بسم الله الرحمن الرحیم

پیشنهاد فنی
احراز اصالت چندعاملی نوین سامان
در زیرساخت شبکه و امنیت

نسخه ۱.۳

اردیبهشت ماه ۱۴۰۲

فهرست مطالب

۱ مقدمه

بر اساس نتایج مطالعات و بررسی‌هایی که در حوزه امنیت اطلاعات و ارتباطات صورت گرفته است، اشتباهات و ناآگاهی کاربران در حفظ و استفاده از کلمه‌های عبور و همچنین خطاهای پیاده‌سازی و مدیریتی در روند احراز هویت بر اساس کلمه عبور، یکی از مهمترین نقاط فروپاشی امنیت بوده است. بر این اساس، یکی از نیازمندی‌های امنیتی حیاتی، لزوم استقرار سازوکارهای قوی برای احراز اصالت کاربران است.

سیستم احراز اصالت چند عاملی[۱] سامان (با نام تجاری Saman-MFA) متشکل از مجموعه کاملی از روش‌ها و فرآیندهای استاندارد، قابل اعتماد، امن و کاربرپسند برای احراز اصالت است که با هدف تحقق مفهوم احراز اصالت قوی[۲] ورود کاربران به سامانه‌ها، تجهیزات و برنامه‌های کاربردی توسعه یافته است. فرآیندهای احراز اصالت سیستم Saman-MFA، بدون نیاز به تغییر در روال‌های جاری احراز اصالت سیستم‌ها (که به‌طور عمده احراز اصالت مبتنی بر کلمه عبور هستند) بر روی آن‌ها قرار گرفته و یک لایه امنیتی قابل اطمینان برای احراز اصالت، تشکیل می‌دهند.

از آن‌جایی که محصول Saman-MFA فرآیند احراز اصالت سامانه‌های سازمان را بر عهده دارد، پایداری[۳] و در دسترس بودن[۴] آن بسیار حائز اهمیت است. از این رو، شرکت پیام‌پرداز با طراحی معماری HA و Load Balancing خود مبتنی بر بالاترین استانداردهای روز دنیا، می‌تواند بالاترین سطح پایداری به ارمغان آورد. این مستند به تبیین این راهکار می‌پردازد.

۲ سامانه احراز اصالت چندعاملی سامان (Saman-MFA)

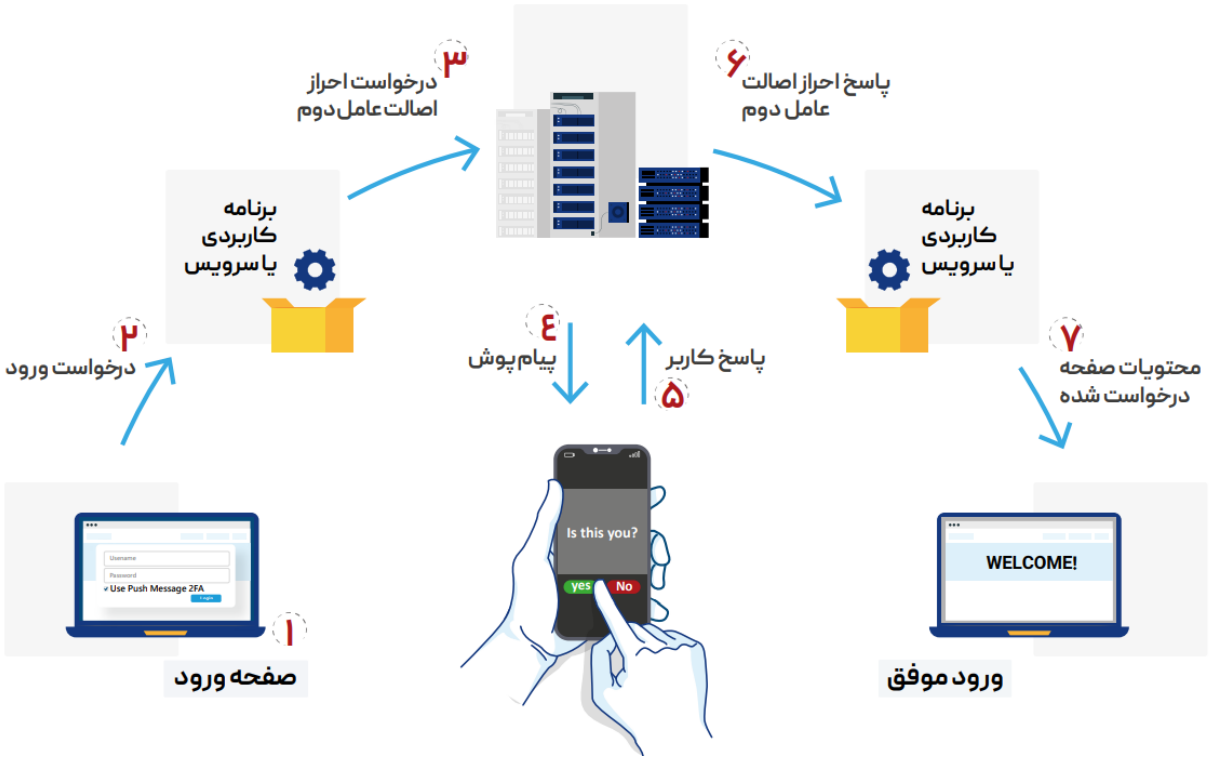
از نظر تجربه کاربری، تمرکز سیستم احراز اصالت Saman-MFA بر روی تلفن‌های همراه هوشمند است. چرا که از یک سو این دستگاه‌ها همواره در دسترس کاربران هستند و از سوی دیگر از انعطاف‌پذیری و قدرت پردازشی قابل قبولی برای تحقق روال‌ها، پروتکل‌ها و الگوریتم‌های امن برخوردار می‌باشند. سیستم احراز اصالت Saman-MFA، فرآیندهای احراز اصالت استاندارد مبتنی بر پیام‌های Push، کدهای TOTP و HOTP، و همچنین روال احراز اصالت بدون کلمه عبور مبتنی بر QR-Code را در قالب اپلیکیشن موبایل اختصاصی بر روی انواع تلفن‌های همراه ارائه می‌دهد.

در شکل زیر روند احراز اصالت مبتنی بر پیام پوش با استفاده از سیستم احراز اصالت سامان در یک سناریوی نمونه نشان داده شده است. همان‌طور که در شکل مشاهده می‌شود، سیستم سامان بدون کاستن از

---

۱ *Multi-Factor Authentication*
۲ *Strong Authentication*
۳ *Stability*
۴ *Availability*

ویژگی‌های امنیتی احراز اصالت بر اساس کلمه عبور، یک لایه احراز اصالت که مستلزم تعامل مستقیم اما کمینه کاربر با تلفن همراه است را اضافه می‌نماید.



به منظور بهره‌برداری حداکثری از سیستم احراز اصالت Saman-MFA، امکانات مدیریت احراز اصالت از جمله افزودن یا حذف کاربر (به‌صورت فردی یا گروهی)، سیاست‌گذاری احراز اصالت و اخذ انواع گزارش‌های احراز اصالت و درخواست‌های ورود تدارک دیده شده است. سامانه‌ها و برنامه‌های کاربردی استفاده کننده از سیستم احراز اصالت Saman-MFA می‌توانند از طریق APIهای تدارک دیده شده، امکانات مدیریت احراز اصالت مورد نظر را به داشبورد مدیریتی سامانه خود بیافزایند. به این ترتیب، مدیران سامانه‌ها و برنامه‌های کاربردی می‌توانند به‌طور یکپارچه و از داشبورد واحد سیاست‌گذاری‌ها، تنظیمات و گزارش‌گیری‌های مربوط به احراز اصالت را به انجام رسانند.

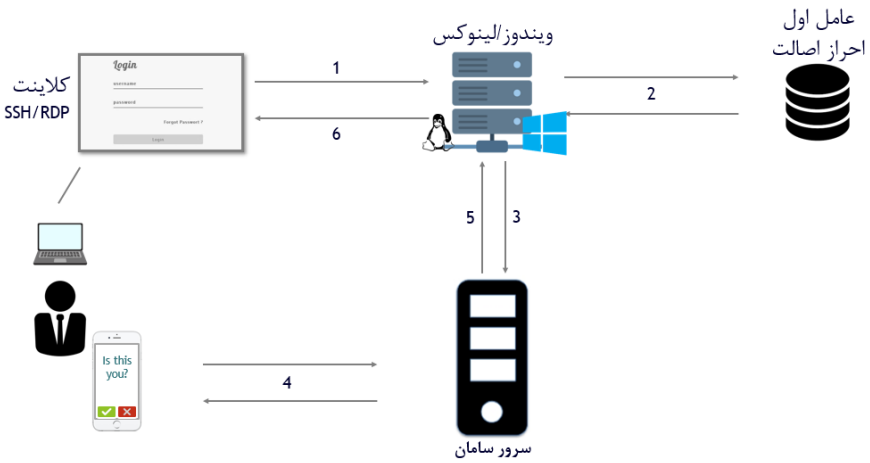
۳ انواع روش‌های احراز اصالت چندعاملی

سامان-MFA روش‌های متنوعی را برای احراز اصالت چندعاملی پشتیبانی می‌کند:

- **پیام‌های پوش؛** در این روش، یک پیام پوش به دستگاه موبایل کاربر ارسال می‌شود و متعاقب آن، یک درخواست ورود در اپلیکیشن موبایل سامان به کاربر نشان داده می‌شود. با تایید این درخواست، احراز اصالت کاربر کامل می‌شود.
- **یکبارررمزهای TOTP؛** کاربر یکبار رمز تصادفی را از اپلیکیشن سامان قرائت و در صفحه ورود در کنار وارد می‌کند. سرور سامان درستی کد وارد شده را بررسی می‌نماید.
- **پیامک؛** کاربر یکبار رمز تصادفی را که از طریق پیامک برای او ارسال شده است قرائت و در صفحه ورود در کنار وارد می‌کند. سرور سامان درستی کد وارد شده را بررسی می‌نماید.
- **ایمیل؛** کاربر یکبار رمز تصادفی را که از طریق ایمیل برای او ارسال شده است قرائت و در صفحه ورود در کنار وارد می‌کند. سرور سامان درستی کد وارد شده را بررسی می‌نماید.
- **روش بدون پسورد (مبتنی بر QRCode)؛** در این روش کافی است کاربر QR Code نمایش داده شده در صفحه ورود را با اپلیکیشن موبایل سامان اسکن نماید. با این کار، یک پیام پوش به دستگاه موبایل کاربر ارسال شده و متعاقب آن، یک درخواست ورود در اپلیکیشن موبایل سامان به کاربر نشان داده می‌شود. با تایید این پیام، اصالت کاربر بدون نیاز به تایپ نام کاربری یا کلمه عبور احراز می‌شود.
- **سخت‌افزارهای تولید یکبارررمز؛** این تجهیزات نیز همانند نرم‌افزارهای تولید یکبارررمزهای TOTP و HOTP امکان تولید اعداد یکبارررمز را خواهند داشت. محصول سامان امکان استفاده از این سخت‌افزارهای تولید یکبارررمز را نیز خواهد داشت.

٤ سناریوی استفاده از سامان-MFA

در ادامه به بررسی یک سناریوی استفاده از سامان-MFA برای اتصال به سیستم‌عامل‌ها می‌پردازیم.



در این سناریو کاربر طبق روال مرسوم به سیستم‌عامل خود دسترسی پیدا می‌کند و پس از ورود عامل اول، سیستم‌عامل ویندوز یا لینوکس نام‌کاربری و رمزعبور را از طرق مرسوم (محلی یا اکتیودایرکتوری) مورد بررسی قرار می‌دهد. پس از آن ایجنت نرم‌افزاری سامان طی تعامل با کاربر روش‌های متعدد احراز اصالت چندعاملی را برای انتخاب به کاربر عرضه می‌نماید. کاربر با انتخاب یکی از روش‌ها فرایند احراز اصالت چندعاملی را آغاز نموده و طی یکی از کانال‌های ارتباطی پوش، پیامک، TOTP و ... احراز اصالت چندعاملی را تکمیل می‌کند. نتیجه به اطلاع ایجنت نرم‌افزاری رسیده و بر اساس آن در مورد دسترسی کاربر تصمیم‌گیری می‌شود. لازم به ذکر است که تنها در فرآیند احراز اصالت چندعاملی در سیستم‌عامل‌ها نیازمند وجود ایجنت بر روی سیستم میزبان خواهد بود و در مابقی تجهیزات و سامانه‌ها نیازی به وجود هیچ‌گونه ایجنت نخواهد بود.

۵ یکپارچه‌سازی و انواع تجهیزات

انواع مختلفی از سامانه‌ها، تجهیزات و برنامه‌های کاربردی می‌توانند احراز اصالت چندعاملی کاربران خود را با استفاده از سامان انجام دهند. در این مستند به تمامی سامانه‌ها، تجهیزات و برنامه‌های کاربردی که از احراز اصالت چندعاملی سامان استفاده می‌کنند، کلاینت گفته می‌شود. مهم‌ترین این کلاینت‌ها عبارتند از:

- سیستم‌عامل ویندوز
- سیستم‌عامل‌های لینوکس و BSD
- زیرساخت‌های مجازی نظیر VmWare و ... .
- تجهیزات شبکه، زیرساختی و امنیتی که احراز اصالت کاربران را با استفاده از پروتکل RADIUS یا LDAP انجام می‌دهند.

کلاینت‌های مختلف برای استفاده از خدمات سامان می‌توانند از یکی راه‌های زیر به سرور سامان متصل شوند:

- **نصب نرم‌افزارهای مربوطه (Agentها):** برای سیستم‌عامل‌های ویندوز و لینوکس نرم‌افزار مخصوصی توسعه داده شده است که پس از نصب آن، احراز اصالت چندعاملی سامان به روند احراز اصالت فعلی سیستم‌عامل (مبتنی بر کلمه عبور و عمده روش‌های دیگر) اضافه می‌شود. بدین ترتیب، کاربر بعد از وارد نمودن کلمه عبور خود، ملزم به احراز اصالت توسط سامان می‌باشد. نرم‌افزار ویندوزی سامان بر روی نسخه‌های ۷، ۸، ۸.۱ و ۱۰ ویندوز قابل نصب و استفاده است. این نرم‌افزار از پروتکل RDP نیز پشتیبانی کرده و دسترسی‌های راه دور به سیستم‌عامل ویندوز را نیز چندعاملی می‌کند. همچنین در نرم‌افزار ویندوز، این امکان وجود دارد که تنها احراز اصالت‌هایی که از طریق پروتکل RDP صورت می‌گیرند توسط سامان چندعاملی شوند. نرم‌افزار لینوکس نیز از توزیع‌های مختلف مطرح لینوکس پشتیبانی کرده و تا کنون بر روی توزیع‌های Debian، Ubuntu، Redhat، Centos و Fedora تست شده است. همچنین

نرم‌افزار BSD نیز از توزیع‌های مطرح این خانواده پشتیبانی کرده و تا کنون بر روی توزیع FreeBSD تست شده است. نرم‌افزار لینوکس و BSD از پروتکل SSH نیز پشتیبانی کرده و دسترسی راه‌دور از طریق SSH را نیز چندعاملی می‌کنند.

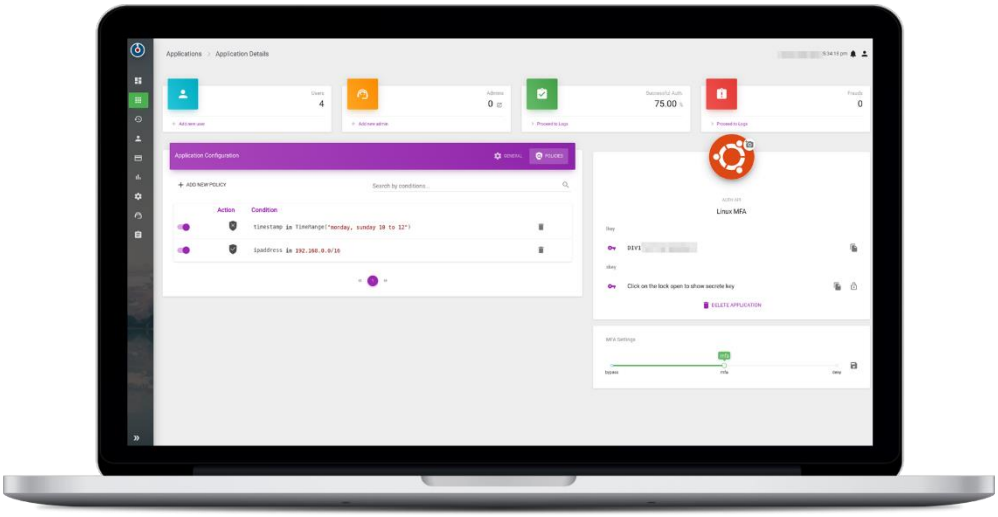
- **استفاده از APIهای REST سامان:** استفاده از این روش برای سامانه‌های نرم‌افزاری توصیه می‌شود که توسط خود سازمان توسعه داده شده‌اند. برای استفاده از این روش، توسعه‌دهندگان سامانه با تغییر صفحه لاگین سامانه و افزودن صفحه لاگین چندعاملی، درخواست احراز اصالت چندعاملی را از طریق APIهای RESTFul به سامان ارسال نموده و منتظر پاسخ سامان خواهند شد. مستندات APIهای سامان در آدرس https://smdev.ir/docs/API قابل مطالعه هستند. لازم به ذکر است، کتابخانه‌های مربوط به فراخوانی این APIها برای بسیاری از زبان‌ها و چارچوب‌ها آماده ارائه هستند.
- **استفاده از سامان-پروکسی:** این روش در تجهیزاتی قابل استفاده است که از پروتکل RADIUS یا LDAP برای احراز اصالت پشتیبانی می‌کنند. در واقع سامان-پروکسی خود یک RADIUS یا LDAP سرور است که بر روی ماشین مجازی سامان یا هر ماشین مجازی دیگر داخل سازمان، نصب می‌شود. پیش‌نیاز این روش آن است که اطلاعات کاربران در LDAP یا سرور RADIUS سازمان ذخیره شده باشند. برای استفاده از این روش کافی است سامان-پروکسی به عنوان RADIUS یا LDAP سرور به تجهیز مورد نظر معرفی گردد. سامان-پروکسی همان‌طور که از نام آن مشخص است، به صورت یک پروکسی عمل کرده و درخواست‌های احراز اصالت مبتنی بر پروتکل‌های LDAP یا RADIUS را دریافت کرده و همزمان با پردازش عامل‌های دوم احراز اصالت، درخواست تایید عامل اول احراز اصالت (مبتنی بر کلمه عبور) را به RADIUS یا LDAP سرور سازمان ارسال می‌کند.

جدول زیر لیست سامانه‌ها و روش اتصالی پیشنهادی سامان را نمایش می‌دهد:

کلاینت	نرم‌افزار سامان	APIهای سامان	سامان-پروکسی
سیستم‌عامل ویندوز	×		×
سیستم‌عامل لینوکس	×		×
سیستم‌عامل BSD	×		×
سامانه‌های نرم‌افزاری		×	×
تجهیزات Cisco از جمله: Cisco ACS / ISE / ISR / Catalyst / SSH Network Device Access / IPSec VPN / ASA			×
تجهیزات Fortinet			×
تجهیزات Juniper			×
WALLIX Bastion PAM			×

۶ سیاست‌گذاری احراز اصالت چندعاملی

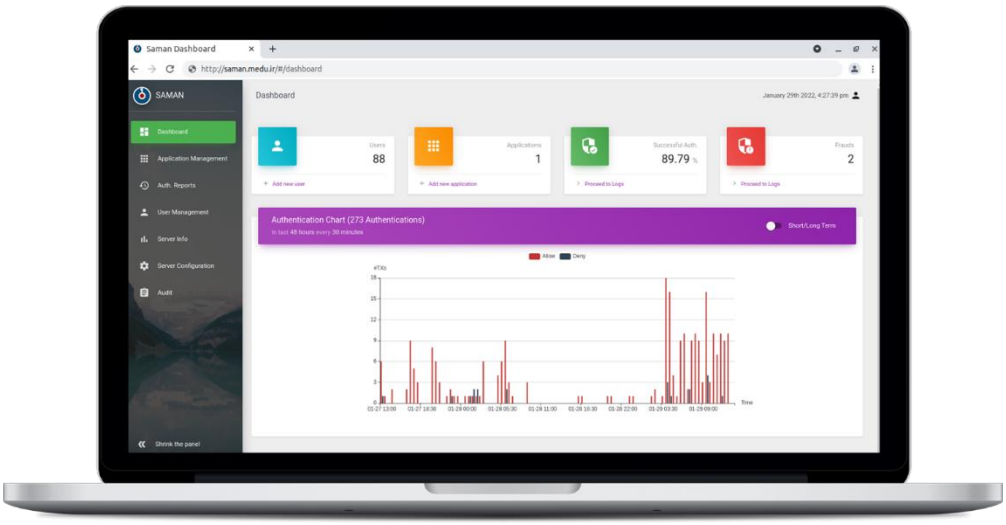
سیاست‌های احراز اصالت، عملکرد MFA و همچنین تخصیص دسترسی‌ها را کنترل می‌کنند. این سیاست‌ها می‌توانند بر روی کاربران، گروه‌ها، دستگاه‌ها، مکان یا زمان دسترسی و سایر فاکتورهای دسترسی تعریف و اعمال شوند. موتور سیاست‌های احراز اصالت سامان، در کنار سیاست‌های از پیش تعریف شده، امکان تعریف و اعمال سیاست‌های دلخواه را نیز فراهم می‌آورد. شکل زیر نمونه‌ای از سیاست‌گذاری‌های محصول سامان-MFA را در داشبورد مدیریتی محصول نمایش می‌دهد.



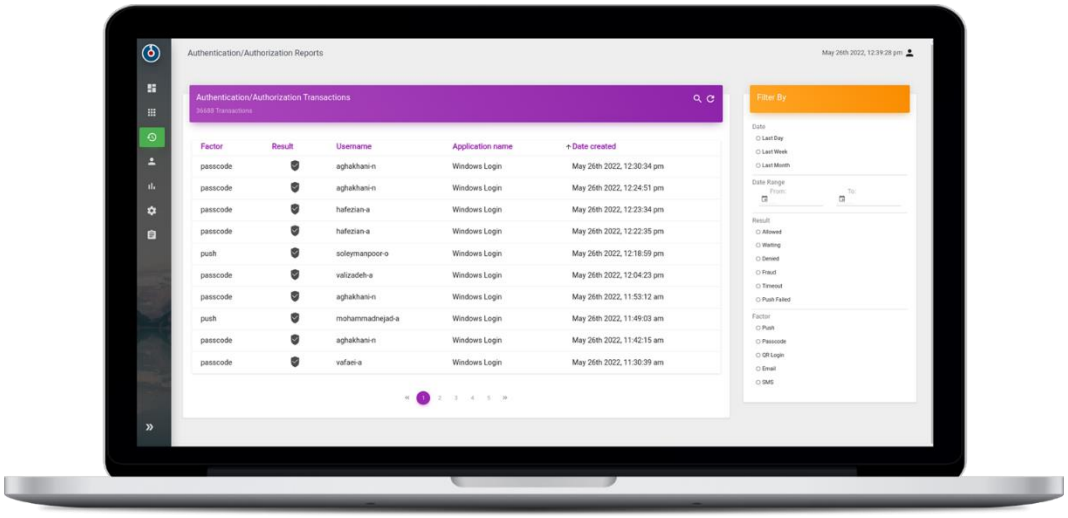
۷ گزارش‌گیری

۷,۱ گزارشات داشبورد مدیریتی سامان

سامان در داشبورد مدیریتی خود نمودارهایی شامل نتایج احراز اصالت چندعاملی در گذر زمان را با توجه به بازه‌های زمانی کوتاه و بلندمدت نمایش می‌دهد. علاوه بر آن، تعداد کاربران، سامانه‌های متصل، نسبت موفق‌بودن احرازاصالت و تعداد تقلب‌های گزارش‌شده در داشبورد مدیریتی سامان نمایش داده می‌شود.

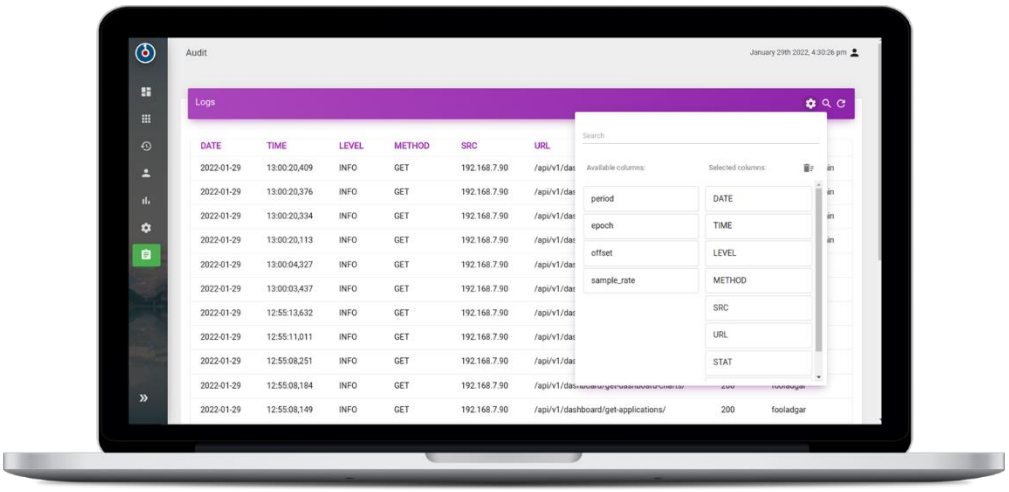


علاوه بر آن سامان گزارشات احراز اصالت را به صورت جدولی نیز نمایش می‌دهد و راهبران سامانه می‌توانند از طریق فیلترکردن آن گزارشات بر اساس پارامترهای مختلف (نظیر عامل، زمان، سامانه‌ی مربوطه، نتیجه احراز اصالت و ...) مدنظر خود را مشاهده نمایند.



۷,۲ رویدادنگاری فعالیت راهبران سامانه

با توجه به استانداردها و دستورالعمل‌های امنیتی سازمان افتا، محصول سامان-MFA کلیه‌ی فعالیت‌های راهبران سامانه را نیز رویدادنگاری می‌نماید و این موضوع به راهبران ممیزی‌کننده سازمان اجازه می‌دهد در صورت بروز نقصان‌هایی در رفتار سامانه‌ها به بررسی این رویدادها بپردازند. شکل زیر، بخش ممیزی داشبورد مدیریتی سامان را نمایش می‌دهد.



۷,۳ ارسال رخدادها به ابزارهای SIEM و به صورت SYSLog

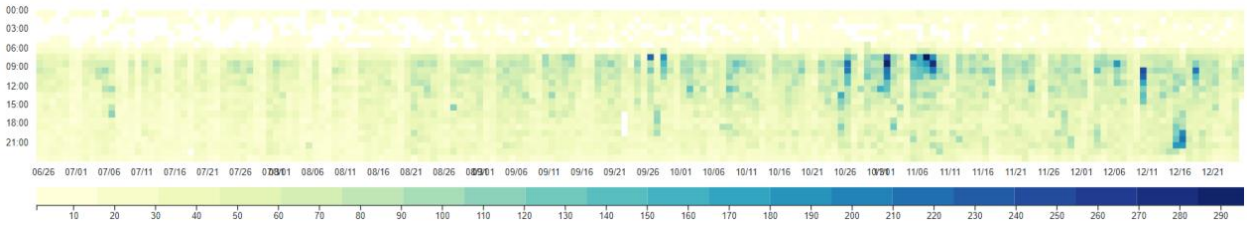
علاوه بر نمایش رخدادهای احرازاصالت و ممیزی در داشبورد مدیریتی سامان، رخدادهای این سامانه در فرمت استاندارد Syslog جمع‌آوری و گزارش می‌شوند. به این ترتیب، اطلاعات رخدادها می‌توانند برای تجزیه و تحلیل بیشتر، در ابزار متنوع تحلیل خودکار وارد شوند.

۷,۴ داشبوردهای هوشمندی کسب‌وکار

به منظور گزارش‌گیری، از یکی از داشبوردهای هوشمندی کسب‌وکار در کنار سامانه پیشنهادی توصیه می‌شود. به این منظور اطلاعات خام احراز اصالت کاربران، دسترسی‌ها و ... را توسط یک View[۱] فقط خواندنی[۲] برای استفاده در داشبورد مربوطه ارائه می‌شود. به این ترتیب می‌توان گزارش‌های مورد نظر را طریق این داشبورد آماده نموده و نمایش داد. شرکت پیام پرداز حداکثر تا ۵ نمونه از گزارش‌های مورد نظر کارفرما را با استفاده این ابزارها آماده و ارائه می‌کند. پس از آن کارفرما با توجه به آموزش‌هایی که از شرکت پیام‌پرداز در

[۱] منظور دستور *View* در پایگاه‌های داده است که یک پرس‌وجو را به صورت فقط خواندنی در دسترس کاربران غیر مدیر قرار می‌دهد. عمدتا این دستور برای گزارش‌گیری استفاده می‌شود.
[۲] *Read only*

مورد نحوه کارکرد این داشبورد دریافت می‌نماید می‌تواند گزارش‌های متنوع مدنظر خود را فراهم نماید. شرکت پیام‌پرداز در صورت نیاز می‌تواند با ارائه مشاوره در این زمینه به سازمان کمک نماید. به منظور ارائه این داشبورد پیشنهاد شرکت پیام‌پرداز استفاده از محصول متن‌بازApache Superset است. نمونه‌ای از گزارش‌های داشبوردهای هوشمندی کسب‌وکار در تصویر زیر موجود است:



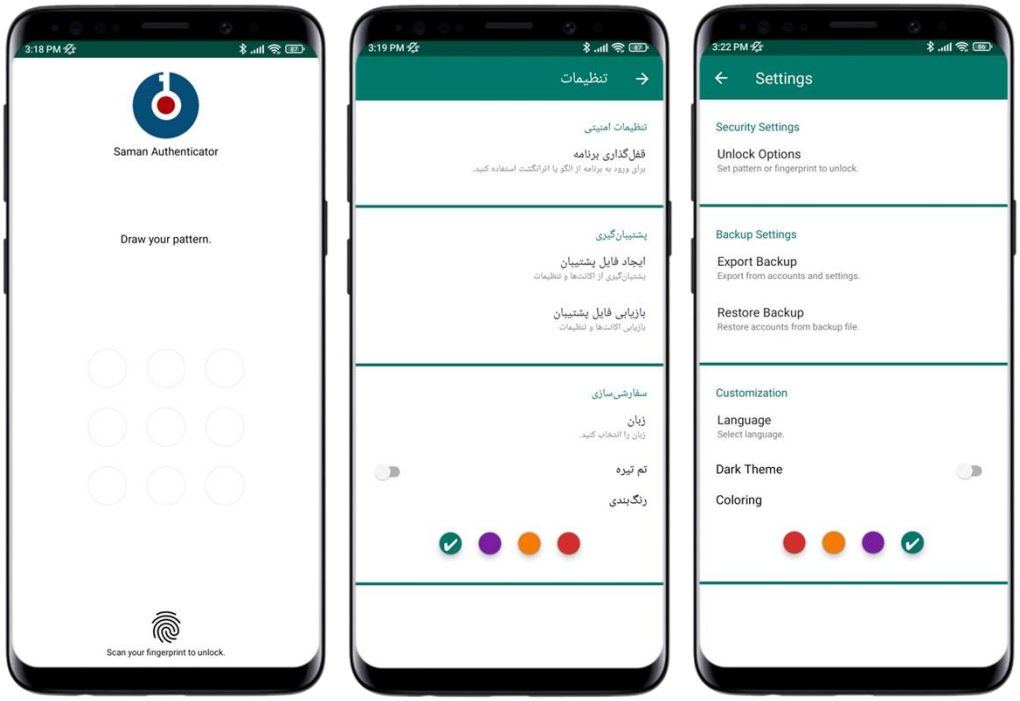
این تصویر نشان‌دهنده‌ی میزان ورود کاربران در ساعات مختلف شبانه‌روز و در گذر زمان است. همان‌گونه که دیده می‌شود، رنگ آبی پررنگ نشان‌دهنده‌ی بیشترین تعداد درخواست احراز اصالت چندعاملی در بازه‌ی زمانی است.

به منظور مدیریت کلیه کاربران و سامانه‌هایی که از سامان-MFA استفاده می‌کنند مدیران سازمان می‌توانند از داشبورد مدیریتی سامان-MFA استفاده کنند. این داشبورد شامل گزینه‌هایی برای مدیریت کاربران، سامانه‌های متصل، مشاهده لاگ‌های احراز اصالت، سیاست‌گذاری فرآیند احراز اصالت و ... است. شکل‌های زیر نمایی از این داشبورد را نمایش می‌دهند.

۸ سهولت کاربری بالا در عین امنیت

سامان برای افزایش سهولت کاربری تلاش کرده است نرم‌افزارهای تلفن همراهی را پیاده‌سازی نماید که از انواع سیستم‌عامل‌های اندروید و IOS پشتیبانی نموده و همچنین امکان پشتیبانی از چند زبان را داشته باشد. اما پیاده‌سازی نرم‌افزار تلفن همراه سامان اگرچه به سهولت کاربری همراه بوده است، اما به امنیت کاربران لطمه‌ای وارد نشده‌است. به عنوان مثال، کاربران می‌توانند از حسگرهای بایومتریک تلفن همراه خود برای حفاظت نرم‌افزار تلفن همراه سامان استفاده نمایند.

تصاویر زیر، نمایی از نرم‌افزار تلفن همراه سامان را ارائه می‌نماید.


3:18 PM
Saman Authenticator
Draw your pattern.
Scan your fingerprint to unlock.
3:19 PM
تنظیمات
تنظیمات امنیتی
قفل‌گذاری برنامه
پشتیبان‌گیری
ایجاد فایل پشتیبان
بازیابی فایل پشتیبان
سفارشی‌سازی
زبان
تم تیره
رنگ‌بندی
3:22 PM
Settings
Security Settings
Unlock Options
Set pattern or fingerprint to unlock.
Backup Settings
Export Backup
Export from accounts and settings.
Restore Backup
Restore accounts from backup file.
Customization
Language
Select language.
Dark Theme
Coloring