McAfee
Together is power.

راهنمای مقاوم‌سازی سامانه امنیت نقاط پایانی مک‌آفی

بر اساس توصیه‌نامه مرکز ماهر

شبکه گستر
امنیت شما | وظیفه ما

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای کامپیوترای کشور (ماهر) توصیه‌نامه‌ای برای امن‌سازی سامانه‌های فناوری اطلاعات در مقابل تهدیدات سایبری احتمالی همزمان با ۱۳ آبان ماه منتشر کرده که در آن طی ۱۰ بند مواردی جهت مقاوم‌سازی سامانه‌ها ارائه شده است.

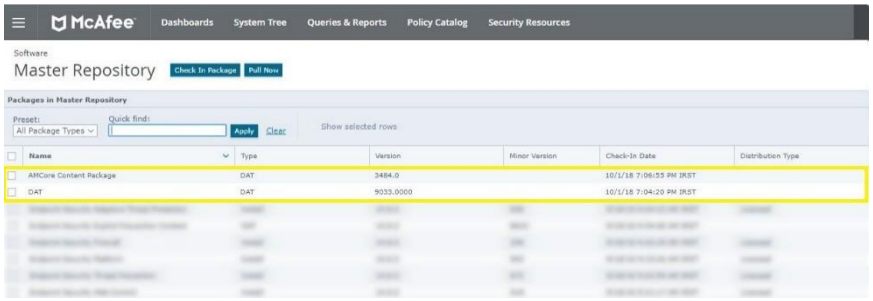
شرکت مهندسی شبکه گستر هم‌راستا با توصیه‌نامه فوق اقدام به انتشار راهنمای مقاوم‌سازی محصولات خود مطابق با بندهای مورد اشاره مرکز ماهر کرده است.

در این راهنما نحوه بررسی تنظیمات سامانه ضدویروس مک‌آفی در جهت اجرای توصیه‌های مرکز ماهر ارائه گردیده است.

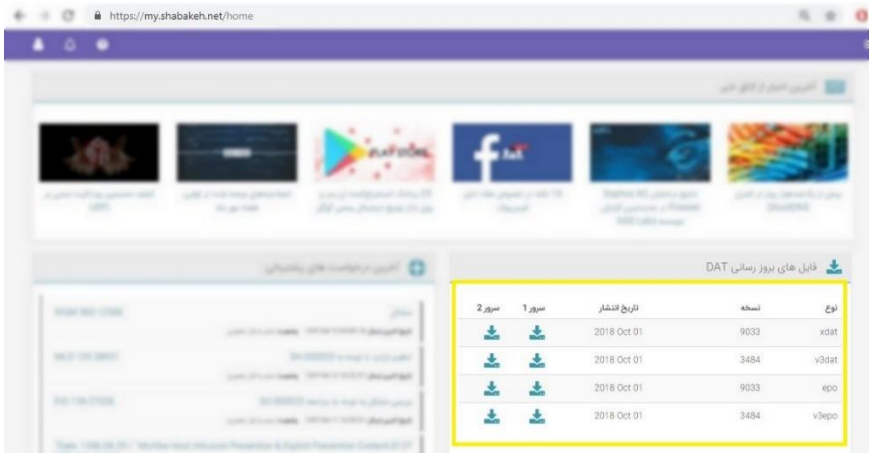
به‌روزرسانی سیستم عامل و نرم‌افزارها

کامپیوترهای مجهز به نرم‌افزارهای McAfee VirusScan Enterprise و McAfee Endpoint Security، از طریق ابزار مدیریتی McAfee ePolicy Orchestrator – به اختصار McAfee ePO – به‌روز می‌شوند. با توجه به انتشار روزانه فایل‌های به‌روزرسانی توسط شرکت مک‌آفی، برای اطمینان از صحت عملیات به‌روزرسانی در سطح شبکه، انجام مراحل زیر در زمانبندی روزانه توصیه می‌گردد:

- در مسیر Menu | Software | Master Repository در کنسول مدیریتی McAfee ePO، شماره نسخه و تاریخ دریافت AMCore Content Package و DAT مورد بررسی قرار گیرد؛ جهت حصول اطمینان، شماره نسخه با شماره نسخه منتشر شده در سامانه خدمات پس از فروش و پشتیبانی شرکت مهندسی شبکه گستر (MY) به نشانی https://my.shabakeh.net مقایسه شود. همچنین در روزهای کاری، انتشار فایل‌های به‌روزرسانی ضدویروس از طریق ایمیل به مشترکین اطلاع‌رسانی می‌شود.



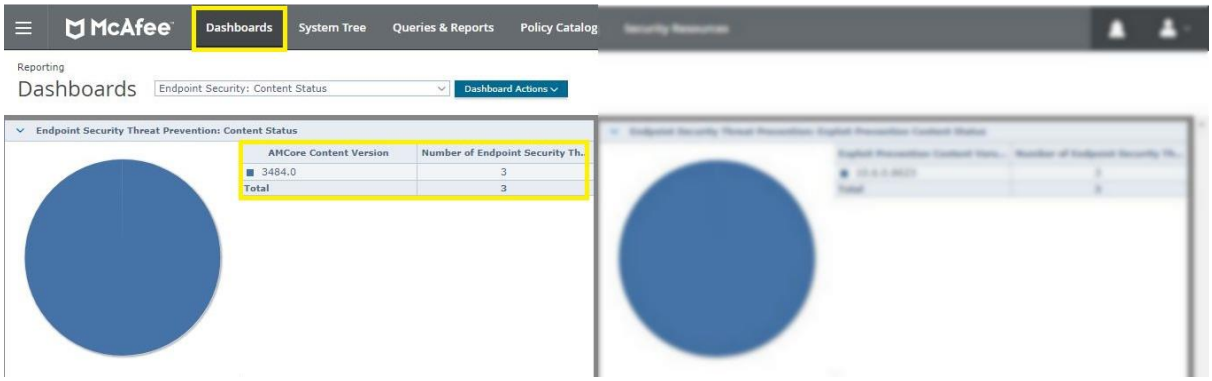
شکل ۱: انباره McAfee ePO



شکل ۲: سامانه خدمات پس از فروش و پشتیبانی شرکت مهندسی شبکه گستر (MY)

در صورت مشاهده اختلال در روند دریافت فایل‌های به‌روزرسانی توسط ابزار مدیریتی McAfee ePO، از طریق شماره تلفن ۴۲۰۵۲ و یا سامانه MY موضوع را جهت بررسی به گروه پشتیبانی شرکت مهندسی گستر منعکس کنید. همچنین امکان دریافت فایل‌های به‌روزرسانی از سامانه MY و قرار دادن آنها در انباره ابزار مدیریتی McAfee ePO فراهم می‌باشد. جهت دریافت اطلاعات بیشتر در این خصوص به راهنمای نصب و راهبری ابزار مدیریتی McAfee ePolicy Orchestrator در بخش پایگاه دانش محصولات در سامانه MY مراجعه شود.

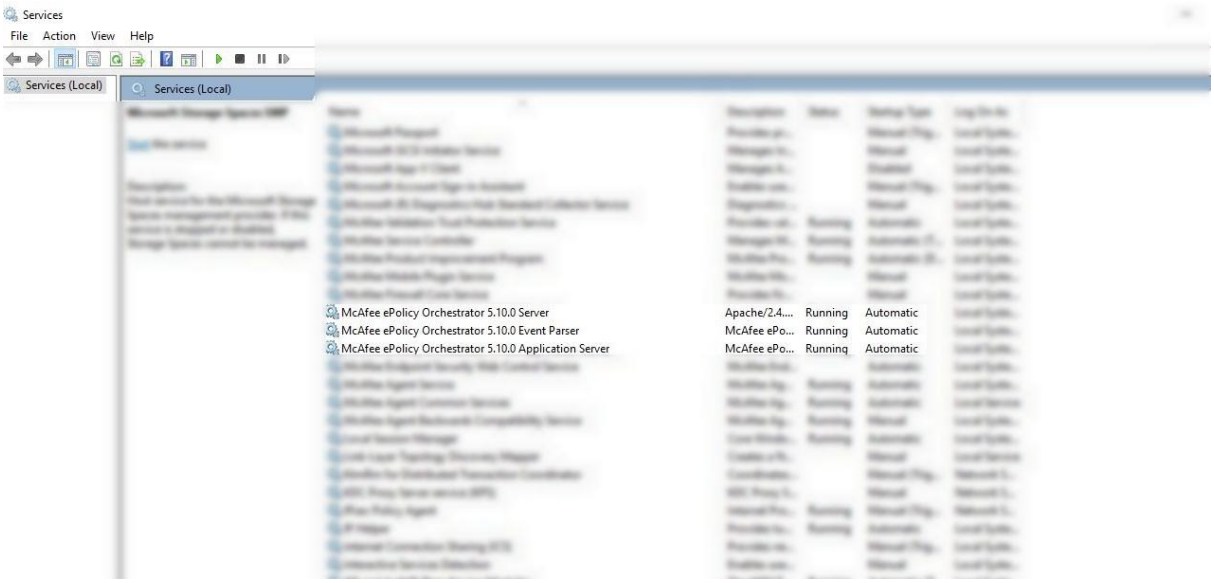
- کنترل وضعیت به‌روزرسانی دستگاه‌های تحت پوشش سامانه ضدویروس مک‌آفی بطور روزانه الزامی می‌باشد. جهت بررسی این موضوع، در کنسول مدیریتی McAfee ePO به داشبورد Endpoint Security: Content Status مراجعه شده و گزارش Endpoint Security Threat Prevention: Content Status مورد بررسی قرار گیرد.



شکل ۳: داشبورد Endpoint Security: Content Status

در صورت عدم دریافت به‌روزرسانی توسط هر یک کامپیوترهای تحت پوشش این سامانه، پس از اطمینان از نکات زیر، موضوع از طریق شماره تلفن ۴۲۰۵۲ یا سامانه MY به گروه پشتیبانی شرکت مهندسی شبکه گستر اعلام شود:

- فراهم بودن ارتباط شبکه‌ای مناسب بین سرور McAfee ePO و کامپیوتر مورد نظر (مراجعه به پیش‌نیازهای ارتباطی سامانه مذکور)
- فراهم بودن حداقل فضای خالی بر روی دیسک سخت کامپیوتر مورد نظر (مراجعه به پیش‌نیازهای McAfee VirusScan Enterprise / McAfee Endpoint Security)
- فعال بودن سرویس‌های McAfee ePO بر روی سرور مدیریتی؛ این سرویس‌ها در بخش Services سیستم عامل سرور قابل بررسی می‌باشند.



شکل ۴: سرویس‌های ابزار مدیریتی McAfee ePO

- در صورت نصب و راه‌اندازی این سامانه به‌صورت توزیع‌شده در سطح شعب سازمان، کنترل وضعیت به‌روزرسانی کامپیوترهای شعب و نیز انباره‌های توزیعی الزامی می‌باشد. برای مشاهده وضعیت انباره‌های توزیعی می‌توان در کنسول مدیریتی McAfee ePO به Menu | Software | Distributed Repositories مراجعه کرد و یا در صورت لزوم گزارش Agent Handler Status را در بخش Menu | Reporting | Queries & Reports مورد بازبینی قرار داد.

تهیه و نگهداری نسخه پشتیبان

جهت اطمینان از پایداری خدمات‌دهی سامانه امنیت نقاط پایانی مک‌آفی و کاهش زمان توقف خدمات‌دهی آن در زمان وقوع مشکلات، تهیه نسخ پشتیبان بر اساس استانداردهای تهیه، نگهداری و بازیابی نسخ پشتیبان الزامی می‌باشد. جهت دریافت اطلاعات بیشتر در خصوص چگونگی تهیه نسخ پشتیبان از ابزار مدیریتی McAfee ePO به مستندات زیر در پایگاه دانش محصولات در سامانه MY مراجعه شود:

- ساخت تصویر لحظه‌ای از ماشین McAfee ePO
- راهنمای بازیابی از حادثه ابزار مدیریتی

بهره‌گیری از رمزنگاری مناسب در تبادل اطلاعات

ارتباط امن بین سفیر (McAfee Agent) و ابزار مدیریتی McAfee ePO همواره برقرار بوده و برای همسان‌سازی و گسترش این سطح امنیت به ارتباط McAfee ePO با پایگاه داده، لازم است تنظیمات مندرج در راهنمای زیر اعمال شود.

https://kc.mcafee.com/corporate/index?page=content&id=KB84628

اتخاذ راه‌حل برای دسترسی ایمن از راه دور برای مدیریت سرویس‌ها و زیرساخت‌ها

به‌منظور تعیین سطح دسترسی شبکه‌ای به کامپیوتر و یا کنسول مدیریتی McAfee ePO لازم است از دیواره آتش (خارجی و یا نصب شده بر روی سیستم عامل کامپیوتر سرویس‌دهنده ابزار مدیریتی) و نیز قابلیت Restrict IP Addresses در مسیر Menu | Server Settings | Logon Protection ابزار مدیریتی مذکور استفاده نموده و دسترسی شبکه‌ای مناسب برای نشانی‌های IP تایید شده، فراهم گردد.

اتخاذ مکانیزم احراز هویت و رمز عبور قوی

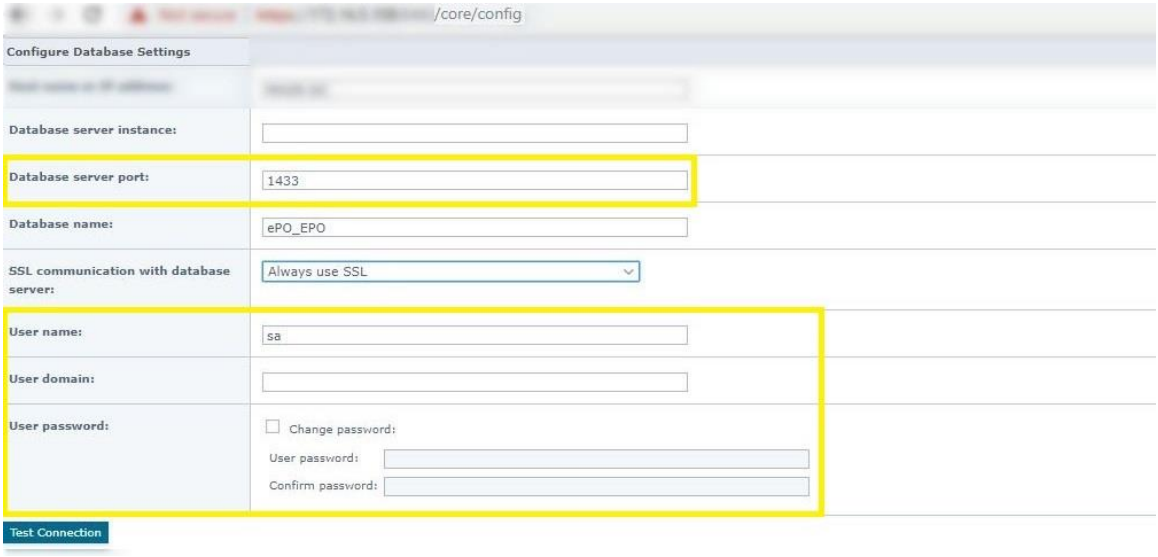
سامانه امنیت نقاط پایانی مک‌آفی، ابزاری کلیدی جهت حفظ امنیت پایدار شبکه بوده و دسترسی غیرمجاز به آن، محرمانگی، یکپارچگی و دسترسی اطلاعات را با خطر جدی مواجه می‌سازد. کاهش این ریسک با اعمال تنظیمات امنیتی مناسب ممکن بوده و رعایت نکات زیر برای تحقق این منظور توصیه می‌گردد:

- امنیت پایگاه داده سامانه امنیت نقاط پایانی مک‌آفی

این سامانه از نرم‌افزار Microsoft SQL Server به‌عنوان پایگاه داده بهره برده و کاهش ریسک دسترسی غیرمجاز به آن با تغییر نام کاربری پیش‌فرض، استفاده از کلمه عبور مناسب و همچنین اعمال سیاست‌های امنیتی بر اساس توصیه‌های کاربردی شرکت

مایکروسافت[1] ممکن می‌گردد. در صورت تغییر سیاست‌های امنیتی در نرم‌افزار Microsoft SQL Server، لازم است با مراجعه به نشانی زیر دامنه تغییرات در تنظیمات ابزار مدیریتی McAfee ePO نیز اعمال شود:

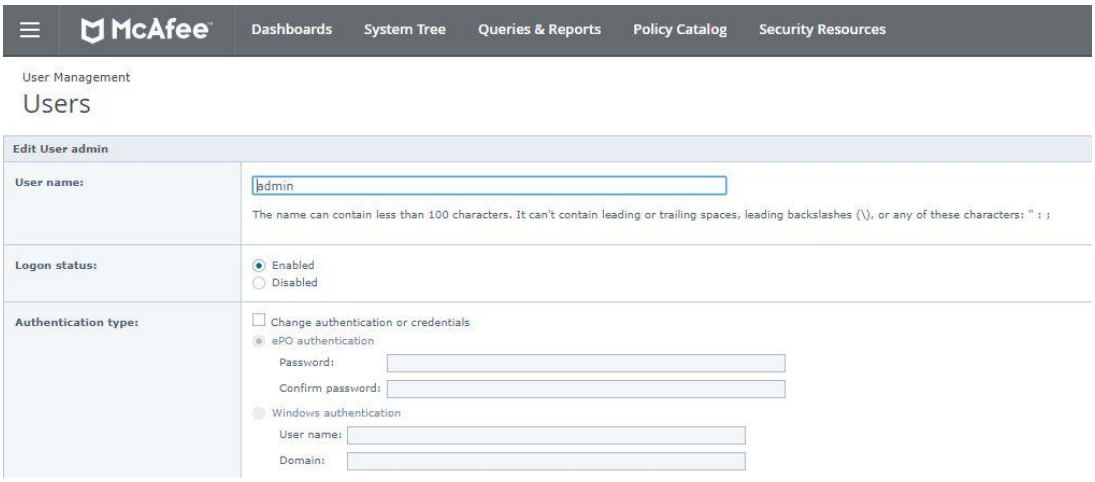
https://[*ePO Server Name or IP*]:8443/core/config



شکل ۵: صفحه تنظیمات ارتباط با پایگاه داده

- تغییر رمز عبور و سطح دسترسی ورود به کنسول مدیریتی McAfee ePO

برای این منظور لازم است در کنسول مدیریتی McAfee ePO به مسیر Menu | User Management | Users مراجعه شده و رمز عبور مناسب برای کاربر مورد نظر ثبت گردد.



شکل ۶: صفحه تنظیمات رمز عبور کاربر

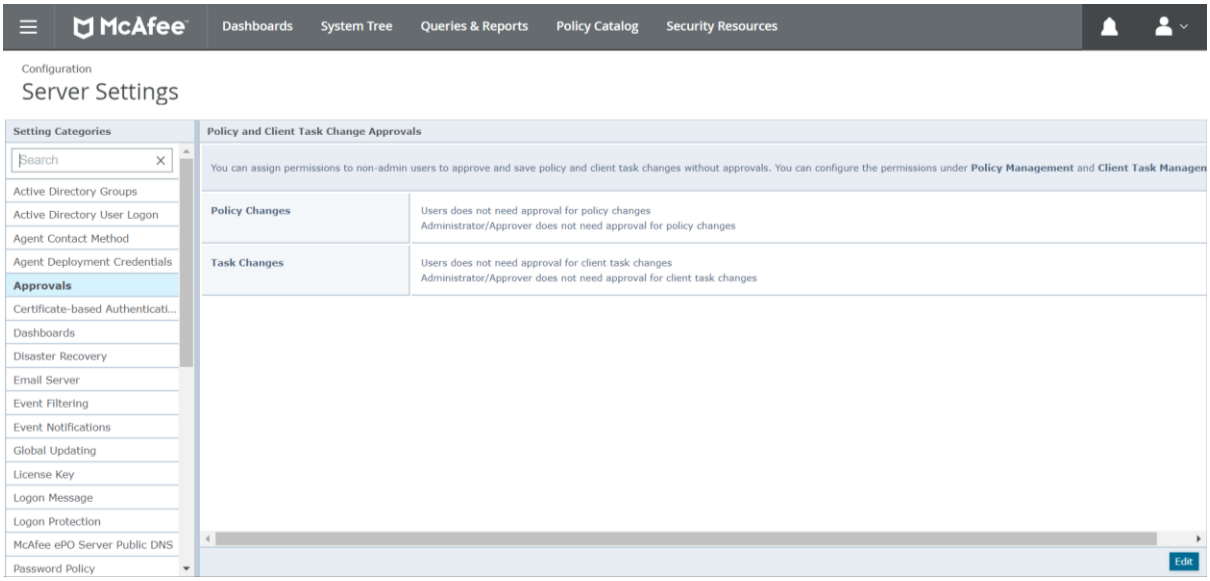
در صورت لزوم کاهش و یا افزایش سطوح دسترسی می‌توان در این صفحه، تنظیمات مربوط به سطح دسترسی کاربر مورد نظر را در بخش Manually assigned permission sets تغییر داد. لازم به ذکر است که امکان استفاده از قابلیت اصالت‌سنجی توسط Microsoft Active Directory Domain Services در ابزار مدیریتی McAfee ePO فراهم بوده و برای این منظور می‌توان گزینه مناسب را در بخش Authentication type در صفحه فوق انتخاب کرد.

[1] https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/sql/sql-server-security

همچنین توصیه می‌شود با مراجعه به Menu | Server Settings | Password Policy سیاست‌های سخت‌گیرانه‌ای نسبت به رمز عبور کاربران دارای دسترسی به کنسول مدیریتی McAfee ePO اعمال شود.

- تایید اعمال تنظیمات

در صورت لزوم دسترسی چند راهبر به کنسول مدیریتی McAfee ePO، استفاده از قابلیت Approvals در مسیر Menu | Server Settings به‌منظور تایید تنظیمات ایجاد شده و یا تغییر یافته توسط مدیریت امنیت، جهت پیشگیری از خطای انسانی و صحت تنظیمات مورد نظر الزامی می‌باشد.



شکل ۷: صفحه تنظیمات Approvals

جمع‌آوری، نگهداری و بررسی رخدادنماها

نگهداری شواهد به‌منظور اطلاع از رخدادها و نیز تولید گزارش‌ها، از جمله قابلیت‌های کلیدی سامانه امنیت نقاط پایانی مک‌آفی است. شواهد تا زمان حذف خودکار آنها در پایگاه داده این سامانه نگهداری می‌شود. جهت تعیین زمان حذف خودکار آنها لازم است زمانبندی مورد نظر در تنظیمات به‌صورت زیر اعمال شود:

۱- ورود به ابزار مدیریتی McAfee ePO
۲- ویرایش فرمان Purge Threat and Client Events در مسیر Menu | Server Tasks
۳- فعالسازی آن با انتخاب گزینه Enabled از قسمت Schedule status
۴- انتخاب زمانبندی مناسب برای گزینه Purge records older than از قسمت Actions
۵- انتخاب زمانبندی اجرای دوره ای این قاعده از قسمت Schedule
۶- ذخیره‌سازی تنظیمات

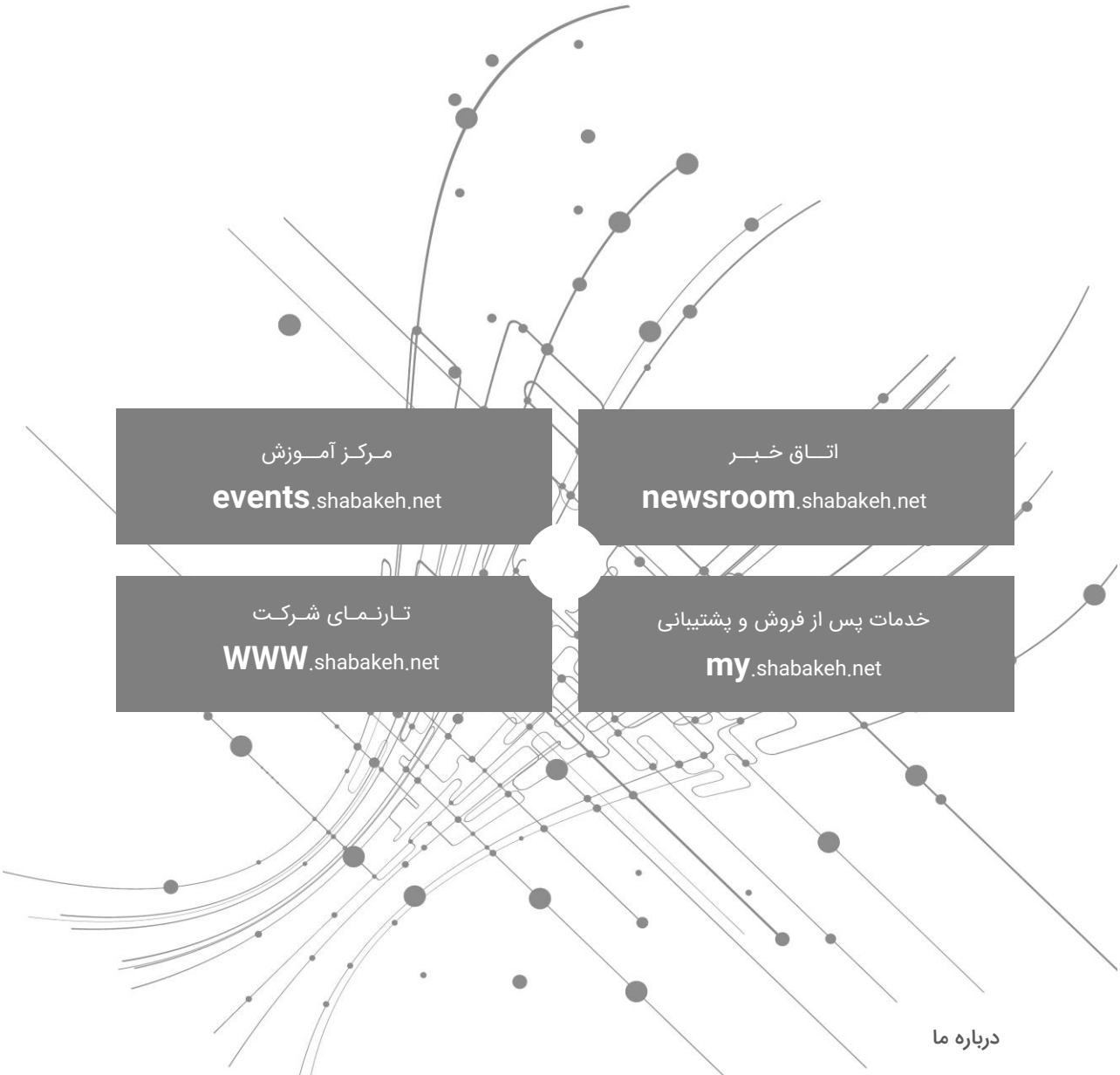
همچنین در بخش Queries & Reports این سامانه، امکان مرور رویدادها از طریق اجرای گزارش‌های پیش‌فرض و یا تولید گزارش‌های جدید فراهم می‌باشد. جهت دریافت اطلاعات تکمیلی در خصوص نحوه مرور گزارش‌ها، در بخش پایگاه دانش محصولات در سامانه MY به راهنمای نصب و راهبری ابزار مدیریتی McAfee ePolicy Orchestrator مراجعه شود. برای اطلاع از وضعیت نصب نرم‌افزارهای امنیتی بر روی کامپیوترها و نیز واکنش آنها در برابر تهدیدات امنیتی، بررسی روزانه داشبوردها و گزارش‌های زیر در ابزار مدیریتی McAfee ePO توصیه می‌گردد:

- داشبورد Endpoint Security: Compliance Status

- داشبورد Endpoint Security: Detection Status
- داشبورد Endpoint Security: Environmental Health
- داشبورد Endpoint Security: Threat Behavior
- داشبورد Endpoint Security: Web Control Activity
- داشبورد Threat Events
- گزارش Agent Communication Summary از منوی Queries & Reports
- گزارش Inactive Agents از منوی از منوی Queries & Reports
- گزارش Agent Uninstalls Attempted از منوی از منوی Queries & Reports

جلوگیری از نشت اطلاعات سازمانی

حفظ محرمانگی اطلاعات حساس به‌منظور ایجاد امنیت پایدار کسب و کار سازمان از جمله اهداف قابل تحقق با استفاده از راهکارهای ارائه شده توسط شرکت مک‌آفی است. نصب و راه‌اندازی نرم‌افزارهای McAfee Data Loss Prevention، McAfee File and Removable Media Protection و McAfee Drive Encryption سازمان را قادر می‌سازد تا وضعیت محرمانگی و نیز خروج اطلاعات سازمانی از طریق روش‌های گوناگون را تحت کنترل داشته و در صورت لزوم سیاست‌ها امنیتی پیشگیرانه را اعمال کند. اطلاعات کامل در خصوص نحوه نصب، راه‌اندازی و نگهداری نرم‌افزارهای مذکور در بخش پایگاه دانش محصولات در سامانه MY قابل دسترس می‌باشد.



درباره ما

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تاسیس شد. این شرکت یکی از باسابقه‌ترین شرکتهای فعال در حوزه امنیت فناوری اطلاعات است. با بیش از ۲۵ سال تجربه موفق در عرضه محصولات و خدمات امنیت شبکه، شرکت شبکه گستر افتخار خدمات‌دهی به هزاران شرکت و سازمان در بخش‌های مختلف کشور را دارد و مجری بزرگترین پروژه‌های نصب و نگهداری نرم‌افزارهای ضدبدافزار و سخت‌افزارهای دیـواره آتش در کشور بوده است.

شبکه گستر
شـرکـت مـهـنـدسـی شـبـکـه گـسـتـر

تهران خیابان شهید دستگردی (ظـفـر) شماره ۲۷۳
تلفن / دورنگار ۴۲۰۵۲ – ۰۲۱
info@shabakeh.net www.shabakeh.net