



DOURAN GROUP

Security & Network Solutions

Security • Network • ERP • Portal • Training



فهرست فعالیت‌های شرکت نوآوران ارتباطات دوران

حوزه	عنوان	شرح	
راهکارهای حوزه امنیت	SOC	مشاوره، طراحی و پیاده سازی مرکز عملیات امنیت شبکه	
	ISMS	مشاوره، طراحی، پیاده سازی و آموزش ISMS مبتنی بر استاندارد ISO27001	
	Network Security	مشاوره، طراحی و پیاده سازی راهکارهای ایمن سازی شبکه	
	Pentest	آزمون نفوذپذیری سازمانها با استفاده از شبیه سازی حملات واقعی نفوذگران و ارائه گزارشات نفوذپذیری	
	Scada Security	مشاوره، طراحی و پیاده سازی راهکارهای ایمن سازی شبکه های صنعتی	
	CERT/CSIRT	مشاوره، طراحی و پیاده سازی مرکز واکنش به حوادث امنیتی (گوهرهای سازمانی)	
راهکارهای حوزه شبکه	NOC	طراحی و پیاده سازی مرکز عملیات شبکه جهت مانیتورینگ شبکه برای شناسایی و رفع مشکلات شبکه	
	DataCenter	مشاوره، طراحی، تامین تجهیزات، نصب و راه اندازی مراکز داده	
	Virtualization	مشاوره، طراحی، تامین تجهیزات و پیاده سازی راهکارهای مجازی سازی	
	Network Support	نگهداری و پشتیبانی شبکه	
	Cloud Computing	مشاوره، طراحی، تامین تجهیزات و پیاده سازی راهکارهای رایانش ابری	
	VoIP-VC	مشاوره، طراحی و پیاده سازی مراکز VoIP و ویدئو کنفرانس	
تامین تجهیزات سخت افزاری و نرم افزاری	طراحی، پیاده سازی و پشتیبانی زیرساخت اکتیو و پسیو مراکز داده		
	سرور و تجهیزات پردازشی	Server and Processing Equipment	
	سوییچ و مسیریاب	Switch and Router	
	سیستم های توزیع کننده ترافیک شبکه / برنامه کاربردی	Distributed Systems, Network Traffic / Application	
	بازیابی اطلاعات و دریافت نسخه پشتیبان	Backup and Recovery	
	امنیت	Security	
	نظارت و پایش	Supervision and Monitoring	
	تامین نرم افزار با لایسنس معتبر	Software Licensing	
	راهکارهای پورتال سازمانی	تحول و نگرش مدرن در مفهوم پورتال با رویکرد یکپارچه به کسب و کار الکترونیک	
		سامانه مدیریت محتوای سازمانی	سامانه فرمساز و فرآیند ساز
سامانه مدیریت وب سرویس		سامانه گزارش ساز	
سامانه فروشگاه ساز		سامانه احراز هویت متمرکز	
آموزش	ارائه برترین کیفیت خدمات آموزشی مهارت محور در حوزه های		
	Network	Security	
	IT Management	Virtualization	
	Servers & Storage	DevOps	

گروه دوران

گروه دوران از موفق ترین مجموعه شرکت های دانش بنیان باهدف ارائه محصولات و خدمات متنوع در زمینه فناوری اطلاعات و ارتباطات تأسیس شد. پس از گذشت بیش از بیست سال از زمان تأسیس، نتایج درخشانی در کارنامه این گروه به ثبت رسیده است. ساماندهی کادری متشکل از ۵۰۰ نفر، بهره گیری از دانش روز دنیا، فعالیت گسترده در زمینه تولید و ارائه نرم افزار و تجهیزات و خدمات تخصصی در چارچوب هفت گروه Security, Network, Telecom, ERP, AI, Portal, Training با افتخار اعلام می کنیم حضور ۵ تیم تولید، فنی، دستگاهی، بازرگانی و آموزشی در قالب ۱ گروه و همکاری نزدیک با شرکت های معتبر بین المللی، توان فنی و اجرایی بالایی را برای گروه دوران در زمینه اجرای پروژه های بزرگ ملی فراهم نموده است. به منظور خدمت رسانی بهتر به وزارتخانه ها، ادارات، مؤسسات و شرکت ها، کارکنان این مجموعه متشکل از مدیران، متخصصان با سابقه و حرفه ای با تکیه بر کار تیمی و تخصص خود و با توجه به نیاز بازار، به تولید، ارائه و به روز رسانی محصولات و راهکارها می پردازند. «اتصال، امن سازی و مکانیزاسیون سازمان ها»، To Connect, Secure & Automate Organization

برخی از افتخارات گروه دوران

- انتخاب به عنوان شرکت دانش بنیان از سوی معاونت علمی و فناوری ریاست جمهوری
- مجری بزرگ ترین پروژه امنیت اطلاعات کشور
- مجری بزرگ ترین پروژه ERP داخلی کشور
- کسب رتبه برتر در بخش نرم افزار و امنیت شبکه کامپی ۲۵
- عضو پانصد شرکت بزرگ ایران در سال مالی ۹۶ و ۹۷ طبق رتبه بندی شرکت های برتر سازمان مدیریت صنعتی

- دارای گواهینامه بین المللی ISO 9001
- کسب رتبه ۱ از سوی شورای عالی داده ورزی (انفورماتیک) کشور در ۵ رشته مختلف: «تولید نرم افزار»، «شبکه»، «امنیت»، «مشاوره و پشتیبانی» و غیر Mainframe
- رتبه ۱ گواهی افتخار، در حوزه مشاوره و استقرار ISMS، ارزیابی امنیتی، امنیت فیزیکی و ...
- دریافت لوح تقدیر برتر در جشنواره ملی ارتباطات و فناوری اطلاعات سال های ۹۱، ۹۲، ۹۳، ۹۴، ۹۵، ۹۶ و ۹۷
- تولیدکننده یکی از قوی ترین فایروال های بومی (DS Gate)، نصب شده در حساس ترین سازمان های کشور
- تولیدکننده اولین IPS 40G پهنای باند اینترنت برترین شرکت در زمینه ارائه تجهیزات امنیتی خارجی با گواهینامه (License) و گارانتی معتبر
- عضو بانک اطلاعاتی صادرکنندگان کشور و اتحادیه صادرکنندگان نرم افزار
- دریافت لوح و تقدیر برگزیده مدیر جهادی از سومین همایش «مدیریت جهادی کشور»
- ارائه خدمات به بیش از چهار هزار مشتری در پانصد و پنجاه شهرستان کشور و چندین کشور خارجی
- دارای بیش از «۳۰» همکار خارجی برای ارائه راهکارهای به روز به مشتریان
- حضور در بیش از ۱۰ دوره مختلف در نمایشگاه های Cebit کشور آلمان و Gitex دبی
- حضور مستمر در بیش از «۸۰» نمایشگاه معتبر داخلی طی سال های گذشته
- عضو سازمان نظام صنفی رایانه ای کشور
- دارای گواهینامه صلاحیت ارائه خدمات در حوزه پدافند سایبری و آموزش
- دارای گواهی صلاحیت ایمنی پیمانکاران

Pen Test

تست نفوذپذیری

آزمون نفوذپذیری، فرآیند ارزیابی معیارهای امنیتی است. معیارهای امنیتی از لحاظ ضعف طراحی، مشکلات فنی و آسیب‌پذیری‌ها بررسی گردیده و نتایج آن در قالب گزارشی کامل، به مدیران و نیروهای فنی ارائه می‌گردد. در این روش‌ها استفاده از به‌روزترین تکنیک‌های تست نفوذ، حملات سایبری واقعی شبیه‌سازی می‌شود تا به این وسیله سطح امنیت یک شبکه یا سیستم مشخص گردد. این امر به سازمان‌ها کمک می‌کند تا با تشخیص به موقع، از دسترسی و آسیب‌رسانی هک‌های واقعی به سرمایه‌های سازمان جلوگیری نمایند.

مزایای بهره‌گیری از خدمات دوران

- بکارگیری تیم فنی توانمند و با تجربه
- بهره‌گیری از ابزارهای تجاری و غیرتجاری
- استفاده از تکنیک‌ها و ابزارهای خصوصی و Oday
- بررسی عدم انطباق وضعیت امنیتی سازمان با استانداردها
- ارائه راهکارهای جامع به منظور برطرف ساختن آسیب‌پذیری‌ها
- ارزیابی بر اساس متدولوژی‌های تست نفوذ از قبیل OWASP، ISSAF، OSSTMM
- بهره‌گیری از تجربه‌های به دست آمده از اجرای پروژه‌های بزرگ برای شرکتها و سازمانهای بانکی، پرداخت الکترونیک (PSP)، نفت، ارتباطات و فناوری اطلاعات، خودروسازی، آب و برق و ..

Network Security Solutions

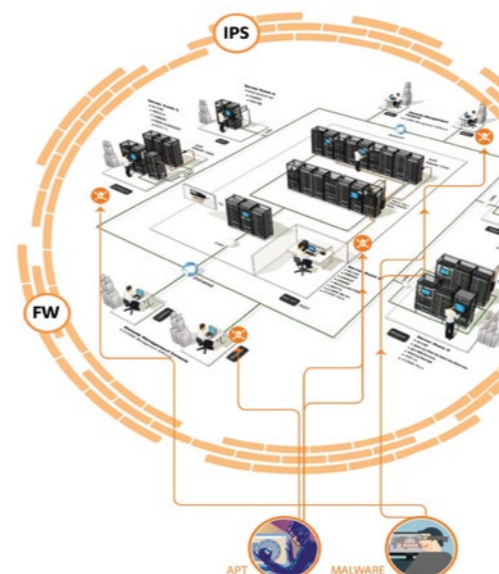
راهکارهای امنیت شبکه

زمانیکه امن‌سازی پیشرفته شبکه برای سازمان‌ها مطرح می‌شود، راهکارهای گروه دوران در این زمینه دارای مزایای فراوانی است که با اتکاء به تجارب اندوخته شده از اجرای پروژه‌های ملی و بزرگ به دست آمده است. گروه دوران با بهره‌گیری از برترین و به روزترین محصولات و راهکارهای امنیتی موجود، از توان بالایی جهت طراحی، توسعه و پیاده‌سازی بستری ایمن برای انتقال اطلاعات سازمانها بهره‌مند می‌باشد.

محصولات و راهکارهای دوران

- مقابله با حملات تکذیب سرویس (DDoS Mitigation)
- هانی پات و هانی نت
- حملات نسل جدید (APT)
- شناسایی و مقابله با C&C و Botnet
- فایروالهای نسل جدید (NG Firewall)
- سیستم‌های تشخیص/پیشگیری از نفوذ (IPS)
- فایروال برنامه‌های تحت وب (WAF)
- پایش فعالیت‌های پایگاه داده (DAM)
- فایروال پایگاه داده (DBF)
- کنترل دسترسی به شبکه (NAC)
- پیشگیری از دست رفتن داده‌ها (DLP)
- رمزنگاری داده‌ها با استفاده از HSM و PKI
- ...

- ### متدولوژی دوران
- شناخت دارایی‌های و عناصر شبکه
 - آنالیز و تحلیل ریسک‌های امنیتی
 - طراحی بر اساس استانداردهای ملی و بین‌المللی
 - تهیه و تامین تجهیزات سخت‌افزاری و نرم‌افزاری
 - پیاده‌سازی طرحهای امنیتی
 - آموزش و آگاهی رسانی
 - ارائه خدمات پشتیبانی



مزایای بهره‌گیری از محصولات و خدمات دوران

- دارای تجربه اجرای بزرگترین پروژه SOC کشور
- بهره‌گیری از تیم متخصص و مجرب بومی
- بکارگیری از محصولات امنیتی بومی
- سیستم مدیریت رویداد و اطلاعات امنیتی (Dsiem)
- سیستم مدیریت یکپارچه تهدید (DSGate)
- سیستم شناسایی/پیشگیری نفوذ (DIPS)
- سامانه مدیریت پیشخوان خدمت (dService Desk)
- داشبورد امنیتی (dDashboard)

وظایف مرکز عملیات امنیت

- شناسایی حوادث امنیتی
- شناسایی موارد تخطی از خط‌مشی‌ها
- شناسایی فعالیت‌های جعل هویت، نفوذ و کلاهبرداری
- تحلیل‌های کارآگاهی
- اعمال تدابیر لازم برای مقابله با حملات
- ایجاد خطوط مبنا و روند طبیعی

عمده مشتریان مرکز عملیات امنیت

- مؤسسات مالی و اعتباری
- بانک‌ها
- سازمان‌های بزرگ دولتی
- زیرساخت‌های صنعتی حیاتی



تأمین امنیت جامع



پایش بلادرنگ وضعیت امنیتی



شناسایی حملات ناشناخته
حفاظت در برابر نسل جدید تهدیدات



هشدار و اعلام حوادث امنیتی



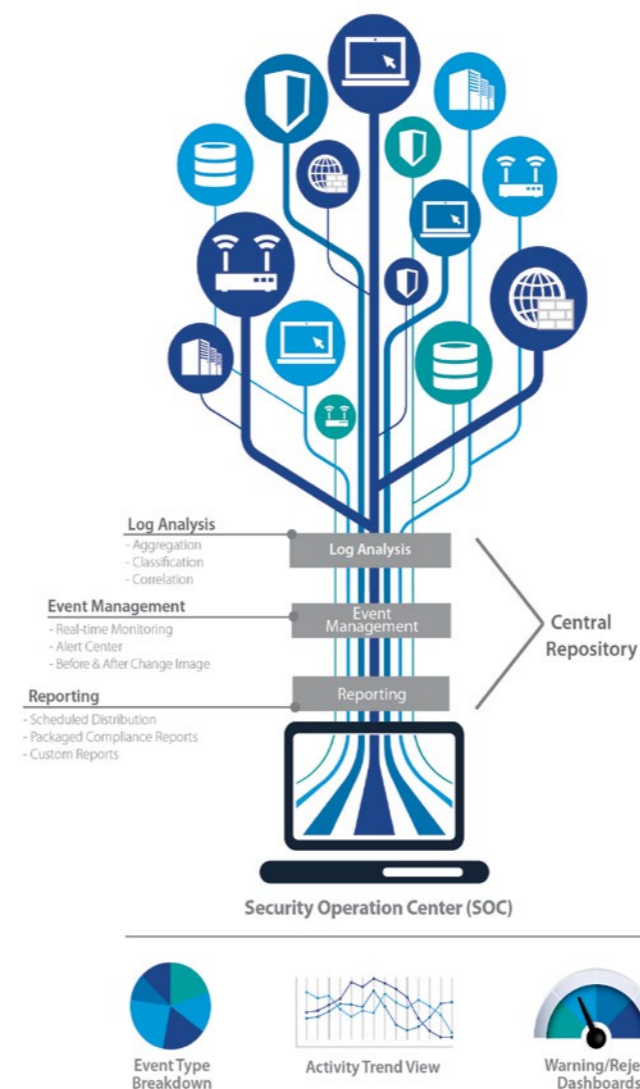
ایجاد گزارش‌های امنیتی سفارشی



SOC

Security Operation Center

مرکز عملیات امنیت



برای مقابله با حملات و تهدیدات در فضای مجازی استفاده از راهکارهای امنیتی مختلف از قبیل راه اندازی انواع فایروال، آنتی ویروس، سامانه‌های شناسایی و پیشگیری نفوذ، احراز هویت متمرکز و غیره در کنار بکارگیری انواع روش‌های مستحکم سازی اجتناب ناپذیر است. به علاوه ممکن است گروه‌های مجزا عهده‌دار مدیریت ابزارهای امنیتی مختلف باشند.

در این صورت شناسایی و تجمیع جزئیات یک حمله به صورت بلادرنگ بسیار مشکل خواهد بود و تحلیل شواهد قانونی بعد از وقوع حمله بسیار کند انجام خواهد شد. مرکز عملیات امنیت ضمن مرتفع کردن مشکلات فوق، محلی برای پایش بلادرنگ و همبستگی امنیتی رویدادنامه‌ها، تجزیه و تحلیل و پاسخگویی به حوادث امنیتی به صورت متمرکز است.

SCADA Security

امنیت سیستم‌های صنعتی

سیستم‌های کنترل صنعتی به منزله هسته مرکزی کنترل و مانیتورینگ، زیرساخت حیاتی نظیر شبکه‌های انتقال و توزیع برق، نیروگاه‌های هسته‌ای، پالایشگاه‌ها، شبکه‌های آب، کارخانه‌های نفت و گاز می‌باشند. اطلاعات و گزارشات مدیریتی، از طریق اینترفیس‌های مختلف به شبکه SCADA منتقل می‌شود. اما با توجه به قدیمی بودن این سیستم‌ها، به امنیت آنها توجه چندانی نشده است. از سال ۲۰۰۰ میلادی به بعد حجم حملاتی که متوجه سیستم‌های SCADA شده است بسیار بالا بوده و روند افزایشی داشته است. با این که اغلب سازمان‌ها ادعا می‌کنند که سیستم SCADA آنها به شبکه متصل نمی‌باشد، تخمین زده می‌شود که بین ۸۰ تا ۹۰ درصد سیستم‌های SCADA به شبکه‌های کامپیوتری سازمان متصل می‌باشد. بنابراین مهاجمین می‌توانند حملات خود را متوجه سیستم‌های SCADA نمایند.

خدمات دوران جهت ایمن سازی شبکه‌های SCADA

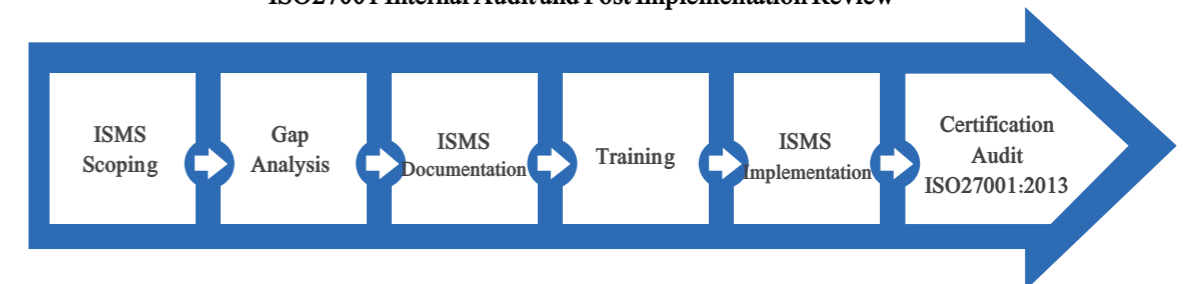
- بررسی معماری موجود از لحاظ امنیتی
- ارزیابی آسیب پذیری سیستم‌های کنترلی
- ارائه راهکارهای عملیاتی با هدف ایمن‌سازی
- پیاده‌سازی امنیت براساس معماری‌های استاندارد
- بررسی عدم انطباق با استانداردهایی از قبیل: ISA99/IEC 62443، CPNI Security Guides.82-NIST 800

ISMS

سیستم مدیریت امنیت اطلاعات

در جهان امروز، اطلاعات کلیدی ترین دارایی و سرمایه در جهت رشد و موفقیت هر سازمان است. به همین منظور باید اقدامات لازم برای حفظ امنیت این سرمایه مهم صورت گیرد. سیستم مدیریت امنیت اطلاعات با راه اندازی فرآیند مدیریت ریسک، محرمانگی، پیکارچگی و در دسترس بودن اطلاعات را تضمین می‌کند و طرفهای ذینفع را از وجود مدیریت کافی بر ریسک‌های امنیتی موجود، مطمئن می‌سازد. طراحی و پیاده سازی سیستم مدیریت امنیت اطلاعات در سازمان‌ها، تحت تاثیر نیازها و اهداف، الزامات امنیتی، فرآیندهای بکار گرفته شده و اندازه و ساختار سازمان، قرار دارد. انتظار می‌رود پیاده سازی یک سیستم مدیریت امنیت اطلاعات، با نیازهای سازمان متناسب شود.

ISO27001 Internal Audit and Post Implementation Review



مزایای بهره‌گیری از خدمات دوران

- کسب رتبه یک نما در حوزه ارائه خدمات مشاوره و استقرار ISMS از سازمان فناوری اطلاعات ایران
- پیاده سازی ISMS در مجموعه دوران و کسب گواهینامه بین المللی ISO27001 از SINCERT ایتالیا
- در کنار هم داشتن چهار تیم فنی امنیت شبکه، امنیت سیستمی، طراحان ابزارهای امنیتی و بازرگانی خارجی، امکان ارائه و پیاده‌سازی راهکارهای خاص امنیتی را برای سازمان‌های طرف قرارداد جهت پیاده‌سازی هرچه بهتر سیستم مدیریت امنیت اطلاعات میسر نموده است
- بهره‌گیری از کارمندان متخصص با مدارک معتبر ملی و بین المللی در زمینه سیستم‌های امنیتی
- مشاوره، طراحی و استقرار سیستم مدیریت امنیت اطلاعات برای شرکت‌های تابعه از صنایع مختلف از قبیل: وزارت نفت، وزارت نیرو، وزارت ارتباطات و فناوری اطلاعات، بانکی، خودروسازی، صدا و سیما و ...



CERT/CSIRT

مرکز واکنش به حوادث امنیتی

مرکز واکنش به حوادث امنیتی، یک تیم امنیتی و یا به عبارت دقیق‌تر، یک سازمان امنیتی است که وظیفه دریافت، بررسی و پاسخگویی به رویدادها و حوادث امنیتی را بر عهده دارد. در حال حاضر در کشور ما این مراکز در قالب گروه‌های واکنش به رخدادهای امنیتی (گوهر) در سازمانها در حال راه اندازی می باشند.

مزایای راه اندازی مرکز CERT

- رسیدگی به آسیب‌پذیری‌ها و حوادث شناسایی شده
- بررسی تنظیمات امنیتی و شناسایی نقاط نفوذ
- بررسی و آنالیز ریسک‌های موجود در یک سازمان
- مدیریت حوادث و بازیابی بعد از وقوع حادثه
- مشاوره امنیتی و ارائه آموزش‌های لازم
- ارزیابی امنیتی ابزارهای مورد استفاده
- تحلیل حملات و همکاری با تیم SOC به منظور بهبود آنالیز رخدادهای

متدولوژی دوران

- تهیه طرح استراتژیک تیم
- جمع‌آوری اطلاعات مورد نیاز و مرتبط
- طراحی اهداف کلی تیم
- ایجاد ارتباط بین هدف تیم و طرح عملیاتی
- پیاده سازی تیم
- ارزیابی تاثیرگذاری تیم

مزایای بهره گیری از خدمات دوران

- همکاری نزدیک با شرکتهای معتبر بین المللی
- تهیه استراتژی لازم جهت پیاده‌سازی
- پیاده سازی با بهره گیری از بهترین ابزارها و روش‌ها
- ایجاد نشریات مربوط به مدیریت حوادث و همچنین راهنماهایی به منظور آگاهی‌رسانی
- آموزش پرسنل کارفرما

Network Support

پشتیبانی شبکه

امروزه، اکثر سازمانهای دولتی و خصوصی برای کاهش هزینه‌های سازمانی خود، پشتیبانی و نگهداری از شبکه، تجهیزات رایانه‌ای و پایگاه‌های داده را برون سپاری می نمایند. شرکت دوران با تشکیل تیم‌های فنی و پشتیبانی متخصص توانسته است این نیاز بازار را نیز به خوبی پاسخ دهد.

برخی از فعالیت‌های قابل اجرا برای سازمانهای مختلف در حوزه پشتیبانی و نگهداری به شرح زیر می باشد:

- پشتیبانی از کلیه نرم افزارها، سخت افزارهای اکتیو و پسیو شبکه
- نگهداری رایانه‌ها، پرینترها، اسکنرها، لپ‌تاپ و سایر تجهیزات موجود در سازمان‌ها
- تامین نیرو، استقرار در محل سازمان و مدیریت و راهبری آنها
- پیگیری و راهبری کارها طبق شرایط مورد نظر کارفرمایان
- مستندسازی و ارائه گزارشات مربوط به تست شبکه، رایانه‌ها و تجهیزات موجود در سازمان
- مدیریت قطعات و تجهیزات مصرفی و ارائه گزارشات مربوطه
- ارائه گزارشات هفتگی، ماهانه و سالانه طبق فرمت‌های مورد نظر کارفرمایان
- بازنگری فرایندهای کار با رویکرد افزایش بهره‌وری با هماهنگی کارفرمایان
- تولید و ارائه شناسنامه تجهیزات و به‌روز رسانی مستمر آنها

NOC

Network Operation Center

مرکز عملیات شبکه

مرکز عملیات شبکه، مکانی مرکزی برای مانیتورینگ هوشمند ابزارها و تجهیزات شبکه یک سازمان می باشد که بصورت پیوسته و خودکار، به شناسایی و رفع خطاها، مدیریت پیکربندی و مانیتورینگ کارایی شبکه می پردازد و از این طریق، کارایی و دسترس پذیری شبکه را به طور قابل توجهی بهبود می بخشد. گروه دوران با توجه به سابقه مدیریت و پشتیبانی شبکه های گسترده اقدام به ارائه خدمات مشاوره، طراحی، تامین تجهیزات و پیاده سازی مراکز عملیات شبکه می نماید.



وظایف اصلی مرکز عملیات شبکه

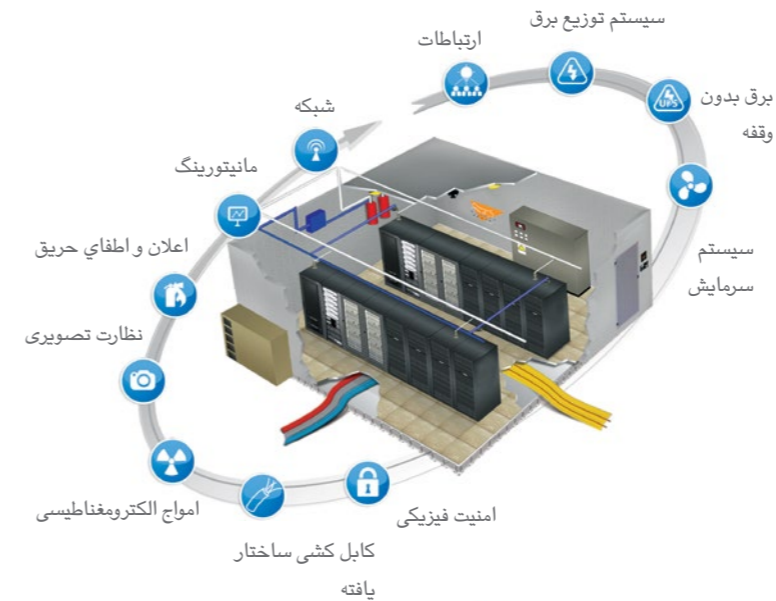
- مانیتورینگ ترافیک شبکه
- مدیریت مشکلات و خطاهای شبکه
- مدیریت پیکربندی شبکه
- مدیریت درخواست ها
- پشتیبانی

مزایای ایجاد مرکز عملیات شبکه

- مانیتورینگ یکپارچه و مرکزی خطاهای شبکه و در حد امکان، جلوگیری از وقوع آنها
- افزایش چشمگیر دسترس پذیری شبکه
- افزایش کارایی شبکه
- کاهش خطاها و مشکلات شبکه
- ایجاد ابزاری جهت به حداقل رساندن ضرر و زیان تجاری
- نگهداری امن، بهینه و بلند مدت سوابق رویدادهای شبکه
- کاهش هزینه های مدیریت شبکه
- به حداقل رساندن ریسک قطعی سیستم ها و تجهیزات شبکه

Data Center

مرکز داده



مزایای پیاده سازی مرکز داده Data Center

- یکپارچه سازی در محیط و مدیریت فضای فیزیکی
- ایجاد امنیت فیزیکی و الکترونیکی بالا
- مقابله با افزونگی و تکرار اطلاعات و اعمال سیاستهای ذخیره و بازاریابی اطلاعات
- بالابردن سرعت پردازش و انتقال اطلاعات
- سهولت در توسعه و بکارگیری فناوری های جدید با حفظ یکپارچگی
- پرسنل کمتر و متخصص تر جهت ارائه خدمات پشتیبانی
- امکان اعمال سیاستهای مدیریتی سریع و به موقع

خدمات گروه دوران در زمینه مرکز داده

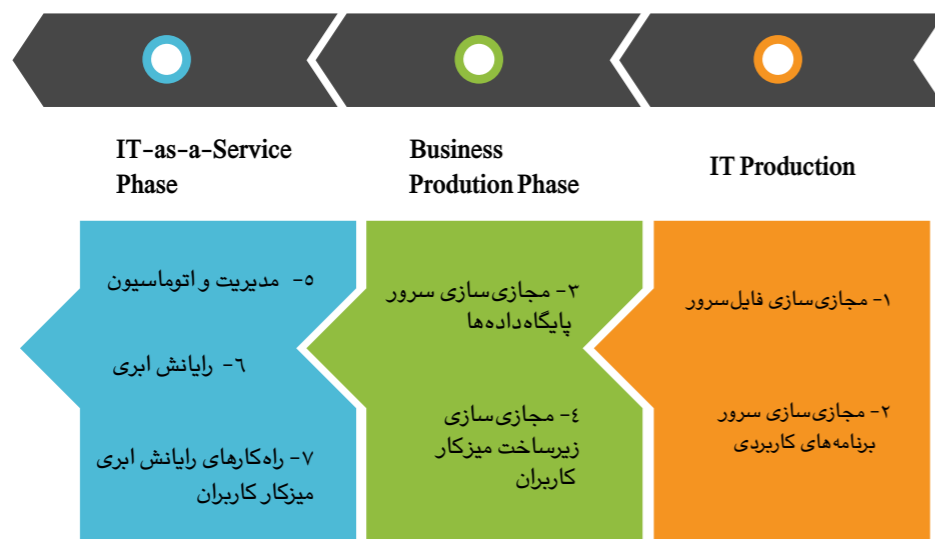
بررسی و شناخت	طراحی	تامین تجهیزات
<ul style="list-style-type: none"> ■ ارزیابی مرکز داده ■ نیازسنجی و شناسایی اهداف ■ شناسایی محدودیت های طراحی ■ بررسی زیرساخت فیزیکی و ارتباطی ■ مستند سازی 	<ul style="list-style-type: none"> ■ طراحی بر اساس استانداردهای: TIA942, BICSI, ISO-27001 ■ طراحی بر اساس مقررات ملی ■ طراحی بر اساس برندهای مختلف ■ تهیه اسناد مناقصه ■ تهیه LOM و LOS 	<ul style="list-style-type: none"> ■ تامین تجهیزات داخلی و خارجی
آموزش	بهره برداری و تحویل	پیاده سازی
<ul style="list-style-type: none"> ■ آموزش حین کار ■ آموزش راهبری مرکز داده ■ آموزش و اطلاع رسانی به پرسنل 	<ul style="list-style-type: none"> ■ بهره برداری از مرکز داده ■ تست و آزمایش زیرساخت ■ تحویل موقت ■ راهبری مرکز داده به صورت موقت ■ تحویل نهایی ■ مانیتورینگ مرکز داده 	<ul style="list-style-type: none"> ■ بکارگیری تیم مجرب فنی ■ استفاده از متدولوژی های مدیریت پروژه ■ نظارت بر اجرای صحیح مرکز داده

Cloud Computing

رایانش ابری

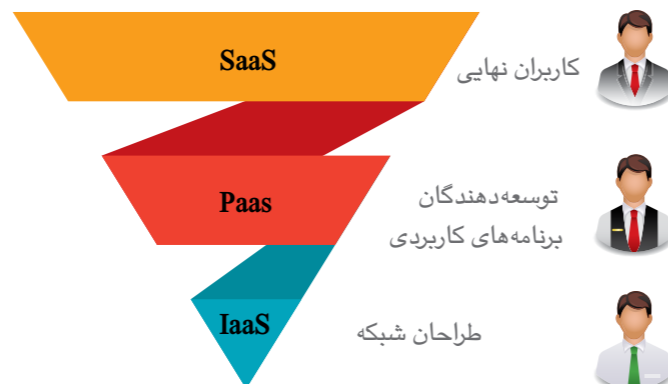
کارشناسان گروه دوران با توجه به تجربیاتی که از اجرای پروژه‌های مجازی‌سازی و زیرساخت‌های شبکه در سازمانهای بزرگ بدست آورده‌اند، آماده ارائه خدمات در خصوص ایجاد ابر خصوصی برای تمامی شرکتها و سازمانها می‌باشند. این خدمات در چارچوب مشاوره، طراحی، تامین تجهیزات، پیاده سازی و پشتیبانی می‌باشد.

مجازی سازی تا رایانش ابری



مزایای اصلی رایانش ابری

- سرعت دسترسی به منابع
- کاهش هزینه های سرمایه ای
- عدم وابستگی به سخت افزار و مکان
- قابلیت اطمینان بالا
- قابلیت اندازه گیری
- امنیت
- نگهداری



Virtualization

مجازی سازی

خدمات گروه دوران



نیاز امروزه سازمان ها تنها مجازی سازی سرور ها و سرویس ها نیست، بلکه مجازی سازی کلیه زیرساخت مراکز داده اعم از زیر ساخت های شبکه مانند سوئیچ ها، روترها، فایروال ها و یا زیر ساخت های ذخیره سازی می باشد.

مجازی سازی سرور (Server Virtualization)

مجازی سازی سرور روشی برای نصب و اجرای همزمان و مستقل چندین سیستم عامل بر روی سرور سخت افزاری می باشد. این مکانیزم علاوه بر صرفه جویی انرژی، افزایش بهره وری از سخت افزار، کاهش دما و مصرف برق مراکز داده و استفاده بهتر از فضای دیتا سنترها را نیز در پی خواهد داشت.

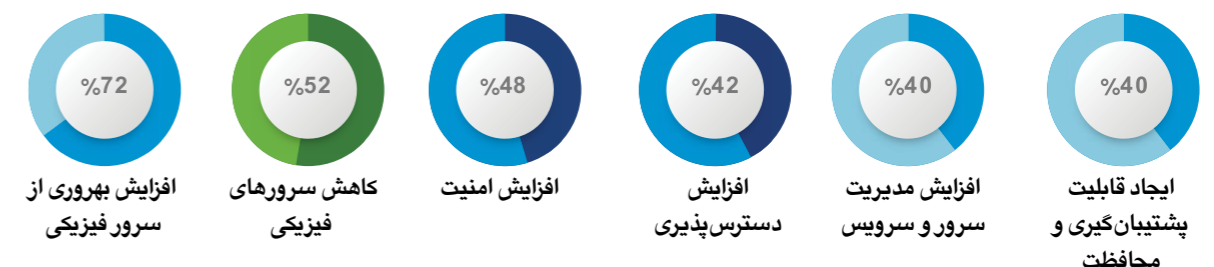
مجازی سازی شبکه (Network Virtualization)

در مجازی سازی شبکه کلیه زیرساخت شبکه اعم از سوئیچ ها، روترها و فایروال ها نیز به صورت مجازی نصب و پیکربندی می شود. این مدل از مجازی سازی سازمان را از وابستگی به تجهیزات سخت افزاری می رهااند.

مجازی سازی دسکتاپ (Virtual Desktop Infrastructure)

در این روش ابری از سیستم های دسکتاپ ایجاد شده و کاربران انتهایی قادر خواهند بود با هر سیستم عامل و از هر مکان به دسکتاپ خود با کمترین پهنای باند دسترسی پیدا کنند. مجازی سازی دسکتاپ، مفهوم تفکیک منطقی دسکتاپها از ماشین فیزیکی است.

مجازی سازی



Consulting, Designing and Implementation

مشاوره، طراحی و پیاده‌سازی

Cisco ACI

Cisco Application Centric Infrastructure (ACI) یک راه‌حل شبکه (SDN) با نرم‌افزار تعریف شده است که برای دیتا سنترها طراحی می‌شود. Cisco ACI اجازه می‌دهد تا زیرساخت شبکه بر اساس سیاست‌های شبکه مثل ساده‌سازی، بهینه‌سازی و تسریع چرخه عمر استقرار برنامه تعریف شود.

Cisco DNA Center

Cisco Digital Network Architecture Center یا به اختصار Cisco DNA Center، یک برنامه کاربردی برای مدیریت شبکه به صورت متمرکز بوده و موجب تسهیل آن می‌شود؛ در واقع استفاده از این تکنولوژی موجب پیشرفت سریع‌تر دنیای IT و همچنین کاهش هزینه‌ها با استفاده از خودکارسازی می‌گردد و آنالیز شبکه باعث بهبود عملکرد شبکه و امنیت و همچنین کاهش ریسک می‌شود.

Software-defined networking

شبکه مبتنی بر نرم‌افزار یا (Software Defined Networking) SDN یک معماری شبکه محسوب می‌گردد، که سطوح کنترل و داده (Control Plane, Data Plane) را از یکدیگر جدا کرده و صفحه‌ی کنترل (اطلاعات شبکه و سیاست‌گذاری) را به یک برنامه به نام کنترلر منتقل می‌نماید.

SD-WAN

شبکه‌های گسترده مبتنی بر نرم‌افزار، همان‌طور که از نام آن مشخص است (software-defined wide-area networks) از نرم‌افزار برای کنترل اتصال، مدیریت و خدمات بین مراکز داده و شعبه‌های ریموت یا نمونه‌های ابری استفاده می‌کنند. شبکه‌های گسترده مبتنی بر نرم‌افزار یا همان SD-WAN سطح کنترل را از سطح داده جدا می‌کند.

(Cisco Secure Network Analytics (Stealth watch

آنالیز امنیتی شبکه Cisco Stealth watch به این صورت است که Cisco Stealth watch مقدار زیادی از داده‌ها را جمع‌آوری می‌کند تا بتواند دید وسیعی و همچنین امنیت درونی بزرگترین شبکه‌ها را فراهم نماید. سازمان‌های بسیاری سرمایه‌گذاری‌های سنگینی روی زیرساخت IT و امنیت خود کرده‌اند. با این حال، حملاتی انجام می‌شود و عوامل داخلی مخرب بدون اینکه عواقبی را تحمل کنند دست به تخریب می‌زنند.

VMware NSX

VMware NSX، یکی از پلتفرم‌های پیشرو برای مجازی‌سازی شبکه به شمار می‌رود که مدل عملیاتی یک ماشین مجازی را برای شبکه ارائه می‌نماید. شبکه‌های مجازی همچون ماشین‌های مجازی Computing از لحاظ برنامه‌ای به صورت مستقل از سخت‌افزارهای اصلی، آماده‌سازی و مدیریت می‌شوند. NSX، مدل شبکه را به طور کامل در نرم‌افزار بازآفرینی نموده و امکان ایجاد و آماده‌سازی هرگونه توپولوژی را از شبکه‌های ساده تا شبکه‌های پیچیده‌ی Multi-Tier میسر می‌سازد. این تکنولوژی، یک مجموعه از سرویس‌ها و فاکتورهای منطقی شبکه مانند فایروال‌ها، Load Balancer، VPN، سوئیچ‌ها، روترهای منطقی و همچنین امنیت بارکاری (Workload) را فعال می‌نماید. علاوه بر آن کاربران می‌توانند شبکه‌های مجازی جداگانه‌ای را از طریق ترکیب سفارشی این قابلیت‌ها ایجاد کنند.

Disaster Recovery Site

این سیاستها و رویه‌هاییست که بر محافظت از یک سازمان در برابر هرگونه تأثیر قابل توجه در صورت بروز حادثه متمرکز است، که ممکن است شامل خرابی دستگاه یا ساختمان، حملات سایبری یا بلایای طبیعی باشد.

DOURAN GROUP

برخی از مشتریان

وزارت ارتباطات و فناوری اطلاعات

وزارت ارتباطات و فناوری اطلاعات، ارتباطات زیرساخت، شرکت مخابرات ایران، شرکت صنایع مخابرات ایران (صاایران)، سازمان تنظیم مقررات و ارتباطات رادیویی، سازمان فناوری اطلاعات

ریاست جمهوری

افتا ریاست جمهوری، پزشک قانونی کل کشور، مرکز ملی لیزر ایران، مرکز آمار ایران، مرکز پژوهش های دانش های بنیادی (فیزیک نظری)، سازمان بورس و اوراق بهادار، سرمایه گذاری ملی ایران، سازمان انتقال خون

وزارت نیرو

وزارت نیرو، شرکت توانیر، مدیریت تولید برق بیستون، آب و فاضلاب روستائی کرمانشاه، آب و فاضلاب شهری یاسوج، توزیع برق غرب مازندران، مدیریت تولید برق گیلان، آب و فاضلاب روستائی گیلان، توزیع برق تبریز، آب و فاضلاب شهری سیستان و بلوچستان، آب منطقه ای ایلام، سازمان آب و برق خوزستان، برق منطقه ای سمنان، برق منطقه ای تهران

وزارت راه و شهرسازی

وزارت راه و شهرسازی، سازمان راهداری و حمل و نقل جاده ای، هواپیمایی جمهوری اسلامی ایران (ایران ایر)، هواپیمایی ماهان، راه و ترابری یاسوج، هواشناسی اصفهان، سازمان هواشناسی کل کشور

وزارت جهاد کشاورزی

سازمان حفاظت محیط زیست، جهاد کشاورزی کردستان، جهاد کشاورزی سیستان و بلوچستان، جهاد کشاورزی اردبیل، جهاد کشاورزی ایلام

وزارت علوم تحقیقات و فناوری

دانشگاه تهران، دانشگاه آزاد نجف آباد، دانشگاه آزاد قزوین، دانشگاه آزاد تهران جنوب، سازمان مرکزی دانشگاه آزاد، دانشگاه آزاد کاشمر، دانشگاه پیام نور فسا، دانشگاه آزاد درود، دانشگاه آزاد آیت آملی، دانشگاه آزاد تنکابن، دانشگاه شهرکرد.

دانشگاه کاشان، دانشگاه کردستان، دانشگاه دولتی ایرانشهر و...

وزارت کشور، استانداری ها

وزارت کشور، استانداری ایلام، استانداری گلستان، استانداری خوزستان، استانداری همدان، استانداری مشهد، استانداری ایلام

وزارت نفت (پالایشگاه و پتروشیمی، شرکت گاز)

وزارت نفت، شرکت ملی گاز ایران، شرکت ملی حفاری ایران، مناطق نفت خیز جنوب، نفت مناطق مرکزی، نفت مناطق مرکزی، منطقه ۹ عملیات انتقال گاز، مناطق ۲، ۵، ۶، ۸، ۱۰ عملیات انتقال گاز، پالایشگاه نفت کرمانشاه، پتروشیمی برزویه، پالایشگاه شازند اراک، بیمارستان صنایع پتروشیمی ماهشهر، پتروفناوران، نفت و گاز گچساران، نفت و گاز آقاجاری، شرکت نفت خزر، پتروشیمی زاگرس، پتروشیمی آریا ساسول.

بانکها و موسسه های مالی و اعتباری

بانک پارسیان، بانک کشاورزی، بانک ملت، بانک شهر، بانک ملی ایران، بانک تجارت، بانک کارآفرین، بانک مسکن، بانک سپه، بانک رفاه، بانک توسعه تعاون، بانک سرمایه، موسسه مالی و اعتباری ثامن، تجارت الکترونیک پارسیان، الکترونیک کارت دماوند، ایران کیش، سایان کارت، فناو کارت

وزارت صنایع

ایران خودرو دیزل، ایران خودرو خراسان، فولاد نطنز

وزارت امور اقتصاد و دارایی

اداره کل امور مالیاتی مازندران، اداره کل امور مالیاتی گیلان، اداره کل امور مالیاتی سمنان، اداره کل امور مالیاتی یاسوج، اداره کل امور مالیاتی ایلام، سازمان امور اقتصاد و دارایی سمنان، سازمان امور اقتصاد و دارایی خراسان رضوی، بانک تجارت، بانک توسعه صادرات، بیمه مرکزی جمهوری اسلامی ایران

وزارت بهداشت، درمان و آموزش پزشکی

دانشگاه علوم پزشکی شهرکرد، دانشگاه علوم پزشکی سیستان و بلوچستان، دانشگاه علوم پزشکی اهواز، دانشگاه علوم پزشکی همدان، دانشگاه علوم پزشکی گلستان، دانشگاه علوم پزشکی اراک، شرکت توزیع دارو پخش، بیمارستان فارابی



نوآوران ارتباطات دوران

تهران، خیابان خرمشهر، خیابان صابونچی، کوچه ایازی، پلاک ۶۲

www.douran.ir

تلفن: ۰۲۱ - ۴۳۵۸۰