درخواست برای ارائه پیشنهاد (RFP)

جهت پروژه

استقرار، راه‌اندازی و پشتیبانی سیستم مدیریت وقایع و رخدادهای امنیتی(SIEM)

مقدمه

با توجه به افزایش ارزش داده‌ها و منابع اطلاعاتی در سازمان و اهمیت مقوله امنیت در حوزه فناوری اطلاعات، پالایشگاه گاز فجر جم در نظر دارد سطح امنیت اطلاعات در بستر شبکه های داخلی (اینترانت) و شبکه اینترنت خود را با بهره‌گیری از راه‌حل‌های هوشمند و یکپارچه تحت عنوان سیستم مدیریت وقایع و رخدادهای امنیتی ارتقاء بخشد.

سیستم مدیریت وقایع و رخدادهای امنیتی تمامی زوایای امنیتی را به صورت بلادرنگ از یک نقطه مرکزی مدیریت و مانیتور می‌کند و تمامی حوادث امنیتی را کشف کرده، سطح ریسک و دارایی‌هایی که تحت تاثیر قرار خواهند گرفت را تشخیص می‌دهد. اگرچه ممکن است هرکدام از تجهیزات امنیتی هشدارهایی را در ارتباط با حملات ایجاد کنند لیکن به دلیل حجم بالای هشدارها و ناهمگن بودن آنها، همچنین اعلام هشدارهای نادرست و رویدادهای شناسایی نشده، عدم وجود ارتباط بین هشدارهای صادر شده از دستگاههای مختلف و نبود سوابق و اولویت هشدارها، نمی توان از تیم امنیتی سازمان انتظار سرعت و دقت لازم در مواجهه با حملات را داشت

شرح کلی پروژه:

پروژه به صورت زیر تعریف گردیده و به شرح ذیل می باشد:

ردیف	نام پروژه	اقدامات هر بخش
۱	استقرار، راه‌اندازی و پشتیبانی سیستم مدیریت وقایع و رخدادهای امنیتی	شناخت سازمان و نیازمندی های دقیق مشتری
		طراحی محیط پیاده سازی
		استقرار و پیاده سازی سامانه
		بهینه سازی سامانه طبق خروجی های فاز شناخت و منطبق کردن سامانه بر اساس کسب و کار سازمان
		آموزش و تحویل
		پشتیبانی و بروزرسانی

*تامین تجهیزات سخت افزاری و سرورهای مورد نیاز متناسب با EPD اعلام شده به عهده کارفرما می باشد.

محدوده فیزیکی پروژه:

ستاد مرکزی شرکت پالایشگاه گاز فجر جم

اهداف مورد نظر برای اجرای پروژه: پیاده سازی سیستم مدیریت وقایع و رخدادهای امنیتی

هدف از اجرای این پروژه ایجاد زیرساختهای لازم به منظور رسیدن به اهداف ذیل در آینده می باشد:

- ارزیابی و بررسی رخدادها و حوادث بصورت آنلاین
- کاهش مدت زمان لازم برای جمع‌آوری اطلاعات رخدادها و هشدارها در مواقع ضروری
- مدیریت نگهداری و پردازش و تحلیل اطلاعات رخدادها و هشدارها و کشف ارتباط بین آن‌ها
- تداوم کسب و کار شرکت و جلوگیری از قطع سرویس‌ها
- شناسایی تهدیدات امنیتی بالقوه و بالفعل در شرکت
- مانیتورینگ، شناسایی و آنالیز نفوذهای پنهانی
- واکنش به تهدیدهای شناسایی شده با هماهنگی منابع و اقدام به موقع

به منظور راه‌اندازی سیستم مدیریت وقایع و رخدادهای امنیتی فازهای اجرایی ذیل در نظر گرفته شده است:

فاز اول، شناخت

در این مرحله ابتدا باید اجزاء و ساختار بخش‌های مختلف سازمان از لحاظ امنیتی و همچنین نیازمندی‌های ادامه‌ی کسب و کار وابسته به فناوری اطلاعات مورد بررسی قرار داد تا بتوان در مورد خطرات احتمالی و نقاط حساس و حیاتی هر دپارتمان و یا کل سازمان دیدی کلی بدست آورد و برای پیاده‌سازی طرح فنی مناسب را تهیه و ارائه نمود. مواردی که در این فاز مورد بررسی قرار می‌گیرند به شرح زیر می باشند:

- شناخت سازمان
- شناخت دغدغه‌های امنیتی سازمان
- شناخت فرآیندها، فعالیت‌ها، کسب و کار و سرویس‌های ارائه شده در سازمان
- شناخت دارایی‌های سایبری سازمان
- شناخت حوزه تهدیدات سازمان
- شناخت سیاست‌های امنیتی مختص سازمان

فاز دوم، طراحی

بررسی اسناد ارائه‌شده شامل :

- تدوین مستندات فاز شناخت و چالش‌های سازمان
- تدوین مستند پیش نیازها و ساختار نصب
- تدوین مستند مانیتورینگ دارایی‌ها

- تدوین مستند سیاست‌های امنیتی
- تدوین مستند روال گزارش‌گیری و بررسی گزارشات
- تدوین مستند منابع انسانی
- تدوین مستند سیستم‌های تولید جریان شبکه و تشخیص نفوذ مبتنی بر میزبان و شبکه

فاز سوم، استقرار و پیاده‌سازی

- نصب و راه‌اندازی زیرساخت نرم‌افزاری سامانه به همراه اعمال لایسنس ماژول‌های سامانه
- انجام تنظیمات لازم در شبکه و حسگرها جهت دریافت LOGها
- بررسی و حصول اطمینان از دریافت LOG از حسگرها

در راستای ارتقاء سطح امنیت شبکه، پیاده‌سازی سامانه مدیریت رویداد و اطلاعات امنیتی با معماری Distributed در شبکه‌های داخلی (اینترانت) (EPD) Event Per Day (350 GB) و شبکه اینترنت (EPD) Event Per Day(150 GB) مدنظر می‌باشد و محصول به کار گرفته شده علاوه بر قابلیت پاسخگویی بایستی به نحوی ارتقاء یابد که قابلیت‌های ذیل را پوشش دهد:

ماژول‌های سامانه	ویژگی‌ها و قابلیت‌ها
تجمیع کننده Log	• قابلیت دریافت اطلاعات از انواع منابع تولید لاگ اعم از تجهیزات امنیتی، سرورها و تجهیزات ذخیره‌سازی • قابلیت تعریف فیلترهای مختلف جهت دریافت لاگ های مورد نیاز و حذف لاگ‌های نامرتبط • قابلیت فشرده‌سازی و رمزنگاری در هنگام ارسال اطلاعات به سامانه • قابلیت حفظ محرمانگی و صحت در هنگام ارسال اطلاعات به سامانه • قابلیت افزودن هر نوع کاربرد یا تجهیز جدید خاص به سامانه • قابلیت دریافت و آنالیز امنیتی ترافیک Netflow از تجهیزات شبکه و امنیت شبکه • قابلیت پشتیبانی از پروتکل‌های مختلف از قبیل syslog و ... • سامانه امکان دریافت لاگها از تمامی سامانه ها، پلتفرم ها، سیستم عامل ها و تجهیزات شبکه، توسط Agent و یا پروتکل های ارتباطی نظیر آن را داشته باشد. • سامانه می بایست قابلیت تجمیع، نرمالیزه کردن و Correlation داده های لاگ و تحلیل آنها را داشته باشد. • پشتیبانی از سنسور های تجهیزات شبکه، پایگاه های داده، سیستم های عامل سرویس های موجود شبکه وغیره، جهت جمع آوری لاگهای شبکه • قابلیت دریافت رخدادها به دو صورت Agent-based و Agentless

	• امکان مدیریت مرکزی Agentها و به روزرسانی آن ها • برچسب زنی داده های ورودی متناسب با Zoneها و شرکت های تابعه و طراحی داشبوردها متناسب با برچسب های واردشده • امکان تعریف و حذف لاگ های نامرتبط
ذخیره رخدادها	• قابلیت نگهداری رخدادها در مراکز داده به مدت طولانی جهت استفاده در جرم‌شناسی دیجیتالی • قابلیت پشتیبانی از قالب‌های داده استاندارد برای نگهداری حمله و حادثه • قابلیت پشتیبانی از retention policy های استاندارد نظیر Hot، Warm و Archive. • مستقل از حالت داده آنلاین که میتواند Hot یا warm باشد باید به صورت real time قابلیت نمایش گرافیکی داده و انجام جستجوی سناریوهای امنیتی وجود داشته باشد. داده های آفلاین نیز بعد از بازیابی مجددا دارای همین قابلیت باشند. • قابلیت آرشیو داده به صورت امن • قابلیت پیاده‌سازی آرشیو داده بر روی انواع راهکارهای ذخیره‌سازی داده. • سامانه بایستی از ساختار موتورهای جستجو برخوردار بوده و از قابلیت indexing چند منظوره، سریع، دقیق و هوشمند جهت واکشی داده‌ها به منظور انجام جستجوهای دقیق روی پایگاه داده و تأمین اطلاعات ورودی برای سایر اپلیکیشن‌ها، برخوردار باشد. • قابلیت دریافت گزارش های مختلف از رویدادها و حوادث به صورت لحظه ای و دوره ای و زمانبندی شده
موتور همبستگی سنجی	• قابلیت تشخیص حملات چندگامی و آهسته با پنجره زمانی • قابلیت تحلیل هشدارهای حسگرهای امنیتی در کنار رویدادهای دیگر حسگرهای شبکه • وجود سناریوهای از پیش تعیین شده جهت تشخیص حملات • قابلیت پایش رخدادها و اعلام حملات • قابلیت ایجاد سناریوهای موردنظر و سناریوهای پیچیده به تعداد نامحدود • قابلیت تشخیص حملات پیچیده با توجه به سناریوهای پیش فرض و ایجاد شده • امکان استفاده از رخدادهای ثبت شده توسط ابزارهای امنیتی در تشخیص حملات • قابلیت پیاده سازی سیاست های امنیتی سازمان در سامانه و استفاده از آنها در تشخیص حملات

	• قابلیت تشخیص حملات براساس رفتار شبکه و تشخیص رفتارهای غیرمعمول • نمایش داده های حمله براساس نوع حمله، مبدأ، مقصد، سطح ریسک و تعداد رویدادها • قابلیت به روز رسانی سناریوهای امنیتی • قابلیت تولید و پیرایش امضاها و قوانین شخصی سازی شده • قابلیت یکپارچه سازی با دستگاه های فعال مانند فایروال ها یا سوییچ های شبکه • قابیلت استفاده از مفاهیم refrence به داده های از پیش تعریف شده مانند list، Table و موارد مشابه در تعریف سناریو (مانند لیست یوزرهای admin، لیست ipهای whitelist/blacklist) • امکان اضافه کردن موارد جدید به صورت خودکار به refrenceهای از قبل تعریف شده • ارسال حوادث در فرمت IODEF به مراکز بالادستی
مدیریت حوادث	• قابلیت اعلام رخدادهای امنیتی مورد نظر کارشناسان توسط پیامک و ایمیل یا اتصال به سیستم های تیکتینگ Third Party • وجود اقدامات مورد نیاز به ازای هر سناریوی امنیتی شناسایی شده توسط موتور همبسته سازی • امکان تخصیص alarmها به افراد مختلف برای انجام اقدامات مقتضی بعدی • قابلیت یادداشت گذاری بر روی رخدادهای امنیتی توسط افراد مختلف SOC • ارسال هشدارهای مربوطه از طریق پیامک و ایمیل • ارائه گزارشی از Stateهای مختلف مرتبط با رویدادهای امنیتی (Detection، Triage، ....) • قابلیت تعریف Tagهای شخصی سازی شده سازمان بر روی قوانین خودکار و هشدارها • توانایی انجام انواع اقدام های notification و اقدام های فعال (SOAR) بعد از بررسی False Positiveها و اطمینان از صحت هشدار امنیتی • ثبت کلیه اعمالی که در فرایند مدیریت حوادث توسط کاربران SOC انجام گردیده است.
واسط کاربر	• قابلیت ایجاد و مدیریت کاربران • قابلیت تعیین محدوده دسترسی برای کاربران سامانه براساس دانش و مسئولیت های کارشناسان • رابط کاربر یکپارچه و کاربرپسند • راهبری آسان جهت ساخت فیلترها و گزارشات و سناریوهای مورد نیاز سازمان • وجود گزارشات آماری و نموداری پیش فرض براساس استانداردها و تطابق ها

	• داشبورد وضعیت امنیتی و وضعیت کلی سامانه و اجزای آن • رابط کاربری تحت وب • مدیریت متمرکز ماژول های سامانه • داشبورد پایش وضعیت منابع سامانه • قابلیت جستجوی پیشرفته بر روی رویدادهای قدیمی و بلادرنگ • قابلیت تعریف visualizeهای دلخواه کارفرما بدون نیاز به تعامل با شرکت و تیم توسعه محصول • قابلیت جستجو بر روی همه داده ها ذخیره شده در بازه های زمانی مختلف گذشته و نمایش خروجی های visualize ها متناسب با زمان تعیین شده • قابلیت داشبورد پویا: در صورت تعریف داشبوردی متشکل از visualizeهای مختلف، تنها با تغییر فیلتر، بازه زمانی یا کلیک بر روی مقادیر نمایش داده شده در داشبورد، کلیه نمایش های گرافیکی با توجه به فیلتر و زمان جدید به روزرسانی گردد. بدون اینکه نیاز باشد تا فیلتر هر visualize به صورت مستقل تغییر کند. • قابلیت گزارش گیری از همه داشبوردهای از پیش تعریف شده و امکان ارسال ایمیل دوره ای به کارشناسان و مدیران مربوطه
پایش جریان ترافیک داده‌های شبکه	• قابلیت دریافت گزارش‌های Netflow علاوه بر استخراج اطلاعات جریان از ترافیک خام • آنالیز ترافیک شبکه • قابلیت یادگیری ماشین (Machin Learning) • قابلیت تشخیص Anomaly • قابلیت تحلیل و نمایش داده‌های کلان • قابلیت تشخیص حملات DDOS • قابلیت پایش ترافیک و میزان تبادل داده‌ها در شبکه • قابلیت ایجاد گزارشات مرتبط با ترافیک داده ها
لیست داشبوردها	• داشبورد نشان دهنده وضعیت Alertهای صادر شده توسط سامانه • وضعیت Malwareهای شناسایی شده • وضعیت هشدارهای صادر شده توسط ماژول‌های IDPS

	• وضعیت Traffic تولید شده • وضعیت Authentication ها • نمایش Changeهای صورت گرفته • داشبورد Web • داشبورد DNS • داشبورد IOC • داشبوردهای Video Wall • داشبوردهای Linux • داشبوردهای Windows • داشبورد Data Base • داشبورد Email • داشبوردهای Metricbeat • داشبوردهای وضعیت کارکرد سیستم • قابلیت افزودن سایر داشبوردهای امنیتی مورد نیاز مرکز عملیات امنیتی به تعداد نامحدود • قابلیت فیلتر کردن نمایش حملات براساس IP ، سرویس، نوع حمله، زمان حمله و غیره • قابلیت نمایش دیاگرام ها و نمودارهای گرافیکی انواع حملات بر روی هر یک از دارایی‌های سیستمی و شبکه‌ای در بازه‌های زمانی مشخص شده توسط راهبر
Agentها	• پشتیبانی از سیستم عامل های Linux و Windows • قابلیت انجام Passive Vulnerability Scan با مقایسه کتابخانه های نصب شده در سرور و مقایسه با دیتابیس آسیب پذیری ها • فیلتر کردن رخدادهای نویزی
مدیریت آسیب‌پذیری	• انجام Active Scan به صورت مداوم و زمان بندی شده • بررسی و اعلام آسیب‌پذیری‌های موجود در سیستم‌ها • یکپارچگی با محصولاتی نظیر Nessus و انجام دوره ای اسکن آسیب پذیری • قابلیت پویش تاریخچه اسکن های انجام شده و خروجی های آنها

	• قابلیت گزارش گیری گرافیکی از نتایج اسکن آسیب پذیری
ویژگی‌های کلی راهکار	• قابلیت توزیع‌پذیری با توجه به معماری شبکه • توسعه‌پذیری بومی سامانه و تمامی زیرسامانه‌های آن • امنیت ارتباط بین اجزای سامانه و برخورداری از مدل امنیتی • پشتیبانی از Replica در سطح داده در پایگاه داده های مجزا به نحوی که در صورت بروز مشکل در سخت افزار، تاثیری در کیفیت و خروجی عملکرد تیم SOC ایجاد نگردد. • پشتیبانی از HA به صورت Active-Active در سطح ماژول های سامانه به منظور مقابله با حوادث غیرمترقبه و اطمینان از عدم قطعی در سامانه • قابلیت مقیاس پذیری متناسب با نیازمندی های سازمان در تمامی سطوح سامانه • قابلیت پشتیبانی از ساختار سلسله مراتبی • پشتیبانی از به روزرسانی سلسله مراتبی • پشتیبانی از دریافت هشدارهای سلسله مراتبی • استفاده از Broker در سطح ماژول های سامانه به منظور مدیریت قطعی دسترسی شبکه در مواقع بحران • قابلیت پشتیبانی Retention Policy در حالت های مختلف Hot، Warm و Cold به منظور مدیریت بهینه منابع و دسترس پذیری به موقع به داده های مورد نیاز سازمان
قابلیت گزارش‌گیری	• قابلیت تهیه گزارش از رویدادها وحملات به تفکیک • قابلیت ذخیره‌سازی گزارش با قالب‌های CSV، PDF، و ... .
سیستم Ticketing	• قابلیت دریافت اطلاعات هشدارهای SIEM به منظور رسیدگی به آن رویداد • قابلیت تعریف Ticket مستقل از موتور همبسته سازی SIEM • قابلیت اتصال با سرور ایمیل سازمان • قابلیت پیگیری گردش Ticket • امکان Assign کردن هشدارها به افراد SOC متناسب با احراز هویت سامانه SIEM • امکان یادداشت گذاری بر روی ticketها • امکان تعیین Severity و Reliability تیکت ایجاد شده

	• امکان انجام اقدام های notification و فعال (SOAR) بر روی خرجی Ticketها • مشاهده کلیه فعالیت هایی که توسط تیم SOC بر روی Ticket مربوطه انجام گرفته است.
تطابق با الزامات و استانداردها	• تعریف Correlation Rule های محصول SIEM پیشنهادی می بایست با الزامات Matrix MITRE تطابق داشته باشد

فاز چهارم، بهینه‌سازی و پیکربندی

- بررسی خروجی‌های اولیه سامانه متناسب با فعالیت سازمان و ساختار شبکه
- سفارشی‌سازی دانش تشخیص و تحلیل حمل‌ات متناسب با شرایط سازمان
- به‌روزرسانی قوانین وارسی و سیاست‌های امنیتی با مشارکت سازمان
- تعیین و اجرای سیاست‌های حذف لاگ‌های قدیمی بر اساس نیازمندی سازمان
- ایجاد داشبوردهای مورد نیاز کارشناسان امنیت
- ایجاد داشبوردها امنیتی
- دریافت لاگ‌های امنیتی از منابع رخداد مورد نیاز
- تست میزان EPS قابل تحمل سخت‌افزار مستقر شده در سازمان
- به‌روزرسانی پلاگین‌های نرمال‌سازی و قوانین همبستگی در صورت لزوم

فاز پنجم، آموزش و تحویل

- آموزش‌های لازم جهت افزودن سنسورهای جدید به سامانه
- آموزش‌های لازم جهت بررسی و دسته‌بندی رخدادها
- آموزش‌های لازم جهت استفاده از گزارشات پیش‌فرض
- آموزش‌های لازم جهت ایجاد گزارشات و داشبوردهای مورد نیاز کارشناسان و مدیران
- آموزش Tuning سامانه و حذف لاگ‌های Noise
- آموزش روش‌های ایجاد Ticket و اعلام حوادث امنیتی در سامانه
- آموزش ایجاد سناریوهای مورد نیاز کارشناسان
- برگزاری دوره آموزشی راهبری و کاربری سامانه

- تحویل کلیه مستندات کاربری سیستم
- تحویل تمامی مستندات پیشنهادی جهت بهینه‌سازی سیستم

فاز ششم، پشتیبانی و بروزرسانی

در دوره پشتیبانی، پیمانکار با توجه به بروزرسانی‌هایی که بر روی سامانه SIEM انجام می‌دهد، موظف است این بروزرسانی‌ها را بصورت آنلاین، حضوری و یا به صورت ارائه یک یا چند فایل بروزرسانی در اختیار کارفرما قرار دهد تا از طریق رابط کاربری این بروزرسانی‌ها در سامانه انجام گیرد. بروز رسانی‌های مذکور شامل موارد زیر می‌باشد:

- ارائه قابلیت‌های جدید
- توسعه پایگاه دانش
- ارائه آخرین نسخه محصول و افزونه‌های بروزرسانی همراه با گزارش ریسک‌های مرتبط به نصب آنها
- اعمال هر نوع تغییرات در فاز پشتیبانی تنها با اخذ مجوز از کارفرما باید انجام پذیرد.
- بروزرسانی برخط و یا آفلاین ماژول‌هایVulnerability Management و Intrusion Detection System توسط پیمانکار
- پاسخگویی و رفع مشکلات به صورت حضوری و غیرحضوری
- بازدید دوره ای از سامانه
- به روزرسانی Threat Intelligence
- مشاوره امنیتی مرتبط با محصولSIEM

زمان پشتیبانی و پاسخگویی می بایست در ساعات اداری و در زمان های اضطراری از طریق یک سیستم تیکتینگ مشخص انجام پذیرد.

مدت زمان اجرای پروژه

طول مدت اجرای فازهای عملیاتی طبق موارد بیان شده در شرح کلی پروژه، به مدت ۳ ماه برای فاز ۱ تا ۵ است.

نحوه ارائه پیشنهاد فنی

پیشنهاد دهندگان می‌بایست شناخت دقیقی از نیازهای سازمان حاصل نموده و طرح پیشنهادی خود را با لحاظ نمودن موارد بیان شده ارائه نمایند.

شرایط الزام شرکت در مناقصه

- دارا بودن پروانه فعال در حوزه خدمات عملیاتی افتا شامل "پیاده‌سازی مرکز عملیات امنیت (SOC) و تیم پاسخ به رخداد " و "راهبری مرکز عملیات امنیت (SOC) و تیم پاسخ به رخداد".
- دارا بودن پروانه فعالیت در حوزه خدمات عملیاتی افتا شامل" امن سازی و مقاوم سازی سامانه ها، زیرساخت ها و سرویس ها"
- دارا بودن گواهی رتبه‌بندی شرکت در شورای عالی انفورماتیک کشور در زمینه امنیت فضای تولید و تبادل اطلاعات با رتبه **یک**.
- دارا بودن گواهی رتبه‌بندی شرکت در شورای عالی انفورماتیک کشور در زمینه پشتیبانی با رتبه **یک**

- دارا بودن سابقه کار مرتبط با موضوع استعلام و ارائه مدارک و رضایت نامه کتبی کارفرمایان قبلی (حداقل ۱۰ مورد)

ارزیابی پیشنهاد دهندگان

پیشنهاد دهندگان لازم است به همراه قیمت پیشنهادی، مستندات ذیل جهت ارزیابی تا تاریخ تعیین شده به سازمان ارائه نمایند.

۱) اطلاعات حقوقی شرکت
۲) مشخصات هیئت مدیره شرکت و سهامداران
۳) اساسنامه، آگهی تاسیس و آخرین اگهی تغییرات
۴) اظهار نامه مالیاتی ۲ سال گذشته
۵) لیست بیمه سه ماه گذشته
۶) گواهینامه‌ها و مجوزهای اخذ شده

پیوست (الف) – فرم پیشنهاد قیمت مناقصه

بدین وسیله شرکت ..... به شماره ثبت ..... با شناسایه ملی ..... و کد اقتصادی ..... اعلام می‌دارد با مطالعه اسناد و مدارک و شرایط مناقصه، از موضوع مورد مناقصه و حدود کار

و نوع فعالیت، آگاهی از مدت اجرای کار، میزان کسورات قانونی، جمع قیمت پیشنهادی بدون احتساب مالیات بر ارزش افزوده به مبلغ ..... (به عدد) و ..... (به حروف) برای **پروژه استقرار سامانه ، .....**، با شرایط مندرج در اسناد و به شرح جدول قیمت ذیل اعلام می‌دارد.

ردیف	شرح	مقدار/واحد	فی	قیمت کل
۱	لایسنس به میزان ۵۰۰ گیگابایت رویداد بر روز به همراه APP ES	۱ نسخه		
۲	هزینه نصب و راه اندازی سامانه نرم افزاری، برای ۲ شبکه	۲ سری		
۳	آموزش	۶۰ ساعت		
جمع کل (بدون مالیات بر ارزش افزوده):				

شرکت:

امضاء صاحبان امضای مجاز شرکت:

مهر شرکت:

تاریخ: