ایمن داده شبکه

خدمات تخصصی شرکت ایمن داده شبکه

ارائه خدمات تخصصی در حوزه طراحی، تأمین، پیاده‌سازی، امن‌سازی، پایش و پشتیبانی زیرساخت‌های فناوری اطلاعات

حوزه‌های تخصصی خدمات شرکت ایمن داده شبکه

شبکه و امنیت شبکه

ارائه خدمات مشاوره، طراحی، پیاده‌سازی، امن‌سازی و پشتیبانی شبکه‌های سازمانی، شبکه های مراکز داده، شبکه های گسترده، امنیت شبکه، فایروال، کنترل دسترسی و معماری امن

پشتیبان گیری و بازیابی

ارائه خدمات مشاوره، طراحی، پیاده‌سازی و پشتیبانی زیرساخت‌های پشتیبان‌گیری در مقیاس‌های بزرگ و چند مرکزداده‌ای، بازیابی اطلاعات و بازگشت از فاجعه با هدف حفاظت از داده‌ها و تداوم سرویس‌های سازمان

ایمیل سازمانی

ارائه خدمات مشاوره، طراحی، پیاده‌سازی، مهاجرت، امن‌سازی و پشتیبانی زیرساخت‌های ایمیل سازمانی با بهره گیری از راهکارهای مختلف متن‌باز و متن‌بسته

زیرساخت مجازی‌سازی

ارائه خدمات مشاوره، طراحی، پیاده‌سازی، امن‌سازی و پشتیبانی زیرساخت‌های مجازی‌سازی شامل مجازی‌سازی لایه های پردازشی، شبکه، ذخیره‌سازی و دسکتاپ با رعایت استانداردهای امنیتی سطح بالا

زیرساخت ذخیره‌سازی وشبکه ذخیره سازی

ارائه خدمات مشاوره، طراحی، پیاده‌سازی و بهینه‌سازی‌بستر شبکه ذخیره‌سازی و زیرساخت‌های ذخیره سازی انبوه توزیع شده و متمرکز در مقیاس های بزرگ سازمانی و دولتی

سیستم عامل و سرویس

ارائه خدمات مشاوره، طراحی، پیاده‌سازی زیرساخت استقرار سیستم عامل‌های متن‌باز و متن‌بسته و سرویس‌های پایه و پیشرفته سیستم عامل‌ها و نرم افزارهای تخصصی مورد بهره برداری

ایمن داده شبکه
ارائه دهنده خدمات جامع فناوری اطلاعات و ارتباطات

sdn.co.ir | info@sdn.co.ir | ۰۲۱-۸۸۵۴۱۰۴۱-۲

..... حوزه‌های تخصصی خدمات شرکت ایمن داده شبکه .....

..... دامنه خدمات تخصصی .....

- شناخت و تحلیل
- مشاوره و طراحی
- پیاده سازی
- بهینه سازی و ارتقاء
- امن سازی و سخت سازی
- مستند سازی
- پشتیبانی و نگهداری در لایه های مختلف
- آموزش تخصصی و سازمانی

مانیتورینگ و مرکز عملیات شبکه

ارائه خدمات مشاوره، طراحی، پیاده سازی و پشتیبانی راهکارهای پایش متمرکز زیرساخت، سیستم عامل، سرویس ها و تجهیزات، مدیریت رخدادها در مراکز داده و شبکه های گسترده جغرافیایی

همگام سازی داده ها

ارائه خدمات مشاوره، طراحی، پیاده سازی، پشتیبانی و بهینه سازی راهکارهای همگام سازی داده ها بین مراکز داده در لایه های مجازی سازی، ذخیره سازی و سیستم عامل و سرویس با هدف افزایش دسترس پذیری، کاهش زمان ازکارافتادگی سرویس ها و فراهم سازی امکان انتقال خودکار یا کنترل شده سرویس به زیرساخت جایگزین در زمان خرابی.

زیرساخت پردازشی

ارائه خدمات مشاوره، طراحی، پیاده سازی، پشتیبانی و بهینه سازی زیرساخت های پردازشی جهت بالابردن میزان کارایی، امنیت و قابلیت اطمینان در سرویس‌دهی و همچنین خوشه بندی جهت بهره بردن از توان تجمیعی پردازشی بصورت همزمان و سراسری

خدمات پایگاه داده پیشرفته سازمانی

ارائه خدمات زیرساخت پایگاه های داده سازمانی جهت ذخیره سازی و مدیریت امن اطلاعات با دسترس پذیری بالا، شامل مشاوره، طراحی، پیاده سازی، پشتیبانی و بهینه سازی، پشتیبان گیری و پایش مستمر

..... ارائه راه‌کارهای یکپارچه برای زیرساختی امن، پایدار و تاب آور .....

- راهکارهای سفارشی
- پشتیبانی تخصصی
- دسترسی پایدار (99.999%)
- عملکرد بهینه
- امنیت پیشرفته

ایمن داده شبکه
ارائه دهنده خدمات جامع فناوری اطلاعات و ارتباطات

sdn.co.ir | info@sdn.co.ir | ۰۲۱-۸۸۵۴۱۰۴۱-۲

ایمن داده شبکه

شرکت ایمن‌داده شبکه با بهره‌گیری از تیم‌های متخصص در حوزه‌های شبکه، امنیت شبکه و زیرساخت‌های سیستمی مرکز داده، با هدف ایجاد و ارتقای Cyber Resilience & Data Protection راهکارها و اقدامات تخصصی متناسب با هر بخش از زیرساخت سازمان را ارائه میدهد.

تاب آوری سایبری و حفاظت از داده

Cyber Resilience & Data Protection

زیرساخت مجازی‌سازی:

طراحی و پیاده‌سازی زیرساخت مجازی‌سازی مبتنی بر Cluster، تخصیص و مدیریت بهینه منابع پردازشی و ذخیره‌سازی، بهره‌گیری از قابلیت‌های High Availability (HA)، Live Migration و مکانیزم‌های Failover، امکان تداوم سرویس‌ها و افزایش دسترس‌پذیری ماشین‌های مجازی فراهم شده و تأثیر خرابی یا تعمیر و نگهداری Host بر سرویس‌های سازمان به حداقل میرسد.

زیرساخت ذخیره‌سازی:

طراحی و پیاده‌سازی معماری مقیاس‌پذیر، افزونه و مقاوم در برابر Failure، پیاده‌سازی مکانیزم‌های مدیریت دسترسی به داده‌ها، بهره‌گیری از Snapshot، Replication و Redundancy و بهینه‌سازی عملکرد و ظرفیت ذخیره‌سازی، دسترس‌پذیری، یکپارچگی و حفاظت از داده‌ها در برابر خرابی تجهیزات، خطاهای عملیاتی، حذف یا تغییرات ناخواسته و از دست رفتن اطلاعات تضمین میشود.

زیرساخت پردازشی:

استقرار معماری به روز و فراهم نمودن افزونگی کامل در تمامی مؤلفه‌های حیاتی سرور در کنار پایش منابع و به‌روزرسانی مستمر firmware سرورها و محدود نمودن دسترسی‌های مدیریتی، دسترس‌پذیری حداکثری سیستم‌ها را تضمین کرده و ریسک قطعی ناشی از اختلالات سخت‌افزاری را به حداقل میرساند.

سیستم عامل Microsoft و Linux و سرویسهای پایه:

امن سازی سرویس های زیرساختی موجود اعم از Directory Services مانند Active Directory، مدیریت هویت و دسترسی، اعمال Policyها، محافظت از سرویس‌های حیاتی و اجرای به‌روزرسانی‌های امنیتی، از زیرساختهای نرم‌افزاری و حسابهای کاربری محافظت میگردد.

ایمن داده شبکه
ارائه دهنده خدمات جامع فناوری اطلاعات و ارتباطات

sdn.co.ir | info@sdn.co.ir | ۰۲۱-۸۸۵۴۱۰۴۱-۲

زیرساخت پشتیبان گیری:

طراحی زیرساخت های گسترده پشتیبان گیری در مراکز داده و تدوین سیاست های پشتیبان گیری مطابق با خطی مشی امنیت سازمان، نگهداری امن جهت صیانت از نسخ پشتیبان، استفاده از اطلاعات پشتیبان گیری شده بصـــورت تغییرناپذیر یا آفلاین، آزمون بازیابی دوره ای، امکان دسترسی مجدد به داده ها پس از بروز خرابی، خطای انسانی، حمله سایبری و بازیابی از فاجعه را به صورت پایدار و قابل اطمینان فراهم می نماید.

Replication:

طراحی و پیاده سازی Replication بین سرویس های مراکز داده و بهره گیری از روش های Sync و Async، همگام سازی داده ها و تداوم سرویس ها در شرایط خرابی یا اختلال فراهم شده و با کاهش RPO و RTO، زمان و میزان از دست رفتن داده ها در فرآیند بازیابی به حداقل می رسد.

زیرساخت شبکه و امنیت شبکه:

طراحی، بازنگری و بهبود مستمر معماری امن شبکه بر پایه رویکرد Defense in Depth، پیاده سازی و بهینه سازی فایروال و سامانه های کنترل دسترسی، بخش بندی و تفکیک و جداسازی شـبکه ها، امن سـازی ارتباطات، کنترل ترافیک و دسترسی ها، پایش مســتمر و شناسایی تهدیدها، سطح امنیت شبکه سازمان را ارتقاء داده و با ایجاد لایه های متعدد دفاعی، از دسترسی های غیرمجاز، نفوذ و گســترش تهدیدات در زیرساخت جلوگیری می شود .

زیرساخت مانیتورینگ:

پایش مســـــتمر، یکپارچه و متمرکز عملکرد، ظرفیت، رخدادهای امنیتی، سلامت تجهیزات، سرویس ها و ارتباطات، تهدیدها و اختلالات را در سریع ترین زمان شناسایی کرده و پیش از تبدیل شدن به بحران، بینش و دید مناسب را جهت انجام اقدامات موثر و بهینه در فرآیند ریشـه یابی، تصـمیم گیری و اقدامات اصلاحی توسط راهبران سرویس، مدیران اجرایی و مشاوران را فراهم می نماید.

از پیشـــگیری، امن سازی و سخت سازی زیرساخت تا شـــناســـایی و مقابله با تهدیدات، حفاظت از داده ها، پشـــتیبان گیری، Replication، Disaster Recovery و بازیابی سریع سرویس ها، تمامی لایه های زیرساخت سازمان به صورت یکپارچه و هدفمند طراحی و مدیریت می شوند؛ به گونه ای که سـازمان بتواند در برابر خرابی تجهیزات، خطاهای انسانی، حملات سایبری و اختلالات زیرســـــاختی تاب آوری خود را حفظ کرده، داده ها و ســـــرویس های حیاتی را محافظت نموده و تداوم کسب وکار را تضمین کند.

ایمن داده شبکه
ارائه دهنده خدمات جامع فناوری اطلاعات و ارتباطات
sdn.co.ir | info@sdn.co.ir | ۰۲۱-۸۸۵۴۱۰۴۱-۲

در مدل امنیتی Zero Trust، هیچ کاربر، دستگاه، سرور یا سرویسی صرفاً بر اساس موقعیت شبکه قابل اعتماد نیست. هر درخواست دسترسی باید به صورت مستمر بر اساس هویت، وضعیت کاربر، سلامت تجهیز، سطح ریسک، نوع سرویس، موقعیت دسترسی و سیاست های امنیتی سازمان احراز هویت و ارزیابی شود.

حوزه های تخصصی و اقدامات موثر جهت پیاده سازی Zero Trust

زیرساخت شبکه و امنیت شبکه

طراحی Micro-Segmentation، کنترل ترافیک شرقی-غربی و شمالی-جنوبی، پیاده سازی فایروال های داخلی، NAC، کنترل دسترسی مبتنی بر سیاست های امنیتی، VPN و دسترسی امن از راه دور.

Microsoft Windows

امن سازی و سخت سازی سیستم عامل ها و سرویس های ویندوزی، مدیریت Group Policy، پیاده سازی Windows Defender، کنترل دسترسی کاربران و مدیریت امنیت کلاینت ها و سرورها.

Linux

امن سازی و سخت سازی سرورهای لینوکسی، مدیریت کاربران و مجوزها، کنترل دسترسی سرویس ها، مدیریت SSH، ثبت و پایش رویدادهای امنیتی و اعمال سیاست های Least Privilege.

Directory Services و احراز هویت

طراحی ساختار امن دامنه، مدیریت چرخه عمر هویت ها، تفکیک حساب های کاربری عادی و مدیریتی، بهره گیری از راهکارهای MFA،یکپارچه سازی احرازهویت، مدیریت گروه ها و دسترسی ها، کنترل سرویس اکانت ها و کاهش ریسک حملاتی مانند Pass-the-Hash و Kerberoasting.

ایمن داده شبکه
ارائه دهنده خدمات جامع فناوری اطلاعات و ارتباطات
sdn.co.ir | info@sdn.co.ir | ۰۲۱-۸۸۵۴۱۰۴۱-۲

VDI و محیط های کاری مجازی

ایجاد محیط کاری ایزوله و کنترل شده، عملیاتی نمودن راهکارهای مبتنی بر RBAC، جداسازی محیط های کابری هر یک از کاربران، محدودسازی انتقال فایل و Clipboard، اعمال سیاست های امنیتی و فراهم کردن دسترسی امن برای کاربران داخلی و دورکار.

سرورها و سرویس های زیرساختی

شناسایی دارایی ها، طبقه بندی سرویس ها، امن سازی و سخت سازی سرورها، کنترل دسترسی مدیریتی، مدیریت حساب های سرویس و اجرای سیاست های دسترسی حداقلی برای سرویس های حیاتی.

زیرساخت مجازی سازی

پیاده سازی اقدامات کنترلی و امنیتی در لایه Hypervisorها و Management Plane، تفکیک شبکه های مدیریتی، کنترل دسترسی مدیران، ثبت فعالیت ها، محدودسازی دسترسی به ماشین های مجازی.

زیرساخت مانیتورینگ

جمع آوری و تحلیل لاگ ها، اتصال به SIEM، پایش رفتار کاربران و مدیران، شناسایی فعالیت های غیرعادی، ایجاد هشدارهای امنیتی، گزارش گیری.

سامانه مدیریت دسترسی (PAM)

با پیاده سازی Privileged Access Management، کاهش سطح حملات و ریسک Lateral Movement، کنترل دسترسی کاربران و مدیران بر اساس حداقل سطح موردنیاز، حفاظت از حساب های مدیریتی، سرورها و سرویس های حیاتی، شناسایی تهدیدها و رفتارهای غیرعادی و پوشش الزامات امنیتی، ممیزی و انطباق سازمانی به همراه دید متمرکز از هویت ها، دارایی ها، دسترسی ها و رویدادهای امنیتی فراهم می گردد. این فرآیند شامل موارد زیر است:

- حذف یا کاهش استفاده از حساب های مدیریتی مشترک
- چرخش خودکار و دوره ای رمزهای عبور
- تأیید دسترسی بر اساس نقش، درخواست و سطح ریسک
- ضبط نشست های مدیریتی و ثبت کامل فعالیت ها
- کنترل دسترسی به سرورهای Windows و Linux
- مدیریت دسترسی به تجهیزات شبکه، پایگاه های داده، Hypervisorها و کنسول های مدیریتی
- محدودسازی دسترسی مستقیم و استفاده از Proxy یا Jump Server امن
- لغو خودکار دسترسی پس از پایان زمان مجاز

ایمن داده شبکه
ارائه دهنده خدمات جامع فناوری اطلاعات و ارتباطات
sdn.co.ir | info@sdn.co.ir | ۰۲۱-۸۸۵۴۱۰۴۱-۲

تداوم کسب وکار و برنامه ریزی بازیابی پس از بحران (BCP/DRP)

Business Continuity & Disaster Recovery Planning

با پیاده سازی Business Continuity وDisaster Recovery ، افزایش تاب آوری و آمادگی سازمان در برابر اختلالات و بحران ها، حفظ دسترس پذیری سرویس ها و سامانه های حیاتی، کاهش زمان و میزان اختلال در ارائه خدمات، طراحی و پیاده سازی سناریوهای بازیابی و بازگشت به سرویس، تعیین اولویت ها و سطوح موردنیاز برای بازیابی، حفاظت و دسترس پذیری داده ها و زیرساخت های حیاتی فراهم می گردد.

جهت تحقق اهداف اسناد BCP/DRP در هر یک از حوزه ها اقدامات ذیل قابل برشمردن است:

Business Impact Analysis و ارزیابی ریسک:

شناسایی سرویس ها و فرآیندهای حیاتی، تعیین اولویت های بازیابی، تحلیل اثرات توقف سرویس و مستندسازی وابستگی های فنی و عملیاتی.

Network & Security:

طراحی مسیرهای ارتباطی افزونه، تفکیک شبکه با VLAN/VRF، پیاده سازی فایروال و کنترل دسترسی، طراحی VPN امن بین مرکزداده اصلی و مرکزداده بحران و پیش بینی سناریوهای Failover ارتباطی.

Data Center و Server Infrastructure:

طراحی زیرساخت های افزونه در سطح برق، سرمایش، رک، تجهیزات شبکه و سرورها، حذف یا کاهش Single Point of Failure و پیش بینی ظرفیت موردنیاز برای اجرای سرویس ها در مرکزداده جایگزین.

Virtualization:

طراحی Clusterها با قابلیت High Availability، استفاده از قابلیت هایی مانند Live Migration و Automated Restart و تعریف Resource Pool و اولویت بندی ماشین های مجازی برای راه اندازی سریع سرویس ها در شرایط بحران.

Storage و Data Protection:

طراحی زیرساخت ذخیره سازی با رعایت افزونگی و Multipathing و فراهم نمودن امکان Mirroring، با هدف حفظ یکپارچگی داده و کاهش زمان بازیابی.

Microsoft و Linux Services:

طراحی افزونگی برای Active Directory، DNS، DHCP، File Services، Database، Application Server، سرویس های وب و سرویس های لینوکسی؛ همچنین بررسی ترتیب راه اندازی و وابستگی میان سرویس ها.

ایمن داده شبکه
ارائه دهنده خدمات جامع فناوری اطلاعات و ارتباطات

sdn.co.ir | info@sdn.co.ir | ۰۲۱-۸۸۵۴۱۰۴۱-۲

Backup:

طراحی زیرساخت پشتیبان گیری و تدوین سیاست ها مبتنی بر مدل 3-2-1-1-0، نگهداری نسخه های خارج از سایت، استفاده از Immutable یا Offline Backup، رمزنگاری، کنترل دسترسی و اجرای تست های منظم Restore.

Replication:

طراحی و پیاده سازی Replication در زیرساخت های ذخیره سازی و مجازی سازی و لایه های سیستم عامل، پایگاه داده و سرویس، انتخاب روش Synchronous یا Asynchronous بر اساس الزامات RTO/RPO، پایش وضعیت Replication و اجرای تست های دوره ای Failover و Failback.

Disaster Recovery Site:

طراحی مرکزداده بحران به صورت Cold، Warm یا Hot Site بر اساس خطی مشی امنیتی سازمان جهت بهره برداری از سرویس ها و میزان بودجه تخصیص یافته و الزامات امنیتی تبیین شده از جمله میزان RTO/RPO، همچنین تعیین ظرفیت پردازشی، ذخیره سازی، شبکه و مجوزهای موردنیاز.

Monitoring، NOC و Alerting:

پایش سلامت تجهیزات اعم از تجهیزات ذخیره سازی، پردازشی، ارتباطی و امنیتی، سیستم عامل، پایگاه های داده و سرویس ها، تعریف Threshold و Alert، ثبت رخدادها و فراهم کردن داشبوردهای عملیاتی به منظور تشخیص سریع خطا.

امنیت و مقابله با تهدیدات سایبری:

جداسازی زیرساخت Backup از شبکه عملیاتی، استفاده از MFA و عملیاتی نمودن راهکارهای مبتنی بر RBAC ، ثبت لاگ، بررسی رفتارهای مشکوک و طراحی سناریوی بازیابی در برابر Ransomware و تخریب عمدی داده ها.

مستندسازی فرآیندهای عملیاتی:

تهیه Runbook و Playbook برای سناریوهای مختلف، تعریف مسئولیت تیم ها، مسیر Escalation، اطلاعات تماس، چک لیست های اجرایی و دستورالعمل بازگشت کنترل شده به سایت اصلی.

در این فرآیند، سناریوهای مختلفی از جمله خرابی سرور یا Storage، قطعی برق یا ارتباطات، از دسترس خارج شدن سایت اصلی، خطای انسانی، خرابی نرم افزاری، آسیب فیزیکی و حملات سایبری بررسی و برای هرکدام فرآیند واکنش، Failover، بازیابی و Failback تعریف می شود. همچنین با اجرای تست های دوره ای Disaster Recovery، شبیه سازی خرابی، بررسی صحت Backupها، اندازه گیری زمان واقعی بازیابی و به روزرسانی مستندات، اطمینان حاصل می شود که طرح تدوین شده صرفاً روی کاغذ باقی نمانده و در شرایط واقعی قابل اجرا است.

ایمن داده شبکه
ارائه دهنده خدمات جامع فناوری اطلاعات و ارتباطات
sdn.co.ir | info@sdn.co.ir | ۰۲۱-۸۸۵۴۱۰۴۱-۲

در فرآیند امن سازی و مقاوم سازی، زیرساخت های فناوری اطلاعات سازمان در تمام لایه ها شناسایی، ارزیابی،امن سازی و سخت سازی و پایش می گردد تا آسیب پذیری های امنیتی کاهش یافته و مقاومت زیرساخت در برابر تهدیدات افزایش می یابد.

اقدامات قابل انجام در هر یک از حوزه ها به شرح زیر خواهد بود:

Network & Security:

پیکربندی امن تجهیزات شبکه و فایروال ها در راستای افزایش سطح امنیت تجهیز، تفکیک شبکه ها، محدودسازی سرویس ها و پورت ها، کنترل دسترسی و کاهش مسیرهای حمله.

Virtualization & VDI:

امن سازی و سخت سازی Hypervisor و Management Plan با بهره گیری از استانداردها و Best Practice ها در راستای رعایت الزامات امنیتی سازمان، تفکیک شبکه های مدیریتی، کنترل دسترسی و Hardening سرور ها و دسکتاپ های مجازی.

Storage & Storage Network:

کنترل دسترسی مدیریتی، تفکیک شبکه مدیریتی دستگاه های ذخیره ساز، پیکربندی شبکه ارتباطی Fabric با بهره گیری از تکنولوژی هایی مانند Zoning, VSAN, Virtual Fabric, LSAN ، رمزنگاری و محافظت از داده ها.

Microsoft & Linux:

امن سازی و سخت سازی سیستم عامل و سرویس های پایه، مدیریت Patch، حذف سرویس های غیرضروری، اعمال Security Policy، Least Privilege و کنترل دسترسی.

Email:

امن سازی و سخت سازی سرویس ایمیل، کنترل دسترسی مدیریتی، TLS، تنظیمات Anti-Spam و Anti-Phishing و کاهش آسیب پذیری سرویس های ایمیل، راه اندازی و پیکربندی و بهینه سازی Mail Gateway.

ایمن داده شبکه
ارائه دهنده خدمات جامع فناوری اطلاعات و ارتباطات
sdn.co.ir | info@sdn.co.ir | ۰۲۱-۸۸۵۴۱۰۴۱-۲

Server & Processing:

امن سازی و سخت سازی زیرساخت پردازشی سرورها، BIOS و Management Interface، کنترل حساب های مدیریتی و سرویس های فعال، امن سازی و سخت سازی و مدیریت دسترسی به سرویس های OOBM (مانند iLO,IMM)

Monitoring & NOC:

پایش مستمر وضعیت امنیتی و پیکربندی زیرساخت، جمع آوری و تحلیل متمرکز Log ها و Event های امنیتی، کنترل تغییرات و شناسایی پیکربندی های ناامن یا غیرمجاز، تعریف Baseline امنیتی و پایش انحراف از آن، شناسایی رفتارها و فعالیت های مشکوک، ایجاد Alert هوشمند از طریق همبستگی رخدادها.

Backup:

امن سازی و سخت سازی زیرساخت Backup، جداسازی دسترسی های ارتباطی زیرساخت Backup و زیرساخت عملیاتی، پیاده سازی MFA ، استفاده از Offline Backup، سخت سازی Repositoryها و محافظت از آن ها در برابر Ransomware و حذف یا تغییر غیرمجاز داده های پشتیبان گیری شده.

Replication:

امن سازی و سخت سازی زیرساخت Replication از طریق تفکیک شبکه و مسیرها، کنترل دسترسی و احراز هویت، رمزنگاری ارتباطات، محدودسازی دسترسی مدیریتی، پایش وضعیت Replication و محافظت از کپی های Replicated در برابر دستکاری، حذف غیرمجاز و انتشار حملات سایبری.

درنهایت با Baseline امنیتی، ارزیابی وضعیت موجود، رفع Misconfiguration، اعمال Hardening، مستندسازی و پایش مستمر، یک زیرساخت استاندارد، کم ریسک و مقاوم در برابر تهدیدات ایجاد می گردد.

پایش و بهبود مستمر	انطباق با استانداردها	پایداری و قابلیت اطمینان	افزایش امنیت	کاهش سطح حمله

ایمن داده شبکه
ارائه دهنده خدمات جامع فناوری اطلاعات و ارتباطات
sdn.co.ir | info@sdn.co.ir | ۰۲۱-۸۸۵۴۱۰۴۱-۲

مانیتورینگ و پایش یکپارچه زیرساخت

Observability & Integrated Infrastructure Monitoring

با پیاده سازی Monitoring و پایش یکپارچه زیرساخت، ایجاد دید متمرکز و لحظه ای بر وضعیت تجهیزات، سرویس ها، سامانه ها و منابع زیرساختی، شناسایی سریع خطاها، اختلالات و رفتارهای غیرعادی، کاهش زمان تشخیص و رفع رخدادها، پایش مستمر عملکرد، ظرفیت و دسترس پذیری اجزای زیرساخت، تعریف آستانه ها و هشدارهای هوشمند زیرساخت فراهم می گردد.

در فرآیند مانیتورینگ و پایش یکپارچه، زیرساخت های فناوری اطلاعات سازمان در تمام لایه ها به صورت یکپارچه تحت رصد و پایش قرار می گیرد و وضعیت عملکرد، دسترس پذیری، سلامت و رویدادهای مرتبط با تجهیزات و سرویس ها به صورت مستمر بررسی می شود. این رویکرد با ایجاد دید متمرکز و جامع بر زیرساخت، امکان شناسایی سریع اختلالات، تحلیل رخدادها، پیشگیری از بروز مشکلات و بهبود مستمر پایداری و کارایی سرویس های فناوری اطلاعات را فراهم می کند.

با جمع آوری و تحلیل متمرکز Metrics، Logs، Events و Alerts از تجهیزات شبکه، سرورها، ماشین های مجازی، Storage، سرویس های Microsoft و Linux، ایمیل، Backup و سایر اجزای زیرساخت، وضعیت سرویس ها و وابستگی میان آن ها را به صورت یکپارچه قابل مشاهده خواهد بود.

Network & Security:

پایش مستمر تجهیزات شبکه و امنیتی، وضعیت ارتباطات و مسیرهای ارتباطی، ترافیک و الگوهای مصرف، خطاها و Packet Loss ، ظرفیت و Throughput ، وضعیت Interface ها و رخدادهای امنیتی؛ همچنین شناسایی رفتارهای غیرعادی و ایجاد هشدار پیشگیرانه .

Virtualization & VDI:

مانیتورینگ Host، Cluster و VM ها، منابع CPU/RAM، Storage و Network ، وضعیت HA و عملکرد ماشین های مجازی، پایش Sessionهای کاربران در VDI، مصرف منابع و ظرفیت محیط های VDI و شناسایی Bottleneck ها و اختلالات احتمالی .

Storage & Storage Network:

پایش Capacity، Performance، وضعیت سلامت سخت افزاری تجهیزات، میزان IOPS، ThroughputوLatency ، وضعیتPool ها وLUN ها، Snapshotها و Replication با هدف شناسایی زودهنگام افت عملکرد یا کمبود ظرفیت.

Server & OS:

پایش منابع CPU، RAM، Disk و Network ، وضعیت Service ها و Processها، Availability، ظرفیت و Performance سرورها، رخدادهای در لایه سیستم عامل و سرویس، تغییرات مهم سیستم عامل و شناسایی مصرف غیرعادی منابع یا توقف سرویس های حیاتی .

ایمن داده شبکه
ارائه دهنده خدمات جامع فناوری اطلاعات و ارتباطات

sdn.co.ir | info@sdn.co.ir | ۰۲۱-۸۸۵۴۱۰۴۱-۲

Email Services:

پایش سلامت Email Services، وضعیت Queueها، Mail Flow و Delivery ، تأخیر و خطاهای ارسال و دریافت، مصرف منابع، وضعیت سرویس ها و رخدادهای مرتبط با Email

Backup & Replication:

پایش Backup Jobها، وضعیت Repositoryها، ظرفیت و مصرف فضای ذخیره سازی، شناسایی خطاهای تکرار شونده و کنترل صحت اجرای فرآیندهای حفاظت از داده .

NOC & Alerting:

ایجاد Dashboard های متمرکز مدیریتی و عملیاتی، تعریف Threshold و Alert، همبستگی و تحلیل Eventها، دسته بندی و اولویت بندی رخدادها، Escalation و ارجاع سلسله مراتبی، ثبت رخدادها و ارائه گزارش های عملیاتی برای واکنش سریع، پیشگیری از تبدیل اختلالات کوچک به بحران و پیکربندی و ارسال هشدار به کاربران مربوطه از طریق SMS، ایمیل و پیام رسان ها.

با یکپارچه سازی اطلاعات مانیتورینگ در تمام لایه های زیرساخت، از شبکه و امنیت تا سرورها، مجازی سازی، ذخیره سازی، Email و Backup ، دید متمرکزی از وضعیت سرویس ها، وابستگی ها، ظرفیت، Performance و رخدادهای امنیتی ایجاد می شود و امکان تشخیص سریع، تحلیل ریشه ای، ظرفیت سنجی و اقدام پیشگیرانه فراهم خواهد شد.

ایمن داده شبکه
ارائه دهنده خدمات جامع فناوری اطلاعات و ارتباطات

sdn.co.ir | info@sdn.co.ir | ۰۲۱-۸۸۵۴۱۰۴۱-۲

Network and Network Security
شبکه و امنیت شبکه

شـــرکت ایمن داده شـــبکه با بهره گیری از تیم های متخصص و تجربه طراحی، پیاده سازی و پشـتیبانی زیرســـــاخت های ارتباطی و امنیتی، با هدف ایجاد شـــبکه ای امن، پایدار، مقیاس پذیر و با دســـترس پذیری بالا، راهکارهای تخصصی متناسب با معماری، نیازمندی ها و الزامات هر سـازمان را ارائه می دهد .

طراحی معماری شبکه و امنیت:

با بررسی زیرساخت موجود و نیازمندی های فنی و امنیتی سـازمان، معماری شـبکه و امنیت بر مبنای اسـتانداردهای فنی، Best Practices و رویکرد Defense in Depth طراحی و بازطراحی می شود. طراحی مکانیزم های افزونگی در تجهیزات و لینک های ارتباطی، تفکیک لایه ها و نواحی امنیتی، بهینه سازی مسیرهای ارتباطی و پیش بینی توسعه آتی شبکه، موجب افزایش پایداری، امنیت، توسـعه پذیری و کاهش نقاط تک خرابی (Single Point of Failure) در زیرســـاخت می شـــود.

شبکه های ارتباطی سازمانی:

با طراحی و پیاده سازی شـبکه هایLAN ، WAN، MAN و SD-WAN ، بهره گیری از فناوری هایی نظیرMPLS ، VPNو Hybrid WAN ، ارتباطی پایدار، امن و مقیاس پذیر میان کاربران، شعب، سایت ها و مراکز داده سازمان فراهم می شود. همچنین با پیاده سازی QoS ، Traffic Engineeringو بهینه سـازی Routing و Switching ، کیفیت و کارایی ارتباطات متناسب با نیاز سرویس های سازمان ارتقا می یابد.

اتصال امن شعب، کاربران و محیط های دورکار:

با طراحی و پیاده سازی ارتباطات امن مبتنی برVPN ، SD-WAN، Zero Trust، راهکارهای Secure Access و راهکارهای سـازمانی مانند APN ، دسترسی شعب، کاربران و نیروهای دورکار به منابع و سرویس های سازمان به صورت کنترل شـده، پایدار و امن فراهم می شود. این رویکرد با اعمال سیاست های دسترسی، احراز هویت و رمزنگاری ارتباطات، سطح امنیت دسترسی های خارج از شبکه سازمان را افزایش می دهد.

شبکه و امنیت مراکز داده:

با طراحی معماری شبکه مراکز داده بر پایه فناوری هایی نظیرCisco ACI ، SDNوEVPN/VXLAN ، زیرساختی مقیاس پذیر، Policy-Based و آماده برای محیط های ابری ایجاد می شـود. پیاده سـازی Micro-Segmentation ، Security Zoning، معماری های Multi-Pod و Multi-Site و مکانیزم های High Availability ، ضمن افزایش امنیت و دسترس پذیری، امکان توسعه و مدیریت یکپارچه ارتباطات میان سرویس ها و مراکز داده را فراهم می کند.

امنیت شبکه و کنترل دسترسی:

با طراحی و پیاده سازی معماری چندلایه امنیتی، بهینه سازی فایروال ها و سامانه های کنترل دسترسـی، Segmentation شبکه، امن سازی ارتباطات، کنترل ترافیک و دسترسی کاربران و سرویس ها و پایش مستمر رخدادهای شبکه، سطح امنیت زیرساخت ارتقا یافته و احتمال دسترسی غیرمجاز، نفوذ و گسـترش تهدیدات در بخش های مختلف شبکه کاهش می یابد.

ایمن داده شبکه
ارائه دهنده خدمات جامع فناوری اطلاعات و ارتباطات

sdn.co.ir | info@sdn.co.ir | ۰۲۱-۸۸۵۴۱۰۴۱-۲

شبکه های مدیریتی و دسترسی امن به تجهیزات:

با طراحی Management Network و معماری مستقل Out-of-Band (OOB) برای مدیریت تجهیزات شبکه، امنیت دسترسی های مدیریتی افزایش یافته و امکان پایش، مدیریت و بازیابی تجهیزات حتی در شرایط بروز اختلال در شبکه عملیاتی فراهم می شود. طراحی DC Management Block و شبکه های مدیریتی مجزا نیز از تداخل ترافیک مدیریتی و عملیاتی جلوگیری کرده و سطح کنترل و امنیت زیرساخت را افزایش می دهد.

اتوماسیون و بهینه سازی شبکه:

با بهره گیری از ابزارها و راهکارهای Network Automation نظیر Ansible و راهکارهای شرکت های ارائه دهنده، فرآیندهای پیکربندی، اعمال تغییرات و مدیریت تجهیزات شبکه استاندارد و خودکار شده و ضمن کاهش خطاهای انسانی، سرعت اجرای تغییرات و یکپارچگی تنظیمات افزایش می یابد. پایش و بهینه سازی مستمر ظرفیت، مسیرها و الگوهای ترافیکی نیز با استفاده از قابلیت ها، امکان شناسایی سریع اختلالات، تحلیل عملکرد سرویس ها را فراهم می نماید.

پایش، تحلیل و مشاهده پذیری شبکه:

با پیاده سازی راهکارهای Network Monitoring ، Network Analytics و Network Detection and Response ، رفتار ترافیک و ارتباطات شبکه به صورت مستمر تحلیل می شود. این راهکارها با شناسایی الگوهای غیرعادی، تهدیدات داخلی، انحراف از رفتار معمول و نشانه های حمله، امکان تشخیص زودهنگام رخدادهای امنیتی، تحلیل دقیق تر علت اختلالات و واکنش سریع تر تیم های عملیاتی و امنیتی را فراهم می کنند.

نوسازی و توسعه زیرساخت شبکه:

با ارزیابی وضعیت تجهیزات و معماری موجود، برنامه ریزی برای ارتقای تجهیزات و مهاجرت زیرساخت های Legacy به معماری های نوین انجام می شود. استفاده از فناوری هایی نظیرEVPN/VXLAN ، SDNو SD-WAN ضمن افزایش مقیاس پذیری و انعطاف پذیری شبکه، امکان توسعه تدریجی زیرساخت بدون ایجاد اختلال گسترده در سرویس های عملیاتی را فراهم می کند.

از طراحی و بازطراحی معماری شبکه و امنیت تا پیاده سازی شبکه های ارتباطی سازمانی، اتصال امن شعب و کاربران دورکار، زیرساخت مراکز داده، کنترل دسترسی، Segmentation، پایش و تحلیل ترافیک، اتوماسیون، بهینه سازی و نوسازی شبکه، تمامی اجزای زیرساخت ارتباطی سازمان به صورت یکپارچه و مبتنی بر الزامات فنی و امنیتی طراحی و مدیریت می شوند؛ به گونه ای که سازمان از ارتباطاتی امن، پایدار، مقیاس پذیر و با دسترس پذیری بالا برخوردار بوده و زیرساخت آن آمادگی لازم برای توسعه سرویس ها، شناسایی سریع تهدیدات و پاسخ گویی به نیازهای آینده را داشته باشد.

ایمن داده شبکه
ارائه دهنده خدمات جامع فناوری اطلاعات و ارتباطات
sdn.co.ir
info@sdn.co.ir
۰۲۱-۸۸۵۴۱۰۴۱-۲

راهکارهای جامع فناوری اطلاعات

راهکارهای ارائه شده توسط ایمن داده شبکه با هدف مدیریت، پایش، حفاظت و تداوم سرویس های فناوری اطلاعات طراحی و پیاده سازی می شوند.

- **مدیریت هویت و دسترسی های مدیریتی (IAM & PAM)**

مدیریت هویت کاربران، کنترل دسترسی های مدیریتی، اعمال اصل حداقل دسترسی، مدیریت حساب های مدیریتی، ثبت و پایش نشست ها و کنترل دسترسی به منابع حساس سازمان.

- **حفاظت، پشتیبان گیری و بازیابی داده (Data Protection, Backup & Recovery)**

طراحی و پیاده سازی راهکارهای پشتیبان گیری، بازیابی اطلاعات، Replication، Immutable Backup و حفاظت از داده ها در برابر حذف، خرابی، خطای انسانی و حملات سایبری.

- **پایش، تحلیل و مانیتورینگ یکپارچه (Integrated Monitoring, Observability & Network Analytics)**

پایش متمرکز تجهیزات، سرویس ها، سرورها، ماشین های مجازی، شبکه، Storage و سامانه های امنیتی، همراه با تحلیل ترافیک و رفتار شبکه، شناسایی ناهنجاری ها و هم بستگی رخدادها با هدف تشخیص سریع اختلالات، تهدیدات و گلوگاه های عملکردی و بهبود مستمر زیرساخت.

- **مدیریت پیکربندی و مقاوم سازی امنیتی (Configuration Management & Security Hardening)**

ارزیابی و مدیریت پیکربندی، شناسایی آسیب پذیری ها، مقاوم سازی سیستم عامل ها و سرویس ها، کنترل انطباق با استانداردهای امنیتی و کاهش سطح حمله زیرساخت.

- **تداوم کسب وکار و بازیابی پس از بحران (Business Continuity & Disaster Recovery)**

طراحی و پیاده سازی سناریوهای تداوم کسب وکار، بازیابی پس از بحران، Failover، Failback و مدیریت سایت پشتیبان با هدف حفظ سرویس های حیاتی سازمان.

ایمن داده شبکه
ارائه دهنده خدمات جامع فناوری اطلاعات و ارتباطات
sdn.co.ir | info@sdn.co.ir | ۰۲۱-۸۸۵۴۱۰۴۱-۲

تامین تجهیزات زیرساخت فناوری اطلاعات

شرکت ایمن داده شبکه تجهیزات مورد نیاز برای طراحی و پیاده سازی زیرساخت های شبکه، مراکز داده، امنیت، پردازش و ذخیره سازی اطلاعات را از برندهای معتبر تأمین و ارائه می کند.

تجهیزات شبکه و ارتباطات

تجهیزات شبکه های LAN و WAN ، SD-WAN، شبکه مراکز داده، Wireless و تجهیزات ارتباطی سازمانی.

تجهیزات امنیت شبکه

تجهیزات فایروال، کنترل دسترسی، امنیت شبکه، Secure Access، Application Delivery و حفاظت از ارتباطات سازمانی.

تجهیزات پردازشی و سرور

سرورها، تجهیزات پردازشی، زیرساخت های مجازی سازی و تجهیزات مورد نیاز برای اجرای سرویس های سازمانی و مراکز داده.

تجهیزات ذخیره سازی و حفاظت از داده

تجهیزات و سامانه های ذخیره سازی، تجهیزات پشتیبان گیری، Replication و زیرساخت های مورد نیاز برای حفاظت و نگهداری داده هایسازمانی.

FORTINET
f5
CISCO
DELL EMC
HITACHI Inspire the Next
Hewlett Packard Enterprise
JUNIPER NETWORKS
DELL Technologies
IBM
ORACLE
HPE aruba networking
Quantum
BROCADE A Broadcom Limited Company
BROADCOM
Sun ORACLE
Lenovo
Array

ایمن داده شبکه
ارائه دهنده خدمات جامع فناوری اطلاعات و ارتباطات
sdn.co.ir | info@sdn.co.ir | ۰۲۱-۸۸۵۴۱۰۴۱-۲