شرکت پالایش گاز فجر جم

استعلام بهای داخلی	شماره تقاضا : 0500016
تلفن: 07731682976 – 09173049908	مامور خرید : بهرامی

آدرس: استان بوشهر - شهرستان جم - شرکت پالایش گاز فجر جم - صندوق پستی ۷۵۵۹۱۴۷۱۲۷

نام و نشانی فروشنده :	شماره تماس :

ردیف	شرح کالا	تعداد	واحد
1	لایسنس به میزان ۵۰۰ گیگابایت رویداد بر روز به همراه APP ES ارائه آموزش SOC Level 1 -ساعت ۳۰ برای ۵ نفر-تخصصی	1	NO
2	نصب و پیاده سازی لایسنس به همراه APP ES برای هر دو شبکه اینترنت و اینترانت. ارائه آموزش SOC Level 2 -ساعت ۳۰ برای ۵ نفر - تخصصی	2	NO

توضیح :

شرح کالاهای ثبت شده در سامانه فرضی میباشد فروشنده میبایست پیشنهادات فنی و مالی خود را بر اساس استعلام بهای پیوست (اطلاعات فنی) بارگذاری نماید . به شرکت هایی که پیشنهاد فنی پیوست ندارند به هیچ وجه ترتیب اثر داده نخواهد شد . پیشنهادات فنی و مالی به صورت تفکیک بارگذاری شود .

ذکر شماره تماس در متن پیشنهادات فنی و مالی الزامی میباشد . اعتبار قیمت حداقل باید یکماه باشد .

محل تحویل کالا انبار شرکت پالایش گاز فجر جم آدرس : استان بوشهر - شهرستان جم - شرکت پالایش گاز فجر جم - امور کالا- خریدهای داخلی - کد پستی ۷۵۵۹۱۴۷۱۲۷ ارسال نمائید.

شرکت های دانش بنیان و تولید کننده داخلی و دارای ایران کد در اولویت میباشند . (اولویت با خرید کالای ساخت ایران)

تولید کنندگان و شرکتهای دانش بنیان مدارک و مستندات الطاق نمایند.

پرداخت وجه کالا ۴۰ روز کاری پس از دریافت و تائید نهایی کالا توسط واحد متقاضی صورت می گیرد . و پرداخت نهایی منوط به ثبت فاکتور در سامانه مودیان و ارائه کد منحصر به فرد مالیاتی می باشد

پاسخ استعلام می بایست یکماه اعتبار داشته باشد . در صورت برنده شدن و ابلاغ سفارش پرداخت وجه پس از دریافت کالا ، تائید فنی و فیزیکی توسط دستگاه مجری انجام خواهد شد

امضا کننده کلیه شرایط فوق را قبول نموده و اجرا می نماید	محل امضاء و مهر فروشنده

توضیحات کلی :

با توجه به رشد تهدیدات سایبری، افزایش وابستگی سازمان به زیرساخت‌های فناوری اطلاعات، توسعه سرویس‌های تحت شبکه و نیاز به پایش متمرکز رخدادهای امنیتی، پیاده‌سازی سامانه مدیریت رویداد و اطلاعات امنیتی (SIEM) به‌عنوان یکی از الزامات راهبردی امنیت اطلاعات سازمان مطرح می‌باشد.

در همین راستا، پیشنهاد تهیه و پیاده‌سازی یک راهکار(Enterprise-Level) در حوزه (SIEM) با قابلیت پردازش حجم بالای لاگ، تحلیل رخدادهای امنیتی و پشتیبانی از توسعه(SOC) سازمانی ارائه گردیده است.

اهداف اجرای پروژه

- ایجاد زیرساخت متمرکز جمع‌آوری و تحلیل لاگ‌ها
- یکپارچه‌سازی رخدادهای امنیتی شبکه داخلی و اینترنت سازمان
- فراهم‌سازی بستر توسعه SOC در سال‌های آتی
- ایجاد قابلیت جستجو، نگهداری و تحلیل رخدادها
- افزایش Visibility بر تجهیزات و سرویس‌های حیاتی
- آماده‌سازی زیرساخت جهت توسعه MSSP/SOC در فازهای بعدی
- ایجاد بستر استاندارد برای مانیتورینگ و تحلیل امنیتی

شرح اقلام پیش‌بینی‌شده در این فاز

1- تهیه لایسنس سامانه SIEM با قابلیت دریافت و پردازش روزانه ۵۰۰ گیگابایت لاگ و پشتیبانی از ماژول امنیتی تحلیل رخدادها.

2- نصب و پیاده‌سازی اولیه سامانه شامل راه‌اندازی هسته SIEM ، اتصال اولیه دو شبکه سازمان (شبکه داخلی و اینترنت)، فعال‌سازی لایسنس و راه‌اندازی اولیه داشبوردهای امنیتی.

رویکرد اجرایی پروژه

با توجه به محدودیت بودجه سنواتی سازمان، اجرای پروژه به‌صورت مرحله‌ای و تدریجی در نظر گرفته شده است تا ضمن کنترل هزینه‌ها، امکان توسعه بلوغ امنیتی سازمان در فازهای آتی فراهم گردد.

در این فاز تمرکز اصلی بر ایجاد زیرساخت SIEM ، متمرکزسازی لاگ‌ها، آماده‌سازی بستر مانیتورینگ و آموزش اولیه تیم داخلی خواهد بود.

موارد انجام‌شونده در این فاز

ردیف	شرح خدمات	وضعیت
1	تهیه لایسنس سامانه SIEM Enterprise	☑
2	نصب و راه‌اندازی اولیه سامانه	☑

3	اتصال دو شبکه سازمان	☑
4	جمع‌آوری متمرکز لاگ‌ها	☑
5	راه‌اندازی داشبوردهای پیش‌فرض امنیتی	☑
6	آموزش اولیه راهبری سامانه	☑
7	آماده‌سازی زیرساخت توسعهSOC	☑

وضعیت آموزش‌ها

ردیف	عنوان آموزش	نوع	وضعیت
1	آموزش راهبری اولیه سامانه	پایه / رایگان	☑
2	آموزش کاربری داشبوردها	پایه / رایگان	☑
3	آموزش جستجو و بررسی رخدادها	پایه / رایگان	☑