ارائه راهکارهای جامع زیرساخت فناوری اطلاعات
Comprehensive IT Infrastructure Solutions

جمهوری اسلامی ایران
وزارت بهداشت

جمهوری اسلامی ایران
معاونت توسعه مدیریت و سرمایه انسانی

جمهوری اسلامی ایران
مرکز راهبری افتا

جمهوری اسلامی ایران
وزارت نفت

جمهوری اسلامی ایران
معاونت امور مجلس

جمهوری اسلامی ایران
ریاست جمهوری

جمهوری اسلامی ایران
وزارت کار و امور اجتماعی

جمهوری اسلامی ایران
ستاد مرکزی مبارزه با قاچاق

بانک صنعت و معدن

بانک رفاه کارگران

بانک ملت

بانک مرکزی جمهوری اسلامی ایران

بانک کارآفرین

بانک تجارت
TEJARAT BANK

بانک صادرات ایران

سازمان نظام صنفی کشاورزی

بیمه مرکزی جمهوری اسلامی ایران

سازمان برنامه و بودجه کشور

سازمان بنادر و دریانوردی

سازمان ملی استاندارد

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

سازمان حفاظت محیط زیست

سازمان بیمه سلامت ایران

سازمان کشتیرانی ج.ا.ا
IRAN LINES

گروه مپنا

دفتر مرکزی: تهران، بلوار کریمخان، خیابان عضدی جنوبی، ساختمان رجاء ۰۲۱-۸۸۹۱۸۱۶۳ ۰۲۱-۸۸۹۱۸۱۳۶

دفتر فنی و مرکز داده: خیابان قائم مقام، خیابان خدری، پلاک ۵۹ ۰۲۱-۸۶۰۷۰۵۶۲ ۰۲۱-۸۶۰۷۰۵۶۲

دانشگاه رجاء: استان قزوین، بلوار شهید نوروزیان، دانشگاه رجاء ۰۲۱-۸۸۹۱۸۱۶۳ ۰۲۸-۳۳۶۷۷۱۰۱

دفتر تحقیق و توسعه: برج پارک علم و فناوری دانشگاه شریف، واحد ۵۰۱ ۰۲۱-۸۸۸۰۹۹۸۶ ۰۲۱-۸۸۸۰۹۹۸۶

Rajaco.com

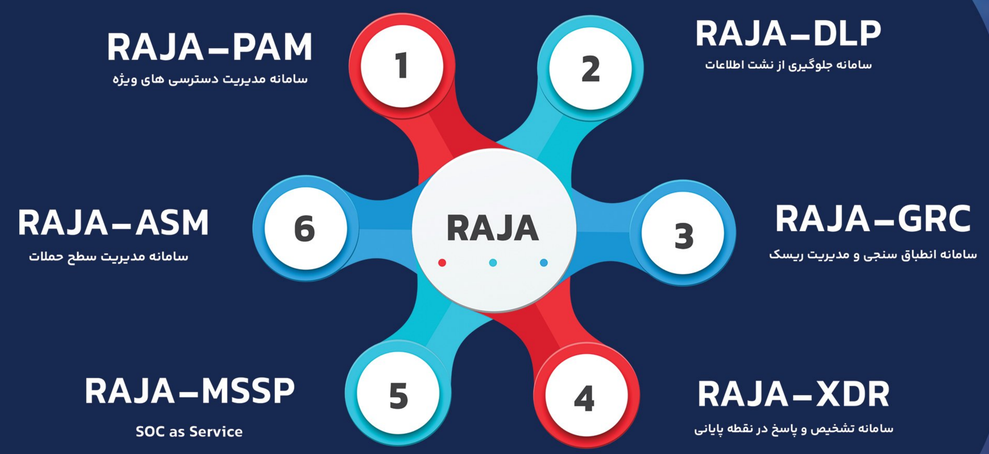
ارائه راهکار های جامع زیرساخت فناوری اطلاعات

Comprehensive IT Infrastructure Solutions

فناوری اطلاعات رجاء
رتبه یک شورای عالی انفورماتیک

TÜV InterCert SAAR ISO 10002:2014
TÜV InterCert SAAR ISO 9001:2015

Rajaco.com



ساختمان ستادی

تهران، کریمخان، آبان جنوبی،
ساختمان رجاء

برج فناوری شریف (R & D)

تهران ، جنب دانشگاه شریف،
طبقه۵ واحد۵۰۱

دانشگاه رجاء

استان قزوین ، بلوار نوروزیان،
دانشگاه رجاء

آزمایشگاه افتا و دیتا سنتر

تهران، قائم مقام، خیابان خدری
پلاک ۵۹

درباره فناوری اطلاعات رجاء

فناوری اطلاعات رجاء

گروه رجاء با بیش از یک دهه سابقه ، شامل شرکت‌های فناوری اطلاعات رجاء ، توسعه سرمایه‌گذاری 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 زیرساخت و خدمات متنوع 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 .

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
+۱۰ سال سابقه دانش بنیان
+۲ تیم تحقیقاتی مستقر در پارک فناوری شریف

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

مجوز ها تاییدیه ها

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

بیش از ده سال سابقه فعالیت

+۵۰۰ تعداد مشتری
+۲۵۰۰ پروژه انجام شده
+۸۵۰۰ لایسنس محصول نصب شده

RAJA PAM

برخی امکانات سامانه RAJA-PAM عبارتست از :

- مشاهده اتصالات در حال انجام شامل صفحه نمایش ، صفحه کیبورد ، کلیپبورد و انتقال فایل
- نوع دسترسی مانند صفحه نمایش اطلاعات کیبورد ، کلیپبورد یا انتقال فایل
- مشاهده وضعیت سامانه به منظور بررسی بار و اطلاعات لحظه ای سامانه
- دسترسی به اطلاعات ثبت شده کاربران یا اتصالات خاص
- ایجاد کاربران «حساس» با اختیارات قابل تعریف
- دریافت کامل تعامل کاربر به صورت فایل ویدیو
- مدیریت دقیق هویت و دسترسی هویت کاربران مبتنی بر نقش
- فرض عدم اعتماد پیش‌فرض، احراز هویت همه کاربران
- برای شناسایی و تحلیل اطلاعات موجود در اسناد، تصاویر و جستجو
- امکان مانیتورینگ و کنترل بدون تأثیر منفی و بهبود تجربه کاربری

AI-Based PAM+

UBA+

PAM

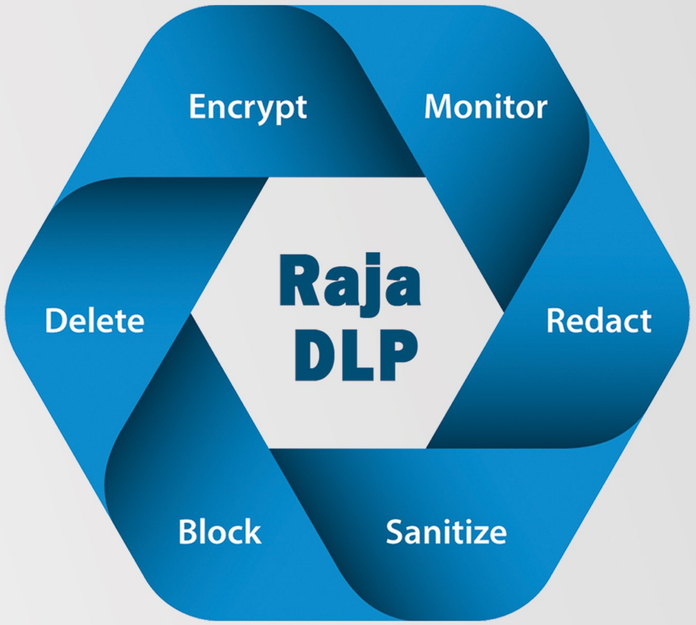
سامانه مدیریت دسترسی های ویژه

نظارت و کنترل بر دسترسي 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,HTTP/S ,SSH ,VNC به تجهیزات حساس سازمانی متصل مي 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 دسترسي ها نخواهد داشت.

RAJA-DLP

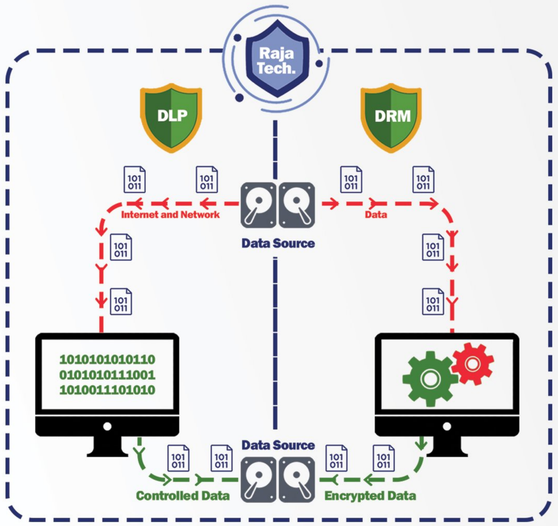
سامانه جلوگیری از نشت اطلاعات

امروزه بیش از هر زمان دیگری، تولید و گردش اطلاعات در بستر فناوری اطلاعات انجام می‌گردد. این اطلاعات به عنوان ارزشمندترین دارایی‌های یک سازمان یا شرکت محسوب شده و نگهداری از آن، نگرانی اصلی سازمان ها و شرکت‌های بزرگ و کوچک دولتی و خصوصی محسوب می‌گردد، 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 می‌گردد. 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 به عنوان راهکار جامع و یکپارچه، امنیت پایانه‌های شبکه و کاربران انتهایی در راستای جلوگیری از نشت اطلاعات سازمانی را بر عهده دارد.



ویژگی های سامانه RAJA-DLP

- سهولت در پیاده سازی عملکرد شفاف و عدم تداخل در کسب وکار جاری سازمان و کاربر
- کنترل دسترسی به منابع براساس حقوق کاربر شرایط سازمان و ضوابط مدون
- مدیریت فرآیند تولید، پردازش، انتقال و امحای دارایی های دیجیتالی سازمان
- امکان توسعه سفارشی قابلیت ها مطابق با نیاز هر سازمان
- کاهش مخاطرات ناشی از سرقت دارایی های سازمان
- اعطای حق مالکیت داده ها به سازمان به جای کاربر
- سلب مسئولیت حفاظت داده های سازمانی از کاربر
- امکان سیاست گذاری بر اساس گروه، رایانه، کاربر
- پشتیبانی از VDI , Thin Client, Domain
- امنیت بالا در مواجهه دسترسی های غیر مجاز
- ارائه سرویس پشتیبانی کامل

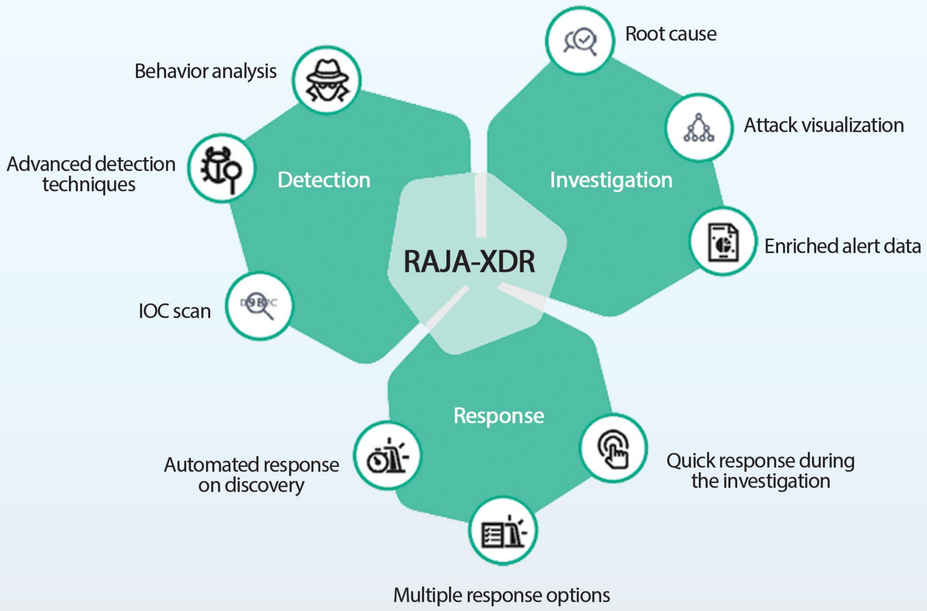


RAJA-XDR

سامانه تشخیص و پاسخ در نقطه پایانی

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.

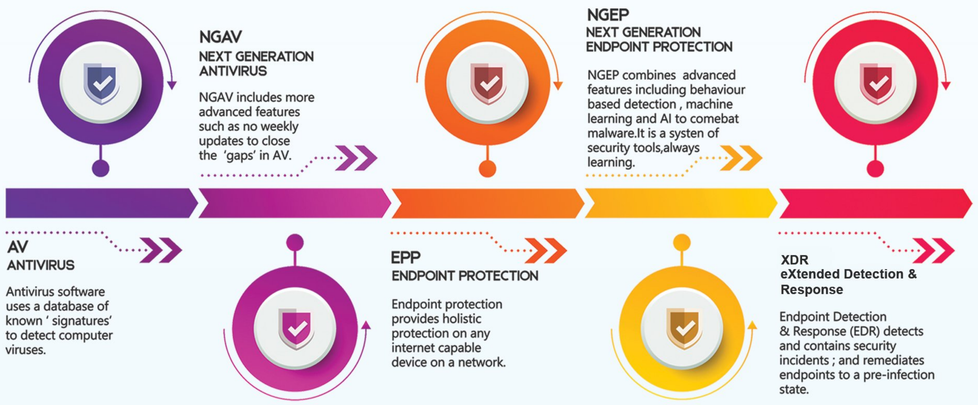
دغدغه های فوق در کنار گسترش روزافزون استفاده از فناوری های جدید نظیر هوش مصنوعی باعث ظهور سامانه eXtended Detection and Response (XDR) شد. این سامانه با تحلیل و شناسایی هرگونه آسیب پذیری، بدافزار یا فعالیت مشکوک در نقاط پایانی شبکه، اقدام به پاسخگویی و اعلام هشدار به مدیران سازمانی می کند. با توجه به بهره گیری از فناوری های جدید ، سامانه فوق سازمان را درمقابل طیف وسیعی از تهدیدات و حملات پیشرفته سایبری محافظت می کند. سامانه بومی RAJA - 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 ، هرگونه ناسازگاری در سیاست امنیتی، فعالیت مشکوک سرویس ها و همچنین بدافزارها را کشف و خنثی می کند.



لزوم بهره گیری از RAJA-XDR

در XDR، 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 جمع‌آوری اطلاعات برای مرکزعملیات امنیت (SOC) بوده و کمک شایانی در تحلیل وجلوگیری 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.



RAJA-GRC

سامانه انطباق سنجی و مدیریت ریسک

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 راستاي 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 داخلي و خارجي است که برای کسب‌وکار مورد نظر تعریف شده‌اند.

قابلیت های کلیدی RAJA - GRC

- 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 PDF, Excel, Word
- تعیین گردش کار زیر پروژه های امن سازی
- قابلیت ارسال Log بر روی SIEM در مراکز SOC
- احراز هویت با اکتیو دایرکتوری
- محاسبات ریسک پرسنلی
- قابلیت گروه بندی پیشرفت دارایی‌ها
- ساخت ارتباطات چندگانه و نمایش گرافیکال ارتباطات
- قابلیت زیر مجموعه بندی نوع دارایی ها
- مدیریت ریسک براساس استانداردهای جهانی
- قابلیت ارزیابی تطبیقی، ممیزی و پذیرش ریسک
- ارزش‌گذاری دارایی براساس C.I.A
- کتابخانه غنی از مراجع استانداردها
- قابلیت مدیریت دسترسی افراد به سامانه همانند مدیر، تحلیل‌گر، ممیز و...

RAJA MSSP

SOC as Service

مرکز عملیات امنیت درقالب خدمات مدیریت شده (MSSP) یک مرکز با استانداردهای امنیتی و فیزیکی بسیار پیشرفته برای Monitoring و مدیریت سیستم ها و تجهیزات امنیتی یک سازمان به صورت برون سپاری شده است.

MSSPها با استفاده از مراکز عملیات امنیت (SOC) با سطح دسترسی بالا طراحی شده‌اند تا علیرغم کاهش پرسنل امنیتی مورد نیاز، با ارائه خدمات به صورت ۲۴*۷ امنیت مورد نیاز سازمان را ارائه نمایند.

در یک مرکز امنیتی علاوه بر مانیتورینگ و انجام خدمات SOC، خدمات پیشرفته امنیتی نظیر Threat Hardening، Forensic، Hunting و... نیز انجام شده و می‌توان گفت یک پکیج کامل برای ارائه خدمات

مزایای استفاده از RAJA-MSSP

- تأمین نمای کلی از وضعیت امنیت اطلاعات و شبکه سازمان
- شناسایی و اولویت‌بندی حوادث و رویدادها از میان حملات اینترنتی و رویدادهای شبکه
- تحلیل رفتار شبکه و تشخیص سریع حوادث
- تطبیق رویدادها با سیاست‌های سازمانی
- پایش ۲۴×۷ تمامی رویدادها به صورت لحظه‌ای
- ارتباط با مراکز کنترل بالادستی نظیر گوهر و ماهر جهت حل حوادث امنیتی
- نظم بخشیدن و استانداردسازی فرآیندهای جاری در سطح سازمان مبتنی بر استاندارد ISO/IEC ۲۷۰۰۱: ۲۰۱۳
- تشخیص آسیب‌پذیری‌ها و حفره‌های امنیتی تجهیزات شبکه و گزارش نقاط آسیب‌پذیر قبل از وقوع حادثه امنیتی
- مدیریت مرکزی حملات و رخدادهای امنیتی و کنترل هوشمندانه و تحلیل تهدیدات با استفاده از گزارشات
- ارائه گزاراشات آماری و تحلیلی به صورت هفتگی، ماهیانه و یا بر حسب تقاضا
- اطلاع رسانی حوادث امنیتی به مسئول مربوطه با استفاده از پیامک، پست الکترونیکی، تماس تلفنی

RAJA ASM

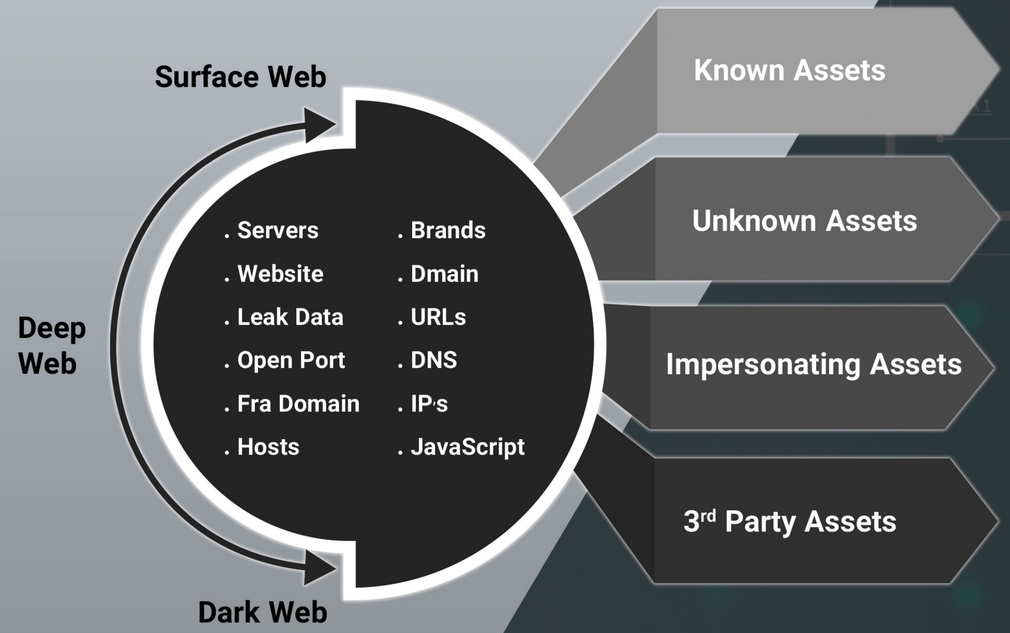
سامانه مدیریت سطح حملات

دلیل اهمیت ASM این است که در طول زمان دارایی سازمان ها شما افزوده می شوند و این تداول در مانیتور آن ها به شما کمک می کند تا تمامی دارایی های (سخت افزار یا نرم افزار) قدیمی و جدید را شناسایی کنید.

لیست دامین های Typo شناسایی کنید برای جلوگیری از فیشینگ

لیست دارایی های که End of line یا بروز رسانی نشده اند را شناسایی کنید (Patch Tuesdays)

در بخش توسعه نرم افزار لیست Library ها یا برنامه های اوپن سورس که در شبکه تان مورد استفاده قرار می دهید را شناسایی کنید(خیلی از بکدورها معمولا لایبری های آلوده وارد سازمان ها می شوند.)



Security Master Plan (SMP)

تدوین و مشاوره طرح امن سازی زیرساخت

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.

Security Assessment & Penetration Test

ارزیابی امنیتی و تست نفوذ

با گرایش روزافزون سازمان ها و شرکت ها به استفاده از فضای تبادل اطلاعات برای پیشبرد اهداف و ماموریت 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 مختل‌کننده‌ی خدمات، شنود، خرابکاری، نقض حریم خصوصی و ... قرار دارد و نپرداختن یا رویکرد نادرست به امنیت آن، خسارت جبران‌ناپذیر مادی و معنوی به بار می آورد.

ارزیابی امنیتی یا Penetration Testing، یك عمل مجاز، برنامه‌ریزی شده و سیستماتیك برای ارزیابی امنیت یک شبکه (شامل تجهیزات فعال و غیرفعال شبکه، سرویس‌دهنده‌ها، سرویس‌گیرنده‌ها، برنامه‌های کاربردی و ...) است که از طریق شبیه‌سازی حمله یك هکر یا نفوذگر خرابکار صورت می‌گیرد. کلیه متخصصان امنیت در حوزه فناوری اطلاعات بر این باورند که تنها روش اطمینان یافتن از امن بودن شبکه‌های رایانه‌ای و زیرساخت‌های ارتباطی و سامانه‌های اینترنتی، انجام عملیات ارزیابی امنیتی (آزمون نفوذپذیری) است.

مخاطبین طرح

مخاطب اصلی این طرح کلیه زیرساخت ها و دستگاه های دارای طبقه بندی کشور بوده و سایر دستگاه ها نیز می توانند به فراخور نیاز خود از آن استفاده نمایند.

خلاصه مدیریتی طرح

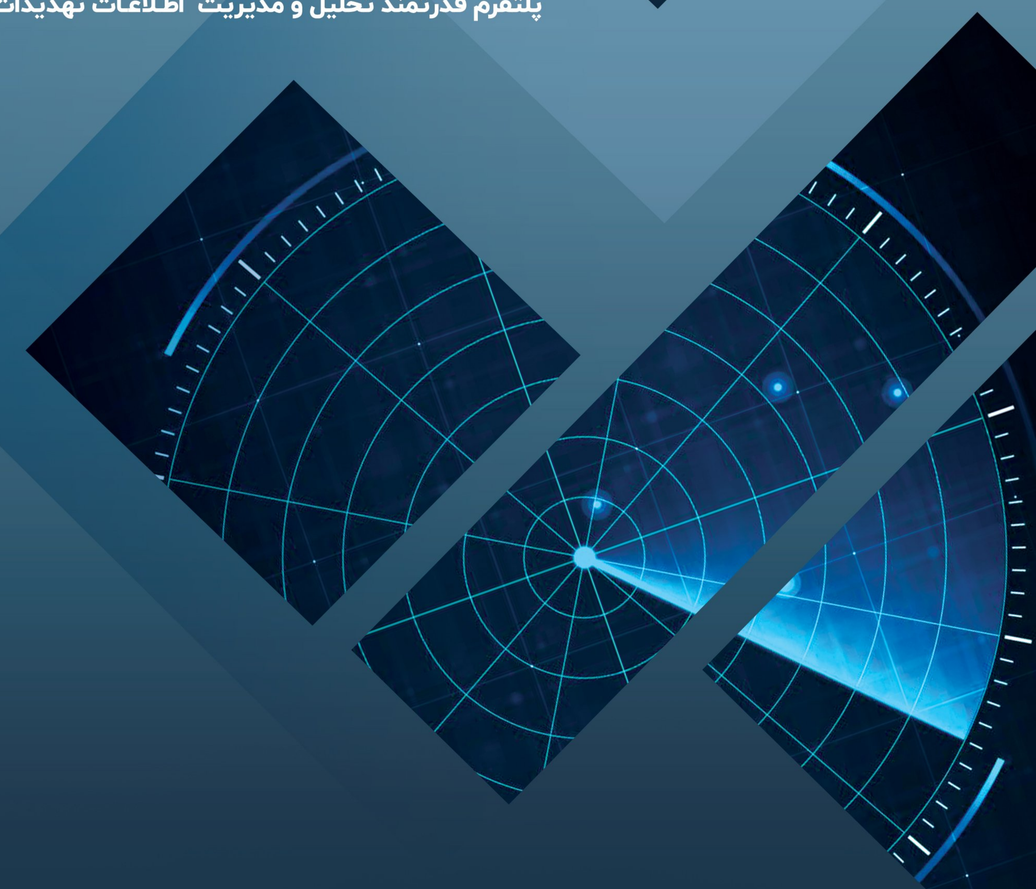
هدف از این طرح، تأمین امنیت فضای تولید و تبادل اطلاعات سازمان و جلوگیری از بروز اختلال در ارائه سرویس های حیاتی آن است. در این طرح الزاماتی برای ایجاد، پیاده‌سازی، نگهداری و بهبود مستمر امنیت اطلاعات در حوزه های زیرساختی ارائه‌شده است.

الزامات طرح امن سازی

این الزامات، کنترل‌های حداقلی به‌منظور کاهش مخاطرات دارای اولویت در زیرساخت‌ها 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.

Raja-CTI

پلتفرم قدرتمند تحلیل و مدیریت اطلاعات تهدیدات سایبری



در عصر پیچیده تهدیدات سایبری، امنیت صرفاً به معنی دفاع منفعل نیست. سازمان‌هایی که می‌خواهند از دارایی‌های اطلاعاتی خود به‌صورت هدفمند محافظت کنند، نیاز به دید تحلیلی، اطلاعات جامع تهدیدات و یکپارچگی عملیاتی با زیرساخت امنیتی خود دارند.

RajaCTI یک پلتفرم قدرتمند تحلیل و مدیریت اطلاعات تهدیدات سایبری (Cyber Threat Intelligence) است که با توانایی تجمیع، تحلیل، مصورسازی و اشتراک‌گذاری اطلاعات، به تیم‌های امنیتی کمک می‌کند تا از سطح رویداد به سطح درک عمیق از تهدید برسند.

یکی از مهم‌ترین قابلیت‌های RajaCTI، فراتر رفتن از تحلیل صرف تهدیدات خارجی است. این پلتفرم با اتصال و یکپارچگی کامل با داده‌های داخلی سازمان (از جمله لاگ‌های SIEM، رویدادهای امنیتی، سیستم‌های تشخیص نفوذ، و تحلیل‌گرهای رفتار کاربران)، امکان بررسی وضعیت داخلی امنیتی سازمان و شناسایی تهدیدات ناشناخته یا درونی را فراهم می‌سازد.

RajaCTI نه تنها سامانه‌ای برای تحلیل تهدیدات بیرونی است، بلکه ابزاری قدرتمند برای پایش هوشمند درون سازمانی، امکان‌سنجی خطرات داخلی، و ارزیابی مستمر سطح امنیت واقعی سازمان محسوب می‌شود.

چرا سازمان‌ها باید از RajaCTI استفاده کنند؟

- بررسی وضعیت و امکان‌سنجی تهدیدات درونی سازمان
- بررسی به روز تهدیدات سایبری و چرخه حملات دنیا به صورت جامع و امن
- تحلیل هوشمند، مبتنی بر غنی‌ترین منابع بین‌المللی تهدیدات سایبری
- یکپارچگی عمیق با SIEM، SOAR و EDR
- تحلیل دقیق و غنی‌سازی داده ها
- افزایش سرعت تشخیص و پاسخ به حوادث امنیتی
- نمایش گرافیکی و درک عمیق از زنجیره حمله (Attack Graphs & TTP Mapping)
- جستجو و فیلتر پیشرفته با کارایی بالا
- رابط کاربری مدرن و تعاملی برای تحلیل سریع

RAJA CTI

Cyber Threat Intelligence

AYYZA

سیستم مانیتورینگ آیزا

بررسی در دسترس بودن Uptime و سرعت بارگذاری Load speed از ۱۷ کشور در پنج قاره

بررسی در دسترس بودن Uptime و سرعت بارگذاری Load speed از ۱۵۰ نقطه کشور

- ۱۵۰ سرور در ۳۰ استان
- تست مستمر کارکرد وبسایت (Performance Test)
- تست امنیت وب سرویس یا وب سایت (security Check)

۵ سرور در هر استان در ۵ مرکز داده متفاوت

Ayyza

سرویس ها و خدمـــــات

Uptime Check

بررسی در دسترس بودن سرویس اینترنتی یا وبسایت در بازه های زمانی ۳۰ ثانیه یکبار

Performance Test

بررسی و مستندسازی صحت بارگذاری کامل وبسایت یا سرویس اینترنتی در مرورگرهای مختلف chrome / firefox / IE / Opera و همچنین از گوشی های مختلف تلفن همراه

SSLCheck

بررسی کیفیت SSL/TSL و تحلیل کیفیت رمزنگاری بکارگیری شده

Load Speed

بررسی مستندسازی سرعت بارگذاری کامل وبسایت از نقاط جغرافیایی مختلف

Iran Access

بررسی دسترسی به وبسایت از داخل و خارج از کشور

Trace Route

کنترل و ردیابی مسیر حرکت دیتا در شبکه، از تمام استان های ایران تا وبسایت شما

SLA Monitoring

پایش خدمات سرویس‌های آنلاین

Trace Route

پایش و پیش بینی حمله منع سرویس

ارائه راهکارهای جامع زیرساخت فناوری اطلاعات
Comprehensive IT Infrastructure Solutions

جمهوری اسلامی ایران
وزارت بهداشت

جمهوری اسلامی ایران
معاونت توسعه مدیریت و سرمایه انسانی

جمهوری اسلامی ایران
مرکز راهبری افتا

جمهوری اسلامی ایران
وزارت نفت

جمهوری اسلامی ایران
معاونت امور مجلس

جمهوری اسلامی ایران
ریاست جمهوری

جمهوری اسلامی ایران
وزارت کار و امور اجتماعی

جمهوری اسلامی ایران
ستاد مرکزی مبارزه با قاچاق

بانک صنعت و معدن

بانک رفاه کارگران

بانک ملت

بانک مرکزی جمهوری اسلامی ایران

بانک کارآفرین

بانک تجارت
TEJARAT BANK

بانک صادرات ایران

سازمان نظام صنفی کشاورزی

بیمه مرکزی جمهوری اسلامی ایران

سازمان برنامه و بودجه کشور

سازمان بنادر و دریانوردی

سازمان ملی استاندارد

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

سازمان حفاظت محیط زیست

سازمان بیمه سلامت ایران

سازمان کشتیرانی ج.ا.ا
IRAN LINES

گروه مپنا

دفتر مرکزی: تهران، بلوار کریمخان، خیابان عضدی جنوبی، ساختمان رجاء ۰۲۱-۸۸۹۱۸۱۶۳ ۰۲۱-۸۸۹۱۸۱۳۶

دفتر فنی و مرکز داده: خیابان قائم مقام، خیابان خدری، پلاک ۵۹ ۰۲۱-۸۶۰۷۰۵۶۲ ۰۲۱-۸۶۰۷۰۵۶۲

دانشگاه رجاء: استان قزوین، بلوار شهید نوروزیان، دانشگاه رجاء ۰۲۱-۸۸۹۱۸۱۶۳ ۰۲۸-۳۳۶۷۷۱۰۱

دفتر تحقیق و توسعه: برج پارک علم و فناوری دانشگاه شریف، واحد ۵۰۱ ۰۲۱-۸۸۸۰۹۹۸۶ ۰۲۱-۸۸۸۰۹۹۸۶

Rajaco.com

ارائه راهکار های جامع زیرساخت فناوری اطلاعات

Comprehensive IT Infrastructure Solutions

فناوری اطلاعات رجاء
رتبه یک شورای عالی انفورماتیک

TÜV InterCert SAAR ISO 10002:2014
TÜV InterCert SAAR ISO 9001:2015

Rajaco.com