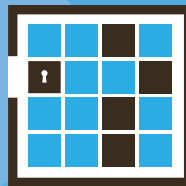


شرکت مهندسی امن گستر پیام پرداز

www.AmnGostar-Co.com



شرکت مهندسی
امن گستر پیام پرداز

برخی از بهره برداران خدمات شرکت مهندسی امن گستر پیام پرداز



شرکت خدمات انفورماتیک



سازمان اسناد و کتابخانه ملی جمهوری اسلامی ایران



رلو آرمین جمهوری اسلامی ایران



سازمان ثبت احوال کشور



شرکت پژوهش و توسعه ملی
National Research & Development Company



جمهوری اسلامی ایران
وزارت کشور



شرکت مهندسی و ارتباطی
فهمیم مشاور



صنایع الکترونیک شیراز



سازمان بهره‌ده خدمات فرعی صنایع



MIDHCO



انجمن رمز ایران



جمهوری اسلامی ایران
ریاست جمهوری



جمهوری اسلامی ایران
وزارت امور خارجه



دانشگاه جهاد



ITRC
مرکز تحقیقات مخابرات ایران



سازمان مخابرات
میرت مخابرات تهران



سازمان مخابرات جمهوری اسلامی ایران



تولید کننده



ایرانسل
MTN



جمهوری اسلامی ایران
وزارت صنعت، معدن و تجارت



وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران



وزارت کشور
استاداری خراسان شمالی



شرکت ارتباطات زیرساخت



هدا اول



شرکت توزیع برق شهرستان اصفهان



شرکت سالی سازان آب برق خوزستان



وزارت کشور
استاداری خوزستان



وزارت کشور
استاداری خوزستان



بانک ایران زمین



بنیاد
تعمیر و نگهداری
۱۳۵۸



بانک آینده
AYANDEH BANK



بانک انصار



بانک ملت
bank mellat



بنیاد
تعمیر و نگهداری
۱۳۵۸



بانک صادرات ایران



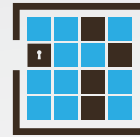
بانک پارسیان



گروه صیبا



سازمان پیمان‌رو و پیمان‌رویی



معرفی شرکت

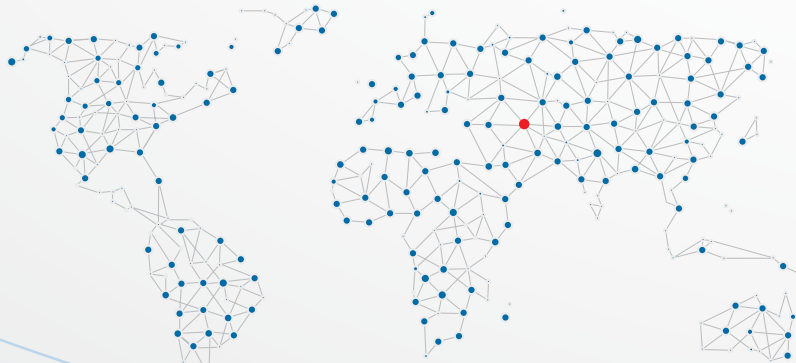
شرکت مهندسی امن گستر پیام پرداز یکی از شرکت‌های زیرمجموعه گروه پیام پرداز است که با هدف ارائه خدمات تخصصی در زمینه امنیت فناوری اطلاعات و ارتباطات تأسیس گردیده است. این شرکت با استفاده از نیروی انسانی متعهد و متخصص رسالت خویش را صیانت از سرمایه های اطلاعاتی کشور قرار داده و در این راستا اقدام به ارائه بسته های مشاوره ای، آموزشی و نرم افزاری مرتبط با امنیت اطلاعات نموده است. خدمات متنوع ارائه شده، مکمل تجهیزات پیشرفته شرکت پیام پرداز است که به صورت کاملاً بومی تولید شده و مورد استفاده گسترده سازمان ها می باشد.

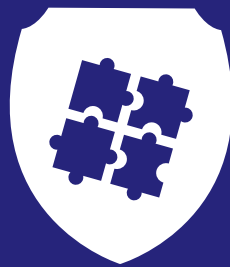
گواهینامه ها و مجوزها

- دارای پروانه فعالیت در نظام ملی مدیریت امنیت اطلاعات (نما) در حوزه مشاوره از سازمان فناوری اطلاعات و مرکز مدیریت راهبردی افتای ریاست جمهوری
- دارای پروانه فعالیت در نظام ملی مدیریت امنیت اطلاعات (نما) در حوزه آموزش از سازمان فناوری اطلاعات و مرکز مدیریت راهبردی افتای ریاست جمهوری
- دارای گواهی رتبه بندی و احراز صلاحیت از شورای عالی انفورماتیک
- عضویت در سندیکای افتا
- عضویت در سازمان نظام صنفی رایانه ای کشور

موضوع فعالیت شرکت

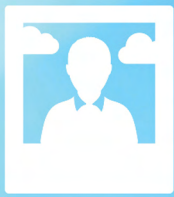
- ارائه راهکارهای جامع امن سازی در همه حوزه های فناوری اطلاعات و ارتباطات
- مشاوره، طراحی و پیاده سازی استانداردهای فناوری اطلاعات (ISMS, ITIL, ...)
- ارائه نرم افزارهای سیستم مدیریت و کنترل های عملیاتی امنیت اطلاعات
- طراحی و پیاده سازی مراکز پاسخگویی به رخدادهای رایانه ای (CERT)
- طراحی و پیاده سازی مرکز عملیات امنیت (SOC)
- انجام آزمون نفوذپذیری (Penetration Test) در سطوح مختلف
- طراحی و اجرای معماری امن مراکز داده، شبکه ها و مجازی سازی
- برگزاری دوره های آموزشی امنیت فناوری اطلاعات و ارتباطات





ISMS

شرکت مهندسی امن گستر پیام پرداز با بهره گیری از کارشناسان خبره و با تجربه در زمینه مشاوره و پیاده سازی سیستم مدیریت امنیت اطلاعات جهت ایجاد یک فضای امن به منظور رسیدن به اهداف سازمانی و تداوم کسب و کار در کنارتان خواهد بود.



سازمان ها در مسیر تعالی خود نیاز به توسعه زیرساخت های فناوری اطلاعات و ارتباطات دارند، اما امنیت یک چالش بزرگ در این مسیر بوده و توسعه ICT سازمانی بدون رعایت ملاحظات امنیتی غیرممکن می باشد. نکته مهم آن است که برقراری امنیت در یک سازمان دفعتاً امکان پذیر نیست و باید این امر به صورت مداوم و در یک چرخه امن سازی شامل طراحی (Plan)، پیاده سازی (Do)، ارزیابی (Check) و اقدام (Action) انجام گیرد. سیستم مدیریت امنیت اطلاعات (ISMS) بر اساس استاندارد ISO 27001:2013 و رویکرد پدافند سایبری کلیه فرایندهای لازم برای ایجاد چرخه امن سازی فناوری اطلاعات سازمانی را تبیین می نماید.



- مشاوره در زمینه طراحی، پیاده سازی، نظارت و نگهداری سیستم مدیریت امنیت اطلاعات (ISMS) (مبتنی بر استاندارد ISO27001:2013)
- مشاوره و پیاده سازی سیستم مدیریت تداوم کسب و کار (BCM) (مبتنی بر استاندارد ISO22301)
- مشاوره و پیاده سازی سیستم مدیریت حوادث و ایجاد تیم واکنش سریع به حوادث امنیتی (CERT)
- مشاوره و پیاده سازی سیستم مدیریت بازیابی حوادث و پایداری (DRM)
- مشاوره و پیاده سازی سیستم مدیریت امنیت اطلاعات مبتنی بر الزامات پدافند غیرعامل
- طراحی و اجرای فرآیندهای امنیت اطلاعات مبتنی بر BPMS بومی (نرم افزار سپهر)
- مدیریت ریسک مبتنی بر نرم افزار ISMS (نرم افزار سپهر)
- مشاوره طراحی و پیاده سازی استاندارد PCI – DSS (Payment Card Industry Data Security Standard)
- مشاوره پیاده سازی مرکز صدور گواهینامه داخلی سیستم مدیریت امنیت اطلاعات
- ممیزی داخلی (Internal Audit)
- تحلیل فاصله (Gap Analysis)

مزایای پیاده سازی سیستم های مدیریت امنیت اطلاعات

- شناسایی ریسک های امنیت اطلاعات و اولویت بندی اقدامات (RTP)
- ایجاد شفافیت برای تصمیم گیری مدیران
- کاهش حوادث امنیت اطلاعات و هزینه های ترمیم خسارات
- آمادگی در شرایط اضطراری
- اطمینان برای رسیدن به اهداف
- بهبود در هدف گذاری و برنامه ریزی های امنیتی
- بهبود مدیریت تداوم کسب و کار
- حفاظت از سرمایه های سازمانی
- امنیت اطلاعات و دارایی های اطلاعاتی
- حفظ محرمانگی، یکپارچگی و دسترس پذیری اطلاعات
- حفظ اطلاعات از بروز تهدیدات
- برنامه ریزی در جهت کنترل آسیب پذیری ها
- مواجهه سریع و اصولی با حوادث امنیت اطلاعات
- ایجاد اطمینان بیشتر برای مدیران، کارکنان، مشتریان و سایر ذینفعان سازمان





خدمات فنی

رشد روزافزون فناوری های اطلاعاتی و ارتباطی، علی رغم ارائه مزایای فراوان در راستای اهدافی همچون تسهیل، تسریع و بهبود فرآیندها و مأموریت های سازمانی، مخاطرات بسیاری را نیز در پی دارد. لزوم مقابله با مخاطرات مزبور، شرکت امن گستر را بر آن داشته تا با اتکا به نیروهای متخصص، مجرب و متعهد به ارائه خدمات فنی در حوزه امنیت از جمله مشاوره، ارزیابی و آزمون های امنیتی، پیاده سازی راهکارهای امنیتی در لایه های مختلف و ... بپردازد.





طراحی، پیاده سازی و بهبود امنیتی شبکه

- طراحی و پیاده سازی شبکه بر اساس اصول دفاع در عمق، ماژولاریتی، مقیاس پذیری سرویس ها و افزایش بهره‌وری عملیاتی
- طراحی مجدد و بهبود امنیتی معماری شبکه و با حفظ دسترس پذیری سرویس دهی سامانه ها و سایر سرویس های اصلی شبکه
- پیاده سازی سرویس های شبکه در راستای اطمینان از عملکرد مناسب، بهبود کارایی و پایداری شبکه مانند AD، Monitoring، NTP
- پیاده سازی سرویس های امنیتی در راستای بهبود امنیت شبکه و اطمینان از عدم نقض پارامترهای امنیتی مانند Patch Management، 802.1x، Privileged User Management، Log & Event Management، Internet & Intranet Access Control، AAA
- آنالیز امنیتی و Network Forensic
- زیرساخت کلید عمومی (PKI) و امضای دیجیتال
- امنیت اتاق سرور و مرکز داده



ارزیابی و امن سازی سامانه های اطلاعاتی

- شناخت، ارزیابی، ارائه راهکار، پیاده سازی و ممیزی سامانه اطلاعاتی در:
 - لایه زیرساخت شامل سیستم عامل، پایگاه داده، وب سرور و سرویس های اصلی شبکه
 - لایه شبکه و ارتباطات شبکه ای شامل تجهیزات شبکه ای و امنیتی و ... مورد استفاده
 - لایه برنامه کاربردی شامل معماری، گروه های کاربری، جریان داده و کنترل های فنی و امنیتی
- ارزیابی امنیتی بر مبنای:
 - ابزار خودکار
 - دستورالعمل های امن سازی مرجع
 - الزامات امنیتی مانند PCI-DSS، 53-800 OWASP ASVS، DISA App Security، NIST و ...
- راهکارهای امنیتی:
 - طرح معماری امنیتی سامانه و امنیت ارتباطات در لایه های کاربرد و شبکه
 - طرح احراز اصالت، مدیریت مجوزها و کنترل دسترسی کلیه موجودیت های درگیر در سامانه از قبیل کاربران، تجهیزات نرم افزاری و سخت افزاری
 - طرح امنیت ذخیره سازی و جریان داده ها در اجزای سامانه از بعد محرمانگی و صحت
 - تدوین کنترل های امنیتی مورد نیاز
 - طرح رویدادنگاری و مدیریت ثبت رخداد
 - طرح پشتیبان گیری از سامانه



امن سازی پیکربندی (Hardening)

- امن سازی پیکربندی زیرساخت های فناوری اطلاعات بر مبنای دستورالعمل های مرجع مانند DISA، NIST، CIS، Vendor Best Practice
- سیستم عامل
- پایگاه داده
- وب سرور
- تجهیزات شبکه: Switch، Router
- تجهیزات امنیتی: Firewall، IDS/IPS



خرید، تامین و پشتیبانی تجهیزات

- Vulnerability Scanner
- Endpoint Security
- Firewall
- SIEM & SOC
- IDS & IPS
- Forensics
- WAF
- DLP (Data Loss Prevention)



■ جعبه سفید (White-Box)

انجام آزمون با در اختیار داشتن اطلاعات نسبتاً کامل از هدف
 - لایه شبکه : آگاهی از معماری شبکه، تجهیزات موجود و مکانیزمهای امنیتی مورد استفاده، OS، DB و ...
 - لایه کاربرد: حساب کاربری عادی و مدیر - در برخی مواقع دسترسی به سورس کد برنامه

■ جعبه خاکستری (Gray-Box)

انجام آزمون با در اختیار داشتن اطلاعات محدودی از هدف
 - لایه شبکه : آگاهی محدود در خصوص معماری شبکه و تجهیزات مورد استفاده و ...
 - لایه کاربرد: حساب کاربری عادی

■ جعبه سیاه (Black-Box)

انجام آزمون بدون در اختیار داشتن هرگونه اطلاعاتی از هدف
 - لایه شبکه : صرفاً نام شرکت یا یک آدرس اینترنتی
 - لایه کاربرد: صرفاً یک URL



حوزه ها

- Cloud
- لایه شبکه
- لایه زیرساخت
- سامانه های کنترل صنعتی
- لایه کاربرد (Web Application , Mobile Application , Client/Server Application)



Mobile Applications

- جمع آوری اطلاعات
- مدل سازی تهدید
- OWASP Top 10
- OASAM 9 Security Controls
- سناریوی اختصاصی
- ارزیابی و تحلیل آسیب پذیری ها
- روش های ایستا
- روش های پویا
- روش های فانزیک
- تدوین گزارش و ارائه راهکار
- مشاوره در پیاده سازی راهکارهای ارائه شده (در صورت نیاز پیاده سازی راهکار)
- ممیزی جهت اطمینان از پیاده سازی راهکار و صحت انجام کار

Web Application

- شناخت اولیه (Primary Recognition)
- کارکرد سامانه / نقش سامانه در فرایندهای سازمان / اهمیت سامانه / گستره کاربران سامانه / محدوده جغرافیایی دسترسی به سامانه
- شناسایی و جمع آوری اطلاعات (Information Gathering and Foot-Printing)
- پویش خودکار و کشف آسیب پذیری ها
- پویش با ابزار خودکار
- بررسی صحت آسیب پذیری های کشف شده توسط ابزار و حذف False/Positive ها
- پویش دستی و کشف آسیب پذیری های شناسایی نشده در پویش خودکار
- انجام آزمون ها منطبق بر ASVS یا OWASP Testing Guide
- تدوین سناریوی آزمون مختص سامانه
- استفاده از ابزارهای غیر خودکار و ابزار تحلیل کد
- نفوذ و Exploit
- تدوین گزارش و ارائه راهکار
- مشاوره در پیاده سازی راهکارهای ارائه شده (در صورت نیاز پیاده سازی راهکار)
- ممیزی جهت اطمینان از پیاده سازی راهکار و صحت انجام کار





نرم افزارهای مدیریت امنیت اطلاعات

شرکت مهندسی امن گستر پیام پرداز در جهت توانمندسازی سازمان ها برای استقرار امنیت اقدام به ارائه راهکار نرم افزاری کامل در قالب سه نرم افزار سیستم مدیریت امنیت اطلاعات سپهر (SEPEHR)، سیستم مدیریت فرآیندهای کسب و کار (BPMS) و نرم افزار جلوگیری از نشر غیر مجاز داده (DLP) نموده است.





نرم افزار سیستم مدیریت امنیت اطلاعات سپهر SEPEHR

- پوشش کامل چرخه طراحی، اجرا، بازنگری و بهبود سیستم مدیریت امنیت اطلاعات
- نگهداری و سازماندهی حجم بالای اطلاعات
- کاهش نیاز به نیروی انسانی
- کاهش زمان و هزینه مورد نیاز برای مدیریت امنیت
- جلوگیری از خطاهای انسانی
- تحلیل کارآمد اطلاعات گردآوری شده
- آزادی عمل در انتخاب متدلوژی مدیریت مخاطرات
- مدیریت موثر مدارک و سوابق
- تضمین بالاتر اجرای فرایندهای سازمان با پشتوانه فناوری اطلاعات (مبتنی بر BPMS)
- ایجاد سهولت در تصمیم گیری مدیران ارشد مبتنی بر اطلاعات موثق



سیستم مدیریت فرایندهای کسب و کار (BPMS) Business Process Management System

- دارای فرم ساز پیشرفته و قابلیت استفاده از ابزارهای متنوع
- قابلیت مدل سازی فرایندهای مختلف مبتنی بر کسب و کار سازمان
- اعمال انواع صحت سنجی ها و شروط منطقی و محاسباتی هنگام طراحی گردش کار
- پشتیبانی استفاده از بانکهای اطلاعاتی مختلف و به کارگیری داده های موجود در آنها هنگام اجرای فرآیند
- امکان صدور هشدارها در قالب ایمیل و پیام کوتاه جهت پیگیری بهینه اجرای فرآیند
- ایجاد بستری مناسب جهت تولید انواع گزارش های کارشناسی و مدیریتی



نرم افزار جلوگیری از نشر غیر مجاز داده (DLP) Data Loss Prevention

- استقرار امنیت اطلاعات بدون ایجاد هیچگونه تغییر در روال های کاری سازمان و بصورت شفاف از دید کاربران
- جلوگیری از خروج غیرمجاز و افشای اطلاعات سازمان
- جلوگیری از نسخه برداری غیرمجاز فایل ها و اطلاعات سازمان
- رویدادنگاری تغییرات اعمال شده روی فایل ها و دایرکتوری ها
- استفاده از الگوریتم های قوی و معتبر جهت رمزنگاری اطلاعات سازمان (قابلیت استفاده از الگوریتم سفارشی مشتری)
- معرفی نرم افزارهای موردنظر (هر نوع نرم افزار بومی یا خارجی) جهت محافظت
- تبادل ایمن اطلاعات با شرکاء و پشتیبانی از دورکاری
- اطمینان از پذیرش سیاست های امنیتی سازمان و پوشش کنترل های ISO27001 و جرایم رایانه ای



این نرم افزار توانایی طراحی و اجرای سیستم مدیریت امنیت اطلاعات را با صرف وقت و هزینه کمتر برای سازمان ها مهیا می کند. به دلیل انعطاف بالای نرم افزار که ناشی از پویایی همه قسمت های آن است، هر سازمان می تواند شیوه نگهداری اطلاعات و انجام محاسبات لازم در نرم افزار را بر اساس روش مدیریت مخاطرات تصویب شده در سازمان، پیکربندی نماید.

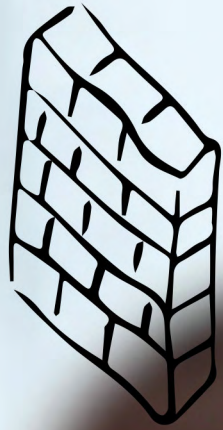
نرم افزار سپهر با تجهیز به موتور فرم ساز و گزارش ساز بسیار قوی، داشبورد، امکان تعریف روش های اجرایی، دستورالعمل ها، چک لیست ها، امکان انتخاب رفتار با مخاطره و اختصاص اقدامات کنترلی مناسب و صدور هشدار از طریق ایمیل و پیام کوتاه، چرخه استقرار سیستم مدیریت امنیت را کامل می کند. سیستم ثبت وقایع بسیار قدرتمند نرم افزار توانایی نظارت کامل بر چگونگی پیاده سازی سیستم را برای مدیران فراهم می کند.

قابلیت های نرم افزار سپهر

- پویایی کامل جهت انطباق با متدولوژی های مختلف مدیریت ریسک
- مبتنی بر وب و دارای امکان پشتیبانی از کاربران متعدد با سطوح دسترسی متفاوت
- قابلیت ورود و صدور اطلاعات با استفاده از فایل های داده موجود در سازمان
- امکان استفاده از توکن علاوه بر نام کاربری و گذرواژه برای احراز هویت دو عاملی
- روش های پیشرفته کنترل دسترسی
- دارای ساز و کار امنیتی سطح بالا به منظور حفاظت از داده های اطلاعاتی نرم افزار
- ثبت کلیه وقایع سیستم و تولید گزارش مناسب از آن
- امکان ارزیابی فاصله وضعیت موجود امنیت با شرایط ایده آل
- وجود گزارشات طراحی شده متناسب با نیازهای کاربران و مدیران
- تولید انواع گزارشات سفارشی با استفاده از موتور گزارش ساز کاملاً پویا و ساخت داشبورد مدیریتی
- تولید انواع نمودار با فرمت میله ای، دایره ای و غیره
- تهیه فهرست کاملی از دارایی های سازمان و اختصاص شناسنامه به آن ها
- جمع آوری خودکار دارایی های سخت افزاری، نرم افزاری، کاربران و پایگاه داده توسط جستجوگر شبکه
- گروه بندی دارایی ها بر اساس نوع دارایی
- امکان رمزنگاری داده های مهم ذخیره شده در پایگاه داده
- ساده سازی ورود اطلاعات با استفاده از ساختار سلسله مراتبی دارایی ها
- قابلیت تولید راهنمای کاربری منطبق با فرهنگ امنیتی سازمان توسط مدیر سیستم
- مدیریت گردش اسناد و نگهداری سوابق اسناد ایجاد شده در سیستم
- صدور هشدار از طریق ایمیل و پیام کوتاه منطبق با تنظیمات روش های اجرایی
- امکان طبقه بندی اسناد از حیث محرمانگی
- قابلیت ایجاد انواع اسناد شامل خط مشی، اهداف، دستورالعمل، چک لیست، روش اجرایی و غیره
- قابلیت ایجاد انواع روش های اجرایی مانند روش اجرایی مدیریت حوادث، مدیریت تغییرات، پشتیبان گیری، کنترل دسترسی
- موتور تولید فرم پیشرفته
- گزارش گیری مناسب از تغییرات و وضعیت اسناد
- مبتنی بر وب و دارای امکان پشتیبانی از کاربران متعدد با سطوح دسترسی متفاوت
- سازگاری با مرورگرها و پلتفرم های مختلف

ET

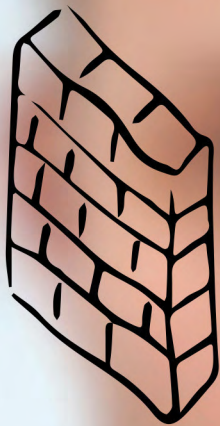
social network



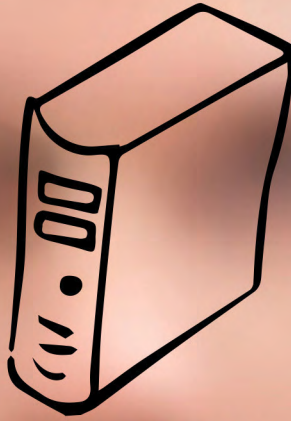
firewall



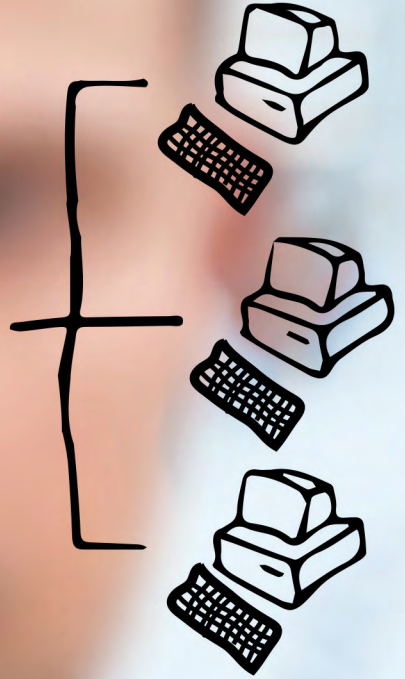
server



firewall



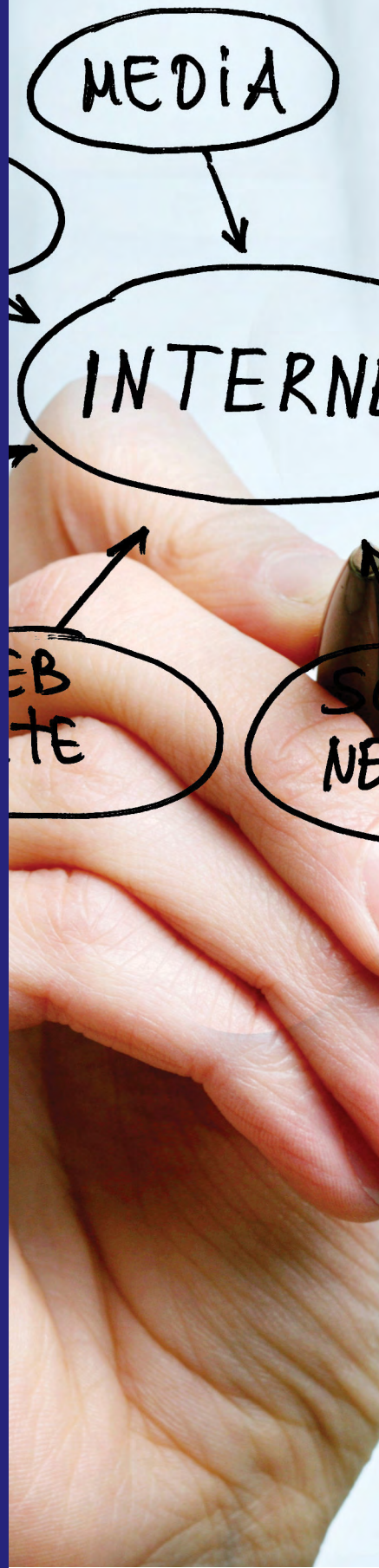
server





آموزش و فرهنگ سازی

گروه آموزش و فرهنگ سازی شرکت امن گستر افتخار دارد با استفاده از تجارب علمی و عملی خود در حوزه فناوری اطلاعات به ویژه امنیت اطلاعات و همچنین بهره گیری از کادر مجرب به برگزاری دوره های آموزشی بپردازد.



خدمات آموزشی

- برگزاری دوره های آموزشی بصورت عمومی
- برگزاری آموزش های درون سازمانی
- تدوین و برگزاری دوره ها بر اساس نیازهای سازمانی
- برگزاری دوره های آموزشی Online
- تولید محتوای الکترونیکی دوره های آموزشی مورد درخواست
- برگزاری همایش های تخصصی در حوزه امنیت شبکه و اطلاعات
- برگزاری سمینارهای فرهنگ سازی امنیتی درون سازمانی

خدمات فرهنگ سازی

- تهیه کلیپ های فرهنگ سازی امنیتی متناسب با نیازهای سازمانی
- طراحی و چاپ پوسترهای فرهنگ سازی امنیتی
- تهیه بسته های فرهنگ سازی شامل مقاله، بروشور و دیگر اقلام مورد درخواست

انتشارات

- ترجمه و انتشار استانداردهای امنیت اطلاعات نظیر سری ISO27000
- تالیف و انتشار کتاب های فرهنگ سازی امنیتی متناسب با وضعیت امنیتی سازمان ها

مهمترین مزایای دوره های گروه آموزشی

- صدور گواهینامه های آموزشی سرمیزی سیستم مدیریت امنیت اطلاعات با اعتبار IRCA انگلستان
- اعطای گواهینامه های آموزشی با مجوز واحد امنیت سازمان فناوری اطلاعات (نما)
- اعطای گواهینامه های آموزشی با مجوز سازمان نظام صنفی رایانه ای و شورای عالی انفورماتیک
- برگزاری اغلب دوره ها بصورت عملی و کارگاهی
- تأمین امکانات مناسب جهت پذیرایی مناسب برای مخاطبین
- بهره گیری از کلاس ها با تجهیزات فنی لازم
- استفاده از اساتید حرفه ای با تجارب عملی در حوزه فناوری اطلاعات
- امکان تخفیفات مناسب برای مشتریان گروه شرکت های پیام پرداز

دارای مجوز
نمای آموزش از
سازمان فناوری اطلاعات

نام دوره	کد دوره	نام دوره	کد دوره	نام دوره	کد دوره
دوره های Linux		دوره های استاندارد و مدیریت امنیت		دوره های کامپتیا	
Linux Essential	LIN01	آشنایی با اصول و مبانی مدیریت امنیت اطلاعات ISO27001:2013	STM01	Network +	CAP01
LPIC-1	LIN02	اصول استقرار سیستم مدیریت امنیت اطلاعات ISO27001:2013	STM02	Security +	CAP02
LPIC-2	LIN03	تشریح الزامات سیستم مدیریت امنیت اطلاعات ISO27001:2013	STM03	دوره های EC-Council	
LPIC-3	LIN04	آشنایی با تغییرات ISO27001:2013 نسبت به ویرایش 2005	STM04	CSCU (امنیت کاربری کامپیوتر)	ECC01
RHCE	LIN05	مدیریت ریسک در امنیت اطلاعات ISO 27005	STM05	CEH-v8.0 (هکری قانونمند)	ECC02
RHCSS	LIN06	سر ممیزی سیستم مدیریت امنیت ISO 27001:2013	STM06	ECSA-v8.0 (تحلیل گری امنیتی)	ECC03
RHCVA	LIN07	سر ممیزی ISO 27001:2013	STM07	CHFI-v8.0 (پیگیری جرایم قانونی)	ECC04
دوره های میکروتیک		تشریح الزامات و ممیزی داخلی سیستم مدیریت تداوم کسب و کار ISO 22301	STM08	ENSA (مدیر امنیت شبکه)	ECC05
MTCNA	MIK01	پیاده سازی سیستم مدیریت تداوم کسب و کار بر اساس ISO 27031	STM09	ECIH (مدیریت حوادث امنیتی)	ECC06
MTCRE	MIK02	مدیریت حوادث امنیت اطلاعات ISO27035:2011	STM10	دوره های حرفه ای امنیت شبکه	
MTCWE	MIK03	ارزیابی اثربخشی سیستم مدیریت امنیت اطلاعات ISO27004:2009	STM11	امنیت شبکه ویژه متخصصان IT	SEC01
MTCTCE	MIK04	PCI-DSS Foundation	STM12	BSDA (Berkeley Software Distribution Associate)	SEC02
MTCUME	MIK05	NIST SP-800	STM13	CISSP	SEC03
MTCINE	MIK06	دوره های مایکروسافت		CISM	SEC04
دوره های Juniper		MCSA: Configuring Windows 8 (optional)	MIC01	اصول و مفاهیم رمزنگاری	SEC05
Juniper Networks Certified Associate Junos (JNCIA-Junos)	Jun01	MCSA: Installing & Configuring Windows server 2012	MIC02	زیرساخت کلید عمومی PKI	SEC06
Juniper Networks Certified Specialist Security (JNCIS-SEC)	Jun02	MCSA: Configuring Advanced Windows server 2012 Services	MIC03	تشریح شبکه های خصوصی مجازی (VPN)	SEC07
Juniper Networks Certified Professional Security (JNCIS-SEC)	Jun03	MCSE: Designing & Implementing a Server Infrastructure	MIC04	بررسی ادله دیجیتال و قوانین فضای سایبری کشور ۱-	SEC08
Juniper Networks Certified Expert Security (JNCIS-SEC)	Jun04	MCSE: Implementing an Advanced Server Infra	MIC05	بررسی ادله دیجیتال و قوانین فضای سایبری کشور ۲-	SEC09
دوره های مجازی سازی		Exchange Server 2016	MIC06	تحلیل بدافزار	SEC10
VMware Certified Professional (VCP)	VMW01	Microsoft TMG	MIC07	کدنویسی امن	SEC11
VMware Virtual Desktop Infra (VDI)	VMW02	دوره های CISCO		مرکز عملیات امنیت SOC ۱-	SEC12
VMware Vcloud (VCAP-CIA)	VMW03	CCNA	CIS01	مرکز عملیات امنیت SOC ۲-	SEC13
VMware Certified Design Expert (VCDX)	VMW04	CCNP (R&S&T)	CIS02	تست نفوذ پیشرفته وب	SEC14
سمینارهای تخصصی		CCNA Security	CIS03	تست نفوذ شبکه های بی سیم	SEC15
طراحی امن شبکه های کامپیوتری	-	CCNP Security (4 courses)	CIS04		
امنیت برای کاربران سازمان	-				
Mobile Hacking	-				





تهران . خیابان شریعتی . بالاتر از پل سیدخندان .
خیابان مجتبایی . کوچه دیانا . پلاک ۴۴ . واحد ۶

تلفن : (۰۲۱) ۲۲ ۸۷ ۶۳ ۰۰
نمبر : (۰۲۱) ۲۲ ۸۷ ۶۳ ۰۰