست‌های امنیتی (سیاست‌های امنیتی کنترل جریان و کنترل دسترسی) از خارج هدف ارزیابی می‌باشد. برای ورود داده باید سیاست‌های تعریف شده بر روی داده اعمال شود، هم‌چنین مشخصه‌های امنیتی مطلوبی برای اینگونه از داده‌ها در نظر گرفته شود. در واقع این خانواده محدودیت‌هایی بر روی داده‌های ورودی از خارج هدف ارزیابی اعمال می‌کند.

- **خانواده انتقال هدف ارزیابی داخلی**

این خانواده الزاماتی را ارائه می‌دهد تا از داده کاربری در زمانی‌که بین بخش‌های مجزای هدف ارزیابی در سراسر کانال داخلی[1] انتقال می‌یابد، حفاظت کند. هم‌چنین در این خانواده، داده‌ها را براساس مشخصه‌های امنیتی از یکدیگر مجزا می‌کنند و برای شناسایی خطا در صحت داده، داده‌های منتقل شده بین بخش‌های هدف ارزیابی پایش می‌شوند.

- **خانواده حفاظت از اطلاعات باقیمانده**

این خانواده اطمینان می‌دهد در زمانی‌که منبع از یک موجودیت غیرفعال آزاد می‌شود و دوباره به یک موجودیت غیرفعال دیگر اختصاص داده می‌شود، هرگونه داده موجود در منابع، در دسترس قرار نمی‌گیرد. این خانواده نیاز دارد که از هرگونه داده موجود در منابع که به طور منطقی حذف یا آزاد می‌شود، محافظت کند، اما ممکن است هنوز در داخل منابع کنترل شده توابع امنیتی هدف ارزیابی اطلاعاتی وجود داشته باشد که به موجودیت غیرفعال دیگری اختصاص داده شود.

[1] Internal channel

- **خانواده عملیات عقب‌گرد به منظور بازگرداندن حالت/ حالت‌های قبل**

عملکرد عقب‌گرد شامل بی‌اثر کردن آخرین عملکرد یا یک سری از عملکردها، محدود شدن به برخی محدودیت‌ها هم‌چون بازه زمانی و برگشت به یک وضعیت شناخته شده قبلی می‌باشد. عقب‌گرد فراهم کننده‌ی قابلیت بی‌اثر کردن عملیات یا مجموعه‌ای از عملیات است تا یکپارچگی داده کاربری را حفظ کند.

- **خانواده صحت داده‌های ذخیره شده**

این خانواده الزاماتی را ارائه می‌کند که از داده کاربری ذخیره شده در کانتینر تحت کنترل توابع امنیتی هدف ارزیابی، محافظت می‌کند. خطای صحت ممکن است داده کاربری ذخیره شده در حافظه یا در یک ابزار ذخیره‌سازی را تحت تاثیر قرار بدهند. این خانواده صحت داده‌های ذخیره شده را حفظ می‌کند و ممکن است در صورت تشخیص خطا، اقدامی در برابر آن انجام بدهد، اما خانواده «انتقال هدف ارزیابی داخلی (حف-اد)» صحت داده کاربری در حال انتقال در هدف ارزیابی را محافظت می‌کند.

- **خانواده محافظت از انتقال محرمانگی داده کاربر در توابع امنیتی هدف ارزیابی داخلی**

این خانواده تعریف کننده الزاماتی است که محرمانگی داده کاربری را در زمانی‌که با استفاده از یک کانال خارجی بین هدف ارزیابی و دیگر محصولات امن IT انتقال می‌یابد، تضمین می‌کند.

- **خانواده محافظت از انتقال صحیح داده کاربر در داخلی عملکرد امنیتی هدف ارزیابی**

این خانواده الزاماتی را تعریف می‌کند تا صحت داده کاربری را که بین هدف ارزیابی و دیگر محصولات امن IT منتقل می‌شود، تأمین کند و داده کاربری را از خطاهای قابل تشخیص بازیابی کند. این خانواده حداقل داده کاربری را جهت اطمینان از تغییر نیافتن پایش می‌کند. همچنین، این خانواده از روش‌های مختلفی جهت اصلاح خطاهای تشخیص داده شده در صحت داده پشتیبانی می‌کند.

شماره	نام عنصر الزام	مؤلفه امنیتی
۱۸	حفاظت از داده های باقیمانده (FDP-RIP)	**نام عنصر: حفاظت از داده های باقیمانده ۱** **شماره مؤلفه: ح‌ف-اب.۱،۱(FDP_RIP.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید تضمین کند که هرگونه محتوی اطلاعات قبلی یک منبع را در زمان [انتخاب: تخصیص منابع به، آزادسازی منابع از] تمام موجودیت های غیر فعال استفاده شده توسط هدف ارزیابی، غیرقابل دسترس کند.
۱۹	عقبگرد ابتدایی (FDP_ROL)	**نام عنصر: عقبگرد ابتدایی ۱** **شماره مؤلفه: ح‌ف-ع‌گ.۱،۱(FDP_ROL.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید [اختصاص: **خط‌مشی‌های عملکرد امنیتی کنترل دسترسی و/یا خط‌مشی‌های عملکرد امنیتی کنترل جریان اطلاعات**] اجرا کنند تا اجازه عقب‌گرد از [اختصاص: **لیستی از عملکردها**] بر روی [اختصاص: **اطلاعات و/یا لیستی از موجودیت‌های غیرفعال**] بدهند.

شماره	نام عنصر	مؤلفه امنیتی
الزام		
۲۰	**نام عنصر: عقبگرد ابتدایی ۱**	
	شماره مؤلفه: ح‌ف-ع‌گ.۲,۱.۱.۲(FDP_ROL.1.2)	
	شرح مؤلفه:	
	توابع امنیتی هدف ارزیابی باید اجازه بدهند عملیات‌ها در حدود [اختصاص: **حدودی به آنچه که عقب گردش ممکن است انجام گیرد، محدود می‌شود**] عقب گرد شوند.	

۴,۷ کلاس شناسایی و احراز هویت

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

نام کلاس: شناسایی و احراز هویت

شرح کلاس: خانواده‌های این کلاس الزاماتی برای تصدیق و تائید هویت کاربر ادعا شده تعریف نموده‌اند. برای اطمینان یافتن از آنکه کاربران همراه با مشخصه‌های امنیتی به طور مثال، هویت گروه‌ها، نقش‌ها) مناسبی می‌باشند، شناسایی و احرازهویت کاربران لازم و ضروری می‌باشد.

شناسایی صریح کاربران مجاز و اختصاص صحیح مشخصه‌های امنیتی به کاربران و موجودیت‌های فعال بسیار مهم و حساس است تا سیاست‌های امنیتی در نظرگرفته شده در عمل پیاده سازی شوند. خانواده‌های این کلاس الزاماتی را فراهم می آورند تا هویت کاربران تعیین و احراز هویت شوند، صلاحیت آنهایی را که با هدف ارزیابی در تعامل هستند تعیین کنند و برای هر کاربر مجاز مشخصه‌های امنیتی 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 را که توابع امنیتی هدف ارزیابی در مواردی که تلاش جهت احراز هویت با شکست مواجه می‌شود، تعریف می‌کند. پارامترهایی هم‌چون تعداد تلاش‌های احراز هویت منجر به شکست و آستانه زمان در الزامات این خانواده تعیین می‌شوند.

- **خانواده تعریف مشخصه امنیتی**[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 کردن مشخصه‌های امنیتی کاربر به کاربران تعریف می‌کند تا در صورت لزوم توابع امنیتی هدف ارزیابی را در تصمیم‌گیری‌های امنیتی پشتیبانی کند.

- **خانواده مشخصات رازها**[3]

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

1 Authentication failures(FIA_AFL)

2 User attribute definition(FIA_ATD)

3 Specification of secrets(FIA_SOS)

- **خانواده احراز هویت کاربر[1]**

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

- **خانواده شناسایی کاربر[2]**

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[3]**

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 می‌شود(به طور کامل یا بخشی از آن). این خانواده الزاماتی را تعریف می‌کند تا ایجاد و نگهداری ارتباط بین کاربر و موجودیت فعال متناظر با آن را فراهم آورد.

شماره الزام	نام عنصر	مؤلفه امنیتی
۲۱	مدیریت رمز عبور (FIA_PMG_EXT.1)	**نام عنصر: مدیریت رمز عبور ۱** **شماره مؤلفه: اش-م‌ع.۱،۱ (FIA_PMG_EXT.1.1)**

1 User authentication(FIA_UAU)
2 User identification(FIA_UID)
3 User-subject binding(FIA_USB)

شماره الزام	نام عنصر	مؤلفه امنیتی
(T		**شرح مؤلفه:**

توابع امنیتی هدف ارزیابی باید قابلیت‌های مدیریت رمزعبور را که در زیر ذکر شده‌اند برای رمزهای عبور سرپرستی فراهم کند:

۱. رمزهای عبور باید بتوانند هرترکیبی ازحروف کوچک و بزرگ، اعداد و کاراکترهای خاص: [انتخاب: "@"، "#"، "$"، "٪"، "^"، "!" "&"، "*"، "(" , ")" [,اختصاص: **کاراکتر دیگر**]] باشند.

۲. حداقل طول رمزعبور باید توسط سرپرست امنیت، قابل تنظیم بوده و۱۵کاراکتر یا بیشتر باشد.

نکته کاربردی:

نویسنده‌ی هدف امنیتی، کاراکترهای خاصی را که توسط هدف ارزیابی پشتیبانی می‌شوند را انتخاب می‌کند. نویسنده این اختیار را دارد تا کاراکترهای خاص بیشتری را با استفاده از عبارت «اختصاص» لیست کند.

«رمزعبور سرپرستی» به آن دسته از رمزعبورهایی اشاره دارد، که سرپرستان از آنها در کنسول محلی یا پروتکل‌هایی که از رمزعبور پشتیبانی می‌کنند(همچون SSH,HTTPS)، استفاده می‌کنند.

۲۲	مدیریت احراز هویت ناموفق (**FIA_AFL**)	**نام عنصر: مدیریت احراز هویت ناموفق ۱** **شماره مؤلفه: اش-ش‌ا.۱.۱(FIA_AFL.1.1)**

شماره	نام عنصر	مؤلفه امنیتی
الزام		

شرح مؤلفه:

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. این احراز هویت می‌تواند بر روی سرپرستی مرکزی و یا ایستگاه کاری کاربر انجام شود.

نکته کاربردی:

- هدف ارزیابی ممکن است برای کاربران مختلف، متدهای احراز هویت متفاوتی استفاده کند و از قوانین مختلفی براساس متدهای احرازهویت/ یا کاربران جهت مدیریت کردن احراز هویت ناموفق بهره بگیرد. رفتاری که در قبال احراز هویت ناموفق، برای سیستم‌های از راه دور و کاربران انسانی صورت می‌گیرد، معمولاً 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.
- رویداد احراز هویت ناموفق با توجه به آخرین نشست موفق در ترمینال شمارش می‌شود.
- هرچند که لیستی از اقدامات می‌تواند توسط هدف ارزیابی، مشخص شود. اما این مجموعه اقدامات باید اطمینان دهد

شماره الزام	نام عنصر	مؤلفه امنیتی
		که از حملات مبتنی بر جستجو در فضاهای ممکن جلوگیری می‌کند.
۲۳		**نام عنصر: مدیریت احراز هویت ناموفق ۱** **شماره مؤلفه: اش-ش‌ا.۱.۲(FIA_AFL.1.2)** **شرح مؤلفه:** زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد معینی رسید یا از آن بیشتر شد، توابع امنیتی هدف ارزیابی باید [اختصاص: **لیست کردن اقداماتی را که بدین منظور در نظر گرفته شده است**] انجام دهد. **نکته کاربردی:** اقداماتی که توسط توابع امنیتی هدف ارزیابی انجام می‌شود می‌توان به قفل کردن حساب کاربری برای یک بازه زمانی، یا پیچیده‌تر کردن عمل احراز هویت مجدد کاربر اشاره نمود.
۲۴	شناسایی و احراز هویت کاربر (**FIA_UIA_EXT**)	**نام عنصر: شناسایی و احراز هویت کاربر** **شماره مؤلفه: اش-ش‌ه.۱.۱ (FIA_UIA_EXT .1.1)** **شرح مؤلفه:**

شماره الزام	نام عنصر	مؤلفه امنیتی

توابع امنیتی هدف ارزیابی، باید پیش از آنکه به موجودیت‌های غیرهدف ارزیابی، جهت شروع رویه شناسایی و احراز هویت نیاز باشد، اقدامات زیر را مجاز کند:

- نمایش هشدارها مطابق با خانواده «دس_ع د.۱»
- [انتخاب: بدون هیچ اقدام دیگر، [اختصاص: **لیستی از سرویس ها، اقداماتی که توسط توابع امنیتی هدف ارزیابی جهت پاسخ دادن به در خواست‌های «غیر هدف ارزیابی» صورت می‌گیرد**]].

۲۵ **نام عنصر: احراز هویت کاربر قبل از هر اقدامی ۲**

شماره مؤلفه: اش-اه.۱,۲(FIA_UAU.2.1)

احراز هویت کاربر (**FIA_UAU**)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی، باید هر ایستگاه کاری یا سرپرست مرکزی را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، با موفقیت احراز هویت کند.

شماره الزام	نام عنصر	مؤلفه امنیتی
		نام عنصر: سازوکار احراز هویت بر اساس رمزعبور ۲ **شماره مؤلفه: اش-اه.۱,۲ (FIA_UAU_EXT .2.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی جهت احراز هویت سرپرستان باید یک سازوکار احراز هویت محلی را مبتنی بر رمز عبور[انتخاب:[اختصاص: **دیگر سازوکارهای احراز هویت**]، هیچکدام] فراهم کند.
۲۶		**نام عنصر: احراز هویت کاربر قبل از هر اقدامی ۶** **شماره مؤلفه: اش-اه.۱,۶(FIA_UID.6.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی، باید **کاربر ایستگاه‌کاری یا سرپرست مرکزی** را در شرایطی که نشست به علت عدم فعالیت قفل شده است مجدداً احراز هویت کند.
۲۷	شناسایی کاربر	**نام عنصر: شناسایی کاربر قبل از هر اقدامی ۲**

شماره الزام	نام عنصر	مؤلفه امنیتی
(FIA_UID)	شماره مؤلفه: اش-اه.۱,۲(FIA_UID.2.1)	

شرح مؤلفه:

توابع امنیتی هدف ارزیابی، باید هر **کاربر ایستگاه‌کاری یا مدیر مرکزی** را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، با موفقیت شناسایی کند.

۵,۷ کلاس مدیریت امنیت

در ادامه مؤلفه‌های امنیتی مورد نیاز کلاس مدیریت امنیت ارائه شده است.

نام کلاس: مدیریت امنیت

شرح کلاس: این کلاس جهت مشخص کردن 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 شوند.
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

1 Banner

- 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.

➢ 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، زمان و دیگر پارامترهای پیکربندی توابع امنیتی هدف ارزیابی باشد.

---

1 Management of functions in TSF (FMT_MOF)

2 Management of security attributes (FMT_MSA)

3 Management of TSF data (FMT_MTD)

- **خانواده لغو[1]**

این خانواده لغو مشخصه‌های امنیتی انواع موجودیت‌ها در هدف ارزیابی را نشان می‌دهد.

- **خانواده انقضای مشخصه امنیتی[2]**

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

- **خانواده مشخصات کارکردهای مدیریت[3]**

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 کنند، 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 می‌شود تا تداوم عملکرد هدف ارزیابی را تضمین کند، مانند عملکردهای پشتیبانی و بازیابی. عملکرد این خانواده بر روی دیگر مؤلفه‌ها در کلاس مدیریت امنیت تاثیر دارد.

- **خانواده نقش‌های امنیتی[4]**

1 Revocation (FMT_REV)

2 Security attribute expiration (FMT_SAE)

3 Specification of Management Functions (FMT_SMF)

4 Security management roles (FMT_SMR)

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 الزام	نام عنصر	مؤلفه امنیتی
۲۸	**نام عنصر: مشخصات توابع مدیریتی ۱** **شماره مؤلفه: م‌د–م‌ت.۱,۱ (۱) ((FMT_MOF.1.1(1))** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید قابلیت تعیین رفتار، غیرفعال سازی، فعال سازی توابع زیر را به سرپرست مرکزی محدود کند.	مدیریت کارکرد در توابع امنیتی هدف ارزیابی (FMT_MOF.) - ممیزی - اسکن بلادرنگ برای پیدا کردن ویروس - اسکن زمانبندی شده برای پیدا کردن ویروس.
۲۹	**نام عنصر: مشخصات توابع مدیریتی ۱** **شماره مؤلفه: م‌د–م‌ت.۱,۱ (۲) ((FMT_MOF.1.1(2))**	

شماره	نام عنصر الزام	مؤلفه امنیتی

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قابلیت تغییر رفتار برای توابعی که به‌صورت دستی، عمل اسکن برای پیدا کردن ویروس را انجام می-دهند را، به کاربران ایستگاه کاری محدود کند.

۳۰ **نام عنصر: مدیریت داده‌های توابع امنیتی هدف ارزیابی ۱**

شماره مؤلفه: م‌د-م‌د.۱,۱ (۱) ((FMT_MTD.1.1(1))

شرح مؤلفه:

مدیریت داده‌های توابع امنیتی هدف ارزیابی (**FMT_MTD**)

توابع امنیتی هدف ارزیابی باید قابلیت‌های پرس و جو، تغییر و حذف کردن موارد زیر را تنها به سرپرست مرکزی محدود کنند:

- اقداماتی که در زمان تشخیص یک ویروس برروی ایستگاه کاری صورت می‌گیرد.
- فایل‌هایی که به‌صورت اتوماتیک برروی ایستگاه کاری اسکن می‌شوند.
- حداقل عمق اسکن فایل‌ها بر روی ایستگاه کاری
- اسکن زمان‌بندی شده بر روی ایستگاه کاری به‌صورت متناوب
- امضاهای اسکن ویروس

شماره	نام عنصر الزام	مؤلفه امنیتی
		• گزارشات ممیزی بر روی سیستم مدیریت مرکزی[1]
۳۱	**نام عنصر: مدیریت داده‌های توابع امنیتی هدف ارزیابی ۱** **شماره مؤلفه: م‌د-م‌ت.۱,۱ (۲) ((FMT_MOF.1.1(2))** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید قابلیت تغییر موارد زیر را به سرپرستی مرکزی و کاربران ایستگاه کاری محدود کند:	• عمق اسکن فایل‌ها برای اسکن‌هایی که به‌صورت دستی بر روی ایستگاه کاری انجام می‌شود. • فایل‌های که بتوان بر روی ایستگاه کاری به‌صورت دستی اسکن نمود.
۳۲	**نام عنصر: مدیریت داده‌های توابع امنیتی هدف ارزیابی ۱** **شماره مؤلفه: م‌د-م‌ت.۱,۱ (۳) ((FMT_MOF.1.1(3))** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید قابلیت پرس و جو، حذف گزارشات ممیزی استفاده شده بر روی ایستگاه کاری را به مدیر مرکزی و	

[1] Central management system

شماره	نام عنصر	مؤلفه امنیتی
الزام		
		کاربران ایستگاه کاری محدود کند.
۳۳	مشخصات عملکردهای مدیریتی (FMT_SMF)	**نام عنصر: مشخصات عملکردهای مدیریتی ۱** **شماره مؤلفه: م‌د-ع‌م.۱,۱ (FMT_SMF.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید توانایی اجرای عملکردهای مدیریت امنیتی زیر را دارا باشند: • فعال و غیرفعال کردن عملکرد هدف ارزیابی بر روی ایستگاه کاری • پیکربندی عملکرد هدف ارزیابی بر روی ایستگاه کاری • به‌روزرسانی امضاهای اسکن ویروس‌ها • پاسخ دهی به اخطارهای هشدار از سیستم مدیریت مرکزی • بازبینی گزارشات ممیزی بر روی سیستم مدیریت مرکزی • افزایش عمق اسکن فایل‌ها بر روی اسکن‌هایی که به‌صورت دستی انجام می‌گیرد. • پاسخ دهی به اخطارهای هشدار که بر روی ایستگاه کاری استفاده می‌شوند.

شماره	نام عنصر الزام	مؤلفه امنیتی
		• بازبینی گزارشات ممیزی بر روی ایستگاه کاری استفاده شده
۳۴	نقش‌های امنیتی (FMT_SMR)	**نام عنصر: نقش‌های امنیتی ۱** **شماره مؤلفه: م‌د-ن‌م.۱,۱ (FMT_SMR.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید نقش‌های زیر را ایجاد و نگهداری نمایند. • مدیر مرکزی • کاربر ایستگاه مرکزی • کاربر شبکه

۶,۷ کلاس حفاظت از توابع امنیتی هدف ارزیابی

در ادامه مؤلفه‌های 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 سازوکارهایی 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، ممکن است به نظر بیاید خانواده‌های این کلاس، تکرار عناصر کلاس محافظت از داده کاربری است، حتی ممکن است هر دوی این کلاس‌ها با سازوکاری 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 کنند که خط مشی‌های توابع امنیتی هدف ارزیابی نتوانند مورد مداخله قرار بگیرند یا دور زده[1] شوند.

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

- پیاده‌سازی توابع امنیتی هدف ارزیابی که سازوکارهای اجرا کننده توابع امنیتی هدف ارزیابی را اجرا و پیاده‌سازی می‌کنند.
- 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[2]

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 می‌شود.

➢ خانواده در دسترس بودن داده‌های ارسال شده توابع امنیتی هدف ارزیابی[3]

1 Bypass
2 Fail secure (FPT_FLS)
3 Availability of exported TSF data (FPT_ITA)

این خانواده قوانینی را تعریف می‌کند که، در هنگام انتقال داده توابع امنیتی هدف ارزیابی بین توابع امنیتی هدف ارزیابی و دیگر محصولات IT از نبود دسترسی به این داده‌ها، جلوگیری می‌کند. 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 محرمانگی داده‌های ارسال شده توابع امنیتی هدف ارزیابی[1]**

این خانواده تعریف کننده‌ی 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 کدهای اجرایی توابع امنیتی هدف ارزیابی باشد.

- **خانواده یکپارچگی داده‌های ارسال شده توابع امنیتی هدف ارزیابی[2]**

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 می‌شود. 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[3]**

1 Confidentiality of exported TSF data (FPT_ITC)

2 Integrity of exported TSF data (FPT_ITI)

3 Internal TOE TSF data transfer (FPT_ITT)

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

- **خانواده محافظت فیزیکی از توابع امنیتی هدف ارزیابی[1]**

مؤلفه‌های حفاظت فیزیکی توابع امنیتی هدف ارزیابی به محدودیت‌هایی بر روی دستیابی فیزیکی غیرمجاز به توابع امنیتی هدف ارزیابی، بازدارندگی از اصلاح فیزیکی غیرمجاز یا جایگزینی توابع امنیتی هدف ارزیابی و مقاومت در برابر اصلاح فیزیکی غیرمجاز یا جایگزینی توابع امنیتی هدف ارزیابی اشاره دارد.
الزامات مؤلفه‌ها در این خانواده این اطمینان را می‌دهد که توابع امنیتی هدف ارزیابی از مداخله فیزیکی و تداخلات محافظت می‌شود. برآورده شدن این مؤلفه‌ها منجر به بسته‌بندی و استفاده توابع امنیتی هدف ارزیابی به صورتی شود که مداخلات فیزیکی قابل تشخیص باشد و یا مجبور به مقاومت در برابر تداخلات فیزیکی شود. بدون این مؤلفه‌ها، 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[2]**

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 می‌شود و هم‌چنین می‌تواند بازیابی شود. این خانواده بسیار مهم است زیرا وضعیت راه‌اندازی توابع امنیتی هدف ارزیابی تعیین کننده حفاظت از وضعیت‌های بعدی می‌باشد.

- **خانواده شناسایی مجدد[3]**

1 TSF physical protection (FPT_PHP)
2 Trusted recovery (FPT_RCV)
3 Replay detection (FPT_RPL)

این خانواده انواع مختلف موجودیت‌ها (به طور مثال، پیغام‌ها، درخواست‌های سرویس، پاسخ‌های سرویس) و اقدامات بعدی را مجدداً شناسایی می‌کند 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[1]

هدف ارزیابی توزیع شده ممکن است نسبت به هدف ارزیابی واحد، به واسطه اختلاف حالت‌ها بین بخش‌های مختلف هدف ارزیابی و تـأخیر در ارتباطـات دارای پیچیـدگی بیشتر باشد. در اغلب موارد هماهنگ سازی حالت‌ها بین عملکردهای توزیع یافته مستلزم یک پروتکل تبادلی است و یک عمل ساده نیست.
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 امـن اسـتفاده کننـد. پروتکـل همگـام‌سـازی اطمینان می‌دهد که دو بخش توزیعی هدف ارزیابی (به طور مثال، میزبان‌ها) حالت‌هایشان را بعد از اقدامات مرتبط امنیتی همگام می‌کنند.

➢ خانواده مهرهای زمانی[2]

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

➢ خانواده سازگاری داده‌های بین توابع امنیتی هدف ارزیابی[3]

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 را برای به اشتراک‌گذاری و تفسیر سازگار صفات و مجوزها، بین توابع امنیتی هدف ارزیابی مربوط به هدف ارزیابی و یک محصول امن IT متفاوت تعریف می‌کند.

---

1 State synchrony protocol (FPT_SSP)
2 Time stamps (FPT_STM)
3 Inter-TSF TSF data consistency (FPT_TDC)

➢ خانواده آزمون موجودیت‌های خارجی[1]

این خانواده الزاماتی را برای توابع امنیتی هدف ارزیابی تعریف می‌کند تا آزمون‌هایی 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 می‌شوند، سخت‌افزار و نرم‌افزاری که تحت هدف ارزیابی اجرا می‌شوند(پلتفرم‌ها، سیستم‌عامل و ...) یا برنامه‌ها و باکس‌های متصل شده به هدف ارزیابی (سیستم‌های تشخیص نفوذ، دیوارهای آتش، سرورهای ورود، سرورهای زمانی و غیره) باشد.

➢ خانواده سازگاری در تکرار داده‌ها در توابع امنیتی هدف ارزیابی در داخل هدف ارزیابی[2]

الزامات این خانواده از آن جهت لازم و ضروری می‌باشد، تا از سازگاری داده توابع امنیتی هدف ارزیابی زمانی‌که در داخل هدف ارزیابی تکرار می‌شود، اطمینان حاصل کند. منظور از سازگاری داده ها، یکسان بودن داده ها در محلها و توابع مختلف است. داده‌ی توابع امنیتی هدف ارزیابی زمانی ناسازگار می‌شود که کانال داخلی بین بخش‌های مختلف هدف ارزیابی نامعتبر شود. اگر اجزای هدف ارزیابی از نظر داخلی تشکیل یک شبکه دهند، در صورت غیر فعال شدن ارتباطات شبکه‌ای، عدم سازگاری بین داده-های تابع امنیتی می‌تواند رخ دهد.

➢ خانواده خودآزمایی توابع امنیتی هدف ارزیابی[3]

این خانواده الزاماتی را برای خودآزمایی توابع امنیتی هدف ارزیابی با توجه به عملکرد صحیح مورد انتظار تعریف می‌کند. اجبار هدف ارزیابی به انجام آزمون بر روی بخشهای حساس و مهم هدف ارزیابی با استفاده از نمونه عملیات‌های ریاضی مثالی از این الزام می باشد. این‌گونه آزمون‌ها می‌تواند در هنگام راه اندازی، به طور متناوب بنا

1 Testing of external entities (FPT_TEE)

2 Internal TOE TSF data replication consistency (FPT_TRC)

3 TSF self test (FPT_TST)

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 می‌شود.

الزامات این خانواده هم‌چنین برای تشخیص عدم صحت داده‌ی توابع امنیتی هدف ارزیابی و یا خود توابع امنیتی هدف ارزیابی (کد اجرایی یا مؤلفه‌های سخت‌افزاری توابع امنیتی هدف ارزیابی) توسط خرابی‌های مختلفی که لزوماً عملکرد هدف ارزیابی را (که توسط دیگر خانواده‌ها اداره شده‌اند) متوقف نمی‌کنند، مورد نیاز است.

چنین خرابی‌هایی می‌تواند یا به دلیل حالت‌های پیش‌بینی نشده خرابی یا سهل‌انگاری‌های مرتبط در طراحی سخت‌افزار، میان‌افزار یا نرم افزار رخ دهد و یا به دلیل تغییر مخرب توابع امنیتی هدف ارزیابی بر اثر حفاظت منطقی و/یا فیزیکی ناکافی صورت گیرد.

شماره الزام	نام خانواده	عنصر امنیتی
۳۵	انتقال داده های توابع امنیتی هدف ارزیابی در داخل هدف ارزیابی (**FPT_ITT**)	**نام عنصر: انتقال داده های توابع امنیتی هدف ارزیابی در داخل هدف ارزیابی ۱** **شماره مؤلفه: ح‌ت-اد.۱.۱ (FPT_ITT.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید از داده‌های خود در مقابل تغییر در هنگام انتقال میان قسمت‌های مجزای **هدف ارزیابی** محافظت نمایند.
۳۶	مهرهای زمانی (**FPT_STM**)	**نام عنصر: مهرهای زمانی ۱**

شماره الزام	نام خانواده	عنصر امنیتی
		شماره مؤلفه: ح‌ت-م‌ز.۱,۱ (FPT_STM.1.1) **شرح مؤلفه:** توابع امنیتی هدف ارزیابی، باید قادر به ایجاد مهرهای زمانی قابل اطمینان برای استفاده **هدف ارزیابی** باشند.
۳۷	محافظت از داده های توابع امنیتی هدف ارزیابی (FPT_SKP_EXT)	**نام عنصر: محافظت از داده های توابع امنیتی هدف ارزیابی (کلیدهای متقارن) ۱** **شماره مؤلفه: ح‌ت-م‌ح-(ت س).۱,۱ (FPT_SKP_EXT.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید از خوانده شدن تمام کلیدهای از پیش به اشتراک گذارده شده، کلیدهای متقارن و کلیدهای خصوصی جلوگیری کند. **نکته کاربردی:** منظور این الزام آن است که یک مدیر قادر به خواندن یا مشاهده کلیدهای شناسایی شده از طریق واسطهای «معمول» نباشد. درحالی‌که واضح است که یک سرپرست می‌تواند مستقیماً حافظه را بخواند و یا کلیدها را مشاهده کند، اما انجام این امور به سادگی

شماره الزام	نام خانواده	عنصر امنیتی
		صورت نمی‌گیرد و ممکن است به کار قابل توجهی نیاز داشته باشد. از این‌رو سرپرست به عنوان یک عامل امن در نظر گرفته می‌شود و فرض می‌شود که سرپرست نمی‌خواهد در چنین مواردی تلاش کند.
۳۸	حفاظت از کلمه عبور سرپرست (FPT_APW_EXT)	**نام عنصر: حفاظت از کلمه عبور سرپرست ۱** **شماره مؤلفه: ح‌ت-م‌پ-(ت س).۱,۱ (FPT_APW_EXT.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید کلمه‌های عبور را به‌صورت متن آشکار ذخیره نکنند.
۳۹	به‌روزرسانی امن (FPT_TUD_EXT)	**نام عنصر: به‌روزرسانی امن ۱** **شماره مؤلفه: ح‌ت-رم-(ت س)۳,۱ (FPT_TUD_EXT.1.3)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید به وسیله روشی قبل از به‌روزرسانی هدف ارزیابی، با استفاده از [انتخاب: سازو کارهای امضای دیجیتال، مقادیر درهم‌سازی منتشر شده] از صحت به‌روزرسانی نرم افزاری/میان افزاری اطمینان حاصل کنند.

شماره الزام	نام خانواده	عنصر امنیتی
		نکته کاربردی:
		سازوکار امضاء دیجیتال اشاره به سومین الزام در عنصر رز-ع ر.۱(۲) دارد.
		درهم‌سازی منتشرشده توسط یکی از توابع مشخص شده در رز-ع ر.۱(۳) تولید می‌شود.
		نویسنده هدف امنیتی باید سازوکارهای پیاده‌سازی شده توسط هدف ارزیابی را انتخاب کند.
۴۰		**نام عنصر: یکپارچگی و صحت داده‌های ارسال شده توابع امنیتی هدف ارزیابی ۱**
		شماره مؤلفه: ح‌ت-ی‌د.۱،۱ (FPT_ITI.1.1)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید قابلیتی ارائه دهد تا تمام تغییرات داده‌های توابع امنیتی هدف ارزیابی را در طول انتقال بین توابع امنیتی هدف ارزیابی و دیگر محصولات امن فناوری اطلاعات که در محدوده معیار [اختصاص: **معیار تغییرات تعریف شده**] هستند شناسایی کند.
۴۱	یکپارچگی و صحت داده‌های ارسال شده توابع امنیتی هدف ارزیابی	**نام عنصر: یکپارچگی و صحت داده‌های ارسال شده توابع امنیتی هدف ارزیابی ۱**
		شماره مؤلفه: ح‌ت-ی‌د.۲،۱ (FPT_ITI.1.2)

شماره الزام	نام خانواده	عنصر امنیتی
	(FPT_ITI)	شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قابلیتی را ارائه دهد تا یکپارچگی تمام داده‌های توابع امنیتی هدف ارزیابی را که بین توابع امنیتی هدف ارزیابی و دیگر محصولات امن فناوری اطلاعات منتقل می‌شوند بررسی کنند و در صورت شناسایی، تغییر [اختصاص: **اقدامی که باید در برابر تغییر شناسایی شده انجام بگیرد**] انجام بگیرد.

۷,۷ کلاس دسترسی به هدف ارزیابی

نام کلاس: دسترسی به هدف ارزیابی

شرح کلاس: این خانواده الزامات عملیاتی برای کنترل نشست‌های کاربری برقرار شده را مشخص می‌کند.

- **خانواده محدودیت‌های حوزه ویژگی‌های قابل انتخاب**[1]

این خانواده الزاماتی را تعریف می‌کند تا حوزه صفات و ویژگی‌های امنیتی نشست را که کاربر ممکن است برای یک نشست انتخاب کند محدود می‌کند.

- **خانواده محدودیت‌هایی در خصوص چندین نشست همزمان**[2]

این خانواده الزاماتی را تعریف می‌کند که تعداد نشست‌های همزمان متعلق به یک کاربر را محدود می‌کند.

---

1 Limitation on scope of selectable attributes (FTA_LSA)

2 Limitation on multiple concurrent sessions (FTA_MCS)

- **قفل کردن نشست‌های شروع شده توسط توابع امنیتی هدف ارزیابی[1]**

این خانواده الزاماتی را برای توابع امنیتی هدف ارزیابی تعریف کرده است تا قابلیتی را برای قفل کردن، باز کردن و خاتمه نشست‌های تعاملی را که توسط توابع امنیتی هدف ارزیابی و کاربر آغاز شده است تعریف می‌کند.

- **علائم دسترسی هدف ارزیابی[2]**

این خانواده تعریف کننده الزاماتی است تا یک پیغام هشدار مشورتی قابل تنظیم را به کاربران با توجه به استفاده مناسب از هدف ارزیابی نمایش دهد.

- **سوابق دسترسی به هدف ارزیابی[3]**

این خانواده الزاماتی را برای توابع امنیتی هدف ارزیابی تعریف کرده است تا نشست‌هایی را که موفقیت آمیز برقرار شده است، تاریخچه تلاش‌های موفق و ناموفق دستیابی به حساب کاربری را به کاربر نمایش دهد.

- **ایجاد نشست هدف ارزیابی[4]**

این خانواده الزاماتی را تعریف می‌کند تا مجوز کاربری جهت برقراری نشستی با هدف ارزیابی را انکار کند.

1 Session locking and termination (FTA_SSL)
2 TOE access banners (FTA_TAB)
3 TOE access history (FTA_TAH)
4 TOE session establishment (FTA_TSE)

شماره الزام	نام عنصر	مؤلفه امنیتی
۴۲	قفل کردن نشست های شروع شده توسط توابع امنیتی هدف ارزیابی (FTA_SSL)	**نام عنصر: قفل کردن نشست های شروع شده توسط توابع امنیتی هدف ارزیابی ۱** **شماره مؤلفه: دس-ق‌ن-(ت‌س).۱,۱ (FTA_SSL.(EXT).1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید پس از [اختصاص: **یک مدت زمان مشخص غیرفعال بودن**]، برای نشست‌های تعاملی مربوط به سرپرست مرکزی یا کاربر ایستگاه کاری، آن نشست را توسط موارد زیر قفل کند: ۱. پاک کردن و دوباره‌نویسی دستگاه‌های نمایش که سبب غیرقابل خوانده شدن محتویات جاری می‌شود. ۲. غیرفعال‌سازی کلیه فعالیت‌های مربوط به دسترسی داده‌های کاربر و دستگاه‌های نمایش.
۴۳		**نام عنصر: قفل گذاری بر روی نشست ها و خاتمه دادن به آنها ۱** **شماره مؤلفه: دس-ق.۲,۱ (FTA_SSL. 1.2)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی پیش از بازگشایی نشست کاربر ایستگاه کاری یا سرپرست مرکزی، باید ملزم کند که رویداد زیر رخ دهد:

شماره	نام عنصر	مؤلفه امنیتی
ه		
الزام		
		• احراز هویت مجدد
۴۴	علایم دسترسی هدف ارزیابی (FTA_TAB)	**نام عنصر: علایم دسترسی هدف ارزیابی ۱** **شماره مؤلفه: دس-ع‌د.۱,۱ (FTA_TAB.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید پیش از آغاز نشست کاربری، یک پیام هشدار را که بیانگر عدم استفاده غیرمجاز از هدف ارزیابی است را نمایش دهند.

۸,۷ کلاس آنتی‌ویروس

در ادامه مؤلفه‌های امنیتی مورد نیاز کلاس کانال‌ها و مسیرهای مورد اعتماد ارائه شده است.

شماره	نام عنصر	مؤلفه امنیتی
الزام		
۲۸	عملیات آنتی‌ویروس (FAV_ACT_(EXT)	**نام عنصر: عملیات آنتی‌ویروس ۱** **شماره مؤلفه: آو-ع‌ا-(ت‌س).۱,۱ (FAV_ACT_(EXT). 1.1)** **شرح مؤلفه:** بلافاصله پس از تشخیص ویروسی در حافظه، توابع امنیتی هدف ارزیابی باید از اجرای مجدد ویروس جلوگیری کنند.
۲۹		**نام عنصر: عملیات آنتی‌ویروس ۱** **شماره مؤلفه: آو-ع‌ا-(ت‌س).۲,۱ (FAV_ACT_(EXT). 1.2)** **شرح مؤلفه:** به محض شناسایی یک فایل ویروسی، توابع امنیتی هدف ارزیابی باید عمل(های) مشخص‌شده‌ای را توسط سرپرست مرکزی انجام دهند. این اعمال بر اساس هر ایستگاه کاری قابل تنظیم هستند و عبارتند از:

شماره	نام عنصر	مؤلفه امنیتی
	الزام	

- پاک کردن ویروس از فایل
- قرنطینه کردن فایل
- حذف کردن فایل
- [انتخاب: [اختصاص: **لیستی از دیگر اقدامات**]، بدون هیچ اقدام دیگر]

۳۰ **نام عنصر: عملیات آنتی‌ویروس ۱**

شماره مؤلفه: آو-ع۱-(ت‌س).۳,۱.(FAV_ACT_(EXT). 1.3)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید به طور پویا فرآیندهایی را که در تلاش جهت ارتباط با یک سیستم راه دور با استفاده از پورت شماره ۲۵ TCP و یا UDP (SMTP) هستند پایش کند و در عین حالی که اجازه برقراری ارتباط را برای فرآیندهای غیرمجاز مسدود می‌کنند، همزمان به فرآیندهای مجاز، اجازهٔ برقراری ارتباط را بدهد.

۳۱ هشدارهای آنتی- **نام عنصر: هشدارهای آنتی‌ویروس ۱**

شماره	نام عنصر	مؤلفه امنیتی
الزام		
ویروس (FAV_ALR_(EXT))	شماره مؤلفه: آو-ها-(ت‌س).۱,۱ (FAV_ALR_(EXT). 1.1)	
	شرح مؤلفه:	
	به محض شناسایی یک ویروس بر روی ایستگاه کاری، توابع امنیتی هدف ارزیابی باید هشداری را بر روی صفحه نمایش آن نشان دهند. هشدار باید شامل اطلاعات شناسایی ویروس و اقدام متقابل انجام شده توسط هدف ارزیابی باشد.	
	نام عنصر: هشدارهای آنتی‌ویروس ۱	
	شماره مؤلفه: آو-ها-(ت‌س).۲,۱ (FAV_ALR_(EXT). 1.2)	
	شرح مؤلفه:	
	توابع امنیتی هدف ارزیابی باید آنقدر نمایش هشدارها را بر روی صفحه نمایش ایستگاه کاری ادامه دهند تا توسط کاربر آن ایستگاه کاری پذیرفته شوند یا نشست کاربر پایان یابد.	
	نام عنصر: هشدارهای آنتی‌ویروس ۱	
	شماره مؤلفه: آو-ها-(ت‌س).۳,۱ (FAV_ALR_(EXT). 1.3)	

شماره **نام عنصر** **مؤلفه امنیتی**

الزام

شرح مؤلفه:

به محض دریافت یک رویداد ممیزی از یک ایستگاه کاری مبنی بر شناسایی یک ویروس، توابع امنیتی هدف ارزیابی باید در صورت فعال بودن نشست، هشداری را بر روی صفحه نمایش سرپرست مرکزی نشان دهند. هشدار باید منشاء رویدادهای ممیزی در ایستگاه کاری، ویروس شناسایی شده و اقدام مقابله‌ای انجام شده توسط هدف ارزیابی را مشخص کند.

نام عنصر: هشدارهای آنتی‌ویروس ۱

شماره مؤلفه: آو-ه‌ا-(ت‌س).۴,۱ (FAV_ALR_(EXT). 1.4)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید نمایش هشدار را بر روی صفحه نمایش سرپرست مرکزی ادامه دهند تا هشدار توسط وی پذیرفته شود یا نشست او پایان یابد.

نکته کاربردی:

حذف چنین هشدارهای ممیزی در برخی سناریوها لازم و ضروری است (مانند گزارش های متعدد از وجود یک ویروس روی تعداد

شماره	نام عنصر	مؤلفه امنیتی
		الزام
		بسیار زیادی از فایلها) زیرا تعداد زیاد هشدارهای تولید شده باعث از کار افتادن منابع سیستم و خستگی سرپرست می‌شود.سیستم خسته کننده می‌شود و یا منابع سرپرست از شکست جلوگیری می‌کنند. این مؤلفه الزام به پذیرفتن هشدارهای تولید شده توسط سرپرست را دارد. پاسخ دادن به تعداد زیادی از هشدارها، خصوصاً در یک بازه زمانی کوتاه، ممکن است سرپرست را از پاسخگویی مناسب به وقایع کلی منع کند. اگر حذف هشدار به نظر لازم و ضروری آمد، باید سناریوهای مختلفی را که ممکن است رخ دهد تحلیل کند، تا برای حذف هشدار دلیل قانع کننده‌ای پیدا کند. راه حل باید برحسب عواملی هم‌چون نوع هشدار باشد، فاصله زمانی و تعداد هشدار بین قدیمی‌ترین هشدارهای تولید شده و جدیدترین هشدار و هر عامل مرتبط دیگر براساس سناریوهایی که ممکن است رخ دهد. تحلیل استفاده شده‌ای که تعیین می‌کند کدام هشدارهای حذف شده باید به طور کلی در هدف امنیتی مستند شود و در گزارش مربوط به اعتبارسنجی لحاظ شود.
۲۸	انجام اسکن توسط آنتی‌ویروس	**نام عنصر: انجام اسکن توسط آنتی‌ویروس ۱** **شماره مؤلفه: آو-اس-(ت‌س).۱,۱ (FAV_SCN_(EXT). 1.1)**

شماره	نام عنصر	مؤلفه امنیتی
الزام		
(	**شرح مؤلفه:**	
FAV_SCN_(EXT)	توابع امنیتی هدف ارزیابی باید بر اساس امضاهای[1] شناخته شده، اسکن بلادرنگی را برای ویروس‌های مبتنی بر حافظه انجام دهند.	
۲۹	**نام عنصر: انجام اسکن توسط آنتی‌ویروس ۱**	
	شماره مؤلفه: آو-اس-(ت‌س).۲,۱ (FAV_SCN_(EXT). 1.2)	
	شرح مؤلفه:	
	توابع امنیتی هدف ارزیابی باید بر اساس امضاهای شناخته شده، بصورت بلادرنگ، زمانبندی‌شده و در صورت درخواست اسکن فایل را انجام دهد.	
۳۰	**نام عنصر: انجام اسکن توسط آنتی‌ویروس ۱**	
	شماره مؤلفه: آو-اس-(ت‌س).۳,۱ (FAV_SCN_(EXT). 1.3)	
	شرح مؤلفه:	

[1] signature

شماره	نام عنصر	مؤلفه امنیتی

الزام

توابع امنیتی هدف ارزیابی باید اسکن زمانبندی شده‌ای را بر اساس زمان و تعداد دفعاتی که توسط سرپرست مرکزی مشخص شده است، انجام دهند.

۳۱ **نام عنصر: انجام اسکن توسط آنتی‌ویروس ۱**

شماره مؤلفه: آو-اس-(ت‌س).۴,۱ (FAV_SCN_(EXT). 1.4)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قادر به انجام اسکن، در صورت درخواست اسکن توسط کاربر ایستگاه کاری باشد.

۸ الزامات تضمین امنیتی

نام کلاس	نام عنصر	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	آنالیز آسیب‌پذیری

Life cycle Support	ALC_CMC.1	برچسب‌گذاری هدف ارزیابی
	ALC_CMS.1	پوشش پیکربندی هدف ارزیابی

جدول ۷: الزامات تضمین امنیتی

۸,۱ کلاس توسعه

اطلاعات مرتبط 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 می‌شوند یا داده-های احراز هویتی که ممکن است پیمایش کننده اتصال باشد، مقابله می‌کنند (از طریق اتصالات یک به یک هدف ارزیابی یا اتصال هدف ارزیابی به VPN Gateway). هم-چنین ممکن است هدف ارزیابی با توجه به پیکربندی‌اش، پیشنهاد حفاظت از دسترسی غیرمجاز به شبکه پشت هدف ارزیابی کند. علاوه بر واسطهای شبکه لازم است که واسطهای سرپرستی (چگونه هدف ارزیابی پیکربندی می‌شود) شرح داده شود.

۸,۱,۱ مشخصات کارکردی

مشخصات کارکردی، واسطهای کارکرد امنیتی هدف ارزیابی را توصیف می‌کند اما نیازی به شرح مفصل و کاملی از این واسطها نیست. 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 شود.

1 TOE Security Specification

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱	مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1D)** **شرح مؤلفه:** توسعه دهنده باید مشخصات کارکردی را ارائه کند.
۲		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.2D)** **شرح مؤلفه:** توسعه دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه کند. **نکته کاربردی:** مشخصات کارکردی دربرگیرنده اطلاعات مستندات راهنمای کاربردی (AGD_OPE) و راهنمای آماده-

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
		سازی (AGD_PRE) و اطلاعاتی که در بخش «خلاصه مشخصات هدف ارزیابی» سند هدف امنیتی ارائه شده است، می‌باشند. با توجه به دلایلی که باید در مستندات و بخش «خلاصه مشخصات هدف ارزیابی» وجود داشته باشند، الزامات کارکردی تضمین می‌شوند. 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 نیست.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۳	مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجـرا کننـده کـارکرد امنیتـی[1] و پشتیبان کننده‌ی الزام کارکرد امنیتی [2] را توصیف کند.
۴		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.2C)** **شرح مؤلفه:** مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجـرا کننـده کـارکرد امنیتـی و پشـتیبان کننده‌ی الزام کارکرد امنیتی را مشخص کند.
۵		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.3C)**

[1] SFR-enforcing TSFI

[2] SFR-supporting TSFI

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: مشخصات کارکردی باید برای دسته‌بندی ضمنی واسطهای غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه کند.
۶		**نام عنصر: مشخصات کارکرد ابتدایی۱** **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		
شماره الزام	نام خانواده	عنصر امنیتی

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۷	مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌کند.
۸		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.2E)** **شرح مؤلفه:** ارزیاب باید مشخص کند که مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی هستند.

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 ارائه می‌شود(تا مشخص شود که آیا می‌تواند نقش خود را برای کارکرد امنیتی ایفا کند).

برای هر محیط عملیاتی که در سند هدف امنیتی ادعای پشتیبانی از آن شده است باید مستند راهنما ارائه شود. این راهنما شامل موارد زیر است:

- 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

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

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱۰	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 که باید در یک محیط پردازشی امن کنترل شوند را توصیف کند، همانند هشدارهای مناسب.
۱۱		**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.2C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف کند که چگونه از واسط‌های در دسترس ارائه شده توسط هدف ارزیابی به‌صورت امن استفاده می‌شود.
۱۲		**نام عنصر: راهنمای کاربردی ۱**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		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 و مقادیر امن را به‌صورت مناسبی تعیین کند.
۱۳		**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 کند، همانند تغییر مشخصات امنیتی موجودیت-های تحت کنترل توابع امنیتی هدف ارزیابی.
۱۴		**نام عنصر: راهنمای کاربردی ۱**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شماره مؤلفه: (AGD_OPE.1.5C) **شرح مؤلفه:** سند راهنمای کاربردی باید تمام مودهای عملیاتی هدف ارزیابی (مودهایی شامل شکست عملیات یا خطای عملیات)، آثار آنها و الزامشان را برای حفظ عملیات در حالت امن مشخص کند.
۱۵		**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 کند تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده‌اند، کاملاً اجرا شوند.
۱۶		**نام عنصر: راهنمای کاربردی ۱**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شماره مؤلفه: (AGD_OPE.1.7C) **شرح مؤلفه:** سند راهنمای کاربردی باید واضح و قابل فهم باشد.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۱۷	راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده در سند راهنمای کاربردی تمام مؤلفه‌های محتوایی را برآورده می‌کند.

۸,۲,۲ راهنمای آماده‌سازی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱۸	راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1D)** **شرح مؤلفه:** توسعه دهنده باید هدف ارزیابی را همراه با سند آماده‌سازی ارائه کند.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱۹	راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1C)** **شرح مؤلفه:**

مؤلفه‌های اقدامات محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		مستندات آماده‌سازی باید تمام مراحل لازم برای پذیرش امن هدف ارزیابی توسط مشتری را مطابق با رویه‌های تحویل توسعه دهنده شرح دهند.
۲۰		**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.2C)** **شرح مؤلفه:** 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.

مؤلفه‌های اقدامات ارزیاب		
۲۱	راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1E)** **شرح مؤلفه:**

مؤلفه‌های اقدامات ارزیاب		
		ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌کند.
۲۲		**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.2E)** **شرح مؤلفه:** ارزیاب باید رویه‌های آماده‌سازی شرح داده شده در سند را بکار ببرد تا تائید کند، هدف ارزیابی می‌تواند به‌صورت امن برای عمل کردن آماده شود.

۸,۳ کلاس آزمون

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

۸,۳,۱ آزمون مستقل

این دسته از آزمون‌ها برای تائید عملکردی که در بخش «مشخصات امنیتی هدف ارزیابی» و مستندات سرپرستی ارائه شده است، صورت می‌گیرند. تمرکز آزمون‌ها بـر روی برآورده شدن الزامات کارکردی مشخص شده در سند هدف امنیتی می‌باشد. فعالیت‌های تضمین حداقل آزمون‌های مربوط به ایـن بخـش‌هـا را معرفـی مـی‌کنـد و ارزیـاب گزارشی از طرح آزمون و نتایج آن آماده می‌کند.

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۲۳	آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1D)** **شرح مؤلفه:** توسعه دهنده باید برای آزمون ، هدف ارزیابی را ارائه کند.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۲۴	آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱**

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		شماره مؤلفه: (ATE_IND.1.1C) **شرح مؤلفه:** هدف ارزیابی باید مناسب آزمون باشد.

مؤلفه‌های اقدامات ارزیاب		
۲۵	آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده، مؤلفه‌های محتوایی را برآورده می‌کند.
۲۶		**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.2E)** **شرح مؤلفه:**

مؤلفه‌های اقدامات ارزیاب		
		ارزیاب باید زیرمجموعه‌ای از توابع امنیتی هدف ارزیابی را بیازماید تا تائید کند که توابع امنیتی هدف ارزیابی به‌صورت مشخص شده عمل می‌کنند.

۸,۴ کلاس آسیب‌پذیری

برای آماده کردن اولیه این پروفایل حفاظتی، انتظار می‌رود آزمایشگاه‌های ارزیابی با تحلیل هدف ارزیابی، آن دسته از آسیب‌پذیری‌هایی را که در این نوع محصولات یافت شده‌اند بیابند. غالباً 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 این دسته از آسیب‌پذیری‌های هدف ارزیابی را مورد آزمون قرار دهند. آزمایشگاه‌ها انتظار دارند توضیحاتی پیرامون احتمال کلی این دسته از آسیب‌پذیری‌ها در مستنداتی که توسط فروشنده به کاربران ارائه می‌شود لحاظ شود. اینگونه اطلاعات در توسعه ابزارهای آزمون نفوذ و همچنین نسخه‌های بعدی پروفایل‌های حفاظتی مورد استفاده قرار خواهند گرفت.

۸,۴,۱ تحلیل آسیب‌پذیری

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۲۷	آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱**

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
		شماره مؤلفه: (AVA_VAN.1.1D) **شرح مؤلفه:** توسعه دهنده باید برای آزمون ، هدف ارزیابی را ارائه کند.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۲۸	آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1C)** **شرح مؤلفه:** هدف ارزیابی باید مناسب آزمون باشد.

مؤلفه‌های اقدامات ارزیاب

شماره الزام	نام خانواده	عنصر امنیتی
۲۹	آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده، تمام مؤلفه‌های محتوایی را برآورده می‌کند.
۳۰		**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.2E)** **شرح مؤلفه:** ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در هدف ارزیابی، در منابع عمومی جستجویی را انجام دهد.
۳۱		**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.3E)** **شرح مؤلفه:**

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
		ارزیاب باید براساس آسیب‌پذیری‌های بالقوه شناسایی شده، آزمون نفوذ را انجام دهد تا مقاومت هدف ارزیابی را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص کند.

۸,۵ 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 می‌شود که توسط کاربر نهایی قابل مشاهده باشد. این به 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 مؤلفه جهت معرفی هدف ارزیابی به‌صورت مجزا از دیگر محصولات یا نسخه‌ای که توسط فروشنده ارائه شده، است (بدین معنی که جدا از برچسب‌گذاری 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 را که توسط مرکز گواهی تائید شده است به آسانی تشخیص دهد.

مؤلفه‌های اقدامات توسعه دهنده

شماره الزام	نام خانواده	عنصر امنیتی
۳۲	قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMC.1.1D)** **شرح مؤلفه:** توسعه دهنده باید هدف ارزیابی و مرجع هدف ارزیابی را ارائه کند.

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

مؤلفه‌های اقدامات ارزیاب

شماره الزام	نام خانواده	عنصر امنیتی
۳۴	قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMC.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌کند.

۸,۵,۲ حوزه پیکربندی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۳۵	حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMS.1.1D)** **شرح مؤلفه:** ارزیاب باید لیست پیکربندی هدف ارزیابی را ارائه کند.

مؤلفه‌های اقدامات محتوایی

شماره الزام	نام خانواده	عنصر امنیتی
۳۶	حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMS.1.1C)** **شرح مؤلفه:** لیست پیکربندی باید شامل خود هدف ارزیابی و مدارک مورد نیاز توسط الزامات تضمین امنیتی باشد.
۳۷		**نام عنصر: پوشش پیکربندی هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMS.1.1C)** **شرح مؤلفه:** لیست پیکربندی باید موارد پیکربندی را به‌صورت یکتا معرفی کند.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۳۸	حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMS.1.1E)**

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌کند.