معیارهای ارزیابی شرکت متقاضی دریافت پروانه خدمت «**پیاده‌سازی مرکز عملیات امنیت**»

جدول (۱). معیارهای ارزیابی

| معیار | ریزمعیار | توضیحات |
|---|---|---|
| **فنی** | صحت، دقت و کیفیت گزارش انجام پروژه | بررسی گزارش فنی پروژه انجام شده براساس موارد ذیل:<br>• طراحی یک مرکز عملیات امنیت براساس سه مولفه ابزار، روال‌ها ونیروی انسانی شرح داده شده باشد.<br>• معماری سامانه SIEM شرح داده شده باشد. |
| | توانایی فنی کارشناسان | • مصاحبه فنی<br>• بررسی سابقه کاری<br>• بررسی مدرک تحصیلی |
| | محصول (سخت‌افزار، نرم‌افزار) و ابزارهای تولیدی در حوزه خدمت مربوطه | تولید سامانه/ابزار در حوزه SOC مد نظر است. برای مثال شرکتی که یک SIEM بومی تولید کرده است، حداکثر امتیاز را کسب خواهد کرد. (به شرط آنکه تمامی ماژول‌ها را خود شرکت تولید کرده باشد) |
| | تدوین مستندات فنی در رابطه با چگونگی انجام پروژه/ ثبت تجربه‌های مفید در رابطه با حل چالش‌ها/تدوین مستندات آموزشی برای کارشناسان | این مورد فعلا بررسی نمی‌شود |
| **امنیتی** | مدیریت اسناد | بررسی طبقه‌بندی اسناد، نحوه ذخیره مستندات محرمانه، مدیریت نسخ و ... |
| | ساختار شبکه شرکت | بررسی شبکه از لحاظ موارد ذیل:<br>• Vlan بندی<br>• تعریف Zone های مناسب<br>• سیستم‌های امنیتی تعبیه شده (فایروال، آنتی ویروس و ...)<br>• ثبت رخدادهای ممیزی (لاگ) برای شبکه و نگهداری متمرکز آن |
| | امنیت فیزیکی | بررسی موارد ذیل:<br>• نحوه کنترل ورود و خروج<br>• دوربین مدار بسته<br>• سیستم اعلام و اطفاء حریق<br>• محافظت از دیتاسنتر (نصب دوربین، تهویه و سیستم‌های سرمایشی، نحوه دسترسی و ...) |
| **کیفی** | محیط فیزیکی شرکت | بررسی محیط شرکت براساس موارد ذیل:<br>• مناسب بودن فضای کاری<br>• جدا بودن بخش امنیت از سایر بخش‌ها<br>• جداسازی گروه‌های کاری (براساس اتاق یا فضای پارتیشن‌بندی شده) |
| | سابقه انجام پروژه | بررسی موارد ذیل:<br>• انجام پروژه در حوزه‌ای که درخواست گواهی داشته است.<br>• انجام پروژه در حوزه‌های مرتبط با گواهی درخواست شده. |
| | توانایی حفظ نیرو انسانی | بررسی موارد ذیل:<br>• شرکت به چه میزان در حفظ نیروهای فنی خود موفق عمل کرده است؟ |

| | | |
|---|---|---|
| | • جدایی نیروهای فنی به چه علت‌هایی بوده است؟ | |
| | مدیریت ارتباط با مشتری | حداکثر امتیاز به موردی اعطا می‌شود که سامانه‌ای برای ارتباط با مشتری مهیا شده باشد و درخواست مشتری به طور سیستماتیک به کارشناس مربوطه ارجاع شود. همچنین امکان گزارش‌گیری کامل از سامانه وجود داشته باشد. |
| | نظامنامه کیفی | بررسی نظام‌نامه کیفی، آیین نامه‌ها و دستورالعمل‌های داخلی، ضوابط استخدام و خاتمه همکاری، ضوابط کاری از قبیل مرخصی، ماموریت، ... |
| | سابقه دریافت گواهی در حوزه خدمت مذکور | بررسی دفعات تمدید گواهی (صرفا برای خدمتی که درخواست داده است) |

جدول (۲). معیارهای سنجش توانایی فنی کارشناسان برای خدمت «**پیاده‌سازی مرکز عملیات امنیت**»

| معیار | تخصص‌های مورد نیاز | منابع |
|---|---|---|
| **دانش پایه** | ✓ احراز هویت<br>✓ کنترل دسترسی<br>✓ رمزنگاری<br>✓ آسیب‌پذیری<br>✓ کدهای مخرب<br>✓ توپولوژی‌های امنیتی و امنیت زیرساخت | ➢ SANS SEC401 |
| **دانش مدیریت رخداد و حوادث** | ✓ معماری امنیت شبکه<br>✓ مانیتورینگ امنیت شبکه<br>✓ مفاهیم پایه SOC | ➢ SANS SEC511<br>➢ SANS SEC530 |
| **دانش تحلیل لاگ و ابزارهای مدیریت رخدادهای امنیتی** | ✓ مانیتورینگ لاگ<br>✓ معماری SIEM<br>✓ آنالیز نقاط پایانی<br>✓ آنالیز هشدارهای SIEM و قواعد همبسته‌سنجی<br>✓ جمع‌آوری شواهد شبکه<br>✓ جمع‌آوری و آنالیز لاگ<br>✓ آنالیز Netflow | ➢ SANS SEC555 |
| **دانش پیاده‌سازی و راه‌اندازی** | ✓ شناخت SIEMهای متن باز<br>✓ شناخت روشهای نرمال‌سازی لاگ<br>✓ قواعد تعریف امضاء و سناریو برای تشخیص حملات<br>✓ شناخت IDS/IPS و چگونگی نوشتن امضاء برای آنها<br>✓ شناخت UTMها و NGFW | - |

**نکات مهم:**

- رزومه فنی نیروها و رزومه شرکت، بروزرسانی گردد.
- در صورت وجود هرگونه ابهام، با شماره تلفن‌های مرکز افتای استان گیلان (**۳۳۲۳٤۷۲۰** و **۳۳۲۳٤۷۳۰**) تماس گرفته شود.