
APK
Engineering and Technical Company
Amn Pardazan Kavir

حس خوب اعتماد...

شرکت فنی و مهندسی
APK | امن پردازان کویر

ماموریت: ایجاد سازمان امن

موقعیت فعلی: جز، پنج شرکت برتر ایران در حوزه امنیت شبکه و اطلاعات

چشم انداز ۱۴۰۴: یکی از سه شرکت پیشرو در زمینه امنیت سایبری در منطقه خاورمیانه

+2000
پروژه های انجام شده

+1000
مشتـــری

1
رتبه یک انفورماتیک

+100
نیروی متخصص

+10
نماینده فعال

8
محصول بومی تولید شده

+15
مجوز و گواهینامه داخلی و خارجی معتبر

+8
سال سابقه تولید محصول سایبری

+10
سال فعالیت در ارائه خدمات امنیتی

Engineering and Technical Company
Amn Pardazan Kavir

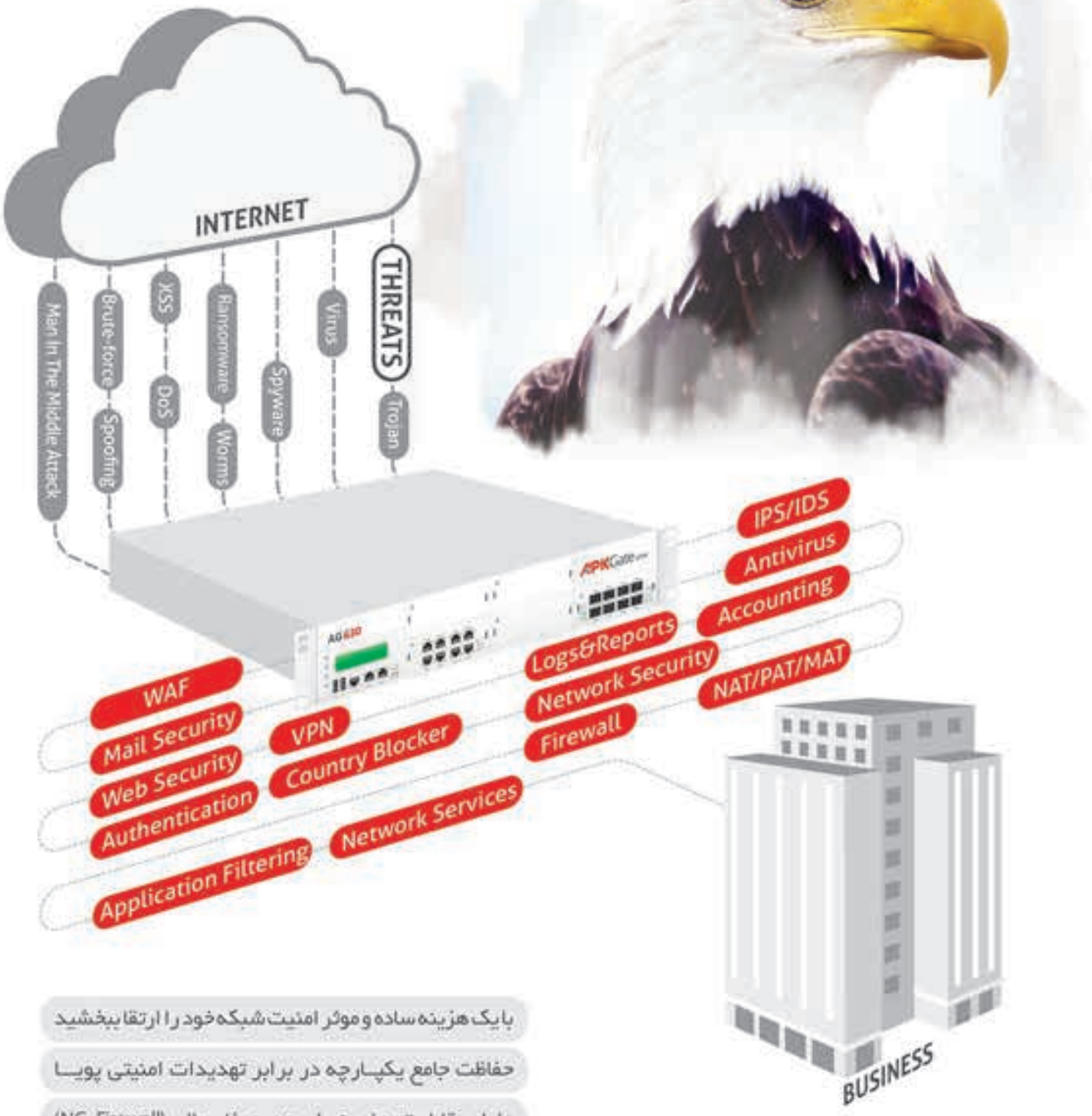
- **رتبه یک** شورای عالی انفورماتیک در زمینه امنیت فضای تبادل اطلاعات
- **رتبه یک** نما در حوزه مشاوره و استقرار استانداردهای امنیت اطلاعات **(ISMS)**
- مجوز افتا در حوزه پیاده سازی مرکز عملیات امنیت و نیم پاسخ به رخداد **(SOC/CERT)**
- مجوز افتا در حوزه ارزیابی امنیتی و **تست نفوذ**
- مجوز افتا در حوزه **امن سازی** و مقاوم سازی سامانه ها، زیر ساخت ها و سرویس ها
- مجوز افتا در حوزه **خدمات فنی** افتا
- مجوز افتا در حوزه پیاده سازی **امنیت فیزیکی** و محیط پیرامونی
- دارای مجوز **دانش بنیان** بودن محصولات

APKGate

Unified Threat Management

سیستم مدیریت یکپارچه تهدیدات

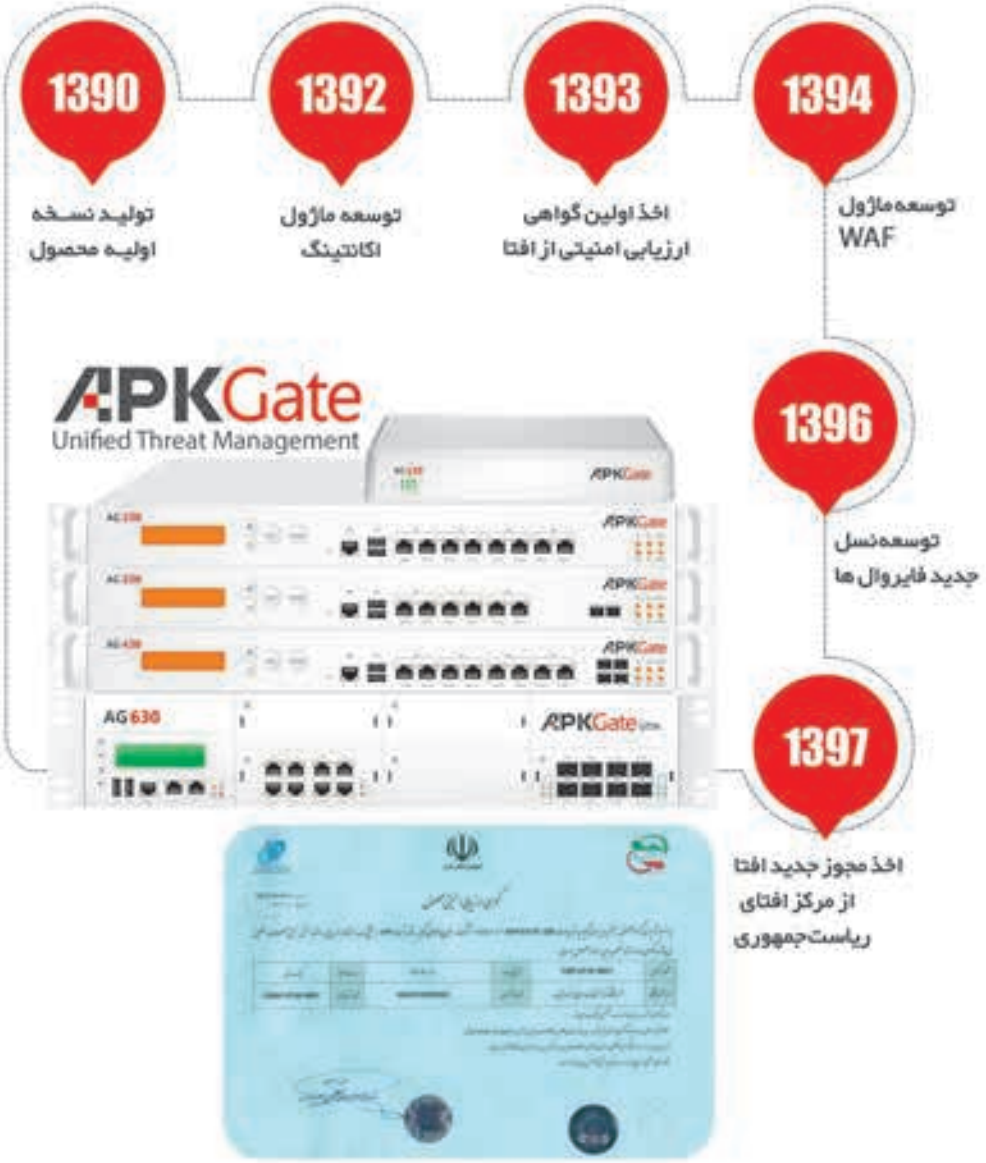
UTM



با یک هزینه ساده و موثر امنیت شبکه خود را ارتقا ببخشید

حفاظت جامع یکپارچه در برابر تهدیدات امنیتی پویا

دارای قابلیت های نسل جدید فایروال (NG Firewall)



- تنها محصول UTM بومی دارای مجوز جدید افتا از مرکز افتای ریاست جمهوری
- دارای ۱۲ مدل مختلف جهت استفاده در شبکه های کوچک، متوسط و بزرگ
- بدون محدودیت در اعمال لایسنس محصول (Life Time)
- یک سال پشتیبانی رایگان به همراه نصب، راه اندازی و آموزش راهبری
- دارای قابلیت به روزرسانی Online و Offline
- قابل ارائه بر روی Platform های سخت افزاری و ماشین مجازی
- امکان ارائه ماژول های WAF, Accounting, Firewall بصورت مجزا
- قابلیت فرمان گرفتن از APK SIEM و پاسخ به Incident Handling

SOC

Security Operation Center

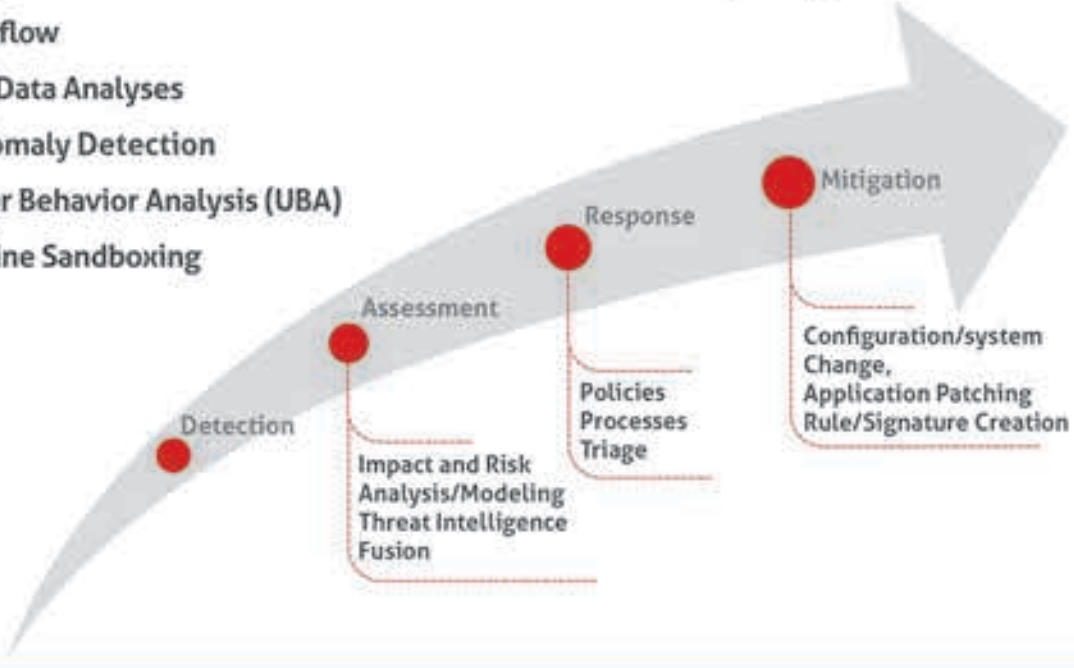
مرکز عملیات امنیت

مرکز عملیات امنیت، محیطی جهت پایش و کنترل امنیت ورود و خروج اطلاعات ، نگرش و تشخیص تهدیدات امنیتی است.

تحلیل و آنالیز رخدادهای موجود و اتخاذ تدابیر امنیتی از خروجی های مهم این مرکز است.

Security Operations
Analytics
Reporting

- IDS
- Netflow
- Big Data Analyses
- Anomaly Detection
- User Behavior Analysis (UBA)
- Online Sandboxing

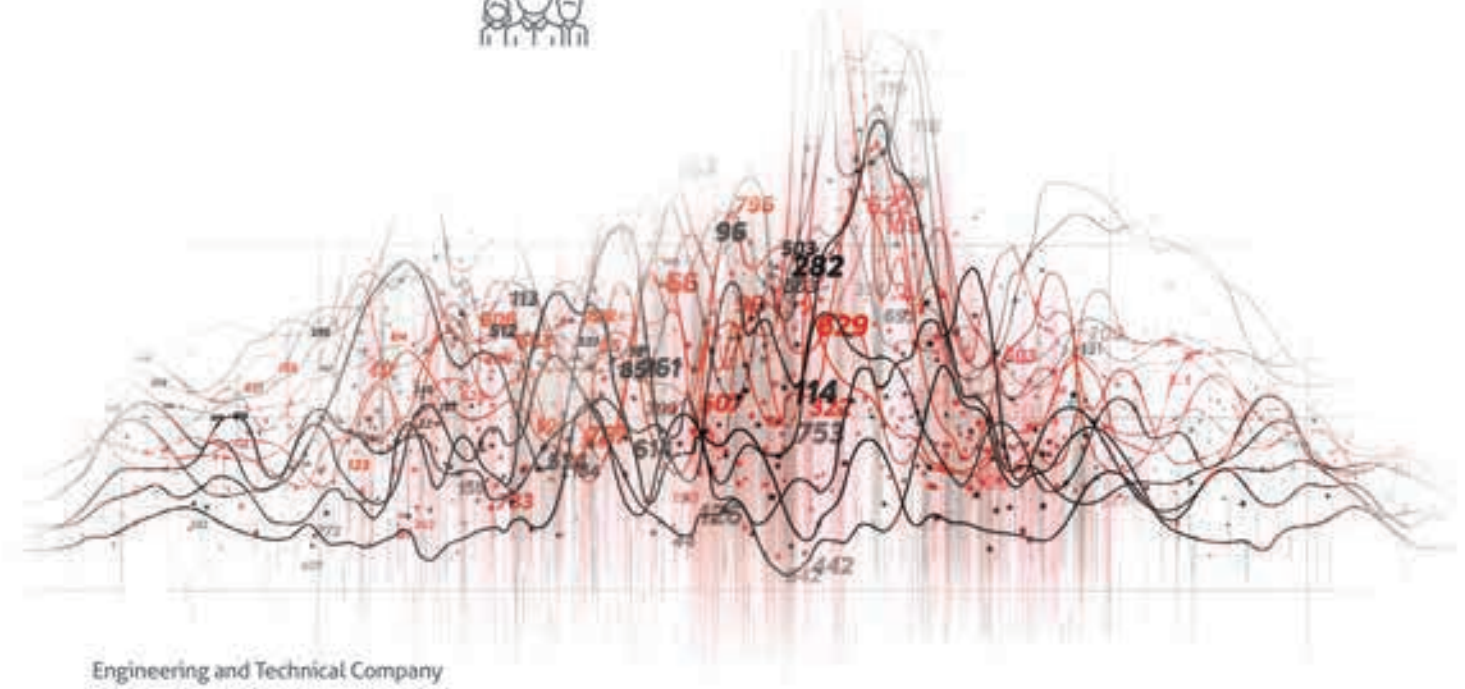


APKBDA

Big Data Analysis

تجزیه و تحلیل داده های بزرگ

Big Data Analysis با هدف تحلیل و نمایش معنی‌دار داده‌ها ایجادشده، داده‌های BDA باترکیب با داده های SIEM خروجی هایی مانند مشاهده Visualizations ترسیم نمودارهای مختلف و تجمیع آنها در داشبورد های پویا را جهت آنالیز تخصصی و تشخیص بلادرنگ بر اساس رفتارهای نرمال قبلی فراهم می نماید.



Engineering and Technical Company

Amn Pardazan Kavir

ISMS

Information Security Managment System
سیستم مدیریت امنیت اطلاعات

ISO 27001 یکی از استانداردهای اصلی جهت استقرار سیستم مدیریت امنیت اطلاعات (ISMS) است. این سیستم با بکارگیری فرآیند مدیریت ریسک، از محرمانگی، صحت و دسترس پذیری اطلاعات محافظت کرده و به طرف های ذینفع این اطمینان را می دهد که ریسک ها به میزان کافی مدیریت می شوند.

تعریف چارچوب سازمان

- شناخت سازمان، نیازها و انتظارات ذینفعان آن
- تعیین قلمرو و پیاده سازی سیستم مدیریت امنیت اطلاعات
- تحلیل کاستی ها (Gap) به منظور شناخت اولیه سازمان

رهبری و تعهد

- تدوین خط مشی امنیت اطلاعات
- تعریف نقش های سازمانی و امنیتی، مسئولیت ها و اختیارات

طرح ریزی

- شناسایی و ارزش گذاری دارایی های اطلاعاتی
- شناسایی، تحلیل، ارزیابی و اولویت بندی سناریوهای ریسک امنیت اطلاعات
- تعریف استراتژی های مقابله با ریسک
- تعریف اقدامات برطرف سازی ریسک (به تفکیک طرح فنی، روش اجرایی، سیاست امنیتی و آگاهی رسانی)
- تعریف اهداف امنیت اطلاعات و اقدامات دستیابی به آنها

پشتیبانی

- تعیین منابع (مالی و انسانی) مورد نیاز جهت پیاده سازی و نگهداری سیستم
- تعیین و رصد الزامات آگاهی رسانی مورد نیاز سیستم
- تعریف ارتباط های درونی و بیرونی مورد نیاز سیستم
- مدیریت متمرکز مستندات و سوابق سیستم

عملیات

- پیاده سازی اقدامات امنیتی
- مدیریت روش های اجرایی
- ارزیابی مجدد سناریوهای ریسک امنیت اطلاعات هنگام و پس از اجرای اقدامات امنیتی

ارزشیابی عملکرد

- پایش و تحلیل شاخص های ارزیابی اثربخشی سیستم
- طرح ریزی، برنامه ریزی و اجرای ممیزی های داخلی و بیرونی
- برگزاری جلسات بازنگری مدیریت و ارزیابی نتایج آنها

بهبود

- تعریف، پایش و ارزیابی نتایج اقدامات اصلاحی و پیشگیرانه

APK InfoSIS

information security implementation system

سامانه مدیریت امنیت اطلاعات

نرم افزار پیاده سازی ISMS

مطابق با سیستم های مطرح جهانی

Engineering and Technical Company

Amn Pardazan Kavir

APKSIEM

Security Information and Event Management

سامانه مدیریت وقایع و امنیت اطلاعات

سیستم تحلیل کننده رفتار شبکه/NBA

Network Behaviour Analyzer

این ابزار رویدادهایی که توسط کاربران، سرورها، تجهیزات و سنسورهای امنیتی در شبکه تولید می‌شود را جمع‌آوری و آن‌ها را به سیستم مدیریت رویدادها ارسال می‌کند.

موتور همبستگی رویداد/LCE

Log Correlation Engine

این بخش به عنوان مغز متفکر APKSIEM با بررسی ارتباطات و وقایع مختلف و با استفاده از اطلاعاتی نظیر آسیب‌پذیری و یا عدم آسیب‌پذیری سیستم به یک تهدید، اقدام به تشخیص، ارزش‌گذاری و رتبه‌بندی

سیستم مدیریت رویدادها/LM

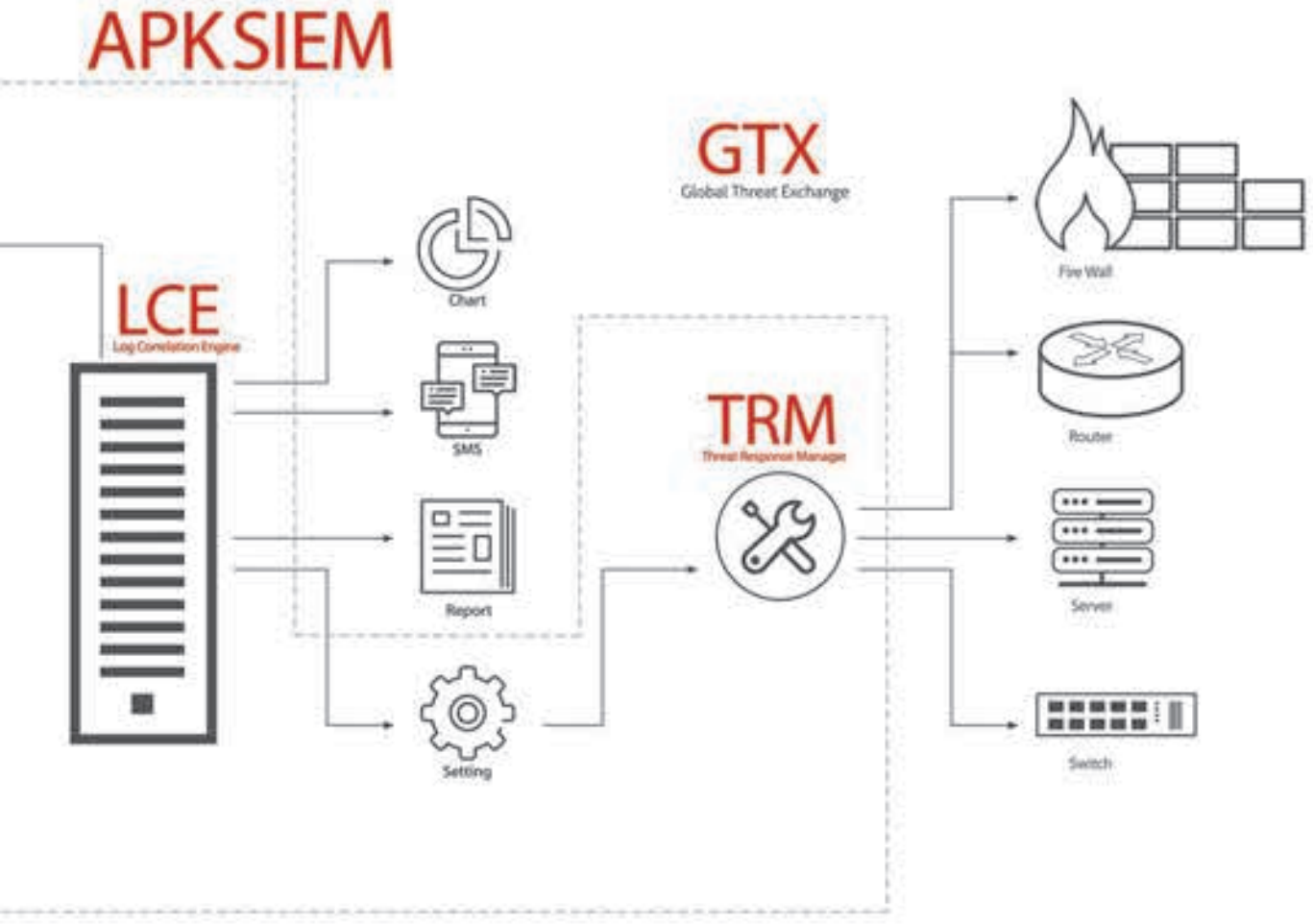
Log Manager

این ابزار وظیفه ذخیره‌سازی رویدادهای جمع‌آوری شده جهت تحلیل و یا تهیه گزارش‌ها را در بازه‌های زمانی متفاوت بنا به سیاست‌های امنیت یک سازمان به‌عهده دارد.

عامل هوشمند/SA

Smart Agent

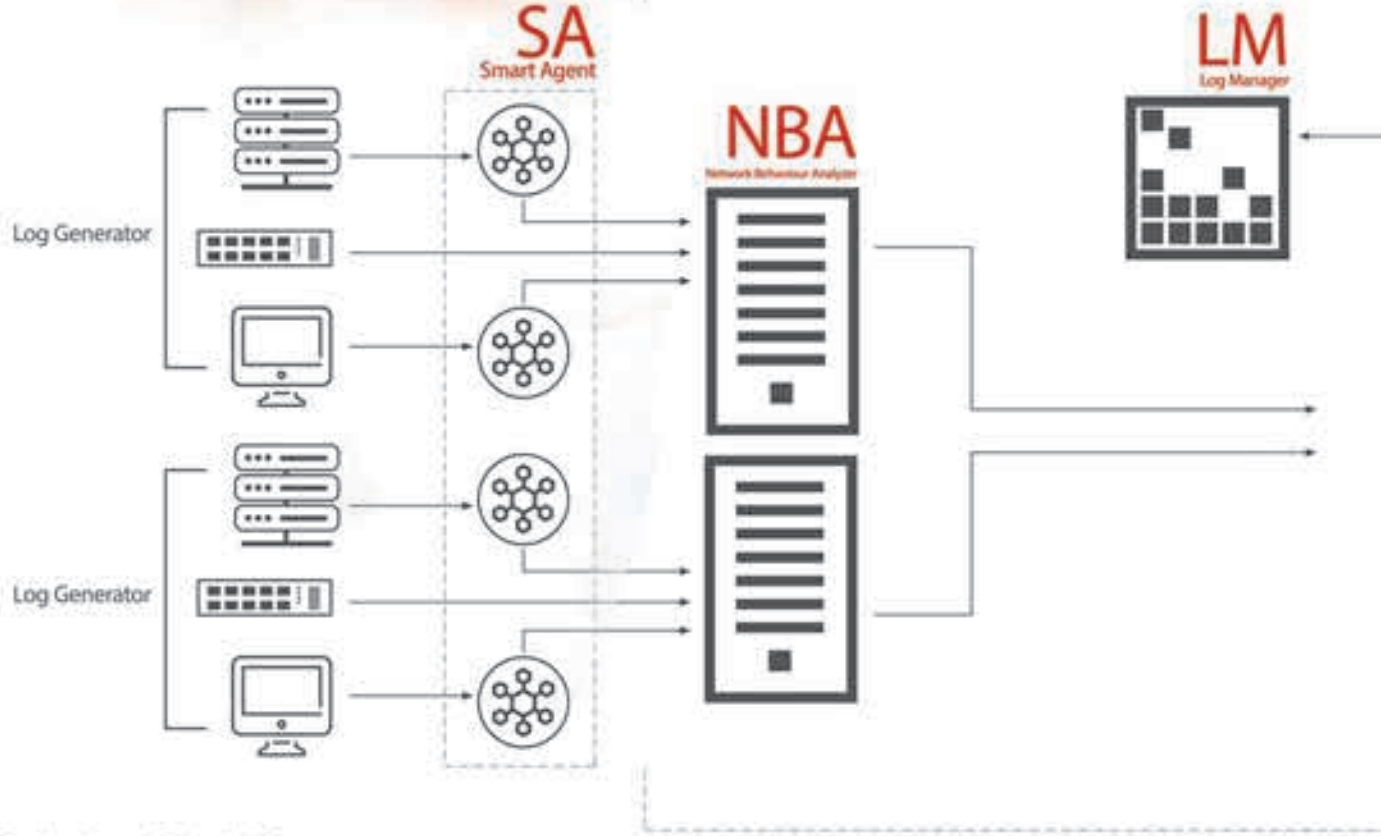
این ابزار بر روی سرورهای مایکروسافتی نصب می گردد.



سیستم بازخورد امنیتی /TRM

Threat Response Manager

یکی از مهمترین قسمت‌های پروژه‌های امنیتی، اعمال تنظیمات امنیتی بر روی تجهیزات شبکه به‌منظور جلوگیری از نفوذ بسته‌های مخرب شناسایی شده پس از تحلیل در سیستم APKSIEM می‌باشد.



Engineering and Technical Company

Amn Pardazan Kavir

PenTest

Penetration Test تست‌نفوذپذیری

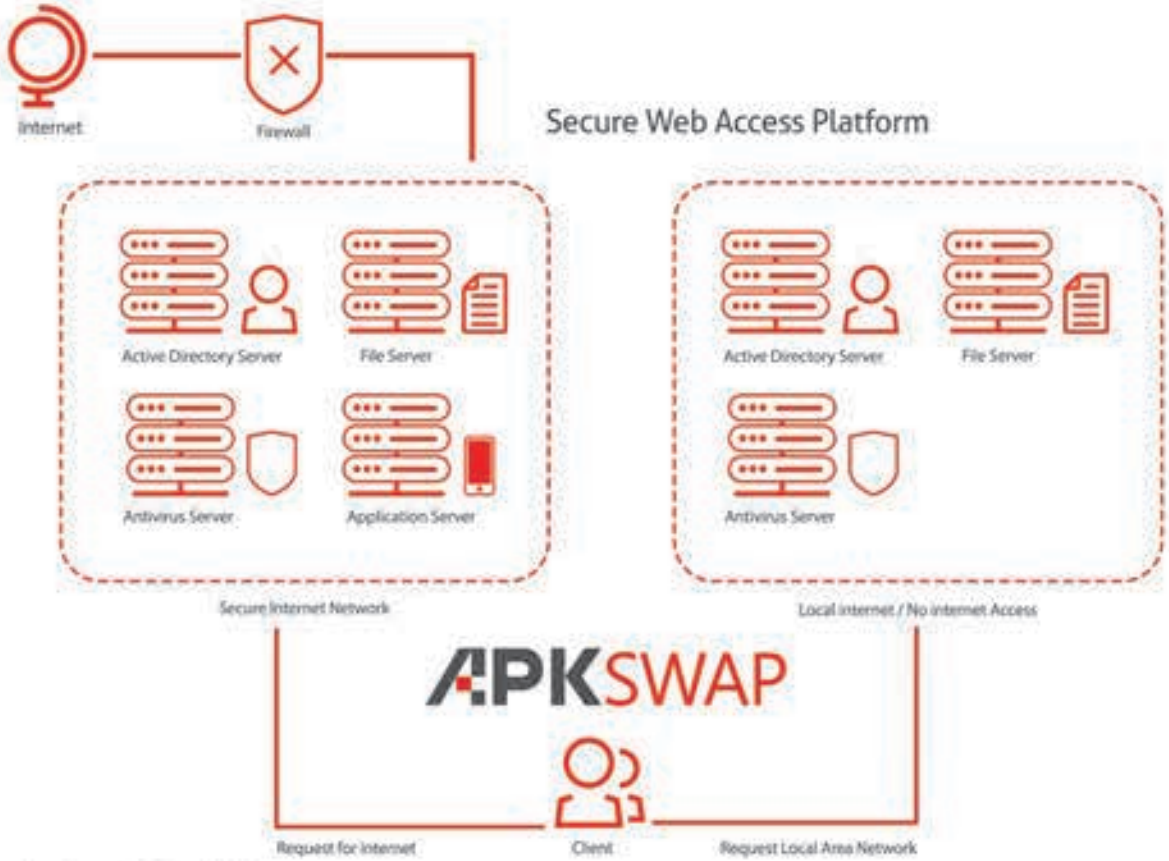
- جمع آوری اطلاعات
- مدل سازی تهدید
- تحلیل آسیب پذیری
- بهره برداری از آسیب پذیری
- حفظ و ارتقاء سطح دسترسی
- گزارش دهی

APKSWAP

Secure Web Access Platform

سامانه دسترسی امن به اینترنت

یکی از دغدغه های مهم مدیران و کارشناسان فناوری در سازمان ها جدا سازی اینترنت از اینترانت است. راهکار APKSWAP با کمترین میزان تغییرات در شبکه، بدون نیاز به خرید تجهیزات، با کاهش عملیات مدیریت کلاینت ها و بدون هیچ گونه اختلال در استفاده از اینترنت جداسازی آن را از اینترانت به صورت کاملا امن مهیا می سازد.



Engineering and Technical Company

Amn Pardazan Kavir

APKCERT

Computer emergency response team

مرکز مدیریت امداد و
هماهنگی عملیات رخدادهای رایانه‌ای

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای ، تیمی است که به یک سازمان مشخص، خدمات و پشتیبانی لازم برای پیشگیری و پاسخ به رویدادهای امنیتی کامپیوتری ارائه می دهد. بنابراین فرآیند بررسی یک رویداد امنیتی که به اصطلاح Incident Handling نامیده می‌شود، وظیفه اصلی یک مرکز CERT می باشد.

- Deep Investigations
- Mitigation/Recommends Changes
- Advanced Investigations
- Prevention
- Threat Hunting
- Forensics
- Malware Reverser

APKGroup

Costumers برخی از مشتریان

شرکت فنی و مهندسی

APK | امن پردازان کویر

تهران . بلوار کشاورز . خیابان شهید نادری
پایین تر از خیابان ایتالیا پلاک ۲ ،واحد ۵۰۵
کدپستی ۱۴۱۶۶۱۳۶۶۹

(۰۲۱) ۴۲۲ ۷۳

یزد . خیابان شهید دکتر چمران
روبروی کارخانه درخشان
کدپستی ۸۹۱۳۷۸۶۹۷۹

(۰۳۵) ۳۶۲ ۹۰ ۹۹۰

apk-group.ir

ISMS SOC UTM PenTest Secure Internet