برگه درخواست ارائه پیشنهاد (RFP)

معاونت پژوهش و توسعه ارتباطات علمی

عنوان پروژه	**توسعه و استقرار آزمایشگاه ارزیابی امنیت، کارکرد و کارایی سامانه‌های ضد بدافزار**
پژوهشکده	امنیت فناوری طلاعات و ارتباطات
گروه	آزمایشگاه امنیت
تاریخ	**۱۴۰۳/۰۳/۰۵**

مقدمه (شامل انگیزه تعریف پروژه و سوابق آن):

ارزیابی محصولات شبکه و بصورت خاص محصولات حوزه امنیت شبکه، بدلیل اهمیت کاربردهای این محصولات در بخش‌های حساس و حیاتی از اهمیت ویژه‌ای برخوردار است. ارزیابی این محصولات هم برای توسعه‌دهندگان محصول و هم برای کاربران حوزه‌های مختلف این محصولات، تاییدپذیری و اطمینان را بدنبال دارد.

به دلیل اهمیت ضد بدافزارها در امنیت سایبری، در سه دهه گذشته شرکت‌های متعددی در حوزه تولید انواع ضد بدافزارها فعالیت داشته‌اند و با پیدایش انواع ضد بدافزارها، نیاز جدی به استانداردسازی، ارزیابی و رتبه‌بندی آنها ایجاد شده‌است. در سطح بین‌المللی، آزمایشگاه‌ها و شرکت‌هایی که در دو دهه اخیر در بحث ارزیابی امنیت و عملکرد ضد بدافزار ظهور یافته‌اند، به سرعت رشد یافته و نقش کلیدی و حیاتی در این حوزه دارند. در بخش‌های مرتبط با ارزیابی امنیتی سامانه‌های ضدبدافزار، آزمایشگاه‌های معیار مشترک بر مبنای اصول استانداردهای CC و CEM (استاندارد معیارمشترک ISO/15408 و استانداردISO/IEC 18045) و پروفایل‌های حفاظتی تدوین شده، مرجع اصلی ارزیابی امنیتی محصولات ضدبدافزار هستند و در بخش ارزیابی عیارسنجی (کارکرد/ کارآیی) آزمایشگاه‌های تخصصی معتبری همچون AV Comparatives و AV-Test و سازمان استانداردهای تست آنتی ویروس AMTSO بعنوان مراجع اصلی و معتبر حوزه ارزیابی ضدبدافزار، فعالیت می‌نمایند. در داخل کشور نیز محصولات بومی در این حوزه تولید شده‌اند که ارزیابی امنیتی و عیارسنجی (کارآیی و کارکردهای) آنان در کنار محصولات معتبر بین المللی و ارایه گواهینامه‌های قابل استناد برای محصولات ضد بدفزار، به‌خصوص در بکارگیری این محصولات در سازمان‌ها و نهادهای حیاتی و حساس، ضروری است و با توجه به محدودیت‌های این حوزه و تحریم‌های خارجی، امکان ارزیابی محصولات داخلی در آزمایشگاه‌های بین المللی به سختی میسر می‌شود و تاکنون محقق نشده است.

آزمایشگاه امنیت پژوهشگاه ارتباطات و فناوری اطلاعات در پژوهشکده امنیت، پروژه‌های مختلفی را با هدف ارزیابی امنیت و عملکرد سامانه‌ها و محصولات حوزه فتا به انجام رسانده است و آزمایشگاه‌های تخصصی ارزیابی سامانه‌های مختلف این حوزه را درحال خدمت رسانی دارد، پروژه جاری در راستای توسعه و استقرار این آزمایشگاه‌ها در حوزه تخصصی ارزیابی محصولات ضدبدافزار، اجرایی می‌گردد.

۱ هدف پروژه:

با توجه به مطالعات و بررسی‌های انجام گردیده و بررسی نیازهای کشور متناسب با سیاست‌های برنامه توسعه و نیز همسویی با برنامه و مأموریت وزارت ارتباطات و سازمان‌های زیر مجموعه، اعلام نیاز نهادهای دولتی مانند زیرساخت‌های ارتباطی و متقاضیان بخش خصوصی (تولید کننده‌های تجهیزات و محصولات حوزه ضد بدافزار بومی)، پروژه طراحی، پیاده‌سازی و استقرار آزمایشگاه ارزیابی ضد بدافزار با اهداف کلان ذیل انجام می‌پذیرد:

- ایجاد مرجعیت در ارزیابی امنیتی، کارکرد و کارایی ضد بدافزارهای ایرانی و خارجی پرکاربرد در کشور بر اساس استانداردها و روش‌های آزمون و ارزیابی آزمایشگاه‌های معتبر جهانی
- ایجاد مرجعیت در ارزیابی امنیتی ضد بدافزارهای ایرانی و خارجی پرکاربرد در کشور بر مبنای آخرین نسخه استاندارد معیار مشترک و روال‌های ارزیابی آزمایشگاه‌های CC
- امکان ارزیابی آن دسته از تجهیزات بومی یا وارداتی نرم‌افزاری شبکه مانند UTM و Firewall که دارای زیر سامانه ضد بدافزار داخلی هستند.
- تلاش در تحصیل نقش و جایگاه بین‌المللی در تراز آزمایشگاه‌های معتبر جهانی ضدبدافزار
- تلاش در یکپارچه‌سازی و خودکارسازی بخشی از فرایندهای ارزیابی ضدبدافزار در آزمایشگاه امنیت

این پروژه نهایتاً با هدف استقرار دو آزمایشگاه ارزیابی امنیت و ارزیابی عیارسنجی محصولات ضد بدافزار اجرایی می‌گردد.

۲ تعاریف و اختصارات

کلمه اختصاری	عبارت کامل	ترجمه فارسی	توضیح
AC	Activity Report	گزارش فعالیت	گزارش نتایج ارزیابی توسط ارزیاب مطابق با روش ارزیابی معیار مشترک
OR	Observation Report	گزارش مشاهدات	گزارش موارد "بی نتیجه" و "رد" واحدهای کاری که همراه یک پاراگراف حکم توجیهی که نظر ارزیاب را شرح می‌دهد
ETR	Evaluation Technical Report	گزارش فنی ارزیابی	گزارش نتایج ارزیابی فنی محصول توسط ارزیاب.
EWP	Evaluation Work Plan	طرح کار ارزیابی	طرحی که بر اساس نگاشت بین ISO 18045 و ISO 15408 تهیه می‌شود و شامل حداقل واحدهای کاری است که ارزیاب باید انجام دهد.
WU	Work Unit	واحد کاری	هراقدام کاری مندرج در طرح کار ارزیابی که ارزیاب باید انجام دهد.
TOE	Target of Evaluation	هدف ارزیابی	به قلمرو تعیین شده در محصول مورد ارزیابی براساس "استاندارد ارزیابی معیارهای مشترک" هدف ارزیابی گفته می‌شود.
PP	Protection Profile	پروفایل حفاظتی (نمایه حفاظتی)	سندی که الزامات امنیتی و کارکردی محصول هدف را بصورت کلی بیان می‌کند.
ST	Security Target	هدف امنیتی	سندی شامل الزامات امنیتی برای هدف ارزیابی خاص که الزامات امنیتی را بصورت جزئی‌تر بیان می‌کند. این سند توسط توسعه دهنده TOE نوشته می‌شود.
Non-TOE	Non- Target of Evaluation	غیر هدف ارزیابی	سخت‌افزار، نرم‌افزار و میان‌افزاری که در استقرار محصول هدف در محیط آزمون نیاز می‌باشند.
SP	Security Problem	مسائل امنیتی	در سندهای ST و PP بخشی تحت عنوان مسائل امنیتی وجود دارد که بطور رسمی ماهیت و حوزه امنیت در نظر گرفته شده توسط TOE را تعریف می‌کند که شامل موارد زیر است. • تهدیدهایی که توسط TOE و محیط عملیاتی مقابله می‌شود. • سیاست امنیت سازمانی که توسط TOE و محیط عملیاتی اجرا می‌شود.

کلمه اختصاری	عبارت کامل	ترجمه فارسی	توضیح
			• فرضیاتی که برای محیط عملیاتی TOE تایید می‌شوند.
TA	Threat Agent	عوامل تهدید	موجودیت‌هایی که می‌توانند بر روی دارایی ها تهدید محسوب می‌گردند.
OSP	Organizational Security Policy	سیاست‌های امنیتی سازمانی	مجموعه‌ای از قوانین که توصیف کننده رفتار امنیتی خاصی هستند. این قوانین توسط "توابع امنیتی هدف ارزیابی" اجرا شده و بصورت مجموعه‌ای از "الزامات کارکردی امنیت" توسط سازمان بهره‌بردار محصول ارائه می‌شوند.
SO	Security Objective	اهداف امنیتی	اهداف امنیتی که برای مقابله با تهدیدهای معرفی شده، برآورده کردن سیاست‌های امنیتی سازمان و/یا فرضیات معرفی شده در ST و PP ارائه می‌شوند.
SR	Security Requirement	الزامات امنیتی	الزاماتی که به زبان استاندارد بیان شده و هدف آن حاصل شدن اهداف ارزیابی برای TOE می‌باشد.
SFR	Security Functional Requirement	الزامات کارکرد امنیتی	بیان کننده کارکردهای امنیتی TOE در قالب کلاس می‌باشد.
SAR	Security Assurance Requirement	الزامات تضمین امنیتی	این دسته از الزامات تضمین می‌کنند که الزامات کارکردی امنیتی توسط TOE برآورده می‌شوند
	Package	بسته (مجموعه الزامات تعیین شده)	نام مجموعه‌ای از الزامات کارکرد امنیتی یا تضمین امنیتی (مانند EAL-۲) است
EAL	Evaluation Assurance Level	سطح تضمین ارزیابی	مجموعه‌ای از الزامات تضمین که نشان دهنده سطح امنیتی محصول می‌باشد. سطوح تضمین از سطح ۱ تا ۷ هستند.
TSFs	TOE Security Functional	توابع امنیتی هدف ارزیابی	بخشی از TOE که برای اجرای صحیح "الزامات کارکرد امنیتی" باید به آن متکی بود. این توابع شامل بخشی از سخت‌افزار، نرم‌افزار و میان‌افزارهای TOE است که بطور مستقیم و غیرمستقیم برای اجرا شدن امنیت باید به آنها متکی بود.
TSF Data	TSF Data	داده‌های توابع امنیتی هدف ارزیابی	داده هایی برای عملیات هدف ارزیابی که اجرای الزامات کارکرد امنیتی وابسته به آن ها است. این داده ها اطلاعات استفاده شده توسط توابع امنیتی TOE هستند.

کلمه اختصاری	عبارت کامل	ترجمه فارسی	توضیح
User Data	User Data	داده‌های کاربری	داده‌های کاربری که عملکرد توابع امنیتی TOE را تحت تاثیر قرار نمی‌دهند. این داده ها اطلاعات ذخیره شده در منابع TOE هستند که توسط کاربران مطابق با الزامات کارکرد امنیتی بکار برده می‌شوند.

۳ قلمرو پروژه (شامل مشتری پروژه، قلمرو منطقی، قلمرو فیزیکی، فناوری مورداستفاده و سایر الزامات نظیر مشخصات فنی):

از آنجا که هدف از انجام این پروژه ارزیابی امنیتی برای محصولات پیشرو و نوین ضد بدافزار می‌باشد، قلمرو این پروژه شامل مطالعه، تحقیق، طراحی، پیاده‌سازی و استقرار آزمایشگاه ارزیابی امنیتی و عیارسنجی براساس ویژگی‌های محصولات ضدبدافزار و تدوین مستندات و روال‌های ارزیابی امنیتی، عیارسنجی (کارکردی و کارایی) محصول هدف و استقرار این دو آزمایشگاه در محل آزمایشگاه‌های امنیت پژوهشگاه ارتباطات می‌باشد. این امر مشتمل بر استقرار رویه‌های تست، نصب و راه اندازی ابزارهای آزمون‌های مختلف، تولید پایگاه داده‌ها و مجموعه‌های داده تست، مورد نیاز هر یک از روال‌های ارزیابی و انجام تست محصول نمونه جهت بازبینی فرایندها و روال‌های آزمون و رفع نواقص می‌باشد. همچنین در ابعاد این پروژه طراحی و پیاده‌سازی "پلتفرم یکپارچه خودکار ارزیابی ضد بدافزار" جهت خودکارسازی برخی فرایندهای ارزیابی و نمایش نتایج ارزیابی‌ها در قالب نمودارها و گزارشات مورد نیاز، درنظرگرفته شده است. شایان ذکر است در ابعاد این پروژه خرید تجهیزات سخت/نرم‌افزاری برای ارزیابی سامانه‌های ضد بدافزار و راه‌اندازی آزمایشگاه‌های مطرح شده در این RFP مدنظر نیست و استقرار آزمایشگاه و طراحی و پیاده‌سازی روال‌های تست بر مبنای تجهیزات موجود در آزمایشگاه امنیت پژوهشگاه و ابزارهای غیر تجاری و دیتاست‌های تولید شده توسط مجری پروژه صورت می‌پذیرد.

۴ مراحل اجرا و شرح خدمات پروژه

مرحله اول: طراحی، پیاده‌سازی و استقرار آزمایشگاه ارزیابی امنیت ضدبدافزار بر مبنای CC (۶ ماه)

این مرحله شامل طراحی و استقرار زیرساخت و فرایندهای گام به گام و کامل (از درخوست توسعه دهنده برای ارزیابی محصول تا صدور گواهینامه) آزمایشگاه‌های ارزیابی امنیتی ضد بدافزار بر مبنای استاندارد معیار مشترک(CC) مستخرج از بخش‌های لازم از آخرین نسخه استانداردهای ISO 15408 و ISO 18045 با بهره‌مندی از طرح‌های معتبر ارزیابی بر اساس آزمایشگاه‌های معیار مشترک کشورهایی مانند کانادا، آلمان، سوئد، ژاپن، انگلستان، هند، سنگاپور و ... می‌باشد. پس از استقرار آزمایشگاه، تست محصول نمونه توسط مجری انجام می‌شود که این محصول با توافق کارفرما، انتخاب می‌گردد و مراحل ارزیابی امنیتی بر مبنای طرح ها و مستندات تهیه شده، به طور کامل در مورد آن اجرا شده و نتایج به کارفرما ارائه می‌شود. همچنین در این فاز طراحی "پلتفرم یکپارچه خودکار ارزیابی ضد بدافزار" انجام خواهد شد که پیاده سازی و تست آن در فاز دوم پیش بینی شده است.

فعالیت‌های پیش‌بینی‌شده برای این مرحله عبارتند از :

۱. امکان سنجی نیازمندی‌های آزمون، در راستای تدوین طرح تست و روال‌های آزمون‌های ارزیابی امنیت ضد بدافزار متناسب با ابزارها و تجهیزات موجود در آزمایشگاه
۲. به‌روزرسانی و تدوین لیست آسیب‌پذیرهای امنیتی سامانه و زیر سامانه‌های ضد بدافزار
۳. به‌روزرسانی و تدوین الزامات کارکردی امنیت برای سامانه و زیر سامانه‌های ضد بدافزار
۴. به‌روزرسانی و ارتقاء پروفایل حفاظتی سامانه ضد بدافزار برای اجرای ارزیابی در سطح تضمین ۳ (EAL3)
۵. تدوین نیازمندی‌های اجرایی ارزیابی کلاس‌های الزامات عملکرد امنیتی و الزامات تضمین امنیتی

- تدوین قالب مستندات مکمل، شامل سند هدف امنیتی (ST) و تمامی مستندات پشتیبان از توسعه دهندگان و ارائه دهندگان محصولات به آزمایشگاه و قالب تمامی گزارش‌های لازم از زمان ارسال درخواست توسعه دهنده برای ارزیابی هدف ارزیابی (TOE) به مرجع صدور گواهی‌نامه تا خاتمه ارزیابی توسط آزمایشگاه و تأیید و صدور گواهینامه (مطابق روال اعلامی آزمایشگاه امنیت).
- تدوین طرح کاری ارزیابی[۱](EWP) بر اساس نگاشت بین ISO 15408 و ISO 18045 شامل تمامی واحدهای کاری[۲](WU) لازم برای اجرای ارزیابی در سطح تضمین ۳ (EAL3) توسط ارزیابان

۶. تدوین طرح تست مستقل (عملکردهای امنیتی-SFRها) و طرح آزمون آسیب‌پذیری برای ارزیابی هدف ارزیابی امنیتی (TOE) در محیط آزمایشگاه توسط ارزیاب‌ها (برای محصولات بومی و وارداتی).

[۱] Evaluation Work Plan
[۲] Work Unit

۷. طراحی زیرساخت لازم برای اجرای فرآیندهای آزمون‌های امنیتی (برای محصولات بومی و وارداتی) شامل:

- طراحی بستر آزمون برای اجرای کامل"طرح کاری ارزیابی".
- طراحی بستر آزمون برای اجرای "تست مستقل" و " آزمون آسیب‌پذیری".
- تدوین لیست ابزارهای مورد نیاز به منظور انجام ارزیابی ضدبدافزارها بر اساس طرح کاری ارزیابی و اجرای آزمون مستقل و آزمون آسیب‌پذیری با استفاده از تجهیزات موجود آزمایشگاه و ابزارهای آزمون متن باز و ... .

۸. تهیه دیتاست‌ها و اطلاعات ورودی لازم برای ارزیابی کلاس‌ها و زیرکلاس‌های الزامات عملکرد امنیتی در انجام آزمون‌های اعلامی، شامل حداقل موارد زیر:

- دیتا ست بدافزارهای مبتنی بر فایل از خانواده‌های مختلف بدافزاری
- دیتا ست بدافزارهای مبتنی بر حافظه
- دیتا ست بدافزارهای فشرده شده
- دیتا ست بدافزارهایی که حالت ماندگاری در سیستم دارند
- دیتا ست بدافزارهای مورد استفاده در حملات فیشینگ

۹. استقرار زیرساخت و فرآیندهای آزمون‌های امنیتی شامل:

- آماده‌سازی بستر ارتباطی سخت افزار/میان‌افزار/نرم‌افزاری شامل نصب و راه‌اندازی تجهیزات شبکه، سرورها و کلاینت‌ها و نصب و پیکربندی‌های نرم‌افزارهای مرتبط
- توسعه و پیاده‌سازی ابزارهای ارزیابی امنیتی مورد نیاز مانند:
  - CryptographyTool
  - Web Crawler
  - PCMark
- نصب و راه‌اندازی ماشین‌های مجازی و دیگر ابزار مورد نیاز.

۱۰. انجام ارزیابی کامل محصول (TOE) نمونه (با توافق کارفرما) شامل:

- اجرای "طرح کاری ارزیابی" در سطح تضمین۳ (EAL3) (مندرج در جدول ۱ " اجزاء ارزیابی در سطح ۳ تضمین" در پیوست الف و نیز مطابق روال اعلامی آزمایشگاه در این خصوص)
- اجرای تست مستقل روی TOE نمونه
- اجرای آزمون آسیب‌پذیری روی TOE نمونه
- تهیه گزارش کامل و ارائه مستندات و نتایج حین اجرای ارزیابی به عنوان "گزارش های میانی " در قالب اسناد و گزارش‌هایی مانند، سند (TRP)، گزارش فعالیت (AR)، گزارش مشاهدات(OR)اسناد نتایج آزمون آسیب‌پذیری (VTR) و سند ارزیابی فنی محصول (ETR).
- تصحیح و تکمیل گزارش‌ها و انجام اصلاحات مورد نظر کارفرما (با مشارکت توسعه دهنده و تیم ارزیاب مجری) و تکرار تا نهایی شدن ارزیابی.

۱۱. طراحی "پلتفرم یکپارچه خودکار ارزیابی ضد بدافزار" بر مبنای روش‌های آزمایشگاه‌های معتبر جهانی شامل:

- تدوین طرح کلان سیستمی و زیرسیستم‌های پلتفرم یکپارچه ارزیابی شامل ورودی‌ها/خروجی‌ها، طرح مفهومی، طرح سیستمی و عملیاتی و طرح فنی این پلتفرم با جزییات کامل(طرح کلان پیشنهادی شامل ۴ بخش زیر است)

- طراحی ماژول دریافت: ابزارها و واسطهای نرم/سختافزاری لازم برای انتقال مجموعه دادهها به پلتفرم و یکپارچه سازی این ماژول (تعبیه) در چارچوب پلتفرم اصلی
- طراحی ماژول پایگاه دانش: جهت ذخیره، بازیابی و بروزرسانی مجموعه دادهها، مستندات، فرمها، و نتایج ارزیابی و یکپارچه سازی این ماژول (تعبیه) در چارچوب پلتفرم اصلی
- طراحی ماژول یکپارچه سازی و ارزیابی خودکار: یکپارچه سازی ابزارهای خودکارسازی تست در پلتفرم اصلی
- طراحی ماژول نمایش خروجیها: ابزارها و واسطهای نرمافزاری، کدها و اسکریپتهای لازم برای تولید انواع گزارش و نمودارها و نمایش و چاپ مستندات خروجی و نمایش نتایج ارزیابی بهصورت خودکار، در قالب متن، جداول و نمودارهای مصوب

مرحله دوم: طراحی، پیادهسازی و استقرار آزمایشگاه عیارسنجی (کارکرد/کارآیی) ضدبدافزار (۶ ماه)

طراحی و استقرار زیرساخت و فرایندهای آزمایشگاه عیارسنجی (کارکرد/کارایی) ضد بدافزار بر اساس استانداردهایی مانند IETF،AMTSO... و همچنین روالهای آزمایشگاههای برتر AV-Test، AV-Comparative، MRG-Effitas ، ISCA-Labs، SE-Labs و رویکردهای منابع معتبر نظیر PC Magazine(PC Mag)، Virus Bulletinو... . پس از استقرار آزمایشگاه، تست محصول نمونه توسط مجری انجام میشود که این محصول با توافق کارفرما، انتخاب میگردد و مراحل آزمون عیارسنجی(کارکرد/کارآیی) بر مبنای طرح ها و مستندات تهیه شده، به طور کامل در مورد آن اجرا شده و نتایج به کارفرما ارائه میشود. همچنین در این فاز پیاده سازی، استقرار و تست "پلتفرم یکپارچه خودکار ارزیابی ضد بدافزار" انجام خواهد شد که طراحی آن در فاز اول انجام شده است.

فعالیتهای پیشبینیشده برای این مرحله عبارتند از:

۱. امکان سنجی آزمایشگاه امنیت پژوهشگاهICT، در راستای تدوین طرح تست و روالهای آزمونهای عملکردی ضد بدافزار متناسب با ابزارها و تجهیزات موجود در آزمایشگاه
۲. تدوین شاخصهای کارکردی سامانههای ضد بدافزار
۳. تدوین شاخصهای کارایی سامانههای ضد بدافزار
۴. طراحی روشهای تست و عیارسنجی شاخصهای کارکردی سامانه ضد بدافزار
۵. طراحی روشهای تست و عیار سنجی شاخصهای کارایی سامانه ضد بدافزار
۶. تدوین نیازمندیهای اجرایی تست و عیارسنجی شاخصهای کارکردی و کارایی
۷. تدوین لیست ابزارهای مورد نیاز برای ارزیابی ضدبدافزارها بر مبنای روش تستهای طراحی شده برای تست و عیارسنجی شاخصهای کارکرد و کارایی و ابزارها و تجهیزات موجود آزمایشگاه
۸. آماده سازی بستر ارتباطی سختافزار/میان افزار/نرمافزاری جهت انجام آزمونها.
۹. نصب و راهاندازی ماشینهای مجازی و دیگر ابزارهای مورد نیاز آزمون.

۱۰. آماده‌سازی بسترهای لازم برای اجرای روش‌های تست و عیارسنجی ضد بدافزارها شامل:

- پیاده‌سازی و اجرای ابزارهای ارزیابی امنیتی، کارکرد و کارایی و یکپارچه‌سازی در "پلتفرم یکپارچه خودکار ارزیابی ضد بدافزار" مانند:
  - Sand Box
  - Yara Engine
  - File Copy Tester
  - App Install Tester
  - App Launch Tester
  - App Download Tester
  - Website Visit Tester
  - Archive Tester
  - AV Test Suite
- آماده‌سازی بستر آزمون عیارسنجی شاخص‌های کارکرد مندرج در جدول شماره ۲ در پیوست الف و نه محدود به آن‌ها
- آماده‌سازی بستر آزمون عیارسنجی شاخص‌های کارآیی مندرج در جدول شماره ۳ در پیوست الف و نه محدود به آن‌ها

۱۱. تهیه دیتاست‌های مورد نیاز برای انجام آزمون‌های کارکردی

۱۲. تهیه دیتاست‌های مورد نیاز برای انجام آزمون‌های معیارهای کارایی

۱۳. پیاده سازی، یکپارچه‌سازی و تست "پلتفرم یکپارچه خودکار ارزیابی ضد بدافزار" طراحی شده در فاز ۱ برای اجرای آزمون‌های ارزیابی امنیت، کارکرد و کارایی

۱۴. تهیه مستندات مورد نیاز جهت ارزیابی امنیت، عملکرد و کارایی ضد بدافزار

۱۵. انجام آزمون‌های عیارسنجی (مطابق لیست نهایی معیارهای تعیین شده)، مرتبط با شاخص‌های مندرج در جدول ۲ و جدول ۳ در پیوست الف (این شاخص‌ها در روند مطالعات پروژه تکمیل و اصلاح می‌گردد) روی محصول نمونه با استفاده از "پلتفرم یکپارچه خودکار ارزیابی ضد بدافزار" ، بازنگری و اعمال اصلاحات در روال‌های تست در صورت لزوم و ارائه نتایج تست در قالب متن، جدول و نمودارهای مصوب

۱۶. تست و ارزیابی نمونه TOE محصولات ضد بدافزار بر مبنای معیار مشترک (ارزیابی امنیتی) به صورت خودکار توسط "پلتفرم یکپارچه خودکار ارزیابی ضد بدافزار" ، بازنگری و اعمال اصلاحات در روالهای تست در صورت لزوم و ارائه نتایج تست در قالب متن، جدول و نمودراهای مصوب

۵ خروجی‌های هر مرحله از اجرای پروژه

خروجی‌های پیش‌بینی‌شده برای هر یک از مراحل اجرای پروژه، عبارت‌اند از :

خروجی‌های مرحله اول:

خروجیهای مرحله اول متناظر با شرح خدمات تبیین شده در بند ۴ RFP برای فاز اول، بصورت کامل در نظر گرفته می‌شود که شامل موارد ذیل می‌باشند:

۱. استقرار زیرساخت طراحی شده برای آزمایشگاه ارزیابی امنیتی سامانه و زیرسامانه‌های ضد بدافزار بر مبنای استاندارد معیار مشترک (CC)، مطابق با طراحی آماده شده، ارائه گزارش کامل نحوه استقرار و راهنمای ارزیابی

۲. لیست به‌روز آسیب پذیرهای امنیتی برای سامانه و زیر سامانه‌های محصولات ضدبدافزار

۳. پروفایل حفاظتی محصولات ضدبدافزار برای ارزیابی در سطح تضمین ۳ (EAL 3)

۴. قالب‌های طراحی شده برای تمامی گزارش‌های لازم از زمان ارسال درخواست از طرف توسعه دهنده به مرجع صدور گواهی‌نامه برای ارزیابی"هدف ارزیابی(TOE) " تا خاتمه ارزیابی توسط آزمایشگاه و تأیید و صدور گواهینامه .

۵. نیازمندیهای کامل برای انجام ارزیابی سامانه و زیرسامانه‌های ضد بدافزار

۶. مستندات طرح کاری ارزیابی(EWP) ، طرح تست مستقل و طرح آزمون آسیب‌پذیری

۷. گزارش آماده سازی و انجام موارد زیر برای اجرای ارزیابی در سطح تضمین۳ (EAL 3) همراه با نحوه آماده‌سازی، آموزش و راهنمای کاربری هر مورد:

- آماده سازی بستر ارتباطی (سخت‌افزار، میان افزار و نرم افزار)
- لیست ابزارهای مورد نیاز، به‌منظور انجام ارزیابی ضدبدافزارها بر مبنای طرح‌های ارایه شده و زیر ساخت آزمایشگاه امنیت
- گزارش نصب و راه‌اندازی ماشین‌های مجازی و دیگر ابزارها مورد نیاز
- گزارش آماده سازی بستر آزمون برای اجرای طرح کاری ارزیابی، تست مستقل و آزمون آسیب‌پذیری
- دیتاست ها و سایر اطلاعات مورد نیاز اجرای طرح کاری ارزیابی، تست مستقل و آزمون آسیب‌پذیری
- گزارش توسعه و پیاده سازی ابزارها

۸. گزارش انجام ارزیابی کامل محصول(TOE) نمونه (با توافق کارفرما) در سطح تضمین ۳ (EAL 3) شامل:

- گزارش اجرای طرح کاری ارزیابی
- گزارش اجرای تست مستقل
- گزارش اجرای تست نفوذ
- گزارش کامل و ارائه مستندات و نتایج حین اجرای ارزیابی به عنوان "گزارش های میانی " در قالب اسناد و گزارش‌هایی مانند، سند (TRP)، گزارش فعالیت (AR)، گزارش مشاهدات(OR) اسناد نتایج آزمون آسیب‌پذیری (VTR) و سند ارزیابی فنی محصول (ETR)

۹. طرح "پلتفرم یکپارچه خودکار ارزیابی ضد بدافزار" شامل طراحی سیستمی، عملیاتی و فنی سامانه و زیر سامانه‌ها، واسط‌های ارتباطی و ... مطابق با شرح خدمات بند ۴

خروجی‌های مرحله دوم:

خروجیهای مرحله دوم متناظر با شرح خدمات تبیین شده در بند ۴ RFP برای فاز دوم، بصورت کامل در نظر گرفته می‌شود که شامل موارد ذیل می‌باشند:

۱. استقرار کامل زیرساخت طراحی شده آزمایشگاه عیارسنجی(کارکرد /کارایی) مطابق با طراحی و روالهای تدوین شده و ارائه گزارش کامل نحوه استقرار و راهنمای ارزیابی
۲. لیست به‌روز شاخص‌های کارکرد و کارآیی سامانه‌های ضد بدافزار
۳. گزارش روال تست‌ها و عیارسنجی شاخص‌های کارکرد/ کارآیی سامانه ضد بدافزار
۴. گزارش نیازمندیهای اجرایی تست و عیار سنجی شاخص‌های کارکرد و کارایی
۵. لیست ابزارهای مورد نیاز برای ارزیابی ضدبدافزارها بر مبنای روش تست‌های طراحی شده برای تست و عیارسنجی شاخص‌های کارکرد و کارایی
۶. گزارش آماده سازی و انجام موارد زیر برای اجرای آزمون عیارسنجی(عملکرد/کارآیی) بر مبنای طرح تست تدوین شده، همراه با نحوه آماده‌سازی، آموزش و راهنمای کاربری هر مورد:
   - آماده سازی بستر ارتباطی (سخت‌افزار، میان افزار و نرم افزار)
   - لیست ابزارهای مورد نیاز، به‌منظور انجام ارزیابی ضدبدافزارها بر مبنای طرح ارایه شده و زیرساخت آزمایشگاه امنیت
   - گزارش نصب و راه‌اندازی ماشین‌های مجازی و دیگر ابزارها مورد نیاز
   - گزارش آماده سازی بستر آزمون برای اجرای طرح عیارسنجی(کارکرد/ کارآیی)
   - دیتاست ها و سایر اطلاعات مورد نیاز اجرای طرح عیارسنجی
   - گزارش توسعه و پیاده سازی ابزارها
۷. پیاده‌سازی، توسعه[1] و استقرار "پلتفرم یکپارچه خودکار ارزیابی ضدبدافزار"(طراحی شده در فاز ۱)، برای اجرای آزمون‌های ارزیابی امنیت، کارکرد و کارایی
۸. تحویل مستندات مورد نیاز جهت ارزیابی امنیت، عملکرد و کارایی ضد بدافزار
۹. گزارش آزمون عیارسنجی(عملکرد/کارآیی) روی محصول نمونه (با توافق کارفرما) در "پلتفرم یکپارچه خودکار ارزیابی ضد بدافزار"، گزارش اعمال اصلاحات و رفع نواقص در روالهای تست و گزارش نتایج تست در قالب متن، جدول و نمودارهای مصوب

[1] Development

۱۰. گزارش انجام ارزیابی امنیتی TOE نمونه (با توافق کارفرما) بر مبنای طرح تست فاز اول در "پلتفرم یکپارچه خودکار ارزیابی ضد بدافزار" ، گزارش اصلاحات و رفع نواقص در روالهای تست و گزارش نتایج تست در قالب متن، جدول و نمودارهای مصوب

۶ حداکثر مدت‌زمان مجاز و اعتبار برای ارائه پیشنهاد و اجرای پروژه

۶-۱ حداکثر مدت‌زمان مجاز برای ارائه پیشنهاد

دریافت‌کننده RFP، می‌بایست حداکثر ۱۴ روز پس از دریافت RFP، پیشنهاد خود را بر اساس مکانیزم پیش‌بینی‌شده دربند ۸ این RFP، تحویل پژوهشگاه ارتباطات و فناوری اطلاعات نماید. پیشنهادهای ارائه‌شده پس‌ازاین تاریخ، قابل وصول توسط پژوهشگاه ارتباطات و فناوری اطلاعات نخواهند بود.

۶-۲ حداکثر مدت‌زمان مجاز برای اجرای پروژه

حداکثر مدت‌زمان پیش‌بینی‌شده و قابل‌پذیرش برای اجرای این پروژه، ۱۲ ماه بر اساس مراحل اجرا و شرح خدمات تبیین شده، می‌باشد. چنانچه پیشنهاد دهنده در فرم پیشنهاد پروژه، مدت‌زمان اجرای پروژه را بیش از مدت زمان مجاز اعلام نماید، قابل وصول توسط پژوهشگاه ارتباطات و فناوری اطلاعات نخواهد بود.

۷ سایر الزامات و محدودیت‌های موجود در اجرای پروژه

علاوه بر محدودیت موجود در خصوص زمان اجرای پروژه، لازم است پیشنهاد دهندگان در تنظیم پیشنهاد خود، موارد ذیل را نیز رعایت فرمایند :

۱. پیشنهاد باید در قالب آخرین نسخه از "فرم پیشنهاد پروژه" موجود در سایت پژوهشگاه ارتباطات و فناوری اطلاعات (حوزه معاونت پژوهش و توسعه ارتباطات علمی، دفتر امور پژوهشی، فرم‌ها)، تنظیم و ارائه گردد.

۲. در جدول ساختار شکست پروژه پیش‌بینی‌شده در بخش ۲-۳-۷ فرم پیشنهاد پروژه، لازم است شرح فعالیت‌های هر مرحله از پروژه (مطابق شرح فعالیت‌های پیش‌بینی‌شده در RFP به همراه موارد احتمالی که پیشنهاد دهنده، انجام آن‌ها را ضروری می‌داند) به همراه کلیه اطلاعات درخواست شده در فرم، به تفکیک برای هر فعالیت و مرحله، ارائه گردد. از خالی گذاشتن ستون‌های این جدول برای فعالیت‌های پروژه، خودداری گردد.

۳. در جدول مشخصات منابع انسانی پیش‌بینی‌شده در بخش ۳-۱ فرم پیشنهاد پروژه، لازم است نام و سایر مشخصات درخواست شده برای کلیه پرسنلی که در اجرای پروژه به‌صورت واقعی مشارکت دارند با ذکر میزان مشارکت درج گردد.

۴. هزینه‌های سربار، تنها برای پیشنهاد دهندگان حقوقی (دانشگاه‌ها) پیش‌بینی‌شده است و شرکت‌ها می‌توانند بجای هزینه سربار، هزینه‌های اضافی متحملِ بابت این پروژه را عنوان نمایند.

۵. مجری پروژه باید در تمام مراحل طراحی و پیاده سازی و همچنین، در پایان پروژه منابع کدها را در اختیار کارفرما قرار دهد.

۸ تحویل پیشنهاد به پژوهشگاه ارتباطات و فناوری اطلاعات

۸-۱ حداقل شرایط پیشنهاد قابل تحویل

پیشنهادهایی قابل وصول می‌باشند که شرایط مندرج دربندهای ۶ و ۷ این RFP را کاملاً رعایت نموده باشند. در زمان ارائه پیشنهاد به پژوهشگاه ارتباطات و فناوری اطلاعات، رعایت شرایط مذکور، کنترل‌شده و در صورت عدم رعایت هر یک از موارد، از تحویل پیشنهاد، خودداری خواهد شد. پیشنهاد دهندگانی که سابقه فعالیت در حوزه ارزیابی و تولید محصولات افتا خصوصا ضدبدافزارها دارند، در اولویت خواهند بود.

۸-۲ نحوه تحویل پیشنهاد

پیشنهاددهندگان می‌بایست پیشنهاد خود را به نام معاونت پژوهش و توسعه ارتباطات علمی به دبیرخانه پژوهشگاه ارتباطات و فناوری اطلاعات، تحویل داده و رسید دریافت نمایند. (درصورتی‌که مدارک به سایر واحدهای دیگر پژوهشگاه تحویل داده شود در فراخوان ثبت نخواهد شد و این پژوهشگاه در قبال آن هیچ‌گونه مسئولیتی ندارد)

۸-۳ نحوه ارزیابی پیشنهاد

ارزیابی پیشنهادهای رسیده بر اساس پارامترهای زیر خواهد بود:

۱- میزان تسلط به ابعاد و جوانب پروژه (امتیاز این ردیف با توجه به سمینار ارائه‌شده توسط پیشنهاد دهنده و نیز مطالب ارائه‌شده در فرم پیشنهاد پروژه در خصوص شرح خدمات، خروجی‌ها، اهداف و . . . تعیین می‌گردد)

۲- نحوهٔ تخصیص منابع انسانی شامل کیفیت و کمیت نیروها (رزومه و سابقه کاری لازم در ارتباط با انجام خدمات موردنیاز پروژه، تعداد و تناسب نیروها با توجه به حجم کار، نوع رابطه استخدامی نیروها بر اساس مدارک ارائه‌شده)

۳- کیفیت ساختار شکست پروژه متناسب با شرح خدمات و اهداف پروژه

۴- کیفیت ساختار سازمانی پیش‌بینی‌شده برای انجام پروژه(تیم‌های اجرایی، مدیریت پروژه و...)

۵- ساختار و روال‌های پیش‌بینی‌شده برای کنترل و مدیریت پروژه و تأیید صحت خروجی‌ها

۶- روال‌ها، متدولوژی و استانداردهای پیشنهادی برای اجرای شرح خدمات

۷- نحوه ارائه زمان‌بندی و پوشش کامل و به‌موقع شرح خدمات

۸- مبلغ پیشنهادی

پیوست الف- اجزاء و شاخص‌های ارزیابی امنیت، کارکرد و کارآیی ضدبدافزار

در این بخش جداول اولیه شاخص‌ها و اجزاء ارزیابی برای ارزیابی امنیت، کارکردها و کارآیی سامانه های ضد بد افزار تبیین شده‌اند. این جداول در بخش ارزیابی امنیت(جدول ۱) بر مبنای استاندارد CC و در بخشهای شاخص‌های عیارسنجی(کارکردی و کارآیی) بر مبنای مشخصه‌های ضدبدافزارهای نوین برتر تدوین شده‌اند. این جداول نسخه اولیه و پیشنهادی برای موارد فوق هستند و توسط مجری، در فازهای پروژه، تدوین، تکمیل و اصلاح خواهند شد.

جدول ۱- اجزاء ارزیابی امنیت در سطح تضمین ۳ بر مبنای CC

کلاس تضمین	مولفه های تضمین
کلاس توسعه (ADV)	توصیف معماری امنیتی (ADV_ARC.1)
	مشخصه عملکردی با خلاصه کامل (ADV_FSP.3)
	طراحی معماری (ADV_TDS.2)
مستندات راهنما (AGD)	راهنمایی عملیاتی کاربر (AGD_DPE.1)
	رویه های آماده سازی (AGD_DRE.1)
پشتیبانی چرخه حیات (ALC)	کنترل های مجوز (ALC_CMC.۳)
	ارائه پیاده سازی پوشش مدیریت پیکربندی (ALC_CMC.۳)
	رویه های تحویل (ALC_DEL.1)
	مدل چرخه حیات تعریف شده توسط توسعه دهنده (ALC_LCD.1)
	شناسه معیارهای امنیتی (ALC_DVS.1)
ارزیابی هدف امنیتی (ASF)	ابعادهای تطابق (ASE_CCL.1)
	تعریف مولف های توسعه (ASE_EDC.1)
	معرفی هدف امنیتی(ST) (ASE_INT.1)
	اهداف امنیتی (ASE_OBJ.2)
	الزامات امنیتی استخراج شده (ASE_REQ.2)
	تعریف مسئله امنیتی (ASE_SPD.1)
	خلاصه مشخصات محصول

کلاس تضمین	مولفه های تضمین
	(ASE_TSS.1)
آزمون ها (ATE)	تجزیه و تحلیل پوشش تست ها (ATE_COV.2)
	تست: طراحی اولیه (ATE_DPT.1)
	تست عملکردی (ATE_FUN.1)
	تست مستقل(نمونه تست) (ATE_IDN.2)
کلاس آسیب پذیری (AVA)	ارزیابی آسیب پذیری (AVA_VAN.2)

جدول۲- شاخص های عیارسنجی کارکردی ضدبدافزارها

ردیف	نام آزمون
۱	دقت حفاظت در برابر بد افزار[۱]
۲	محافظت دنیای واقعی دنیای[۲]
۳	قدرت پاکسازی[۳]
۴	قابلیت پیشگیرانه[۴]
۵	پویش ابتکاری/مبتنی بر رفتار[۵]
۶	پویش "مبتنی بر تقاضا" [۶]
۷	"مبتنی بر دسترسی" [۷]
۸	آزمون کارایی[۸]
۹	قابلیت استفاده[۹]

[۱] Malware Protection test
[۲] Real world Protection Test
[۳] Malware Removal Test
[۴] proactive test
[۵] Heuristic/Behavioral Test
[۶] On-Demand Test
[۷] On-Access Test
[۸] Performance Test
[۹] Usability Test

ردیف	نام آزمون
۱۰	ضد فیشینگ[۱]
۱۱	قابلیت پیشگیری و پاسخ نقطه انتهایی[۲](EPR)
۱۲	آزمون ضد سرقت[۳]
۱۳	کنترل والدین[۴]
۱۴	ضد جاسوسی[۵]
۱۵	هشدار کاذب[۶]
۱۶	امنیت تلفن همراه[۷]
۱۷	برنامه‌های بالقوه ناخواسته[۸](PAU)
۱۸	قابلیت تشخیص و پاسخ نقطه پایانی(EDR)[۹]
۱۹	تشخیص و پاسخ گسترده(XDR)[۱۰]
۲۰	چند موتور همزمان (Multi AV)
۲۱	قابلیت دیواره آتش
۲۲	قابلیت VPN
۲۳	قابلیت فناوری ابری
۲۴	قابلیت هوش مصنوعی
۲۵	بدافزارهای مبتنی بر فایل از خانواده‌های مختلف بدافزاری
۲۶	تشخیص بدافزارهای مبتنی بر حافظه

[۱] Anti-phishing test
[۲] Endpoint prevention and response
[۳] Anti-Ransomware
[۴] Parent Control Test
[۵] Anti-Spam test
[۶] False Alarm Test
[۷] Mobile Security Review Test
[۸] Potentially Unwanted Applications
[۹] Endpoint Detection and Response
[۱۰] Extended detection and response

ردیف	نام آزمون
۲۷	تشخیص بدافزارهای فشرده شده
۲۸	تشخیص بدافزارهایی که حالت ماندگاری در سیستم دارند

جدول ۳- شاخص‌های عیارسنجی کارآیی ضد بد افزارها

ردیف	معیار	معادل انگلیسی
۱	مدت زمان اسکن	SCAN TIME
۲	مدت زمان اسکن‌های برنامه ریزی شده	SCHEDULED SCAN TIME
۳	مدت زمان لازم برای نصب	INSTALLATION SIZE
۴	حجم لازم برای نصب	INSTALLATION TIME.
۵	تعداد کلیدهای رجیستری اضافه شده	REGISTRY KEYS ADDED
۶	مدت زمان بالاآمدن سیستم	BOOT TIME
۷	مدت زمان راه اندازی رابط کاربری	USER INTERFACE LAUNCH TIME
۸	مدت زمان بالاآمدن مرورگرهای اینترنت	CHROME LAUNCH TIME
۹	استفاده از حافظه در حین بیکار بودن سیستم	MEMORY USAGE DURING SYSTEM IDLE
۱۰	مقدار حافظه لازم در حین اسکن اولیه	MEMORY USAGE DURING INITIAL SCAN
۱۱	مدت زمان لازم برای بارگزار ی اطلاعات از اینترنت توسط مرور گر	BROWSE TIME
۱۲	سرعت کپی، انتقال و حذف فایل	FILE COPY, MOVE AND DELETE.
۱۳	تبدیل فرمت فایل	FILE FORMAT CONVERSION.
۱۴	مدت زمان فشرده سازی فایل و باز کردن فایل‌های فشرده	FILE COMPRESSION AND DECOMPRESSION
۱۵	مدت زمان نوشتن، باز کردن و بستن فایل	FILE WRITE, OPEN AND CLOSE