رزومه عمومی نگاره پرداز امن گستر ایرانیان

مستند V1

شرکت نگاره پرداز امن گستر ایرانیان

تاریخ مستند: ۱۴۰۲/۰۸/۰۱

تولید و توسعه سامانه‌های امنیتی

شرکت نگاره پرداز امن گستر ایرانیان

رزومه و شرح خدمات شرکت	
درخواست کننده :	شرکت نگاره پرداز امن گستر ایرانیان
موضوع سند	پروپوزال
تاریخ تهیه	۱۴۰۲/۰۸/۰۱
نام دپارتمان	
تایید کننده	
برنامه نویس سامانه	
تهیه کننده سند	

شناسه شرکت تهیه کننده

شماره ثبتی	۶۰۸۷۸۵
مدیر عامل	سید محمد مشفقی زاده
تلفن تماس	
شماره فاکس	
آدرس	استان تهران، شهرستان تهران، بخش مرکزی، شهر تهران، پاسداران (تهرانسر مرکزی)، کوچه سی و یکم، خیابان شهیدسعیدطالبی، پلاک ۱۶، طبقه ۱
پست الکترونیک	info@ iraniansec.ir

فهرست مطالب

۱- درباره ی ما

شرکت نگاره پرداز امن گستر ایرانیان یک شرکت پیشرو در حوزه امنیت سایبری در کشور ایران است. با سال ها تجربه در این صنعت، ما بهترین خدمات امنیتی را برای مشتریانمان ارائه می دهیم.

تیم ما متشکل از متخصصان برجسته و کارآزموده در زمینه های مختلف امنیت سایبری از جمله تست نفوذ، مدیریت ریسک، حفاظت از شبکه و دستگاه ها، حفاظت از اطلاعات حساس و ممنوعه و رمزنگاری. متخصصان ما با استفاده از آخرین تکنولوژی ها و روش های نوین، با ایجاد اطمینان حداکثری از امنیت دیجیتال مشتریانمان میکوشند.

ما به شرکت ها و سازمان های مختلف در تمام حوزه های صنعتی خدمات ارائه می دهیم. از شرکت های کوچک تا بزرگ، ما میتوانیم به شما کمک کنیم تا داده ها، سیستم ها و شبکه های خود را در برابر تهدیدات سایبری محافظت کنید. با توجه به مشاوره های ما، سازمان شما میتواند از آسیب های امنیتی جلوگیری کند و در صورت لزوم، به سرعت واکنش مناسب را نشان دهد.

ما به افتخار می پذیریم که با بهره گیری از روش های مجازی سازی و الگوریتم های پیشرفته، به حفاظت از داده ها و اطلاعات حیاتی سازمان ها کمک کنیم. فرایند های امنیتی ما به محض ایجاد تهدیدات و نفوذها پاسخ می دهند و در مقابل عملیات نفوذ،رمزنگاری و رمزگشایی لازم انجام می دهند.

با تکیه بر تجربه، تخصص و تکنولوژی پیشرفته، شرکت نگاره پرداز امن گستر ایرانیان به شما اعتماد بخشی در امنیت سایبری خود خواهد داد.

۲- دوره های آموزشی

ما در آموزشگاه امنیت، به عنوان یک مجموعه آموزشی حرفه‌ای در حوزه امنیت فعالیت می کنیم. هدف ما ارائه آموزش‌های کامل و عملی در زمینه امنیت سایبری است تیم ما از اساتید و متخصصان حرفه‌ای تشکیل شده است که تجربه و دانش خود را در اختیار دانشجویان قرار می‌دهند آموزشگاه ما بر اساس روش‌های مدرن و به‌روز، به دانشجویان کمک می کند تا مهارت‌های لازم برای تامین امنیت سایبری و فیزیکی را کسب کنند ما به دانشجویان فرصت می‌دهیم تا با استفاده از تجربه عملی و پروژه‌های تیمی، مهارت های خود را تقویت کنند و در صنعت امنیت تأثیرگذار باشند آموزشگاه ما از تجهیزات و فضای آموزشی مناسب برخوردار است تا به دانشجویان امکان آموزش عملی و شبیه‌سازی سناریوهای واقعی را بدهد با انتخاب آموزشگاه ما، شما در محیطی حمایت‌کننده و دوستانه قرار می گیرید که به شما کمک می کند در مسیر حرفه‌ای خود پیشرفت کنید ما همچنین ارائه مشاوره و راهنمایی در زمینه شغلی و مسیر حرفه‌ای دانشجویان خود را برعهده داریم.

۲-۱ وبینارهای امنیت (آگاهی رسانی امنیت)

در سال های اخیر و با گذر زمان، حملات سایبری بسیار پیشرفته‌تر از گذشته شده‌اند و با توجه به آمارهای ارایه‌شده از سوی شرکت‌های امنیتی مختلف، در اغلب حملات سایبری سراسر دنیا، نفوذ اولیه به سازمان‌ها با هدف قرار دادن کارکنان آن‌ها صورت گرفته است. بنابراین اگر کارکنان سازمان شما از آگاهی و آمادگی لازم برای مقابله با تهدیدات سایبری‌ای که در کمین آن‌هاست برخوردار نباشند، مهم‌ترین نقطه‌ی ضعف امنیت سازمان شما به حساب خواهند آمد. به این ترتیب یک اشتباه ساده از سوی یک کارشناس ناآگاه می‌تواند تمام فرایندها و معماری پیچیده‌ی امنیت سایبری سازمان شما را کم‌اثر یا بی‌اثر کند. تیم امنیت ما به صورت دوره ای وبینارهای رایگان جهت آگاهی رسانی از حملات سایبری برگزار می نماید جهت اطلاع از زمان و نحوه برگزاری به وبسایت ما(**Iraniansec.com**) مراجعه نمایید

۲-۲ آموزش سازمانی

یکی از بزرگ‌ترین چالش‌های پیش روی سازمان‌ها در امن‌سازی زیرساخت‌های فناوری اطلاعات خود و محافظت از آن‌ها در برابر مهاجمین، کمبود نیروی متخصص امنیت سایبری در سطح دنیا است. یکی از راهکارهای مورد استفاده‌ی این سازمان‌ها برای کم‌رنگ‌تر کردن این مساله، تامین بخشی از متخصصین امنیت مورد نیاز خود با استفاده از آموزش پرسنل مستعد و علاقه‌مند به امنیت سایبری در داخل سازمان است. این چالش در ایران نیز وجود دارد و حتی در بسیاری موارد، بیش از کشورهای توسعه یافته یا در حال توسعه احساس می‌شود .علاوه بر موارد ذکر شده، بسیاری از سازمان‌ها و شرکت‌ها دارای تیم امنیت سایبری متخصص هستند اما نیاز دارند تا دانش تیم امنیت سایبری خود را تقویت یا به‌روزرسانی کنند. در همین راستا «آکادمی امنیت ایرانیان» آمادگی دارد تا در راستای برگزاری دوره‌های تخصصی امنیت سایبری با سازمان‌ها و شرکت‌ها همکاری نماید. دوره‌های آموزشی بنابر نوع درخواست سازمان‌ها می‌تواند در محل آموزشگاه، در محل سازمان و یا به صورت آنلاین برگزار شود. همچنین سازمان‌ها می‌توانند با عقد قرارداد میان‌مدت، یک یا چند مسیر آموزشی را برای پرسنل خود خریداری نمایند. به عنوان مثال، یک سازمان با انتخاب مسیر «متخصص پاسخ به تهدیدات سایبری»، می‌تواند

تا آموزش افراد مورد نظر خود را از سطح پایه‌ی فناوری اطلاعات تا سطح خبره‌ی پاسخ به رخدادها، به «آکادمی امنیت ایرانیان» برون‌سپاری کند. مسیرهای آموزشی به‌گونه‌ای طراحی شده‌اند تا پاسخ‌گوی نیاز منابع انسانی سازمان‌ها در انواع تخصص‌های امنیت سایبری شامل ارزیابی امنیتی، امن‌سازی و دفاع، پاسخ به تهدیدات، کارشناس لایه‌های مختلف مرکز SOCو غیره باشد.

۳-۲ درباره اساتید

اساتید ما جزو اساتید با سابقه و حرفه‌ای در حوزه آموزش امنیت سایبری هستند و تمامی مجوزهای لازم اعم از مجوز افتا، فنی حرفه ای و... برای تدریس دوره‌های سایبری را دارا می باشند هدف ما ارائه آموزش‌های کاربردی و عملی در زمینه امنیت سایبری به دانشجویان و علاقه‌مندان است تجربه‌ی طولانی‌مدت ما در این حوزه، به ما کمک نموده تا روش‌های به‌روز و کارآمد را در آموزش امنیت سایبری به‌کار ببریم.ما با استفاده از روش‌های تدریس تعاملی و مطالعات موردی، به دانشجویان خود کمک خواهیم نمود تا مفاهیم پایه و پیچیده امنیت سایبری را درک کنند با تجربه و دانش فنی اساتید ما، به دانشجویان ابزارها و تکنیک‌های لازم برای محافظت از داده‌ها و سیستم‌های خود را آموزش می‌دهیم با استفاده از مثال‌های عملی و تمرینات تجربی، ما به دانشجویان خود کمک می‌کنیم تا در مواجهه با تهدیدات سایبری به صورت خودکار و هوشمندانه عمل کنند.

۳ – مشاوره امنیت سایبری

مشاوره امنیت شبکه یک سرویس حرفه ای بوده که به سازمان ها کمک می کند از امنیت شبکه های کامپیوتری خود اطمینان حاصل کنند. یک مشاور امنیت شبکه با مشاوره به سازمان ها برای شناسایی آسیب‌پذیری‌های بالقوه ای که در داده ها و اطلاعات دیجیتال آن‌ها وجود دارد کمک کرده و سپس استراتژی‌هایی را برای کاهش این خطرات اتخاذ و به سازمان اعلام می کند.

تقاضا برای خدمات مشاوره امنیت شبکه در سال های اخیر به سرعت رشد نموده، زیرا کسب و کارها به طور فزاینده ای برای انجام عملیات خود به فناوری های دیجیتال متکی می باشند. با افزایش حملات سایبری، سازمان ها نیاز به سرمایه گذاری در اقدامات امنیتی سایبری قوی برای محافظت از اطلاعات حساس خود را تشخیص می دهند. شرکت‌های مشاوره امنیت شبکه با ارائه تخصص مورد نیاز برای محافظت از شبکه‌های خود در برابر تهدیدات سایبری در حال تکامل، به سازمان ها کمک می کنند تا از این منحنی جلوتر بمانند.

۳-۱ مشاور امنیت شبکه چه می کند؟

مشاور امنیت شبکه معمولاً با انجام یک ارزیابی جامع از زیرساخت فناوری اطلاعات یک سازمان شروع می شود. این شامل تجزیه و تحلیل اجزای سخت افزاری و نرم افزاری شبکه، ارزیابی سیاست ها و رویه های امنیتی سازمان و شناسایی آسیب پذیری های امنیتی بالقوه می باشد. بر اساس این ارزیابی، مشاور یک طرح امنیتی سفارشی برای سازمان مورد نظر با توجه به نیازها و خطرات خاص سازمان می پردازد.

۳-۲ انتخاب شرکت مشاور امنیت شبکه واجد شرایط

هنگام انتخاب یک مشاور امنیت شبکه، مهم است که ارائه دهنده ای را انتخاب کنید که سابقه موفقیت آمیز داشته باشد. سازمان ها باید به دنبال شرکت مشاوره ای باشند که تجربه کار با سازمان های مشابه شما را داشته و بتواند با استفاده از نیروهای متخصص با تجربه تمامی چالش های امنیتی سازمان خود را پاسخ دهند.

علاوه بر این، انتخاب مشاوری که در مورد آخرین تهدیدات و روندهای امنیت سایبری به روز باشد، مهم می باشد. این امر مستلزم آموزش و آموزش مداوم است تا اطمینان حاصل شود که مشاور به دانش و تخصص لازم برای محافظت از سازمان شما در برابر تهدیدات سایبری نوظهور مجهز باشد.

مشاوره امنیت شبکه یک سرویس ضروری برای سازمان هایی که می خواهند از اطلاعات، داده ها و دارایی های دیجیتال خود در برابر تهدیدات سایبری محافظت کنند میباشد. مشاور امنیت با شناسایی و کاهش خطرات امنیتی، توسعه سیاست‌های امنیتی مؤثر و اجرای اقدامات امنیتی قوی، می‌تواند به سازمان‌ها کمک کند تا از منحنی جلوتر بمانند و یک محیط فناوری اطلاعات ایمن و سازنده را حفظ نمایند.

قطعا! مشاوره امنیت شبکه یک زمینه پیچیده و چند وجهی بوده و جنبه های مختلفی وجود دارد که باید هنگام توسعه یک استراتژی امنیت شبکه مؤثر در نظر گرفت. در اینجا جزئیات بیشتری وجود دارد که ممکن است به شما در درک بهتر نقش مشاور امنیت شبکه کمک کند.

٤- خدمات تست نفوذ(وب ، شبکه ، زیرساخت)

۴-۱ تست نفوذ چیست؟

در جوامع امروزی، تلاش برای بهبود وضعیت کنونی (در هر زمان و مکان و هر موقعیتی) به یک اصل تبدیل شده است. در واقع یکی از اصول مهم در تمامی سطوح و گرایشهای کلیه استانداردها، در پیش گرفتن فرآیندهایی است که بهبود وضعیت را در پی داشته باشد. بخصوص این امر در تکنولوژی اطلاعات یکی از اصول تخطی ناپذیر و غیر قابل اجتناب است. حال اگر وارد حیطه شبکه های کامپیوتر و نیز نرم افزارهای گوناگون شویم، باید برای این فرآیند، راههای متناسب با آن را در اتخاذ کنیم. یکی از عمومی ترین و مهمترین ای راه حلها در این بخش ،استفاده از فرآیند تست نفوذ است. نفوذ کردن به شبکه های کامپیوتری و دسترسی به منابع یک شبکه، در حالت معمول، امری غیر قانونی تلقی می شود. اما یک متخصص امنیت، با بستن قراردادی با صاحبان و مدیران شبکه و یا یک نرم افزار ، علاوه بر قانونی کردن آن، نتایج آن را به نفع شما باز می گرداند. او از دید یک هکر به برنامه یا شبک شما نگریسته و تلاش می کند تا کلیه مشکلات و شکافهای امنیتی آن را شناسایی و به شما ارائه دهد. بدین وسیله، شما با رفع این معایب،علاوه بر بالابردن میزان امنیت سرویسهای خود و جلب رضایت بیشتر مشتریان، راه را بر نفوذگران مخرب سد می کنید.

شرکت نگاره پرداز امن گستر ایرانیان برای انجام تست نفوذ از استاندارد های زیر استفاده می نماید

ISO/IEC 27001

ISO/IEC 27002

OSTTMM (Open Source Security Testing Methodology Manual)

OWASP (Open Web Application Security Project) 2013

LPT (Licensed Penetration Tester methodology from EC-Council)

*** کلیه ابزارهای که در طول پروژه از آنها استفاده می شود ابزارهای استاندارد بوده و به هیچ عنوان آسیبی به سیستم ها وارد نخواهد نکرد.**

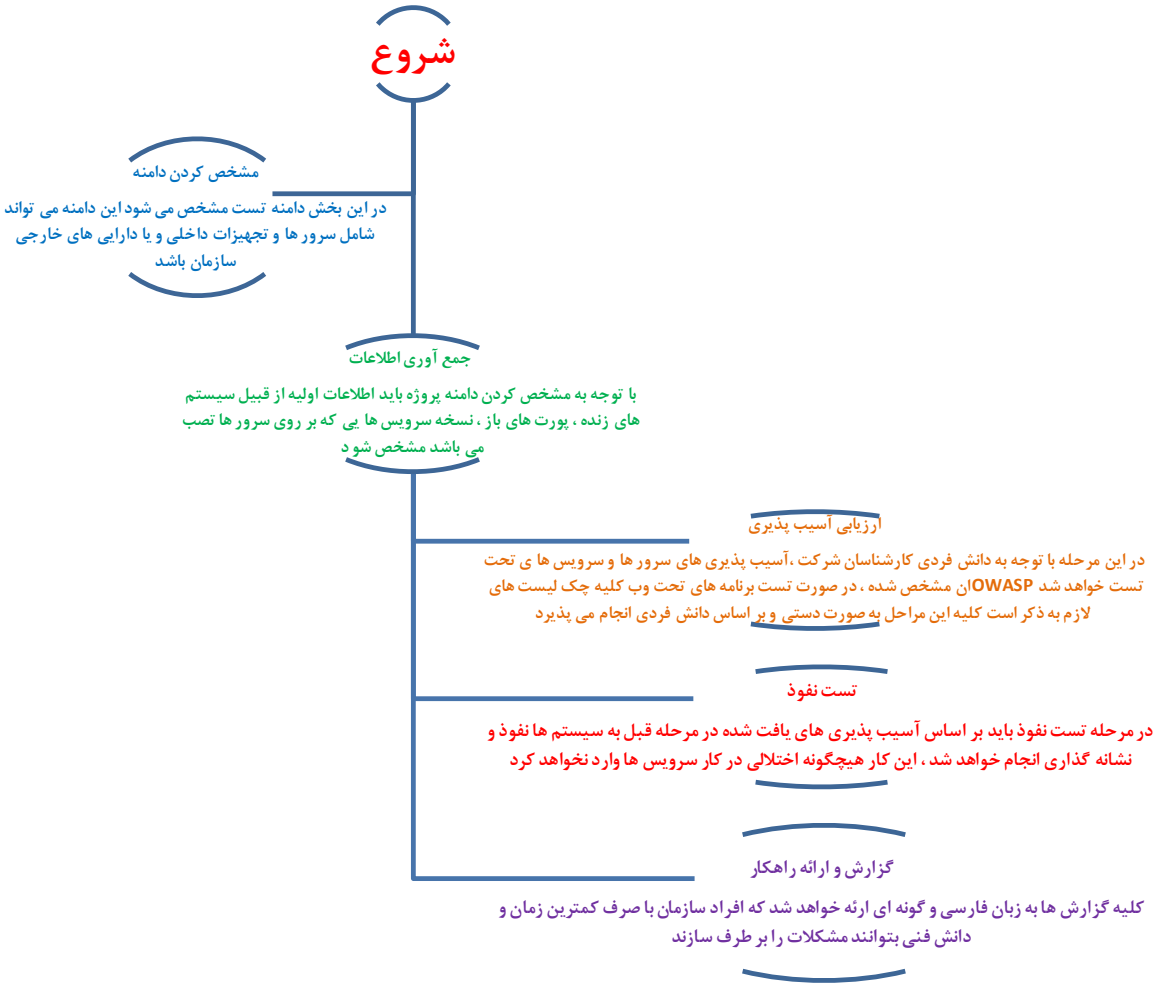
۲-۴ روش های تست نفوذ

White Box: در این حالت تیم تست نفوذ اطلاعات کامل در باره موضوع مورد تست دارد و همچنین دسترس به منابع داخلی شبکه نیز دارد. معمولا از این نوع تست برای ارزیابی آسیب پذیری های داخل شبکه استفاده می شود.

Gray Box: در این حالت دسترسی به منابع داخلی محدود می باشد و اطلاعات کاملی در اختیار تیم قرار نمی گیرد.

Black Box: در این حالت هیچ گونه دسترسی و اطلاعاتی به تیم تست نفوذ داده نمی شود .معمولا این نوع تست نفوذ برای وب سرور ها و برنامه های کاربردی تحت وب انجام می شود

۴-۳ مراحل تست نفوذ



۴-۴ در فرآیند تست نفوذ کامل موارد ذیل مورد ارزیابی قرار خواهند گرفت:

- تست نفوذ به سامانه های تحت وب و API ها بر اساس استاندارد owasp top 10
- تست نفوذ به هاست های ویندوزی و لینوکسی
- تست نفوذ به سرورها و سرویس دهنده های ویندوزی
- تست نفوذ به تجهیزات شبکه روتر و سوییچ ها
- تست نفوذ به سرورهای ایمیل و استخراج میل های سازمانی
- تست نفوذ به Active Directory
- شبیه سازی نفوذ های پیشرفته APT هاشامل تشخیص حادثه، پاسخگویی، تجزیه و تحلیل بدافزار، توانایی‌های بازرسی امنیتی و نظارت بر جعل

- به‌کارگیری مجموعه‌ای از حملات با هدف سرقت اطلاعات محرمانه کارکنان یا دستیابی فیزیکی به محل‌ها و دارایی‌های دیجیتال
- تست حملات ترکیبی (مهندسی اجتماعی و حملات APT ها)
- شبیه سازی حملات باج افزاری برای تشخیص میزان تخریب در صورت وقوع
- تست نفوذ حملات فیشینگ
- تست نفوذ حملات منع سرویس دهی (DOS ، DDOS)
- تست نفوذ حملات MITM (Man In The Middle)
- تست نفوذ ارسال فایل های آلوده از طریق ایمیل شرکت ها
- تست نفوذ به بسترهای رمزنگاری شده (SSL hijacking)
- تست نفوذ و بررسی رمزهای عبور (Brute Force، Dictionary Attack)
- تست نفوذ keylogger ها
- حملات مربوط به شبکه های وایرلس

۵- خدمات راه اندازی و نصب(SOC)

۵-۱ مشاوره و طراحی SOC

در مراکز SOC از سه ماژول عمده تشکیل شده اند:

ماژول اول شامل زیر ساخت و تجهیزات فنی است که از تولیدکنندگان پیام های مربوط به رخدادهای امنیتی، تجهییزات جمع آوری و طبقه بندی اولیه اطلاعات، پایگاه های داده نگهداری، ذخیره و بازیابی اطلاعات و ... تشکیل شده اند.

ماژول دوم، شامل فرآیندها و کارکردهای تعریف شده، دستورالعمل ها، روال ها و نحوه انجام فعالیت ها و عملیات امنیتی توسط کارشناسان راه اندازی SOC و متخصصین مرکز پیاده سازی SOC است.

ماژول سوم، شامل نیروهای انسانی مرکز SOC و ساختار سازمانی و سلسله مراتب های موجود به جهت انجام فعالیت ها و عملیات در مراکز SOC است.

۵-۲ مزایای پیاده سازی SOC

به طور کلی، پیاده سازی SOC در سازمان ها و نظام های کسب و کار، باعث افزایش عمومی و جزیی سطح آگاهی سازمان از وقایع امنیتی می‌شود که این امر دارای مزایای متعددی برای سازمان می‌باشد. از مهمترین مزایای ایجاد مراکز SOC در یک سازمان می توان به موارد زیر اشاره کرد:

جلوگیری از بروز فجایع امنیتی در سازمان ها

کاهش اختلالات سرویس های کسب و کار که به دلیل بروز رخدادهای غیر مجاز امنیتی رخ میدهند

کاهش مخاطرات و ریسک های امنیتی

جلوگیری از دست رفتن اطلاعات سازمانی و یا تغییرات فیر مجاز در اطلاعات سازمانی

افزایش چشم گیر آمادگی سازمان به جهت مقابله با مخاطرات امنیتی

افزایش آگاهی و بینش جامع سازمانی در رابطه با رخدادهای مرتبط با امنیت

رویکرد نگاره پرداز امن گستر ایرانیان در انجام پروژه های فناوری اطلاعات در تمامی حوزه های فنی، مبتنی بر ایجاد متدولوژی های یکپارچه و ماژولار است. این متدولوژی ها بر مهندسی رفتار یک سیستم جامع، در چرخه های عمر سیستم تاکیددارند.

پروژه هایی که در زمینه مراکز عملیات امنیت و پیاده سازی SOC نیز انجام می‌شوند، از این قاعده مستثنا نیستند و رویکرد کلان شرکت در رابطه با این پروژه ها به همین صورت است.

بدین ترتیب، با اتکا بر چنین رویکردی، شرکت به این توانایی دست یافته است، تا راهکارهای جامع را به طور کامل، از ابتدا تعریف نموده، آن را طراحی و پیاده سازی نماید و پس از آن به بهینه سازی و پشتیبانی راهکارها بپردازد.

همچنین، با استفاده از چنین رویکردی، شرکت به این توانایی نیز دست یافته است، تا به اقتضا بر شرایط پروژه، هر کدام از فازها و مراحل یک پروژه را به تنهایی، بدون این که در سایر فازها و مراحل درگیر باشد، با اخذ ورودی های اطلاعاتی لازم از فعالیت های انجام شده پیشین و ارائه خروجی های اطلاعاتی لازم به جهت ادامه کار توسط تیم فنی دیگر، انجام دهد.

استفاده از این چنین رویکرد مشترکی، در تناقض با نیازمندی ها و فعالیت های فنی پروژه از دیدگاه فازهای کلان نبوده و تفاوت های تکنولوژیک و فنی پروژه هایی که در این حوزه) راه اندازی (SOC انجام می پذیرند، تنها بر روی فعالیت های درون فازهای مختلف تأثیرگذار خواهند بود، نه در متدولوژی و رویکرد کلان انجام پروژه.

لیست خدمات ما در حوزه SOC به شرح ذیل می باشد جهت کسب اطلاعات بیشتر به وبسایت ما (Iraniansec.com) مراجعه نمایید.

امکان سنجی و نیازسنجی مرکز عملیات امنیت شبکه(SOC)

تحلیل و آنالیز امکان سنجی و نیازسنجی مرکز عملیات امنیت شبکه(SOC)

طراحی مرکز عملیات امنیت شبکه(SOC)

اجرا و پیاده سازی مرکز عملیات امنیت شبکه(SOC)

مهندسی مجدد و بهینه سازی مرکز عملیات امنیت شبکه(SOC)

مشاوره و نظارت مرکز عملیات امنیت شبکه(SOC)

نگهداری، پشتیبانی و راهبری مرکز عملیات امنیت شبکه(SOC)

تست عملکرد مرکز عملیات امنیت شبکه (SOC)

۶- نمایندگی رسمی آنتی ویروس

شرکت شرکت نگاره پرداز امن گستر ایرانیان نمایندگی رسمی فروش محصولات آنتی ویروس پادویش و کسپرسکی می باشد.برای کسب اطلاعات بیشتر به وبسایت ما مراجعه نمایید.

۷- خدمات امن سازی (وب ، شبکه ، زیرساخت)

- تغییرات لازم در ساختار شبکه
- ارائه راه کارهایی برای جلوگیری از حملات APT ها
- امن سازی باگ های کشف شده توسط تیم قرمز
- هاردنینگ نمودن سرور های ویندوزی
- هاردنینگ نمودن Active Direcorty
- هاردنینگ هاست
- امن سازی سرورهای وب
- امن سازی بستر VPN
- بررسی و ارایه راهکاری برای پیشرفته APT ها
- بررسی و جلوگیری از اجرای برنامه های مخرب
- کشف باج افزارها و جلوگیری ازتخریب فایل های سیستم
- ایجاد سیستم بکاپ گیری روزانه با حداکثر امنیت
- جمع اوری لاگ های مناسب برای فارنزیک احتمالی حملات
- Secure Coding برای سامانه ها و ابزارهای تحت وب
- نوشتن Rule های مناسب برای فایروال ها
- نوشتن Rule هایی برای تشخیص حملات در SIEM
- بهینه سازی عملکرد splunk
- راه اندازی تیم SOC
- تامین امنیت میل سرورها
- جلوگیری از حملات فیشینگ
- امن سازی و جلو گیری از حملات مربوط به گذرواژه ها
- تهیه چک لیستهای امن سازی تجهیزات و سامانه ها
- بررسی و پیاده سازی سیاست های امن سازی
- مشاوره در خصوص تولید امن نرم افزار های تحت وب

۸- برخی از مشتریان شرکت

شرکت پتروشیمی اروندان

شرکت ایرانیان خودرو

سازمان آب و برق خوزستان

سازمان حج و زیارت

مشاور امنیت در دیوان عدالت اداری

شبکه فناوری و نوآوری ایران

بانک آیند

قوه قضاییه

سازمان تعزیرات حکومتی

شهرداری کهریزک

صدا و سیما