فاز ۱ – شناخت و ارزیابی وضعیت موجود (۱۵٪ – حدود ۱۴۰ نفرساعت)

هدف فاز

کسب شناخت جامع از وضعیت موجود زیرساخت فناوری اطلاعات، دارایی‌های نرم‌افزاری و سخت‌افزاری، وضعیت امنیتی و فرآیندهای مدیریتی سازمان؛ به‌منظور پایه‌گذاری صحیح برای فازهای بعدی (طراحی، نظارت و بهبود امنیتی).
در این فاز، مشاور به‌عنوان بازوی فنی و ناظر مستقل کارفرما عمل می‌کند و موظف است کلیه ارزیابی‌ها را بر اساس چک‌لیست‌های مرکز مدیریت راهبردی افتا، الزامات پدافند غیرعامل و استاندارد ISMS انجام دهد.

دامنه خدمات و فعالیت‌ها

۱. ارزیابی جامع امنیت سایبری سازمان

- بررسی ساختار امنیتی فعلی شرکت، شامل نحوه سازماندهی امنیت، ترکیب کارگروه‌ها و سطح تفویض اختیار در حوزه فاوا.
- تحلیل سیاست‌ها و کنترل‌های امنیتی در تمامی سطوح فناوری اطلاعات.
- شناسایی نقاط ضعف و کاستی‌های سیاستی، ساختاری و عملیاتی موجود.
- بررسی نقش‌ها، شرح وظایف و مسئولیت‌های تعریف‌شده برای واحدهای امنیت زیرساخت و امنیت برنامه‌های کاربردی.
- بررسی وضعیت موجود دفاع در عمق (Defense in Depth) و تطبیق آن با نیازهای سازمان.

۲. بررسی دارایی‌ها و زیرساخت‌های فنی

- دارایی‌های اتاق سرور: شامل سرورها، ذخیره‌سازها (SAN، TAPE، NAS و...)، تجهیزات شبکه و تجهیزات پشتیبان.
- دارایی‌های زیرساخت شبکه: اکتیو و پسیو (سوئیچ‌ها، روترها، فایروال‌ها، UPS، رک‌ها، کابل‌کشی و...)
- دارایی‌های شبکه امن: شامل تجهیزات فایروال، UTM، VPN، و تجهیزات تفکیک شبکه.
- دارایی‌های پشتیبانی و نگهداری: بررسی تجهیزات مانیتورینگ، پشتیبان‌گیری و Backup Recovery.
- دارایی‌های نرم‌افزاری و سامانه‌های حیاتی: سیستم‌عامل‌ها، سرویس‌های زیرساختی (DNS، AD، DHCP و...) و برنامه‌های کاربردی کلیدی.
- بررسی دارایی‌های ذخیره‌سازی و پشتیبان‌گیری: تحلیل وضعیت موجود Tape، SAN، NAS و ساختار Disaster Recovery فعلی.

۳. تحلیل فرآیندها و رویه‌های فناوری اطلاعات

- بررسی فرآیندهای مستند و جاری در حوزه IT شامل نگهداری، پشتیبانی، مدیریت تغییر، امنیت شبکه و مدیریت کاربران.
- ارزیابی نحوه تدوین و اجرای رویه‌ها، دستورالعمل‌ها و فرآیندهای عملیاتی امنیت اطلاعات.(SOPs)
- ارزیابی میزان هم‌پوشانی یا تضاد بین رویه‌های فعلی با استانداردهای افتا و.ISMS
- بررسی سطح آگاهی و فرهنگ امنیتی در میان کارشناسان فناوری اطلاعات.

۴. ارزیابی خدمات، پروژه‌ها و قراردادهای جاری

- بررسی پروژه‌های جاری مرتبط با حوزه فناوری اطلاعات و امنیت سایبری.
- ارزیابی قراردادهای برون‌سپاری فعلی از منظر امنیتی، SLAها و الزامات کنترلی.
- تحلیل میزان هم‌راستایی پیمانکاران فعلی با الزامات امنیتی سازمان.
- ارائه گزارش وضعیت موجود قراردادها با تمرکز بر شاخص‌های عملکرد، ریسک و کنترل امنیتی.
- پیشنهاد بهبود یا بازنگری در قراردادهای فاوا جهت کاهش نقاط آسیب‌پذیری.

۵. بررسی وضعیت فیزیکی زیرساخت

- شناسایی نقاط آسیب‌پذیر فیزیکی (رک‌ها، اتاق سرور، کنترل دسترسی فیزیکی، تهویه، آتش‌سوزی و...)
- تحلیل وضعیت تجهیزات پسیو از نظر انطباق با الزامات پدافند غیرعامل.
- ارزیابی شرایط امنیتی محیط‌های حیاتی (مانند مراکز داده و اتاق کنترل شبکه).

۶. بررسی شبکه از دیدگاه امنیتی

- شناخت جامع از کلیه اجزای لایه‌های شبکه، تجهیزات، نرم‌افزارها و پروتکل‌های ارتباطی.
- بررسی معماری منطقی و فیزیکی شبکه، مسیرهای تبادل داده، و نحوه تفکیک شبکه‌های داخلی و خارجی.
- بررسی سطح امنیت تجهیزات مرزی، فایروال‌ها و تجهیزات امنیتی موجود.
- تحلیل ترافیک، روش‌های کنترل دسترسی، و نحوه نظارت بر فعالیت‌های کاربران.

۷. بررسی وضعیت پشتیبان‌گیری و بازیابی

- ارزیابی فرآیندهای Backup وRestore ، زمان‌بندی، و سیاست‌های نگهداری نسخه‌های پشتیبان.
- ارزیابی نقاط شکست در فرآیند Disaster Recovery و ارائه پیشنهاد برای افزایش قابلیت اطمینان.

۸. تحلیل سازمانی و نقش تیم فناوری اطلاعات

- بررسی وظایف فعلی تیم IT و میزان هم‌پوشانی با وظایف امنیتی.
- تحلیل ساختار گزارش‌دهی، ارتباط بین واحدها و کارگروه‌های امنیتی.
- پیشنهاد ساختار بهینه برای تفکیک وظایف امنیت، شبکه، و پشتیبانی.

۹. مشاوره در تحلیل شکاف (Gap Analysis)

- مقایسه وضعیت فعلی سازمان با وضعیت مطلوب براساس استانداردهای امنیتی ملی و بین‌المللی.
- شناسایی نقاط ضعف در کنترل‌ها، رویه‌ها و معماری شبکه.
- اولویت‌بندی شکاف‌ها براساس سطح ریسک، اهمیت دارایی‌ها و قابلیت اصلاح.

۱۰. تدوین گزارش نهایی فاز شناخت

در پایان فاز ۱، مشاور موظف است گزارش رسمی شامل موارد زیر را ارائه دهد:

1. گزارش کامل شناخت وضعیت موجود(As-Is Report)
2. نقشه جامع دارایی‌ها(Asset Inventory Map)
3. چک‌لیست ارزیابی بلوغ امنیتی سازمان
4. تحلیل ریسک دارایی‌های حیاتی
5. پیشنهاد نقشه راه ارتقاء امنیتی اولیه

شاخص‌های کلیدی عملکرد(KPI)

شاخص	هدف	حد انتظار
درصد پوشش دارایی‌های شناسایی‌شده	تکمیل جامع نقشه دارایی‌ها	≥۹۵٪
زمان تحویل گزارش شناخت	حداکثر مدت برای فاز ۱	≤۳۰ روز
دقت داده‌های جمع‌آوری‌شده	صحت اطلاعات در مستندات	≥۹۰٪
انطباق با استانداردهای افتا وISMS	بررسی و مستندسازی کامل	۱۰۰٪

خروجی‌های قابل تحویل(Deliverables)

1. **گزارش شناخت وضعیت موجود(As-Is Report)**
2. **نقشه دارایی‌ها و زیرساخت‌ها(Network & Asset Map)**
3. **گزارش بلوغ امنیتی و ریسک‌ها(Maturity & Risk Assessment)**
4. **پیشنهاد بهبود اولیه و نقشه راه امنیتی(Initial Security Roadmap)**

فاز ۲ – طراحی چارچوب نظارت و سیاست‌های امنیتی (۲۰٪ – حدود ۱۹۰ نفرساعت)

هدف فاز

هدف این فاز، تدوین چارچوب نظارت امنیتی، بازطراحی سیاست‌ها و فرآیندهای کنترل امنیتی سازمان است تا مبنای فنی و مدیریتی لازم برای نظارت و پایش مرکز عملیات امنیت (SOC) فراهم گردد.
در این فاز، مشاور موظف است کلیه طرح‌ها و فرآیندهای نظارتی را با استانداردهای افتا، ISMSو پدافند غیرعامل منطبق ساخته و در کنار کارفرما، چارچوب اجرایی نظارت و سیاست‌گذاری را ایجاد نماید.

دامنه خدمات و فعالیت‌ها

۱. طراحی ساختار امنیت و نقش‌ها

- تحلیل ساختار فعلی امنیت در سازمان و بازتعریف گروه‌ها و کارگروه‌های امنیتی.
- طراحی و مستندسازی ساختار بهینه امنیت سازمان بر اساس الگوی دفاع در عمق.(Defense in Depth)
- تعریف نقش‌ها و مسئولیت‌ها برای تیم‌های امنیت زیرساخت، امنیت برنامه‌های کاربردی، و امنیت اطلاعات.
- تعیین شرح وظایف دقیق برای هر گروه امنیتی (نظارت، تحلیل، واکنش، سیاست‌گذاری).
- ایجاد ساختار سلسله‌مراتبی گزارش‌دهی برای اطمینان از هماهنگی میان تیم‌های IT و امنیت.

۲. بازطراحی سیاست‌ها، کنترل‌ها و فرآیندهای امنیتی

- مرور و بازبینی کلیه سیاست‌ها و دستورالعمل‌های امنیتی موجود در سازمان.
- تدوین سیاست‌های امنیت اطلاعات جدید در تمامی سطوح فناوری اطلاعات، از جمله:
  - مدیریت دسترسی کاربران و احراز هویت چندمرحله‌ای.(MFA)
  - مدیریت پچ‌ها، وصله‌های امنیتی و کنترل تغییرات.(Change Management)
  - سیاست‌های پشتیبان‌گیری، بازیابی، و حفظ محرمانگی داده‌ها.
  - سیاست‌های کنترل دسترسی فیزیکی و منطقی.
  - سیاست‌های مربوط به شبکه‌های امن، اینترنت، اینترانت و.Cloud Access
- انطباق سیاست‌های جدید با الزامات مرکز افتا و استاندارد.ISO/IEC 27001
- تدوین روش اجرایی امنیتی برای بخش‌های حیاتی شبکه(Firewall) ، SIEM، Endpoint Securityو(...

۳. طراحی فرآیندهای مدیریتی امنیت اطلاعات (ISMS)

- طراحی ساختار ISMS و معرفی نقش‌ها و مسئولیت‌ها برای پیاده‌سازی آن.

- تعریف فرآیندهای مدیریت ریسک، ارزیابی تهدید، و پاسخ به رخداد.(Incident Management)
- تدوین طرح مدیریت تداوم کسب‌وکار (BCP) و بازیابی از بحران.(DRP)
- تدوین چک‌لیست‌های ارزیابی امنیتی (Security Checklists) برای دارایی‌های حیاتی.
- طراحی الگوی گزارش‌دهی امنیتی و مستندسازی فرآیندهای امنیت اطلاعات.(SOPs)
- تطبیق ISMS با فعالیت‌های SOC به‌منظور هم‌راستایی راهبری امنیت اطلاعات و عملیات امنیتی.

۴. تدوین و استانداردسازی مستندات برون‌سپاری

- بررسی قراردادهای جاری در حوزه امنیت و فناوری اطلاعات.
- تدوین اسناد یکپارچه برون‌سپاری برای پروژه‌های امنیتی آتی.
- تهیه **شرح خدمات (SOW)** برای پیمانکاران اجرایی پروژه SOC و سایر پروژه‌های امنیتی.
- تنظیم چارچوب **درخواست پیشنهاد (RFP)** برای انتخاب مجریان پروژه‌های امنیتی آینده.
- تعیین معیارهای فنی و کیفی ارزیابی پیشنهادهای پیمانکاران.
- تدوین فرآیند ارزیابی فنی و مالی پیشنهادها با همکاری کمیته امنیت و فاوا.
- مستندسازی شاخص‌های کلیدی برای برون‌سپاری ایمن و شفاف (امنیت، SLA، KPI، محرمانگی).

۵. مشاوره در فرآیندهای حقوقی و قراردادی امنیت سایبری

- ارائه مشاوره حقوقی در خصوص الزامات امنیتی قراردادهای فاوا.
- پیشنهاد بندهای امنیتی و محرمانگی برای الحاق به قراردادهای جدید.
- بررسی انطباق پیمانکاران با بندهای امنیتی در قراردادهای جاری.
- مشاوره در تدوین ضوابط حقوقی برای حفاظت از داده‌های سازمانی و اسرار تجاری.

۶. طراحی چارچوب نظارت و کنترل امنیتی

- تدوین **Security Oversight Framework**شامل ساختار گزارش‌دهی، پایش و بازخورد.
- طراحی فرآیندهای ارزیابی عملکرد پیمانکاران اجرایی.SOC
- تعیین شاخص‌های کلیدی نظارت(KPI) ها (برای هر حوزه امنیتی.
- طراحی قالب گزارش‌های ماهانه و دوره‌ای برای کارفرما.
- تدوین مکانیزم رسمی "Change Request" برای مدیریت تغییرات در پروژه‌ها.

۷. مشاوره در انطباق با استانداردها و نهادهای بالادستی

- مشاوره جهت اجرای الزامات مرکز افتا در حوزه ISMS و.SOC
- همکاری در جلسات و کمیته‌های امنیتی سازمان.
- پاسخ‌گویی کارشناسی به مکاتبات رسمی سازمان‌های بالادستی مانند مرکز افتا یا پدافند غیرعامل.
- ارائه راهکار برای رفع مغایرت‌ها و پاسخ به گزارش‌های ممیزی امنیتی.

۸. تدوین طرح بهبود امنیت زیرساخت‌ها

- بررسی نتایج فاز شناخت و استخراج فهرست شکاف‌ها.(Gap List)
- تدوین طرح جامع بهبود امنیت زیرساخت.(Network Improvement Plan)
- طراحی سناریوهای ارتقاء امنیتی برای شبکه، سرویس‌ها و فرآیندهای پشتیبان.
- مشاوره برای انتخاب راهکارهای نرم‌افزاری و سخت‌افزاری بهینه جهت تقویت امنیت.
- اولویت‌بندی پروژه‌های اصلاحی براساس ریسک و اهمیت سرویس.

شاخص‌های کلیدی عملکرد(KPI)

شاخص	هدف	حد انتظار
تدوین کامل چارچوب نظارت	طراحی Oversight Framework تأییدشده	۱۰۰٪
میزان انطباق سیاست‌های جدید با الزامات افتا	انطباق کامل	۱۰۰٪
زمان تحویل طرح سیاست‌های امنیتی	تکمیل در زمان مقرر	≤۶۰ روز
رضایت کارفرما از طرح ISMS و مستندات برون‌سپاری	تأیید کتبی	≥۹۰٪

خروجی‌های قابل تحویل(Deliverables)

1. **سند چارچوب نظارت امنیتی(Security Oversight Framework Document)**
2. **سیاست‌ها و دستورالعمل‌های بازنگری‌شده امنیت اطلاعات(Security Policies & Procedures)**
3. **طرح جامع ISMS و فرآیندهای امنیتی(ISMS Process Design)**
4. **اسناد برون‌سپاری وRFP های امنیتی(Security RFP Package)**
5. **چک‌لیست‌های نظارتی و ارزیابی پیمانکاران(Vendor Assessment Checklists)**
6. **طرح بهبود امنیت زیرساخت‌ها(Network Security Improvement Plan)**

فاز ۳ – نظارت و پایش اجرای مرکز عملیات امنیت(SOC)

(۵۰٪ – حدود ۴۷۵ نفرساعت)

هدف فاز

در این فاز، مشاور به‌عنوان بازوی نظارتی فنی کارفرما از ابتدای اجرای پروژه SOC تا زمان تحویل نهایی در کنار تیم کارفرما و پیمانکار اجرایی حضور دارد.

هدف، اطمینان از اجرای صحیح، منطبق با استانداردها و مستندات مصوب فازهای پیشین، و همچنین ارزیابی اثربخشی عملکرد مرکز عملیات امنیت است.

مشاور در این مرحله به هیچ عنوان وارد اجرای مستقیم (Configuration یا Deployment) نمی‌شود و صرفاً در نقش ناظر ارشد، تحلیل‌گر و کنترل‌گر کیفیت فعالیت می‌کند.

دامنه خدمات و فعالیت‌ها

۱ .نظارت بر اجرای پروژه SOC توسط پیمانکار اجرایی

- بررسی برنامه زمان‌بندی و طرح اجرایی پیمانکار براساس ساختار شکست کار.(WBS)
- کنترل انطباق فعالیت‌های اجرایی با الزامات امنیتی، طرح مصوب و استانداردهای افتا.
- حضور در جلسات فنی، کمیته‌های راهبری و ارزیابی پیشرفت پروژه.
- پایش مستمر خروجی‌ها و مستندات پیمانکار و تطبیق آن‌ها با شرح خدمات و برنامه زمان‌بندی مصوب.
- شناسایی انحرافات احتمالی و ارائه گزارش رسمی به کارفرما همراه با پیشنهاد اصلاحی.
- بررسی و تأیید صورت‌وضعیت‌های پیمانکار از منظر پیشرفت فنی و تحققMilestone ها.

۲ .مشاوره در طراحی و پیاده‌سازی سامانهSIEM

- بررسی طرح معماری پیشنهادی SIEM و ارزیابی ساختار جمع‌آوری و همبستگی رخدادها.
- نظارت بر طراحی جریان داده‌ها، منابع لاگ(Log Sources) ، و سیاست‌های تجمیع و فیلترینگ.
- ارزیابی تطابق معماری SIEM با نیازمندی‌های امنیتی سازمان و مدل داده‌های افتا.
- نظارت بر فرآیند پیکربندی (Tuning) ابزارهای SIEM جهت بهبود دقت و کارایی در تشخیص حملات.
- ارزیابی عملکرد SIEM از منظر سرعت جستجو، دقت هشدارها و نرخ.False Positive
- بررسی و تحلیل گزارش‌های عملکردی و داشبوردهای مدیریتی.SOC

۳ .نظارت بر سیاست‌های امنیتی و تشخیص تهدیدات

- ارزیابی سیاست‌های امنیتی تعریف‌شده درSIEM ، IDS/IPSو سایر ابزارهای امنیتی.
- بررسی تطابقSignature ها وRule های امنیتی با تهدیدات روز و الزامات افتا.
- تحلیل نحوه شناسایی حملات در لایه‌های مختلف شبکه و سرویس‌ها.
- پایش مداوم میزان اثربخشی سامانه‌ها در تشخیص و پاسخ به رخدادها.(Detection Efficiency)
- ارائه پیشنهاد برای بهبود قوانین، تنظیمات و پارامترهای امنیتی جهت کاهش نرخ هشدار کاذب.

۴ .نظارت بر تیم واکنش به رخدادهای امنیتی(CERT / CSIRT)

- بررسی فرآیند پاسخ‌گویی به رخدادهای امنیتی.(Incident Response Workflow)
- نظارت بر تشکیل و عملکرد تیم‌هایTier 1 ، Tier 2وTier 3 در.SOC
- بررسی نحوه ثبت، طبقه‌بندی و رسیدگی به رخدادهای امنیتی.
- ارزیابی کیفیت تحلیل فنی و ریشه‌ای (Root Cause Analysis) در رخدادها.
- ارائه پیشنهاد برای بهبود مستندسازی و فرآیند Escalation میان تیم‌های پاسخ‌گو.
- نظارت بر اقدامات اصلاحی پس از هر رخداد امنیتی.(Post-Incident Review)

۵ .مشاوره و نظارت بر قابلیت‌هایThreat Hunting

- طراحی سناریوهای جستجوی تهدید (Threat Hunting Scenarios) با تمرکز بر تهدیدات پیشرفته.
- ارزیابی توانایی تیم SOC در شناسایی رفتارهای مشکوک.(Anomaly Detection)
- نظارت بر اجرای فعالیت‌های Threat Intelligence و استفاده از منابع IOC وTTP های شناخته‌شده.
- ارائه راهکار برای خودکارسازی فرآیندهای جستجو (Automation) و بهبود بهره‌وری تیم.SOC
- گزارش‌گیری دوره‌ای از نتایج Threat Hunting و میزان موفقیت آن در کشف تهدیدات پنهان.

۶ .تحلیل رویدادها و مدیریت لاگ‌ها

- پایش جمع‌آوری متمرکز لاگ‌ها از تمامی دارایی‌های فناوری اطلاعات.
- نظارت بر پالایش (Normalization) و ذخیره‌سازی بلندمدت لاگ‌های حیاتی.(Retention Management)
- ارزیابی امنیت، ظرفیت و کارایی سیستم.Log Management
- بررسی صحت داده‌ها، میزان از دست رفتن رخدادها و نحوه دسترسی کنترل‌شده به لاگ‌ها.
- پیشنهاد راهکارهای افزایش قابلیت اطمینان و مقیاس‌پذیری سیستم جمع‌آوری لاگ.

۷ .بررسی و ارزیابی اثربخشی کلیSOC

- ارزیابی میزان دستیابی به اهداف عملکردی SOC شامل:
  - **MTTD (Mean Time to Detect)**
  - **MTTR (Mean Time to Respond)**
  - **Incident Containment Rate**
  - **False Positive Ratio**
- ارزیابی سطح بلوغ عملیاتی.(SOC (Operational Maturity Assessment
- بررسی انطباق عملکرد SOC با استانداردهایNIST CSF ، ISO 27035و الزامات افتا.
- تحلیل شکاف‌های عملیاتی و پیشنهاد بهبود مستمر.(Continuous Improvement)

۸ .مشاوره در ابزارها و فناوری‌های امنیتی مکمل

- ارزیابی و نظارت بر کارایی ابزارهای زیر در فرآیندهای:SOC
  - **Identity Engine ،HSM ،PAM ،DLP ،EDR ،Firewall ،UTM**
- بررسی نحوه یکپارچگی داده‌ها میان این ابزارها و.SIEM
- پایش صحت تنظیمات امنیتی (Policy Tuning) و بررسی وصله‌های امنیتی مرتبط.(Patch Management)
- پیشنهاد اصلاحات و راهکارهای فنی جهت بهبود هم‌افزایی ابزارهای امنیتی.

۹ .گزارش‌دهی، ممیزی و ارزیابی عملکرد پیمانکار

- تهیه گزارش‌های نظارتی ماهانه شامل وضعیت پیشرفت، مشکلات، مغایرت‌ها و پیشنهادات اصلاحی.
- بررسی کیفیت مستندات و محصولات فنی ارائه‌شده توسط پیمانکار اجرایی.
- ارزیابی میزان انطباق خروجی‌های پیمانکار با الزامات شرح خدمات و طرح مصوب.
- ارائه گزارش رسمی به کارفرما در مورد نقاط قوت و ضعف عملکرد پیمانکار.
- طراحی و اجرای چک‌لیست ارزیابی عملکرد پیمانکار در حوزه امنیت سایبری و.SOC
- پیشنهاد اقدامات اصلاحی و زمان‌بندی اجرای آن‌ها.

۱۰ .تحلیل امنیت سرویس‌ها و سامانه‌ها

- بررسی امنیت سرویس‌های حیاتی سازمان از منظر دسترسی، پیکربندی و حفاظت داده‌ها.
- ارزیابی لایه‌های امنیتی سرویس‌های کاربردی حیاتی.
- مشاوره در بهینه‌سازی تنظیمات امنیتی، Hardeningسیستم‌ها و بهبود مدیریت وصله‌ها.

شاخص‌های کلیدی عملکرد(KPI)

شاخص	هدف	حد انتظار
میزان پایش مستمر دارایی‌ها	نظارت دائمی بر کلیه دارایی‌های حیاتی	۱۰۰٪
اثربخشی تشخیص و پاسخSOC	کاهش MTTD و MTTR نسبت به ماه اول	≥۳۰٪ بهبود
دقت در هشدارهای امنیتی	کاهش False Positive نسبت به خط پایه	≥۴۰٪
انطباق عملکرد با الزامات افتا	هم‌خوانی کامل گزارش‌ها با استاندارد ملی	۱۰۰٪

خروجی‌های قابل تحویل(Deliverables)

1. **گزارش‌های ماهانه نظارت بر اجرای(SOC (Monthly Oversight Reports**
2. **گزارش ارزیابی عملکرد SIEM و ابزارهای امنیتی(Performance Evaluation Report)**
3. **چک‌لیست ارزیابی عملکرد پیمانکار و مغایرت‌ها(Audit Checklist & Deviation Report)**
4. **گزارش تحلیلی Threat Hunting و(Incident Handling (Analytical Report**
5. **گزارش بلوغ عملیاتی(SOC (SOC Maturity Assessment Report**
6. **پیشنهادات اصلاحی و طرح بهبود مستمر امنیت(Continuous Improvement Plan)**

فاز ۴ – تحلیل نهایی، آموزش و بهبود مستمر

(۱۵٪ – حدود ۱۴۵ نفرساعت)

هدف فاز

هدف از این فاز، ارزیابی نهایی سطح بلوغ امنیت سایبری سازمان پس از اجرای پروژهSOC ، انتقال کامل دانش به تیم داخلی کارفرما، و تدوین برنامه بهبود مستمر برای حفظ و ارتقای امنیت زیرساخت‌ها در آینده است.
مشاور موظف است ضمن ارائه گزارش نهایی شامل نتایج تحلیلی، شاخص‌ها، انحرافات و اقدامات اصلاحی، کارگاه‌های آموزشی تخصصی برای تیم‌های فنی و مدیریتی برگزار نماید تا دانش ایجادشده در پروژه به‌طور مؤثر منتقل شود.

دامنه خدمات و فعالیت‌ها

۱ .تحلیل نهایی عملکردSOC

- بررسی جامع عملکرد مرکز عملیات امنیت در دوره ۱۸ ماهه اجرای پروژه.
- تحلیل میزان تحقق اهداف عملکردی SOC در مقایسه با شاخص‌های طراحی‌شده KPI) و.(SLA
- ارزیابی اثربخشی فرآیندهای پایش، پاسخ به رخداد، و مدیریت تهدیدات.
- بررسی موانع، نقاط ضعف و دستاوردهای پروژه از منظر فنی، سازمانی و مدیریتی.
- تحلیل علل انحراف از اهداف مصوب و مستندسازی Lessons Learned برای استفاده در پروژه‌های آینده.
- مستندسازی تجارب و دانش فنی به‌دست‌آمده از پیمانکار اجرایی و تیم.SOC

۲ .ارزیابی سطح بلوغ امنیت سایبری

- انجام ممیزی نهایی امنیتی (Final Security Audit) با محوریت شاخص‌های بلوغ امنیتی.(Maturity Level)
- اندازه‌گیری بلوغ در ابعاد زیر:
  - **فرآیندها و سیاست‌ها(Governance & Process Maturity)**
  - **فناوری و ابزارها(Technology Maturity)**
  - **پاسخ‌گویی به رخدادها(Incident Response Maturity)**
  - **آگاهی و فرهنگ امنیتی(Awareness & Training)**
- مقایسه وضعیت فعلی (Post-Implementation) با وضعیت اولیه (As-Is) برای سنجش بهبود کمی و کیفی.
- محاسبه شاخص‌های پیشرفت امنیتی و ترسیم نمودار روند رشد بلوغ امنیتی سازمان.

۳ .تدوین برنامه بهبود مستمر امنیت(Continuous Improvement Plan)

- تحلیل شکاف‌های باقیمانده در ساختار امنیتی و تعیین اقدامات اصلاحی.
- تدوین طرح بهبود امنیتی بلندمدت با رویکرد .**PDCA (Plan–Do–Check–Act)**
- ارائه پیشنهادات مرحله‌ای برای ارتقاء فناوری‌های امنیتی، فرآیندهای مدیریتی و ساختارهای کنترلی.
- طراحی نقشه راه امنیت سایبری سه‌ساله با اولویت‌بندی اقدامات کوتاه‌مدت، میان‌مدت و بلندمدت.
- تعریف شاخص‌های نظارت دوره‌ای (Continuous Security KPIs) جهت حفظ سطح امنیت پس از پایان قرارداد.

۴ .آموزش و انتقال دانش

- برگزاری کارگاه‌های تخصصی برای کارشناسانSOC ، تیم امنیت اطلاعات و مدیران.IT
- طراحی سرفصل‌های آموزشی شامل موضوعات زیر:
  - اصول مدیریت امنیت و الزامات افتا و.ISMS
  - تحلیل رخدادها، واکنش سریع و گزارش‌دهی امنیتی.
  - آشنایی باSIEM ، Threat Huntingو مدیریت هشدارها.
  - روش‌های بهبود مستمر و پایش شاخص‌های امنیتی.
- تهیه بسته آموزشی شامل اسلایدها، سناریوها و دستورالعمل‌های فنی.
- انتقال دانش پروژه به تیم داخلی کارفرما از طریق جلسات حضوری و مستندسازی.
- ارزیابی میزان یادگیری و توانمندسازی تیم داخلی پس از پایان آموزش.

۵ .مستندسازی و تحویل نهایی

- تهیه و تحویل کلیه مستندات پروژه شامل:
  - گزارش‌های فازهای ۱ تا ۴ (با پیوست‌ها و تحلیل‌ها).
  - مستند نهایی ارزیابی امنیتی.(Final Assessment Report)
  - گزارش بلوغ امنیتی و نمودارهای تحلیلی.
  - برنامه بهبود مستمر.(CIP)
  - خروجی‌های آموزشی، دستورالعمل‌ها و فایل‌های پشتیبان.
- ارائه جلسه نهایی به مدیریت ارشد سازمان جهت جمع‌بندی نتایج و پیشنهادات راهبردی.
- تحویل نهایی و رسمی پروژه پس از تأیید کارفرما و بستن پرونده فنی.

شاخص‌های کلیدی عملکرد(KPI)

شاخص	هدف	حد انتظار
میزان برگزاری کارگاه‌های آموزشی	انتقال مؤثر دانش پروژه	حداقل ۲ کارگاه تأییدشده
تحویل گزارش نهایی و برنامهCIP	تکمیل مستندات پایانی	≤۴۵ روز از پایان فاز ۳
سطح بلوغ امنیتی پس از پروژه	افزایش نسبت به وضعیت اولیه	≥۲ سطح ارتقاء
میزان انطباق با الزامات افتا وISMS	تحقق الزامات فنی و مدیریتی	۱۰۰٪

خروجی‌های قابل تحویل(Deliverables)

1. **گزارش نهایی ارزیابی امنیت سایبری(Final Security Assessment Report)**
2. **برنامه بهبود مستمر امنیت سایبری(Continuous Improvement Plan – CIP)**
3. **گزارش بلوغ امنیتی نهایی(Security Maturity Analysis)**
4. **پکیج آموزشی تخصصی(Training Package)**
5. **مستندات کامل پروژه و خروجی‌های فازهای قبلی(Final Documentation Set)**
6. **گزارش رسمی جمع‌بندی پروژه برای مدیریت ارشد(Executive Summary Report)**

پیوست – A شرح خدمات فنی(Technical Scope of Work)

هدف

ارائه جزئیات فنی و خدمات قابل‌انتظار از مشاور در تمامی فازهای پروژهSOC ، با تمرکز بر ارزیابی امنیتی، تحلیل زیرساخت، و نظارت تخصصی بر عملیات امنیت اطلاعات.

---

۱ .خدمات مشاوره امنیت سایبری

- تحلیل معماری امنیتی سازمان شامل ساختار شبکه، سرویس‌ها، سامانه‌های حیاتی و دارایی‌های بحرانی.
- شناسایی تهدیدات بالقوه در حوزه‌های شبکه، سرور، پایگاه داده و کاربران.
- پیشنهاد طرح دفاع چندلایه (Defense-in-Depth) بر اساس ریسک‌های شناسایی‌شده.
- تحلیل و ارزیابی تطبیق با الزامات ملی افتا، پدافند غیرعامل و.ISO/IEC 27001
- مشاوره برای افزایش کارایی، امنیت و در دسترس‌پذیری خدمات IT.

۲ .خدمات مشاوره زیرساخت و فناوری

- بررسی کامل زیرساخت‌های شبکه.(LAN, WAN, VLAN, VPN)
- تحلیل ساختار ارتباطی بین سایت‌ها، مراکز داده و سرویس‌های حیاتی.
- ارزیابی طراحی منطقی شبکه از نظر تفکیک نواحی امنیتی.(Security Zones)
- بررسی عملکرد فایروال‌ها، UTM، IDS/IPS، Load Balancerو تجهیزات مانیتورینگ.
- تحلیل وضعیت مجازی‌سازی (VMware, Hyper-V) و پلتفرم‌های ابری در صورت وجود.
- ارزیابی سیستم‌های ذخیره‌سازی (SAN, NAS, Tape) و پشتیبان‌گیری.(Backup/DR)

۳ .خدمات نظارت بر SOC وSIEM

- نظارت تخصصی بر طراحی و پیاده‌سازی SOC توسط پیمانکار اجرایی.
- تحلیل معماری SIEM از منظر جمع‌آوری، پردازش و همبستگی رخدادها.
- بررسی عملکرد سیستم در پردازش لاگ‌ها، هشدارها و ترافیک شبکه.
- تحلیل و تنظیم قوانین شناسایی (Detection Rules) و سطح حساسیت هشدارها.
- ارزیابی صحت و کارایی فرآیندهای Tuning در.SIEM
- طراحی شاخص‌های عملکرد برای SOC و گزارش‌گیری مدیریتی.

۴ .خدمات تحلیل امنیتی و تست نفوذ

- مشاوره در انجام تست نفوذ (Penetration Test) بر روی سامانه‌های حیاتی.
- بررسی نتایج آزمون‌ها و ارائه تحلیل فنی از نقاط آسیب‌پذیر.
- پیشنهاد اقدامات اصلاحی برای برطرف‌سازی ضعف‌ها.
- بررسی دوره‌ای آسیب‌پذیری‌ها و ریسک‌های امنیتی.(Vulnerability Assessment)

۵ .خدمات Threat Hunting وIncident Response

- طراحی فرآیند جستجوی تهدید (Threat Hunting) براساس IOC و رفتارهای مشکوک.
- تحلیل تهدیدات پیشرفته و کشف حملات در مراحل اولیه.
- مشاوره در تحلیل رخدادها و پاسخ سریع به تهدیدات.
- ارزیابی عملکرد تیم‌های1 Tier ، 2 Tierو 3 Tier در واکنش به رخداد.
- تدوین فرآیند Incident Lifecycle و مستندسازی رویدادها.

۶ .خدمات امنیت کاربران وEndpoint ها

- ارزیابی سیاست‌های امنیتی ایستگاه‌های کاری و کاربران.(Endpoint Security)
- بررسی وضعیت آنتی‌ویروس، EDR، فایروال شخصی و کنترل دسترسی‌ها.
- تحلیل روند وصله‌گذاری (Patch Management) و کنترل به‌روزرسانی‌ها.
- پیشنهاد اقدامات بهبود امنیت کاربران داخلی و خارجی.

۷ .مشاوره در طراحی فرآیندهای امنیت اطلاعات(ISMS)

- طراحی، بازبینی و پیاده‌سازی فرآیندهای.ISMS
- تدوین دستورالعمل‌ها، چک‌لیست‌ها و سیاست‌های امنیتی سازمان.
- ارزیابی انطباق فرآیندها با الزامات ISO 27001 و ضوابط افتا.
- طراحی الگوی کنترل مستندات و ممیزی امنیتی دوره‌ای.

۸ .مدیریت تغییرات و پیکربندی(Change & Configuration Management)

- ارزیابی فرآیند مدیریت تغییر در حوزه امنیت.
- تدوین دستورالعمل کنترل تغییرات و پیگیری آن در پروژه‌های.IT
- پایش صحت اجرای کنترل تغییرات امنیتی در تجهیزات و سیستم‌ها.

۹ .پایش و گزارش‌دهی امنیتی

- طراحی قالب‌های گزارش امنیتی شامل شاخص‌ها، روندها و هشدارهای بحرانی.
- تدوین سیستم گزارش‌گیری برای سطوح مدیریتی و عملیاتی.
- گزارش‌گیری ماهانه از وضعیت امنیتی، پیشرفت پروژه و ریسک‌های شناسایی‌شده.

پیوست – B الزامات احراز صلاحیت پیمانکار

هدف

تضمین انتخاب پیمانکار دارای صلاحیت فنی، سوابق معتبر و گواهی‌های لازم برای ارائه خدمات مشاوره و نظارت امنیت سایبری.

۱ .الزامات عمومی

- ثبت رسمی شرکت و دارا بودن سابقه فعالیت در حوزه امنیت سایبری حداقل ۵ سال.
- ارائه مستندات مالی، اساسنامه و مجوزهای معتبر مرتبط با خدمات فناوری اطلاعات.
- برخورداری از نیروی انسانی متخصص با سوابق اجرایی مشابه.

۲ .الزامات فنی و گواهی‌ها

- رتبه ۱ شورای عالی انفورماتیک در حوزه امنیت فضای تبادل اطلاعات.
- دارا بودن گواهی افتا در حداقل یکی از زمینه‌های زیر:
  - خدمات مدیریتی امنیت اطلاعات
  - خدمات مشاوره و نظارت امنیتی
  - خدمات آزمون و ارزیابی امنیتی
- دارا بودن حداقل یکی از گواهی‌های بین‌المللی زیر برای اعضای تیم کلیدی:
  - **SANS ،CCNP Security ،LPIC2 ،NSE2 ،OSCP ،CEH ،ISO 27001 LA ،CISM ،CISSP**
- سابقه انجام حداقل ۱۰ پروژه موفق در حوزهSOC ، ISMSیا امنیت شبکه.
- ارائه گواهی حسن انجام کار از حداقل ۳ کارفرمای معتبر.

۳ .الزامات تیم مشاوره

نقش	حداقل صلاحیت	شرح وظیفه
مشاور ارشد امنیت(Lead Consultant)	CISSP / ISO 27001 LA	هدایت فنی پروژه و تأیید خروجی‌ها
تحلیلگر SOC وSIEM	NSE2 / SIEM Specialist	ارزیابی عملکرد SOC و تحلیل داده‌ها
کارشناس ارزیابی ریسک	CEH / ISO 27005	تحلیل ریسک و آسیب‌پذیری‌ها
کارشناسISMS	ISO 27001 Implementer	تدوین فرآیندها و سیاست‌های امنیتی
مستندساز فنی	ISO 27001 Internal Auditor	تهیه گزارش‌ها و مستندات رسمی

پیوست – C چک‌لیست ارزیابی و کنترل پیشرفت

هدف:ایجاد ساختار نظام‌مند برای ارزیابی مستمر عملکرد پیمانکار و سنجش پیشرفت پروژه در تمامی فازها.

۱ .چک‌لیست ارزیابی فنی

حوزه ارزیابی	شاخص	وضعیت	توضیحات
انطباق با الزامات افتا	رعایت کامل ضوابط ملی	☐بلی / ☐ خیر	
کیفیت مستندات	دقت و پوشش محتوایی	☐عالی / ☐ متوسط / ☐ ضعیف	
عملکرد تیم مشاور	تخصص، همکاری، پاسخ‌گویی	☐عالی / ☐ متوسط / ☐ ضعیف	
گزارش‌دهی دوره‌ای	تطابق با قالب و زمان‌بندی	☐بلی / ☐ خیر	
مدیریت تغییرات	ثبت، تحلیل و پیگیری تغییرات	☐بلی / ☐ خیر	

۲ .شاخص‌های کلیدی ارزیابی عملکرد(KPI Matrix)

شاخص	نوع	هدف	حد انتظار
پیشرفت فعالیت‌های نظارتی	کمی	میزان تحقق برنامه فازها	≥۹۵٪
انطباق مستندات فنی	کیفی	دقت و شفافیت مستندات	≥۹۰٪
رضایت کارفرما	کیفی	سطح تعامل و کیفیت خروجی	≥۹۰٪
انحراف زمانی پروژه	کمی	تأخیر نسبت به برنامه	≤۵٪

۳ .الگوی گزارش ماهانه

- گزارش ماهانه باید شامل بخش‌های زیر باشد:

1. خلاصه مدیریتی(Executive Summary)
2. فعالیت‌های انجام‌شده در ماه جاری
3. فعالیت‌های برنامه‌ریزی‌شده برای ماه بعد
4. انحراف‌ها و مشکلات مشاهده‌شده
5. پیشنهادات اصلاحی
6. شاخص‌های عملکرد ماهانه(KPI Dashboard)

۴ .گزارش نهایی و ارزیابی پایانی

در انتهای پروژه، چک‌لیست ارزیابی نهایی براساس معیارهای زیر تکمیل می‌شود:

- دستیابی به اهداف تعریف‌شده درRFP
- میزان انطباق خروجی‌ها با الزامات استانداردها
- رضایت فنی و مدیریتی کارفرما
- تکمیل فرآیند انتقال دانش و آموزش

خروجی‌های نهایی پیوستC

1. **چک‌لیست رسمی ارزیابی پیشرفت پروژه**
2. **الگوی گزارش ماهانه رسمی(Monthly Progress Template)**
3. **فرم ارزیابی نهایی پروژه(Final Evaluation Form)**