پلتفرم حاکمیت یکپارچه امنیت سایبری بادبـــان

مدیریت آسان و حرفه‌ای امنیت سایبری

بادبان
BAADBAAN

مأموریت بادبـان

بادبان، یک پلتفرم نرم‌افزاری با مأموریت حاکمیت و مدیریت یکپارچه و جامع امنیت سایبری و امنیت اطلاعات است که انواع مختلفی از استانداردها و الزامات ملی و بین‌المللی را پشتیبانی می‌کند. رویکرد بادبان ایجاد نگاهی کل‌نگر و جامع به امنیت سایبری در سازمان از بالاترین سطح حاکمیتی تا جزئی‌ترین سطوح فنی است. از این رو بادبان قابل بهره‌برداری توسط مدیران ارشد امنیت، مدیران میانی و کارشناسان فنی مرتبط با حوزه امنیت سایبری و امنیت اطلاعات می‌باشد.

بادبان
BAADBAAN

امتیازات منحصر بفرد

- تأییدیه امنیتی محصول از مرکز راهبردی افتا
- مجوز حقوق مالکیت فکری از وزارت فرهنگ
- تأییدیه فنی از شورای عالی انفورماتیک
- مورد تأیید به‌عنوان محصول دانش‌بنیان
- پلتفرم بومی با طراحی و توسعه اختصاصی

قابلیت‌های کلیـدی

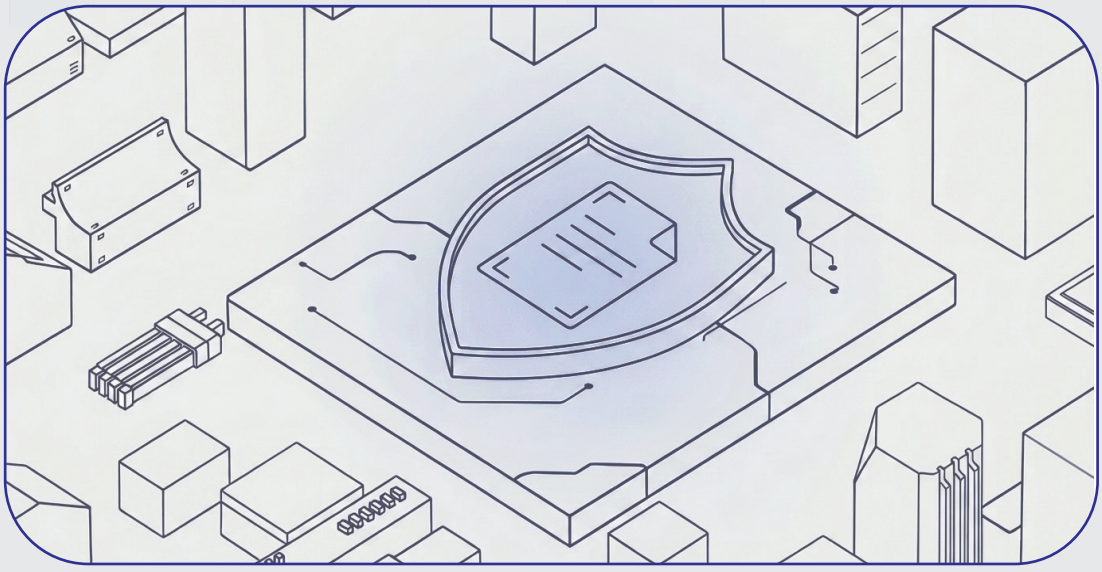
- پشتیبانی از استانداردها و الزامات گوناگون
- پیاده‌سازی مدیریت امنیت اطلاعات (ISMS)
- تسهیل دریافت گواهینامه و ممیزی
- مدیریت آسیب‌پذیری‌های فنی‌و آزمون نفوذ
- پوشش استانداردهای ملی و بین‌المللی
- استفاده از سیستم‌های خبره در تحلیل ریسک
- گزارش‌ها و داشبوردهای سفارشی
- استقرار سلسله‌مراتبی (مرکز و زیرمجموعه‌ها)

پایگـاه دانـش

- پشتیبانی از استانداردهای پیش‌فرض بین المللی مانند:

ISO/IEC 27001 (ISMS), ISO 22301 (BCMS), NIST 800-53, CIS Security Controls

- پشتیبانی از الزامات و استانداردهای پیش‌فرض ملی مانند طرح امن‌سازی زیرساخت‌های حیاتی افتا و طرح ضربتی افتا
- امکان اضافه کردن انواع استانداردها، الزامات، ابلاغیه‌ها، چک‌لیست‌های سفارشی و اختصاصی
- امکان سفارشی‌سازی اطلاعات ریسک، آسیب‌پذیری، تهدید، پیامد، بلوغ، انطباق و ممیزی توسط کاربر



مدیریت ریسک

- کاتالوگ تهدیدات و پیامدها
- متدولوژی و آستانه پذیرش ریسک
- پایگاه دانش آسیب‌پذیری‌ها، تهدیدات و پیامدها
- پرسشنامه آسیب‌پذیری، تهدید و پیامد
- ارتباط بین آسیب‌پذیری، تهدید و پیامد در تشکیل سناریوی ریسک
- ارزیابی، تحلیل و مقابله با ریسک
- گروه‌بندی‌ها و آیتم‌های پیش فرض و متنوع ریسک
- استراتژی‌های مقابله با ریسک
- کاهش خودکار سطح ریسک پس از انجام فعالیت RTP
- درج RTP خودکار و هوشمند بر اساس آستانه پذیرش ریسک
- امکان ایجاد پرسشنامه سفارشی و اختصاصی برای آسیب پذیری، تهدید و پیامد
- گزارشات ریسک و کنترل دسترسی

	عملیات	عنوان آیتم ریسک	مقدار آسیب پذیری	سطح آسیب پذیری	مقدار تهدید	سطح تهدید	مقدار پیامد رویداد	سطح پیامد رویداد
1		امنیت تجهیزات اداری	5	خیلی زیاد	4.8	خیلی زیاد	7.05	متوسط
2		فرآیند مدیریت آسیب‌پذیری‌ها	2.38	متوسط	4.04	خیلی زیاد	7.21	متوسط
3		لپ‌تاپ‌ها و تجهیزات قابل حمل	5	خیلی زیاد	3.55	زیاد	9	زیاد
4		ریسک سناریو محور_سناریو سفارشی	1	خیلی کم	5	خیلی زیاد	6	کم
5		تجهیزات یوپی‌اس	5	خیلی زیاد	3.41	زیاد	8.14	زیاد
6		آیتم سفارشی‌سازی شده	5	خیلی زیاد	4.69	خیلی زیاد	8	متوسط
7		امنیت فیزیکی و محیطی	4	زیاد	2.67	متوسط	10	بحرانی

مدیریت آسیب‌پذیری‌های فنی

- ورود اطلاعات آسیب‌پذیری‌ها از ابزارهایی مانند:

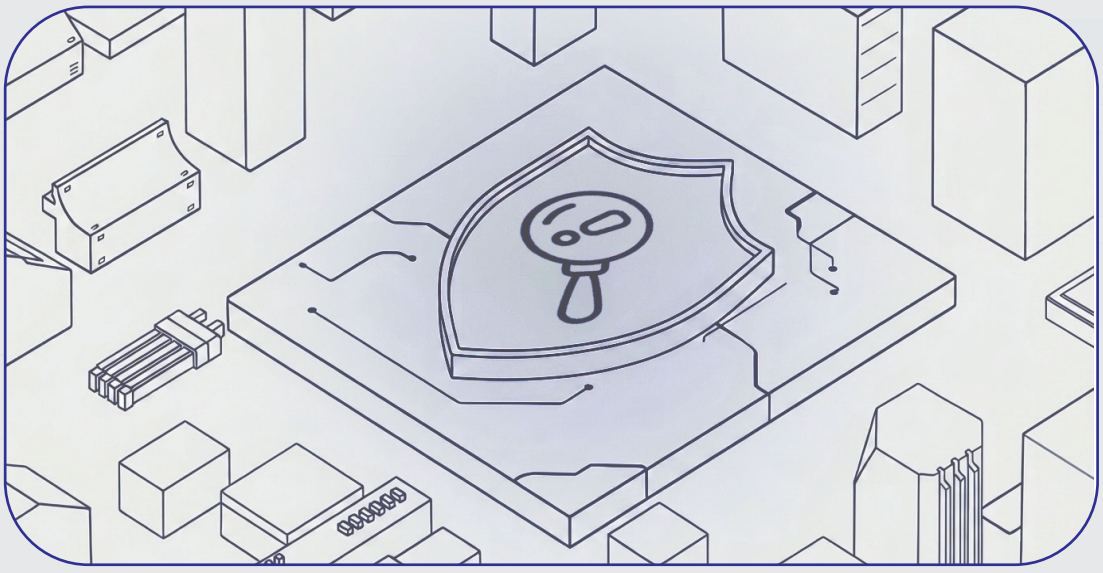
  Acunetix, Nessus, OpenVAS, Netsparker

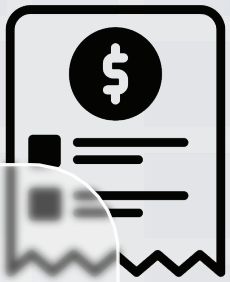
- ورود اطلاعات آسیب‌پذیری‌های وب، شبکه، موبایل و دسکتاپ از طریق فایل‌های اکسل و فرم‌های برنامه
- ارتباط اتوماتیک آی‌پی‌ها با دارایی‌ها از طریق جستجوی خودکار در انواع فیلدهای دارایی
- مدیریت آسیب‌پذیری‌های فنی و چرخه کامل رفع آسیب‌پذیری از طریق RTP ریسک فنی و کارتابل
- بهره‌برداری از هر دو روش مبتنی بر CVSS و RBVM (مدیریت آسیب‌پذیری‌های مبتنی بر ریسک)
- نگهداری تاریخچه آسیب‌پذیری‌ها و طرح‌های مقابله با ریسک
- کاهش تعداد آسیب‌پذیری‌ها به صورت خودکار پس از تأیید نهایی و بستن فعالیت در کارتابل

آدرس	دارایی ها	Critical	High	Medium	Low	Info	RTP	مقدار Exploit	مقدار پیامد	مقدار ریسک	سطح Exploit	سطح پیامد	سطح ریسک
10.10.220.106	سرور شماره ۰۰۱	8	32	12	0	182	0	5	4.08	8.52	خیلی زیاد	خیلی زیاد	زیاد
10.10.220.99	سرور شماره ۰۰۲	2	16	4	0	180	0	3	5	8.9	متوسط	خیلی زیاد	زیاد
10.10.220.86		63	55	16	3	170	0	5	5	9.34	خیلی زیاد	خیلی زیاد	بحرانی
10.10.220.21		50	130	28	0	172	0	5	4.78	9.2	خیلی زیاد	خیلی زیاد	بحرانی
10.10.67.167		47	45	13	2	192	0	5	4.73	9.18	خیلی زیاد	خیلی زیاد	بحرانی
10.10.67.40		8	58	18	2	299	0	5	5	8.92	خیلی زیاد	خیلی زیاد	زیاد
10.10.32.103		5	27	12	0	195	0	2	4.67	7.28	کم	خیلی زیاد	زیاد
10.10.200.61		25	36	25	2	212	0	5	5	9.04	خیلی زیاد	خیلی زیاد	بحرانی
portal.myorg.ir	پرتال سازمانی من	0	0	8	0	17	8	5	5	10	خیلی زیاد	خیلی زیاد	بحرانی

شناخت

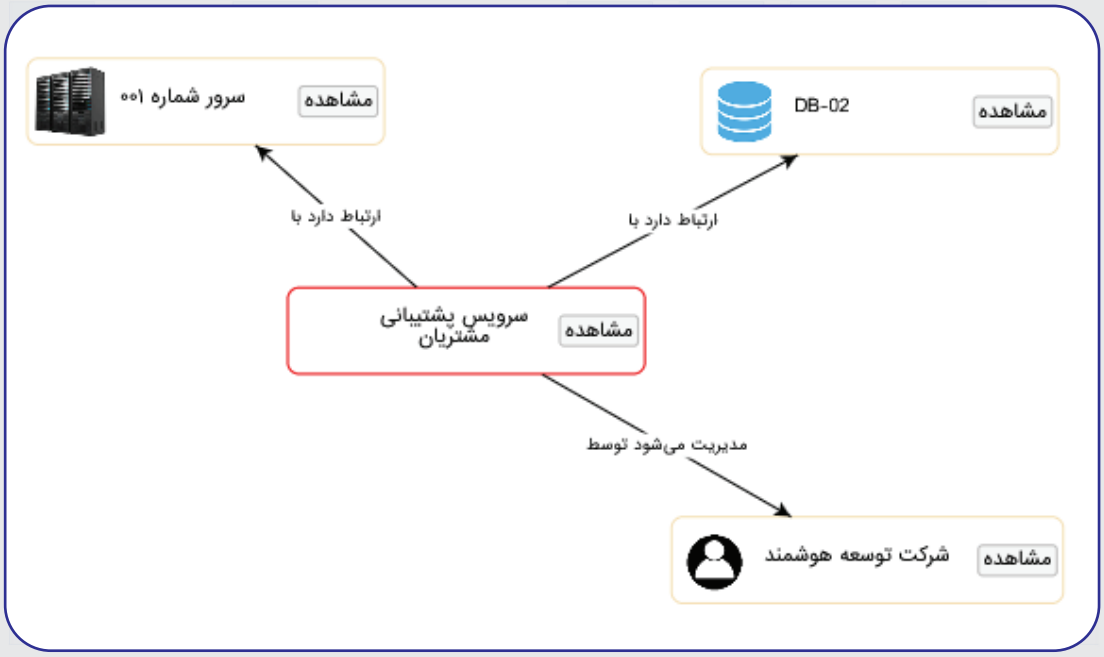
- طبقه‌بندی اطلاعات
- شناخت ذینفعان و انتظارات
- تعریف الزامات بالادستی، قوانین و مقررات
- تعریف اهداف استراتژیک سازمان
- رابطه اهداف با ISMS و BCMS
- تعریف عوامل بیرونی و درونی در ISMS
- تعریف عوامل بیرونی و درونی در BCMS
- تأثیر هر یک از عوامل بر روی اهداف (مثبت و منفی)
- گزارش تأثیر عوامل بر اساس ماتریس SWOT





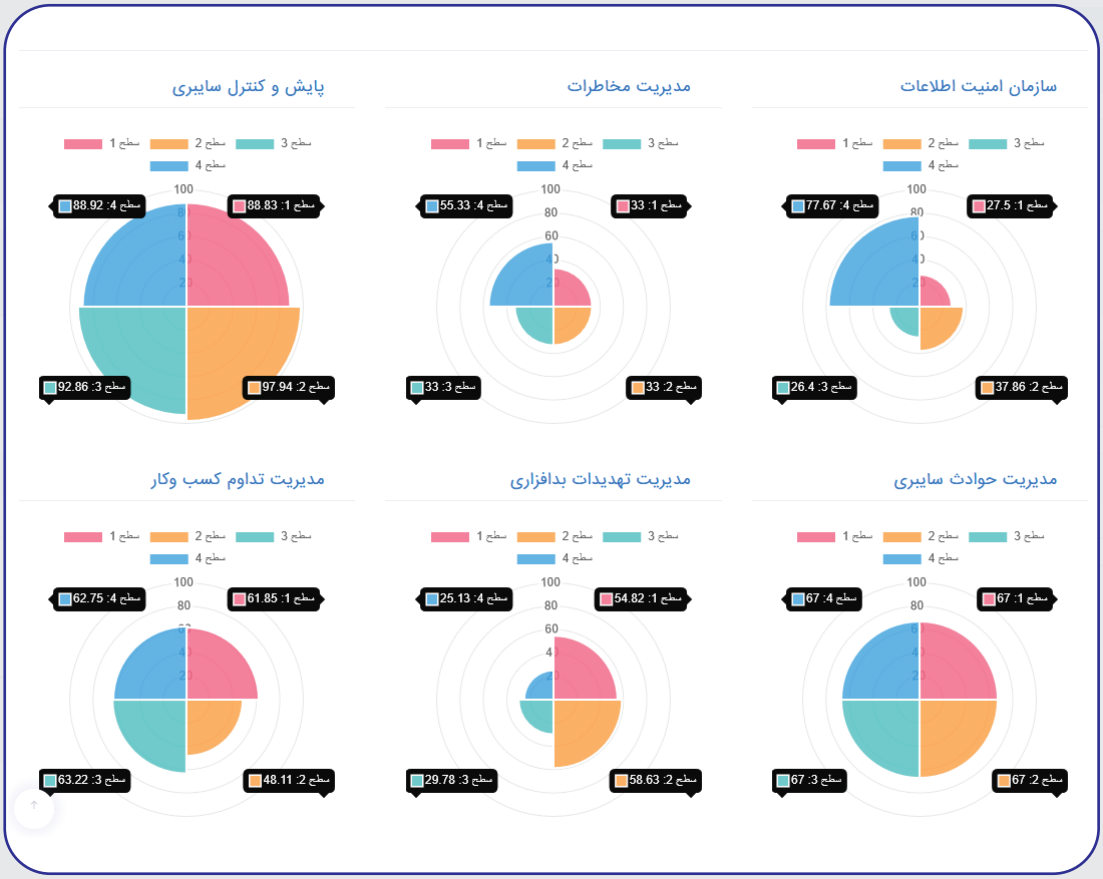
مدیریت دارایی‌ها

- گروه‌بندی سلسله‌مراتبی چند سطحی دارایی‌ها
- فیلدهای داینامیک و دلخواه برای گروه‌های مختلف دارایی
- کنترل دسترسی به صورت نقش محور، مالک محور و فیلد محور
- تعریف ارتباطات بین گروه‌های دارایی
- بارگذاری اطلاعات از طریق فرم برنامه و فایل‌های اکسل
- شناسایی خودکار ماشین‌های مجازی
- شناسایی خودکار از طریق بارگذاری فایل NMAP
- ارتباط با دیگر ابزارهای شناسایی خودکار در قالب توسعه



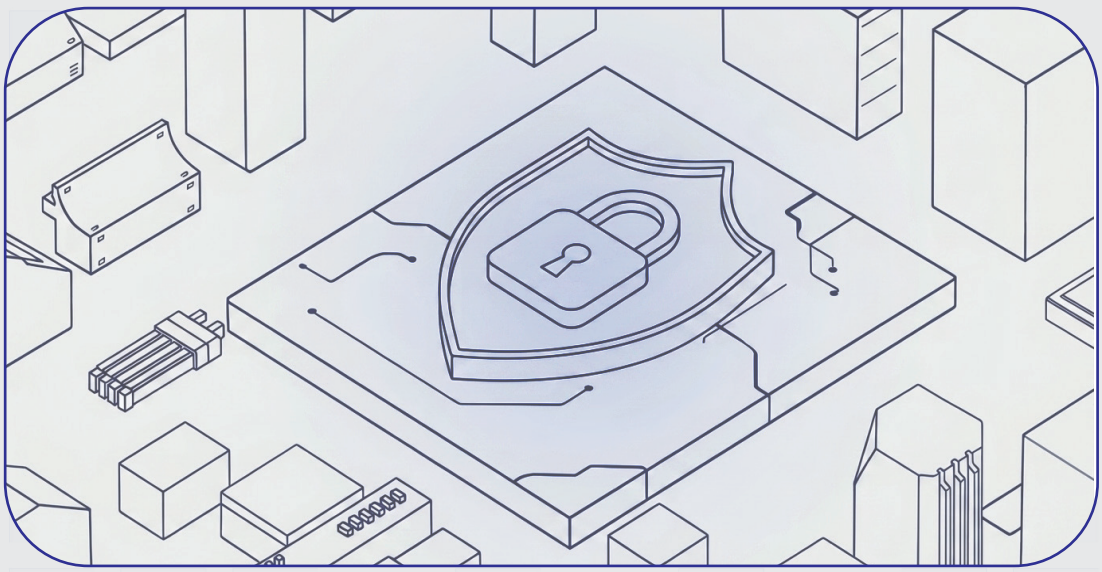
ارزیابی بلوغ، انطباق‌سنجی و ممیزی

- ارزیابی بلوغ بر اساس استانداردهای مختلف و دلخواه
- طرح زیرساختی‌های حیاتی افتا شامل پرسشنامه‌ها و گزارشات
- طرح ضربتی افتا شامل پرسشنامه‌ها و گزارشات
- تعریف دوره‌های مختلف بلوغ، انطباق‌سنجی و ممیزی
- کنترل دسترسی بر اساس بخش، سمت و کاربر
- گزارشات متنوع و مختلف بر اساس بلوغ، انطباق و ممیزی



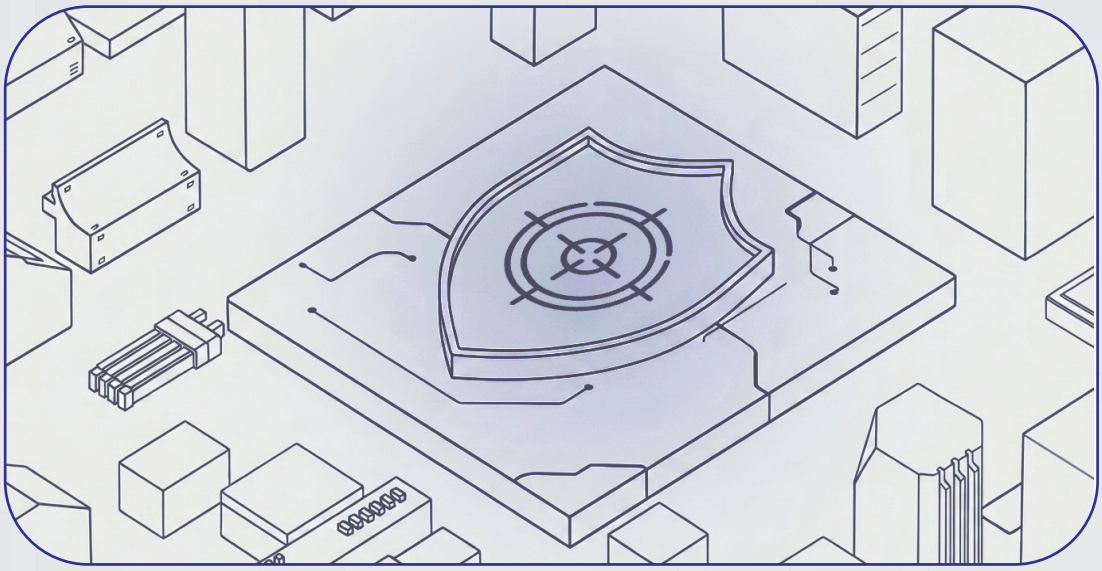
حاکمیت امنیت و خط‌مشی‌ها

- تنظیمات متدولوژی و آستانه پذیرش ریسک
- نگاشت بین استانداردهای مختلف در قالب چارچوب مرجع
- بیانیه کاربردپذیری (SOA)
- بارگذاری و دسترسی به اسناد مختلف شامل خط‌مشی‌ها، دستورالعمل‌ها و ...



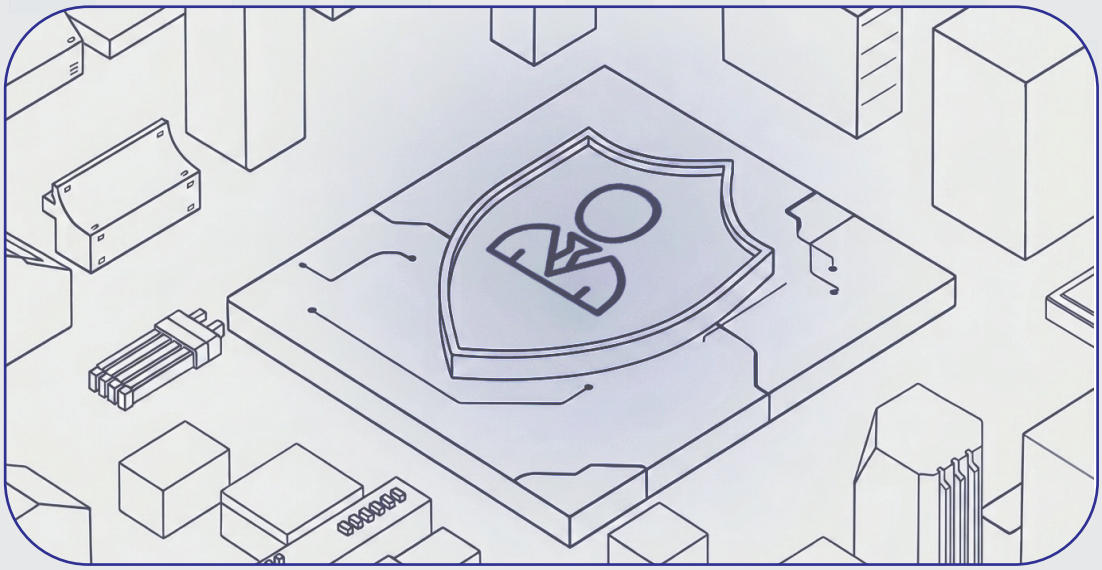
اندازه‌گیری اهداف و عملکرد

- تعریف انواع شاخص‌های اثربخشی و کارایی
- امکان درج طرح و اقدام برای هر یک از شاخص‌ها
- شناسایی اتوماتیک و خودکار شاخص‌ها توسط پلتفرم بادبان
- تعریف اهداف امنیتی سازمان
- ارتباط اهداف امنیتی با اهداف استراتژیک
- اندازه‌گیری خودکار میزان پیشرفت اهداف استراتژیک



مدیریت تداوم کسب و کار

- مشخص کردن فعالیت‌های حیاتی کسب و کار
- تعریف منابع لازم برای کارکرد هر یک از فعالیت‌های حیاتی
- تعریف دامنه پذیرش
- شناسایی اثرات وقفه
- شناسایی زمان‌های وقفه
- تحلیل اثرات وقفه بر فعالیت‌های حیاتی
- تحلیل پیامد کسب و کار (BIA)
- تعیین مقادیر RTO, RPO, MTPD, MBCO
- مدیریت ریسک سرویس‌ها و فرآیندهای حیاتی

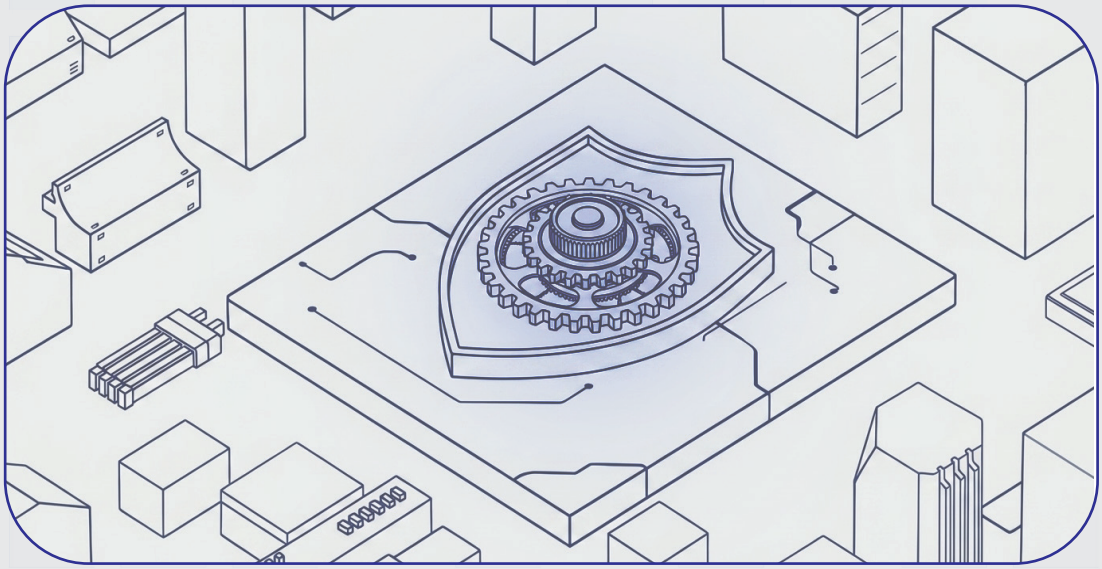


گزارش و داشبورد

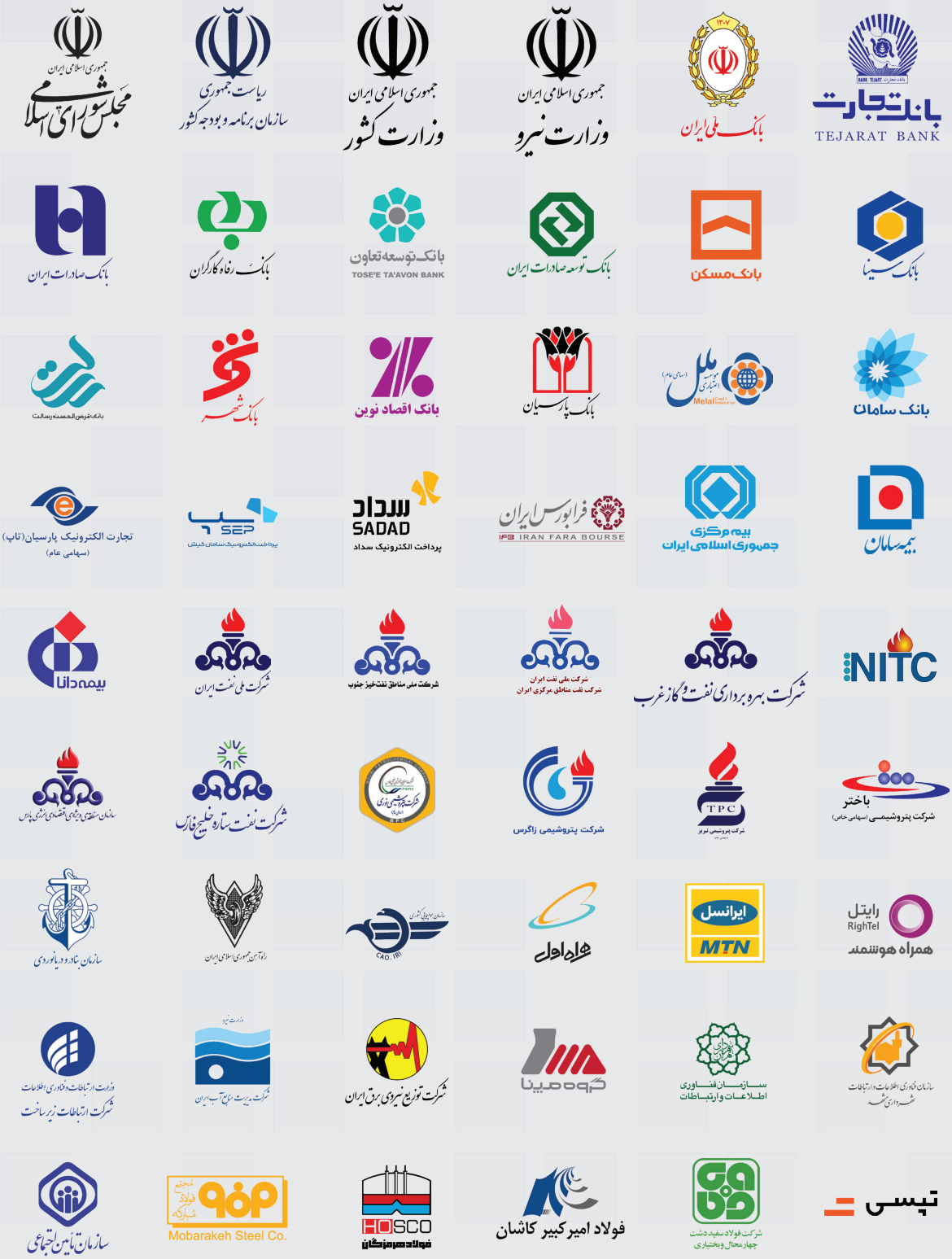
- اکسپورت اطلاعات در تمامی گریدها و ماژول‌ها در قالب فایل اکسل
- تهیه نمودار از اطلاعات ماژول‌های مختلف
- تعریف داشبوردهای مختلف
- اضافه کردن نمودارهای تولید شده به داشبورد دلخواه

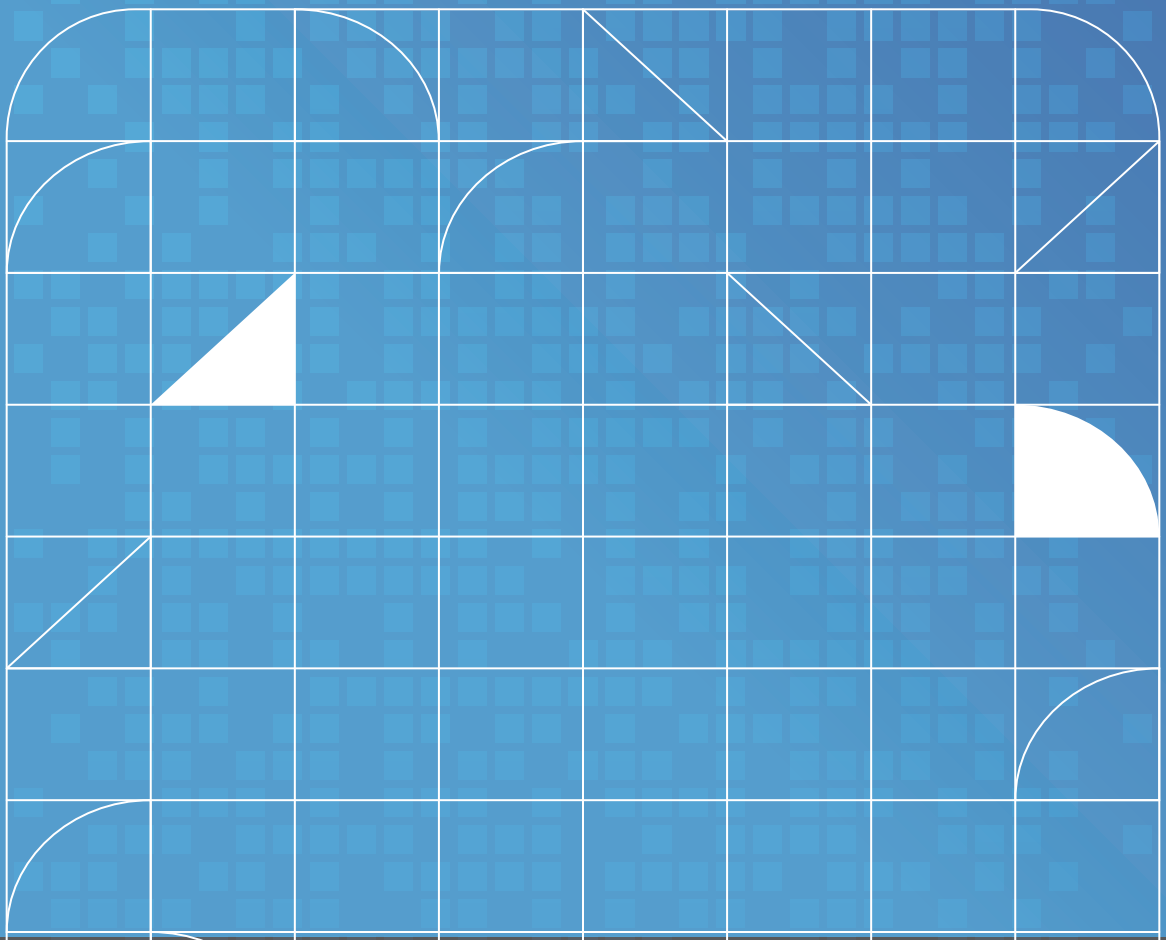
تنظیمات و کاربـران

- تنظیمات مختلف ماژول‌ها
- تنظیمات امنیتی سامانه
- امکان پشتیبانی از احراز هویت دو عاملی
- تعریف بخش‌ها و سمت‌ها (چارت سازمانی)
- امکان ورود اطلاعات از طریق فایل اکسل
- تعریف کاربران محلی یا ارتباط با اکتیودایرکتوری
- احراز هویت محلی یا مبتنی بر اکتیودایرکتوری
- رویدادنگاری سامانه
- قابلیت سلسله‌مراتبی و پشتیبانی از چندین سازمان زیرمجموعه



مشتریـان بادبـان





ABSHAR
DATA PROCESSING

داده پردازان آبشار

تهران، میدان آرژانتین، ابتدای بلوار آفریقا، پلاک ۱۲، واحد ۷

۰۹۱۹۵۰۰۰۷۵۳ - ۰۲۱۸۸۵۰۰۵۴۲

www.abshar.co , info@abshar.co