CANDOO

Smart Data Processing

داده پردازی هوشمند کندو

آشنایی با "داده پردازی هوشمند کندو"

شرکت "داده پردازی هوشمند کندو" درسال ۱۴۰۲ به منظور ارائه خدمات فناوری اطلاعات و ارتباطات به ویژه درحوزه امنیت اطلاعات تاسیس گردید. هدف اصلی ما ارائه راهکارهای جامع امنیت، جهت حفاظت از اطلاعات و دارایی‌های دیجیتال سازمان‌ها می‌باشد.

درتلاش هستیم با خدمات مشاوره، اجرا، پیاده‌سازی و راهبری پروژه‌ها و همچنین ارائه راهکارهای نوآورانه و انعطاف پذیر، به نیازها و انتظارات بازار پاسخ دهیم. ما با توسعه دانش و مهارت کارکنان خود، به افزایش بهره وری و ارزش آفرینی می‌پردازیم.

CANDOO

Smart Data Processing

داده پردازی هوشمند کندو

چشم انداز و ماموریت

شرکت "داده پردازی هوشمند کندو" با ایجاد یک محیط امن و مطمئن برای اطلاعات و داده‌های مشتریان خود، به رشد و توسعه کسب و کارهای مختلف کمک می‌کند. ما با بهره‌گیری از دانش و تجربه متخصصان خود، از آخرین تکنولوژی‌ها و استانداردهای بین‌المللی در زمینه امنیت اطلاعات استفاده می‌کنیم.

مفتخریم که با ارائه خدمات مشاوره، طراحی، پیاده‌سازی، اجرا و پشتیبانی، به بهبود کیفیت و کارایی سیستم‌های اطلاعاتی مشتریان خود کمک نماییم. ما با ایجاد ارتباطات موثر و مستمر با مشتریان و شرکای تجاری خود، به دنبال ایجاد اعتماد و رضایت آن‌ها بوده و با توجه به نیازها و انتظارات بازار، به دنبال ارائه راهکارهای نوآورانه و انعطاف‌پذیر هستیم. همچنین با توجه به تغییرات و چالش‌های محیط کسب و کار، به دنبال یادگیری و تحول می‌باشیم. ما با توجه به رسالت و اهداف خود، به دنبال رسیدن به جایگاه برترین‌ها در زمینه فناوری و امنیت اطلاعات هستیم.

شعار ما:

"سپر امنیتی ما، همراهی قدرتمند برای آینده‌ی شما"

CANDOO

Smart Data Processing

داده پردازی هوشمند کندو

ارائه راهکارهای جامع امنیت اطلاعات:

این خدمت خود دربرگیرنده بسیاری از خدمات امنیت اطلاعات می‌باشد که به صورت یکپارچه و درهم تنیده می‌باشد: یک خدمت که به تهیه و اجرای یک برنامه و سیاست کاری در حوزه امنیت اطلاعات می‌پردازد و اهداف، استراتژی‌ها، فعالیت‌ها و معیارهایی را برای رسیدن به سطح امنیت مطلوب در یک بازه زمانی مشخص تعیین می‌نماید.

۱. رمزنگاری قوی داده‌ها: حفاظت از اطلاعات با رمزنگاری از مبدا تا مقصد

۲. مدیریت دسترسی‌های ممتاز: کنترل دقیق دسترسی‌ها بر اساس نقش و مسئولیت (RBAC)

۳. مدیریت رخداد سایبری: شناسایی سریع و واکنش به تهدیدات و ناهنجاری‌ها

۴. آموزش و آگاهی کاربران: افزایش آگاهی و توانمندی کاربران در زمینه امنیت اطلاعات

۵. پشتیبانی و بازیابی : حفاظت از داده‌ها و اطمینان از بازگشت‌پذیری اطلاعات

۶. ارتباطات امن: فراهم کردن ارتباطات امن و رمزنگاری شده

۷. پویش آسیب‌پذیری : بررسی و پویش دوره‌ای آسیب پذیری‌ها در جهت اطلاع از میزان امنیت سامانه‌ها. نصب وصله های امنیتی

۸. توسعه امن نرم‌افزار: به کارگیری روش‌های امنیتی در فرآیند توسعه و طراحی نرم افزار و سرویس ها

۹. آزمون تست نفوذ: آزمون و ارزیابی امنیتی دوره‌ای سامانه‌ها جهت شناسایی و رفع آسیب‌پذیری‌ها

۱۰. مدیریت تهدیدات : پیشگیری و شکار تهدیدات جهت مقابله با رخداد های محتمل

۱۱. شناسایی تهدیدات داخلی: رصد، پیشگیری و مقابله دربرابر تهدیدات داخلی.

۱۲. راه اندازی SIEM: راه اندازی و استقرار نرم افزارهای جمع‌آوری لاگ و رویدادها

۱۳. طرح تداوم کسب وکار: برنامه ریزی و اجرای طرح تداوم کسب و کار و بازیابی از فاجعه

۱۴. راه اندازی SOC و NOC: جهت پایش و رصد تمامی رویدادها

۱۵. ارزیابی سطح بلوغ امنیتی سازمان: شناسایی نقاط ضعف و بهبود آن ها براساس به‌روش‌های روز دنیا

۱۶. مشاوره، اجرا و پیاده‌سازی استانداردهای امنیت: استانداردهای ۲۷۰۰۱، ۳۱۰۰۰، ۵۵۰۰۱، ۲۲۳۰۱، ۲۰۰۰۰ و سایر استانداردهای امنیتی

CANDOO

Smart Data Processing

داده پردازی هوشمند کندو

آزمون تست نفوذ:

یک روش بررسی فنی است که با استفاده از روش‌های شبیه‌سازی حملات، آسیب‌پذیری‌ها و نقاط ضعف سیستم‌ها و شبکه‌های اطلاعاتی را شناسایی می‌کند. این تست‌ها از طریق شبکه‌ها، برنامه‌ها یا سیستم‌های مختلف اجرا می‌شوند تا به سازمان‌ها کمک کنند آسیب‌پذیری‌های امنیتی خود را بشناسند و در مقابل حملات سایبری آماده شوند.

اهداف اصلی تست نفوذ:

شناسایی نقاط ضعف: شناسایی آسیب‌پذیری‌ها و نقاط ضعف

ارزیابی وضعیت امنیتی: ارزیابی وضعیت در برابر حملات سایبری

تقویت امنیت: ارائه راهکارها و توصیه‌هایی برای بهبود

پویش آسیب پذیری:

پویش آسیب‌پذیری عبارت است از یک فرآیند جامع و سیستماتیک برای بررسی و تجزیه و تحلیل سیستم‌ها، شبکه‌ها و برنامه‌های کاربردی به منظور شناسایی و آشکارسازی نقاط ضعف امنیتی.

این خدمات با استفاده از ابزارها و تکنیک‌های مختلف، شناسایی آسیب‌پذیری‌های ممکن را فراهم می‌کنند تا سازمان‌ها بتوانند این ضعف‌ها را شناسایی و پس از شناسایی، اقدامات پیشگیری و تقویت امنیتی را اتخاذ کنند. این فرآیند به عنوان یک ابزار اساسی برای مدیریت ریسک‌های امنیتی مورد استفاده قرار می‌گیرد.

CANDOO

Smart Data Processing

داده پردازی هوشمند کندو

پیاده‌سازی استانداردهای امنیتی:

پیاده‌سازی و اجرای استانداردهای امنیتی نقش بسیارحیاتی درحفاظت ازاطلاعات سازمانی دارد. این فرآیند می‌تواند بسیارگسترده و شامل مراحل مختلفی مانند بررسی و تحلیل، طراحی و تدوین سیاست‌ها، آموزش و آگاهی‌رسانی، ممیزی و ارزیابی و ... باشد. این فرآیندها باید به طورمداوم پیگیری شده و با توجه به تغییرات درمحیط کسب و کارو تکنولوژی‌های جدید، به روزرسانی شوند تا امنیت اطلاعات سازمان حفظ شود.

مهمترین استانداردهای امنیتی:

1. استاندارد ISO 27001 (امنیت اطلاعات)
2. استاندارد ISO 31000 (مدیریت ریسک)
3. استاندارد ISO 55001 (مدیریت دارایی ها)
4. استاندارد ISO 22301 (تداوم کسب و کار)
5. استاندارد ISO 20000 (مدیریت خدمات فناوری اطلاعات)

راه اندازی مرکز عملیات SOC و NOC:

راه‌اندازی مرکز عملیات امنیت (SOC) و مرکز عملیات شبکه (NOC) نیازمند برنامه‌ریزی دقیق و فرآیندهای مشخصی است. این مراکز هدف اصلی خود را برای مدیریت و نظارت برامنیت و عملکرد شبکه و سیستم‌ها در سازمان تعریف می‌کنند.

این مراکز به عنوان مرکزهای اصلی نظارت و پاسخگویی به وقوع حوادث و رویدادهای امنیتی یا فنی در سازمان عمل می‌کنند و نیازمند یک برنامه ریزی دقیق و اجرای مداوم هستند تا کارایی بالایی داشته باشند.

CANDOO

Smart Data Processing

داده پردازی هوشمند کندو

طرح تداوم کسب وکار:

طرح تداوم کسب و کار، یک راهبرد جامع برای بازیابی از فاجعه و حفظ پایداری کسب و کار است. این طرح با ارزیابی دقیق دوره‌های ریسک و مخاطرات ممکن، برنامه‌های موثری برای مقابله با بحران‌ها و فاجعه‌های محتمل ایجاد می‌کند. با استفاده از سناریوهای شبیه‌سازی و آمادگی برای وقوع حوادث، این طرح امکان بازیابی سریع و مؤثر پس از فاجعه را فراهم می‌کند.

به این منظور یک تیم تداوم کسب و کار ایجاد و نقش‌ها و مسئولیت‌های آن‌ها تعیین می‌گردد. همچنین باید این طرح به طور منظم آزمایش، ارزیابی و بهبود داده شود.

مدیریت حوادث امنیتی:

مدیریت حوادث امنیتی به معنای برنامه‌ریزی، شناسایی، پیشگیری، و پاسخگویی به حوادث و رویدادهای امنیتی است. این فرایند شامل مراحل مختلفی است که از جمله آن‌ها می‌تواند موارد زیر باشد:

۱. شناسایی و تحلیل حوادث
۲. پیشگیری و حفاظت
۳. تدوین طرح پاسخگویی
٤. آزمون و تمرینات
٥. مانیتورینگ و ارزیابی پس‌ازحادثه

مدیریت حوادث امنیتی به سازمان‌ها کمک می‌کند تا در صورت وقوع حوادث، از دست دادن اطلاعات، زیرساخت‌ها و حتی اعتبار را به حداقل برسانند و سریعاً به وضعیت عادی بازگردند.

CANDOO

Smart Data Processing

داده پردازی هوشمند کندو

امن سازی و هاردنینگ:

هدف این رویکرد، تقویت سیستم‌ها و شبکه‌ها در مقابل تهدیدات امنیتی مختلف، از جمله حملات سایبری و نفوذهای مخرب، با هدف حفظ امنیت داده‌ها و اطمینان از پایداری و عملکرد صحیح سیستم‌ها می‌باشد.

هدف از امن‌سازی سیستم‌ها کاهش خطر امنیتی با ازبین بردن حمله بالقوه و یا متراکم کردن سطح حمله سیستم است.

امن سازی موجب کاهش فرصت برای مهاجمین می‌گردد.

ارزیابی سطح بلوغ امنیت:

بلوغ سازمانی معیار سنجش کیفیت عملیات یک شرکت است. یک شرکت با سطح بلوغ بالا می تواند با چالش ها روبرو شود و از فرصت ها استفاده کند. بهبود بلوغ سازمانی فرآیندی تدریجی است که بر خودسازی تاکید دارد.

ارزیابی سطح بلوغ امنیتی یک فرآیند جامع برای سنجش کیفیت و قابلیت اطمینان سیستم‌ها و فرآیندهای امنیتی در سازمان‌هاست. این ارزیابی‌ها به سازمان‌ها کمک می‌کنند تا نقاط ضعف امنیتی خود را شناسایی کرده و برنامه‌هایی را برای بهبود و تقویت امنیت داده‌ها و فرآیندهای خود اجرا کنند.

CANDOO

Smart Data Processing

داده پردازی هوشمند کندو

هوش تجاری:

هوش تجاری یک فرایند تحلیلی و فناورانه است که به کمک مجموعه‌ای از ابزار و روش‌های تحلیل داده‌ها، اطلاعات و دانش درونی یک سازمان را به صورت مفهومی و قابل فهم برای تصمیم‌گیری‌های استراتژیک تبدیل می‌کند.

هوش تجاری از اطلاعاتی که در داخل یک سازمان تولید می‌شود (از جمله داده‌های مالی، فروش، مشتریان و ...) استفاده می‌کند تا مدیران و تصمیم‌گیران را قادر به ارزیابی و تحلیل بهتر و دقیق‌تر وضعیت فعلی سازمان و پیش‌بینی روندها کند.

هوشمندسازی:

هوشمندسازی خانه و کسب و کار با استفاده از فناوری اطلاعات

- استفاده از سیستم‌های خانه هوشمند برای کنترل نورپردازی، دما، رطوبت و ...
- ارتقاء سیستم‌های اطلاعاتی در کسب و کار برای بهبود عملکرد و کاهش هزینه‌ها.

استفاده از اینترنت اشیاء (IOT)

- امکان جمع‌آوری داده‌های بیشتر و بهبود تصمیم‌گیری.

سیستم‌های هوش مصنوعی (AI)

- پیاده‌سازی الگوریتم‌های هوش مصنوعی در کسب و کار برای پیش‌بینی نیازها و بهینه‌سازی فرآیندها.

امنیت:

- ارتقاء سیستم‌های امنیتی با استفاده از تکنولوژی هوشمند.
- رمزنگاری داده‌ها و حفاظت از حریم خصوصی.