- مدیریت و کنترل سطوح دسترسی کاربران ارشد، برنامه ها و سیستم های عمل
- جلوگیری از اعمال سهوی یا عمدی دستورات مخرب با دسترسی سطح بالا بر روی سیستم های حیاتی
- مدیریت دسترسی برای کاربران از راه دور
- محافظت در برابر تهدیدات امنیتی ناشی از دسترسی در سطوح بالا
- احراز هویت یکپارچه و دو عاملی
- ضبط تصاویر دسترسی کاربران به سیستم با قابلیت جستجو

مقدمه: افزایش تهدیدات امنیتی پیچیده و هدفمند توسط مهاجمان خارجی و خودی های مخرب ، محافظت صحیح از اطلاعات مهم و حساس را برای سازمان ها بسیار دشوار کرده است. وظیفه حفاظت از این دارایی ها به مراتب سخت تر شده است چرا که محیط های فناوری اطلاعات پیچیده تر شده و به طور گسترده در نقاط جغرافیایی و ابر توزیع شده اند.

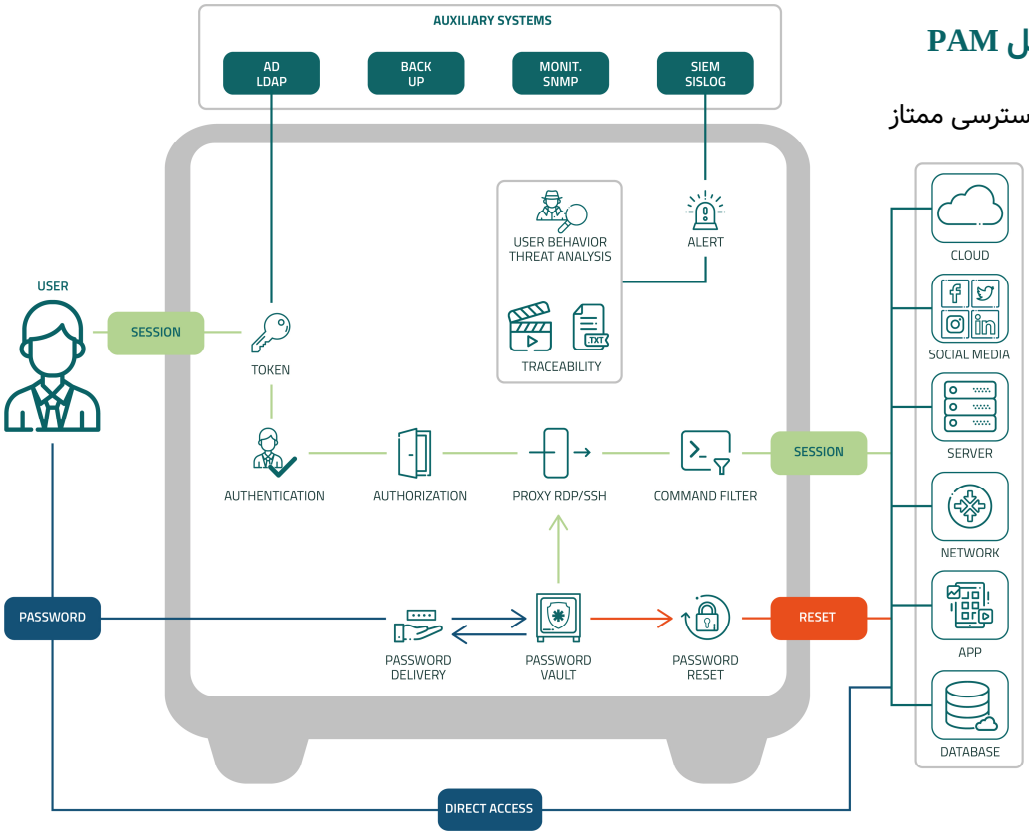
بسیاری از نقض های برجسته اخیر دارای یک نکته مشترک هستند: **آنها با مصالحه با رمزهای عبور به نتیجه رسیده اند.**

سوء استفاده از حسابهای ممتاز به شدت باعث حمله سایبری می شود. در حملات اخیر به شرکت و سازمانها، در بسیاری از موارد ، رمزهای عبور کاربر نهایی در ابتدا از طریق تکنیک های مختلف مهندسی اجتماعی هک می شوند. سپس مجوزها برای دسترسی به حسابهای ممتاز - کلیدهای پادشاهی - افزایش می یابد. این دسترسی غیرمجاز می تواند هفته ها یا حتی ماه ها به راحتی قابل شناسایی نباشد و به هکرها اجازه می دهد اطلاعات را برای راحتی و راحتی خود ببینند و سرقت کنند.

متجاوزان حساب های ممتاز را به سرقت برده و از زیرساخت های کل شرکت سو استفاده کرده اند. متاسفانه ، بسیاری از مدیران فناوری اطلاعات درک کاملی از نحوه عملکرد حسابهای ممتاز و همچنین خطرات مرتبط با سازش و سو استفاده از آنها ندارند. این امر باعث می شود که آنها و سازمان هایشان در برابر آسیب های احتمالی پولی و اعتباری بسیار آسیب پذیرتر باشند. مدیریت دسترسی ممتاز Previldge Access Management-PAM راهکاری برای مقابله با این مسله است.

## نحوه کار راه حل PAM

جریان مدیریت دسترسی ممتاز



## عملکردها

### محافظت از شبکه های اجتماعی

یوزر/پسورد شبکه های اجتماعی شرکت خود را در برابر نشریات بی مورد و کاربران با نیت بد مدیریت کرده و آنها را حفظ کنید.

### اسکن و کشف

جستجوی دستگاه ها و اعتبار ( یوزر/پسورد) معتبر در شبکه خود را به صورت خودکار انجام دهید و راه حلی را آماده کنید تا تمام خواسته های دسترسی را تامین کند.

### جلسات لاگ شده

کاربرانی را که جلسه ثبت شده ، نظارت شده و ۱۰۰٪ ضبط شده را اجرا می کنند ، از جمله جلسات همزمان ، مشخص کنید.

### ضبط جلسه

100٪جلسات از راه دور انجام شده در senhaseguraرا در فیلم های فشرده با کیفیت عالی ، شامل جلسات همزمان ضبط کنید.

### تغییر خودکار

هروقت که زمان استفاده منقضی می‌شود، گذرواژه ها به صورت خودکار تغییر می‌یابد .

### تایید کار

کنترل دسترسی به یک دستگاه مدیریت شده یا اعتبارنامه شخصی از طریق گردش کار تایید چندسطحی و انعطاف پذیر حفظ کنید.

### برنامه به برنامه

اعتبارنامه ادغام بین سیستم ها ، پایگاه داده ها یا پیکربندی شده در کد منبع را به SENHASEGURA وارد کنید.

### سرور جهش

دسترسی ها از طریق Putty یا RDP می توانند از طریق جلسات انجام شوند، بدون اینکه رمز ورود در معرض کاربر درخواست کننده قرار گیرد. همه فعالیتهای کاربر تحت نظارت قرار می گیرد.

### ممیزی دستورات (Commands Audit)

هشدارهای دستورات در جلسات SSH ، Telnetو پایگاه داده حتی برای کاربران سرپرست را پیکربندی کنید.

### محافظت چندگانه

نگهداری مضاعف از رمزهای عبور را ایجاد کنید و مطابقت خود را با کنترل های امنیتی و حسابرسی خود حفظ کنید.

## مدیریت اعتبارنامه

### مدیریت چرخه کامل اعتبار دسترسی بالا(مدیران)

کاربرد: مدیریت دسترسی متمرکز برای محافظت و کنترل استفاده از اعتبارنامه

### نحوه کار

با تعریف گروه مجاز، کاربرانی که اجازه دسترسی راه دور یا دسترسی به یک دستگاه را دارند به گروه مجاز اضافه می کنیم.

### ویژگی ها

- ذخیره امن اعتبارنامه
- تعریف گروهها برای تفکیک دسترسی.
- انعطاف پذیری در فرآیند تایید
- چندین کاربر می توانند درخواست دسترسی به همان حساب ممتاز را داشته باشند
- دسترسی اضطراری برای مشاهده فوری رمز عبور
- حفاظت مضاعف از رمزهای عبور
- ادغام با Help Desk و ابزارهای مدیریت تغییر
- تغییر رمزهای عبور با زمان مصرفی یا بعد از مشاهده آن ها
- تغییر خودکار رمز عبور

### ویژگی های فنی

- استفاده از بیت های AES 256 ، SHA 256 ، RSA 2048 bit s یا استانداردهای رمزگذاری بالاتر
- ادغام با سرویس اکتیو دایرکتوری

### فواید

- به دست آوردن سطح امنیتی
- مطابقت با استانداردهای امنیتی
- ضمانت تحویل رمز عبور ایمن
- سود عملیاتی در روند تغییر رمز عبور
- احراز هویت شفاف در سیستم یا دستگاه بدون نمایش گذرواژه

## تجزیه و تحلیل تهدید

### تجزیه و تحلیل خودکار اقدامات حیاتی

کاربرد: نظارت بر محیط برای شناسایی و هشدار مشکوک بودن اقدامات انجام شده با اعتبار ممتاز

### نحوه کار

لیستی از دستورات و رفتارهای مشکوک در محیط با توجه به خطر آنها طبقه بندی می شود و در صورت شناسایی ، به آنها اطلاع داده می شود و در یک صفحه گرافیکی تلفیق می شود

### ویژگی ها

- داشبورد گرافیکی با خطرات و تهدیدها
- هشدارهای دقیق درباره فعالیت مشکوک
- تجزیه و تحلیل جلسه کاربر
- حسابرسی ، هشدار و مسدود کردن دستورات
- ثبت لاگ های مربوط به دستورات
- علامت گذاری روی علائم نگارشی
- شناسایی حرکت جانبی و ارتفاع امتیاز
- هشدارهای مربوط به فعالیت مشکوک برای SIEM / SYSLOG.

### ویژگی های فنی

- خودآموزی در مورد عملکرد ماشین و رفتار کاربر
- مسدود کردن دستورات براساس لیست سفید و لیست سیاه
- پاسخ خودکار برای تشخیص تهدیدها

### فواید

- کشف آسیب پذیری های احتمالی
- کاهش زمان پاسخ برای حمله
- مسدود کردن خودکار اعتبارنامه های مسروقه
- قابل مشاهده بودن تهدید
- اطلاعات کامل مربوط به داخل

## ضبط جلسه و حسابرسی

### دسترسی به سرور بدون افشای رمز عبور

کاربرد: ضبط جلسات از راه دور که از طریق سنهاسگورا انجام شده استبه منظور شناسایی اقدامات نادرست

نحوه کار: senhasegura یک هش منحصر به فرد برای هر جلسه ثبت می کند و بدنوسیله شناسایی کارهایی که هر کاربر در هنگام دسترسی انجام داده است میسر می‌شود.

### ویژگی ها

- ضبط جلسات در فرمت ویدیویی
- ضبط دستورات تایپ شده در محیط های RDP و SSH
- بررسی جلسه یا تولید پرونده MP4
- جستجو در جلسات ضبط شده با استفاده از مجموعه معیارهایی مانند کاربر یا دستورات تایپ شده
- نظارت بلادرنگ جلسات

### ویژگی های فنی

ضبط جلسه و لاگ صفحه کلید می توانند برای موارد زیر استفاده شود:

- اقدامات انجام شده در تمام جلسات انجام شده از طریق سنهاسگورا
- اقدامات انجام شده در دستگاه هدف ، سیستم یا صفحه HTTP
- دسترسی از راه دور به گروهی از کاربران یا دستگاه ها
- جلساتی که از طریق مشتری محلی در ایستگاه کاربر (PuTTy , Terminal Service) انجام می شود.

### فواید

- قابلیت ردیابی کلیه اقدامات انجام شده ، از جمله اقدامات انجام شده توسط اشخاص ثالث
- کاهش زمان عیب یابی
- نظارت بلادرنگ
- شناسایی اقدامات مشکوک
- مخزن شواهد ایزوله ، رمزگذاری شده و محافظت شده

## Scan Discovery

اعتبارات ممتاز را بطور خودکار کشف کنید

کاربرد: ویژگی Scan Discovery محیط پیرامون را اسکن کرده و امکان ثبت خودکار دستگاه ها و اطلاعات کاربری را در سنهاسگورا فراهم می کند

### نحوه کار

Scan Discovery می تواند در هر محیطی اجرا گردد یا روی بخش خاصی از شبکه اعمال شود .همچنین می توان افزونه های جستجوی مورد استفاده را تنظیم کرد.سنهاسگورا همچنین می تواند از طریق پروتکل استاندارد (RDP ، SSH / TELNET )بدون نیاز به نصب عامل محلی (Agent) متصل شود.

### ویژگی ها

- اسکن منظم شبکه بر اساس محدوده IP
- شناسایی خودکار حساب های ممتاز در محیط های: Unix, Linux, Windows, Oracle , MS SQL or MySQL

### ویژگی های فنی

- این راه حل توانایی شناسایی هر نوع دستگاه متصل به شبکه های شما مانند سرورها ، پایگاه داده ها ، دستگاه های شبکه یا ایستگاه های کاری را دارد.

### فواید

- کشف خودکار دارایی ها و اعتبارنامه‌ها در شبکه
- پشتیبانی کامل از دستگاه ها و سیستم ها
- ثبت آسان وسایل و اعتبارنامه ها
- استقلال روند موجودی دارایی
- ارزیابی دوره ای محیط برای شناسایی دستگاه ها و اعتبارنامه های جدید

## مدیریت کلید SSH

کنترل ایمن چرخه کلید SSH

کاربرد: ذخیره سازی امن، چرخش و کنترل دسترسی ها برای محافظت از کلید SSH

### نحوه کار

مدیریت کلید SSH در راه حل متمرکز شده است. جفت کلیدها را به طور خودکار مطابق با سیاست امنیتی شرکت شما تغییر می دهد.

### ویژگی ها

- اسکن سرور Linux و شناسایی کلیدSSH
- سازماندهی لیستی از ارتباطات مابین سرورها
- کلیدهای SSH با انتشار دستی تنظیم مجدد می شوند
- انتشار کلیدSSH
- گزارش های کلیدی نگاشت
- گزارش دسترسی و گزارش استفاده از کلید SSH

### ویژگی های فنی

رمزگذاری کلیدهای ذخیره شده SSH و کلیه ارتباطات با استفاده از این کلیدها

### فواید

- مدیریت متمرکز کلیدهای SSH
- کنترل و ردیابی کلیدهایSSH
- مدیریت روابط اعتماد بین کلیدهای SSH و سیستم
- مسدود کردن دسترسی غیرمجاز به حسابهای ممتاز با استفاده از کلیدهایSSH

## هویت برنامه

از شر کلمه عبور سخت و دسترسی مبتنی بر شخص خلاص شوید

کاربرد: امکان حذف اعتبارنامه درج شده در کدهای منبع ، اسکریپت ها و پرونده های پیکربندی

### نحوه کار

این راه حل از الگویی برای تغییر رمز ورود اعتبار برنامه استفاده می کند و رمز ورود رمزگذاری شده جدید را در پایگاه داده خود ذخیره می کند .اعتبارنامه را می توان با اتصال API مشاهده کرد یا مستقیماً در مجموعه اتصال سرور برنامه قرار داد.

### ویژگی ها

- تغییرات رمز عبور در برنامه های قدیمی انجام می شود:
- HTTP، HTTPSو SocialNetworks ؛ ادغام بین پایگاه داده و برنامه یا یک استخر اتصال
- رابط دسترسی از راه دور با ضبط جلسه
- الگوهایی برای تغییر رمزهای عبور برنامه در قالب باز و قابل شنیدن

### ویژگی های فنی

- تغییر رمز ورود اطلاعات کاربری در سرورهای برنامه
- محدودیت دسترسی بر اساس IP، Pathو Token API
- پشتیبانی یکپارچه سازی توسط REST API ها

### فواید

- رعایت استانداردهای امنیتی
- استفاده از API اتصال راه حل
- مدیریت متمرکز اعتبار نامه های برنامه
- کنترل دسترسی گرانول : امکان دسترسی از راه دور بدون نمایش رمز عبور
- احراز هویت قابل اطمینان از تمام درخواست های رمز عبور

## تجزیه و تحلیل رفتار

به طور خودکار رفتار کاربر را نظارت کنید

کاربرد: شناسایی ، هشدار و پاسخگویی برای فعالیتهایی که توسط اعتبارنامه های ممتاز انجام می شود ، مراحل حیاتی در مدیریت دسترسی است.

### نحوه کار

این راه حل دارای مکانیزم خودآموزی برای شناسایی و پاسخگویی به هرگونه تغییر در رفتار کاربر و الگوهای دسترسی است

### ویژگی ها

- تجزیه و تحلیل جلسه کاربر بر اساس تاریخچه رفتار
- شناسایی دسترسی ها یا نمایش های مشکوک توسط مجموعه ای از معیارها ، مانند تعداد زیاد یا مدت زمان غیر معمول
- شناسایی رفتارهای غیر معمول به همراه هشدارها برای.SIEM / SYSLOG
- الگوریتم های توسعه یافته به طور مداوم با رفتار کاربر سازگار می شوند.
- داشبورد دقیق با نمایش تصویری حوادث و تهدیدها.

### ویژگی های فنی

این راه حل یک سری تحلیل متغیرها مانند ایستگاه مبدا را انجام می دهد. سیستم هدف یا تلاش برای اجرای دستورات مسدود می شود.

فواید

- محدودیت در سو استفاده
- کاهش خطرات سرقت اطلاعات
- کنترل عملکردهای کاربر سرپرست
- شناسایی سریع حملات و حسابهای به خطر افتاده
- پاسخ خودکار به سرقت احتمالی اعتبارنامه

## امتیازات ایستَاه کاری

امتیازات ایستگاه های کاری را محدود کنید.

کاربرد: این امکان را می دهد تا ویژگی Run As را در ایستگاه های کاری برای برنامه هایی که نیاز به اعطای امتیاز دارند، اجرا کنید

### نحوه کار

برنامه های کاربردی مجاز به استفاده از این نوع ارتقا امتیاز قبلا در راه حل ذکر شده اند و استفاده از آنها فقط به کاربران مجاز محدود می شود.

### ویژگی ها

- اجرای برنامه ها در ایستگاه های کاری بدون نمایش رمز عبور به کاربر
- سابقه استفاده از این دسترسی ها در راه حل سنهاسگورا

ویژگی های فنی

- برای ایستگاه های کاری پلت فرم ویندوز ، یک عامل محلی قادر است برنامه ها را با درج خودکار اعتبارنامه، اجرا کند.

فواید

- انطباق با استانداردهای امنیتی
- اجرای برنامه های نیازمند مجوز Admin، بدون افشای رمزهای عبور
- کنترل ارتفاع امتیاز در ایستگاه های کاری
- کاهش خطر حمله بدافزار
- گزارشات جامع در مورد استفاده از اعتبارنامه

## حفاظت از اطلاعات ممتاز

از اطلاعات مهم و حساس کسب و کار خود محافظت کنید.

کاربرد: ذخیره اطلاعات شخصی ، مانند گذرواژه های شخصی و گواهینامه های دیجیتالی

### نحوه کار

این راه حل کل چرخه عمر اطلاعات ذخیره شده را مدیریت می کند ، به عنوان مثال ، هنگامی که تاریخ انقضا یک گواهی دیجیتال نزدیک است ، گزارش می دهد.

### ویژگی ها

- ذخیره گواهینامه های دیجیتالی
- ذخیره گذرواژه های شخصی
- هشدار در مورد انقضا اطلاعات ذخیره شده
- صفحه جستجوی اطلاعات کاربر پسند
- لاگ استفاده و تغییر اطلاعات ممتاز
- اجازه اشتراک اطلاعات با سایر کاربران

### ویژگی های فنی

- پشتیبانی برای استفاده از گواهینامه های دیجیتالی معتبر توسط.ICP-Brasil

### فواید

- انطباق با استانداردهای امنیتی
- مدیریت متمرکز اعتبارنامه ها
- کنترل خودکار اطلاعات ممتاز
- استفاده از گواهینامه های دیجیتال برای دسترسی به سیستم ها و خدمات
- احراز هویت خودکار با استفاده از اعتبارنامه های دسترسی شخصی

## سخت افزار امنیتی PAM

افزایش امنیت و عملکرد راه حل.PAM

کاربرد: راه حل سخت افزاری مبتنی بر لوازم با سیستم عامل سفارشی و پایگاه داده اختصاصی تعبیه شده.

### نحوه کار

این تجهیزات سخت افزاری در مراکز داده و مکان های دسترسی کنترل شده نصب شده اند و راه حل پس از تنظیمات اولیه شبکه برای استفاده آماده است .

### ویژگی ها

- محافظت دربرابر حملات فیزیکی
- محافظت از کلید رمزگذاری شده در سخت افزار
- ذخیره کلیدهای متقارن در سخت افزار
- تخریب داده ها در صورت نقض دستگاه

### ویژگی های فنی

- HSMجاسازی شده
- ماژول TPM
- منبع تغذیه اضافی و داخلی
- افزونگی منبع تغذیه برق بدون وقفه عملیاتی
- رمزگذاری دیسک و افزونه

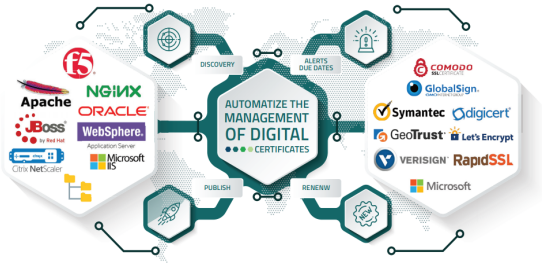
### فواید

- مشخصات مختلف برای پاسخگویی به نیازهای شما
- در دسترس بودن بالا و فن آوری های بازیابی خرابی که در این راه حل وجود دارد
- در دسترس بودن راه حل بدون در نظر گرفتن زیرساخت و ابزار مجازی سازی

## مدیریت چرخه حیات گواهی های دیجیتال

### مدیریت خودکار و متمرکز

مدیریت گواهی نامه سنهاسگورا، تمام چرخه حیات گواهینامه را در داخل سازمان مدیریت می کند .از زمان کشف آن از طریق اسکن خودکار در وب سایت ها ، دایرکتوری ها و وب سرورها ، تا تمدید خودکار گواهینامه از طریق CA خارجی یا داخلی.




### فواید

#### مدیریت گواهینامه ها

نمای کامل و متمرکز کلیه گواهینامه ها و وضعیت مربوط به آن.

#### کاهش و غیرقابل دسترس بودن

کاهش عدم دستیابی که ممکن است به دلیل انقضای گواهینامه ها یا به دلیل خطاهای انسانی در انتشار آن به وجود بیاید.

#### کارایی عملیاتی

اتوماسیون در مدیریت چرخه حیات گواهینامه و همچنین اعتبار سنجی از طریق API های کامل.

#### افزایش امنیت

برنامه هایی با گواهینامه های ایمن ، با رعایت پیش نیازها و سیاست های امنیتی سازمان.

### کارکردها

#### کشف گواهی نامه ها

تمام گواهینامه های دیجیتالی را که به صورت خودکار و دوره ای در شبکه شما استفاده می شود ، کشف کنید.

#### تجدید و انتشار

به طور خودکار تمدید و انتشار دوره ای گواهینامه ها را پیکربندی کنید و از انقضا جلوگیری کنید.

#### تولید الزامات

اطلاعات موردنیاز را با استفاده از اطلاعات از قبل ثبت شده و کاهش خطاهای ایجاد گواهی ها فراهم کنید.

#### امضای گواهی نامه

از یکپارچه سازی با CA های بازار استفاده کنید تا به طور خودکار گواهینامه های داخل راه حل ، از جمله Self-Signed را امضا کنید.

#### تجدید و انتشار

کنترل کامل انقضا (*درختان گواهینامه های *)تحت مدیریت را حفظ کنید . هشدارها را در دوره های قابل تنظیم برای تیم های خاص ارسال کنید.

#### شناسایی آسیب پذیری ها

وضعیت کلیه گواهینامه ها را به صورت گرافیکی تجسم کنید ، شناسایی کنید که برای مثال کدام گواهی از رمزنگاری خارج از سیاست های امنیتی سازمان استفاده می کند.

## ممیزی کنترل CONTROL AUDIT

### جلوگیری از نشت داده و انطباق با LGPD

PCI, ISO, LGPD, GDPR

با اتوماسیون دسترسی های ممتاز و رسیدن به بلوغ در فرایندهای حسابرسی شده، بر چالش های کنترل های نظارتی غلبه کنید.

دسترسی شخص ثالث

دسترسی شخص ثالث را کنترل کنید و فقط فعالیتهای خاص را به روش نظارت شده و برای مدت زمان از پیش تعیین شده در دسترس قرار دهید.

سو استفاده ممتاز PRIVILEGE ABUSE

لیست های سفید را حتی برای کاربران سرپرست در محیط SSH / Telnet و پایگاه های داده تعیین کنید .

رمزهای عبور سخت

رمزهای عبور ثبت شده در کدهای منبع برنامه های قدیمی را حذف کنید .تغییر رمز ورود را به صورت همزمان در پرونده های پیکربندی و سرویس های وابسته ایجاد کنید.

ضبط جلسه

بدون نیاز به نمایش گذرواژه برای کاربر مورد نیاز و ضبط ۱۰۰٪ دسترسی ، گروههای کاربری را که می توانند جلسات را در دستگاههای مهم شروع کنند ، مشخص کنید.

سرقت اطلاعات

دسترسی به اطلاعات معقول را تفکیک کنید ، محیطهای حیاتی را مجزا کرده و وقایع را به هم پیوند دهید تا هرگونه رفتار مشکوک را شناسایی کنید.

سازگاری و حسابرسی

گزارش تهیه شده برای ارائه متنوع ترین کنترل ها و خواسته های ممیزی ها و نهادهای نظارتی

کنترل شخص ثالث

با استفاده از گروه ها و پروفایل های دسترسی ، می توان محدودیت فعال سازی تامین کنندگان و کاربران شخص ثالث را در محیط IT محدود کرد ، با دادن اجازه دسترسی کنترل شده فقط به یک دستگاه یا سرویس خاص در شبکه شما و برای مدت زمان از پیش تعیین شده

آنالیز تهدیدها

تهدیدات احتمالی و رفتارهای مشکوک را در زمان واقعی دنبال کنید، بمنظور مشاهده اقدامات انجام شده با اعتبار ممتاز، از نشت اطلاعات جلوگیری کنید ، زمان پاسخ را کاهش دهید یا حتی قطع و حمله کنید.

رمزهای عبور سخت

اطلاعات کاربری ثبت شده در کد منبع و پرونده های پیکربندی را حذف کرده و از داده های مهم محیط محافظت کنید مدارک مستقیماً توسط senhasegura به برنامه ها تحویل داده می شود و دیگر توسط API تیم توسعه دهنده شناخته نخواهد شد.

ضبط جلسه

تمام جلسات از راه دور انجام شده از طریق راه حل با اطمینان از ردیابی کامل اقدامات ، در یک فایل قالب ویدیویی ثبت می شوند .فایل ضبط شده می تواند مشاهده یا برون ریزی گردد و به عنوان شواهد حسابرسی یا برای تجزیه و تحلیل عیب یابی ارسال شود.

**INTEGRATION**
- Unix, Linux, Windows
- Oracle, MS SQL, PostgreSQL, MySql, oTHERS
- Router, Switch, Balancer
- Firewall, IPS, IDS
- Storage
- Apache, JBOSS, IIS, GLASSFISH, TOMCAT, SAP
- Facebook, YouTube, Gmail, WEBAPPLICATION
- HTTPS, SSH, TELNET, RDP, VNC, TN3270
- Main Frame

**AUTHENTICATION**
- UMS AD, LDAP
- RADIUS, TACACS
- Local, Double Factor, Certificate

**CLUSTER AND AVAILABILITY**
- High availability
- Disaster Recovery
- Multi Site

**MOBILITY**
- IOS / Android

**SECURITY**
- ASSH
- HTTPS
- Cryptography RSA 2048, ECC, AES 256, SHA 256
- HSM

**DEVSECOPS**
- DOCKER
- KUBERNETES
- JENKINS
- OUTHERS

## DevOps

چابکی و امنیت رمزها و اعتبارنامه در سراسر پایپلاین توسعه نرم افزار

کاربرد: محافظت از اعتبارنامه ها و رمزها در برنامه ها ، اسکریپت ها و هویت ماشین در سراسر پایپلاین

### نحوه کار:

مدیریت رمز Senhasegura DevOps پایپلاین توسعه را برای شناسایی داده های حساس اسکن می کند ، اجازه می دهد رمزها را بدون نیاز به بازسازی مجدد به گردش دربیاورید. به این ترتیب ، می توان داده های حساس مورد استفاده برنامه ها ، کانتینرها ، ابزارهای اتوماسیون در محیط های تولید را از تیم های توسعه جدا کرد.

### کارکردها

- حفاظت و مدیریت رمزها و مدارک دیگر مورد استفاده در محیط های DevOps ؛
- کشف ، موجودی و مدیریت رمزها درسراسر محیط DevOps ؛
- تنها راه حل PAM برای ارایه یک IAM یکپارچه ابری.
- مدیریت متمرکز رمزهای مشترک و رمزهای عبور سخت کدگذاری شده
- دسترسی گرانولی برای اجازه اجرای اصل حداقل امتیاز principle of least privilege (PoLP)
- داشبورد و گزارشات متمرکز برای دید کامل در محیط

### ویژگی های فنی

- ادغام با ابزارهای اصلی DevOps ، شامل کانتینر سازی وCI / CD
- مجموعه ای از API های امن و انعطاف پذیر برای ادغام آسان و سریع
- یک راه حل کاملاً مقیاس پذیر و یکپارچه با پلت فرم امنیتی senhasegura

### فواید

- کاهش خطر و افزایش سطح امنیتی در سراسر پایپلاین DevOps
- انطباق با استانداردها و سیاست های امنیتی
- سود عملیاتی در مدیریت مخفی
- مهارت بیشتر برای تیم های توسعه و عملیات
- سرعت در استقرارDevSecOps


درباه Senhasegura: سنهاسگورا توسعه دهنده محصولات PAM ( مدیریت دسترسی ممتاز) یک شرکت برزیلی است که محصول آن در گارتنر دارای بالاترین رتبه می باشد. محصول PAM سنهاسگورا ، کاملترین و جامع ترین محصول در بازار است.شرکت ریان سامانه آرکا به عنوان نماینده انحصاری سنهاسگورا در ایران، خدمات فروش و پشتیبانی آن را به عهده دارد.

رایان سامانه آرکا- نماینده انحصاری سنهاسگورا در ایران

تهران، خیابان شهید بهشتی ، خیابان پاکستان ، کوچه چهارم ، پلاک ۱۱ ، طبقه چهارم ، واحد ۷
تلفن: ۸۸۸۰۴۹۶۱ | دورنگار: ۸۹۷۸۳۷۳۷ | کدپستی : ۱۵۳۱۶۴۵۹۱۸
www.arka.ir info@arka.ir
arka رایان سامانه آرکا