ردەبندی

عادی

معرفی و رزومه شرکت

صبا سیستم صدرا

این صفحه به طور پیش فرض سفید در نظر گرفته شده است.

شناسنامه مستند

عنوان مستند	معرفی و رزومه شرکت
نسخه	۱,۳
رده‌بندی	عادی
تهیه‌کننده	واحد فروش و بازاریابی
کلمات کلیدی	معرفی شرکت، رزومه

سابقه مستند

نسخه	تهیه‌کننده	تأییدکننده	توضیحات
1.3	واحد فروش و بازاریابی	مدیریت	

چکیده

این مستن حاوی معرفی، چشم انداز، مشتریان، محصولات و خدمات شرکت صبا سیستم صدرا می‌باشد.

Saba System Sadra

فهرست مطالب

۱- معرفی شرکت

شرکت صبا سیستم صدرا از شرکت‌های دانش بنیان مورد تایید معاونت فناوری ریاست جمهوری می‌باشد. مجموعه تشکیل دهنده شرکت صبا سیستم صدرا دارای بیش از ده سال تجربه در پیاده‌سازی شبکه‌های گسترده و امن اطلاعاتی و مدیریت و نگه‌داری سیستم‌های فن‌آوری اطلاعات، در سازمان‌های مالی و بانکی کشور است. سابقه انجام پروژه های مشترک متعدد در زمینه‌های فوق باعث ایجاد هماهنگی و توان‌مندی مدیریتی و فنی بالایی در این شرکت شده است. خدمات شرکت شامل "امنیت‌اطلاعات" ، "شبکه و مرکزداده" و "مخابرات" است.

شرکت صبا سیستم صدرا آماده ارایه خدمات حرفه‌ای امنیت اطلاعات با توجه به نیاز کسب‌وکار سازمان‌ها است. این خدمات شامل خدمات مدیریتی، فنی و آموزشی در ارزیابی وضعیت امنیت اطلاعات، امن‌سازی، نظارت و ممیزی امنیت‌اطلاعات است. این خدمات با رویکرد جامع به "مدیریت مخاطرات کسب‌وکار" در "سیستم مدیریت امنیت اطلاعات" به مشتریان ارائه می گردد.

با توجه به گسترش شبکه‌های کامپیوتری و همچنین افزایش نیاز به ایجاد مراکز داده در سازمان‌ها، شرکت صبا سیستم صدرا با بهره‌گیری از نیروهای مختصص و مجرب در این زمینه، آماده ارائه خدمات زیر به سازمان‌ها و موسسات می‌باشد: مشاوره، طراحی، نصب، اجرا و نظارت بر پروژه‌های مرکز داده مشاوره، طراحی، نصب، اجرا و نظارت بر پروژه‌های شبکه و امنیت شبکه ، مشاوره، طراحی، نصب، اجرا و نظارت بر پروژهای ارائه‌دهنده سرویس‌های مبتنی بر IP

۲- ماموریت

شرکت صبا سیستم صدرا سرمایهگذاری و توسعهی کسب و کارهای متنوع و پایدار مبتنی بر فناوری اطلاعات و ارتباطات را مأموریت خود میداند.

شرکت صبا سیستم صدرا تجمیع مناسبی از شایستگیهای محوری همچون سرمایه انسانی متخصص و نوآور، اعتبار، امکان ارائه خدمات و راهکارهای جامع نرمافزاری و سختافزاری را در خود جای داده است.

۳- ارزش های بنیادی

- خلق ارزش برای تمامی ذینفعان
- ارزشمندسازی سرمایههای فکری
- پیشرو در نوآوری و خلاقیت مبتنی بر دانش و فناوری
- تشویق سرمایهگذاری جسورانه و کارآفرین

۴- مشخصات کلی شرکت

حوزه فعالیت	امنیت اطلاعات و شبکه
تاریخ تاسیس	۱۳۷۸/۰۸/۱۲
آدرس	تهران – میدان فاطمی – خیابان فاطمی – بین دائمی و شیخلر – پلاک ۱۶۰– طبقه
تلفن	۸۸۹۹۰۳۷۲و۷۵
فکس	۸۸۹۹۹۰۳۶
آدرس وب‌سایت	www.ssystems.ir

۵- مشتریان

- شرکت شبکه الکترونیکی پرداخت کارت (شاپرک)
- شرکت ملی نفت ایران
- بانک آینده
- شرکت پرداخت نوین آرین
- شرکت توسعه فناوری اطلاعات گردشگری ایران
- بانک گردشگری
- شرکت ملی حفاری ایران
- شرکت نفت و گاز پارس
- شرکت ایده‌های تجارت هوشمند سیمرغ
- شرکت مدیریت اکتشاف
- شرکت ساخت تجهیزات سپاهان
- شرکت نفت مناطق مرکزی ایران
- شرکت توسعه پتروایران
- شرکت نفت خزر
- شرکت پایانه های نفتی ایران
- پژوهشگاه صنعت نفت
- سازمان بهداشت و درمان صنعت نفت
- شرکت بیمه پارسیان
- سازمان فناوری اطلاعات ایران
  - اداره کل فناوری اطلاعات استان البرز
  - اداره کل فناوری اطلاعات استان قزوین

- اداره کل فناوری اطلاعات استان مازندران
- اداره کل فناوری اطلاعات استان خوزستان
- اداره کل فناوری اطلاعات استان سمنان
- اداره کل فناوری اطلاعات استان آذربایجان شرقی
- اداره کل فناوری اطلاعات استان فارس
- اداره کل فناوری اطلاعات استان کرمان

۶- معرفی محصولات

۱-۶- هانی پات کندو (Honeypot)

در سال‌های اخیر شاهد افزایش قابل توجهی در پیچیدگی تهدیدات امنیتی و حملات ناشناخته سایبری بوده‌ایم. با توجه به ضعف تجهیزات امنیتی فعلی برای کشف این حمله‌های ناشناخته و پیچیده، نیاز است که از راهکارهای جدیدی برای شناسایی این تهدیدات استفاده کنیم. یکی از این راهکارها، استفاده از سیستم هانی‌پات است که در سال‌های اخیر به یکی از مهمترین اجزای مراکز عملیات امنیت (SOC) و معماری امنیت شبکه سازمان‌ها تبدیل شده است. هانی‌پات یک سیستم امنیتی است که بر خلاف سیستم‌های امنیتی دیگر، ارزش آن در کشف شدن، مورد حمله قرار گرفتن و به خطر افتادن است! بسته به نیاز سازمان، می‌توان از هانی‌پات برای مقاصد مختلفی از جمله شناسایی حمله‌ها و فعالیت‌های غیرمجاز در شبکه، کشف و جمع‌آوری بدافزار، فریب دادن نفوذگر و کند کردن روند حمله استفاده کرد.

هانی‌پات کندو، سیستمی با سنسورهای توزیع شده و قابلیت مدیریت متمرکز است که در قالب تجهیز سخت‌افزاری پیاده‌سازی شده است. این سیستم هانی‌پات به صورت منفعل در شبکه قرار گرفته و سرویس‌های شبیه‌سازی شده را به منظور کشف حمله و بدافزار، در معرض تعامل با نفوذگر قرار می‌دهد. با استفاده از هانی‌پات کندو می‌توان حمله‌های جدید، فعالیت‌های غیر مجاز در شبکه و بدافزارها را در زمان مناسبی ردیابی و شناسایی کرد. سنسورهای این سیستم هانی‌پات را بسته به نیاز می‌توان در مکان‌های متفاوتی از شبکه قرار داد و حمله‌های شناسایی شده توسط آن‌ها را به صورت بلادرنگ مشاهده و تحلیل کرد.

قابلیت ها و مزایا

- امکان پیاده‌سازی به صورت مستقل و توزیع‌شده
  - نسخه مستقل کندو
  - نسخه توزیع‌شده کندو

- سرور مدیریت
- سنسورهای هانی‌پات
- سنسورهای هانی‌پات ICS / SCADA

- مدیریت و پیکربندی متمرکز سنسورهای هانی‌پات
- نمایش بلادرنگ حمله‌های شناسایی شده
- سرویس‌های شبیه‌سازی شده
  - پروتکل‌های SSH، SMB، SIP (VoIP)، MySQL، MSSQL، HTTP/HTTPS، FTP و TFTP
  - امکان شبیه‌سازی سرویس‌های جدید مورد نیاز مشتریان
- سنسور هانی‌پات مخصوص سیستم‌های کنترل صنعتی
- شناسایی و گزارش تمام ارتباطات ورودی به هانی‌پات
- شبیه‌سازی فایل سیستم و دستورات لینوکس
- بازپخش نشست‌های SSH
- تشخیص کدهای مخرب
- جمع‌آوری و ذخیره بدافزار
- پویش بدافزارهای جمع‌آوری شده
- ارسال بدافزار به سیستم‌های تحلیل بدافزار
- رابط کاربری گرافیکی (مبتنی بر وب و SSH)
- گزارش‌گیری و مصورسازی پیشرفته
  - رسم گراف حملات
- شناسایی کشور و سیستم‌عامل نفوذگر
- اطلاع‌رسانی رخدادها از طریق ایمیل و SMS
- ارسال رخدادها به سیستم‌های جمع‌آوری و تحلیل لاگ (SIEM)

ذخیره رخدادها در قالب PDF و IDMEF

۲-۶- ماورا (SIEM)

به منظور غلبه بر حملات و تهدیدات مختلف امنیتی، سازمان‌ها از ابزارها و تکنولوژی‌های امنیتی متعددی مانند آنتی‌ویروس‌ها، فایروال‌ها و سیستم‌های تشخیص نفوذ استفاده می‌کنند. استفاده از تکنولوژی‌های مختلف و متعلق به تولیدکننده‌های متفاوت، منجر به تولید حجم بسیار بالای رویدادهای ثبت شده با فرمت‌های متنوع شده است. این امر پیچیدگی زیادی در شبکه سازمان از نظر بررسی وقایع و رفتارهای امنیتی شبکه ایجاد می‌کند. از این رو نیاز به روش متمرکزی وجود دارد تا بتوان رویدادها و داده‌های گزارش شده را مانیتور کرده و ارتباط بین آن‌ها را کشف کرد و از این طریق تهدیدها و حملات را شناسایی نمود.برای رسیدن به این هدف یکی از روش‌های اصلی که سازمان‌های متعددی در سراسر دنیا از آن استفاده می‌کنند، سیستم‌های مدیریت اطلاعات و رویدادهای امنیتی (SIEM) است.

ماورا یک محصول SIEM است که اطلاعات مربوط به رویدادهای امنیتی تجهیزات و برنامه‌های کاربردی موجود در شبکه را جمع‌آوری کرده و با استفاده از تکنولوژی‌های هوشمند به بررسی و شناسایی ریسک‌هایی که حملات متعدد و پیچیده به همراه دارند، می‌پردازد. همچنین این محصول محتوای هر تهدید و اهمیت دارایی‌هایی که مورد هجوم قرار می‌دهد را در نظر می‌گیرد، ریسک‌ها را ارزیابی می‌کند، تجهیزات و دارایی‌هایی که در شبکه وجود دارد را شناسایی کرده و تهدیدات واقعی که متوجه هر یک از آن‌هاست را کشف می‌کند.

ویژگی‌ها و مزایا

- پشتیبانی از انواع حسگرها به منظور جمع آوری لاگ‌های تولید شده
- قابلیت یکپارچه شدن با انواع تکنولوژی‌ها و تجهیزات شبکه و امنیتی
- مانیتورینگ بلادرنگ و امکان مشاهده‌ی لحظه‌ای رویدادها
- قابلیت جستجو بر اساس پارامترهای مختلف در رویدادها

- نرمال‌سازی انواع مختلف داده‌ها و لاگ‌ها
- توانایی نمایش همه رویدادهای مربوط به یک نام کاربری در همه منابع
- استفاده از موتور همبستگی پیشرفته
- امکان اضافه نمودن سناریوهای جدید برای کشف حملات و تهدیدات
- استفاده از پایگاه دانش قوی
- نمایش خودکار راهکارهای مقابله با هر تهدید در کنار هشدارهای تولید شده
- دسته‌بندی هشدارهای تولید شده
- استفاده از سیستم Ticketing برای پیگیری حوادث و مشکلات
- مدیریت دارایی‌های شبکه و امکان اولویت دهی به آن‌ها
- مجهز به سامانه کشف نفوذ مبتنی بر شبکه و میزبان
- مجهز به سامانه کشف و مدیریت آسیب‌پذیری‌ها
- مجهز به داشبوردهای متنوع و کارآمد برای پیگیری رویدادها
- ارائه وضعیت امنیت شبکه توسط داشبوردهای امنیتی
- گزارش‌گیری و اطلاع‌رسانی جامع
- ذخیره‌سازی داده‌ها با امضای دیجیتال
- مدیریت حجم لاگ‌ها و پشتیبانی از ذخیره‌سازی داده‌ها روی NAS و SAN
- امکان آرشیو کردن لاگ خام، رویدادها و هشدارها
- امکان پیاده‌سازی به صورت متمرکز و توزیع شده
- پشتیبانی نرم‌افزاری و امکان اعمال تغییرات بر حسب نیاز مشتری
- امکان پشتیبان گیری از پیکربندی سیستم
- رابط کاربری گرافیکی (مبتنی بر وب و SSH)

۳-۶- آذرام (WAF)

روند رو به رشد استفاده از برنامه‌های کاربردی تحت وب و سهولت دسترسی به آن‌ها، برنامه‌های کاربردی تحت وب را به هدف مهمی برای مهاجمین، جهت نفوذ به سامانه‌های اطلاعاتی سازمان‌ها تبدیل کرده است. از طرفی دیگر، ماهیت نرم‌افزاری خدمات ارائه شده بر روی وب و درصد بالای آسیب‌پذیری‌های ناشی از اشتباهات برنامه‌نویسی نسبت به سایر آسیب‌پذیری‌ها، امروزه برنامه‌های کاربردی تحت وب را به یکی از بزرگترین چالش‌های امنیتی مسئولین IT هر سازمان تبدیل کرده است.

علی‌رغم اتخاذ راهکارهای معمول جهت پیشگیری از این دسته آسیب‌پذیری‌ها، همچنان امکان وجود آسیب‌پذیری در این نرم‌افزارها وجود دارد، لذا چنانچه به دلایلی آسیب‌پذیری موجود در برنامه کاربردی طی مراحل مختلف چرخه تولید نرم‌افزار و پس از آن شناخته نشود و یا مهاجم از یک حمله DAY-۰ جهت بهره‌برداری از یک آسیب‌پذیری استفاده نماید، در صورت وجود مکانیزم‌های پیش‌گیرنده دیگر، به منظور بررسی ارتباطات در لایه برنامه کاربردی، به میزان قابل توجهی امکان پیشگیری از این حملات وجود دارد.

آذرام، دیواره آتش برنامه‌های کاربردی تحت وب (Web Application Firewall) است که با قرارگیری بر سر راه ارتباطات مابین کاربر و برنامه کاربردی تحت وب و بررسی داده‌های ردوبدل شده از طریق پروتکل HTTP/S مانع ارسال درخواست‌های مخرب از طریق مهاجمین و یا بات‌های تحت شبکه به سمت برنامه کاربردی تحت وب می‌شود و بدین طریق با میزان بسیار زیادی از حملات رایج در حوزه برنامه‌های کاربردی تحت وب مقابله می کند.

ویژگی‌ها و مزایا

- پوشش دهنده ۱۰ آسیب پذیری مهم OWASP
- منطبق بر نیازمندی‌های بند ۶,۶ استاندارد PCI DSS 3.0

- پیاده‌سازی در قالب سخت‌افزار تحت شبکه، مجزا از سرویس‌دهنده‌های وب و پشتیبانی از چندین سرویس‌دهنده
- به‌روزرسانی آنلاین و آفلاین از طریق سرورهای به‌روزرسانی در داخل ایران
- تولید مجموعه قوانین امنیتی سفارشی سازی شده با حضور تیم متخصص در محل مشتری
- بهره‌گیری از به‌روز ترین قوانین امنیتی و امضاء حملات، توسعه یافته در آزمایشگاه‌های بین‌المللی امنیت نرم‌افزار
- پیشگیری آنی از حملات ناشناخته از طریق مکانیزم Virtual Patching
- گزارش‌گیری و اطلاع‌رسانی جامع حملات انجام شده به همراه جزییات و آمارهای مورد نظر
- کاهش بار پردازشی حاصل از رمزگشایی پروتکل HTTPS با امکان HTTPS Offloading
- کاهش بار ترافیکی حاصل از ارسال درخواست‌های نامعتبر از سمت پویش‌گرها، بات‌های تحت شبکه و سایر بدافزارها
- دسترس‌پذیری بالا با پشتیبانی همزمان از دو دستگاه آذرام
- توازن بار ترافیکی بین چندین سرویس‌دهنده وب افزونه
- پشتیبانی از سرویس‌های تحت وب و تکنولوژی‌های مبتنی بر SOAP,AJAX,XML و...
- پیشگیری از بارگذاری فایل‌های مخرب

۷- معرفی خدمات

۱-۷- خدمات امنیت اطلاعات

شرکت صبا سیستم صدرا آماده ارایه خدمات حرفه‌ای امنیت اطلاعات با توجه به نیاز کسب و کار سازمان‌ها است. این خدمات شامل خدمات مدیریتی، فنی، و آموزشی در ارزیابی وضعیت امنیت اطلاعات، امن‌سازی، نظارت و ممیزی امنیت اطلاعات است. این خدمات با رویکرد جامع به «مدیریت مخاطرات کسب و کار» در «سیستم مدیریت امنیت اطلاعات» به مشتریان ارایه می‌گردد.

۱-۱-۷- طراحی و پیاده‌سازی مرکز عملیات امنیت (SOC)

امروزه مهاجمین دسترسی راحت‌تری به ابزارهای نفوذ دارند و برای نفوذ به سیستم‌های کامپیوتری نیاز به داشتن دانش حرفه‌ای زیادی نیست، از این رو تعداد حملات فضای سایبر روز به روز در حال افزایش است. از طرف دیگر نوع حملات نیز به صورت پیچیده در آمده است و بیشتر حملات به صورت توزیع شده صورت می‌گیرد که این موضوع کشف و شناسایی آن‌ها را نسبت به حملات متمرکز سخت‌تر می‌کند. سازمان‌ها برای افزایش سطح امنیت خود، به تکنولوژی‌ها و ابزارهای مختلف امنیت روی می‌آورند و از شرکت‌های مختلف محصولات امنیتی تهیه می‌کنند. هر چند این موضوع می‌تواند سطح امنیت سازمان‌ها را تا حدی بالا ببرد ولی برای تضمین امنیت کافی نیست زیرا هر یک از این تکنولوژی‌ها و ابزارها حوزه مشخصی را پوشش داده و محافظت می‌کنند. این ابزارها در سازمان‌ها مانند جزیره‌های جدا از هم هستند که نیاز است برای تشخیص حملات پیچیده به خصوص حملات توزیع آن‌ها یکپارچگی و هماهنگی وجود داشته باشد.

مرکز عملیات امنیت(SOC) مجموعه‌ای از ابزارها، فرآیندها و عوامل انسانی است که مانیتورینگ متمرکز رخدادها، جمع‌آوری، تحلیل و مدیریت رخدادها را انجام می‌دهد و امکان یکپارچه‌سازی و ایجاد هماهنگی بین ابزارها و تکنولوژی‌های مختلف را فراهم می‌کند. شرکت صبا سیستم صدرا با توجه به ضرورت مرکز عملیات امنیت برای سازمان‌های کشور اقدام به توسعه ابزار بومی ماورا (SIEM) نموده است که هسته اصلی SOC می‌باشد، همچنین با توجه به در اختیار داشتن نیروی متخصصی که یکی از اولین پروژه‌های مرکز

عملیات کشور در سطح را راه‌اندازی کرده‌اند، قادر است مرکز عملیات امنیت را با توجه به نیاز سازمان‌ها طراحی و پیاده‌سازی کند.

خدمات قابل ارائه :

- طراحی ساختار مرکز عملیات امنیت با توجه به هدف تعریف شده برای مرکز
- سفارشی‌سازی و طراحی فرآیندها و رویه‌های مرکز با توجه به نیازها و فرآیندهای موجود سازمان مشتری
- تهیه و راه‌اندازی ابزارهای مورد نیاز مرکز
- آموزش تخصصی عوامل انسانی مرکز
- ارائه خدمات پشتیبانی و ارائه طرح توسعه و تداوم کسب و کار مرکز و طرح بازیابی از فاجعه
- ارائه برنامه‌های آموزشی مدون منطبق با استانداردهای معتبر در حوزه آموزش امنیت اطلاعات مانند NISTجهت بروز نگه داشتن دانش نیروهای مرکز
- مشاوره به سازمان‌ها جهت گزینش و استخدام نیروهای متخصص مورد نیاز مرکز

۲-۱-۷- طراحی و راه‌اندازی مرکز واکنش رخداد(CERT)

با توجه به گسترش حملات و سوانح امنیتی، برای جلوگیری از کاهش آسیب‌ها و هزینه‌های ناشی از این سوانح، لازم است تیمی برای واکنش سریع به فوریت‌های امنیتی در سازمان‌ها در نظر گرفته شود. مرکز واکنش به رخداد(CERT) تیمی است که در صورت بروز حوادث امنیتی راه‌حل‌هایی برای رفع و مقابله ارائه می‌کند. همچنین با توجه به افزایش سطح تهدیدات این تیم اقدامات لازم برای پیشگیری از وقوع رخداد را نیز انجام می‌دهد.

شرکت صبا سیستم صدرا با توجه به تجربه انجام پروژه‌های متعدد در زمینه‌های مختلف امنیت اطلاعات و با توجه به ارتباط مناسب با دانشگاه و تعامل با اساتید و دانشجویان رشته امنیت اطلاعات، این توانایی را دارد کلیه

اقدامات لازم برای راه‌اندازی مرکز CERTاعم از طراحی معماری و رویه‌ها، جذب نیروی متخصص مورد نیاز و آموزش آن‌ها را انجام دهد.

خدمات قابل ارائه:

- تعریف ماموریت و محدوده فعالیت مرکز با توجه به نیازمندی‌ها و وضعیت امنیتی فعلی سازمان مشتری
- طراحی معماری و ساختار داخلی مرکز CERT
- تعریف خط‌مشی‌ها، جریان‌های کاری و اطلاعاتی مورد نیاز مرکز با توجه هدف مرکز، رویه‌ها قوانین سازمان مشتری
- تامین، نصب و راه‌اندازی ابزارهای مورد نیاز برای عملکرد بهینه مرکز CERT
- تدوین برنامه‌های آموزشی دوره‌ای برای کارمندان مرکز جهت به روز نگه داشتن دانش آن‌ها
- آموزش تخصصی نیروی انسانی مرکز CERT
- ارائه کلیه خدمات پشتیبانی و نگهداشت مرکز CERT با توجه به نیازهای مشتری

۳-۱-۷- مشاوره، آموزش و هدایت در فرآیند برقراری چرخه حیات توسعه امن نرم‌افزار(SDL)

امنیت نرم‌افزار وابستگی شدید به چرخه حیات توسعه آن دارد. در صورتی که امنیت در مراحل نیاز سنجی، آنالیز، طراحی، پیاده سازی، تست، و راه‌اندازی نرم افزار در نظر گرفته نشده باشد، به احتمال زیادی دارای آسیب پذیری امنیتی خواهد بود و این آسیب‌پذیری‌های بعضاً منطقی توسط روش‌های معمول مدیریت ریسک قابل رفع نیستند.

کشف هر آسیب پذیری در مراحل ابتدایی تولید نرم افزار هزینه نگهداری نرم‌افزار را به مراتب کاهش می‌دهد. به طور مثال هزینه کشف و رفع هر خطا در هر مرحله از چرخه حیات تولید نرم افزار یک دهم کشف و رفع همان خطا در مرحله بعد از چرخه است.

به همین منظور شرکت مایکروسافت با ارائه SDL، چرخه حیاتی برای تولید نرم افزار ارائه کرده است که امنیت را در تمامی مراحل تولید نرم افزار لحاظ می‌کند. شرکت صبا سیستم صدرا با توجه به سابقه طولانی در بررسی امنیت، مشاوره و امن سازی نرم افزارهای بومی و آشنایی با معضلات امنیتی صنعت نرم افزار کشور به ارائه خدمات مشاوره، هدایت، آموزش و نظارت بر پیاده‌سازی SDL برای شرکت‌های تولید کننده نرم افزار می‌پردازد.

شرکت صبا سیستم صدرا با آموزش امنیت به پرسنل دخیل در چرخه تولید نرم افزار در هر سطحی و با توجه به نقش هر یک از کارکنان، نیازمندی اولیه SDL را برای کارفرمایان برآورده می‌سازد. سپس با مشاوره و هدایت کارکنان کارفرما از آغازین مراحل ساخت نرم افزار بر اجرای SDL توسط ایشان نظارت کرده و امنیت را از ابتدای چرخه تولید تا انتهای استقرار نرم افزار در محل مشتریان برقرار می‌سازد و بدین ترتیب هزینه نگهداری نرم افزار به میزان قابل توجهی برای سازندگان آن کاهش می‌یابد.

خدمات قابل ارائه:

- آموزش مفاهیم امنیت به پرسنل کارفرما با توجه به نقش آن‌ها (تحلیلگر، طراح، برنامه نویس، تستر، نیروهای عملیاتی)
- مشاوره و هدایت تحلیلگران در تعریف نیازمندی‌های امنیتی نرمافزار و بازبینی نیازمندی‌های تعریف شده
- بررسی امنیتی طراحی نرم افزار جهت تشخیص زودهنگام آسیب‌پذیری‌های امنیتی منطقی و ارائه راه حل به منظور رفع آن‌ها
- هدایت تیم برنامه‌نویس جهت کدنویسی امن
- بررسی امنیتی ابزارها و بسترهای مورد استفاده در تولید نرم افزار و ارایه راه‌حل‌های جایگزین امن
- تعریف test caseهای امنیتی white box و black box
- راهنمایی جهت رفع آسیب‌پذیری‌های امنیتی کشف شده در مرحله تست

- تست نفوذ و ارزیابی امنیتی نرم افزار در محیط عملیاتی

٤-١-٧- مشاوره و پیاده‌سازی مدل بلوغ امنیت سازمانی و مدل بلوغ امنیت محصولات

مدل بلوغ امنیت ابزاری برای سنجش سطح بلوغ امنیت یک سازمان یا یک محصول است. بدون استفاده از مدل بلوغ، تصمیم گیری درباره وضعیت فعلی امنیت سازمان و برنامه‌ریزی جهت ارتقاء آن بسیار دشوار خواهد بود. در واقع مدل بلوغ امنیت است که نشان می‌دهد فعالیت‌های امنیتی، سیستم مدیریت امنیت اطلاعات، و چرخه حیات توسعه امن تا چه حد به بهبود وضعیت امنیت کمک کرده و نقاط ضعف امنیت در چه بخش‌هایی متمرکز شده است.

شرکت صبا سیستم صدرا دارای تجربه زیاد در ارزیابی وضعیت امنیتی سازمان‌ها بوده و با استفاده از متدولوژی‌های بلوغ امنیت به تعیین سطح بلوغ امنیت سازمان‌ها و محصولات آن‌ها می‌پردازد و برای افزایش این سطح بلوغ برنامه‌ای مدون به مشتریان خود ارایه می‌نماید.

شرکت صبا سیستم صدرا با استفاده از معیارهای دو مدل بلوغ امنیت BSIMM و OPEN PRISMA سطح بلوغ محصولات تولیدی سازمان‌ها را اندازه گیری می‌کند. همچنین این شرکت با بهره‌گیری از معیارهای مدل بلوغ VIST PRISMA سطح بلوغ فرآیندهای مدیریت امنیت سازمان را می‌سنجد. پس از سنجش میزان بلوغ امنیتی سازمان و محصولاتش، شرکت صبا سیستم صدرا نقشه راه را برای بهبود سطح بلوغ امنیتی سازمان‌ها و محصولاتشان به ایشان ارایه می‌کند.

خدمات قابل ارائه:

- استفاده از مدل BSIMM برای مقایسه امنیتی محصولات سازمان با تولیدکنندگان برتر جهانی
- استفاده از مدل OpenSAMM برای سنجش سطح بلوغ امنیت محصولات
- ارایه راه کار و نقشه راه برای بهبود سطح بلوغ امنیتی محصولات سازمان با استفاده از مدل OpenSAMM

- تطبیق فعالیت‌های ISMS سازمان با مدل NIST PRISMA جهت سنجش سطح امنیت سازمان
- تدوین و تنظیم فعالیت‌های ISMS سازمان جهت ارتقاء سطح بلوغ امنیتی آن

۵-۱-۷- برقراری سیستم‌های مدیریت امنیت اطلاعات بر اساس استانداردهای سری ISO27000

چالش امنیت اطلاعات در دنیای مجازی مسأله‌ای باز و حل نشده است. در رویکرد سنتی به مسأله امنیت اطلاعات، برقراری کنترل‌های امنیت به صورت موردی و براساس نیاز فعلی پاسخی به تهدیدات امنیتی بوده است. وجود کنترل‌های امنیتی به صورت موردی و غیر یکپارچه، سازمان را در معرض سوء استفاده خرابکاران از ریسک‌های در نظر گرفته نشده قرار می‌دهد.

سیستم مدیریت امنیت اطلاعات به صورت یک چرخه منظم ریسک‌های امنیتی را تشخیص داده و راه حل مناسب را پیدا می‌کند. سپس این راه‌حل‌ها را پیاده سازی و بر حسن اجرای آن‌ها نظارت کرده و در صورت نیاز آن‌ها را بهبود می‌بخشد. وجود یک سیستم مدیریت امنیت اطلاعات باعث می‌شود سازمان تهدیدات امنیتی بالقوه را شناسایی کرده و برای آن‌ها راه حل مناسب پیدا کند و این اعمال را به صورت مداوم و در قالب یک چرخه تکراری اجرا کند.

سال‌ها تجربه متخصصان شرکت صبا سیستم صدرا آن‌ها را بر این باور داشته است که برقراری امنیت در یک سازمان بدون برقراری سیستم مدیریت امنیت اطلاعات امکان پذیر نمی‌باشد. بدین منظور پرسنل شرکت با رویکردی تخصصی به ISMS آماده ارایه انواع خدمات مشاوره، طراحی، پیاده سازی و ممیزی سیستم مدیریت امنیت اطلاعات برای مشتریان است. تجربه علمی متخصصان شرکت در بومی سازی امنیت و نگهداری امنیتی سازمان‌های مشتری، این شرکت را به گزینه مناسبی برای اجرای پروژه‌های ISMS تبدیل نموده است.

خدمات قابل ارائه :

- تعیین محدوده (Scope) سیستم مدیریت امنیت اطلاعات

- ارزیابی ریسک‌های امنیتی براساس متدلوژی‌های کمی به صورت دوره‌ای و منظم
- تدوین و بازبینی خط‌مشی‌های امنیتی و نظارت بر اجرای آن‌ها بر اساس شرایط سازمان مشتری
- تدوین آیین‌نامه‌ها و راهنماهای امنیتی براساس خط‌مشی‌های امنیتی تدوین شده
- مدیریت ریسک‌های امنیتی شامل اجتناب، کاهش اثر ، انتقال و پذیرش ریسک
- طراحی و تدوین روال‌های پاسخ به رخدادهای امنیتی
- طراحی و تشکیل تیم پاسخ به رخدادها و سوانح امنیتی
- تدوین طرح تداوم کسب و کار و بازیابی از بحران(BCP/DRP) برای سازمان مشتری
- مشاوره و اجرای سیستم مدیریت امنیت اطلاعات جهت دریافت گواهی‌نامه

٦-١-٧- ارزیابی امنیتی و امن سازی برنامه های کاربردی

از آنجاکه برنامه های کاربردی امروزه به هدف اول مهاجمین جهت نفوذ به زیرساخت اطلاعاتی سازمان ها تبدیل شده‌اند، ارزیابی و امن سازی مناسب آن ها می تواند به میزان قابل توجهی ریسک کلی سازمان را کاهش دهد.

تیم متخصص امنیت نرم افزار شرکت صبا سیستم صدرا با داشتن نیروهای مجرب و مسلط به دانش روز امنیتی و ابزارهای مورد نیاز جهت ارزیابی امنیتی و امن سازی برنامه های کاربردی و همچنین پیش زمینه کاری در حوزه توسعه برنامه های کاربردی با تکنولوژی های مختلف نظیر C++/C این امکان را فراهم می کنند تا تمامی مراحل ارزیابی و امن سازی را به صورت کاملاً تخصصی و مطابق با نیازهای مشتری اجرا نمایند.

خدمات ارزیابی امنیتی می تواند بنا به نظر مشتری به صورت جعبه سیاه (بدون در اختیار گذاشتن کد منبع برنامه کاربردی) و جعبه سفید (بررسی امنیتی کد منبع) و یا ترکیبی از هر دو، ارائه شده و گزارش مربوطه در قالبی کاملاً استاندارد و قابل فهم برای سطوح مختلف سازمانی تولید شود (در صورت نیاز نمونه ای از حملات مهم با سوء استفاده از آسیب پذیری های کشف شده، برای کارفرما به صورت زنده نمایش داده می شود).

پس از مرحله ارزیابی، نیروهای متخصص و مسلط به تکنولوژی مرتبط با هر برنامه کاربردی، نظر فنی خود را در خصوص راهکارهای قابل ارائه در تکنولوژی مربوطه، جهت کاهش و یا پیشگیری از مخاطرات مرتبط با هر آسیب پذیری ارائه می دهند. در صورت نیاز کارفرما، این تیم اقدام به مشاوره و یا آموزش برنامه‌نویسان و طراحان سازمانی کرده تا امکان برطرف کردن هرچه سریع تر آسیب پذیری های کشف شده، برای سازمان فراهم گردد.

خدمات قابل ارائه :

- تست نفوذپذیری برنامه های کاربردی
- ارزیابی امنیتی جعبه سیاه برنامه های کاربردی
- ارزیابی امنیتی جعبه سفید و بررسی امنیتی کد برنامه های کاربردی
- تست fuzzing نرم‌افزارهای سیستمی و برنامه های کاربردی با معماری Client-Server
- مهندسی معکوس نرم افزارهای سیستمی و پروتکل های بومی
- مشاوره، نصب و پیکربندی Web Application Firewall و Web Application Honeypot
- مشاوره و امن سازی انواع برنامه های کاربردی با تکنولوژی .NET، J2EE، Python، C/C++، و PHP
- مشاوره و پیاده سازی امنیت در چرخه تولید نرم افزار (SDL)
- ارزیابی و تحلیل ریسک و تولید مدل تهدید نرم افزار
- برگزاری دوره های مقدماتی و پیشرفته امنیت برنامه های کاربردی برای برنامه‌نویسان و طراحان سازمان

۷-۱-۷- ارزیابی، تحلیل، کاهش و مدیریت ریسک‌های امنیتی

مدیریت ریسک‌های امنیتی عمده ترین فعالیت مدیریت امنیت اطلاعات است. در یک نگاه کلی برخورد با ریسک‌های امنیتی شامل شناسایی، تحلیل، ارزیابی و در نهایت واکنش در قبال ریسک است. در فعالیت شناسایی ریسک، ریسک‌های امنیتی شناخته شده و سپس در ارزیابی، شدت اثر و احتمال وقوع هریک تعیین می‌گردد. پس از شناسایی و ارزش‌گذاری ریسک‌ها و مخاطرات امنیتی باید آنها را مدیریت نمود. مدیریت ریسک شامل اجتناب از ریسک با استفاده از کنترل‌های مناسب امنیتی، انتقال ریسک و در نهایت پذیرش ریسک است.

شرکت صبا سیستم صدرا به شناسایی دارایی های اطلاعاتی سازمان پرداخته و پس از ارزش گذاری آنها با استفاده از متدلوژی معتبرOVTAVE تهدیدات امنیتی را ارزیابی می‌کند. در این مرحلهOCTAVE شاخص ریسک هر یک از دارایی‌های اطلاعاتی مذکور را براساس اهمیت آن دارایی و میزان تهدید بالقوه آن مشخص می‌کند.

در فاز مدیریت ریسک شرکت صبا سیستم صدرا با پیاده‌سازی کنترل‌های امنیتی براساس استانداردISO27001,ISO27002 از ریسک‌های اولویت بالا در سازمان مشتری اجتناب می‌نماید. در صورتی که ریسک قابل اجتناب نباشد با استفاده از کنترل‌های امنیتی مناسب اثر رخداد آن ریسک کاهش داده می‌شود. در صورتی که ریسک قابل اجتناب یا کاهش نباشد ، شرکت صبا سیستم صدرا به مشتریان خود راه‌حل‌هایی جهت انتقال یا پذیرش ریسک ارائه می دهد.

خدمات قابل ارائه :

- ارزش گذاری دارایی های سازمان و ساختAsset Inventory
- شناسایی و ارزیابی ریسک‌های امنیتی براساس متدلوژیOCTAVE
- مشاوره، طراحی و پیاده‌سازی کنترل‌های امنیتی براساس استاندارد سری ISO27000 و Best Practiceها جهت اجتناب از ریسک یا کاهش اثر آن

- مشاوره به مشتری جهت انتقال ریسک یا پذیرش آن
- آموزش مدیریت ریسک به بخش امنیت سازمان و ارایه طرح (Plan) آن جهت اجرای برنامه مدیریت ریسک به صورت مداوم و درون سازمانی

۸-۱-۷- مشاوره و راه‌اندازی زیرساخت‌های امنیت اطلاعات و ارتباطات

برقراری امنیت و پیاده سازی بسیاری از کنترل‌های امنیتی بدون وجود زیرساخت مناسب امکان پذیر نیست. فایروال، WAF، Honey pot، SIEM، IDS/IPS زیر ساخت کلید عمومی، تصدیق اصالت چند فاکتوری، رمز نگاری ارتباطات، ذخیره سازی رمز شده و... زیرساختهای فنی به منظور پیاده سازی خط‌مشی‌ها و کنترل‌های امنیتی در سازمان هستند. بدون استفاده از این تکنولوژی‌ها امکان برقراری امنیت در سازمان و پیاده سازی سیستم مدیریت امنیت اطلاعات غیر ممکن خواهد بود.

شرکت صبا سیستم صدرا با شناخت کامل از محصولات امنیتی موجود در بازار و همچنین ارایه محصولات امنیتی SIEM و WAF در سبد محصولات خود، امکان مشاوره، طراحی و اجرای زیرساخت‌های امنیتی برای مشتریان خود را به وجود آورده است.

تجربه نیروی متخصص امنیت این شرکت در به کارگیری و بومی‌سازی فناوری‌های زیرساخت امنیت اطلاعات باعث شده که این شرکت علاوه بر توانایی در برپاسازی زیرساخت‌های امنیت با استفاده از محصولات رایج در بازار قابلیت یافتن، جذب و بومی‌سازی فناوری‌های جدید مورد نیاز مشتریان خود باشد.

خدمات قابل ارائه:

- طراحی امن و بازبینی امنیت طراحی مرکز داده
- انتخاب، پیکر بندی و راه اندازی فایروال، UTM، Antivirus، TPS/IDS
- نصب، پیکربندی و راه اندازی Honey pot
- نصب، پیکر بندی و راه اندازی SIEM

- نصب، پیکر بندی و راه اندازی WAF
- مشاوره و راه اندازی زیرساخت کلید عمومی مبتنی بر RSA و ECC
- مشاوره و راه اندازی تصدیق اصالت چند فاکتوری(OTP، توکن، Biometric،...)
- مشاوره، طراحی، راه اندازی VPN و ارتباطات رمزشده
- مشاوره و راه اندازی سیستم‌های ذخیره سازی امن و رمز نگاری شده
- مشاوره و راه اندازی سیستم‌های Authorization و ACL

۹-۱-۷- تشخیص و پیگیری جرایم رایانه‌ای(Computer Forensics)

زمانی که اتفاق امنیتی در سازمانی به وقوع می‌پیوندد، علاوه بر اجرای طرح تداوم کسب و کار، باید احتمال خرابکاری یا نفوذ مورد بررسی قرار گیرد. درصورت مثبت بودن نتیجه بررسی، سازمان می‌تواند با پیگیری جرم و کشف نفوذ گر و علت رخداد،بخشی از خسارت وارده را توسط دستگاه‌های انتظامی و قضایی جبران نماید. به عمل بررسی احتمال خرابکاری و نفوذ و کشف نفوذگر و علت رخداد و جمع‌آوری شواهد محکمه پسند، «پیگیری جرایم رایانه‌ای» گفته می‌شود.

برای پیگیری جرایم رایانه ای, نیاز به وجود بستر اطلاعاتی مناسب است که راه‌اندازی آن نیاز به تخصص و تجربه‌ی کافی دارد زیرا ترکیب تیم پیگیری جرایم رایانه ای بسیار متنوع و متشکل از متخصصان امنیت اطلاعات و مسایل حقوقی است و هزینه ی ایجاد چنین تیمی برای سازمان ها توجیه پذیر نیست.

خدمات قابل ارائه:

- راه‌اندازی بستر مناسب برای اطلاع از رخدادهای امنیتی در لحظه وقوع
- راه‌اندازی بستر مناسب برای جمع آوری شواهد محکمه پسند برای رخدادهای امنیتی
- پیگیری مسایل حقوقی جهت به اثبات رساندن ادعا

۲-۷- خدمات آموزش امنیت اطلاعات

۱-۲-۷- آگاهی‌رسانی امنیت

آگاهی‌رسانی امنیت تنها برای حساس کردن پرسنل به مسائل امنیتی بوده و در قالب جلسات موردی، ایمیل، پوستر و. . . به آگاه سازی کارکنان در مورد یک مسأله امنیتی خاص می‌پردازد. شرکت صبا سیستم صدرا در آگاهی‌رسانی امنیتی به نیروی انسانی مشتریان خود اعمال زیر را انجام می‌دهد:

- تدوین طرح و برنامه آگاهی‌رسانی
- برگزاری جلسات آگاهی‌رسانی
- تهیه و تدوین محتوا برای رسانه‌های آگاهی‌رسانی امنیت

۲-۲-۷- آموزش امنیت مبتنی بر نقش

با اینکه دوره‌های آموزشی امنیت فراوانی به صورت آماده در بازار یافت می‌شوند، اکثر این دوره‌ها برای پرسنل و نقشی که در سازمان ایفا می‌کنند مناسب نیستند. آموزش‌های مبتنی بر موضوع معمولاً پرسنل را برای انجام وظایف امنیتی خود آماده نمی‌کنند زیرا مطالب آن‌ها تخصصی بوده و همه وظایف را پوشش نمی‌دهد، از سوی دیگر این دوره‌ها معمولاً حاوی مطالب زیادی هستند که در حیطه عملکرد پرسنل نمی‌گنجد. به همین منظور NISTپیشنهاد برگزاری دوره‌های امنیتی مبتنی بر نقش افراد را می‌دهد. در همین راستا شرکت صبا سیستم صدرا به ارایه دوره‌های آموزشی مبتنی بر نقش به پرسنل مشتریان خود می‌پردازد. خدمات آموزش مبتنی بر نقش شرکت این شرکت عبارت است از:

- شناسایی نقش‌های سازمانی نیازمند آموزش امنیت
- نیاز سنجی و تعیین سطح آموزش برای نقش‌ها
- برنامه ریزی و طراحی Plan آموزش امنیت
- طراحی دوره‌های بومی امنیت سازمان برای نقش‌ها با توجه به فرهنگ سازمانی مشتری
- اجرا و برگزاری دوره‌های آموزشی

- ارزیابی کارایی دوره‌های آموزش به منظور بهبود و تقویت آن‌ها و سنجش سطح بلوغ امنیت

۳-۲-۷- دوره‌های تخصصی امنیت

علاوه بر آموزش مبتنی بر نقش لازم است پرسنل امنیت اطلاعات هر سازمان به منظور کسب توانایی در انجام بهتر وظایف، دوره‌های آموزش تخصصی فنی و مدیریتی امنیت را فرا گیرند. به همین منظور شرکت صبا سیستم صدرا در راستای رفع این نیاز مشتریان با برگزاری دوره‌های آموزشی تخصصی امنیت، اقدام به انتقال دانش امنیت تخصصی و عملیاتی به پرسنل امنیت اطلاعات آن‌ها می‌نماید. این دوره‌ها عبارتند از:

- آموزش سیستم مدیریت امنیت اطلاعات ISMS
- آموزش CEH
- آموزش طراحی امن شبکه و مرکز داده
- آموزش امنیت شبکه و بررسی امنیتی تجهیزات شبکه و امنیت بی‌سیم
- آموزش نصب، راه اندازی و تست FireWallو UTM
- آموزش امنیت ویندوز
- آموزش امنیت یونیکس و سیستمهای کد منبع باز
- آموزش امنیت پایگاه‌های داده
- آموزش Honeypot
- آموزش بررسی امنیت نرم افزار و تست امنیتی نرم‌افزار
- آموزش امنیت نرم‌افزار (طراحی، پیاده سازی)
- آموزش رمز نگاری کاربردی

۸- رتبه شورای عالی انفورماتیک

زمینه فعالیت	رتبه	تعداد کار مجاز	ظرفیت مجاز (میلیون ریال)	تعداد کار اشغال شده	تعداد کار آزاد
امنیت فضای تولید و تبادل اطلاعات	۱	۱۲	نامحدود	۰	۱۲
تولید و پشتیبانی نرم افزارهای سفارش مشتری	۱	۱۲	نامحدود	۰	۱۲
خدمات پشتیبانی	۳	۹	٤۳۲۰۰	۰	۹
شبکه داده ها ی رایانه ای و مخابراتی	۳	۹	٤۰۵۰۰	۰	۹
مشاوره و نظارت بر اجرای طرح های انفور ماتیک، فناوری اطلاعات و ارتباطات	٤	۷	۱۳۵۰۰	۰	۷

Saba System Sadra

صبا سیستم صدرا