قـــرارداد مشاوره با موضوع
پیاده سازی و راهبری مرکز عملیات امنیت بصورت میزبانی شده (Hosted) در ستاد وزارت ارتباطات و فناوری اطلاعات

این قرارداد براساس جزء (۵) بند (ث) ماده (۱۶) آیین نامه خرید خدمات مشاوره موضوع بند هـ ماده (۲۹) قانون برگزاری مناقصات فی مابین "وزارت ارتباطات و فناوری اطلاعات" به نشانی تهران، خیابان دکتر شریعتی، بالاتر از چهارراه شهید قدوسی، ساختمان معاونت توسعه سرمایه انسانی و مدیریت منابع با نمایندگی آقای غلامرضا امیدی با سمت معاون توسعه سرمایه انسانی و مدیریت منابع که در این قرارداد منبعد اختصاراً کارفرما نامیده می شود از یک طرف و شرکت نوآوران ارتباطات دوران به شماره ثبت۲۳۱۴۵، شناسه ملی ۱۰۱۰۲۷۲۵۱۴۰، کد اقتصادی۴۱۱۱۱۴۷۵۳۴۷۴، به نشانی: تهران، شهید بهشتی، خیابان شهید عبدالمجید صابونچی، خیابان شهید فرشاد ایازی (نهم)،پلاک ۶۲، طبقه اول کد پستی:.۱۵۳۳۷۶۳۸۱۱ تلفن: ۴۳۵۸۸۰۰۰ با نمایندگی و امضاء مجاز آقایان حسین داماد ممقانی با شماره ملی ۱۷۵۳۶۱۵۳۴۸ با سمت مدیر عامل و علیرضا عابدی نژاد با شماره ملی ۰۴۹۱۵۰۰۹۹۸ با سمت رئیس هیئت مدیره که حسب آخرین آگهی تغییرات ثبت شده در روزنامه رسمی شماره ۲۳۲۴۵ مورخ ۱۴۰۳/۱۰/۲۲ دارای حق امضاء می باشند و در این قرارداد منبعد اختصاراً مشاور نامیده می شود از طرف دیگر به شرح ذیل منعقد می‌گردد و طرفین ملزم به رعایت کلیه مفاد آن می باشند.

ماده ۱- موضوع قرارداد :

موضوع قرارداد عبارتست از: پیاده سازی و راهبری مرکز عملیات امنیت، بصورت میزبانی شده (Hosted) در ستاد وزارت ارتباطات و فناوری اطلاعات مطابق با شرح خدمات پیوست قرارداد که به رویت و تایید مشاور رسیده است و جزء لاینفک قرارداد می‌باشد.

ماده ۲- مبلغ قرارداد و نحوه پرداخت :

مبلغ کل قرارداد بدون احتساب مالیات بر ارزش افزوده **۳۶۸,۳۹۷,۲۷۲,۰۲۱ ریال** (سیصدو شصت و هشت میلیارد و سیصد و نود و هفت میلیون و دویست و هفتاد و دو هزار و بیست و یک ریال) به تفکیک به شرح مندرج در جدول ذیل می‌باشد:

فاز	شرح فازهای کاری	مدت زمان	بهای کل (ریال)
۱	تحلیل وضع موجود به همراه تأمین، طراحی و نصب نیازمندی های نرم افزاری (ابزار بومی SIEM)	۱۵ روز از شروع قرارداد	۱۰۰,۰۰۰,۰۰۰,۰۰۰
۲	طراحی و نصب نیازمندی های نرم افزاری (ابزار بومیUBA,XDR)	۳۰ روز از زمان اتمام فاز اول	۷۰,۰۰۰,۰۰۰,۰۰۰
۳	اجرای خدمات تست نفوذ ، اجرای طرح Network Auditing و مقاوم سازی شبکه	۴۵ روز از زمان اتمام فاز دوم	۵۵,۰۰۰,۰۰۰,۰۰۰
۴	طراحی، اجرا و استقرار مرکز عملیات امنیت (SOC) به همراه طرح مدیریت امنیت اطلاعات (ISMS)	۹۰ روز از زمان اتمام فاز سوم	۳۰,۰۰۰,۰۰۰,۰۰۰
۵	اجرای خدمات مستمر امنیت و ارایه گزارشات مدون	۳۶۵ روز از زمان اتمام فاز چهارم	۱۱۳,۳۹۷,۲۷۲,۰۲۱
	جمع کل	**۵۴۵ روز**	**۳۶۸,۳۹۷,۲۷۲,۰۲۱**

نحوه پرداخت: مبلغ هر فاز پس از انجام کامل خدمات آن فاز و اخذ گواهی حسن انجام کار از ناظرین قرارداد، تأیید صورت وضعیت توسط کارفرما و کسر کسورات قانونی به مشاور قابل پرداخت خواهد بود.

تبصره: پرداخت مالیات بر ارزش افزوده در صورت ارائه گواهینامه ثبت نام در نظام مالیات بر ارزش افزوده به عهده کارفرما می باشد.

ماده ۳- مدت قرارداد :

مدت قرارداد ۵۴۵ روز از تاریخ ۱۴۰۴/۰۶/۱۷لغایت ۱۴۰۵/۱۲/۱۵ مطابق برنامه زمانبندی مندرج در جدول ذیل ماده (۲) تعیین می‌گردد.

ماده ٤- محل اجرای قرارداد :

محل اجرای قرارداد وزارت ارتباطات و فناوری اطلاعات می‌باشد.

ماده ٥- کسورات قانونی :

کلیه کسورات قانونی متعلقه به این قرارداد شامل انواع بیمه و مالیات و عوارض وغیره اعم از اینکه قبل یا بعد از انعقاد قرارداد به موجب قانون وضع شود بعهده مشاور است و کارفرما مجاز خواهد بود از پرداخت هایی که به مشاور صورت می پذیرد کسر و به حسابهای مربوطه واریز نماید.

تبصره: تسویه حساب منوط به رعایت مفاد ماده ۳۸ قانون تأمین اجتماعی می باشد.

ماده ٦- تعهدات مشاور :

۶-۱- مشاور موظف است ظرف مدت ۷ روز کاری از تاریخ ابلاغ قرارداد یک نفر را بعنوان مدیر پروژه و نماینده تام الاختیار خود جهت پاسخگویی و انجام هماهنگی های لازم در انجام خدمات موضوع قرارداد کتباً به کارفرما معرفی نماید.

۶-۲-مستقل از هر شرط صریحی در قرارداد، مشاور در مقابل کارفرما به ازای هر پی‌آمد ناشی از تأخیر، ضعف عملکرد، نقض قرارداد و اجرای آن و قصور و تقصیر انجام شده متعهد و مسئول است.

۶-۳-مشاور نسبت به افعال کارکنان خود و قصور و تقصیر آنها در مقابل کارفرما مسئول می باشد و هرگونه ادعایی در این خصوص را از خود سلب می نماید.

۶-۴- مشاور، کارفرما را در مقابل هر ادعا، خسارت، مخارج و هزینه شامل آنهائی که توسط کارکنان خود در ارتباط با اجرای پروژه مطرح می‌گردند مصون و مبری می‌سازد.

۶-۵-مشاور متعهد به رعایت و انجام کلیه نکات و راهکارهای فنی مرتبط با موضوع قرارداد که از سوی کارفرما مشخص و تعریف می شود، می باشد.

۶-۶- هر صورتجلسه یا توافق کتبی طرفین در طول مدت قرارداد در حکم مفاد قرارداد محسوب شده و لازم الاجرا می باشد.

۶-۷- مشاور متعهد می گردد اجرای موضوع قرارداد را در چارچوب استانداردهای تعیین شده توسط کارفرما انجام دهد.

تبصره۱: مشاور و کارفرما می توانند حین اجرای قرارداد در خصوص تغییر در روش عمل با استاندارد و یا بخشهایی که استاندارد و یا ضوابط تعیین شده ندارد توافق کتبی نموده و براساس توافق حاصله بدون دریافت هزینه مازاد بر مبلغ قرارداد عمل نمایند.

۶-۸-مشاور موظف است از طریق ارایه زمانبندی، شکست کار (WBS) و گزارشهای پیشرفت کار ماهانه، کارفرما را از اقدامات انجام شده و پیشرفت و تاخیرات احتمالی پروژه و در صورت وجود تاخیر، از راهکارهای ارائه شده به جهت مقابله با آن تاخیر، مطلع نماید.

۶-۹- آموزش و انتقال دانش توسط مشاور در حین انجام کار به پرسنل کارفرما الزامیست.

۱۰-۶-هرگاه طرف قرارداد و پیمانکاران دیگری در حال انجام کاری با کارفرما باشند که به تشخیص کارفرما به موضوع این قرارداد مرتبط باشد ، مشاور متعهد است، بدلیل همبستگی پروژه‌ها در جلسات هماهنگی شرکت نموده و هماهنگیهای لازم را با مشاوران و پیمانکاران دیگر به اتفاق ناظر پروژه بعمل آورده و تسهیلات لازم را برای آنان فراهم آورد.

۱۱-۶- مشاور متعهد است در مواردی که متوجه ارتباط و نیاز به هماهنگی با سایر پروژه‌های کارفرما شود، مورد را کتباً به کارفرما اطلاع دهد و در صورتی که نیاز به اعمال اصلاحاتی در شرایط اجرای قرارداد باشد، موظف به همکاری در جهت اعمال اصلاحات لازم می باشد. (هماهنگی و یکپارچه‌سازی کلی این تغییرات بعهده ناظر و کارفرماست).

۱۲-۶-تأمین پرسنل مورد نیاز جهت انجام موضوع قرارداد و هرگونه رابطه حقوقی و قراردادی و کلیه هزینه های مربوط به آنان اعم از حقوق، مزایا، بیمه و غیره بر عهده مشاور می باشد و کارفرما در این خصوص هیچگونه تعهدی ندارد.

۱۳-۶-تأمین هرگونه ابزار سخت افزاری مرتبط با موضوع قرارداد به عهده مشاور می باشد.

۱۴-۶- مشاور مکلف است نسبت به آموزش عوامل اجرایی خود جهت تردد در ساختمانهای وزارت اقدام نماید.

۱۵-۶- مشاور در انجام موضوع قرارداد ، به هیچ وجه حق افشاء و یا بهره برداری از اطلاعات در اختیار مرتبط با این قرارداد، نرم افزارها و سایر مدارک و مستندات وزارت را حتی پس از فسخ و یا خاتمه قرارداد ندارد. در غیر این صورت ضمن پیگیری قضایی توسط کارفرما، مشاور مسئول جبران هرگونه خسارتی می باشد که ممکن است در اثر عدم رازداری حاصل شود.

تبصره ۲ : مشاور متعهد می گردد کلیه اطلاعات، اسناد، مدارک و موضوعات مرتبط با قرارداد و یا تولید شده حین اجرای قرارداد را محرمانه تلقی کرده و تحت هیچ شرایطی اطلاعات، مدارک، داده های تکنیکی، تجارب و دانش فنی ای که توسط کارفرما در اختیار وی گذاشته شده است را فاش ننماید، مگر اینکه مجوز رسمی و کتبی کارفرما را در این رابطه اخذ کرده باشد.

تبصره ۳ : مشاور متعهد می گردد دستیابی به اطلاعات محرمانه یاد شده در تبصره قبل را محدود به آن‌دسته از کارشناسان، مشاوران و طرفهای قرارداد خود نماید که برای انجام درست وظایف و ارائه خدمات، واقعا به آنها نیاز دارند و مشاور باید ماهیت محرمانه بودن اطلاعات را به اشخاص فوق اطلاع داده و نسبت به عدم افشای موارد ، کنترل و نظارت لازم را بعمل آورد. در هرحال هرگونه مسئولیت حقوقی و قانونی ناشی از عدم رعایت مفاد این تبصره از سوی کارکنان مشاور، مستقیماً به عهده مشاور می باشد.

۱۶-۶-کلیه موارد مندرج در شرح خدمات پیوست به عنوان بندهای قرارداد تلقی گردیده و برای مشاور لازم الاجرا می‌باشد.

۱۷-۶-مشاور متعهد است وظایف و خدمات خود را دقیقاً مطابق با شرایط قرارداد و شرح خدمات پیوست انجام داده و تمام مهارت، دقت و سعی و تلاش خود را برای ارائه خدمات یاد شده با کیفیت مناسب بکار برد.

۱۸-۶-مشاور موظف است در طول مدت قرارداد توانایی پرداخت حقوق پرسنل را از محل منابع خود داشته باشد و عذر عدم توانایی مالی از وی مسموع نخواهد بود.

ماده ۷- تعهدات کارفرما :

۱-۷- کارفرما تعهد می‌نماید در صورت تایید انجام کلیه تعهدات مشاور از سوی ناظر قرارداد، مبالغ صورت وضعیت ها را مطابق با ضوابط و شرایط مقرر در قرارداد، در وجه مشاور پرداخت نماید .

۲-۷- در صورت نیاز و تشخیص مشاور و تأیید کارفرما به استقرار تیم کارشناسی مشاور در محل‌ها و اماکن وابسته به کارفرما، کارفرما محل کار و امکانات لازم را در حداقل عرف کاری برای استقرار تیم مشاور را در اختیار قرار خواهد داد.

۳-۷ کارفرما متعهد به تأمین زیرساخت ارتباطی لازم برای اجرای موضوع قرارداد براساس شریط اختصاصی قرارداد می باشد.

۴-۷-کارفرما متعهد است در شرایطی که قراردادهای متعددی را همزمان در حال اجرا دارد که شرایط، محصولات و خدمات آنها به هم ارتباط پیدا می کنند، هماهنگی و یکپارچه‌سازی آنها را با کمک ناظرین قراردادها انجام داده و شرایط جدید اجرای این قرارداد را نیز به اطلاع مشاور برساند.

ماده ۸- خسارت تأخیر:

در صورت تأخیر مشاور در انجام هر یک از تعهدات مندرج در این قرارداد و حسب تشخیص کارفرما، خساراتی به شرح ذیل محاسبه و از مطالبات و تضامین و سپرده های مشاور کسر خواهد گردید:

۱-۸-در مواردی که در پیوست قرارداد، دستورالعملی برای محاسبه خسارت تعیین شده باشد ، بر همان اساس کارفرما نسبت به کسر خسارت عمل خواهد نمود.

۲-۸-در مواردی که در پیوست قرارداد دستورالعملی برای محاسبه خسارت تعیین نشده باشد از بابت هر روز تأخیر معادل دو هزارم مبلغ کل قرارداد به عنوان خسارت تأخیر در انجام تعهدات از مطالبات و سپرده های مشاور و تضامین موضوع این قرارداد، کسر خواهد گردید.

۳-۸-مبالغ مذکور دین قطعی مشاور محسوب و وی حق هرگونه اعتراض را از خود سلب و ساقط می نماید. ضمن اینکه کسر مبلغ فوق از قرارداد، تکلیف مشاور را نسبت به ایفای اصل تعهد ساقط نمی کند. درصورت تأخیر مشاور در انجام تعهدات و مفاد قرارداد، کارفرما میتواند علاوه بر مطالبه و کسر خسارت تأخیر نسبت به فسخ یکطرفه قرارداد و ضبط مطالبات و سپرده ها و تضامین مشاور اقدام نماید.

تبصره : مواردی که قانوناً فورس ماژور (مندرج در ماده ۱۴) محسوب می شود از شمول این ماده مستثنی است و در صورت وقوع فورس ماژور مدت قرارداد طبق نظر کارفرما تعدیل خواهد گردید.

ماده ۹- جبران خسارت :

درصورتیکه در اثر اجرای قرارداد خسارتی توسط مشاور یا عوامل اجرائی او به تجهیزات کارفرما وارد شود مشاور مکلف به جبران سریع (حداکثر ظرف ۷۲ ساعت) خسارت حادث شده میباشد و در صورت عدم اجرای تعهد موضوع این بند کارفرما راساً و با تشخیص خود نسبت به ترمیم خرابی اقدام و هزینه‌های مربوطه به اضافه ۳۰٪ بالاسری را از مطالبات و سپرده ها و تضامین مشاور کسر و برداشت خواهد کرد.

تبصره: چنانچه میزان خسارت ناشی از تأخیر یا تعلل در اجرای مفاد قرارداد بیش از مبلغ مطالبات و سپرده ها و تضمین انجام تعهدات مشاور باشد، مشاور متعهد است حداکثر ظرف یک هفته پس از ابلاغ کتبی به وی، باقیمانده را از سایر دارائیهای خود نقداً جبران و پرداخت نماید.

ماده ۱۰- تضمین انجام تعهدات :

مشاور برای تضمین انجام تعهدات خود پنج درصد (۵٪) از کل مبلغ قرارداد را که معادل ۱۸,۴۲۰,۰۰۰,۰۰۰ریال (هجده میلیارد و چهارصد و بیست میلیون ریال) می‌باشد طی یک فقره ضمانتنامه بانکی معتبر غیرقابل انتقال و قابل تمدید به شماره ۲۶۶۸۳۲۰۱۱۵۱۷۱۱۸۲۳۰مورخ ۱۴۰۴/۰۶/۱۷ عهده بانک پاسارگاد شعبه شهید بهشتی غربی تسلیم کارفرما نموده و کارفرما می تواند درصورت عدم انجام هریک از تعهدات و یا ورود خسارت از سوی مشاور یا هر نوع قصور یا تقصیر در اجرای هریک از مفاد قرارداد، برای جبران قسمتی از خسارت وارده بدون قید و شرط تمام یا قسمتی از وجه ضمانتنامه را ضبط و به نفع خود وصول نماید. وصول وجه ضمانتنامه مذکور توسط کارفرما موجب بریُ الذمّه شدن مشاور نمی گردد و صرفاً وجه التزام تخلف و تعهدات مشاور محسوب شده و توسط کارفرما قابل اخذ است. تضمین مذکور پس از خاتمه قرارداد در صورت انجام کلیه تعهدات موضوع قرارداد و عدم ورود خسارت از سوی مشاور و تأیید آن توسط ناظرین قرارداد، به مشاور مسترد خواهد شد.

تبصره: درصورتی که پس از استرداد تضمین مذکور احراز گردد، خسارتی به کارفرما در زمان حاکمیت قرارداد، از سوی مشاور یا کارکنان وی به نحو مستقیم یاغیر مستقیم وارد شده باشد، مشاور مسئولیت جبران کلیه خسارات وارده را بنا به تشخیص و اعلام کارفرما از محل اموال موجود خود می پذیرد و استرداد تضمین مأخوذه و خاتمه مدت قرارداد نافی مسئولیت های مشاور در خصوص اعمال وی و کارکنانش نخواهد بود.

ماده ۱۱- سپرده حسن اجرای کار:

بابت حسن اجرای کار معادل ۱۰٪ از هر پرداخت کارفرما به مشاور کسر و به حساب سپرده کارفرما واریز میشود. آزادسازی این سپرده پس از اتمام قرارداد و انجام کلیه تعهدات و تأیید حسن کار انجام شده توسط ناظر قرارداد و موافقت کارفرما خواهد بود.

ماده ۱۲- نمایندگی ونظارت در اجرا ی قرارداد :

نماینده فنی کارفرما و ناظر این قرارداد "رئیس مرکز توسعه فناوری اطلاعات، امنیت و هوشمندسازی" یا نماینده معرفی شده از سوی ایشان خواهند بود که بر انجام تعهدات قرارداد توسط مشاور نظارت خواهند داشت. بدیهی است کلیه پرداختها بعد از تائید صحت و انجام کامل موضوع قرارداد توسط نماینده فنی کارفرما و ناظر قرارداد به مشاور انجام خواهد شد .

ماده ۱۳- فسخ قرارداد :

کارفرما می‌تواند در طول مدت قرارداد (موضوع ماده۳) در صورت تحقق هر یک از موارد زیر ضمن ضبط تضمین ماخوذه و وصول خسارت وارده از محل مطالبات و سپرده ها و تضامین مربوط به مشاور. قرارداد را با اخطار کتبی فسخ نماید. مشاور ضمن امضای این قرارداد حق فسخ یک طرفه این قرارداد را از خود سلب و ساقط می‌نماید.

۱۳-۱- هرگاه مشاور ورشکسته گردد و یا اعلام ورشکستگی نماید یا منحل شود .

۱۳-۲- هرگاه به تشخیص کارفرما، مشاور در انجام هر یک از تعهدات خود قصور یا تقصیر ورزیده یا کیفیت خدمات ارائه شده مطابق نظرکارفرما نباشد و یا به هردلیل از انجام موضوع قرارداد خودداری کند.

۱۳-۳- هرگاه به تشخیص کارفرما مشخص شود اجرای قرارداد کلاً یا جزئا به غیر واگذار شده است .(موضوع ماده ۱۵)

۱۳-۴- هرگاه شرایط مندرج در ماده ۱۸ این قرارداد (دخالت واسطه) برای کارفرما احراز گردد.

ماده ۱٤- حوادث قهری (فورس ماژور) :

هرگونه تاخیر طرفین دراجرای تعهدات که ناشی از فورس ماژور (جنگ، شورش، زلزله، سیل، آتش سوزی، اعتصاب عمومی، شیوع بیماری های مُسری) باشد تخلف طرف مربوطه از اجرای مفاد قرارداد تلقی نمی شود. هرگاه به علل قانونی یا عوامل قهریه غیر قابل پیش بینی مشاور قادر به انجام تعهدات قرارداد نبا شد باید مراتب را پس از وقوع،حداکثر ظرف مدت ۷۲ ساعت کتباً به کارفرما اعلام نماید تا پس از رفع حالت فورس ماژور به تعهدات خود عمل نماید.

تبصره۱: درصورتیکه مدت فورس ماژور بیش از ۴۵ روز باشد کارفرما می تواند قرارداد را خاتمه نماید.

تبصره۲: وقوع حادثه قهریه باید از طرف مقامات ذیصلاح دولت جمهوری اسلامی ایران رسماً گواهی شود و گواهی مزبور از سوی مشاور به کارفرما ارائه گردد.

تبصره۳:افزایش سطح دستمزد و قیمت کالاها و ارز و تحریم و تورم از موضوع فورس ماژور خارج می باشد.

ماده ۱۵- حق واگذاری و انتقال قرارداد :

مشاور تحت هیچ عنوان حق انتقال و یا واگذاری قرارداد را به غیر کلاً و یا جزئاً ندارد و در صورت تخلف مشاور از این تکلیف، کارفرما حق دارد ضمن فسخ قرارداد و ضبط و برداشت مطالبات، سپرده ها و تضمین مأخوذه نسبت به وصول سایرخسارات وارده از هرحیث و جهت اقدام نماید.

ماده ۱۶- قوانین ومقررات حاکم برقرارداد :

قرارداد حاضر از هر حیث تابع قوانین «جمهوری اسلامی ایران» می باشد و چنانچه بین طرفین اختلافی پیش آید که نتوان از راه مذاکره حل و فصل نمود رأی مراجع ذیصلاح قانونی برای طرفین لازم الاجراء می باشد و طرفین تا حل اختلاف ملزم به انجام تعهدات خود می باشند.

ماده ۱۷- منع قانونی :

مشاور رسماً اعلام می نماید که مشمول ممنوعیت قانون « منع مداخله کارکنان در معاملات دولتی» مصوب ۲۲ دیماه ۱۳۳۷نمی باشد. مشاور تعهد می نماید که منافع این قرارداد را به هیچیک ازاشخاص یا افرادی که در قانون مذکور پیش‌بینی شده است انتقال نداده و یا آنان رابه مشارکت قبول نکند. بدیهی است درصورت تخلف قرارداد باطل بوده و مشاور مشمول تبعات حقوقی و کیفری ناشی از عدم رعایت این ماده خواهد بود و در این خصوص کارفرما هیچ مسئولیتی نخواهد داشت.

ماده ۱۸- عدم دخالت واسطه :

مشاور اعلام می نماید که بابت قرارداد حاضر واسطه‌ای وجود نداشته و هیچگونه حق دلالی و کمیسیون و نظایر آن نپرداخته و نخواهد پرداخت و چنانچه خلاف این مطلب به نحوی از انحاء معلوم شود کارفرما حق خواهد داشت قرارداد را طبق ماده ۱۳ فسخ نموده و ضمانتنامه مشاور را به نفع خود ضبط نماید.

ماده ۱۹- نشانی طرفین برای ارسال اطلاعیه ها ومکاتبات :

هرگونه مکاتبه ای که طبق این قرارداد بعنوان « کارفرما » و یا « مشاور » باشد، باید به نشانی های مذکور در صدر قرارداد ارسال و یا تحویل پست سفارشی شود. در مورد فاکس متعاقباً باید تأییدیه لازم به نحو مزبور ارسال شود. هرگاه یکی از طرفینِ قرارداد نشانی خود را در مدت قرارداد تغییر دهد باید ظرف ۴۸ ساعت موضوع را کتباً به طرف دیگر اعلام نماید و تا زمانیکه نشانی جدید به طرف دیگر اعلام نشده است، کلیه نامه‌ها و اوراق و اظهارنامه‌ها به نشانی مذکور در آغاز این قرارداد ارسال و ابلاغ قانونی تلقی خواهد شد.

ماده ۲۰ – افزایش یاکاهش موضوع قرارداد

کارفرما مختار است تا پایان مدت قرارداد بطور یک جانبه با اعلام قبلی و به صورت کتبی تا ۲۵ درصد از خدمات موضوع قرارداد را کسر و یا به آن اضافه نماید در اینصورت مبلغ و مدت زمان قرارداد به تناسب موضوع مورد درخواست کاهش و یا افزایش خواهد یافت و مشاور در هر صورت متعهد به رعایت کلیه مفاد قرارداد بدون تغییر در قیمت واحد خواهد بود. همچنین مشاور متعهد است با اعلام و ابلاغ افزایش موضوع قرارداد حداکثر ظرف یک هفته نسبت به تهیه الحاقیه بر تضمین انجام تعهدات خود و افزایش مبلغ تضمین مطابق افزایش حاصله اقدام نماید. در غیر اینصورت کارفرما حق دارد به طور یک جانبه قرارداد را طبق ماده ۱۳ این قرارداد فسخ نماید.

ماده ۲۱- تغییرات مدت قرارداد :

مدت قرارداد در صورت پیش آمدن هر یک از موارد ذیل میتواند بنا به تشخیص کارفرما تغییر یابد :

۱. تغییر حدود خدمات (موضوع ماده ۲۰ قرارداد)
۲. وقوع حوادث قهریه براساس مقررات و بروز شرایط اضطراری به تشخیص کارفرما
۳. تعلیق کارها از طرف کارفرما
۴. تأخیر مجاز از سوی مشاور به تشخیص کارفرما

در پایان مدت اولیه قرارداد (قبل از اتمام قرارداد)، مجموعه تغییرات مدت ناشی از بندهای فوق مورد بررسی نهایی قرار گرفته و کارفرما نتیجه را به مشاور ابلاغ مینماید.

ماده ۲۲- دارا بودن دانش فنی موضوع قرارداد :

مشاور صریحاً اعلام می دارد که دانش فنی لازم (مطابق شرح خدمات پیوست)جهت انجام موضوع قرارداد را دارا می‌باشد و با امضای قرارداد هیچگونه عذری بر عدم اجرای پروژه در طول مدت قرارداد نخواهد داشت.

ماده ۲۳- محل تامین اعتبارقرارداد :

مبلغ این قرارداد از محل اعتبار طرح ایجاد و توسعه زیرساخت های یکپارچه ابری و خدمات دولت هوشمند به شماره ۱۳۰۲۰۳۴۰۱۳ تأمین و پرداخت می باشد.

ماده ٢٤- قطعیت مفاد قرارداد :

مشاور صریحاً اعلام و اقرار می نماید که ازشرایط، اوضاع واحوال، امکانات و محل اجرای قرارداد اطلاع کامل داشته و با لحاظ جمیع جهات و ضمن سلب حق هرگونه اعتراضی، اقدام به انعقاد این قرارداد نموده است ، لذا پس از انعقاد قرارداد نمی تواند به دلایلی ازقبیل عدم محاسبه کافی و امثال آن معترض وهیچگونه ادعا ویا مطالبه ای از این جهت پذیرفته نیست.

ماده ۲۵- خاتمه قرارداد:

هرگاه پیش از اتمام مدت قرارداد، کارفرما بدون آنکه تقصیری متوجه مشاور باشد، بنا به مصلحت خود یا علل دیگر، تصمیم به خاتمه دادن قرارداد بگیرد، خاتمه قرارداد را کتباً به مشاور ابلاغ می‌نماید. بدیهی است ما به ازای تعهدات انجام شده که مورد قبول کارفرما می باشد به مشاور پرداخت خواهد شد.

ماده ٢٦- نسخ قرارداد :

این قرارداد در ۲۶ ماده، ۱۱ تبصره در ۳ نسخه تهیه و تنظیم شده که پس از امضاء و مبادله قرارداد برای طرفین لازم الاجراء خواهد بود. کلیه نسخ این قرارداد دارای اعتبار بوده و در حکم واحد می باشد.

مهر و امضاء کارفرما :
نام ونام خانوادگی نماینده: غلامرضا امیدی
سمت: معاون توسعه سرمایه انسانی و مدیریت منابع
محل امضاء :

مهر وامضاء مشاور:
نام ونام خانوادگی نماینده: حسین داماد ممقانی
سمت : ~~مدیر عامل~~
محل امضاء :
نام ونام خانوادگی نماینده: علیرضا عابدی نژاد
سمت : رئیس هیئت مدیره
محل امضاء :
نوآوران ارتباطات دوران
(سهامی خاص - ش ث ۴۲۱۴۷۵)

تهران، خیابان دکتر شریعتی، بالاتر از چهارراه شهید قدوسی (قصر)، ورودی شماره۴،ساختمان مرکزی
● کدپستی:۱۶۳۱۷۱۳۴۶۱

"شرح خدمات مورد نیاز "

مقدمه و اهداف پروژه

با عنایت به گسترش روزافزون حوزه فناوری اطلاعات و ظهور راهکارهای مختلف ارائه خدمات در این حوزه و به تبع آن، گسترش بیش از پیش تهدیدات و مخاطرات امنیتی، لزوم تمهید و به کارگیری راهکارهای مقابله بصورت اثربخش با مخاطرات امنیتی مزبور و نیز مقاوم سازی زیرساخت ها، سامانه ها، پیاده سازی مرکزعملیات امنیت و پاسخ دهی به رخدادهای سایبری و همچنین مانیتورینگ پیوسته شبکه به عنوان یک نیاز اصلی مطرح می گردد

از این رو وزارت ارتباطات و فناوری اطلاعات در راستای ارتقای سطح امنیت سایبری و به منظور بهره گیری حداکثری از توان متخصصان و کارشناسان برجسته در حوزه امنیت و مراکز عملیات امنیت، قصد دارد یک پروژه جامع شامل راه‌اندازی مرکز عملیات امنیت (SOC) بصورت میزبانی شده (Hosted) در ستاد وزارت ارتباطات و فناوری اطلاعات، پیاده‌سازی سامانه‌های مرتبط و ممیزی امنیت شبکه و همچنین پیاده‌سازی سامانه مدیریت امنیت اطلاعات (ISMS) را به مرحله اجرا درآورد. لذا هدف از این پروژه، کاهش ریسک‌های امنیتی، افزایش تاب‌آوری سایبری، رعایت الزامات استانداردهای بین‌المللی و بهبود نظارت و پاسخ به حوادث امنیتی است

۱ – تعاریف

- پروژه

در سرتاسر این سند، منظور از "پروژه"، ارائه خدمات"پیاده سازی و راهبری مرکز عملیات امنیت ، بصورت میزبانی شده (Hosted) در ستاد وزارت ارتباطات و فناوری اطلاعات" می باشد .

- کارفرما

در سرتاسر این سند منظور از "کارفرما"، مرکز توسعه فناوری اطلاعات، امنیت و هوشمند سازی مستقر در ستاد وزارت ارتباطات و فناوری اطلاعات می باشد.

۲ – گستردگی جغرافیایی پروژه

محل اجرای پروژه ، ستاد وزارت ارتباطات و فناوری اطلاعات واقع در شهر تهران و همچنین ادارات ارتباطات و فناوری اطلاعات استانها می باشد

۳ – محدوده اجرای پروژه

اجرای پروژه محدود به مراکز داده موجود در ستاد وزارت ارتباطات و فناوری اطلاعات واقع در شهر تهران و همچنین شرکت ارتباطات زیرساخت و سازمان فناری اطلاعات واقع در شهر تهران می باشد

٤ - دامنه خدمات مورد انتظار (Scope of Work)

در این پروژه پیاده سازی مولفه های ذیل مورد انتظار است :

- ممیزی شبکه
- طراحی و پیاده سازی سیستم مدیریت امنیت اطلاعات مطابق استانداردهای ISO/IEC ۲۷۰۰۱
- پیاده سازی سامانه های مرتبط با مرکز SOC (نظیر SIEM,XDR و غیره) بصورت میزبانی شده (Hosted) در ستاد وزارت ارتباطات و فناوری اطلاعات
- پیاده سازی و راهبری مرکز عملیات SOC

لازم به ذکر است خدمات ارائه شده در مرکز عملیات امنیت و مرکز مانیتورینگ شبکه به منظور شناسایی و پاسخدهی به رخدادها، می بایست مطابق با نیازمندی های طرح بلوغ **مرکز راهبردی افتا** ریاست جمهوری باشد

۵- شرح خدمات مورد نیاز

۵-۱) تحلیل وضع موجود و نیازسنجی

انتظار میرود مشاور با انجام طرح Network Auditing در ادامه شناسایی دارایی ها جهت نصب و راه اندازی مرکز عملیات امنیت، موارد عدم پیکربندی صحیح، پالیسی های نیازمند به بروزرسانی، عدم انطباق با استانداردهای امنیتی و حتی تجهیزات مورد نیاز جهت بهبود وضعیت شبکه را شناسایی و درصورتیکه قابلیت پیاده سازی وجود داشته باشد توسط مشاور اقدامات موردنیاز انجام شود و چنانچه مقدمات مورد نیاز جهت پیاده سازی محقق نشده باشد طرح پیاده سازی و زمانبندی مربوطه را ارائه نموده تا پس از تامین از سوی کارفرما عملیاتی شود. همچنین در ادامه موارد ذیل نیز مورد انتظار است :

- انجام ممیزی جامع از دارایی‌های شبکه، سامانه‌ها و تجهیزات.
- اجرای تست نفوذ داخلی و خارجی (۱۰ سامانه)
- ارائه گزارش‌های آسیب‌پذیری و پیشنهادات اصلاحی
- ارایه مستندات کامل طرح Network Auditing

۵-۲) طراحی و پیاده سازی مرکز عملیات امنیت (SOC) بصورت میزبانی شده (Hosted) در ستاد وزارت ارتباطات و فناوری اطلاعات به همراه تهیه و تحویل مستندات

در این بخش پس از استخراج اطلاعات مورد نیاز، توجه به موارد و خروجی های ذیل الزامی است .

۵-۲-۱) انواع طراحی شامل مستندات طراحی که در برگیرنده عناوین ذیل بوده و میبایست در خروجی های ارائه شده ، به شکل مشخص قابل مشاهده و بررسی باشند:

- طراحی مفهومی
- طراحی منطقی و ساختاری
- طراحی زیرساخت فیزیکی مرکز عملیات امنیت

- لیست محصولات و سرویس های مورد نظر(LOS & LOM)
- ملاحظات جانبی در طراحی با در برگیرنده ارکان:
  - قابلیت گسترش (Scalability)
  - دسترس پذیری (Availability)

۲-۵-۲) طراحی و پیاده سازی مولفه های مرکز عملیات امنیت - کارفرما انتظار دارد تا با انجام این پروژه، به مستندات فنی لازم به منظور پیاده سازی مرکز عملیات امنیت با مولفه های ذیل دست یابد:

- عوامل تکنولوژیکی: فناوری ها و ابزارهای اصلی مرتبط با مرکز عملیات امنیت
- سیستم مدیریت لاگ :
  - ارائه راهکار به منظور جمع آوری لاگ تجهیزات شبکه
  - ارائه معیارهای انتخاب محصول. مقایسه و ارائه فهرست کوتاه محصولات با توجه به ساختار کارفرما
- انتظار می رود مشاور با توجه به ساختار گسترده، وضعیت موجود را بررسی کارشناسی کرده و در خصوص چگونگی جمع آوری لاگ ها و ارسال به سیستم مدیریت لاگ به صورت چند سطحی ارائه نظرنماید.
- سیستم مدیریت اطلاعات و رخدادهای امنیتیSIEM : با توجه به ساختار وزارت ارتباطات و فناوری اطلاعات انتظار میرود مشاور با تامین و نصب SIEM بومی در مزکر داده وزارت ارتباطات ، لایسنس مادام العمر را در این خصوص فراهم سازد.
- سامانه مدیریت و ارزیابی آسیب پذیریها : باتوجه به ساختار شبکه و تجهیزات موجود، مشاور میبایست به منظور نصب و راه اندازی نرم افزار اسکن آسیب پذیری ها(Open Source) اقدامات مقتضی را انجام دهد.
- لازم بذکر است تمام الزامات امنیتی جهت اتصال سرور به مرکز داده وزارت می بایست توسط مشاور تامین و پیاده سازی گردد.
- سایر ابزارهای مرتبط با مرکز عملیات امنیت
  - سامانه تیکتینگ
  - سامانه The Hive & cortex
  - سامانه Wazuh
  - سامانه XDR بومی به منظور پایشUBA کلاینت ها
  - سامانه شناسایی/پیشگیری نفوذ(Snort)
  - سیستم بازرسی قانونی
  - استفاده از ML جهت شناسایی تهدیدات

سازمان آموزش ارتباطات سیار ایران
سهامی خاص - ش ث ۲۱۱۲۴۵
www.ict.gov.ir
تهران، خیابان دکتر شریعتی، بالاتر از چهارراه شهید قدوسی (قصر)، ورودی شماره۴،ساختمان مرکزی
• کدپستی:۱۶۳۱۷۱۳۴۶۱

- سیستم Intelligence Threat به صورت رسمی(نه محدود به سایتهای رایگان)
- راهکارهای UBA جهت شناسایی تهدیدات داخلی
- راهکارهای مقابله با بدافزار
- راهکارهای پیشگیری از نشر داده
- راهکارهای پایش صفحات وب مخرب
- راهکارهای پایش فعالیت پایگاه داده ها

۲-۵-۳) طراحی و پیاده سازی سیستم مدیریت امنیت اطلاعات (ISMS)

پیاده سازی و کنترل فرآیندهای مورد نیاز جهت استقرار سیستم مدیریت امنیت اطلاعات وجود برنامه های مدون جهت بررسی عواقب ناشی از تغییرات ناخواسته و کنترل تغییرات واقدام به کاهش هرگونه عوارض جانبی ضروری می باشد . باتوجه به فاز Planning در سیستم مدیریت امنیت اطلاعات، مشاور می بایست براساس اطلاعات Inventory asset انجام شده در فاز شناخت جهت راه اندازی مرکز عملیات امنیت اقدامات مقتضی در راستای شناسایی ریسک های موجود و ارائه سطوح ریسک های هر دارایی جهت شناسایی دارایی های تحت تاثید در حملات و رویدادهای سایبری را برعهده خواهد داشت.لازم بذکر است اطلاعات دارایی ها در فاز شناخت socو نتایج حاصل از ریسک های ارزیابی شده ضمن کمک به بهبود سطح امنیت زمینه سازی پیاده سازی سیستم مدیریت امنیت اطلاعات و پیاده سازی کاملتر فرایندها خواهد بود.برخی از فرایندهای مورد نظر عبارت اند از:

- فرایند های کسب وکاری
  - فرآیند سنجش معیار اندازه گیری
  - فرآیند بهبود فرآیندها
  - فرآیند تداوم کسب وکار
- فرآیندهای مربوط به فناوری
  - فرآیند مدیریت پیکربندی
  - فرآیند راهبری سیستم
  - فرآیندهای عملیاتی
  - فرآیند مد یریت رخداد
  - فرآیند عملیات روزانه

۲-۵-۴) طراحی ساختار سازمانی مرکز عملیات امنیت

انتظار میرود در پیشنهادفنی به منظور شفافیت ساختار سازمانی مرکز عملیات امنیت موارد زیرمشخص گردد:

- اختیارات مرکز عملیات امنیت
- نقشها و وظایف کارکنان
  - مدیر مرکز عملیات امنیت
  - کارشناسان راهبری SIEM بصورت مقیم
- ویژگیهای عمومی کارکنان
- نیازمندیهای آموزشی

۲-۵-۵) طراحی روش تعاملات مرکز عملیات امنیت

- گردش کاری فرا سازمانی در مرکز عملیات امنیت
- گردش کاری درون سازمانی در مرکز عملیات امنیت
- تعاملات مرکز عملیات امنیت با مراجع بالادستی

۲-۵-۶) طراحی و پیاده سازی زیرساخت فیزیکی مرکز عملیات امنیت

- پیاده سازی الزامات فیزیکی مکان مرکز عملیات امنیت
- استقرار فیزیکی کارکنان (تامین نیروی انسانی توسط مشاور صورت می پذیرد)
- طراحی و پیاده سازی مولفه های پروژه در مراکز داده، سرورها وکلاینت ها

در مرکز عملیات امنیت مشابه با دیگر مراکز داده می بایست اصول امنیت فیزیکی رعایت شود. در این راستا مشاور می بایست ضمن طراحی نقشه و جانمایی فضاهای مرکز عملیات امنیت سایبری، مشخصات تجهیزات سخت افزاری مانند سرورها،کالینت ها و ... و الزامات امنیت فیزیکی متناسب با مرکز عملیات امنیت وزارت ارتباطات و فناوری اطلاعات را تهیه و پیاده سازی نماید.

تهران، خیابان دکتر شریعتی، بالاتر از چهارراه شهید قدوسی (قصر)، ورودی شماره۴،ساختمان مرکزی
• کدپستی:۱۶۳۱۷۱۳۴۶۱

۳-۵) تامین و پیاده سازی نیازمندی های مرتبط با استقرار مرکز عملیات امنیت مشتمل بر :

۳-۵-۱) نیازمندی های نرم افزاری بشرح جدول ذیل:

ردیف	شرح	مشخصات لایسنس
۱	سامانه SIEMبومی	پیشنهاد مشاور-لایسنس مادام العمر و پشتیبانی یکساله
۲	سامانه OpenVAS	متن باز
۳	سامانه TheHive & Cortex	متن باز(سامانه تیکتینگ)
۴	Wazuh	متن باز
۵	سامانه Snort	متن باز
۶	سامانه های UBA & XDR	سامانه بومی

و همچنین سامانه های :

- سامانه تیکتینگ
- سامانهHIDS
- سیستم بازرسی قانونی
- استفاده از ML جهت شناسایی تهدیدات
- سیستم Intelligence Threat به صورت رسمی(نه محدود به سایتهای رایگان)
- راهکارهای UBA جهت شناسایی تهدیدات داخلی
- راهکارهای مقابله با بدافزار
- راهکارهای پیشگیری از نشر داده
- راهکارهای پایش صفحات وب مخرب
- راهکارهای پایش فعالیت پایگاه داده ها

تهران، خیابان دکتر شریعتی، بالاتر از چهارراه شهید قدوسی (قصر)، ورودی شماره۴،ساختمان مرکزی کدپستی:۱۶۳۱۷۱۳۴۶۱

۳-۵-۲) نیازمندی های مرتبط با حوزه نیروی انسانی متخصص بشرح جدول ذیل است که باید توسط مشاور در پروژه تامین گردد

ردیف	عنوان	میزان حضور	تعداد نفرات
۱	کارشناس تحلیلگر سطح یک	۸*۵ (ساعات اداری روزهای کاری)	۲ نفر
۲	کارشناس تحلیلگر سطح دو	۸*۵ (ساعات اداری روزهای کاری)	۱ نفر
۳	کارشناس تحلیلگر سطح سه *	۱ روز در هفته	۱ نفر
۴	مدیر مرکز *	بصورت موردی حسب نیاز پروژه	۱ نفر

*حسب شرایط پروژه و در صورت بروز حادثه امنیتی ممکن است براساس شرایط تعداد مراجعه تغییر نماید.

۴-۵) پیاده سازی و پیکر بندی مولفه های مرکز عملیات امنیت

قبل از شروع به پیاده سازی مرکز عملیات امنیت، مشاور موظف به اجرای موارد ذیل است :

- مشاور موظف است قبل از اجرای پروژه، لیست دارایی های که با موضوع مناقصه در ارتباط است را بررسی کرده و در صورت نیاز تمامی مستندات و لیست های موجود را بروزرسانی نماید.
- مشاور موظف است قبل از اجرای پروژه تمامی سرورها و سرویس های عملیاتی را به صورت کامل بررسی کرده و در صورت مشاهده هر گونه شواهدی از آلودگی به یک بدافزار مشاهده نمود، گزارش های لازم را ارائه نمائید.
- مشاور موظف است تمامی گزارش های آسیب پذیری موجود را بررسی و میزان ریسک آن را مشخص نماید و آن دسته از آسیب پذیری هایی که منجر به بروز اختلال در عملکرد مرکز SOC میشوند شناسایی و در صورت نیاز طرح خود برای رفع مشکل آن ها را ارائه کند.
- مشاور موظف است امن سازی و مقاوم سازی سرورها ، سرویس ها و زیرساخت ارتباطی و معماری شبکه در محدوده پروژه را مورد بررسی قرار داده و در صورت نیاز طراحی های لازم را برای بهبود و ارتقاء سطح امنیتی کارفرما ارائه دهد.
- مشاور موظف است تنظیمات تجهیزات و سامانه های امنیتی شامل فایروال ، فایروال سامانه های تحت وب و غیره را مورد بررسی قرار داده و نیازمندی های امنیتی مورد نیاز مرکز عملیات امنیتی را ارائه کند. به علاوه، پیمانکار بایستی توانمندی های لازم را داشته باشد که در صورت درخواست کارفرما و توافق طرفین، انجام تنظیمات و فرآیند بهینه سازی را بر روی تجهیزات و سامانه های امنیتی اعمال نماید.
- مشاور موظف است عملیات Hunting را در محدوده پروژه انجام داده که بتوان با تحلیل اطلاعات و رخدادها از نگاه امنیتی بر روی دارایی های، تهدیدات موجود را شناسایی و راهکارهایی عملیاتی بمنظور جلوگیری از وقوع حادثه را به کارفرما ارائه و اجرا نماید. به علاوه، پیمانکار بایستی توانمندی های لازم را داشته باشد که در صورت درخواست کارفرما عملیات امن سازی را نیز بر عهده گیرد.

- مشاور موظف است در فاز طراحی جانمایی تمامی سنسور های امنیتی مورد نیاز که در عملکرد مرکز SOC تاثیرگذار می باشند را شناسایی کرده و طرح جامعی را جهت استقرار سنسورها بر اساس وضعیت موجود ارائه کند.
- مشاور موظف است وضعیت امنیتی شبکه را بررسی کرده و در صورت نیاز طرح بهبود امنیت را به منظور نظارت و دسترسی نود های شبکه ای غیرمجاز به شبکه پیاده سازی کند. این راهکار بایستی با بخش مدیریت دارایی ابزار SIEM یکپارچه شود. لازم به ذکر است در این بخش لایسنس مادام العمر برای SIEM بومی ارائه دهد .
- مشاور موظف است علاوه بر گزارشات ماهیانه، گزارشات Security Advisory را با فرمت و بازه زمانی مشخص شده توسط کارفرما تهیه و ارائه نماید.
- مشاور موظف است استقرار کارشناسان به مدت یکسال راهبری مرکز را به نحو احسن و مطابق با SLA فی مابین انجام دهد.

پس از اتمام طراحی و تحویل مستندات مرکز عملیات امنیت سایبری بر اساس موارد مطروحه در مرحله قبل، مشاور موظف است نسبت به موارد ذیل اقدام نماید :

۴-۵-۱) تزریق اطلاعات توپولوژی شبکه، نام دارایی‌ها، وضعیت دارایی‌ها و آسیب‌پذیری‌ها به پایگاه دانش سیستم

۴-۵-۲)نصب، راه اندازی و تست مجتمع‌سازی اجزا و دریافت رخدادنماها از کلیه تجهیزات تنظیم شده

۴-۵-۳)تنظیم حسگرهای شبکه جهت انتقال رویدادها و جمع آوری آنها

۴-۵-۴)تنظیم تجهیزات جهت ارسال کپی ترافیک خام یا اطلاعات جریان ترافیک

۴-۵-۵)راه اندازی بخش کشف دارایی و ارزیابی آسیب پذیری و استخراج اطلاعات شبکه توسط آنها

۴-۵-۶)انتخاب و تعریف گزارش‌های لازم در سیستم متناسب با نیاز کارفرما

۴-۵-۷)انجام تنظیمات چرخش داده در سطح مدیریت رخدادنماها و مدیریت اطلاعات جریان

۴-۵-۸)تعریف داشبوردها و گزارشهای دلخواه متناسب با نیازمندیهای کارفرما

۴-۵-۹)بررسی انواع ورودی های دریافتی و تنظیم سطح رخدادنما در تجهیزات ارسال کننده

۴-۵-۱۰)سفارشی سازی و افزودن قوانین همبستگی مورد نیاز خاص بر طبق شرایط کارفرما

۴-۵-۱۱)بررسی الگوهای استخراج شده توسط بخش کشف الگو و تعریف قوانین وارسی و همبستگی مورد نیاز به تناسب شرایط شبکه و سیاستهای کارفرما

۴-۵-۱۲)بررسی خروجی‌های حملات اولیه سیستم و میزان‌سازی پایگاه‌دانش جهت کاهش خروجی‌های مثبت کاذب و افزایش کارایی سامانه در استفاده از منابع

۴-۵-۱۳)تعریف فیلترهای حذف تکراری و حذف رویدادهای ناخواسته در پلاگین های نرمال سازی

۴-۵-۱۴) پیاده سازی سامانه SIEM براساس موارد ذیل :

- پیمانکار موظف است سنسور های تحلیل ترافیک و حملات امنیتی را در تمامی مناطق امنیتی مهم در شبکه نصب کند و ترافیک های داخل VLAN های مهم شبکه را بررسی نماید.

تهران، خیابان دکتر شریعتی، بالاتر از چهارراه شهید قدوسی (قصر)، ورودی شماره۴،ساختمان نوران پستی:۱۶۳۱۷۱۳۴۶۱

- تمامی سرویس های مهم و حیاتی کارفرما مانند ایمیل سازمانی،پورتال و غیره بایستی بررسی و تحت نظارت سامانه SIEM قرار بگیرند و حملات مرتبط با هر یک از آنها ، به صورت کامل در ابزار SIEM شناسایی شوند.
- پیمانکار موظف است راهکارهای عملیاتی در خصوص دفاع و تشخیص حملات پیشرفته ای مثل Tunneling و ... را ارائه نماید.
- پیمانکار موظف است راهکارهای عملیاتی به منظور جلوگیری از حملات بر روی سامانه های وب کارفرما و افزایش امن پذیری آنها را ارائه نماید.
- پیمانکار موظف است تمامی فرآیند های ارتباطی بین مرکز SOC و سایر بخش های سازمانی را به صورت کامل طراحی و مستند کرده و آن را پیاده سازی نماید.
- پیمانکار موظف است در پیاده سازی مرکز SOC، افزونگی و Fault Tolerance را در تمامی لایه ها محقق سازد.
- پیمانکار موظف است در پیاده سازی مرکز SOC ، امکان توسعه و گسترش حوزه تحت پایش مرکز را درنظر گیرد.
- پیمانکار موظف است در پیاده سازی مرکز SOC، مانیتورینگ بلادرنگ و متمرکز رویدادها، اطلاع رسانی آلارم ها از طریق پیامک و یا ایمیل و ارائه داشبوردهای کارا جهت مصور سازی اطلاعات و رویدادها، را مدنظر قرار دهد.
- مشاور موظف است در مدیریت داده ها موارد زیر را رعایت نماید:
  - ایجاد بالاترین سطح فشرده سازی داده ها
  - ذخیره سازی اطلاعات بصورت رمز شده جهت استفاده در Forensics
  - ارسال و دریافت لاگ ها بصورت ایمن جهت حفظ محرمانگی و صحت داده ها در طول مسیر ارتباطی
  - طراحی مناسب برای اتصال به SAN و NAS جهت نگهداری لاگ ها به مدت حداقل یک سال
- مشاور موظف است در بروزرسانی انلاین و افلاین موارد زیر را رعایت نماید:
  - بروزرسانی قوانین همبستگی و امضاها
  - بروزرسانی پایگاه دانش سامانه ها
  - بروزرسانی ماژول های سامانه ها
- مشاور موظف است در دریافت لاگ موارد زیر را رعایت نماید:
  - امکان دریافت لاگ از مکانیزم های مختلفAgent base وAgentless نظیر syslog، Sysmon.SNMP و غیره
  - امکان نرمال سازی فرمت لاگ های دریافتی
  - امکان دریافت و تحلیل ترافیک های NetFlow از تجهیزات شبکه

- امکان فیلتر کردن پارامترهای لاگ های دریافتی

- مشاور موظف است در تحلیل لاگ برنامه های تحت وب موارد زیر را رعایت نماید:
  - دریافت لاگ و تحلیل لاگ تجهیز WAF
  - ساخت داشبورد و گزارشات Real-Time برای نمایش وضعیت وب سایت های حساس و حیاتی
  - انجام تنظیمات لازم جهت دریافت Mirror ترافیک وب و تحلیل و نمایش درخواست های رسیده به برنامه های کاربردی تحت وب
- مشاور موظف است در پایگاه دانش موارد زیر را رعایت نماید:
  - امکان بروزرسانی از داخل و امکان بروزرسانی افلاین از طریق فایل های مربوطه
  - امکان جستجو در نمونه رخدادهای قابل پشتیبانی در سامانه و بررسی خصوصیات و دسته بندی های انها
  - پشتیبانی از Threat Intelligence Feeds
  - قابلیت همگام سازی با سامانه اسکن آسیب پذیری های مورد استفاده
- مشاور موظف است در خصوص داشبوردها و گزارشات موارد زیر را رعایت نماید:
  - امکان ارائه گزارش از رویدادها و حملات به تفکیک
  - امکان ارائه گزارش از آسیب پذیری های تجهیزات سیستمی و شبکه ای
- با توجه به مطالب گفته شده،اهم اقدامات موررد انتظار در صورت بروز حادثه امنیتی عبارت اند از:
  - تطابق با چهارچوب یا استاندارد های بین المللی، رسمی و شناخته شده
  - تشکیل تیم واکنش به رخداد های امنیتی
  - آموزش تیم واکنش به رخداد
  - تدوین و پیاده سازی فرآیند ها و SOP های مدیریت حوادث
  - تدوین فرآیند های Escalation بین SOC و سایر بخش ها
  - راه اندازی خدمات شناسایی حوادث شامل شناسایی تهدید اولیه و ریشه یابی (RCA)
  - پیشنهاد، نصب و یکپارچه سازی نرم افزار های رایگان و متن باز جهت تسهیل فرآیند مدیریت حوادث (نظیر The hive)
  - راهکار سنجش عملکرد تیم واکنش به رخداد
  - راهکار ثبت و ذخیره سازی تمامی مدارک و شواهد دیجیتال
  - ارائه داشبورد آگاهی رسانی و Advisory
  - اطلاع رسانی امنیتی در حوزه خدمات پیشگیرانه

۴-۵-۱۵) پیاده سازی سامانه XDR

- تأمین، نصب و پیکربندی ابزارهای SIEM/XDR با قابلیت مقیاس‌پذیری.
- تنظیم Ruleها، همبستگی رویدادها، تحلیل رفتار کاربران، و پاسخ‌دهی خودکار

۴-۵-۱۶) پیاده سازی ISMS

- تحلیل Gap، تهیه سیاست‌ها و رویه‌ها، اجرای ممیزی داخلی.
- پیاده سازی طرح ISMS مطابق با استاندارد ISO/IEC ۲۷۰۰۱.

۴-۵-۱۷) اجرای خدمات خودکارسازی و عملکرد سامانه بر اساس هوش مصنوعی

با توجه به حساسیت کسب وکار مورد بحث و نواحی تحت پوشش و همچنین محدودیت های استفاده از نیروهای متخصص، پیشنهاد دهنده الزاماً می بایست برای راهکاری که ارائه می دهد، مؤلفه های مرتبط با خودکارسازی را که در ادامه به ویژگی های اصلی و مهم آن خواهیم پرداخت، بیافزاید. در راهکار ارائه شده برای سامانه های SIEM می بایست ویژگی خودکارسازی با شرایط زیر موجود باشد:

- ارسال خودکار هر تهدید شناسایی شده به تفکیک سطح مخاطره تهدید به سامانه اعلان و اخطار تهدیدات (Ticketing)
- غنی سازی تهدید دریافتی از SIEM توسط سامانه مذبور و بازارسال (Forward) آنها برای مسئول یا ذینفع مشخص شده بصورت خودکار.
- امکان اعلان بسته تحلیلی شناسایی شده با قابلیت Customization فیلدهای تشکیل دهنده آن، به صورت ایمیل، پیامک و مهمتر از همه به یک پیامرسان (Messenger) که ویژگی یکپارچگی با سامانه های SIEM و Ticketing را از طریق API در آن فراهم باشد، از مهمترین امکانات راهکار پیشنهادی باید باشد.
- امکان واکنش به رخداد شناسایی شده با کمک Script های متنوع و قابل توسعه با زبان های رایج مانند Python, Bash
- ارائه راهکار نهایی بر اساس تصمیم گیری هوش مصنوعی (Machine Learning Toolkit App) در لایه های مختلف از مرحله تولید بسته نتایج همبسته سنجی تا مرحله ثبت در پایگاه داده.

لازم بذکر موارد فوق الذکر الزاماً باید در یکپارچگی حداکثری با SIEM بوده تا بتوان از آن برای مقاصد مختلف بالاخص در شناسایی تهدیدات مبتنی بر رفتارسنجی ترافیک استفاده گردد.

۵-۵) ارایه خدمات امنیتی مستمر در مرکز SOC

۵-۵-۱) ارایه خدمات مستمر راهبری مرکز SOC

- با توجه به اینکه وزارت ارتباطات و فناوری اطلاعات در نظر دارد عملیات راهبری و پشتیبانی مرکز SOC خود را پس از پس از اتمام فاز راه اندازی به مدت ۱۲ ماه به شرکت منتخب واگذار نماید انتظار میرود سطح سرویس مورد نظر توسط پیمانکار رعایت شده و در مدت یک سال دانش راهبری ابزار مستقر شده به پرسنل کارفرما منتقل شود و در صورتی که کارفرما متناسب با شرایط زمانی تصمیم به راهبری سامانه را داشت، قادر به انجام آن باشد. همچنین با توجه به این مهم که پیمانکار موظف به تامین نیروی انسانی متخصص به منظور پایش و رصد رخداد ها را برعهده خواهند داشت. اهم اقدامات مدنظر در فاز راهبری عبارت اند از:

- حضور نیروهای مقیم در سطح کارشناس شناسایی رخدادها و کارشناس پاسخدهی به رخدادها در روز های حساس و تعطیلی ها
- مدیریت ، راهبری و بهینه سازی سامانه ها و ابزار های موضوع مناقصه به مدت یک سال پس از اتمام فاز راه اندازی
- پوشش کامل مدیریت چرخه حوادث در سطح کارفرما شامل خدمات تحلیل لاگ و ترافیک، ترياژ، تحلیل آسیب پذیری ، واکنش به حوادث امنیتی و غیره مطابق SLA مورد توافقی
- بروزرسانی لیست دارایی ها و موجودیت ها در محدوده موضوع مناقصه
- رصد مستمر فضای سایبری، شناسایی تهدیدات و اجرای عملیات حفاظتی در برابر آنها
- تهیه گزارش های موردی و دوره ای (ماهانه) به صورت کارشناسی و مدیریتی
- برخورد ویژه با تمامی آسیب پذیری هایی که در سطح جهانی عمومی شده اند و برای آنها Exploit ارائه شده است
- ایجاد Signature های تخصصی برای کارفرما به منظور مقابله با تهدیدات مهم
- تحلیل ترافیک و شناسایی حملات و رفتار های مشکوک با استفاده از Signature های تجاری

۵-۵-۲) ارایه خدمات شناسایی و تحلیل رخدادهای حاصله از تغییرات در لایه های مختلف سرویس

در بسته راهکار نهایی ارائه شده، پیشنهاد دهنده محترم می بایست برای شناسایی و اعلان هرگونه تغییرات در لایه های مختلف از جمله موارد زیر راهکاری کامل و در یکپارچگی کامل با سامانه های SIEM ارائه دهد.

- تغییر در فایلهای سیستمی و یا غیر سیستمی (File Systems, or Non-System Files)
- فایل های تنظیمات سرویس ها (Configuration Files)
- کلیدهای رجیستری (Registry Keys)
- کتابخانه های سیستم عامل (Libraries files dll, ...)
- هر گونه فایلی که در سیستم عامل نقشی در ارائه سرویس عملیاتی کسب و کار داشته باشد

از دیگر ویژگی های مورد انتظار می توان به موارد ذیل اشاره نمود:

- قابلیت تطبیق با مراجع معتبر مانند NIST, PCI-DSS و ...
- قابلیت ارائه داشبوردهای درلحظه و Real-Time
- قابلیت ارسال تیکت یا اخطار با فرمت های Email, SMS, Sent to ۳th Party Apps
- قابلیت شناسایی محتوای تغییر یافته در فایل های تحت پایش (Content Base Monitoring)
- قابلیت شناسایی تغییرات بر اساس Previous Base-Lines با کمک Hash-Code های مرجع
- قابلیت تولید گزارشات دوره ای

تهران، خیابان دکتر شریعتی، بالاتر از چهارراه شهید قدوسی (قصر)، ورودی شماره۴،ساختمان مرکزی
● کدپستی:۱۶۳۱۷۱۳۴۶۱

۶-۵) آموزش ، انتقال دانش و تحویل مستندات

مشاور موظف است در راستای اجرای پروژه، نسبت به آموزش و انتقال دانش لازم در زمینه موضوع پروژه به کارکنان و متخصصان کارفرما اقدام لازم را صورت داده و نسبت به تهیه و تحویل مستندات کامل پروژه از زمان شروع تا زمان اتمام آن به نمایندگان کارفرما اقدام نماید.

٦ – تبیین فازهای کاری و زمان‌بندی پروژه

فاز	شرح فازهای کاری	مدت زمان	درصد	برآورد هزینه (ریال)
۱	تحلیل وضع موجود به همراه تأمین، طراحی و نصب نیازمندی های نرم افزاری (ابزار بومی SIEM)	۱۵ روز		
۲	طراحی و نصب نیازمندی های نرم (ابزار بومیUBA،XDR)	۳۰روز		
۳	اجرای خدمات تست نفوذ ، اجرای طرح Network Auditing و مقاوم سازی شبکه	۴۵ روز		
۴	طراحی، اجرا و استقرار مرکز عملیات امنیت (SOC) به همراه طرح مدیریت امنیت اطلاعات (ISMS)	۹۰ روز		
۵	اجرای خدمات مستمر امنیت و ارایه گزارشات مدون	۳۶۵ روز		

۷- روش ارزیابی سطح خدمات SLA و جرائم پروژه

اولویت یک حادثه یا رویداد امنیتی بر اساس معیارهای زیر مشخص می‌گردد:

- نوع حادثه یا رویداد
- اهمیت حادثه یا رویداد
- میزان (شدت) حادثه یا رویداد

لازم بذکر ا ست این طبقه‌بندی بر ا ساس نوع حادثه یا رویداد و اهمیت آن با توجه به شرایط سرویس یا تجهیز موجود انجام می‌گردد.جدول زیر نحوه محاسبه اولویت با دو معیار میزان اهمیت و میزان حساسیت (شدت) رویداد یا رخداد را بر اساس رویکرد تجهیز SIEM، سامانه تیکتینگ و سطوح را بررسی و مشخص میکند:

Analyze Matrix									
SIEM Rating	۱	۲	۳	٤	٥	٦	۷	۸	۹ ۱۰
Level Priority	Very Low		Low		Medium		High		very High

Probability Rating	P۳	P۲	P۱

جدول زیر تعریف احتمال‌های اختصاص‌یافته در ماتریس ارزیابی را توضیح میدهد.

Probability Rating	Descriptions
P۱	Very High severity incident. Incident at this level will have devastating effect, without an immediate response will cause to significant operation downtime to the organization; significant damage, corruption or loss of critical information and damage to the IT capabilities of the organization.
P۲	High and Medium severity incident. Incident at this level is potentially dangerous, without careful management and implementation of appropriate safeguard measures will escalate to high-risk incident.
P۳	Low and Very Low severity incident. Incident at this level is controllable and should be straightforward to avoid and manage with the right safeguard measure and response; any potential impact can be reduced at minimal cost.

باتوجه به جداول فوق و درنظر گرفتن دو فاکتور Ticket Workaround و Ticket Acknowledgment،به ازای هر SLA در اولویت های ۱،۲ و ۳ ، زمان های T۱,T۲و T۳ به شرح زیر مدنظر می باشند:

جدول ۱: زمانبندی شناسایی و رفع

	T۱ (شناسایی و تشخیص)	T۲ (ریشه یابی و ارائه راهکار)	T۳ (مرتفع نمودن و بروزرسانیKB)
P۱	کمتر از ۶ ساعت	کمتر از ۱۲ ساعت	کمتر از ۲۴ ساعت
P۲	کمتر از ۱۰ ساعت	کمتر از ۱۸ ساعت	کمتر از ۳۶ ساعت
P۳	کمتر از ۲۴ ساعت	کمتر از ۳۶ ساعت	کمتر از ۴۸ ساعت

لازم بذکر است که رویدادها و رخدادهای امنیتی با سطوح متوسط، زیاد و خیلی زیاد به صورت حادثه امنیتی شناسایی می شوند در عمل می‌توان این سطوح را در هنگام بروز حادثه به گروه با اولویت بالاتر و سریع‌تر جهت بررسی بیشتر منتقل نمود باتوجه به توضیحات فوق، سطح SLA مورد انتظار به شرح جدول زیر می باشد:

SLA			
ردیف	نوع خدمات	سطح خدما مورد انتظار	جرائم عدم ارائه خدمات
۱.	Monitoring & Incident Alerting	- مانیتورینگ ۷×۲۴×۳۶۵ها در چهار سطح: ○ اولویت بحرانی ○ اولویت بالا ○ اولویت متوسط ○ اولویت پائین -ثبت تیکت برای تمامی رخدادها در تمامی سطوح به شرح ارزیابی سطح خدمات	● انجام تعهدات ۸۰٪ به بالا؛ بدون جریمه ● انجام تعهدات ۷۰ تا ۸۰٪ ؛ معادل ۱ درصد از پرداخت ماهانه ● انجام تعهدات ۶۰ تا ۷۰٪ ؛ معادل ۲ درصد از پرداخت ماهانه ● انجام تعهدات ۵۰ تا ۶۰٪ ؛ معادل ۳ درصد از پرداخت ماهانه ● انجام تعهدات زیر ۵۰٪ ؛ معادل ۱۰ درصد از پرداخت ماهانه
۲.	Network Threat Hunting Details	- ارسال جزئیات مربوطه بصورت ماهانه	● معادل ۵ درصد از پرداخت ماهانه
۳.	Reports Dashboards	-ارائه گزارشات ماهانه تا سوم هر ماه -ارائه گزارشات فصلی تا ۱۰ روز پس از اتمام فصل -ارائه دسترسی به داشبورد های مرکز SOC بصورت ۷×۲۴×۳۶۵ -ارائه دسترسی به سامانه تیکتینگ مرکز SOC بصورت ۷×۲۴×۳۶۵	● معادل ۵ درصد از پرداخت ماهانه
۴.	Service uptime	-ضمانت بالا بودن سرویس های پروژه موضوع قرارداد بصورت ۷×۲۴×۳۶۵	●انجام تعهدات ۹۵٪ به بالا؛ بدون جریمه ●انجام تعهدات ۹۰ تا ۹۵٪ ؛ معادل ۱ درصد از پرداخت ماهانه ●انجام تعهدات ۸۵ تا ۹۰٪ ؛ معادل ۳ درصد از پرداخت ماهانه ●انجام تعهدات ۸۰ تا ۸۵٪ ؛ معادل ۵ درصد از پرداخت ماهانه ●انجام تعهدات زیر ۸۰٪ ؛ معادل ۱۰ درصد از پرداخت ماهانه