

NETWORK & SECURITY



DOURAN
GROUP

Network, Security, ERP, AI



تهران، خیابان شهید بهشتی، خیابان صابونچی
خیابان ایازی، پلاک ۶۲ ۰۲۱-۴۳۵۸۸

www.douran.com

www.douran.ir

ما برای آنگه ایران خانه خوبان شود، رنج دوران برده ایم

برخی از افتخارات گروه دوران

DOURAN
GROUP

DOURAN

www.douran.com
www.douran.ir

گروه دوران یکی از موفق‌ترین مجموعه شرکت‌های دانش‌بنیان می‌باشد. که با هدف ارائه محصولات و خدمات متنوع در زمینه فناوری اطلاعات و ارتباطات تأسیس گردیده است. این گروه که بیش از ۲۳ سال از تأسیس آن می‌گذرد با ساماندهی کادری «۵۰ نفره و بهره‌گیری از دانش روز دنیا، فعالیت گسترده‌ای در زمینه تولید و ارائه نرم‌افزار و تجهیزات و خدمات تخصصی در چارچوب ۷ گروه Security، ERP، Net work، Telecom، AI، Portal و Academy دارد. حضور پنج تیم تولید، فنی، سیستمی، بازرگانی و آموزشی در قالب یک گروه و همکاری نزدیک با شرکت‌های معتبر بین‌المللی، توان فنی و اجرایی بالایی را برای این گروه در زمینه اجرای پروژه‌های بزرگ ملی فراهم نموده است.

سرمایه‌های انسانی این مجموعه از مدیران با تجربه و کارشناسان خلاق و سخت‌کوش تشکیل یافته است و برای دستیابی به مأموریت گروه که اتصال، امن‌سازی و مکانیزاسیون سازمان هاست تلاش می‌کند.

«منتخب معاونت علمی و فناوری ریاست جمهوری به عنوان شرکت دانش بنیان

«مجری بزرگترین پروژه امنیت اطلاعات کشور

«مجری بزرگترین پروژه ERP داخلی کشور

«کسب رتبه برتر در بخش نرم افزار و امنیت شبکه الکامپ ۲۵

«عضو ۵۰۰ شرکت بزرگ ایران در سال مالی ۹۶ و ۹۷ طبق رتبه بندی شرکت های برتر سازمان مدیریت صنعتی

«دارای گواهینامه بین المللی ISO ۲۷۰۰۱

«دارای گواهینامه بین المللی ISO ۹۰۰۱

«دارای رتبه یک از شورای عالی انفورماتیک کشور در رشته‌های مختلف: تولید، نرم افزار، شبکه، امنیت، مشاوره، پشتیبانی، آموزش و پژوهش و غیر MainFrame

«دارای رتبه یک از سازمان فناوری اطلاعات ایران، در حوزه مشاوره و استقرار ISMS، ارزیابی امنیتی، امنیت فیزیکی و...

«دریافت برترین لوح و تندیس در جشنواره ملی ارتباطات و فناوری اطلاعات سالهای ۹۰، ۹۲، ۹۳، ۹۵، ۹۶، ۹۷

«تولید کننده یکی از قوی ترین فایروال های بومی (DSGate)، نصب شده در حساس ترین سازمان های کشور

«تولید کننده اولین IPS 40G پهنای باند اینترنت

«برترین شرکت در زمینه ارائه تجهیزات امنیتی خارجی با لایسنس و گارانتی معتبر

«عضو بانک اطلاعاتی صادر کنندگان کشور و اتحادیه صادر کنندگان نرم افزار

«دریافت لوح و تندیس برگزیده مدیر جهادی از سومین همایش مدیریت جهادی کشور

«دارای بیش از ۴۰۰ مشتری در ۵۵ شهرستان کشور و دهها کشور خارجی

«دارای بیش از ۳۰ پارتنر خارجی برای ارائه راه حل های 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 مهندسی رایانه ای استان تهران





DOURAN GROUP

www.douran.com
www.douran.ir

خدمات و محصولات حوزه شبکه و امنیت شرکت داده پردازان دوران

محصولات حوزه شبکه و امنیت

سیستم فایروال نسل جدید شامل قابلیت های UTM ، DPI ،NGFW	ARIO
فایروال مخصوص برنامه های تحت وب با قابلیت جلوگیری از حمله به وب سرورها	ARIO-WAF
سیستم سخت افزاری مدیریت یکپارچه تهدیدات (UTM) ، شامل مازول های VPN ،IDS/IPS، ...	DSGate
سیستم رمز کننده ترافیک شبکه لایه ۲ و ۳	Ario-VPN
راهکارهای جلوگیری از حملات DDoS	Ario-DDoS
راه حل جامع نرم افزاری و سخت افزاری مدیریت رخدادهای امنیتی جهت مراکز SOC	DSIEM
سیستم مانیتورینگ جامع تجهیزات شبکه های کامپیوتری و شبکه های صنعتی (نسل جدید سیستم NOC دوران)	NetAlive
سامانه مدیریت، نظارت و تعیین سطح دسترسی بر پروتکل های ارتباطی	PAM
راهکارهای آنتی ویروس و ضد بد افزار	راهکارهای آنتی ویروس و ضد بد افزار
گروه سیستم های ERP دوران (Infoyar) و راهکارهای هوش مصنوعی دوران (Douran Eye)	راهکارهای سازمانی دوران

خدمات و محصولات حوزه شبکه و امنیت شرکت داده پردازان دوران

خدمات حوزه شبکه و امنیت

مشاوره ، طراحی و پیاده سازی مرکز عملیات امنیت شبکه و مرکز عملیات مانیتورینگ شبکه	SOC/NOC
مشاوره، طراحی ، پیاده سازی و آموزش ISMS مبتنی بر استاندارد ISO27001	ISMS
مشاوره، طراحی ، پیاده سازی راهکارهای ایمن سازی شبکه	Network Security
آزمون نفوذ پذیری سازمان ها با استفاده از شبیه سازی حملات واقعی نفوذگران و ارائه گزارشات نفوذ پذیری	PenTest
مشاوره، طراحی، تامین تجهیزات ، نصب و راه اندازی مراکز داده	Data Center
برگزاری دوره های فوق تخصصی در حوزه ICT در داخل و خارج از کشور	Training

شرکت داده پردازان دوران به عنوان شرکت مادر گروه شرکت های دوران با تکیه بر بیش از ۲۳ سال تجربه حضور در صنعت فناوری ارتباطات و اطلاعات کشور توانمندی اجرای پروژه های امنیت های ملی و شبکه را در سطح پروژه ها و سازمان های ملی و کشوری دارا می باشد. این توانمندی بر سوابق و تجارب، سرمایه های انسانی متخصص و مجرب، تانیدیه ها و صلاحیت های قانونی و کشوری و رضایت مندی صدها سازمان و نگاه تکیه دارد.



محصول Ario شرکت داده پردازان دوران نسل جدید محصول پر قدرت DSGate و یک راه حل جامع برای مقابله با تهدیدهای شبکه و تامین دیواره آتش، بررسی ترافیک شبکه، مانیتورینگ رفتارهای کاربران و برنامه‌های کاربردی، محافظت از اطلاعات و خدمات سازمان، اندازه گیری ایمنی ترافیک، پالایش Accounting, DPI, VPN, Server & Multiple Gateway Load Balancing, SSL Inspection, Captive Portal گزارش های جامع و نمودارهای مختلف است. مدیران شبکه می توانند سیاست های مختلفی را جهت بررسی و مانیتورینگ پهنای باند، مدیریت برنامه های کاربردی و ... اعمال نمایند.

با توجه به توسعه زیرساخت های ارتباطی در سازمان ها و به تبع آن گسترش استفاده از اینترنت در سازمان ها، همواره امنیت، مانیتورینگ و تحلیل ترافیک شبکه برای مدیران در سازمان امر بسیار مهمی بوده است. همچنین با تحلیل این گزارش ها مدیران شبکه می توانند تهدیدات امنیتی و ترافیکی را قبل از بروز مشکل شناسایی و رفع کنند و در نهایت روند کاری شبکه خود را بصورت گرافیکی و ملموس مشاهده کنند. در همین راستا شرکت داده پردازان دوران اقدام به طراحی و تولید محصول جدیدی با نام Ario کرده است. این محصول با پیشوانه سال ها تحقیق و تجربه در زیرساخت های بزرگ کشور و همچنین تیمی متخصص و کاملاً حرفه ای تولید شده است.

DOURAN
www.douran.com
www.douran.ir



ARIO

DPI (Deep Packet Inspection)
NGFW (Next Generation Firewall)
UTM (Unified Threat Management)
WAF (Web Application Firewall)
Accounting
Traffic Analyzer



طبقه بندی ترافیک

« این محصول قابلیت طبقه بندی ترافیک بر اساس معیارهای مختلف مانند پروتکل، برنامه های کاربردی، آدرس وب و ... را ارائه می کند.

مدیریت ترافیک شبکه

« قابلیت تعریف چندین صف ترافیکی
« قابلیت تعریف و اختصاص پهنای باند بر اساس کاربر، گروه، پروتکل، برنامه های کاربردی، کاربران و یا گروه دیگر
« قابلیت الویت بندی ترافیک

مسیریابی بر اساس معیارهای کیفی ترافیک

« اندازه گیری کیفیت APP های دلخواه روی لینک های مختلف و انتخاب لینک بر اساس کیفیت بهتر
« مسیریابی بر اساس تعداد Session بر روی هر لینک

Application / Protocol Control

« شناسایی بیش از صد پروتکل و صدها برنامه کاربردی مبتنی بر الگو (Pattern-Based)، رفتار برنامه و Heuristic
« تشخیص برنامه های ناشناخته بر اساس قواعد تعریف شده توسط کاربر و اعمال کنترل روی آنها
« قابلیت تعریف الگوی دلخواه برای شناسایی برنامه های اختصاصی سازمان
« قابلیت مسدودسازی برنامه های کاربردی هم در جهت ارسال و هم دریافت
« قابلیت کنترل برنامه ها بر اساس زمان
« الویت بندی پهنای باند برای برنامه های حیاتی
« قابلیت فیلترینگ معکوس روی برنامه های کاربردی

Proxy & SSL Inspection

« بازرسی عمیق ترافیک هایی که به صورت SSL Encrypted در حال رد و بدل هستند

Intrusion Control

« طراحی و پیاده سازی Engine به صورت کاملاً بومی و بدون استفاده از محصولات Open Source
« تشخیص و پیشگیری از بیش از 15000 حمله رایج در لایه های مختلف
« شناسایی مبتنی بر الگو و رفتار
« طبقه بندی حملات بر اساس میزان حساسیت با امکان تغییر توسط کاربر
« بروزرسانی بانک حملات به صورت خودکار و دستی
« تشخیص و جلوگیری از ترافیک و پروتکل های ناهنجار
« تولید گزارشات جامع از حملات و رفتارهای مشکوک

URL Filtering

« قابلیت پالایش کلیه ترافیک
« قابلیت تعریف محدودیت بر اساس سیاست های مختلف
« امکان اعمال محدودیت کاربران

ARIO DOURAN

محمول آریو

DPI (Deep packet Inspection)

- « قابلیت شناسایی برنامه های کاربردی
- « قابلیت شناسایی برنامه های پرکاربرد در ایران
- « قابلیت مسدودسازی و یا اعمال محدودیت بر روی پهنای باند مورد استفاده توسط هر پروتکل و یا برنامه

اندازه گیری کیفیت ترافیک مصرفی (QOE)

- « قابلیت اندازه گیری Packet Loss و Latency به تفکیک پروتکل، برنامه های کاربردی و آدرس
- « قابلیت اندازه گیری میزان DNS Retransmit و DNS Lost ...

احراز هویت کاربران

- « روش های متنوع احراز هویت کاربران و اعمال سیاست بر اساس نام کاربری
- « پشتیبانی از پروتکل های Radius، LDAP و احراز هویت بصورت Local

مدیریت و گزارش گیری متمرکز

- « مدیریت چند دستگاه از طریق کنسول مرکزی
- « جمع آوری و مرتب سازی Log از چندین دستگاه به صورت متمرکز

اندازه گیری ایمنی ترافیک (Safety Level)

- « این محصول به صورت اتوماتیک برای هر اتصال، سطح ایمنی مشخص می کند. این سطح با استفاده از پارامترهای مختلف ارزیابی می گردد.

SSO Plus Module (Optional)

- « قابلیت دریافت اطلاعات کاربران شامل نوع سیستم عامل، وضعیت آنتی ویروس، وضعیت فایروال، نام کامپیوتر و ... بدون نیاز به نصب (Agent)
- « قابلیت تعریف سیاست های مختلف بر اساس اطلاعات اخذ شده
- « بررسی و مشاهده وضعیت کاربران در بازه های زمانی مختلف
- « قابلیت امتیازدهی به کاربران بر اساس وضعیت امنیتی سیستم
- « امکان محدودسازی کاربران بر اساس IP

Log & Report

- « امکان ارائه گزارش های مختلف بر اساس میزان مصرف کاربران و IP و برنامه های مختلف در بازه های زمانی و پارامترهای مختلف
- « امکان تولید لاگ در سطوح مختلف (System, Session, Real Time)
- « پشتیبانی از Protocol, Group, User, DstIP, SrcIP, DstPort, SrcPort در لاگ ها
- « قابلیت مشاهده وضعیت ترافیک از سیستم بصورت Real Time
- « امکان ذخیره محلی لاگ ها و پشتیبانی از Syslog
- « امکان گزارش کامل از وضعیت حجم مصرفی و ترافیک مصرفی کاربران
- « ایجاد فایل گزارش با فرمت های مختلف، ذخیره و یا ارسال آن
- « گزارش سایت های بازدید شده توسط کاربر
- « ارائه لاگ فعالیت های کاربر مدیر دستگاه
- « گزارش های مقایسه ای از آمار ترافیک در زمان های مختلف
- « ارائه تاریخچه مصرف کاربران و برنامه ها در بازه های زمانی مشخص شده
- « ارائه Session Log بر اساس فرمت های تعریف شده

FEATURES

- » AI-based Machine Learning
- » Automatic profiling (white list)
- » Web server and application signatures (black list)
- » IP Reputation
- » IP Geolocation and BGP AS number
- » HTTP RFC compliance
- » Native support for HTTP/2
- » WebSocket protection and signature enforcement

Deployment Options

- » Reverse Proxy
- » Inline Transparent
- » True Transparent Proxy
- » Offline Sniffing

Application Delivery

- » Layer 7 server load balancing
- » URL Rewriting
- » Content Routing
- » HTTPS/SSL Offloading

Authentication

- » Active and passive authentication
- » Site Publishing and SSO
- » SSL client certificate Support

Other

- » IPv6 Ready
- » Clustering
- » High Availability (Active-Active, Active-Passive)

Security Service

- » Web Services signatures
- » XML and JSON protocol conformance
- » Malware detection
- » Protocol Validation
- » Brute force protection
- » Syntax-based SQLi detection
- » HTTP Header Security
- » Operating system intrusion signatures
- » L2-L7 Stateful Network Firewall
- » DDoS prevention
- » Advanced correlation protection
- Using multiple security elements
- » Web Defacement Protection

Application Attack Protection

- » OWASP Top 10
- » Cross Site Scripting
- » SQL Injection

Web Security

- » Cross Site Request Forgery
- » Session Hijacking
- » Built- in Vulnerability Scanner
- » Third-party scanner integration (virtual patching)

Application Attack Protection

- » Web user interface
- » REST API
- » Centralized login and reporting
- » User/device tracking
- » Real- time dashboards
- » OWASP Top 10 attack categorization
- » Geo IP Analytics

عنوان مثال با استفاده از قابلیت Machine Learning موجود در این محصول، می توان Pattern مربوط به ترافیک شبکه خود را شناسایی کرده و در صورت مشاهده ترافیک مشکوک و مغایر با Pattern شناسایی شده آن را مسدود نمود.

اصولا Ario-WAF به عنوان یک راه حل امنیتی کارآمد، به منظور هماهنگی با دیگر راه حل های امنیتی شبکه مانند فایروال ها و سیستم های پیشگیری از نفوذ برای ارائه یک استراتژی جامع امنیتی به کار برده می شود.

در حال حاضر وب سرورها و برنامه های کاربردی تحت وب بزرگترین هدف هکرها جهت نفوذ به زیرساخت های اطلاعاتی شرکت ها و سازمان ها می باشند و با توجه به رشد روز افزون این حملات، فایروال برنامه های کاربردی تحت وب (Web Application Firewall) به منظور مقابله با این حملات عرضه شده است.

در این راستا محصول Ario-WAF با هدف مقابله با انواع تهدیدهای برنامه های تحت وب و محافظت از اطلاعات و خدمات سازمان ها طراحی شده است. این محصول کلیه سرویس های امنیتی مورد نیاز برای جلوگیری از حملات تحت وب را با کارایی بالا ارائه می نماید.

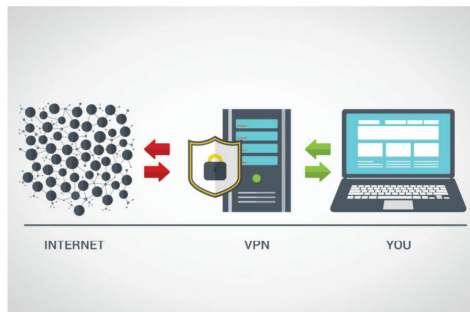
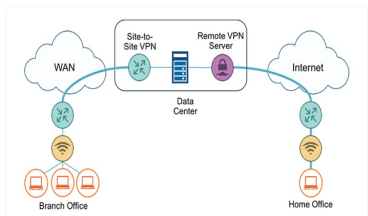
محصول Ario-WAF تهدیدات لایه ۷ را به صورت کامل شناسایی و بررسی می نماید و با استفاده از Signature های قدرتمندتر (در قیاس با فایروال های سنتی) با تحلیل منطق و رفتار و ترافیک Request و Response، از وب سایت و وب سرورها در برابر حملات اینترنتی محافظت به عمل می آورد.

با استفاده از Ario-WAF نه تنها می توان حملات شناخته شده را شناسایی نمود، بلکه می توان از حملات ناشناخته Zero Day نیز جلوگیری کرد. به

ARIO-WAF

Douran Web Application
Firewall

فایروال مخصوص برنامه های تحت وب
جهت جلوگیری از حمله به وب سرورها



ویژگی‌های کلیدی

- « امکان اضافه کردن الگوریتم جدید رمز کننده و استفاده از الگوریتم های بومی مراکز حساس امنیتی توسط مدیر سیستم »
- « امکان رمز کردن کلیه اطلاعات شبکه هم در لایه ۲ و هم در لایه ۳ »
- « مجهز به سیستم تشخیص هویت جهت شناسایی Device های مجاز و غیرمجاز »
- « امکان ارتباط با قفل سخت افزاری (که توسط مدیر برنامه ریزی می‌شود) از طریق USB »
- « اختصاص یک حافظه بر روی سیستم جهت نگهداری کلیدهای رمز کننده ها و سایر اطلاعات امنیتی و امکان دسترسی مستقیم مدیر سیستم به این حافظه »
- « امکان اختصاصی نمودن مکانیزم احراز هویت رمزنگاری و توافق کلید توسط مدیر سیستم »
- « ارسال تمامی اطلاعات بصورت رمز شده »
- « پشتیبانی از انواع الگوریتم های رمز کننده »
- « پشتیبانی از توزیع بار بر روی چند تونل و تشخیص قطع شدن تونل »
- « اعمال قواعد مدیریت پهنای باند به ازاء کاربر ، سرویس و نرم افزار »

موارد کاربرد

- « رمزنگاری ارتباط مراکزی با داده های حساس »
- « ایجاد مسیر امن برای انتقال داده های دارای طبقه بندی در مراکز حساس امنیتی »
- « سازمان ها و شرکت هایی با شعب و دفاتر پراکنده »
- « سازمانهایی با توپولوژی شبکه ای پیچیده بدلیل سهولت قرارگیری در شبکه »

www.douran.com
www.douran.ir

سیستم رمز کننده ترافیک شبکه لایه ۲ و ۳

امروزه اشتراک گذاری داده ها و دسترسی سریع به منابع و سرورهای اطلاعاتی امری ضروری می‌باشد که به لحاظ مشکلات بالای امنیتی شامل تضمین محرمانگی ، صحت داده های تبادل یافته و عدم انکار در سازمانها از آن استفاده نمیشود. محصول Ario-VPN یک محصول کاملا بومی به منظور ایجاد بستر لازم برای تبادل داده در شبکه های ناایمن است.

محصول Ario-VPN به منظور اتصال امن بین سازمانها و شعب آنها در بستر اینترنت است که با استفاده از الگوریتمهای استاندارد و بومی و با پشتیبانی انواع پروتکل VPN با تنظیمات ایجاد تغییر در شبکه نصب می



ویژگی های راه حل:

- « قرارگیری در شبکه در مدل های مختلف (Layer ۳ – Bridge – Tap)
- « توانایی شناسایی حملات در مدل های مختلف (Protocol – Volumetric – Application Layer)
- « کنترل آمار بر اساس پارامترهایی نظیر (PPS – SPS – Inbound – Outbound) بر روی حملات، برنامه ها و ...
- « نمایش وضعیت شبکه بصورت گرافیکی (Network Visualization)
- « شناسایی رفتار مشکوک در بستر شبکه
- « سفید سازی ترافیک و جدا کردن ترافیک حملات از ترافیک عادی و سالم
- « تشخیص کامل Session initiate شده بر اساس (IP, AS, Geo) ...
- « سفید سازی برنامه ها نظیر فیلیمو، آپارات و ... بر اساس الگو
- « سفید سازی بر اساس IP, AS, Geo و ...
- « امکانات کامل بر روی IDS/IPS و WAF
- « قابلیت نمایش اطلاعات آماری در برنامه های جانبی اعم از بومی، OpenSource و ...
- « دارای لیست IP Reputation
- « دارای لیست Bad Domain
- « استفاده درست از منابع و پیکربندی در هنگام حملات برای جلوگیری از Bypass
- « انواع مختلف اکشن ها در صورت شناسایی حملات
- « توانایی اعمال اکشن در صورت تشخیص حمله بر روی ISP بالا دست بر اساس مسیریابی
- « قابلیت پیکربندی تمام ماژول های سیستم توسط کاربر
- « قابلیت تجمیع کردن لاگ های سیستم برای ارسال به سیستم مانیتورینگ

Ario DDoS DOURAN

www.douran.com
www.douran.ir

Ario DDoS

راهکارهای جلوگیری از حملات DDoS

محصول ArioDDoS برای جلوگیری از حملات DDoS با تکنیک ها و الگوریتم های مختلف در شبکه هایی با ابعاد کوچک تا بزرگ طراحی شده است. این محصول امکانات فراوانی برای شناسایی حملات در لایه های مختلف شبکه و نوع های مختلف حملات DDoS را دارا می باشد. همچنین این محصول توانایی شناسایی حملات در بستر وب، کلاینت ساید و سرور ساید را نیز دارا می باشد.

مخاطبین این محصول:

- « سازمان های زیرساختی و ارائه کننده پهنای باند
- « ارائه کنندگان سرویس اینترنت و هاستینگ
- « سازمان ها و اداراتی که سرویس های خود را روی اینترنت ارائه می کنند.

DSIEM

DOURAN SIEM

سیستم مدیریت رخدادهای امنیتی دوران

سیستم SIEM دوران، به جهت تجزیه و تحلیل بلادرنگ داده های امنیتی برای مقابله با تهدیدهای داخلی و خارجی در مراکز SOC تولید شده است. همچنین وظیفه این سیستم جمع آوری، ذخیره سازی، تحلیل و گزارش روی داده های ابزارها، نرم افزارها و برنامه های کاربردی سازمانها برای پاسخ به حوادث، پیگیری قانونی و تنظیم مجدد قوانین تطبیقی می باشد.

این سیستم، با ایجاد یک چتر امنیتی روی کلیه تجهیزات و نرم افزارهای سازمان، تمامی رخدادها را دریافت کرده و بصورت بلادرنگ آنها را نرمال سازی کرده و جهت تشخیص رخدادهای بهم پیوسته ی غیر معمول، آنها را به موتور تحلیل گر ارسال می کند. موتور تحلیل گر دوران با کمک پایگاه دانش قوی، بصورت بلادرنگ فعالیت های مشکوک را تشخیص داده و پس از اولویت بندی و تشخیص میزان ریسک، بلافاصله آن را گزارش می نماید. از ویژگی های سیستم SIEM دوران ارتباط مستقیم و لحظه ای با سامانه های تیکتینگ مانند جیرا و سامانه های پاسخ دهی به تهدیدات مانند ITSM و ITOM می باشد.

امکانات

- « دریافت اطلاعات ترافیک شبکه و ثبت، گزارش گیری و استفاده از آن در موتور تحلیل گر
- « رمزگذاری و فشرده سازی انتقال اطلاعات بین تجهیزات و سرورهای دریافت لاگ
- « تشخیص لاگ های تجهیزات متنوع و تبدیل به فرمت استاندارد و یکسان سازی شده
- « پایگاه دانش قوی برای تشخیص سناریوهای مختلف حملات، خرابکاریها و هر نوع اتفاق ناخوشایند در سیستمها
- « امکان اضافه کردن سناریوهای جدید به پایگاه دانش جهت مقابله با تهدیدهای جدید بصورت ترکیبی از قوانین و شرایط بر روی داده های مختلف تجهیزات
- « پشتیبانی از ایجاد لیست های پویا و بکارگیری آنها در موتور تحلیل گر
- « ارسال انواع هشدار با امکان زمانبندی و سطح بندی و انجام خودکار عملیات اصلاحی
- « انجام انواع اکشن اتوماتیک در صورت رسیدن به شرایط از پیش تعیین شده
- « ذخیره سازی لاگ ها برای مدت طولانی و گزارش گیری روی آنها
- « پشتیبانی از حجم بسیار بالای لاگ با EPS های بسیار زیاد
- « داشبوردهای مدیریتی متنوع جهت کارشناسان و مدیران با امکان ساخت داشبورد جدید
- « گزارشات تحلیلی و پویای متنوع جهت تحلیل اطلاعات
- « قابلیت رویکرد ردیابی و حفاظت از Endpoint ها (EDR)
- « قابلیت ادغام محصولات و سرویس های مختلف در Agent محصول دوران SIEM (کمک به شناسایی تهدیدات و اعمال محدودیت ها)
- « قابلیت توزیع پذیر بودن محصول برای پیاده سازی در سازمان هایی با مقیاس بالای داده
- « جداسازی رویدادها و هشدارهای مهم از موارد کم اهمیت و بدون استفاده



DOURAN

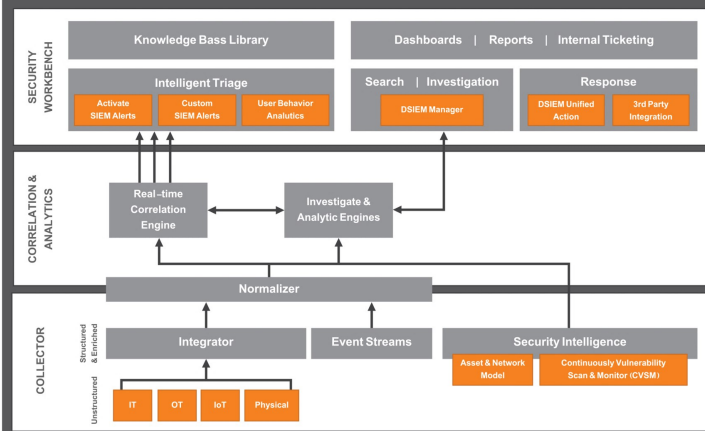
www.douran.com
www.douran.ir



DSIEM

DOURAN SIEM

DSIEM Architecture





DOURAN-PAM

راهکار امنیتی برای نظارت و مدیریت سطح دسترسی دوران

بخش اعظم تهدیدات بصورت سهوی یا عمدی از داخل سازمان ها اتفاق می افتد. استفاده از این راهکار امنیتی، باعث امن نگه داشتن سازمان شما در مقابل حوادث ناخواسته یا سو، استفاده از سطوح بالای دسترسی می شود. برخی از کاربران با دسترسی بالا می توانند پروتکل های امنیتی موجود را نادیده بگیرند و آنها را دور بزنند. این یک آسیب پذیری بزرگ برای امنیت سازمان است که با استفاده از PAM می توان این موضوع را مدیریت نمود. در ضمن رویکرد جهانی به دورکاری کارکنان و ضرورت دسترسی راه دور آنها به منابع IT، بیش از گذشته نیاز به راهکار PAM و مدیریت سطح دسترسی را برای سازمان ها ضروری ساخته است.

مزایا و قابلیت ها

- « طبقه بندی کاربران و تعیین سطح دسترسی مشخص به هر کدام که می توانند دسترسی محدود یا بالا داشته باشد
- « عدم نیاز به پسوردهای مستقیم برای استفاده از منابع مشخص شده برای هر کاربر
- « ایجاد سیستم نظارت مداوم برای کاربران بصورت ضبط تصویر یا ذخیره دستورات وارد شده
- « محدودسازی کاربران بعد از اتصال به منابع تعریف شده بر اساس پروتکل های استاندارد، مانند عدم استفاده از Clipboard
- « ایجاد تاریخچه عملکرد هر کاربر بر اساس (منابع استفاده شده، تاریخ، ساعت، مدت زمان اتصال و ...)
- « امکان قطع یک ارتباط باژ توسط مدیر سامانه
- « پشتیبانی از ۴ پروتکل رایج دسترسی از راه دور: RDP و TELNET, SSH, VNC
- « عدم نیاز به پسوردهای مستقیم سیستمی برای کاربران
- « قابلیت اتصال و استفاده از طریق دستگاه های Touch مانند تلفن همراه هوشمند یا تبلت
- « ایجاد دسترسی برای کاربران به یک یا مجموعه ای متفاوت از منابع ناهمگون
- « ایجاد سیستم نظارت نامحسوس برای منابع با اطلاعات طبقه بندی شده
- « پشتیبانی از احراز هویت چند وجهی
- « محدودسازی کاربران برای دسترسی به منابع شبکه در روزها و ساعت های از پیش تعیین شده
- « محدودسازی تعداد اتصالات همزمان کاربران به یک منبع
- « محدودسازی کاربران به اجرای یک برنامه خاص
- « محدودسازی استفاده از کلیپبورد به منظور انتقال دو طرفه اطلاعات
- « محدودسازی نقل و انتقال دو طرفه فایل
- « محدودسازی تنظیمات ظاهری مانند (menu animation, Aero, theme, wallpaper)
- « محدودسازی سخت افزاری (printing, audio)
- « مشاهده فهرست اتصالات در حال انجام و خاتمه پذیرفته به همراه جزئیات اتصال
- « دریافت کامل تعامل کاربر بصورت فایل ویدئو
- « قابلیت جستجو در ورودی های صفحه کلید به منظور یافتن دستورات یا ورودی های مخاطره آمیز
- « قطع دسترسی کاربر بصورت لحظه ای
- « امکان Export تعامل کاربر بصورت ویدئو (صفحه نمایش) و فایل های متنی (کیبورد)
- « طبقه بندی کاربران و امتیاز دسترسی مشخص به هر کدام

www.douran.com
www.douran.ir

NetAlive

DOURAN Monitoring System

سیستم مانیتورینگ تجهیزات دوران

با گسترش بکارگیری تجهیزات و نرم افزارهای مختلف در سازمانها ، همواره یکی از مشکلات راهبران شبکه ها این بوده است که چگونه از صحت عملکرد این تجهیزات مطمئن شوند. بدین جهت ، محصول مانیتورینگ دوران ، با هدف بهینه سازی کارایی و دسترسی پذیری زیرساخت های فناوری اطلاعات تولید شده است .

مانیتورینگ دوران به شما در شناسایی و رفع سریع گلوگاهها و قطع ارتباطاتی که اهداف کلیدی را تهدید می کنند یاری می رساند و شما می توانید با استفاده از محصولات تکمیلی دیگر دوران مراحل رفع مشکلات را نیز مدیریت نمایید .

برخی از امکانات مهم

- « امکان تشخیص اتوماتیک تجهیزات شبکه با روش های مختلف و مانیتورینگ آنها
- « پشتیبانی از انواع پروتکل های کاربردی جهت مانیتورینگ مانند: (SNMP ، تمامی ورژن ها) ، Telnet ، WMI ، ICMP ، ... ،
- « پشتیبانی از انواع روش های خاص مانیتورینگ برای مانیتور کردن دیتابیسها ، مجازی سازی ها ، وب سرورها ، میل سرور ها و Storage ها
- « امکان مانیتورینگ تجهیزات صنعتی
- « قابلیت مانیتورینگ تجهیزات ، بررسی شرایط محیطی
- « امکان مانیتورینگ دیتاسترها و مراکز عملیات

- « امکان استفاده از نقشه های متنوع و تو در تو و گراف های آنلاین برای نمایش وضعیت تجهیزات و ارتباط بین آنها
- « سیستم ارسال هشدار با امکان تعیین نوع هشدار و طبقه بندی و مرحله بندی ارسال شامل هشدارهای پیام کوتاه، ایمیل، کارتابل، ساخت تغییرات و پیگیری راه دور، اجرای دستور خاص، ...
- « انجام انواع اکشن اتوماتیک در صورت رسیدن شرایط از پیش تعیین شده
- « امکان بکارگیری سیستم با استفاده از Agent و یا بدون Agent
- « امکان Categorize کردن مانیتور ها و نتایج آنها

- « امکان تعریف بازه های زمانی ثابت و متغیر برای آیتمها
- « دارا بودن موتور تحلیل گر بسیار قوی و با سرعت بالا
- « داشبوردهای مدیریتی متنوع جهت کارشناسان و مدیران با امکان ساخت داشبورد جدید و اشتراک داشبوردها
- « گزارشات پویای متنوع جهت تحلیل اطلاعات در بازه های زمانی متنوع
- « ارتباط با سایر سیستم های دوران مانند Service Desk جهت مدیریت حوادث و مشکلات و همچنین مدیریت تجهیزات IT
- « پلتفرم قدرتمند دارای دیتابیس ORACLE

راهکارهای ضد بدافزار و آنتی ویروس

در دنیای امروز با توجه به وجود انواع تهدیدات سایبری پیشرفته مانند APT ها، باج افزارها و ...، حفاظت از کسب و کار امری اجتناب ناپذیر است. نصب و پیاده سازی آنتی ویروس جز، مهم ترین و ضروری ترین راهکارهای تامین امنیت در سازمان می باشد. در این میان انتخاب آنتی ویروس مناسب بر اساس نیاز و منابع سازمان و پیاده سازی آن به شکل صحیح مهم ترین دغدغه خواهد بود. شرکت دوران با تامین لایسنس از تولید کنندگان اصلی و ارائه مشاوره، نصب و پیاده سازی آنتی ویروس توسط کارشناسان خبره، پاسخگوی نیاز سازمان ها در برابر بدافزارها و تهدیدات سایبری می باشد. همچنین این شرکت توانسته است با ارائه بهترین برندهای آنتی ویروس در بازار و با تکیه بر توانایی های تیم تخصصی آنتی ویروس خود، در صدر بهترین شرکت های ارائه کننده آنتی ویروس در کشور قرار گیرد.

ANTI-VIRUS SOLUTIONS



چرا دوران؟

- « ارائه لایسنس اصلی از تولید کنندگان مطرح دنیا
- « تجربه پیاده سازی آنتی ویروس در بیش از دو هزار سازمان مختلف در سطح کشور
- « دارای نمایندگی رسمی با بالاترین درجه از معتبرترین شرکت های تولید کننده محصولات ضد بدافزار
- « تیم پشتیبانی تخصصی آنتی ویروس دارای گواهی های معتبر فنی از تولید کنندگان محصول
- « ارائه مشاوره، پیاده سازی و آموزش آنتی ویروس در سازمان های کوچک و بزرگ
- « دارای گواهی نصب و پشتیبانی محصولات فتا از سازمان فناوری اطلاعات ایران (گواهینامه افتا)
- « ارائه محصولات کارآمد در حوزه End-Point Security از جمله محصول بومی Desktop Suite

OUR CLIENTS

برخی از مشتریان گروه دوران

نهادهای حاکمیتی و قوه قضائیه و مقننه

مجلس شورای اسلامی، صدا و سیما، جمهوری اسلامی ایران، سازمان پزشکی قانونی کشور، سازمان زندان ها و اقدامات تامینی و تربیتی کشور، سازمان تعزیرات حکومتی کشور، سازمان روزنامه رسمی کشور، دانشگاه علوم قضائی

ریاست جمهوری

سازمان حفاظت محیط زیست، مرکز آمار ایران، سازمان بورس و اوراق بهادار، سازمان ملی استاندارد ایران، سازمان خصوصی سازی، سازمان هوا و فضا، مرکز ملی علوم و فنون لیزر ایران، سازمان بهزیستی کشور، سازمان هدفمند سازی یارانه ها، سازمان اسناد و کتابخانه ملی ایران

وزارت ارتباطات و فناوری اطلاعات

سازمان تنظیم مقررات و ارتباطات رادیویی، شرکت ارتباطات زیرساخت، سازمان فناوری اطلاعات، پارک فناوری اطلاعات و ارتباطات، شرکت مخابرات ایران، شرکت پست، پست بانک ایران، پژوهشگاه علوم و فناوری اطلاعات ایران

وزارت نیرو

وزارت نیرو، شرکت توانیر، شرکت های برق منطقه ای

تهران، زنجان و ایلام، شرکت آب و نیرو، شرکت آب و برق خوزستان، سازمان انرژی های تجدیدپذیر و بهره وری انرژی برق، شرکت های آب و فاضلاب یاسوج، سیستان و بلوچستان و شرکت توزیع برق های تبریز، مازندران و ...

وزارت نفت

شرکت ملی نفت ایران، شرکت ملی گاز ایران، هلدینگ پتروشیمی خلیج فارس، شرکت پژوهش و فناوری پتروشیمی، شرکت ملی حفاری ایران، مناطق نفت خیز جنوب، شرکت های ملی پخش فرآورده های نفتی استان های کرمان، ایلام، هرمزگان و شرکت گاز استان های اصفهان، سمنان و خراسان جنوبی، پژوهشگاه صنعت نفت، صندوق بازنشستگی صنعت نفت، شرکت پالایش نفت کرمانشاه، پالایشگاه آبادان، شرکت نفت خزر، پالایشگاه شیراز، شرکت نفت ایرانول، نفت و گاز اروندان، خطوط لوله و مخابرات نفت، بهره برداری نفت و گاز گچساران، شرکت های پتروشیمی لرستان، کارون، ماهشهر، بیستون و بیمارستان منابع پتروشیمی ماهشهر

وزارت علوم، تحقیقات و فناوری

دانشگاه های تهران، ارومیه، سلمان فارسی، مازندران، امام

صادق، علوم و معارف، صنعتی کرمانشاه، مذاهب اسلامی، تربیت مدرس، علوم بهزیستی و توانبخشی، امیرالمومنین، میبد و دانشگاه های آزاد اسلامی، سازمان مرکزی جنوبی و سازمان حفظ نباتات، سازمان مرکزی تعاونی روستایی

بانک ها و موسسه های مالی و اعتباری

بانک ملی ایران، بانک رفاه، بانک ملت، بانک تجارت، بانک کشاورزی، بانک مسکن، بانک توسعه تعاون، بانک پارسیان، بانک شهر، بانک کارآفرین، موسسه مالی و اعتباری ثامن، اقتصاد نوین، پست بانک و ...

وزارت بهداشت، درمان و آموزش پزشکی

سازمان انتقال خون، دانشگاه های علوم پزشکی اهواز، تبریز، سیستان و بلوچستان، همدان، گلستان، اراک و بیمارستان های خاتم الانبیا، امام علی، پارس، روحانی، ۲۲ بهمن و سازمان بیمه سلامت

وزارت جهاد کشاورزی

سازمان تحقیقات، آموزش و ترویج کشاورزی، سازمان جنگل ها و مراتع کشور، سازمان دامپزشکی کشور، سازمان امور

عشایر ایران، سازمان شیلات ایران، سازمان جهاد کشاورزی استان های ایلام، خراسان جنوبی، هرمزگان، تهران، خراسان جنوبی و سازمان حفظ نباتات، سازمان مرکزی تعاونی روستایی

وزارت صنایع و معادن

سازمان توسعه تجارت ایران، سازمان صمت استان های آذربایجان شرقی، اردبیل، ایران خودرو، سایپا

سایر وزارتخانه ها

وزارت تعاون، کار و رفاه اجتماعی، وزارت میراث فرهنگی، گردشگری و صنایع دستی، وزارت کشور، وزارت ورزش و جوانان، وزارت راه و شهرسازی، سازمان هواشناسی کشور، سازمان تامین اجتماعی، سازمان حج و زیارت، سازمان اوقاف و امور خیریه، هواپیمایی جمهوری اسلامی ایران هما، استانداری های تهران، خوزستان، ایلام، خراسان رضوی و ...

www.douran.com
Info@douran.com