فناوری اطلاعات رجاء
RAJA INFORMATION TECH.

TÜV INTER CERT SAAR ISO 10002:2014

TÜV INTER CERT SAAR ISO 9001:2015

فهرست

درباره شرکت فناوری اطلاعات رجاء

About Raja Information Tech.

گروه رجاء با بیش از یک دهه سابقه، شامل شرکت‌های فناوری اطلاعات رجاء، توسعه سرمایه گذاری رجاء و دانشگاه رجاء می باشد که در زمینه فناوری اطلاعات و ارتباطات در حوزه های خدمات مختلف زیرساخت و امنیت، تولید و فروش انواع نرم‌افزارهای بانکی، صنعتی و خدمات متنوع دیگر فعالیت دارد.

شرکت فناوری اطلاعات رجاء با تکیه بر دانش روز و کادری مجرب با انجام ابر پروژه های ملی توانسته در عرصه IT، پیشتاز در سطح کشور باشد.

شرکت برتر حوزه امنیت اطلاعات

- رتبه یک شورای عالی انفورماتیک
- عضو نظام صنفی رایانه ای و سندیکا افتا
- پروانه تولید نرم افزار از وزارت صمت

مجوزها و تأییدیه ها

- ۳+ مجوز از مرکز افتا ریاست جمهوری
- ۳+ مجوز از سازمان فناوری اطلاعات
- ۲+ مجوز از سازمان پدافند غیر عامل

نیروهای متخصص

- ۱۰۰+ کادر ستادی و کارشناسان فنی
- ۱۰۰+ هیئت علمی دانشگاه رجاء
- ۵۰+ متخصص تحقیق و توسعه

دانش بنیان

- ۱۰+ محصول و خدمت دانش بنیان
- ۸+ سال سابقه دانش بنیان
- ۲+ تیم تحقیقاتی مستقر در پارک فناوری شریف

بیش از ده سال سابقه فعالیت

- ۱۰۰۰+ تعداد مشتری
- ۲۵۰۰+ پروژه انجام شده
- ۸۵۰۰+ لایسنس محصول نصب شده

ساختمان ستادی

تهران، کریمخان، آبان جنوبی، ساختمان رجاء

برج فناوری شریف (R&D)

تهران ، جنب دانشگاه شریف، طبقه۵ واحد ۵۰۱

دانشگاه رجاء

استان قزوین ، بلوار نوروزیان، دانشگاه رجاء

آزمایشگاه افتا و دیتا سنتر

تهران،حافظ،جنب دانشگاه امیرکبیر،پلاک ۱

ISO 10002:2014

ISO 9001:2015

ارزش های شـرکت
Company values

- حرکت در مسیر تعالی از طریق شناسـایی و پایـش ملموس و مبتنی بر شواهد در تمامی ابعاد سازمان
- افـزایش اثربخـشی با بـهره برداری از فنـاوری های به روز در جهت خلاقیت و نوآوری
- اجرای تعهدات شرکت با بهترین کیفیـت در زمان مقرر و با هزینه مناسب
- پشتیبانی و پاسخگویی سریع و مشتری مداری
- در نظر داشتن اصل کیفیت و بهبود مستمر
- ارائه کیفیت بالای خدمات پس از فروش
- رشد و بالندگی بر مبنای شایسته سالاری
- ارتقای پایدار وجهه تجاری شرکت
- پیشتازی در فناوری


مجوز افتا در حوزه ارزیابی امنیتی


پروانه تولید نرم افزار از وزارت صمت


مجوز سازمان پدافند غیر عامل


مجوز سازمان تنظیم مقررات


مجوز افتا در حوزه امن سازی زیرساخت


عضو حقوقی سندیکا افتا از سال ۹۵


مجوز سندیکا افتا


مجوز نظام صنفی رایانه ای


مجوز شورای عالی انفورماتیک


مجوز سازمان پدافند غیر عامل

محصولات افتا

ISO 10002:2014

ISO 9001:2015

RAJA PAM

سامانه مدیریت دسترسی‌های ویژه

Privileged Access Management

نظارت و کنترل بر دسترسی های راه دور کاربران مجاز و پیمانکاران به تجهیزات مستقر در مراکز داده و منابع حساس شبکه سازمان اعم از سرورها، تجهیزات شبکه ای و امنیتی از نگرانی های جدی مدیران سازمانی محسوب می گردد. این کاربران با استفاده از پروتکل های مختلف دسترسی راه دور نظیر RDP,Telnet ,SSH ,VNC به تجهیزات حساس سازمانی متصل می شوند. این در حالیست که معمولا این پروتکل ها فاقد امکانات کیفی ثبت رخداد و رویدادنگاری بوده و لذا مدیر امنیت سازمان، نظارت لازم را بر اینگونه دسترسی ها نخواهد داشت.

سامانه RAJA-PAM ، راهکاری است که به منظور مدیریت دسترسی های ویژه ارایه شده تا به سهولت و بدون نیاز به تغییر در فرآیندهای سازمانی، سطح نظارت بالایی را بر اینگونه دسترسی های راه دور فراهم آورد. این سامانه امکان نظارت و پایش بر دسترسی های راه دور را از طریق ضبط و نمایش فیلم، ثبت رخداد و امکان جستجو بر جلسات فراهم می نماید. همچنین مدیر قادرست سیاست های فیلترینگ لازم را نیز بر مبنای امکان اجرای برنامه ها و فرامین در جلسات دسترسی اعمال نماید.

مزایای استفاده از سامانه RAJA-PAM

- امکان جستجوی مقادیر خاص، رویدادهای ویژه و فرامین تایپ شده درفیلم های ضبط شده
- نظارت و کنترل بر پروتکل های متداول دسترسی راه دور نظیر RDP, SSH ,Telnet , VNC
- تعیین لیست‌های سفید و سیاه از دستورات و یا پوشه‌های هر سرور برای کاربران
- امکان استقرار به دو صورت شفاف و غیر شفاف در شبکه
- ضبط و پخش جلسات دسترسی بصورت فیلم
- فیلترینگ فرامین و برنامه ها

کاربردهای سامانه RAJA-PAM

احراز اصالت و کنترل دسترسی کاربران

- امکان تعریف یک یا چند گروه بازرسی که توانایی نظارت بر جلسات کاربران را دارا باشند
- احراز اصالت کاربران از طریق اکتیو دایرکتوری
- احراز اصالت کاربران بصورت محلی

پشتیبانی از پروتکل های دسترسی راه دور رایج

- Telnet
- VNC
- RDP
- SSH

امکان جستجو در فیلم های جلسات نشست

- اندیس گذاری تصاویر به منظور افزایش سرعت جستجو
- قابلیت جستجو بر متون مشاهده شده کاربران
- قابلیت جستجو در عناوین پنجره‌های باز شده
- قابلیت جستجو در واژگان تایپ شده کاربران

ثبت رخدادها

- ثبت رخدادهای مهم سیستمی و شبکه ای
- ثبت رخدادهای عملکردی کاربران

دسترس پذیری بالا

- قابلیت دسترسی بالا و مقاومت در برابر خرابی
- امکان همگام سازی خودکار بین سرورهای افزونه

نظارت بر جلسات نشست کاربران با امکان ذخیره سازی

- ذخیره سازی هر نشست کاربر بصورت فیلم مجزا
- رمزنگاری فیلم های ضبط شده

نظارت زنده بر جلسات نشست کاربران

- امکان مانیتورینگ زنده فعالیت کاربر
- امکان قطع نشست کاربر

امکان فیلترینگ

- فیلترینگ فرامین
- فیلترینگ برنامه های اجرایی

امکان نسخه برداری از اطلاعات مبادله شده

- نسخه‌برداری از فایل‌ها و اطلاعات مبادله شده کاربران با سرورها

تعامل با سامانه های مدیریت رخداد و حوادث ایمنی

- امکان ارسال رخدادها به SOC
- ارائه گزارشات متنوع تحلیل رویدادهای امنیتی

کنسول مدیریتی

- کنسول مدیریتی مبتنی بر وب

RAJA DLP

سامانه جلوگیری از نشت اطلاعات

Data Loss Prevention

همه روزه اخبار جدیدی در مورد نشت اطلاعات، تهدیدات کامپیوتری و سوءِ استفاده کاربران، منتشر می‌شود. این گونه اشتباهات غالباً به دلیل عدم کنترل و نظارت بر سیستم های کامپیوتری رخ می‌دهد.

در گذشته بسیاری از حملات با هدف تخریب اتفاق افتاده‌اند. اما با گذشت زمان و ورود به عصر اطلاعات و ارتباطات هدف حملات نیز تغییر کرده است. امروزه تلاش مهاجمین در راستای دستیابی به اطلاعات سازمانی است. بسیاری از گزارشگران و مشاوران هزینه‌های امنیتی را تا میلیاردها دلار بر آورد کرده‌اند. با توجه به افزایش کاربران سیستم‌های اطلاعاتی دسترسی آسان به اطلاعات و رشد و فرایند کاربران مطلع تعداد سوءِ استفاده‌ها از فناوری و انواع تهدیدها افزایش یافته است. گسترش این نوع حملات لزوم تشکیل تیم امنیتی و یک نرم افزار امنیتی کاملا بومی و مستقل را بیش از پیش مشخص می‌نماید.

سامانه جلوگیری از نشت اطلاعات (RAJA-DLP)

امروزه بیش از هر زمان دیگری، تولید و گردش اطلاعات در بستر فناوری اطلاعات انجام می گردد. این اطلاعات به عنوان ارزشمندترین دارایی‌های یک سازمان یا شرکت محسوب شده و نگهداری از آن، نگرانی اصلی سازمان‌ها و شرکت‌های بزرگ و کوچک دولتی و خصوصی محسوب می گردد، چرا که دسترسی‌های غیرمجاز به اطلاعات و دانش در هرمجموعه بسته به نوع فعالیت آن علاوه بر تبعات مالی فراوان، منجر به از بین رفتن اعتبار و جایگاه آن می گردد. در حالی که عمده توجه سازمان‌ها به ساختارها و ابزارهای امنیتی به سمت سرویس‌دهنده معطوف است، نتایج بررسی‌ها نشان از وجود خطرات بزرگی در زمینه نشت/افشای عمدی و یا سهوی اطلاعات از داخل سازمان و توسط کاربران آن می‌دهد. از این رو لازم است جهت حراست از اطلاعات، تدابیری اندیشیده شود.

سامانه کاملا بومی RAJA-DLP در جهت پوشش حداکثری امنیت در نقاط انتهایی شبکه (Client) طراحی شده است. جهت تحقق این هدف، هر دو رویکرد پیشگیری از نشت داده (DLP/DRM) به‌صورت بهینه در سامانه RAJA-DLP پیاده‌سازی گردیده است. در نتیجه این سامانه به‌عنوان راهکار جامع و یکپارچه، امنیت پایانه‌های شبکه و کاربران انتهایی در راستای جلوگیری از نشت اطلاعات سازمانی را بر عهده دارد.

راهکارهای اجرایی برای جلوگیری از نشت اطلاعات

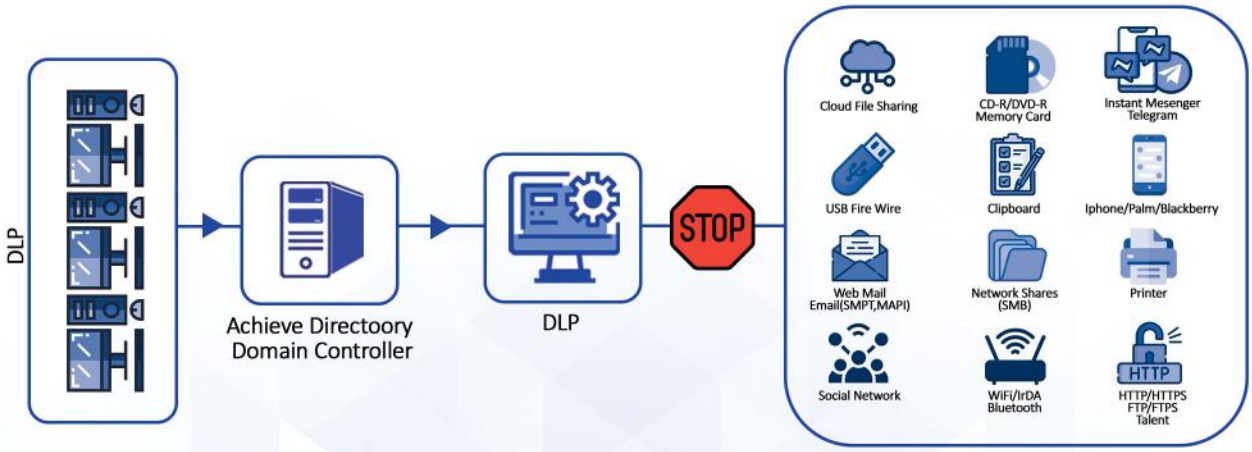
دو رویکرد در زمینه جلوگیری از نشت اطلاعات وجود دارد:

- کنترل و نظارت بر گذرگاه‌های ورود و خروج اطلاعات (DLP)

در رویکرد اول درگاه‌های خروج اطلاعات مانند حافظه‌های جانبی و دیسک‌ها و یا بستر شبکه همچون اینترنت و ایمیل، کنترل و نظارت می‌شوند. مهمترین ضعف این روش، وابستگی آن به سامانه DLP و باقی ماندن اطلاعات به‌صورت خام است. بنابراین اطلاعات و دارایی‌های سازمانی همچنان در خطر نشت می‌باشند و در صورت خروج اطلاعات امکان سوءِ استفاده از آنها وجود دارد.

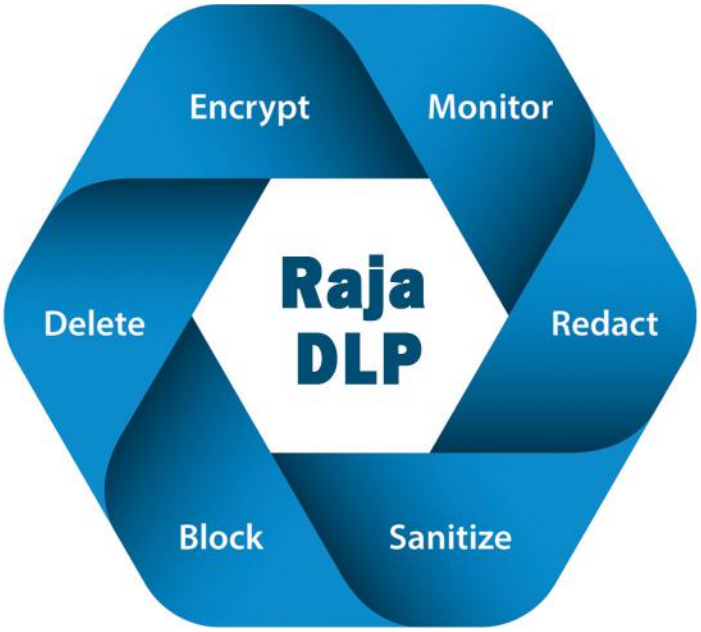
- رمزنگاری اطلاعات از لحظه تولید (DRM)

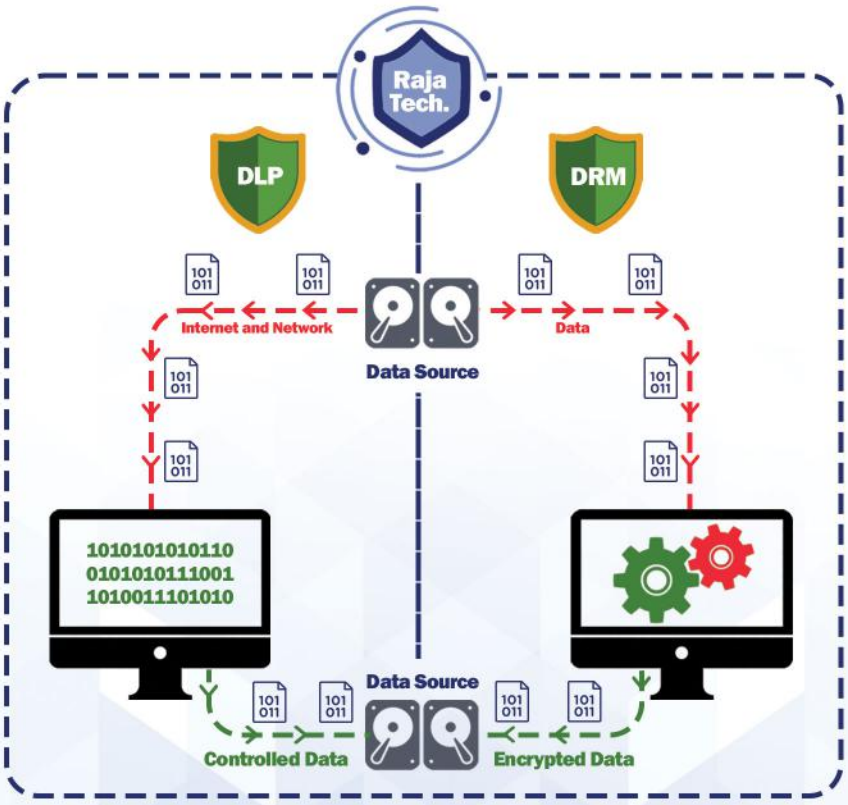
در رویکرد دوم اصل حفاظت مبتنی بر رمزنگاری اطلاعات است. در این روش اطلاعات از لحظه تولید، رمزنگاری شده و کاربر در صورت داشتن مجوز قادر به باز کردن و استفاده از آن می‌باشد. به این روش اصطلاحاً DRM(Digital Right Management گفته می‌شود. ابزار DRM برای هر گونه اطلاعات یا داده، می‌تواند بالاترین سطح امنیت را با توجه به فرایندهای یک سازمان یا شرکت ایجاد نماید. لازم به ذکر است کلیه فرایند رمزنگاری و رمزگشایی نامحسوس بوده و نیازی به دخالت کاربر نمی‌باشد.



ویژگی های سامانه RAJA-DLP

- سهولت در پیاده‌سازی، عملکرد شفاف و عدم تداخل در کسب‌وکار جاری سازمان و کاربر
- کنترل دسترسی به منابع براساس حقوق کاربر، شرایط سازمان و ضوابط مدون
- مدیریت فرآیند تولید، پردازش، انتقال و امحای دارایی‌های دیجیتالی سازمان
- امکان توسعه سفارشی قابلیت‌ها مطابق با نیاز هر سازمان
- کاهش مخاطرات ناشی از سرقت دارایی‌های سازمان
- اعطای حق مالکیت داده‌ها به سازمان به جای کاربر
- سلب مسئولیت حفاظت داده‌های سازمانی از کاربر
- امکان سیاست‌گذاری بر اساس گروه، رایانه، کاربر
- پشتیبانی از VDI , Thin Client , Domain , WorkGroup
- امنیت بالا در مواجهه دسترسی‌های غیرمجاز
- ارائه سرویس پشتیبانی کامل





کنترل اسناد

- رمزنگاری و رمزگشایی خودکار فایل‌ها با تعریف مسیر از پیش تعیین شده (HOT/COLD FOLDER)
- کنترل Clipboard و جلوگیری از عملکرد ابزارهای فیلم‌برداری و عکس‌برداری از صفحه نمایش
- رمزنگاری خروجی برنامه‌های کاربردی با استفاده از قابلیت Data Protection
- پشتیبانی از الگوریتم‌های رمزنگاری بومی/غیربومی با طول کلید مختلف
- رمزنگاری فایل‌های موجود بر روی رایانه بر اساس نوع آن‌ها

کنترل درگاه‌های سخت‌افزاری فیزیکی و مجازی

- تهیه لیست سیاه و سفید از سخت افزارهای مجاز و غیرمجاز جهت اتصال به رایانه
- تهیه خودکار فهرستی از دارایی های سخت افزاری رایانه ها و بروزرسانی آنها
- ثبت لیست سیستم عامل و مشخصات آن‌ها

کنترل ابزارهای جانبی

- امکان ردیابی اسناد چاپ شده با استفاده از Watermark
- کنترل دسترسی کاربر به چاپگر

کنترل شبکه و اینترنت

- امکان اعمال فیلترهای مختلف بر روی ویژگی های بسته های شبکه
- تعریف لیست سیاه و سفید برای آدرس های اینترنتی
- گزارش گیری از آدرس های اینترنتی مشاهده شده

مانیتورینگ

- تهیه گزارش از لیست نرم‌افزارها و سرویس‌های موجود در سیستم و تغییرات آنها
- تهیه گزارش از بروز رسانی‌های سیستم عامل و تغییرات آنها
- تهیه گزارش از لیست درایورها و تغییرات آن

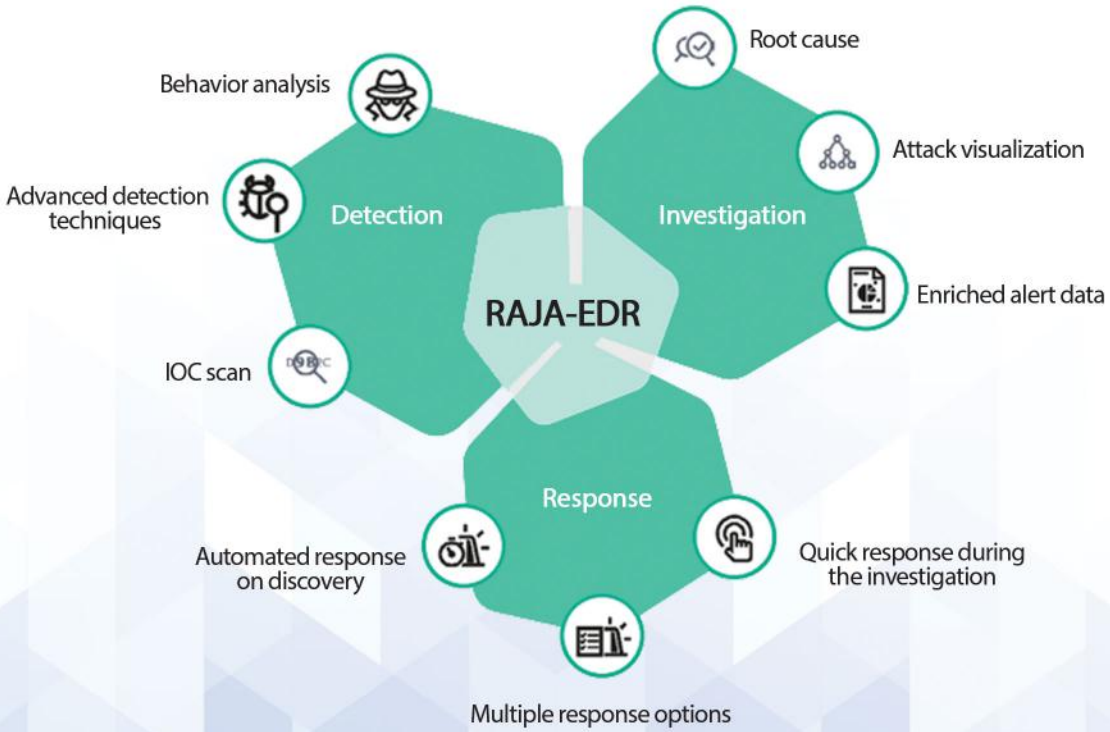
RAJA EDR

سامانه تشخیص و پاسخ به نقطه پایانی
Endpoint Detection and Response

در گذشته حملات و بدافزارها، محدود بوده و الگوی آنها توسط آنتی ویروس و دیواره آتش قابل تشخیص بود. با فراگیر شدن استفاده از فناوری اطلاعات و اهمیت آن، بر پیچیدگی و گسترش تهدیدات و آلودگی ها افزوده شد. به طوری که بر اساس ارزیابی های انجام شده توسط موسسات مطالعاتی نظیر گارتنر، ابزارهای فوق به تنهایی کارایی لازم را در مواجهه با حملات و بدافزارها ندارند.

دغدغه های فوق در کنار گسترش روزافزون استفاده از فناوری های جدید نظیر هوش مصنوعی باعث ظهور سامانه Endpoint Detection and Response (EDR) شد. این سامانه با تحلیل و شناسایی هر گونه آسیب پذیری، بدافزار یا فعالیت مشکوک در نقاط پایانی شبکه، اقدام به پاسخگویی و اعلام هشدار به مدیران سازمانی می کند. با توجه به بهره گیری از فناوری های جدید، سامانه فوق سازمان را درمقابل طیف وسیعی از تهدیدات و حملات پیشرفته سایبری محافظت می کند.

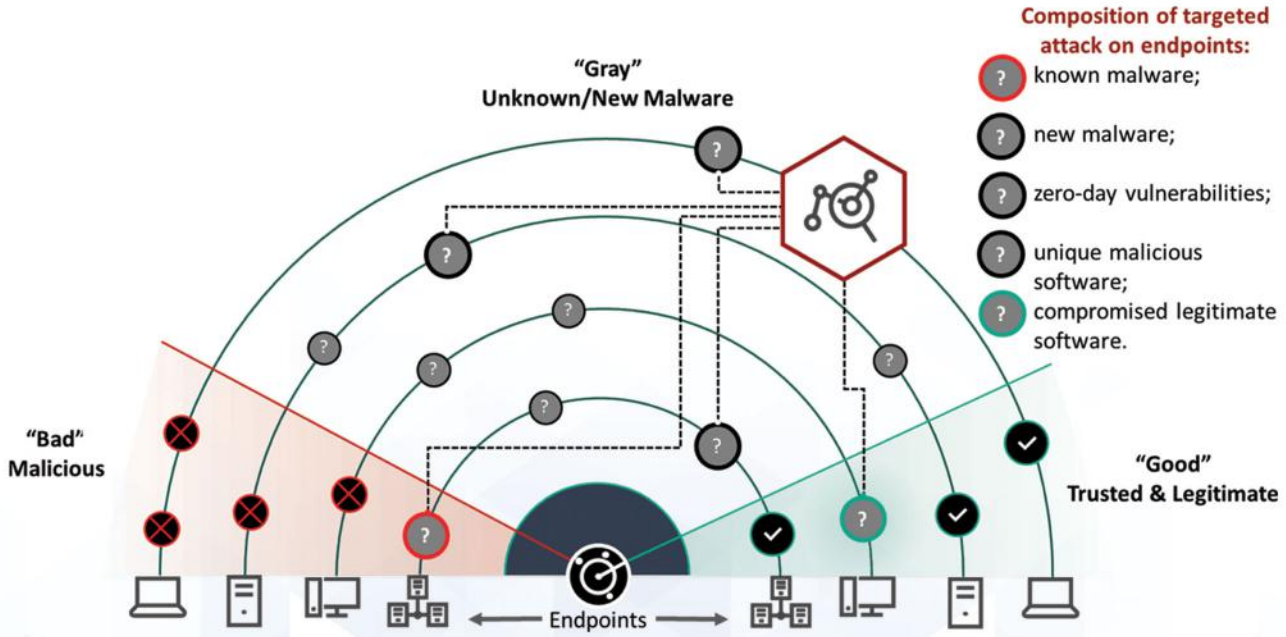
سامانه بومی EDR شرکت فناوری اطلاعات رجاء با هدف تأمین امنیت حداکثری در شبکه های سازمان و نقاط انتهایی آن طراحی و تولید شده است و در تعامل با سایر محصولات و تکنولوژی ها نظیر DLP، هر گونه ناسازگاری در سیاست امنیتی، فعالیت مشکوک سرویس ها و همچنین بدافزارها را کشف و خنثی می کند.



لزوم بهره‌گیری از RAJA-EDR

در EDR، یکپارچه‌سازی یکی از مهم‌ترین اولویت‌ها بوده و این سامانه با پوشش حجم وسیعی از نیازمندی‌های حوزه امنیت از قبیل مدیریت، کنترل و نظارت بر داده‌های سازمانی و رویدادها، تا حدود زیادی نیاز مدیران را پوشش می‌دهد. گزارش‌های خروجی این سامانه یکی از مهم‌ترین ابزارهای جمع آوری اطلاعات برای مرکز عملیات امنیت (SOC) بوده و کمک شایانی در تحلیل و جلوگیری از مخاطرات امنیتی می‌نماید.

با توجه به‌سرعت رشد و تغییرات در حوزه فناوری اطلاعات، نیازمندی سازمان‌ها نیز همواره رو به افزایش و تغییر می‌باشد، لذا بومی بودن این سامانه سبب تسریع در افزودن قابلیت‌های جدید و سازگاری با نیاز سازمان می‌شود.



در اینجا به ذکر برخی دلایل لزوم به کارگیری EDR پرداخته شده است:

- افزایش تعداد حملات به نقـاط انتـهایی شبکه؛ این در حالیـست که از انـواع فایـروال‌ها، آنـتی ویـروس و سـازوکار افزایش ضـریب امـنیت سـرویـس‌هـا و سـخت افزارها در سازمـان استفاده می‌شود اما باز هم مورد حمـلات جدی و گاهـا جبـران ناپـذیر قرار می گیرد. این موضـوع به قـدری مهـم است که ناکافی بـودن راه حل‌های پیـشین بـرای سازمان‌ها مسجل شده است.

- یکی دیگر از عوامل، پیشرفته‌تر شدن حملات سایبری است که غالباً این گونه حملات آسـان‌تر از نفوذ به شبکه است. این گونه حـملات از این لحاظ پیـچید گی به شکلی هستند که توسط راه حل‌های امنیتی گذشته معمولی قابل تشخیص نمی باشد یعنی جهت حمله از بدافزار استفاده نمی‌شود و تنها با آنالیز واکنش‌ها توسط EDR قابل شناسایی هستند.
- با استفاده از این راه کار سیاست‌ها به صورت خودکار جهت مقابله با حملات اعمال می‌شوند.
- تمام لاگ‌ها در یک سرور جمع آوری شده و امکان رسیدن به یک دید گاه عمیق در شبکه وجود دارد.
- مدیریت فرآیند تولید، پردازش، انتقال و امحای دارایی‌های دیجیتالی در سازمان انجام می‌شود.
- کنترل دسترسی به منابع براساس حقوق کاربر، شرایط سازمان و ضوابط مدون اعمال می‌شود.
- هزینه و مخاطرات ناشی از سرقت اطلاعات و دارایی‌های سازمان کاهش می‌یابد.
- مسئولیت حفاظت داده‌های سازمانی از کاربر سلب می‌شود.
- هزینه کلی در مدیریت IT و امنیت شبکه کاهش می‌یابد.
- حق مالکیت داده‌ها به سازمان اعطا می‌شود.

اجزای تشکیل دهنده RAJA-EDR

Detection (شناسایی مخاطرات و تهدیدات)

بخش های مختلفی در سیستم برای یافتن و تحلیل مخاطرات وجود دارد:

- NSM (Network Security Management): جمع آوری، تجزیه و تحلیل نشانه ها و هشدارها در سطح ترافیک شبکه برای جلوگیری، شناسـایی و پاسخ به حـملات ونفـوذهای رایج شبکه بر عهـده این بخش می باشد.
- IDS (سیستم تشخیص نفوذ): وظیفه شناسایی فعالیت بد افزارها، ناهنجاری ها و Rootkitها در سـطح ترافیک شبکه بر عهده دارد.

- Log Data Analysis (تجزیه و تحلیل اطلاعات گزارشات): گزارشات ارسال شده توسط سنسورها، توسط سرور پردازش شده و مواردی نظیر خطای برنامه یا سیستم عامل، تنظیمات و پیکربندی غلط، فعالیت های مخرب یا موفقیت آمیز، نقض خط مشی و سایر موارد امنیتی و عملیاتی اطلاع داده می شود.
- File integrity Monitoring: تغییرات بر روی فایل های موجود بر روی یک سرور یا کلاینت ومشخصه های آن را نظارت کرده و گزارش می کند.
- Vulnerability Detection (شناسایی آسیب پذیری ها): با استفاده از یک مرجع (CVE) آسیب پذیری های موجود بر روی سیستم را شناسایی کرده و به مدیر شبکه کمک می کند قبل از وقوع حمله نسبت به رفع آسیب پذیری اقدام کند.
- Configuration Assessment (صحت سنجی پیکربندی امنیتی کاربران نهایی): این بخش استانداردها و شاخص‌های ایمنی را مانیتور می کند و پایانه یا نرم افزارهای آسیب پذیر را جهت رفع آسیب‌پذیری معرفی می کند.
- Security Analytics (آنالیز امنیتی): از بخش های مهم سامانه بوده و وظیفه آن پردازش گزارشات جهت کشف هر گونه فعالیت مخرب، بدافزار و ... می باشد و مکانیزم آن به شرح ذیل می باشد:
  - آنالیز رفتاری: با تجزیه و تحلیل رفتار کاربر، سیستم عامل و برنامه های کاربردی، هر گونه موارد غیرعادی را گزارش می کند.
  - نظارت و آنالیز شبکه: کلیه فعالیت های کاربران نهایی و برنامه های کاربردی را در سطح شبکه را تحلیل و بررسی می کند.
  - هماهنگ سازی، خودکار سازی و پاسخ امنیتی (SOAR): تکنولوژی است که از طریق آن می‌توان متوجه فرایند رخدادهای امنیتی شد و مطابق آن تصمیم گیری کرد.
  - جرم شناسی: این راهکار با بررسی الگوی حملات در گذشته و داده های موجود، احتمال وقوع مخاطرات و حمله را گزارش می کند.

Detection (شناسایی مخاطرات و تهدیدات)

سامانه RAJA-EDR پس از تشخیص هر نوع ناهنجاری در سطح شبکه، مدیران سازمان را با استفاده از پیامک و Email و داشبوردهای اختصاصی درجریان رخداد قرار می دهد. هم چنین در تعامل با سایر ابزار های امنیتی نظیر DLP و SOC و ... سعی در خنثی سازی حمله می کند. همچنین از دسترسی عامل خطر به فایل ها و منابع جلوگیری می کند.

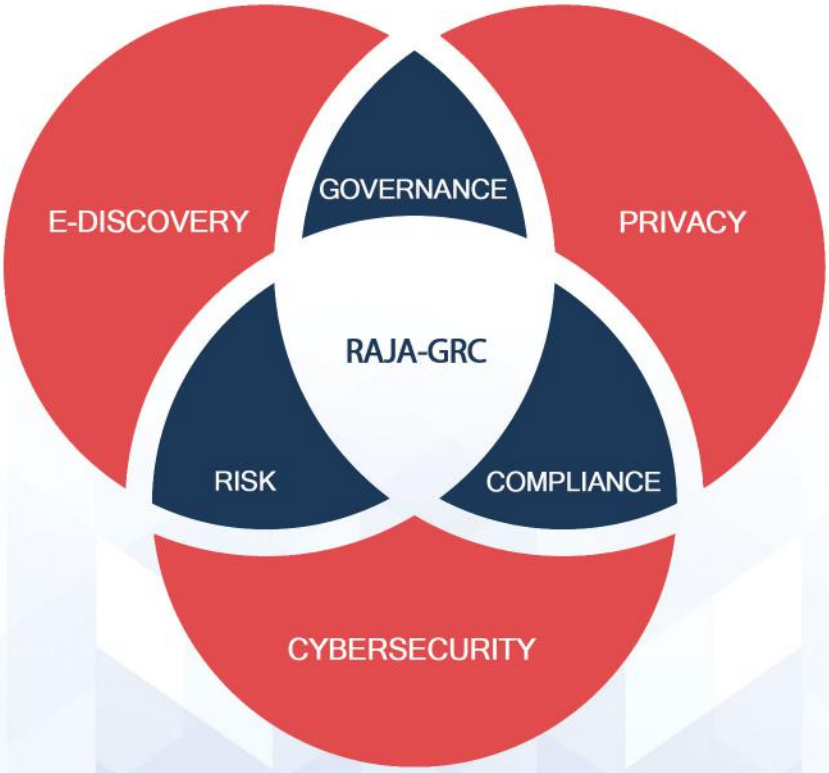
RAJA GRC

سامانه مدیریت و کنترل ریسک

Governance,Risk management & Compliance

در چند سال اخیر، سازمان‌ها و بانک ها با افزایش جدی در ریسک‌های عملیاتی و کسب‌وکار مواجه شده اند. همچنین چگونگی مدیریت و راهبری فعالیت‌های سازمان و بانک‌ها، همراستا با نیازهای ذینفعان، مقررات و الزامات داخلی و بین‌المللی، بازار و ریسک‌های کسب و کار و فرهنگ سازمان به عنوان مهمترین چالش‌های پیش رو در همه صنایع و خصوصا صنعت بانکی مطرح گردیده است. به منظور برطرف نمودن چالش‌های مذکور، در چند سال اخیر در سطح بین‌المللی استقرار مفهوم GRC مورد توجه جدی قرار گرفته است.

استقرار RAJA-GRC تمامی فعالیت‌های سازمان در سه حوزه حاکمیت، مدیریت ریسک و انطباق با الزامات را پوشش می‌دهد. فرایندهای مرتبط با حاکمیت(Governance)، ساختاری برای راهبری و اعمال اختیارات لازم در راستای حصول اهداف استراتژیک سازمان ارائه می‌نماید؛ مدیریت ریسک، شامل فرایندهای شناسایی، تحلیل، ارزیابی و کنترل ریسک می‌باشد؛ و انطباق با الزامات به معنای استقرار فرایندهای لازم در اطمینان از اجرای قوانین و استانداردهای داخلی و خارجی است که برای کسب‌وکار مورد نظر تعریف شده‌اند.



اجـرای مدل یکـپارچه GRC ، نیـازمند تعریف و ایجـاد ارتبـاطات واضح و بدون ابـهام میان نقـش‌ها و مسـئولیت‌ها در این فـرایندها می باشد. همچنین برای پیشبرد این فرایندهای در هم آمیخته لازم اسـت تا یک نقطه مرجع در سـازمان تعیـین و مـنابع اطـلاعاتی مشترک ایـجاد شوند. برای استقرار GRC ، بررسـی و مطالعه چارچوب‌ها و اسـتانداردهای این حوزه ضروری اسـت. با پیاده‌سـازی صحیح ، انتظار می‌رود که تصمیمات جامع‌تر، مبتنی بر ریسک و به منظور کاهش هزینه‌ها و افـزایش بهره‌وری سازمان‌ها و بانک‌ها قابل حصول باشد.

شرکت فناوری اطـلاعات رجـاء با تحـقیق و توسعه سامـانه بومی RAJA-GRC طی پنـج سال اخیر مطابق با مـدل بلوغ و الزامـات طرح امـن سازی افـتا ، اسـتانداردهای C2M2, ISMS, BCP/BCM و سـایر اسـتانداردها و سیاسـتنامه های داخلی سـازمان ها ، گـامی موثر در مـدیریت و انـطباق ریسک در بخش دولتی و خصوصی برداشته است.

RAJA-GRC

راه حلی ساده برای یکپارچه سازی روند ممـیزی و هم سـطح نمودن فرآیند های محـاسـبه انطباق سنـجی ها و مخـاطرات حوزه فناوری بالاخـص حـوزه بـانکداری بـوده کـه با خود کارسازی روند ممیزی در سطح کارشناسـان فـنی ، قادر به برآورد دوره ای از میزان انطباقـات با چـک لیسـتهای فـنی تدوین شـده از تجربـیات فـنی و دانـش روز امـن سـازی خواهد بود.

قابلیت های کلیدی نرم افزار

نرم‌افزار RAJA-GRC با بکارگیری جدیدترین تکنولوژی های روز جهانی در بستر تحت وب ارائه گردیده که به واسطه این امر در هر زمان بدون نیاز به نرم افزار واسط ، قابل دسترس خواهد بود. علاوه بر آن میتوان به قابلیت های کلیدی زیر نیز اشاره نمود:

- جمع آوری تمامی دارایی های موجود در مجموعه به صورت سلسله مراتبی و قابلیت اتصال API
- اعلانات امنیتی مندرج در منابع معتبر به صورت دوره ای یا همزمان(Security Advisory)
- تعریف زیر مجموعه های سازمان (سازمان ، بخش ، پست سازمانی ، کاربر)
- ظاهر زیبا و کاربر پسند با قابلیت نمایش در صفحه نمایش های مختلف
- تعریف دانشنامه برای محاسبات انطباق سنجی ، ریسک ، سطح و بلوغ
- داشبورد مدیریتی جهت مشاهده کلی وضعیت سازمان در لحظه
- گزارشگیری و خروجی فایل های Word , Excel , PDF
- تعیین گردش کار زیر پروژه های امن سازی
- قابلیت ارسال Log برروی SIEM در مراکز SOC
- احراز هویت با اکتیو دایرکتوری
- محاسبات ریسک پرسنلی
- و...

خدمات افتا

ISO 10002:2014

ISO 9001:2015

حفاظت از زیرساخت های حیاتی ملی برای ایجاد جامعه‌ای امن، ایمن و مقاوم در قبال حملات سایبری و سایر مخاطرات طبیعی و انسانی، امری ضروری است. در این راستا زیرساخت‌های حیاتی نیازمند سازوکارهایی برای حفظ محرمانگی، یکپارچگی و دسترس‌پذیری دارایی های خود می باشند. با توجه به نوپایی مفهوم امنیت فضای تولید و تبادل اطلاعات و با عنایت به میزان تأثیر آن بر امنیت ملی کشور، پرداختن به این موضوع و نهادینه سازی آن به‌عنوان یک ضرورت و اولویت تلقی می شود.

- **مخاطبین طرح**

مخاطب اصلی این طرح کلیه زیرساخت ها و دستگاه های دارای اطلاعات مهم بوده و سایرسازمان ها نیز می توانندبه فراخور نیاز خود از آن استفاده نمایند.

- **خلاصه مدیریتی طرح**

هدف از این طرح، تأمین امنیت فضای تولید و تبادل اطلاعات سازمان و جلوگیری از بروز اختلال در ارائه سرویس های حیاتی آن است . در این طرح الزاماتی برای ایجاد، پیاده‌سازی، نگهداری و بهبود مستمر امنیت اطلاعات درحوزه های زیرساختی ارائه‌شده است.

- **الزامات طرح امن سازی**

این الزامات، کنترل‌های حداقلی به‌منظور کاهش مخاطرات دارای اولویت درزیرساخت‌ها است و هدف از این بخش جهت‌دهی راهبردی به فعالیت‌های ملی در حوزه امنیت سایبری زیرساخت‌ها و ارائه یک نقشه راه، برای توسعه هم‌زمان امنیت سایبری در بخش‌های مختلف کشور در سال‌های پیش رو است. سطح بلوغ امنیتی مطلوب سازمان در هر یک از الزامات این طرح، می‌تواند بر اساس سطح قابل‌پذیرش مخاطرات سازمان تعیین گردیده و این سطح در برنامه عملیاتی سازمان تصریح و به تأیید مرکز افتا خواهد رسید.

شرکت فناوری اطلاعات رجاء با اخذ مجوز امن سازی زیرساخت از مرکز افتا و با تکیه بر دانش و تجربه خود ، سازمان ها را در جهت استقرار طرح امن سازی و پیاده سازی الزامات و استانداردها یاری می کند.

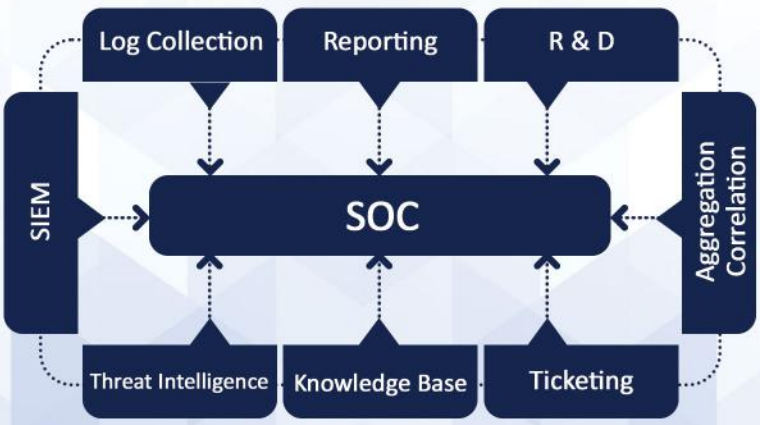
مـرکـز عملیـات امنیـت
Security Operations Center

مرکز عمـلیات امـنیت مجموعـه‌ای است که با پـایش تمامی فعالیـت‌های ورود و خروج شـبکه، رخـدادهای امنیتی را جمـع آوری و تحـلـیل کرده و در صورت برخـورد با مخاطـرات امنـیتی با تولـید هشـدارهای امـنیتی و انـجام اقـدامات مناسب مانع از به خطر افتادن امنیت سازمان می‌شود.

علت نیاز سازمان ها به SOC

امـروزه با افـزایـش قـدرت تهدیدات، حمـلات امنیـتی و هکرها، برقراری امنیـت در سازمان‌ها و شرکت ها یک امـر مـهم و حیاتـی محـسـوب می‌شود. یکـی از موثرتـرین و سـریـع‌ترین راه‌هـای تشخیص مخاطرات امنـیتی، بررسـی گـزارشـات و رخـدادها در سـرورها و تجهیزات سازمان ها است که توسط مرکز SOC انجام می‌شـود. مرکز عملیات امنیت می‌تـواند حملات درحـال انجـام را شناسایی کـرده و با اقـدامات مناسب، آنها را خنثـی کند.

از این رو شـرکت فناوری اطـلاعات رجاء پیـاده‌سـازی مرکز عمـلیات امنیـت را علاوه بر بانک‌ها و سازمان‌های بزرگ، به سـازمان‌ها و تجارت‌های کوچک نیز توصیه می کند.

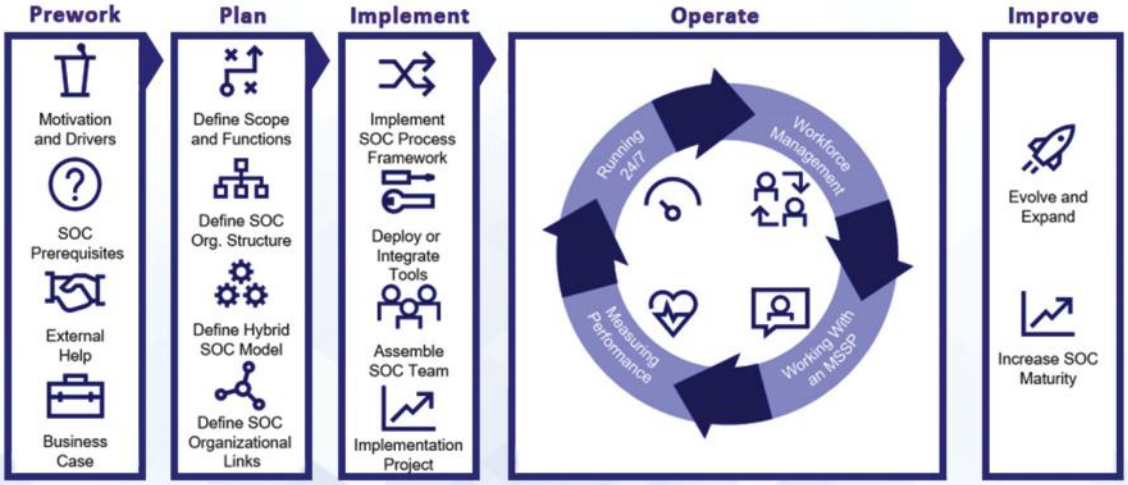


مزایای استفاده از SOC

- نقطه تماس متمرکز برای رسیدگی به مشکلات امنیتی کاربران و راهبران شبکه
- جمع آوری و آنالیز ترافیک شبکه و تولید گزارشات امنیتی در سطوح مختلف
- پایش امنیتی تجهیزات، شبکه‌های ارتباطی و رایانه‌ها، به صورت ۲۴/۷
- شناسایی تهدیدات و حملات امنیتی در کمترین زمان ممکن
- پاسخ‌دهی به مشکلات و رخدادهای امنیتی
- کاهش هزینه‌های مدیریت امنیت شبکه
- مدیریت و پایش لحظه ای تهدیدات

وظایف اصلی SOC

- مدیریت رخدادها به وسیله راهکارهای امنیتی
- محافظت فعالانه و شبانه‌روزی از شبکه
- آگاهی بلادرنگ از تهدیدات امنیتی
- مدیریت آسیب‌پذیری‌ها



ارزیابی امنیتی و تست نفوذ

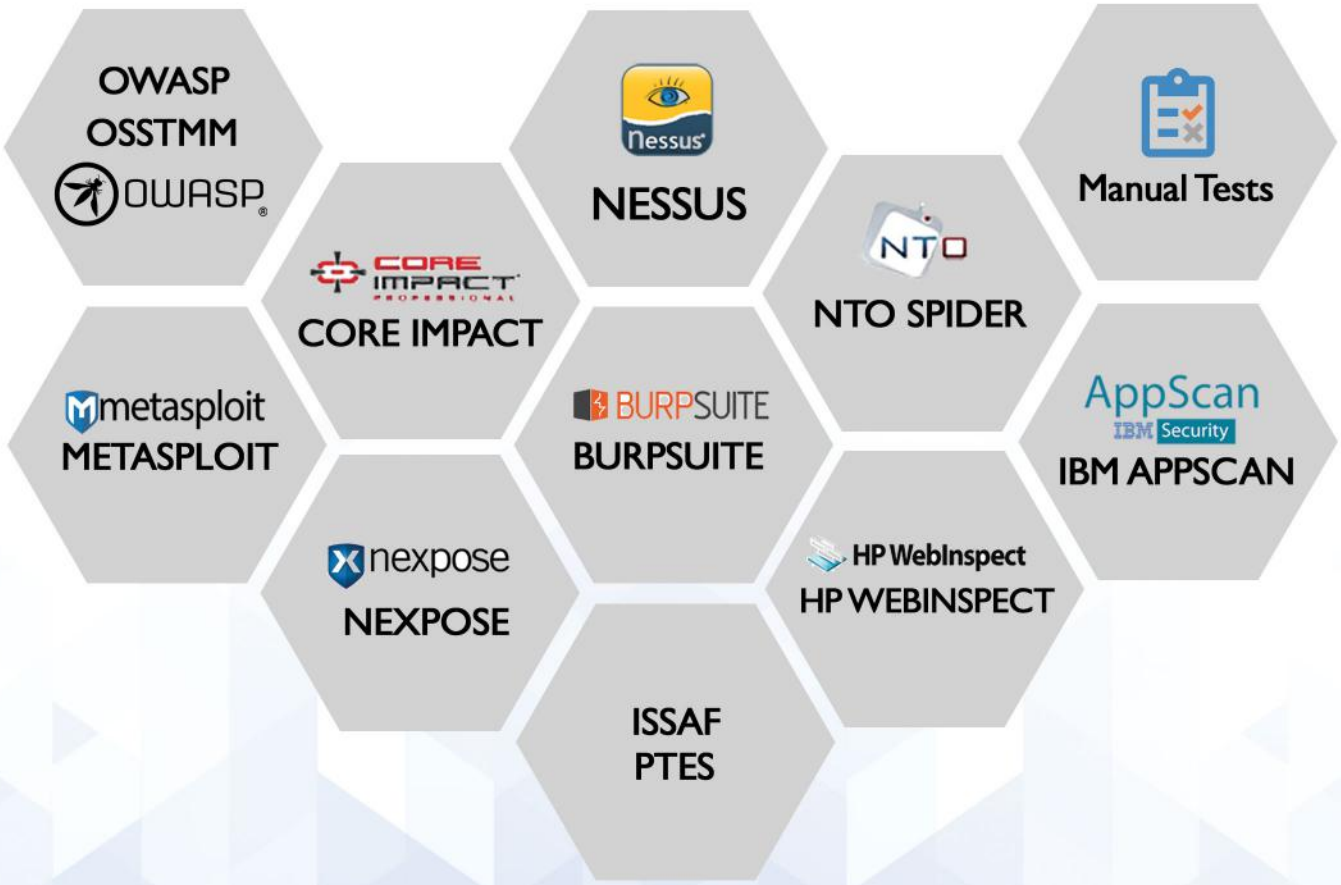
Security Assessment & Penetration Testing

با گرایش روزافزون سازمان ها و شرکت ها به استفاده از فضای تبادل اطلاعات برای پیشبرد اهداف و مأموریت خود، لازم است امنیت آن بیش از گذشته مورد توجه قرار گیرد. بستر تبادل اطلاعات در معرض چالش‌ها ، آسیب‌ها و تهدیدهای گوناگونی نظیر تخریب بانک‌های اطلاعاتی، حملات مختل کننده‌ی خدمات، شنود، خرابکاری، نقض حریم خصوصی و ... قرار دارد و نپرداختن یا رویکرد نادرست به امنیت آن، خسارت جبران‌ناپذیر مادی و معنوی به بارمی آورد.

ارزیابی امنیتی یا Penetration Testing، یک عمل مجاز، برنامه ریزی شده و سیستماتیک برای ارزیابی امنیت یک سازمان (شامل تجهیزات فعال و غیرفعال شبکه، سرویس‌دهنده‌ها، سرویس گیرنده‌ها، برنامه‌های کاربردی و ...) است که از طریق شبیه‌سازی حمله یک هکر یا نفوذ گر صورت می گیرد. کلیه متخصصان امنیت در حوزه فناوری اطلاعات بر این باورند که تنها روش اطمینان یافتن از امن بودن شبکه‌های رایانه‌ای و زیر ساخت‌های ارتباطی و سامانه‌های اینترنتی، انجام عملیات ارزیابی امنیتی (آزمون نفوذپذیری) است.

ارزیابی امنیتی یکی از فعالیت‌های اصلی شرکت فناوری اطلاعات رجاءِ بوده و چند تیم با نام تیم ارزیابی در واحد فنی و عملیات این شرکت وجود دارد. سه دسته فعالیت توسط اعضای تیم ارزیابی انجام می‌شود.

- ارزیابی زیرساخت: این فعالیت شامل بررسی تنظیمات سخت‌افزار، نرم افزار، مسیریاب‌ها، Firewallها، Serverها و سیستم‌های Desktop برای حصول اطمینان از این است که این تنظیمات مطابق با سیاست‌های سازمان و تنظیمات استاندارد صورت گرفته است.
- تست نفوذ: در این فعالیت امنیت یک سازمان با انجام حملات طراحی شده بر روی سیستم‌ها و شبکه به منظور شناخت نقاط آسیب‌پذیر بررسی و ارزیابی می‌شود. قبل از انجام تست نفوذ لازم است موافقت مدیریت سازمان حاصل شده باشد زیرا ممکن است انجام برخی از این تست‌ها توسط سازمان منع شده باشد.به صورت White-Box , Gray-Box , Black-Box در کلیه سطوح مانند : Web Application/ Mobile Application /Network Layers /Core Systems /Hypervisors /Industrial Infrastructure
- پویش: در این فعالیت از ابزارهای پویش آسیب‌پذیری‌ها موجود در شرکت استفاده می‌شود تا سیستم‌ها و یا شبکه‌های آلوده یا آسیب‌پذیر تشخیص داده شوند.



امنیت زیرساخت های صنعتی

TÜV INTER CERT SAAR
ISO 10002:2014

TÜV INTER CERT SAAR
ISO 9001:2015

RAJA IDS

سامانه تشخیص نفوذ صنعتی

Industrial Intrusion Detection System

ساختار مورد استفاده در شبکه های صنعتی یا برق و پروتکل های رایج آنها با شبکه های کامپیوتری متفاوت است. کشف حملات نیاز به IDS هایی دارد که علاوه بر قابلیت پردازش بسته های این پروتکل ها، مشخصات خاص شبکه های صنعتی یا برق و دستگاه های خاص آنها را در نظر بگیرند. توسعه این تکنولوژی نیاز به تحقیقات بنیادی و تیم بین رشته ای دارد. تاکنون دو نوع IDS برای شبکه های صنعتی و برق که ماحصل بیش از پنج سال تحقیق و توسعه می‌باشد توسط شرکت فناوری اطلاعات رجاء تولید شده است که در ساختارهای شبیه سازی آزمایشگاه آپا دانشگاه تربیت مدرس در فاز عملیاتی می باشد.

مشخصات فنی:

- تکنولوژی غیر فعال (Passive)
- طراحی برای پروتکل مختلف
- پشتیبانی از پروتکل‌های صنعتی مانند EtherCat , S7 , IEC 104 , DNP3
- پشتیبانی از پروتکل‌های ارتباطی مانند OPC
- امکان پشتیبانی از پروتکل‌های میترینگ مانند DLMS/COSEM
- سیستم مدیریت لاگ مرکزی با توانایی ارسال و مدیریت هشدارها

امنیت سایبری در زیرساخت‌های حیاتی و حساس

نظارت و کنترل زیرساخت‌های حساس و حیاتی با ظهور سیستم‌های کنترل صنعتی، توسعه و پیشرفت چشمگیری داشته‌اند. هرچند ساختار و عملکرد سیستم‌های کنترلی، پیشرفت شایان توجهی داشته، اما موضوع امنیت سایبری در آن‌ها چندان مدنظر قرار نگرفته و این زیرساخت‌ها را در معرض تهدید قرار داده است. با توجه به عدم ارتقای امنیت در سیستم‌های کنترل صنعتی همگام با توسعه و پیشرفت آن‌ها، این امکان برای مهاجمین سایبری فراهم گردیده تا با استفاده از ساده‌ترین روش‌ها بتوانند خسارات جبران ناپذیری به زیرساخت‌های کشور وارد کنند. شرکت فناوری اطلاعات رجاء با توجه به احساس نیاز کشور در این حوزه راهکار جامع و یکپارچه امنیت سایبری در زیرساخت‌های صنعتی را تدوین نموده است که در ادامه به معرفی آن می‌پردازیم.

راهکار جامع و یکپارچه امنیت سایبری در زیرساخت‌های صنعتی

راهکار جامع و یکپارچـه امنیت زیرساخت‌های صنعتی با اتکا به استانداردها و بهترین روش های معرفی شده در دنیا، در نظر گرفتن شرایط بومـی کشـور و هم چـنین عـدم تحمـیل هـزینه هنگـفت به زیرساخـت‌های کشـــور طراحی شـده اسـت. راهـکار مذکور با اتکا به مجموعه‌ای از خـدمات و محصولات ارائـه شده توسط شـرکت فناوری اطلاعات رجاء در حوزه امنـیت سیستم‌های کنترل صنعتی، توانایی مرتفع نمودن تهدیدات بالقوه و بالفعل در این حوزه را دارد.

گام های راهکار جامع و یکپارچه سازی امنیت سایبری

- **شناسایی و ارزیابی**

مرحله اول مربوط به شنـاسایی و ارزیابی واحد صنعتی به منـظور یافتن نقاط ضـــعف امنیتی می‌باشد و شامل موارد زیر است:

- شناسایی آسیب‌پذیری‌ها و ارزیابی پیکربندی سیستم‌ها شامل سرورها، ایستگاه‌های کاری، ایستگاه‌های مهندسی، تجهیزات صنعتی مانند PLCها، RTUها، و...
- ممیزی تطابق با طرح ها و استانداردهای شاخص در حوزه امنیت سیستم‌های صنعتی و زیرساخت‌های حیاتی
- شناسایی فرآیندهای عملیاتی ، دارایی‌ها، شبکه و ارتباطات واحد صنعتی
- ارزیابی معماری شبکه و پیکربندی تجهیزات زیرساخت شبکه صنعتی
- تست نفوذ به شبکه صنعتی (تحت شرایط خاص)
- ارزیابی مخاطرات

• طراحی و امن‌سازی

در بخش امن‌سازی با توجه به آسیب‌پذیری‌ها و نقاط ضعف شناسایی شده در فاز ارزیابی، راهکار امنیتی بر اساس مفهوم دفاع در عمق جهت رفع آسیب‌پذیری‌های شناسایی شده و امن‌سازی ارائه و پیاده‌سازی می‌شود. بر این اساس خدمات زیر در این بخش ارائه می‌شود:

- ارائه راهکار جهت مطابقت با استانداردها و طرح های شاخص در حوزه امنیت سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی
- استقرار راهکارهای Endpoint Security در ایستگاه‌های کاری، سرورها، و ایستگاه‌های مهندسی جهت مقابله با بدافزار
- رفع آسیب‌پذیری‌های شناسایی شده در شبکه صنعتی در مرحله ارزیابی از طریق اعمال وصله
- امن‌سازی پیکربندی سیستم‌ها شامل ایستگاه‌های کاری، سرورها، ایستگاه‌های مهندسی و...
- اصلاح معماری شبکه صنعتی بر اساس مفهوم بخش بندی شبکه و تعریف مناطق امنیتی
- آموزش و آگاهی رسانی در حوزه امنیت شبکه های صنعتی
- امن سازی و مقاوم‌سازی پیکربندی تجهیزات زیرساخت
- استقرار راهکارهای مدیریت تغییرات در شبکه صنعتی

در این بخش می توان از محصولات بومی زیر استفاده کرد:

- سامانه تشخیص نفوذ صنعتی RAJA-IIDS
- سامانه مدیریت دسترسی های ویژه RAJA-PAM
- سامانه تحلیل نقاط پایانی RAJA-EDR
- سامانه پیشگیری از نشت داده RAJA-DLP

• تشخیص

از آن جایی که آگاهی از وضعیت شبکه و تشخیص رویدادهای امنیتی در زمان مناسب تأثیر زیادی در انتخاب پاسخ به شکل موثر و بهینه و حداقل ساختن اثرات منفی آن دارد، می توان از سیستم‌های تشخیص نفوذ مبتنی بر شبکه، سیستم‌های تشخیص نفوذ مبتنی بر میزبان ها و در سطوح بالاتر از سامانه مدیریت اطلاعات و رخدادهای امنیتی(SIEM) بهره برد.

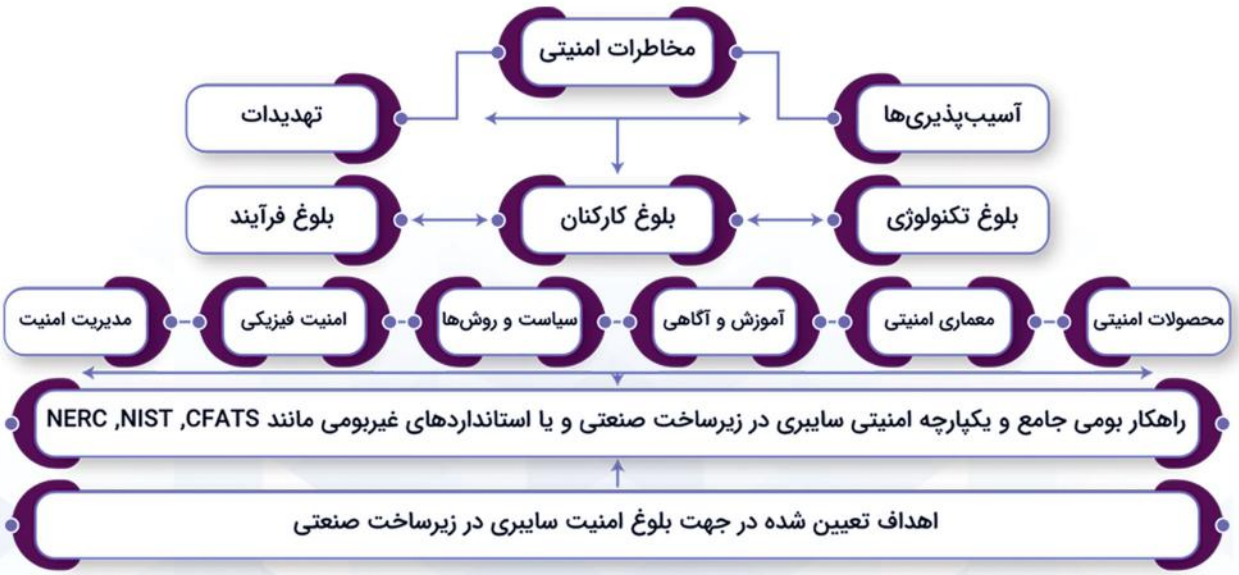
بعد از پیاده‌سازی تجهیزات تشخیصی، با اتکا به استقرار سامانه مدیریت امنیت اطلاعات و رخدادهای صنعتی IT به عنوان قلب تپنده مرکز عملیات امنیت صنعتی می توان بسیاری از موارد مربوط به امنیت دارایی‌های زیرساخت صنعتی را پوشش داد.

پاسخگویی به رخدادها

با اینکه پس از اجرای فازهای ارزیابی و امن‌سازی سطح حمله سیستم به شـدت محدود می‌شود اما به دلیل ماهـیت متغیر تهدیدات هیچ گاه نمی توان احتمال روی دادن حمـلات سایـبری را به صفر رساند. پیاده‌سازی فاز تشخیص ، امکان شناسایی رخدادهای احتمالی را فراهم می کند و در کنار آن وجود قابلیت پاسخ به رخـدادهای امنـیتی و بازیابی سیـستم از اهـمیت بالایی برخـوردار است. دراین حوزه خدمات زیر توسط شرکت فناوری اطلاعات رجاءِ ارائه می‌شود:

- ارائه طرح های پاسخ به رخدادهای امنیتی بر اساس استانداردهای مدیریت رخداد جهت تضمین استمرار کسب و کار و بازیابی پس از بحران
- رسیدگی به رخدادهای امنیتی شامل واکنش در محل، خدمات جرم‌شناسی و پی جویی حملات و رخدادها، و ترمیم و بازیابی سیستم‌ها
- تحلیل و بررسی مصنوعات و ابزارهای مورد استفاده در حملات و فعالیت های غیرمجاز همچون بدافزارها
- بلوغ امنیت سایبری مبتنی بر اهداف تعیین‌شده و ایجاد چرخه حیات
- ارائه طرح تاب‌آوری سایبری و ارزیابی آن در زیرساخت صنعتی

بعد از پیاده‌سازی کامل راهکـار جامـع و یکپارچه امـــنیت زیرساخت‌های صنـعتی که متشکل از مجموعـه‌ای از خدمات و محصولات بومی تولـید شده توسـط شرکت فناوری اطلاعات رجاءِ است، اهداف بلوغ امنیت در زیرساخت تعیین خواهد شد و معماری امنـیت پیاده‌سـازی شده مبـتنی بر راهـکار جامع سعی به گـذراندن مراحل بلوغ خود خواهد کرد. بعد از گذراندن هدف اول بلوغ، اهـداف بعدی مشخص خواهد شد و این چرخه بطور متوالی درجهت بهبود و ارتقای امنیت سایبری در زیرساخت مدنظر تکرار خواهد شد.



راهکارهای بانکی

ISO 10002:2014

ISO 9001:2015

طراحی و توسعه نرم‌افزار سفارش مشتری

Software Designing & Development

شرکت دانش بنیان فناوری اطلاعات رجاء با داشتن دانش فنی و متخصصین لازم در حوزه تحلیل و مدل سازی فرآیندهای سازمانی و با تکیه بر خط تولید نرم افزار خود (SLP) شامل واحدهای طراحی، معماری نرم افزار، برنامه نویسی و تست نرم افزار آمادگی دارد براساس فرآیندهای اختصاصی سازمان ها و با لحاظ کردن اهداف و استراتژی های آن ها، نرم افزارسفارشی مورد نیاز سازمان ها را طراحی و پیاده سازی نماید.

متخصصین شرکت مطابق با استانداردهای مهندسی نرم افزار و الگوهای بین المللی که براساس فرهنگ کسب‌و کار ایرانی بومی سازی شده است، ابتدا فرآیندها و دستورالعمل های سازمان را شناسایی و تحلیل کرده (As is) و پس از مقایسه با روش های جهانی و داخلی (Best Practice)، فرآیندهای بهینه سازی شده مطلوب (To be) را ارائه می کنند.

این شرکت موفق به اخذ پروانه تولید صنعتی نرم افزار از وزارت صمت، برای تولید نرم افزار در مقیاس بزرگ (Enterprise) شده است.

مشاوره پروژه‌های نرم‌افزاری در سطح ملی

National IT Projects Consultent

شرکت فناوری اطلاعات رجاء ارائه دهنده مشاوره IT به سازمان ها و شرکت ها در حوزه های مختلف با ده سال سابقه فعالیت می باشد. شاخص پروژه های انجام شده در سطح ملی، مشاوره و نظارت در طرح ادغام پنج بانک کشور در بانک سپه و مهاجرت به بانکداری نوین الکترونیکی می باشد. سایر خدمات مشاوره ای این شرکت به شرح ذیل می باشد:

- دسترس پذیری (در حوزه استانداردهای دسترس پذیری الکترونیکی، شرکت رجاء مفتخر به ارائه خدمات مشاوره در این حوزه به پنج بانک و سه شرکت بیمه ای در کشور می باشد.)
- خدمات مشاوره 5G در چند سال اخیر رشد ترافیک داده به میزان چند صد برابر، افزایش تعداد دستگاه‌ها، تجهیزات متصل به شبکه‌های بی‌سیم به میزان چند ده برابر و متنوع شدن سرویس‌های مورد تقاضای کاربران، توسعه شبکه‌های فعلی را فراتر از نسل چهار و یا همان شبکه‌های نسل پنجم 5G مطرح می‌سازد. در همین راستا، شرکت فناوری اطلاعات رجاء خدمات مشاوره ای خود را به منظور بررسی نسل پنجم شبکه ارتباطی از منظر فنی و اقتصادی راه اندازی نموده است.
- تحول دیجیتال (در سال های اخیر تحول دیجیتال در سازمان ها و شرکت‌های بزرگ گسترش یافته است و در جهت یکپارچه سازی تمامی فعالیت های سازمان، تحول دیجیتال به کار گرفته شده است. در همین راستا، شرکت فناوری اطلاعات رجاء خدمات مشاوره ای خود را در راستای ایجاد تحول دیجیتال در سازمان ها ارائه می دهد)

توسعه سامانه های دولت الکترونیک

Development of E-government & E-services

شرکت رجاء، با توجه به تجربیات خود در راه اندازی بیش از یکصد سرویس الکترونیکی در پنج سال گذشته، در حوزه ارائه خدمات مشاوره دولت الکترونیک نیز فعال می باشد و در این زمینه به سازمان ها و نهادهایی مانند کمیسیون اجتماعی و دولت الکترونیک، سازمان فناوری اطلاعات، نهاد ریاست جمهوری، معاونت توسعه مدیریت سابق، وزارت خانه ها و... خدمات مشاوره در سطوح ملی و سازمانی ارائه نموده است.

همچنین با اخذ تأمین کنندگی سرویس برای دفاتر پیشخوان، از سال ۱۳۹۹ تاکنون خدمات بسیاری از دستگاه های دولتی را بر بستر GSB ارائه می نماید.

راهکار جامع آنتی فیشینگ بانکی

Comprehensive Banking Anti-phishing Solution

راهکار یکپارچه متشکل از هفت ماژول با کمک تکنیک‌های مختلف اقدام به تشخیص سایت‌های فیشینگ می نماید. هر کدام از تکنیک‌های موجود در قالب یک ماژول در این راهکار پیاده سازی شده است. به طور کلی راهکارهای تشخیص صفحات فیشینگ به عنوان راهکارهای امنیتی خارج از دامنه سازمانی بانک تعریف می‌شوند. به عبارت دیگر با کنترل‌های امنیتی مستقر در داخل سازمان قابل تشخیص نمی‌باشند. لذا پویش فضای کسب کار سازمانی در بیرون سازمان برای این منظور هدف گذاری می‌شود.

برای تشخیص صفحات فیشینگ بانکی باید از پویش خودکار و دائم سه منبع اطلاعاتی بهره‌مند شد. این منابع عبارتند از: شبکه‌های اجتماعی، صفحات وب و برنامک‌های موبایلی. نظر به پیچیدگی پویش کامل این منابع، یک راه‌ار موثر باید پایش موثر و کارا را در دستور کار قرار دهد. لذا با توجه به تجربه شرکت رجاء در حوزه رصد رخدادهای سایبری در نظام بانکی، ماژول‌های زیر برای راه‌کار جامع آنتی فیشینگ بانکی در قالب یک راهکار یکپارچه پیاده سازی شده است.

ابر پروژه های ملی انجام شده

National Projects

- مشاوره در حوزه فناوری اطلاعات، پروژه مهاجرت به بانکداری الکترونیک نوین بانک سپه (Core-Banking)
- اجرای طرح امن سازی زیرساخت و تدوین نقشه راه امنیت فناوری اطلاعات (Security Master Plan)
- تامین سرویس های دولت الکترونیک برای ۷۰۰۰ دفتر پیشخوان در سراسر کشور
- مشارکت در توسعه زیرساخت های شبکه دولت با بیش از بیست هزار Node
- طراحی، نظارت و پیاده سازی مراکز عملیات امنیت (SOC) متعدد در کشور
- مشاور فناوری اطلاعات طرح ملی ادغام پنج بانک کشور در بانک سپه
- سابقه همکاری در حوزه افتا با بانک های دولتی و خصوصی کشور
- ارزیابی امنیتی و تست نفوذ سامان های متعدد دولتی و خصوصی
- طراحی و پیاده سازی ۳۲ مرکز داده در ۳۲ استان

برخی از مشتریان ما

Provide Comprehensive IT Infrastructure Solutions

ارائه راهکارهای جامع زیرساخت فناوری اطلاعات

دفتر مرکزی

تهران، بلوار کریمخان، آبان جنوبی، ساختمان رجاء

۰۲۱ ۸۸۹۱۸۱۳۶

۰۲۱ ۸۸۹۱۸۱۶۳

دفتر فنی و مرکز داده

جنب دانشگاه امیر کبیر، کوچه رشت، پلاک ۱

۰۲۱ ۶۶۴۰۹۲۸۸

۰۲۱ ۶۶۴۰۸۶۲۲

دفتر تحقیق و توسعه

برج پارک علم و فناوری دانشگاه شریف، واحد ۵۰۱

۰۲۱ ۸۸۸۰۹۹۸۶

۰۲۱ ۸۸۸۰۹۹۸۶

Rajaco.com