به نام خدا

راهنمای آزمایشگاه‌های ارزیابی امنیتی محصولات فتا

مرکز مدیریت راهبردی افتا

مهر ۹۳
نسخه ۱,۰

پیشگفتار

با رشد روز افزون تهدیدات در فضای فناوری اطلاعات، مسئله امنیت جایگاه ویژه‌ای پیدا نموده است. بدین جهت تولیدکنندگان محصولات فناوری اطلاعات، سعی در تولید محصولاتی دارند که با تهدیدات روزافزون مقابله نماید. در این راستا تولیدکننده ادعا می‌نماید که محصول دارای کارکرد امنیتی است. برای تائید ادعای تولید کننده و اخذ گواهی امنیتی، محصول براساس استاندارد ارزیابی معیار مشترک در آزمایشگاه های مورد تائید مرکز افتا و سازمان فناوری اطلاعات ارزیابی می‌گردد.

در این سند چارچوب الزاماتی در رابطه با آزمایشگاه مورد تائید مرکز افتا و سازمان فناوری اطلاعات و روال ارزیابی محصول و نقش و ارتباطات آزمایشگاه در آن شرح داده شده است.

فهرست

۱. هدف از ارائه سند

این سند یکی از مجموعه اسناد «طرح ارزیابی امنیتی» است که به عنوان راهنمای آزمایشگاه‌های ارزیابی امنیتی محصولات فتا توسط مرکز افتا و سازمان فناوری اطلاعات تهیه شده است. هدف از این سند کمک به درک کارمندان آزمایشگاه نسبت به نقش خود پیش از، در طول و پس از ارزیابی محصولات/ پروفایل حفاظتی می‌باشد.

۱,۱ معرفی اصطلاحات

مرجع اصطلاحات بکار رفته در این سند، سند «طرح ارزیابی امنیتی» می باشد.

۲,۱ نقش ها در ارزیابی امنیتی محصولات

به منظور برقراری امنیت در محصولات فناوری اطلاعات، مرکز افتا و سازمان فناوری اطلاعات طرحی را تحت عنوان «طرح ارزیابی امنیتی» تدوین نموده‌اند تا انطباق محصولات فناوری اطلاعات و پروفایل‌های حفاظتی را بر استاندارد ارزیابی معیار مشترک بررسی نمایند.
ذی نفعان اصلی «طرح ارزیابی امنیتی» عبارتند از:

- تولید کننده

تولید کننده محصول یا پروفایل حفاظتی، از سازمان درخواست ارزیابی محصول یا پروفایل حفاظتی می‌نماید.

- آزمایشگاه

آزمایشگاه براساس سند «اعتباربخشی آزمایشگاه» و توسط سازمان و مرکز افتا اعتباربخشی شده و مجوز فعالیت دریافت می‌کند تا براساس استاندارد ارزیابی امنیتی معیار مشترک و با استفاده از متدلوژی ارزیابی معیار مشترک و سایر متدلوژی‌ها، آیین نامه‌ها و دستورالعمل‌های ابلاغی مرکز افتا، ارزیابی امنیتی انجام دهد.

- مرکز افتا

به عنوان یک نهاد دولتی بالاترین سطح در استاندارد ارزیابی معیار مشترک است که منطبق بودن آزمایشگاه‌های ارزیابی امنیتی بر روال‌ها و خط‌مشی‌های این مرکز را بررسی می‌نماید. مرکز افتا برای آزمایشگاه‌های ارزیابی امنیتی، راهنمای فنی ارائه نموده و در حین/پس از ارزیابی آزمایشگاه، انطباق نتایج ارزیابی امنیتی محصولات فتا را با استاندارد ارزیابی معیار مشترک تائید می‌نماید و محصولات

ارزیابی شده توسط آزمایشگاه را جهت صدور گواهی به سازمان فناوری اطلاعات معرفی می‌نماید. مرکز افتا مرجع تفسیر و اصلاح آیین نامه‌ها، دستورالعمل‌ها، روال‌ها و خط مشی‌ها می‌باشد.

- سازمان فناوری اطلاعات

به عنوان یک نهاد دولتی همراه با مرکز افتا بالاترین سطح در استاندارد ارزیابی معیار مشترک است که درخواست ارزیابی محصول از سوی تولید کننده را دریافت و با هماهنگی مرکز افتا به آزمایشگاه ارجاع می‌دهد، همچنین منتشر کننده اسناد عمومی مرتبط با طرح ارزیابی امنیتی بوده و برای محصولی که توسط آزمایشگاه با موفقیت ارزیابی و توسط مرکز افتا تائید شده، گواهی صادر نموده و نام محصول گواهی شده همراه مستندات مربوط به آن منتشر می‌کند.

۳,۱ ساختار سند

این سند یکی از مجموعه اسناد تهیه شده توسط مرکز افتا برای شرح چگونگی عملکرد «طرح ارزیابی امنیتی» می‌باشد و بیان کننده روالهایی است که آزمایشگاه ارزیابی محصولات افتا باید از آنها پیروی نمایند. این سند شامل فصل‌های زیر می‌باشد:

فصل اول: هدف از ارائه سند را شرح می‌دهد. فصل دوم الزامات برای کاندیدا شدن و تائید شدن آزمایشگاه را بیان می‌کند. فصل سوم الزامات آزمایشگاه را شرح می‌دهد.

فصل چهارم: نظارت بر حوزه ارزیابی امنیتی محصولات را بیان می‌کند.

۲. ارزیابی امنیتی محصولات

در این بخش فرایند ارزیابی امنیتی محصولات و اقدامات ذی نفعان طرح ارزیابی امنیتی در طول مراحل مختلف ارزیابی محصول شرح داده می‌شود.

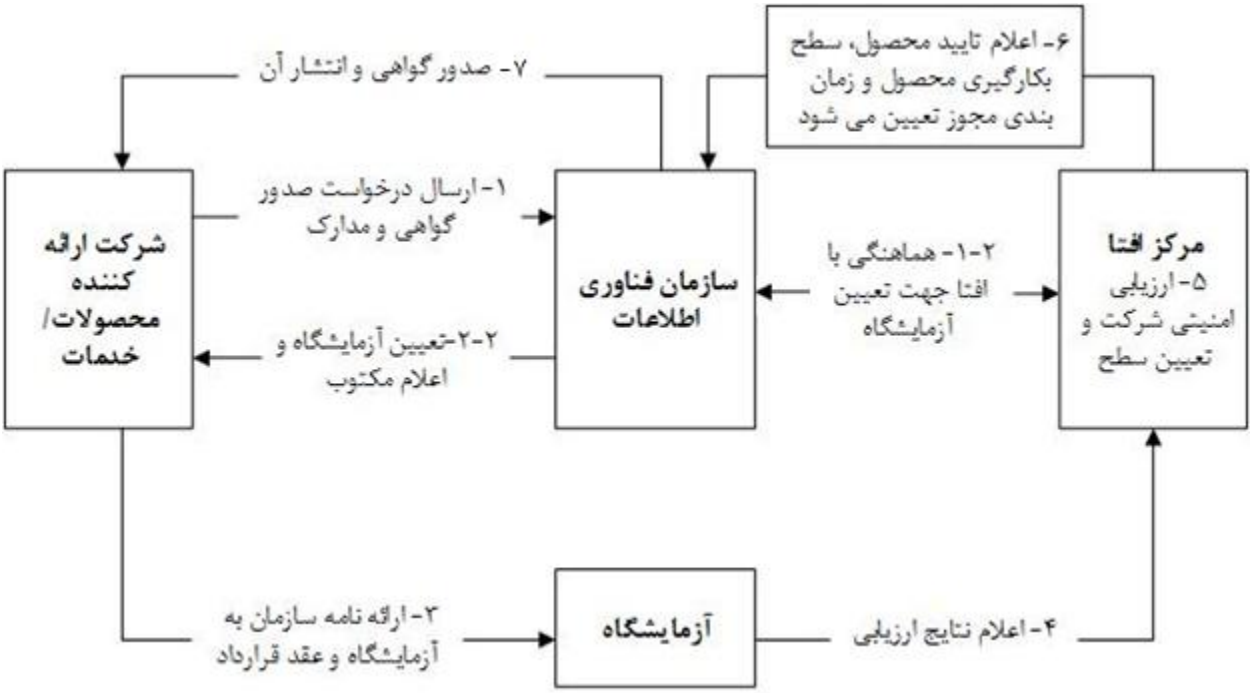
لازم به تاکید است که علاوه بر محصولات، پروفایل‌های حفاظتی نیز باید مورد ارزیابی قرار گیرند. جهت ارزیابی پروفایل حفاظتی لازم است نشان داده شود که این سند بی عیب و نقص و محتوای قسمت‌های مختلف آن باهم سازگار است. ارزیابی پروفایل حفاظتی ممکن است به تنهایی انجام شود (براساس کلاس APE[۱] استاندارد ارزیابی معیار مشترک) یا ممکن است به عنوان بخشی از ارزیابی اولیه محصول در قبال پروفایل حفاظتی صورت گیرد. پروفایل حفاظتی ارزیابی شده و به تأیید رسیده توسط سازمان منتشر می‌شود.

همانگونه که در بخش آزمایشگاه‌ها شرح داده شد آزمایشگاه‌ها باید قادر به انجام ارزیابی بی‌طرفانه در رابطه با برآورده نمودن الزامات امنیتی توسط هدف ارزیابی باشند. این فرآیند تائید می‌کند که ارزیابی مطابق آنچه که در

[۱] Assurance Protection Profile Evaluation

طرح ارزیابی امنیتی ارائه شده، انجام می‌شود و نتایج آزمایشگاه با حقایق ارائه شده در سند «گزارش فنی ارزیابی» سازگار است.

در شکل شماره (۱) فرایند ارزیابی امنیتی محصولات نشان داده شده است.



شکل ۱- فرایند ارزیابی امنیتی محصولات فتا

مطابق شکل شماره (۱) فرایند کلی ارزیابی امنیتی محصولات به شرح ذیل می‌باشد:

۱- تهیه مقدمات ارزیابی و آماده سازی اسناد و مدارک مورد نیاز توسط تولید کننده و مراجعه به سازمان و ارائه درخواست ارزیابی امنیتی محصول

۲- ارجاع درخواست ارزیابی از طرف سازمان به مرکز افتا و تعیین آزمایشگاه با هماهنگی با آن مرکز و اعلام مکتوب به تولید کننده و ارسال رونوشت آن به آزمایشگاه

۳- مراجعه تولید کننده به آزمایشگاه معرفی شده همراه با نامه معرفی سازمان و انعقاد قرارداد بین تولید کننده و آزمایشگاه

۴- انجام ارزیابی امنیتی محصول توسط آزمایشگاه و اعلام نتایج به مرکز افتا

۵- ارزیابی امنیتی شرکت و تعیین سطح فعالیت آن توسط مرکز افتا

۶- اعلام تأیید/عدم تأیید محصول، سطح بکارگیری آن و مدت اعتبار مجوز توسط مرکز افتا به سازمان بر اساس جمع‌بندی نهایی نتایج ارزیابی‌ها که توسط مرکز افتا انجام می‌شود.

۷- صدور گواهی توسط سازمان بر اساس بند ۶ (اعلام نظر مرکز افتا) و انتشار آن

فرایند فوق در چهار فاز اصلی انجام می‌شود که عبارتند از:
فاز اول: آماده سازی
درخواست تولید کننده
توافق اولیه بین آزمایشگاه و تولید کننده

فاز دوم: ارزیابی اسناد هدف امنیتی
بررسی و نهایی سازی سند هدف امنیتی

فاز سوم: ارزیابی فنی
ارزیابی روش تست محصول و روش تست آسیب‌پذیری

فاز چهارم: پایان ارزیابی محصول
صدور گواهی
نگهداری

تذکر: آزمایشگاه‌هایی که در فرایند ارزیابی امنیتی محصول معرفی می‌شوند، قبلاً مطابق سند <<اعتبار بخشی آزمایشگاه>> از سازمان و مرکز افتا گواهی فعالیت دریافت کرده و مورد تأیید آن دو نهاد هستند.

در ادامه با جزئیات بیشتر فعالیت های ارزیابی و اعتباربخشی شرح داده شده است.

۱,۲ فاز اول: آماده‌سازی

۱,۱,۲ درخواست تولید کننده

هدف فاز اول تعیین مناسب بودن هدف ارزیابی، می‌باشد. در این مرحله تولید کننده براساس سند "راهنمای تولید کننده" درخواست خود را برای ارزیابی محصول به سازمان فناوری اطلاعات ارسال نموده و سازمان پس از انجام اقدامات مورد نیاز و هماهنگی با مرکز افتا، آزمایشگاهی را برای ارزیابی آن محصول به تولید کننده معرفی می نماید.

۲,۱,۲ توافق اولیه بین آزمایشگاه و تولید کننده

حداقل الزامات لازم برای شروع ارزیابی یک محصول عبارتند از:

- معرفی نامه سازمان به تولیدکننده جهت ارزیابی در آزمایشگاه معرفی شده

- عقد قرارداد ارزیابی بین آزمایشگاه و تولید کننده (الزامات مرکز افتا که در قرارداد ارزیابی محصول باید رعایت شوند در ابلاغیه «راهنمای قرارداد ارزیابی امنیتی محصول» بیان شده است)
- تأیید سند هدف امنیتی در مرکز افتا
- هدف ارزیابی قابل قبول برای ارزیابی

برای برآورده کردن موارد مذکور، تولید کننده پس از تعیین آزمایشگاه، به آزمایشگاه مربوطه مراجعه می‌نماید. تولید کننده برای ارزیابی محصول در آزمایشگاه باید معرفی نامه سازمان را به آزمایشگاه تعیین شده ارائه دهد.
آزمایشگاه باید همزمان با عقد قرارداد، ضمن اطلاع رسانی به مرکز افتا، مسئول گروه ارزیابی آن محصول را نیز معرفی نماید.
در این مرحله توافقات و هماهنگی‌های زیر بین آزمایشگاه و تولید کننده انجام می‌پذیرد:

- تهیه سند هدف امنیتی شامل شرح عملکرد محصول و اطلاعات حوزه فیزیکی و منطقی محصول توسط تولید کننده و توافق بر روی آن
- توافق بر روی روالهای ارتباطی و تعیین افراد رابط توسط تولید کننده
- توافق بر روی کلیت طرح کاری ارزیابی توسط آزمایشگاه و تولید کننده
- توجیه تولیدکننده در رابطه با روال ارزیابی توسط آزمایشگاه

تولید کننده مسئول ارائه سند هدف امنیتی و محصول مورد ارزیابی (هدف ارزیابی) می‌باشد. ساختار هدف ارزیابی ممکن است متنوع بوده و از سخت‌افزار، نرم‌افزار و میان‌افزار تشکیل شده باشد. همچنین ممکن است هدف ارزیابی ترکیبی از چندین محصول فناوری اطلاعات باشد. تولید کننده باید تمام مستندات لازم را در اختیار آزمایشگاه قرار دهد تا ارزیابی با موفقیت انجام گیرد. آزمایشگاه نیز می‌باید متعهد گردد که در کلیه مراحل ارزیابی، صرفاً اطلاعات مربوط به ارزیابی محصول (مطابق با دستورالعمل‌های ابلاغی) را درخواست نماید و نسبت به تأمین امنیت فناوری اطلاعات و ارتباطات آزمایشگاه و حفاظت از اطلاعات مرتبط با ارزیابی امنیتی محصولات و عدم افشاء اطلاعات[۲] اطمینان دهد و نتایج ارزیابی امنیتی محصولات باید در سیستم‌هایی که از نظر فیزیکی از شبکه اینترنت، مجزا هستند، نگهداری نموده و ضوابطی مناسب و مورد تائید مرکز افتا برای حفاظت از اطلاعات را اعمال نماید. در صورت اختلاف میان آزمایشگاه و تولید کننده در خصوص نوع، میزان، نحوه تحویل و حفظ اطلاعات و نیز هر گونه اختلافی در مرحله ارزیابی محصول توسط آزمایشگاه، مرکز افتا در این خصوص قضاوت خواهد کرد.
در ادامه این مرحله باید برآورده شدن الزامات لازم برای سند هدف امنیتی بررسی گردد. در این زمینه مرکز افتا ابلاغیه‌ای تحت عنوان «پذیرش سند هدف امنیتی در ارزیابی» ارائه نموده است. سه قسمت «شرح هدف ارزیابی» و «الزامات کارکرد امنیتی» و «مشخصه‌های امنیتی هدف ارزیابی» در سند هدف امنیتی باید دقیق

[۲] -Non-Disclosure Agreement (NDA)

نوشته شوند تا منعکس کننده‌ی کارکرد محصول باشد. همچنین باید اطلاعات جزئی لازم برای انجام ارزیابی نیز ارائه گردد. آزمایشگاه در ابتدا مطابقت ساختار کلی سند هدف امنیتی با قالب تعریف شده در «راهنمای نوشتن پروفایل حفاظتی/سند هدف امنیتی» را بررسی و سپس محتوای سند را براساس کلاس ASE[۳] مورد ارزیابی قرار می‌دهد، و نتایج ارزیابی را برای مرکز افتا ارسال می‌نماید.
هنگامیکه سند هدف امنیتی محصول، ادعای انطباق به یک پروفایل حفاظتی معتبر دارد و نگاشت مستقیمی بین محتوای آنها وجود دارد، آزمایشگاه ممکن است با مبنا قرار دادن پروفایل حفاظتی معتبر و ارزیابی شده، نیازی به ارزیابی بیشتر برای کلاس ASE نداشته باشد. اما در صورت عدم انطباق کامل سند هدف امنیتی با پروفایل حفاظتی، آزمایشگاه برای بررسی الزامات کلاس ASE، پروفایل حفاظتی را به صورت دقیق مبنا قرار می‌دهد. لازم به ذکر است نویسنده سند هدف امنیتی ممکن است جزئیات و قابلیت‌های بیشتری نسبت به پروفایل حفاظتی در نظر بگیرد.

۲,۲ فاز دوم: ارزیابی اسناد هدف ارزیابی

۱,۲,۲ مرحله بررسی و نهایی‌سازی سند هدف امنیتی

در این مرحله و پس از تکمیل موفقیت آمیز کلاس ارزیابی سند هدف امنیتی توسط آزمایشگاه، این سند باید به تأیید مرکز افتا برسد تا اطمینان حاصل شود که سند هدف امنیتی به درستی و با شفافیت دقیق تهیه شده و مطابق با سیاستهای آن مرکز می‌باشد. در این راستا آزمایشگاه بسته «بررسی و نهایی سازی سند هدف امنیتی» را تهیه و برای مرکز افتا ارسال می نماید. این بسته شامل سند هدف امنیتی و گزارش تست ارزیابی آن و نیز مستندات راهنمای کار با محصول (در صورت وجود) و کلیه مستندات آماده شده توسط تیم ارزیابی در این زمینه می‌باشد. گزارش تست ارزیابی سند هدف امنیتی باید مبین این باشد که تمام الزامات لازم در کلاس ASE به درستی برآورده شده‌اند. مرکز افتا مستندات دریافتی را بررسی و در صورت لزوم اقدام به برگزاری جلسه‌ای برای رفع ابهامات می‌نماید که در آن جلسه ارزیاب آزمایشگاه و نماینده تولید کننده حضور خواهند داشت.

۲,۲,۲ جلسه نهایی‌سازی سند هدف امنیتی و شروع ارزیابی

هدف از این جلسه بررسی و نهایی‌سازی سند هدف امنیتی و بیان نقش و وظایف تولید کننده، آزمایشگاه و مرکز افتا (به عنوان ناظر)، بیان انتظارات هر سه بخش و توافق بر روی زمانبندی و طرح کاری ارزیابی می‌باشد. در این جلسه نمایندگان مرکز افتا، آزمایشگاه و تولید کننده شرکت می‌کنند. ورودی جلسه، سند هدف امنیتی، گزارشات ارزیابی سند هدف امنیتی، سوالات تیم ارزیابی، قرارداد، زمانبندی و طرح کاری ارزیابی و خروجی آن

[۳] Assurance Security target Evaluation
کلاس ASE یکی از چندین کلاس تضمین استاندارد ارزیابی معیار مشترک می‌باشد، در این کلاس الزاماتی برای سند هدف امنیتی تعریف شده است.

تأیید سند هدف امنیتی و گزارش ارزیابی آن توسط مرکز افتا، تأیید زمانبندی و طرح کاری ارزیابی توسط هر سه بخش و تنظیم صورتجلسه است.

در این جلسه ابتدا ارزیاب باید در ارتباط با سند هدف امنیتی و اثبات اینکه این سند کلیه الزامات مورد نیاز طرح ارزیابی امنیتی را برآورده می‌کند، شرح و توضیح دهد. در این ارائه، مطالب زیر باید توسط ارزیاب بیان گردند:

- شرح حوزه فیزیکی و منطقی هدف ارزیابی
  - تمام اجزای محیطی مورد نیاز هدف ارزیابی، اجزای هدف ارزیابی و اجزای محیطی باید به صورت شفاف بیان گردند و با هم نیز سازگار باشند.
  - بیان تمام وابستگی های امنیتی که هدف ارزیابی ممکن است نسبت به محیط داشته باشد.
- بیان حوزه کارکردهای امنیتی هدف ارزیابی
- بیان مدل‌ها/پیکربندی‌های استفاده از محصول
- بیان تمام تعاملات بین اجزای هدف ارزیابی و محیط، نظیر پروتکل‌ها، صحت داده، حفاظت از افشاء داده، احراز هویت نقطه پایانی، حفاظت از تکرار داده. در نظر گرفتن چنین فاکتورهایی در هدف ارزیابی توزیع شده یا مستقر در یک سیستم، بسیار مهم می‌باشد.
- بیان چگونگی پیاده سازی الزامات کارکرد امنیتی در هدف ارزیابی
  - این بیان حداقل باید بر روی عملکرد سازوکارهای ارزیابی که برای دست یافتن به الزامات کارکرد امنیتی استفاده می‌شوند، متمرکز گردد.
  - تنها برشمردن الزامات کارکرد امنیتی یا ارائه نگاشتی از عملکرد امنیتی و الزامات کارکرد امنیتی کافی نمی‌باشد؛ بلکه ارزیابی باید قادر به توصیف معماری و عملکرد هدف ارزیابی با جزئیات کافی باشد به طوری که امنیت محصول را به طور منطقی توجیه نماید.
- شرح و تصمیم گیری در مورد کامل بودن و شمول هر یک از الزامات کارکرد امنیتی بیان شده
- بیان کارکرد امنیتی رمزنگاری و الزامات مربوطه
- برای هر یک از سیاستهای کارکرد امنیتی انواع کاربران و ویژگیهای آنها بیان شود.
- بیان هر تغییر صورت گرفته در محصول به خاطر الزامات ایجاد شده در هدف امنیتی برای محصول در بازه بررسی هدف امنیتی در آزمایشگاه
- بیان و شرح اثبات پذیرش سند هدف امنیتی بر اساس ابلاغیه «راهنمای پذیرش سند هدف امنیتی»
- بیان و شرح اثبات پذیرش هدف ارزیابی بر اساس ابلاغیه «راهنمای پذیرش هدف ارزیابی»

پس از آنکه فاز ارزیابی سند هدف امنیتی با موفقیت طی شد، موارد زیر باید مشخص شود:

- برنامه طرح کاری ارزیابی محصول توسط آزمایشگاه
- پروتکلهای ارتباطی بین سه بخش
- افراد ارزیاب
- زمانبندی تحویل گزارش‌های ارزیابی

پس از تعیین موارد فوق، محصول وارد فاز ارزیابی امنیتی می‌گردد.

۳,۲,۲ ارزیابی اسناد مرتبط با هدف ارزیابی

در این مرحله آزمایشگاه اسناد لازم برای ارزیابی امنیتی محصول را از تولید کننده دریافت می‌نماید و الزامات آورده شده در بخش سوم استاندارد ارزیابی مشترک برای کلاسهای توسعه، چرخه حیات و راهنمای کاربر را بر روی آنها بررسی می‌نماید و در صورت لزوم نیز اقدام به بازدید از محل تولید کننده و بررسی ارزیابی روالهای الزامی می‌نماید. در هر مورد آزمایشگاه نقصانهای موجود را به تولید کننده اعلام نموده و تولید کننده موظف به رفع ابهامات و برطرف کردن نواقص می‌باشد. یک نسخه از تمام اسناد، گزارشها و مکاتبات در این مرحله باید توسط آزمایشگاه در همان زمان به مرکز افتا ارسال شود.

آزمایشگاه در این مرحله محصول را از تولید کننده دریافت می‌نماید و صحت برخی مستندات مربوطه را بررسی می‌کند. همچنین در صورت نیاز از تولید کننده درخواست آموزش استفاده و پیکربندی محصول را می‌نماید و تولید کننده موظف به ارائه آموزش‌های درخواستی می‌باشد. لازم به ذکر است که تولید کننده باید اطلاعات فنی محصول را در اختیار تیم ارزیابی قرار دهد، پس از موفقیت محصول در کلاسهای مذکور، آزمایشگاه گزارش این کلاسها را برای مرکز افتا ارسال می‌نماید و وارد فاز ارزیابی فنی محصول می‌گردد. لازم به ذکر است در این مرحله کلیه الزامات کلاس توسعه مورد بررسی قرار نگرفته و الزاماتی که نیاز به بررسی فنی دارند در فاز ارزیابی فنی مورد بررسی قرار می‌گیرند.

۳,۲ فاز سوم: ارزیابی فنی

قبل از شروع این فاز، آزمایشگاه باید بسته‌ای در اختیار مرکز افتا قرار دهد. این بسته شامل مستندات تمام اقدامات صورت گرفته می‌باشد. این مستندات به عنوان ورودی اصلی در ارزیابی‌های آزمایشگاه به کار می‌روند.

فاز ارزیابی فنی شامل دو بخش «روش تست محصول» و «روش تحلیل آسیب‌پذیری» می‌باشد. تا پیش از این فاز کلاس‌های ASE[۴]، AGD[۵] و بخشی از کلاس‌های ADV[۶] و ALF[۷] پوشش داده شده است. در ادامه دیگر بخش‌های کلاسهای ADV و ALF و دو کلاس ATE[۸] و AVA[۹] پوشش داده می‌شود.

۴ - کلاس ارزیابی هدف امنیتی

۵ - کلاس مستندات راهنما

۱,۳,۲ ارزیابی روش تست محصول

در این بخش باید اقدامات انجام گرفته در کلاس‌های ADV و ATE بررسی گردد. از آنجا که شناسایی صحیح کارکرد امنیتی هدف ارزیابی و واسطهای کارکرد امنیتی برای تست مهم می‌باشند، فاز ارزیابی فنی مربوط به این حوزه همراه با طرح تست می‌باشد.

پس از اطمینان حاصل شدن از آنکه سند هدف امنیتی تمام مولفه‌های ارزیابی را برآورده نموده، تیم ارزیابی دیدکلی نسبت به طرح تست تولیدکننده به دست می‌آورد و می‌تواند با استفاده از «سند هدف امنیتی»، «راهنمای کار با محصول» و «مستندات توسعه»، طرح تست تیم ارزیابی را پایه ریزی و برنامه ارزیابی را تدوین و زمانبندی نماید. پس از آن اقدام به اعلام طرح تست خود برای مرکز افتا می‌کند.

آزمایشگاه (ارزیاب) باید موارد زیر را قبل از شروع تست محصول به مرکز افتا ارائه نماید:

- مستنداتی که نتایج فاز ارزیابی سند هدف امنیتی را بیان می‌دارند.
- سند هدف امنیتی بروزرسانی شده
- گزارش ارزیابی بروز شده تمام مواردی از کلاسهایASE، ADV و ATE و AGD که با موفقیت ارزیابی شده‌اند. لازم است تا این مرحله، تمام عنصرهایی که انجام خانواده تست مستقل در کلاس ارزیابی تست[۱۰] به آنها وابسته است، مورد ارزیابی قرار گرفته باشند و گزارش ارزیابی آنها تهیه شده باشد.
- طرح تست تیم ارزیابی شامل:
  - مدل/پیکربندی تست
  - زمانبندی تست
  - روش تست کارکردی
  - موارد مورد نیاز برای هر تست کارکردی شامل:
    - شرایط اولیه تست
    - توصیف مراحل تست با جزئیات کافی جهت بررسی موثر بودن تست
    - نتایج مورد انتظار تست

۶ - کلاس توسعه
۷ - کلاس چرخه حیات
۸ - کلاس ارزیابی تست
۹ - کلاس تحلیل آسیب‌پذیری
۱۰ -ATE-IND

- تمام مستندات تست تولید کننده
- مشخصات کارکردی محصول، مستندات طراحی و تحلیل تست پوشش
- ثبت فعالیت‌های صورت گرفته توسط تیم ارزیابی
- معرفی تیم ارزیابی
- گزارش تغییرات سند هدف امنیتی نسبت به نسخه ابتدایی

۱,۱,۳,۲ نظارت بر تست

مرکز افتا بر تست‌هایی که ارزیاب‌های آزمایشگاه انجام می‌دهند، نظارت می‌کند. مجموعه تست باید شامل برخی از تست‌های تولید کننده و همچنین برخی از تست‌های مستقل (تست‌هایی که ارزیاب انجام می‌دهد) باشند. مرکز افتا باید منطبق بودن نتایج تست با گزارش سند تست تولید کننده را تأیید نماید.

۲,۳,۲ ارزیابی روش تحلیل آسیب‌پذیری

هدف از تحلیل آسیب‌پذیری، بررسی آسیب‌پذیری‌های بالقوه در محصول و تحلیل اثر چنین آسیب‌پذیری‌هایی بر روی امنیت محصول می‌باشد. ارزیاب براساس نتایج تحلیل آسیب‌پذیری و درکی که از تحلیل سند هدف امنیتی، مستندات کلاس توسعه، مستندات و رویه‌های کاربری و همچنین تست کارکردی هدف ارزیابی به دست می‌آورد، طرح تحلیل آسیب پذیری و تست نفوذ را تهیه می‌نماید. این طرح باید پس از تکمیل فاز تست تهیه و به مرکز افتا تحویل داده شود.

ارزیاب باید موارد زیر را دو هفته قبل از جلسه اعتبارسنجی روش تحلیل آسیب‌پذیری به مرکز افتا ارائه نماید:

- سند هدف امنیتی بروزرسانی شده
- گزارش ارزیابی بروز شده تمام مواردی از کلاس‌های ADV و ATE و AGD که با موفقیت ارزیابی شده‌اند. لازم است تا این مرحله، تمام عنصرهایی که انجام عنصر AVA-VAN به آنها وابسته است، مورد ارزیابی قرار گرفته باشند و گزارش ارزیابی آنها تهیه شده باشد.
- گزارش نهایی تست
- گزارش طرح تحلیل آسیب‌پذیری
- موارد طرح تست نفوذ تیم ارزیابی شامل:
  - مدل/پیکربندی تست نفوذ
  - زمانبندی تست نفوذ

- روش تست نفوذ
- موارد مورد نیاز برای هر تست نفوذ شامل:
  - شرایط اولیه تست نفوذ
  - توصیف مراحل تست نفوذ با جزئیات کافی
  - نتایج مورد انتظار تست نفوذ
- ثبت فعالیت‌های صورت گرفته توسط تیم ارزیابی
- معرفی تیم ارزیابی

۱,۲,۳,۲ جلسه بررسی اعتبارسنجی روش تحلیل آسیب‌پذیری

هدف از برگزاری این جلسه تأیید طرح تست نفوذ و تحلیل آسیب‌پذیری است و شرکت کنندگان آن مرکز افتا و آزمایشگاه می‌باشند. ورودی جلسه سند هدف امنیتی، مستندات جلسات قبلی، گزارش ارزیابی، گزارش تست، گزارش تحلیل آسیب‌پذیری، طرح تست نفوذ و ملاحظات مرکز افتا بوده و خروجی آن تأیید طرح تست نفوذ و گزارش تحلیل آسیب‌پذیری می‌باشد.

ارزیاب باید موارد زیر را برای ارائه به نماینده مرکز افتا آماده نماید:

- هر تغییری که در سند هدف امنیتی نسبت به جلسه قبل رخ داده است.
- مشخص نمودن طرح تست نفوذ تیم ارزیابی
- هر مورد مهم ارزیابی که پس از آخرین جلسه یافت شده است.
- بیان هر تغییر صورت گرفته در محصول به خاطر الزامات ایجاد شده در محصول در بازه بررسی محصول در آزمایشگاه

۲,۲,۳,۲ نظارت بر تحلیل آسیب‌پذیری

مرکز افتا بر فرایند تست نفوذ نظارت می‌نماید.

۴,۲ فاز چهارم: پایان ارزیابی محصول

پس از پایان ارزیابی فنی، آزمایشگاه باید بسته‌ای در اختیار مرکز افتا قرار دهد. این بسته شامل مستندات تمام اقدامات صورت گرفته می‌باشد. این مستندات به عنوان ورودی اصلی جهت تایید ارزیابی در مرکز افتا به کار می‌روند. مرکز افتا مستندات این فاز را بررسی و ملاحظات مورد نظر را پیش از «جلسه بررسی اعتبارسنجی نهایی» به آزمایشگاه ارائه می‌نماید، تا در این جلسه مورد استفاده قرار گیرد و بتوان با استفاده از آن گزارش «جلسه بررسی اعتبارسنجی نهایی» را تهیه نمود. برای تکمیل ارزیابی لازم است این مرحله با موفقیت طی شود.

این فاز متمرکز بر نتایج تست تیم ارزیابی است و نسبت به برطرف شدن تمام موارد مطرح شده قبلی اطمینان می‌دهد.

اقداماتی که ارزیاب پیش از جلسه باید انجام دهد:

- ارزیاب باید موارد زیر را سه هفته قبل از جلسه به مرکز افتا ارائه نماید:
  - سند هدف امنیتی نهایی
  - گزارش نهایی ارزیابی و نسخه پیش‌نویس گزارش اعتبارسنجی
  - تمام مستنداتی که موارد صورت گرفته در فازهای قبلی را بیان می‌نمایند.
  - نتایج تیم تست
  - ارائه اسناد تیم ارزیابی
  - تمام مدارک نهایی تولید کننده

- ارزیاب باید به تمام سوالات و ابهامات مرکز افتا پاسخ دهند.

۱,۴,۲ جلسه بررسی اعتبارسنجی نهایی

هدف از برگزاری جلسه، بررسی نتایج تست است. موضوع اصلی جلسه، نتایج تست، گزارش نهایی ارزیابی، سوالات و پیشنهادات مربوطه می‌باشد. در این جلسه مرکز افتا، آزمایشگاه و تولید کننده حضور خواهند داشت. ورودی جلسه سند هدف امنیتی نهایی، گزارش ارزیابی نهایی، مستندات جلسات قبلی، نتایج تست، ملاحظات مرکز افتا است. در این جلسه ارزیاب باید موارد زیر را به صورت رسمی ارائه دهد:

- مشخص نمودن هرتغییر در سند هدف امنیتی نسبت به فاز قبلی
- بیان رویدادهای مهم که در طول تست رخ داده است:
  - بیان هر تستی که موفق نبوده و با همکاری تولید کننده رفع شده و آنچه که آزمایشگاه در قبال آن انجام داده است.
  - بیان و شرح هر انحرافی که نسبت به طرح تست رخ داده است.
- بیان هر تغییر صورت گرفته در محصول به خاطر الزامات ایجاد شده در محصول در بازه بررسی محصول در آزمایشگاه.
- محصول تعریف شده در سند هدف امنیتی کاملاً در گزارش ارزیابی منعکس شده و این گزارش به طور کامل نتایج ارزیابی را منعکس می‌نماید.

- بیان و شرح الزاماتی که در تست پوشش داده نشده‌اند.

در پایان این جلسه، آزمایشگاه نسخه پیش‌نویس «گزارش نتایج ارزیابی امنیتی محصول» را تهیه نموده و به مرکز افتا ارسال می‌نماید تا آن مرکز در مورد صدور/ عدم صدور گواهی محصول، تصمیم گیری نماید و آن مرکز بر اساس جمع بندی نتایج ارزیابی‌ها، محصول را برای صدور/ عدم صدور گواهی به سازمان معرفی می‌کند و سازمان در صورت مثبت بودن نظر مرکز افتا گواهی محصول را صادر و منتشر می‌نماید.

تذکر: همانگونه که ذکر گردید، آزمایشگاه صرفاً ارزیابی امنیتی محصول را بر عهده داشته و گواهی برای محصولات صادر نمی‌کند و در مواردی که تولید کننده‌ای خارج از فرایند ارزیابی امنیتی محصولات، مستقیما برای ارزیابی امنیتی محصولی به آزمایشگاه مراجعه نماید، آزمایشگاه پس از اطلاع به مرکز افتا صرفاً مجاز به انجام ارزیابی امنیتی و تحویل نتایج آن به تولید کننده و مرکز افتا می‌باشد و به هیچ عنوان حق ارائه و یا صدور هیچ نوع گواهی برای محصول ندارد.

۳. الزامات آزمایشگاه

آزمایشگاه‌های ارزیابی امنیتی باید الزامات زیر را برآورده نمایند:

- الزامات مطرح شده در سند «راهنمای اعتباربخشی آزمایشگاه»
- دارا بودن معیارهای مشخص شده برای ارزیابی امنیتی و دیگر الزامات طرح ارزیابی امنیتی تعریف شده که در سند «راهنمای آزمایشگاه‌ها» مطرح شده است
- موارد مطرح شده در تعهدنامه اخذ شده از آزمایشگاه
- انجام ارزیابی امنیتی بر اساس استانداردها، آیین نامه‌ها، مقررات و ضوابط ابلاغی مرکز افتا
- پایبندی به شرایطی که بر اساس آنها اعتبار بخشی شده است
- ارائه نتایج ارزیابی امنیتی محصولات، صرفاً به مرکز افتا و تولید کننده
- تأمین امنیت فناوری اطلاعات و ارتباطات آزمایشگاه و حفاظت از اطلاعات مرتبط با ارزیابی امنیتی محصولات و عدم افشاء اطلاعات[۱۱] و نگهداری نتایج ارزیابی امنیتی محصولات در سیستم‌هایی که از نظر فیزیکی از شبکه اینترنت، مجزا هستند.
- رعایت انصاف و بی طرفی و حفظ استقلال آزمایشگاه
- انجام ارزیابی امنیتی در حداقل زمان ممکن
- حفظ رکورد: هر آزمایشگاه ملزم به انجام ارزیابی و مستند نمودن آن در سامانه کیفی خود می‌باشد. در پایان انجام هر فعالیت، نتایج مستند و به عنوان رکورد در سامانه کیفی آزمایشگاه وارد می‌شود. هر

[۱۱] -Non-Disclosure Agreement (NDA)

رکورد باید شامل اطلاعات در مورد افراد انجام دهنده کار و تاریخ انجام کار باشد. این رکوردها به عنوان بخشی از فرایند نظارت بر اعتبارسنجی توسط اعتبارسنج به کار برده می‌شود. رکوردهای آزمایشگاه برای اعتبارسنج در طول اعتبارسنجی مهم و حیاتی هستند.

- در صورتی که آزمایشگاه برای انجام بخشی از فرایند ارزیابی امنیتی محصول نیاز به مشاور یا پیمانکار داشته باشد، می‌باید قبلاً با ذکر جزئیات به اطلاع مرکز افتا رسانده و پس از تأیید آن مرکز در خصوص استفاده از پیمانکار/ مشاور و نیز تأیید صلاحیت آن‌ها، اقدام نماید.
- .....

۴. نظارت بر ارزیابی امنیتی محصولات

همانگونه که در سند <<طرح ارزیابی امنیتی>> ذکر شد، نظارت بر ارزیابی امنیتی محصولات در چند سطح انجام می‌شود که یکی از این سطوح، نظارت بر فرایند ارزیابی امنیتی محصولات می‌باشد. این نظارت، نظارت بر فرایند ارزیابی امنیتی محصولات و پایش عملکرد ذی نفعان می‌باشد. پس از آنکه فرایند ارزیابی امنیتی آغاز می‌شود، مرکز افتا بر عملکرد ذی نفعان نظیر تولید کننده و آزمایشگاه نظارت می‌کند. در طول ارزیابی امنیتی محصول مراحل مختلفی طی خواهد شد که نقطه پایانی هر مرحله به عنوان یک نقطه بازبینی و تأیید در نظر گرفته می‌شود. رفتن به مرحله بعد منوط به انجام کامل مرحله قبل و تأیید آن توسط مرکز افتا می‌باشد. برخی از نقاط بازبینی عبارتند از:

- پایان نهایی سازی سند هدف امنیتی و شروع ارزیابی
- بازبینی متدهای تست و متدهای بررسی آسیب پذیری
- گزارش نهایی ارزیابی
- .....

هدف از این نظارت آن است که اطمینان حاصل شود کلیه طرفهای درگیر در این فرایند، وظایف خود را به درستی انجام می‌دهند و به استانداردها، خط مشی‌ها، آیین نامه‌ها، مقررات، روالها و دستورالعمل‌های ابلاغی پایبند هستند. این نظارت در کل فرایند ارزیابی انجام می‌شود و بدیهی است که تأیید نتایج ارزیابی آزمایشگاه و مجوز صدور گواهی محصولات منوط به آن می‌باشد. بدین منظور نماینده/ نمایندگانی از سوی مرکز افتا جهت نظارت در فرایند ارزیابی امنیتی محصولات معرفی می‌شوند و آزمایشگاه موظف است کلیه مستندات و اطلاعات لازم را در اختیار آنان قرار دهد. همچنین نامبردگان در صورت نیاز در کلیه مراحل انجام ارزیابی امنیتی حضور خواهند داشت. این نظارت در بخش‌های مختلف فرایند ارزیابی امنیتی محصولات در بخش (۲) این سند، در هر مرحله شرح داده شد. در پایان نتایج نهایی ارزیابی محصولات نیز بایستی به تأیید آن مرکز برسد.