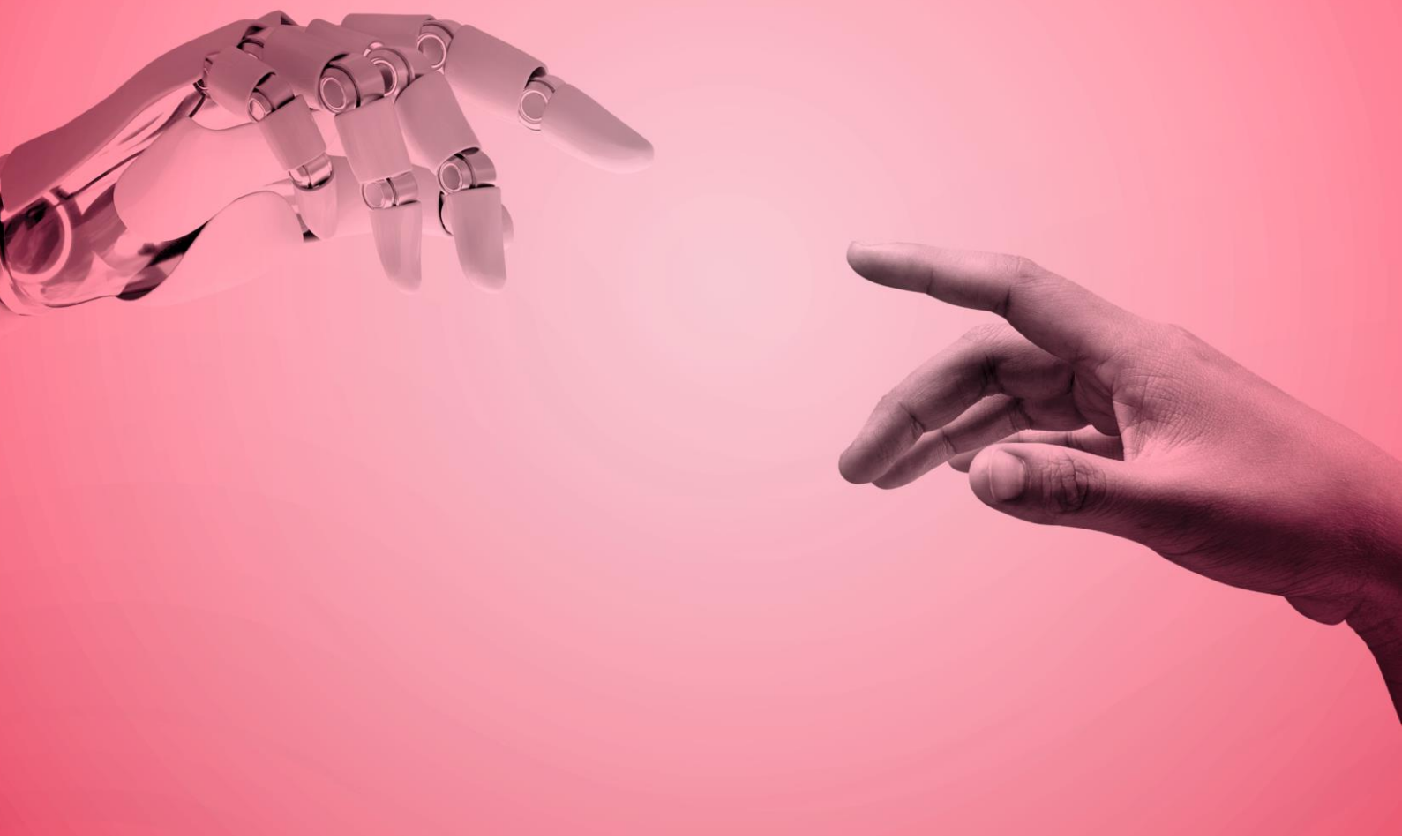

نسل جدید DLP

ZECURION DLP 13 + AI

آگاهی بیشتر، ریسک کمتر.

Rev 1.6

ZECURION

arka
رایان سامانه آرکا

20 ویژگی کلیدی DLP نسل جدید Zecurion

1
مدیریت کامل کانال‌های نشت داده

مدیریت تمامی کانال‌های بالقوه نشت داده به منظور کاهش ریسک نشت اطلاعات و اطمینان از رعایت مقررات و استانداردها.

2
سیاست‌ها و مقررات تطبیقی

ایجاد یک سیاست واحد برای چندین یا تمامی کانال‌های انتقال داده با بهره‌گیری از روش‌های مختلف شناسایی محتوا.

3
فهرست هوشمند کارکنان

نظارت بر شاخص‌های حیاتی مانند سطح ریسک، بهره‌وری، رویدادها، سیاست‌های فعال‌شده و وضعیت‌های احساسی.

4
کنسول مدیریت یکپارچه

Zecurion DLP رابطی مبتنی بر وب برای تمام ماژول‌ها ارائه می‌دهد که داشبورد قابل تنظیمی دارد و مدیریت متمرکز از راه دور را آسان و کارآمد می‌سازد.

5
ذخیره‌سازی فایل‌ها و پیام‌ها

تمامی داده‌های جمع‌آوری‌شده مانند فایل‌ها، پیام‌ها، رویدادها و رخدادها در یک پایگاه‌داده امن ذخیره می‌شوند. این امکان را فراهم می‌کند تا گزارش‌هایدقیق تهیه کرده، تحقیقات قانونی انجام دهید و مدارک لازم برای فرآیندهای حقوقی را گردآوری کنید.

6
استخراج محتوای فایل

با استفاده از شناسایی خودکار بیش از ۵۰۰ قالب فایل بر اساس ساختار داخلی آن‌ها (و نه فقط پسوند)، این سیستم می‌تواند فایل‌های رمزگذاری‌شده را نیز شناسایی کرده و فایل‌های فشرده (حتی تو در تو) را استخراج کند. بنابراین هیچ داده‌ای بدون تحلیل کامل از شبکه خارج نمی‌شود.

7
پروفایل‌های رفتاری

توسعه پروفایل‌های رفتاری بر اساس الگوهای مشخص (مثلاً کاربران از راه دور، کارکنان بخش‌های خاص و...)، Zecurion DLP نشان می‌دهد که رفتار یک کاربر تا چه حد با الگوهای مشخص‌شده تطابق دارد. همچنین، گردآوری و سازمان‌دهی تمامی آدرس‌های ایمیل، پروفایل‌های شبکه‌های اجتماعی و حساب‌های پیام‌رسانی فوری کارکنان برای اطمینان از قابلیت پیگیری ارتباطات کاربران.

8
تحلیل رفتار کاربر با شناسایی ناهنجاری‌ها

ایجاد پروفایل‌های رفتاری برای تمامی کاربران به‌منظور شناسایی فعالیت‌های غیرعادی مانند: وضعیت کارمند جدید، اولین اتصال از راه دور، افزایش فعالیت، تعامل با افراد ناشناس و... شناسایی تهدیدها به‌صورت پیشگیرانه، تیم امنیتی را هشدار داده و امکان واکنش سریع را فراهم می‌سازد.

9
ثبت وقایع

ثبت خودکار تمامی رویدادهای داخلی و اقدامات مدیر سیستم جهت تسهیل نگهداری و ردیابی سریع مشکلات احتمالی. این کار به ارزیابی ریسک و پیشگیری از رویدادهای امنیتی کمک می‌کند.

10
رابط برنامه‌نویسی REST API

بسیاری از وظایف مدیریتی و نظارتی از طریق درخواست‌های HTTP REST API قابل انجام است که امکان خودکارسازی امنیت و یکپارچه‌سازی با سایر ابزارها و پلتفرم‌های زیرساخت IT شما را فراهم می‌کند.

11
NEW!
حالت تعلیق عامل DLP در نقطه پایانی

امکان توقف فعالیت عامل نقطه پایانی توسط کاربر (با تایید مسئول امنیتی)، که انعطاف‌پذیری بیشتری را فراهم می‌سازد در حالی که پروتکل‌های امنیتی همچنان مؤثر باقی می‌مانند.

12
ارزیابی احساسی

ارزیابی احساسات کارکنان بر اساس هشت واکنش احساسی پایه برای شناسایی گروه‌های پرریسک. سیستم گزارشی از پویایی احساسی هر کارمند ارائه می‌دهد که در قالب نموداری واضح و قابل درک نمایش داده می‌شود. این قابلیت دید عمیق‌تری نسبت به احساسات کارکنان فراهم کرده و در شناسایی اعضای تیم با وفاداری پایین مؤثر است.

ZECURION

13
مقایسه رفتارها

تحلیل رفتار کاربران (UBA) رفتار فعلی کاربران را با میانگین رفتار آن‌ها مقایسه می‌کند. انحرافات قابل توجه ممکن است نشانه‌ای از تهدیدات احتمالی امنیت اطلاعات یا استفاده غیرمجاز از اعتبارنامه‌ها باشد. همچنین می‌توان رفتار دو کاربر یا یک کاربر با یک گروه را مقایسه کرد.

14
نقشه ارتباطات کاربران

Zecurion DLP یک نمودار تعاملی از ارتباطات و کانال‌های ارتباطی کاربران ایجاد می‌کند که امکان شناسایی روابط پنهان را فراهم می‌سازد. این ابزار تحلیل ارتباطات مشکوک که ممکن است نشان‌دهنده کلاهبرداری داخلی یا خطر نشت داده باشند را ممکن می‌کند.

15
گزارش‌گیری جامع

با بیش از ۲۰ گزارش از پیش تنظیم‌شده و گزینه‌های سفارشی‌سازی، این پلتفرم ابزاری قدرتمند برای ممیزی امنیتی و تحقیقات فراهم می‌سازد. می‌توان به‌راحتی گزارش‌ها را تولید و تحلیل کرد و با چند کلیک جزئیات رخدادها را بررسی کرد.

16
یکپارچه‌سازی با Active Directory

کاربران، گروه‌ها و نام میزبان رایانه‌ها با Active Directory هماهنگ می‌شوند تا یکپارچگی با زیرساخت IT شما را بهبود بخشند. این امر امکان شناسایی کاربران با نام در گزارش‌ها و رویدادها را فراهم می‌سازد و روند مدیریت را ساده‌تر می‌کند.

17
ارزیابی مبتنی بر ریسک

Zecurion DLP امتیاز ریسک و روند آن را برای هر کارمند نمایش می‌دهد. هر پروفایل کاربر شامل پنج شاخص ریسک است که اطلاعاتی دقیق برای تحقیقات ارائه می‌دهند: میانگین ریسک شرکت، ریسک روز گذشته، ریسک کنونی، میانگین ریسک روزانه، و میانگین ریسک روزانه در هفت روز گذشته.

18
ماژول تحقیقات

این ماژول روند بررسی رویدادها را ساده کرده و مدت زمان واکنش به حوادث را کاهش می‌دهد. با ارائه نمای ۳۶۰ درجه از وظایف در حال انجام، وضعیت آن‌ها، مراحل تحقیق، افراد مسئول و مهلت‌ها، بار کاری تیم امنیت سایبری را کاهش می‌دهد. اعضای تیم می‌توانند در طول بررسی نظر بدهند، همکاری کنند، مستندات پیوست کنند و رویدادها را به‌عنوان شواهد ضمیمه نمایند.

NEW!

19
شکستن رمز عبور برای فایل‌های آرشیو شده رمزنگاری‌شده

Zecurion DLP امنیت داده را ارتقاء می‌دهد و امکان بررسی فایل‌های حساس را فراهم می‌سازد. با استفاده از واژه‌نامه داخلی قابل تنظیم، مسئول امنیت می‌تواند رشته‌های رمز عبور احتمالی را تعیین کند تا فرآیند رمزگشایی تقویت شود. هنگام شناسایی یک آرشیو رمزنگاری‌شده، سیستم به‌طور خودکار روش‌های رمزگشایی را در درگاه‌ها و نقاط پایانی اعمال می‌کند. پس از رمزگشایی، تحلیل دقیق فایل انجام می‌شود تا از نشت داده جلوگیری و رعایت قوانین حفظ شود.

NEW!

20
سیاست‌های تقویت‌شده آنلاین/آفلاین و واکنش‌های سیستمی

سیاست‌های به‌روزرسانی‌شده به عامل نقطه پایانی اجازه می‌دهد اتصال به شبکه سازمان را تشخیص داده و بر اساس آن، مجموعه‌ای خاص از سیاست‌ها را اجرا کند. واکنش‌های جدید سیستم شامل اجرای اسکریپت پیوست‌شده یا اجرای یک برنامه مشخص، آغاز وظیفه‌ای جدید در ماژول IRP (برنامه واکنش به حادثه) و تنظیم سطوح دسترسی فایل‌ها برای رد دسترسی در ACL فایل می‌باشد.

ADVANCED FEATURES

کشف عکس‌برداری از صفحه‌نمایش

AI

این قابلیت نوآورانه مبتنی بر هوش مصنوعی، نحوه برخورد با امنیت را متحول کرده و کاربرانی را شناسایی می‌کند که پیش‌تر قابل‌ردیابی نبودند. هرگاه فردی تلاش کند از صفحه‌نمایش با گوشی هوشمند عکس بگیرد، Zecurion DLPفوراً این اقدام را از طریق وب‌کم تشخیص داده و بلافاصله رایانه را غیرفعال می‌کند. این فناوری پیشرفته با استفاده از دو شبکه عصبی، شناسایی قابل اطمینانی از گوشی هوشمند ارائه می‌دهد و در مدت زمان بسیار کوتاه (تا ۰٫۰۶ ثانیه) حادثه امنیتی را گزارش می‌کند.

واترمارک صفحه‌نمایش

مسئولین امنیت می‌توانند واترمارک‌هایی شامل نام کاربر، اطلاعات رایانه و تاریخ را روی برنامه‌های خاص) مانندMS Office ، CRMو (...اعمال کنند. این واترمارک‌ها به‌طور واضح برای کاربران قابل مشاهده هستند و ممکن است آن‌ها را از گرفتن اسکرین‌شات یا عکس از فایل‌های حساس منصرف کند.

گزارش شبیه به چت

این گزارش یکپارچه تحلیل ارتباطات بین دو کاربر را با گردآوری تمامی پیام‌ها از پلتفرم‌های مختلف پیام‌رسانی (مانند واتساپ، تلگرام و...) در یک رابط شبیه به برنامه‌های پیام‌رسان محبوب، ساده می‌سازد. این رابط امکان مشاهده تمام پیام‌های ثبت‌شده، دسترسی به فایل‌ها، و گوش دادن به پیام‌های صوتی و تماس‌ها را از یک مکان مرکزی فراهم می‌کند.

ضبط میکروفون و وب‌کم

NEW!

با فعال‌سازی قابلیت ضبط از میکروفون یا وب‌کم هر رایانه در هر زمان، می‌توان هر رایانه‌ای را به یک سیستم نظارتی تبدیل کرد. هنگامی‌که کاربر بین برنامه‌های فعال دسکتاپ جابه‌جا می‌شود، می‌توان اسکرین‌شات یا تصویر وب‌کم تولید کرد.

اتصال زنده به دسکتاپ و وب‌کم

اتصال بلادرنگ به رایانه کارمند جهت ارزیابی فوری فعالیت‌های او. امکان مشاهده هم‌زمان تصویر زنده از طریق وب‌کم برای درک بهتر شرایط فراهم است.

جلوگیری از اسکرین‌شات

در صورت نیاز، مسئول امنیت می‌تواند قابلیت گرفتن اسکرین‌شات را برای کاربر غیرفعال کند.

ثبت اسکرین‌شات و کلیدهای فشرده‌شده

امکان پایش تمام کلیدهای فشرده‌شده توسط کاربران یا گروه‌های مشخص و گرفتن اسکرین‌شات در بازه‌های زمانی تعیین‌شده از هر رایانه. این ویژگی به اجرای سیاست‌های امنیت داخلی و مدیریت داده‌ها کمک کرده و از نشت احتمالی اطلاعات جلوگیری می‌کند.

کنترل برنامه‌ها، نرم‌افزار و سخت‌افزار

NEW!

برای کاهش ریسک استفاده کاربران از برنامه‌های مضر) مانندTOR ، کلاینت‌های تورنت، ابزارهای ناشناس‌ساز و بازی‌ها(، می‌توان دسترسی به برنامه‌ها را مدیریت کرد. می‌توان فهرست سفید یا سیاه از برنامه‌ها برای کاربران یا گروه‌های خاص ایجاد کرد. همچنین قابلیت عامل DLP ارتقاء یافته و می‌تواند تغییرات در فهرست نرم‌افزارهای نصب‌شده و پیکربندی سخت‌افزار را شناسایی و پایش کند.

مخفی‌سازی عامل نقطه پایانی از کاربران

این راهکار می‌تواند عامل DLP را از دید کاربران درTask Manager ، برنامه‌ها و ویژگی‌ها، کنسول‌های خدمات سیستم و File Explorer مخفی نگه دارد تا هیچ اثری از آن برای کاربر قابل مشاهده نباشد.

COMPONENT OVERVIEW

Traffic Control	پایش ترافیک شبکه و مدیریت جریان داده‌ها در بیش از ۱۰۰ سرویس مختلف به منظور کاهش خطر نشت اطلاعات، چه به‌صورت عمدی و چه ناخواسته.
Device Control	رویکردی دقیق و سطح‌بندی‌شده برای محدودسازی دسترسی و حفاظت از داده‌ها فراهم می‌کند، در حالی‌که استفاده قانونی و مجاز از اطلاعات را تسهیل می‌نماید.
Discovery	اطلاعات حساس ذخیره‌شده به‌صورت نامناسب را در دیسک‌های محلی، پوشه‌های اشتراکی، Microsoft SharePoint، Microsoft Exchangeو هر پایگاه داده‌ای که از ODBCاستفاده می‌کند، شناسایی کرده و امکان اتخاذ اقدامات پیشگیرانه برای جلوگیری از نشت یا سرقت داده‌ها را فراهم می‌سازد.
Staff Control NEW!	راهکار مدیریت پیشرفته برای دورکاری، Staff Control، ساعات کاری را پایش می‌کند، فعالیت‌های کارکنان در محیط کار را ثبت می‌نماید و سطح بهره‌وری را ارزیابی می‌کند. گزارش فعالیت کاربران با جزئیات پیشرفته، در نسخه جدید در دسترس است.
User Behavior Analytics	این ماژول از ۱۵ شاخص استفاده می‌کند و از پروفایل‌سازی احساسی بهره می‌برد. تحلیل رفتار کاربران پارامترهای فعلی کارمندان را با مقادیر آماری میانگین آن‌ها مقایسه می‌کند، و انحراف‌های قابل‌توجه به‌عنوان شاخص‌های احتمالی تهدید در نظر گرفته می‌شوند.
Screen Photo Detector AI	این قابلیت نوآورانه مبتنی بر هوش مصنوعی، تحول بزرگی در حوزه امنیت ایجاد کرده است، چراکه فعالیت‌های پنهان پیشین کاربران داخلی را شناسایی و متوقف می‌کند. هنگامی‌که فردی تلاش می‌کند با استفاده از گوشی هوشمند از صفحه‌نمایش عکس بگیرد، Zecurion DLPبلافاصله از طریق وب‌کم این اقدام را تشخیص داده و سیستم را قفل می‌کند. این فناوری انقلابی با بهره‌گیری از دو شبکه عصبی، شناسایی دقیق گوشی‌های هوشمند را تضمین کرده و در کمتر از ۰.۰۶ ثانیه وقوع حادثه امنیتی را علامت‌گذاری می‌نماید.
Investigation Workflow Automation	این ماژول فرآیند تحقیقات را ساده کرده و چرخه واکنش به حوادث را کاهش می‌دهد. با ارائه یک نمای ۳۶۰ درجه جامع از وظایف در حال اجرا — شامل وضعیت‌ها، میزان پیشرفت تحقیقات، افراد مسئول و مهلت‌ها — حجم کاری تیم امنیت سایبری را به‌طور قابل‌توجهی کاهش می‌دهد. در جریان تحقیقات، اعضای تیم می‌توانند روی وظایف نظر ثبت کنند، پیشرفت‌ها را با همکاران در تمامی سطوح(از CISO تا تحلیل‌گران) به اشتراک بگذارند و اسناد و شواهد مربوط به حادثه را ضمیمه کنند.
Risk-based Assessment	دیدی جامع از فعالیت‌های کارکنان ارائه می‌دهد و آن‌ها را بر اساس پارامترهای کلیدی از جمله ریسک، بهره‌وری، تطابق با سیاست‌ها و وضعیت احساسی ارزیابی می‌کند. هر پروفایل کارمند، تمام رویدادهای مرتبط را در یک صفحه واحد و به‌صورت ترتیب زمانی نمایش می‌دهد؛ هر رویداد نیز قابل کلیک بوده و اطلاعات جزئی را در اختیار قرار می‌دهد. افسر امنیتی کارکنانی با ریسک بالا را با دقت بیشتری زیر نظر خواهد داشت، در حالی‌که افراد کم‌ریسک با محدودیت‌های کمتری مواجه خواهند بود.
Data Classification AI	Zecurion از تکنیک‌های پیشرفته‌ای مانند اثر انگشت دیجیتال، تحلیل مبتنی بر واژه‌نامه، یادگیری ماشین و تطبیق الگوها برای شناسایی و مدیریت دقیق داده‌ها در سراسر چرخه عمر آن‌ها استفاده می‌کند. این فناوری‌ها، حفاظتی قدرتمند برای اطلاعات حساس فراهم می‌سازند؛ صرف‌نظر از قالب یا محل ذخیره‌سازی آن‌ها. علاوه بر این، فناوری تشخیص نوری نویسه (OCR) با استخراج جزئیات حساس از اسناد اسکن‌شده یا عکس‌برداری‌شده، دقت طبقه‌بندی داده‌ها را به‌طور چشمگیری افزایش می‌دهد.

طبقه‌بندی داده‌ها با هوش مصنوعی

راهکار Zecurion DLP از تکنیک‌های متنوعی برای شناسایی داده‌ها بهره می‌برد تا حفاظت کامل در برابر نشت اطلاعات فراهم شود. فرقی نمی‌کند که داده‌ها به‌صورت عمدی به سرقت رفته باشند، به خطر افتاده باشند یا ناخواسته به اشتراک گذاشته شده باشند؛ یکی از این روش‌های شناسایی می‌تواند موضوع را کشف کرده و هشدار دهد.

کلیدواژه‌ها و واژه‌نامه‌ها

این روش از مجموعه‌ای از رشته‌های متنی همراه باwildcard ها برای شناسایی موضوعات خاص استفاده می‌کند. این تکنیک امکان تطبیق دقیق کلمات را فراهم کرده و در عین حال، با استفاده از صرف(morphology) ، ریشه‌یابی و ترکیب کلمات، خطاهای مثبت کاذب را کاهش می‌دهد. همچنین کاربران می‌توانند علاوه بر ۳۰+ واژه‌نامه از پیش‌تعریف‌شده، واژه‌نامه‌های سفارشی خود را نیز ایجاد کنند.

الگوها و عبارات منظم

ابزاری قدرتمند برای جستجوی داده‌های ساختاریافته هستند که می‌توانند الگوهایی مانند شماره کارت اعتباری، شماره تأمین اجتماعی، شماره حساب IBAN، آدرس‌های URL و ایمیل را شناسایی کنند.

اثر انگشت دیجیتال

از طریق جمع‌آوری انواع خاصی از اسناد، امکان شناسایی نسخه‌های واقعی اسناد یا بخش‌هایی از آن‌ها را فراهم می‌کند. این اثرانگشت‌ها به‌صورت خودکار هنگام افزودن اسناد جدید به‌روزرسانی می‌شوند. الگوریتم‌های Shingles و روش بیزی برای ردیابی توالی واژگان و وزن‌دهی دسته‌بندی‌ها استفاده می‌شوند تا دقت شناسایی اسناد افزایش یافته و سرعت پردازش بهبود یابد.

اثر انگشت فرم‌های خالی

NEW!

این ویژگی به سیستم اجازه می‌دهد تا فرم‌های متنی پرشده را شناسایی کند. این قابلیت به سازمان‌ها کمک می‌کند تا اسناد حاوی اطلاعات حساس را حتی در صورتی که فرم اولیه خالی بوده باشد، بهتر شناسایی و مدیریت کنند.

اثر انگشت فایل‌های باینری با استفاده از الگوریتم SHA-256

NEW!

SHA-256 یک تابع هش رمزنگاری است که مقدار هش ۲۵۶ بیتی (۳۲ بایتی) تولید می‌کند و معمولاً به‌صورت عدد هگزادسیمال نمایش داده می‌شود. این الگوریتم به‌طور گسترده برای تأیید صحت و یکپارچگی داده‌ها استفاده می‌شود، چرا که برای هر ورودی منحصربه‌فرد، یک هش منحصربه‌فرد تولید می‌کند. حتی تغییر کوچکی در ورودی باعث تغییر کامل هش خواهد شد، که برگشت‌ناپذیر بودن و احتمال بسیار پایین تلاقی را تضمین می‌کند. این به‌روزرسانی، روشی قدرتمندتر برای شناسایی و طبقه‌بندی فایل‌های باینری فراهم می‌سازد و دقت محافظت از داده‌ها را افزایش می‌دهد.

ZECURION

یادگیری ماشین (Machine Learning)

یادگیری ماشین اسنادی را شناسایی می‌کند که از نظر کلیدواژه‌ها و شاخص‌های معنایی، شباهت زیادی به گروه اسناد ارسالی دارند.

الگوهای تصویری مبتنی بر هوش مصنوعی (AI-Based Image Templates)

این ویژگی قادر است امضاها، مهرها و اسناد ساختاریافته مانند گذرنامه یا گواهی‌نامه رانندگی را از طریق شناسایی الگوهای تصویری – نه فقط متن – تشخیص دهد. این قابلیت نیازمند تنظیم اولیه فایل‌های تحلیلی است تا سیستم بتواند در آینده، موارد مشابه مانند تصویر مهر شرکت (با هر رنگ یا زاویه‌ای) را به‌عنوان اطلاعات محرمانه شناسایی کند.

تشخیص نوری نویسه (OCR)

یک تکنیک ارزشمند برای شناسایی اطلاعات حساس یا محرمانه‌ای است که از طریق اسکن یا عکس‌برداری ذخیره شده‌اند تا از روش‌های دیگر شناسایی در امان بمانند Zecurion DLP. این قابلیت را با ادغام موتورهای قدرتمند شخص ثالث مانند ABBYY FineReader و Google Tesseract توسعه داده تا بتواند متن را از تصاویر استخراج و شناسایی کند.

ماشین بردار پشتیبان (SVM - Support Vector Machine)

این روش امکان ایجاد یک طبقه‌بند را فراهم می‌سازد که متون مرتبط با یک موضوع خاص را بر اساس تحلیل دو مجموعه سند شناسایی می‌کند: اسناد مرتبط با موضوع و اسنادی با زبان مشابه که مرتبط نیستند. هرچه تعداد اسناد در هر مجموعه بیشتر باشد، دقت طبقه‌بندی بالاتر خواهد رفت. در آزمایش‌های بعدی، زمانی که احتمال تطبیق برای اسناد مرتبط بیش از ۹۰٪ باشد، عملکرد سیستم قابل قبول تلقی می‌شود.

NEW!

شناسایی الحاق فایل‌های باینری (Binary File Concatenation Detection)

این قابلیت به شناسایی زمانی کمک می‌کند که چند فایل باینری در یک فایل بزرگ‌تر ادغام شده‌اند. این امر امکان ردیابی بهتر اطلاعات حساس پنهان‌شده یا ترکیب‌شده در فایل‌های دیگر را فراهم می‌سازد.

NEW!

شناسایی اتصالات پروتکل ریموت دسکتاپ (RDP Detection)

سیستم قادر است اتصال‌های RDP را شناسایی کند تا دسترسی‌ها بهتر مدیریت شده و جلسات ریموتی که ممکن است اطلاعات حساس را در معرض خطر قرار دهند، به‌طور کامل نظارت شوند. این موضوع امنیت کلی را ارتقاء می‌دهد.

NEW!

تحلیل محتوای کدهای QR (QR Content Analysis)

این ویژگی کدهای QR موجود در اسناد یا تصاویر را تحلیل می‌کند تا محتوای درون آن‌ها بررسی شود. از این طریق، سازمان‌ها می‌توانند خطرات احتمالی ناشی از کدهای QR را شناسایی کرده و از دسترسی غیرمجاز به داده‌ها جلوگیری کنند و در عین حال، با سیاست‌های امنیتی مطابقت داشته باشند.

ZECURION

شرکت رایان سامانه آرکا، توزیع کننده انحصاری Zecurion در ایران

درباره Zecurion

شرکت Zecurion در سال ۲۰۰۱ در مسکو تأسیس شد و از آن زمان تاکنون به یکی از مراجع جهانی در حوزه راهکارهای امنیت فناوری اطلاعات تبدیل شده است. این شرکت از منافع بیش از ۱۰۰۰۰ مشتری سازمانی در بیش از ۷۰ کشور در سراسر جهان محافظت می‌کند.

Zecurion به دلیل نوآوری‌های برجسته خود، از جمله فناوری‌های ثبت اختراع‌شده، شناخته‌شده است و محصولاتی پیشرفته ارائه می‌دهد؛ از جمله:

- سیستم پیشگیری از نشت داده نسل جدید
- نظارت و محافظت متمرکز بر داده‌ها
- درگاه امن وب

با دریافت تقدیر و جوایز از مراجع معتبر بین‌المللی مانند Gartner و IDC، Zecurion همواره در خط مقدم صنعت امنیت اطلاعات قرار داشته و راهکارهایی پیشرفته، با قابلیت استقرار سریع و تمرکز بر کاهش تهدیدات درون‌سازمانی ارائه می‌دهد .

شرکت رایان سامانه آرکا، بیش از 15 سال سابقه در ارائه، نصب، راه‌اندازی، استقرار و پشتیبانی محصولات DLP، یکی از شرکت‌های پیشرو در امر راهکارهای جلوگیری از نشت داده است.

تهران، خیابان شهید بهشتی ، خیابان پاکستان ، کوچه چهارم ، پلاک ۱۱ ، طبقه چهارم ، واحد ۷
تلفن: ۰۲۱-۹۱۳۰۰۴۷۶ | دورنگار: ۰۲۱-۸۸۸۰۴۹۶۱ | کدپستی : ۱۵۳۱۶۴۵۹۱۸
www.arka.ir info@arka.ir
رایان سامانه آرکا

شرکت رایان سامانه آرکا، توزیع کننده انحصاری Zecurion در ایران