Cyberno

smart security for smart people

تولید محصولات و ارائه خدمات در حوزه امنیت نرم‌افزار
مطابق با استانداردهای جهانی

021-91094330 | تهران، میدان رسالت، خیابان فرجام، خیابان شهید حسینعلی، پلاک ۹ | info@cyberno.ir

www.cyberno.ir

سایبرنو
Cyberno

معرفی سایبرنو

شرکت دانش بنیان مهندسی دنیای فناوری امن ویرا با نام تجاری سایبرنو شرکتی فعال در حوزه امنیت سایبری است که طیف گسترده ای از محصولات و خدمات را در بازار ارائه می دهد. دامنه محصولات سایبرنو، امنیت برنامه های تلفن همراه و سامانه های تحت وب، ابزارهای جرم یابی و شناسایی حملات پیشرفته پایدار (APT)، آزمایشگاه تحلیل خودکار بدافزار و دیگر ابزارهای حوزه امنیت نرم افزار را پوشش می دهد. تیم فنی سایبرنو از سال ۱۳۹۱ در آزمایشگاه مهندسی معکوس دانشگاه علم و صنعت ایران فعالیت های علمی خود را آغاز نمود. در سال ۱۳۹۹ با تکیه بر چندین سال سابقه و تجارب علمی متخصصین خود تصمیم به ثبت قانونی شرکت گرفته و تا به امروز محصولات و خدمات زیادی در حوزه امنیت نرم افزار به سازمان های خصوصی و دولتی ارائه داده است. سایبرنو تلاش داد با رویکردهای نوآورانه و پیشرفته فنی، بستری فراهم آورد تا نیازهای امروزه سایبری کشور را با ارائه راهکارهای Software as a service و Security as a Service برطرف سازد.

امنیت ایمیل

Mail Security Gateway

پویشگر چند موتوره سایبرنو

Cyberno MultiScanner

انتقال امن فایل سایبرنو

Cyberno SFT

کیوسک امن سایبرنو

Cyberno Secure Kiosk

درایو امن سایبرنو

Cyberno Secure Drive

آزمایشگاه امنیت تلفن همراه

Mobile Security Lab

فازر هوشمند سایبرنو

Cyberno Smart Fuzzer

جعبه شن سایبرنو

Cyberno SandBox

کیوسک امن سایبرنو

Cyberno Secure Kiosk

یکی از عواملی که یک سازمان مورد نفوذ قرار می‌گیرد ورود فایل‌های بدافزار یا آسیب‌پذیر به درون سازمان از طریق حافظه‌های فلش، لوح‌های فشرده یا هارد دیسک‌های اکسترنال می‌باشد. کیوسک امن سایبرنو دستگاهی است که در ورودی یا نقاط حساس سازمان شما همانند مراکز داده قرار می‌گیرد. این دستگاه در واقع به عنوان نگهبان امنیت دیجیتال سازمان شما عمل می‌کند.

چنانچه فردی قصد انتقال فایل به درون سازمان شما از طریق حافظه‌های فلش، هارد دیسک اکسترنال یا... را داشته باشد، باید آن را به کیوسک امن سایبرنو متصل نماید. کیوسک امن سایبرنو فایل‌ها را ابتدا با حداقل **۵ ضدویروس** مورد بررسی قرار می‌دهد، چنانچه حاوی بدافزار باشد، اجازه ورود نمی‌کند، در غیر این صورت بررسی می‌کند که آیا آسیب‌پذیر است یا خیر؟ به عنوان مثال نسخه‌های قدیمی نرم‌افزار Adobe Reader اجازه ورود ندارند. چنانچه آسیب‌پذیر نیز نباشد، بررسی می‌شود که آیا فایل حاوی قابلیت‌هایی هست که می‌تواند برای حمله مورد استفاده قرار گیرد؟ به عنوان مثال فایل‌های doc. که دارای ماکرو هستند، اجازه ورود ندارند. تنها در صورتی اجازه ورود این فایل‌ها داده می‌شود که ماکروهای آن حذف شود.

از جمله قابلیت‌های کیوسک امن سایبرنو عبارت است از

سازگار با استانداردهای امنیتی داخلی و خارجی

فرآیند انتقال امن فایل‌ها به درون سازمان یکی از مواردی است که در اکثریت چک‌لیست‌ها و استانداردهای امنیتی داخلی و خارجی مد نظر قرار گرفته است. بنابراین استفاده از کیوسک امن سایبرنو شما را با آخرین استانداردهای امنیتی سازگارتر می‌کند .

پشتیبانی از فایل‌سیستم‌های مختلف

کیوسک امن سایبرنو از فایل‌سیستم‌های APFS، HFS، NTFS، ext، FAT و... پشتیبانی می‌کند.

کیوسک امن سایبرنو

Cyberno Secure Kiosk

استفاده از ۳۰ ضدویروس برای بررسی محتوای فایل‌ها

فایـل‌های ورودی سازمان می‌توانند با حداقل **۵** و حداکثر **۳۰** ضدویروس مورد بررسی قرار گیرند. استفاده از این تعداد ضدویروس برای بررسی فایل‌ها عملا امکان ورود بدافزار به درون سازمان را به زیر **1%** کاهش می‌دهد.

قابلیت بررسی فایل‌های خروجی از سازمان

کیوسک امن سایبرنو می‌تواند از خروج فایل‌های حساس از سازمان شما نیز جلوگیری کند. به این صورت که تنها فایل‌های تاییدشده توسط مدیر شبکه اجازه خروج از سازمان و قرار گرفتن در حافظه جانبی شخصی کاربر را دارد.

امکان شناسایی آسیب‌پذیری‌های نرم‌افزار مبتنی بر پایگاه داده CVE

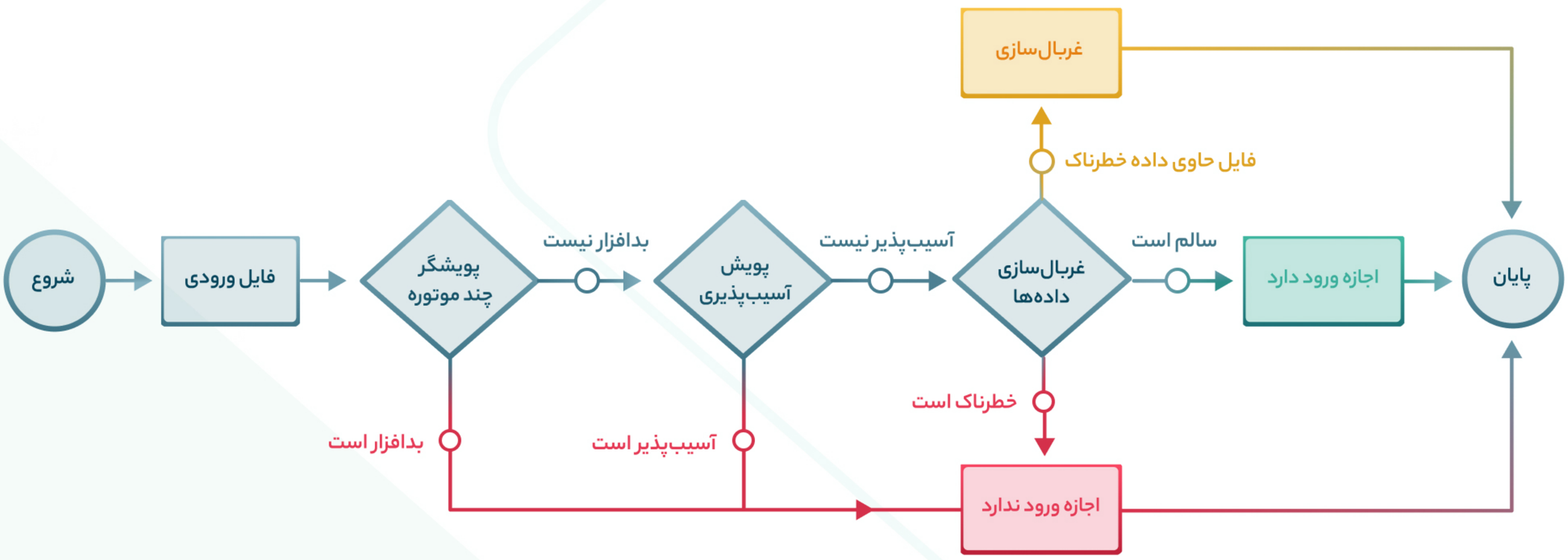
فایل‌های ورودی سازمان در پایگاه داده CVE جستجو می‌شوند. چنانچه فایل‌های ورودی آسیب‌پذیری سطح بالایی داشته باشند، آنگاه اجازه ورود به درون سازمان را ندارند.

پشتیبانی از انواع مختلف تجهیزات ذخیره‌سازی اطلاعات

کیوسک امن سایبرنو امکان پشتیبانی از حافظه‌های فلش، هارد دیسک اکسترنال، MicroSD، SD-Card، فلاپی، CD و DVD را دارد.

پشتیبانی از درایوهای رمزشده با BitLocker

کیوسک امن سایبرنو امکان بررسی فایل‌های موجود در درایوهای رمزشده با BitLocker را نیز دارد.



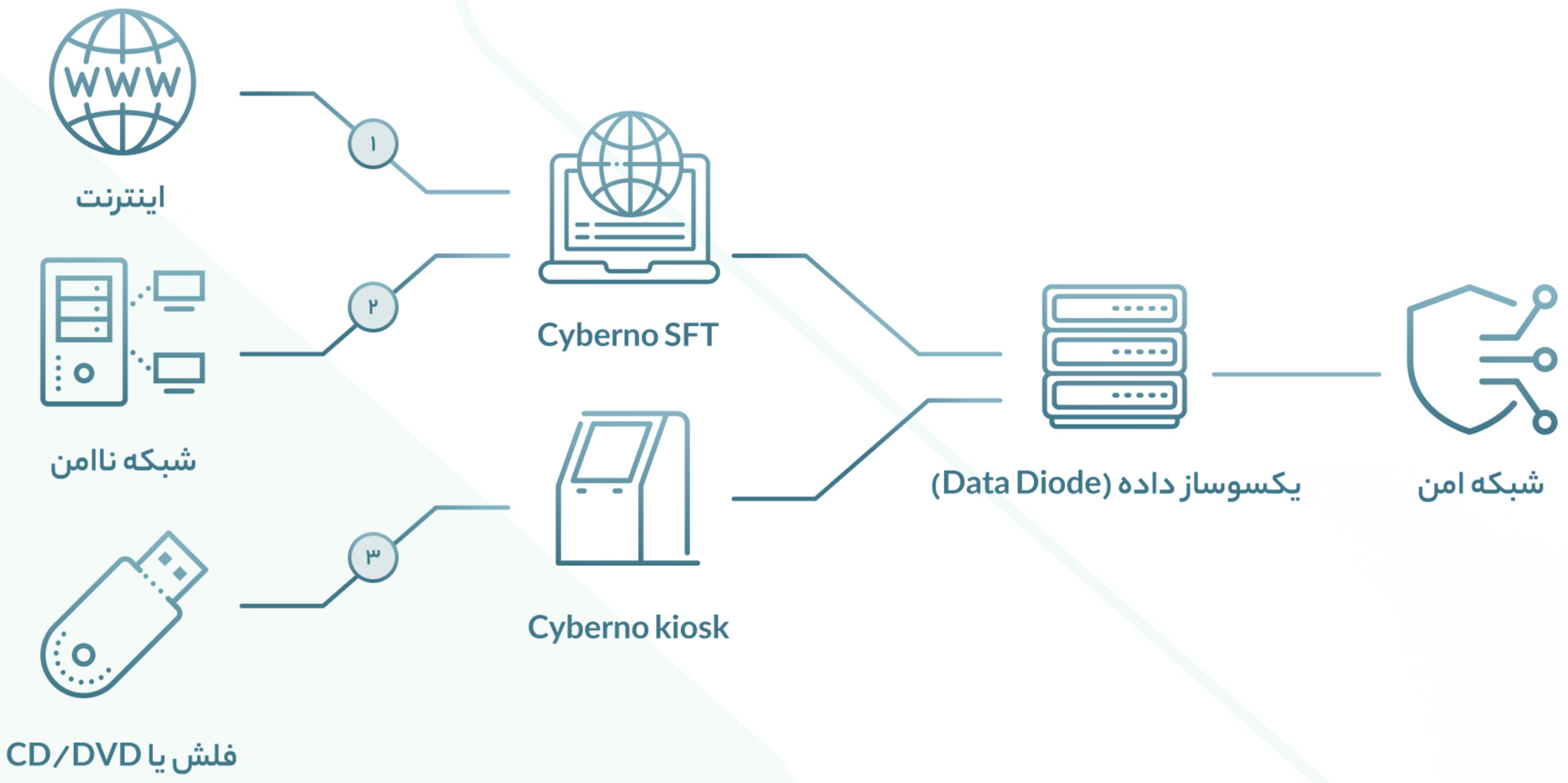
انتقال امن فایل سایبرنو

Cyberno SFT

امروزه اکثریت سازمان‌ها جهت جلوگیری از آلودگی و نفوذ به شبکه داخلی اقدام به جداسازی آن از شبکه اینترنت کرده‌اند. به عبارتی شبکه‌های داخلی اکثریت سازمان‌ها امروزه نوعی Airgap-Network هستند. با این حال ورود فایل از اینترنت یا شبکه ناامن به درون شبکه Airgap ممکن است باعث نفوذ یا آلوده شدن آن به بدافزار گردد. با توجه به این موضوع ورود فایل به شبکه‌های داخلی سازمان‌ها همواره یکی از چالش‌های مدیران IT بوده است.

سامانه انتقال امن فایل سایبرنو (Cyberno Secure File Transfer) یا به طور خلاصه Cyberno SFT راهکاری است که می‌تواند این چالش مدیران IT را حل کند. با استفاده از این سامانه به محض اینکه هر فایلی بخواهد وارد شبکه امن شما گردد، مورد بررسی امنیتی از لحاظ وجود بدافزار یا آسیب‌پذیری قرار می‌گیرد. با استفاده از این سامانه و ترکیب آن با سامانه کیوسک امن سایبرنو می‌توانید نظارت دقیقی برای کلیه فایل‌های ورودی و خروجی از شبکه سازمان خود داشته باشید.

از مهم‌ترین قابلیت‌های انتقال امن فایل می‌توان به موارد زیر اشاره کرد



انتقال امن فایل سایبرنو

Cyberno SFT

فیلتر کردن فایل‌ها بر حسب فرمت

شما می‌توانید مشخص کنید چه فایل‌هایی با چه فرمت‌هایی اجازه ورود به سازمان دارند.

غربال‌سازی فایل‌ها

محتوای خطرناک برخی فایل‌ها همانند ماکروهای فایل PPTX، DOCX، کدهای جاوا اسکریپت در فایل‌های PDF و... قبل از ورود به درون شبکه داخلی حذف خواهند شد.

پویشگر چندموتوره

فایل‌های شما با استفاده از چندین موتور ضدویروس (بین 5 تا 35 موتور) مورد بررسی قرار خواهند گرفت تا احیانا حاوی بدافزار نباشند.

شناسایی حملات Zero-Day

سامانه با استفاده از یک راهکار مبتنی بر Multi-Layer Sandbox و همچنین نگهداری فایل‌ها در فضای موقت به مدت مشخص می‌تواند اقدام به شناسایی حملات Zero-Day نماید.

پنل کاربری تحت وب

کاربران و افرادی که می‌خواهند به سازمان شما فایل ارسال کنند، می‌توانند این کار را از طریق یک سامانه تحت وب انجام دهند، بنابراین نیاز به نصب هیچگونه نرم‌افزاری ندارند.

سازگاری با انواع مختلف دیتا دیود

امکان تجمیع سامانه با دیتا دیود وجود دارد. بنابراین تنها فایل‌های امن امکان عبور از دیتا دیود و ورود به شبکه داخلی را خواهند داشت.

نظارت و لاگ‌گیری از کلیه فایل‌های ورودی/خروجی

مدیران IT سازمان می‌توانند نظارت دقیقی بر ورود/خروج فایل بر سازمان داشته و کلیه رفتارها لاگ‌گیری می‌گردد. همچنین امکان ارسال لاگ‌ها به انواع مختلف سامانه‌های SIEM وجود دارد.

سایبرنو
Cyberno

پویشگر چند موتوره سایبرنو

Cyberno MultiScanner

همانطور که می‌دانید امروزه بدافزار به یکی از اصلی‌ترین دلایل نشت اطلاعات سازمان‌ها تبدیل شده است. بدافزارهای امروزی ابزارهایی بسیار پیچیده هستند. توسعه‌دهندگان بدافزارهای APT قبل از انتشار تلاش می‌کنند که ساختار ضدویروس‌ها را شناسایی کرده و بدافزار را به‌گونه‌ای توسعه دهند که توسط آن‌ها قابل شناسایی نباشد. با توجه به این موضوع ضدویروس‌های امروزی نمی‌توانند نرخ شناسایی ۱۰۰% داشته باشند و تمام بدافزارهای موجود را شناسایی کنند. برای افزایش کارایی ضدویروس‌ها می‌توان توان چندین ضدویروس را با هم ترکیب کرد تا بیشترین نرخ شناسایی ممکن را داشته باشیم.

پویشگر چند موتوره سایبرنو سامانه‌ای است که بیش از **۳۰ ضدویروس** و ابزار شناسایی بدافزار همانند Yara را با هم ترکیب کرده و در قالب یک خدمت به شما ارائه می‌دهد.

از جمله قابلیت‌های این سامانه می‌توان به موارد زیر اشاره کرد

تحلیل کلیه داده‌های سازمان شما

پویشگر چندموتوره سایبرنو می‌تواند کلیه فعالیت‌های بدخواهانه در سازمان را شناسایی و مسدود نماید. کلیه فایل‌های عبوری از ترافیک داخلی شبکه شما، ترافیک وب، فایل‌های موجود در سرورها و دیسک‌های شما، فایل‌های موجود در پرتال‌های سازمانی و پست‌های الکترونیکی ارسالی و دریافتی همگی می‌توانند توسط پویشگر چندموتوره سایبرنو مورد بررسی و مسدودسازی قرار گیرند.

پویشگر چند موتوره سایبرنو

Cyberno MultiScanner

عدم وجود نقطه تکی شکست

اعتماد همیشگی به یک تولیدکننده ضدویروس به معنای وجود نقطه تکی شکست در سازمان شماست. چرا که کافیست بدافزار بتواند از قابلیت‌های محافظتی آن ضدویروس عبور کند، آنگاه تمام سازمان شما آلوده خواهد شد. با استفاده از پویشگر چند موتوره نقطه تکی شکست شناسایی بدافزار را در سازمان خود از بین ببرید.

قابلیت تجمیع با سایر ابزارهای امنیتی

این سامانه دارای رابط‌های GraphQL، REST API و ICAP می‌باشد. در نتیجه امکان ارتباط با سایر ابزارهای امنیتی به خصوص ابزارهای SIEM را دارا می‌باشد.

قابلیت تجمیع اطلاعات تحلیلگران بدافزار

این سامانه دارای یک نسخه تحت وب می‌باشد که از طریق آن تحلیلگران بدافزار سازمان می‌توانند داده‌های خود را با یکدیگر به اشتراک بگذارند. به عنوان مثال می‌توانند تحلیل‌های خود را راجع به یک فایل در سامانه قرار دهند یا اینکه نظر نهایی خود (بدافزار یا سالم بودن فایل) را در سامانه ثبت کنند.

تحلیل پویا بدافزارها

این سامانه برعکس سامانه‌های پویشگر چندموتوره موجود امکان تحلیل پویا بدافزارها توسط ابزارهای ضدویروس را نیز دارد. به عبارتی فایل مشکوک در یک محیط امن اجرا شده و عملکرد ضدویروس بعد از چند دقیقه اجرا در محیط مورد بررسی قرار می‌گیرد. چنانچه ضدویروس عملکرد بدخواهانه‌ای در هنگام اجرا کشف نماید، فایل به عنوان بدافزار شناسایی می‌شود.

TREND MICRO · 360 TOTAL SECURITY · avast · AVG Anti-Virus · McAfee · EMSISOFT ANTI-MALWARE · F-Secure · HAURI · Bitdefender · panda · AVIRA · COMODO SSL CERTIFICATE · eset · ClamAV · Microsoft · Arcabit · Filseclab · AhnLab · VirusBlokAda · GDATA · Symantec Endpoint Protection · VIPRE · F-PROT ANTIVIRUS · nProtect The Global Security Solution · Dr.WEB® · SOPHOS Security made simple. · RISING LION-STRONG SECURITY · NANO antivirus · KASPERSKY lab · XVIRUS · K7 SECURITY

سایبرنو
Cyberno

امنیت ایمیل

Mail Security Gateway

حمله به ایمیل‌های سازمانی (BEC)، یکی از رایج‌ترین روش‌های هکرها برای هک کردن سازمان‌ها است. اگرچه می‌توان با تنظیمات درست ایمیل سرور و کلاینت‌های ایمیل مانند Microsoft Outlook، جلوی بسیاری از تهدیدات ابتدایی را گرفت، اما برای مقابله با تهدیدات پیشرفته و نوین که روز به روز به پیچیدگی آن‌ها اضافه می‌شود، به لایه امنیتی دیگری مانند راهکار امنیت ایمیل سایبرنو نیاز دارید.

استقرار این سامانه روی ایمیل سرورهای سازمان شما به این معنی است که هر ایمیل، پیش از ورود به صندوق ورودی (inbox) کارکنان شما، با تعداد زیادی موتور آنتی ویروس پویش می‌شود. در صورت شناسایی فایل‌های بدافزاری، لینک‌های فیشینگ، لینک‌هایی به دامنه‌هایی با اعتبار پایین و دیگر موارد مشکوک در ایمیل دریافتی، پویشگر چندموتوره سایبرنو از ورود ایمیل به صندوق ورودی (inbox) ایمیل سازمانی کارکنان سازمان شما، جلوگیری می‌کند.

از مهم‌ترین قابلیت‌های راهکار امنیت ایمیل سایبرنو می‌توان به موارد زیر اشاره کرد

- مجهز بودن به فناوری Multi-AV و نرخ تشخیص بالای ۹۸ درصد!
- انجام تحلیل‌های ایستا و پویا روی فایل‌های ضمیمه در جعبه‌شن (sandbox)
- برخورداری از فناوری خلع‌سلاح و بازسازی عمیق محتوا (Deep CDR)
- بررسی لینک‌های موجود در ایمیل‌ها برای مقابله با حملات فیشینگ (phishing)
- شناسایی و مسدودسازی ایمیل‌های spam (هرزنامه) با نرخ تشخیص حدود ۹۹ درصد!
- قابلیت حذف ضمیمه‌های مشکوک بر حسب فرمت فایل

امنیت ایمیل

Mail Security Gateway

اسکن ایمیل‌های ورودی با پویشگر چندموتوره سایبرنو

راهکار امنیت ایمیل سایبرنو با Multi-AV بومی پویشگر چندموتوره می‌تواند هر ایمیل دریافتی را با بیش از ۳۰ موتور آنتی ویروس و در زمانی بسیار کوتاه اسکن کند.

تحلیل فایل‌های ضمیمه در جعبه‌شن (sandbox)

سامانه جعبه شن راهکار امنیت ایمیل سایبرنو می‌تواند فایل‌های اجرایی، مایکروسافت آفیس، PDF، پاورشل و... را در محیطی امن و ایزوله اجرا و بررسی کند و در نتیجه می‌تواند جلوی تهدیدات ایمیل پیشرفته را بگیرد.

فناوری خلع‌سلاح و بازسازی عمیق محتوا (Deep CDR)

این فناوری فایل‌ها را می‌شکند، بخش‌های مشکوک و خطرناک آن‌ها را حذف می‌کند و با سرهم کردن بخش‌های سالم و امن، فایلی سالم و بی‌خطر تحویل می‌دهد.

مقابله با حملات فیشینگ

راهکار امنیت ایمیل سایبرنو می‌تواند اعتبار دامنه لینک‌های موجود در ایمیل‌های دریافتی را بررسی و از یادگیری ماشین برای مقابله با حملات فیشینگ و BEC استفاده کند.

قابلیت لیست سیاه

مدیر سامانه می‌تواند لیستی از فرمت‌های غیر مجاز را تعریف کند تا ایمیل‌های دارای ضمیمه‌هایی با این فرمت‌ها فرصت ورود به inbox کاربر را پیدا نکنند.

سایبرنو
Cyberno

جعبه شن سایبرنو

Cyberno SandBox

طبق آمار منتشرشده توسط شرکت کسپرسکی در سال ۲۰۱۸ روزانه حدود ۳۲۰ هزار نمونه بدافزار جدید شناسایی می‌شود. مطمئنا این حجم از بدافزار به طور دستی قابل تحلیل نیست. بنابراین ابزارهای تحلیل خودکاری باید وجود داشته باشند که بتوانند گزارشی با جزئیات کامل از نمونه بدافزار به سرعت و بدون مداخله کاربر ایجاد نمایند. جعبه شن سایبرنو سامانه‌ای تحت وب است که می‌تواند برای تحلیل خودکار فایل‌های مشکوک سیستم عامل ویندوز مورد استفاده قرار گیرد.

از جمله مزایای جعبه شن سایبرنو عبارت است از

- قابلیت تحلیل انواع مختلف فایل PE
- رهگیری مبتنی بر قلاب‌اندازی در سطح هسته
- رهگیری مبتنی بر قلاب‌اندازی در سطح کاربر
- رهگیری درخواست‌های مرتبط با پردازش‌ها و نخ‌ها
- رهگیری درخواست‌های مرتبط با فایل
- رهگیری درخواست‌های مرتبط با رجیستری
- رهگیری درخواست‌های مرتبط با شبکه
- شناسایی روش‌های مرسوم ضداشکال‌زدایی
- قابلیت ثبت خطاهای ماشین مجازی
- امکان ارسال فایل از طریق رابط کاربری تحت وب و ویندوز
- امکان ارسال فایل از طریق API جهت استفاده در زبان‌های برنامه‌نویسی مختلف
- تهیه گزارش تحلیل در قالب‌های مختلفی همچون JSON، PDF و XML

جعبه شن سایبرنو

Cyberno SandBox

سرور جعبه شن سایبرنو

مسئول تحلیل، یادگیری ماشین
و شنود ترافیک شبکه

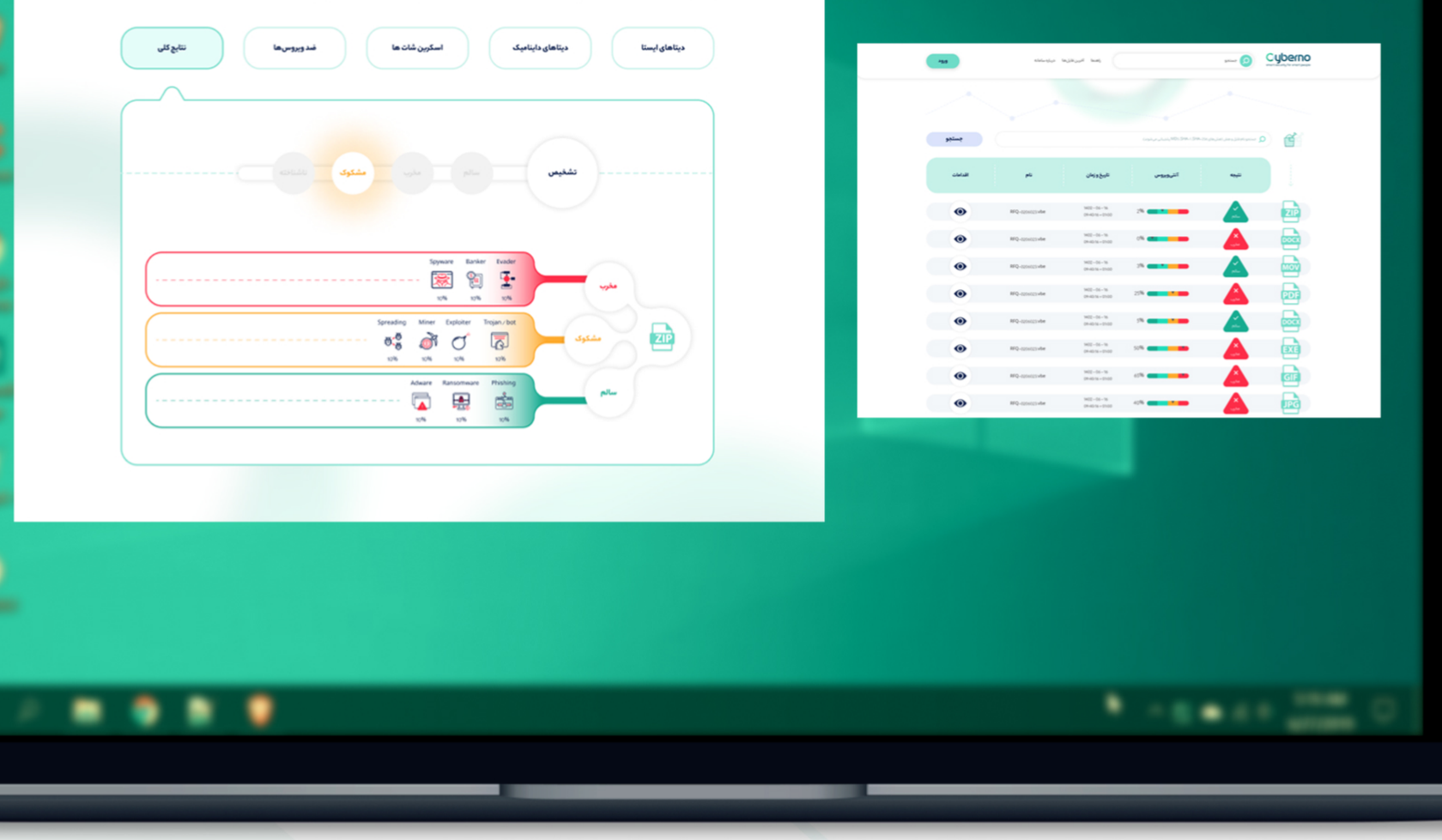
ماشین‌های تحلیل

ماشین‌هایی که بدافزار روی
آن‌ها اجرا می‌گردند

شبکه مجازی

شبکه‌ای ایزوله شده برای
اجرای تحلیل

اینترنت / شبکه داخلی



سایبرنو
Cyberno

فازر هوشمند سایبرنو

Cyberno Smart Fuzzer

همانطور که می‌دانید فازینگ (Fuzzing) فرآیندی است که در آن به یک نرم‌افزار ورودی‌های تصادفی داده شده تا ورودی‌هایی را پیدا کنیم که باعث ایجاد خطا در برنامه می‌شوند. با استفاده از این فرآیند می‌توان آسیب‌پذیری‌های موجود در برنامه را کشف کرد. به ابزارهایی که فرآیند فازینگ را انجام می‌دهند، فازر (Fuzzer) می‌گویند.

عملیات فازینگ یک روش جعبه سیاه می‌باشد، یعنی نیازی به کد منبع نرم‌افزار ندارد. البته از این روش برای کشف آسیب‌پذیری‌های برنامه‌های متن‌باز نیز استفاده می‌شود، چرا که کشف آسیب‌پذیری با استفاده از فازر بسیار سریع‌تر از بررسی دستی یا خودکار کدهای برنامه می‌باشد.

برخی از مزایای یک فازر عبارت است از

کشف آسیب‌پذیری بدون نیاز به صرف وقت یا تلاش زیاد

به محض اینکه فازر را اجرا کردید، دیگر نیاز نیست کار خاصی انجام دهید. یک فازر می‌تواند روزها یا حتی ماه‌ها بدون نیاز به دخالت شما به فعالیت خود ادامه دهد. به محض کشف آسیب‌پذیری فازر شما را با خبر می‌کند.

امکان کشف آسیب‌پذیری‌هایی که به طور دستی به سادگی قابل کشف نیستند.

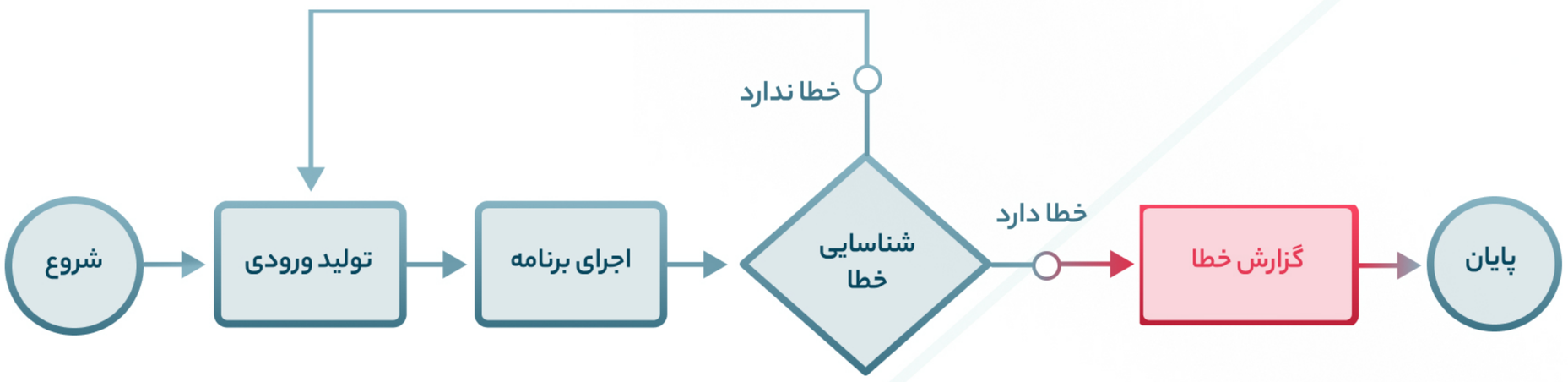
فازر هوشمند سایبرنو ابزاری است که امکان کشف خودکار آسیب‌پذیری را در برنامه‌های تحت وب و برنامه‌های سیستم عامل ویندوز فراهم می‌کند. این فازر برعکس فازرهای مرسوم ورودی تصادفی یا ورودی مبتنی بر فرمت فایل ایجاد نمی‌کند، بلکه با استفاده از ابزار Intel Pin و استفاده از الگوریتم‌های یادگیری ماشین سعی می‌کند میزان Coverage برنامه را در هر بار اجرا شناسایی نماید و در هر بار ورودی‌هایی به برنامه بدهد که بیشترین میزان Coverage را داشته باشند. به این ترتیب بدون نیاز به تعیین ورودی برنامه و با حداکثر سرعت امکان کشف آسیب‌پذیری‌های برنامه وجود دارد.

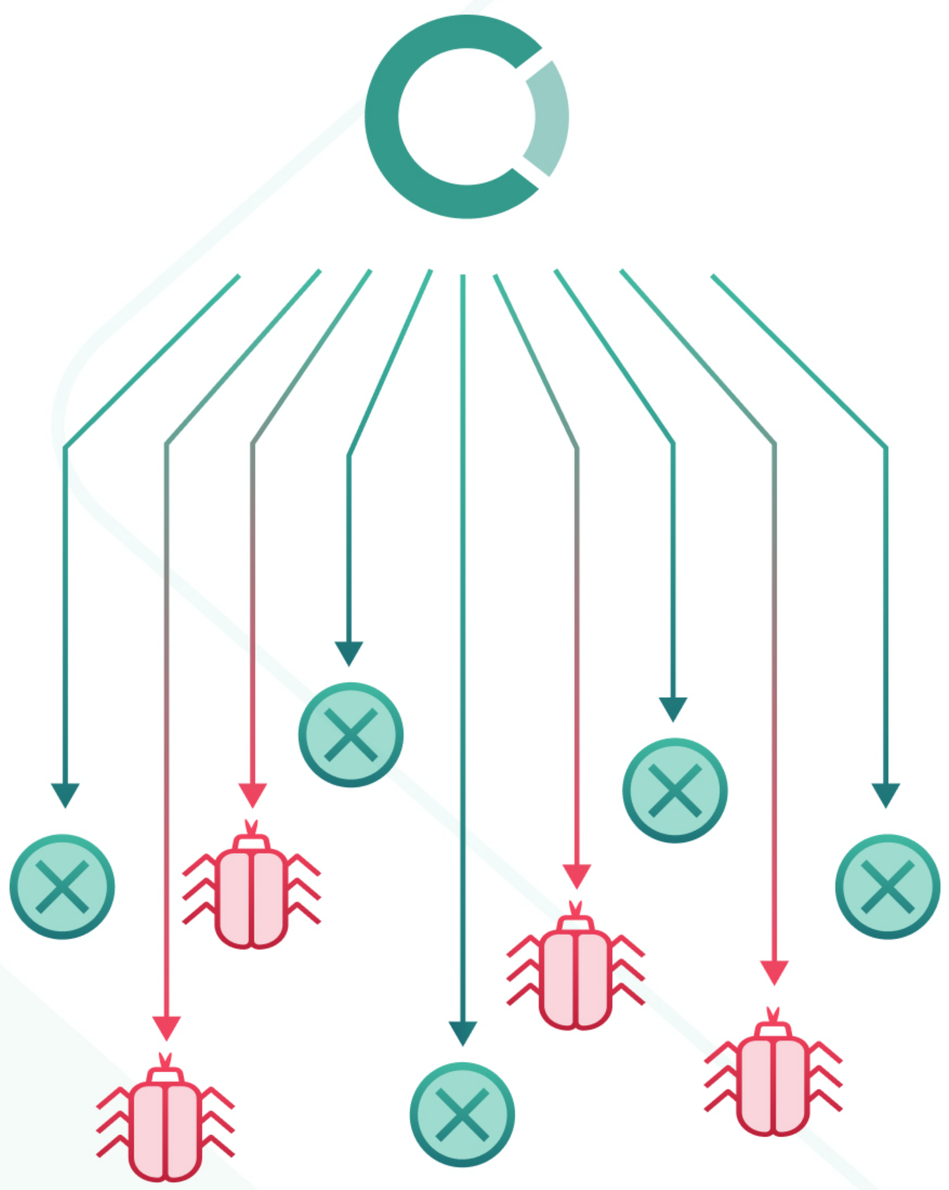
فازر هوشمند سایبرنو

Cyberno Smart Fuzzer

برخی از قابلیت‌های فازر هوشمند سایبرنو عبارت است از

- امکان شناسایی آسیب‌پذیری در برنامه‌های نوشته‌شده برای سیستم عامل ویندوز. (فایل‌هایی اجرایی EXE و DLL)
- امکان تحلیل درایورهای سطح هسته سیستم عامل ویندوز با ارسال IOCTL یا IRP.
- امکان فازینگ برنامه‌های تحت وب.
- قابلیت قرارگیری در چرخه CI/CD و ارتباط با ابزارهای GitLab CI/CD، Jenkins و...
- پشتیبانی از Rest-API برای تجمیع با سایر ابزارهای توسعه.
- قابلیت مقیاس‌پذیری و امکان ایجاد Fuzzing Farm.





سایبرنو
Cyberno

آزمایشگاه امنیت تلفن همراه

Mobile Security Lab

امروزه تلفن‌های همراه هوشمند به عنوان جزء جدانشدنی زندگی افراد پذیرفته شده است. با توسعه و فراگیر شدن استفاده از برنامه‌های Android و iOS و فراهم شدن بستری برای تراکنش‌های مالی و همچنین همه‌گیر شدن شبکه‌های اجتماعی که منجر به تبادل گسترده اطلاعات حساس و شخصی شده است، انجام آزمون‌های امنیتی و رفع نقاط ضعف برنامه شما برای حفظ امنیت اطلاعات و حفاظت از حریم خصوصی کاربرانتان به امری ضروری تبدیل شده است.

شرکت سایبرنو با ارائه‌ی سرویس بررسی امنیتی برنامه‌های تلفن همراه تلاش بر رفع نیاز توسعه‌دهندگان و همچنین دغدغه‌های کاربران عمومی تلفن همراه کرده است. نسخه رایگان این محصول (که از طریق وبسایت قابل استفاده است) می‌تواند حدود **۵۰** آسیب‌پذیری متداول در برنامه‌های تلفن همراه را شناسایی نماید. همچنین شما می‌توانید جهت تست نفوذ برنامه تلفن همراه خود مطابق با استاندارد MASVS با ما تماس حاصل فرمایید.

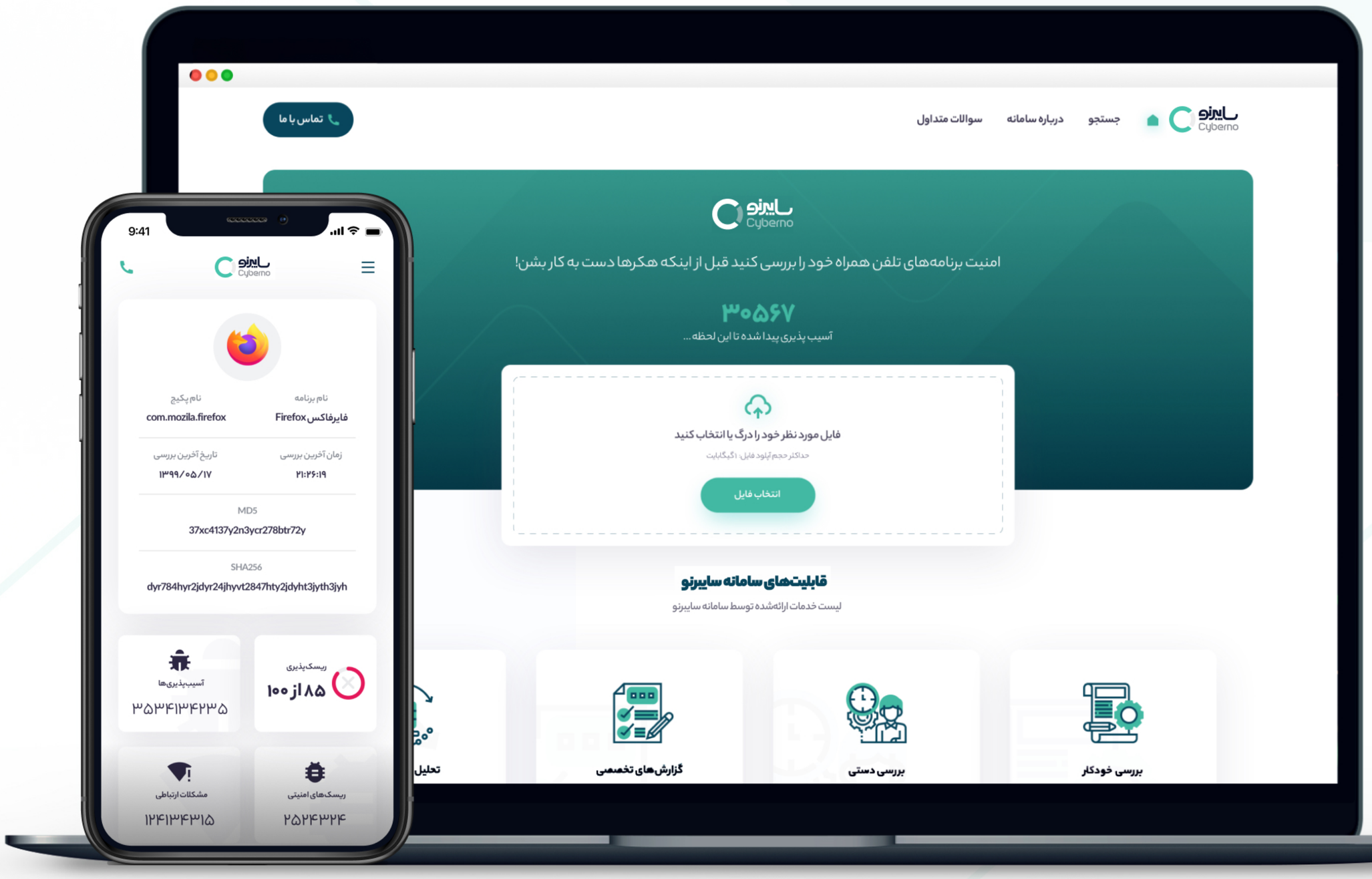
همچنین این سامانه دارای امکان تعیین بدافزار یا سالم بودن فایل اجرایی با استفاده از قابلیت‌های جعبه شن تعاملی و سامانه پویشگر چندموتوره نیز می‌باشد.

برخی از مواردی که در تست نفوذ برنامه تلفن همراه مورد بررسی قرار می‌گیرد، عبارت است از

- بررسی ایستا شامل دیکامپایل برنامه (Native، کراس پلتفرم) و بررسی کدها
- بررسی پویا شامل بررسی فعالیت‌های شبکه، لاگ‌ها و...
- بررسی معماری و مدل مجوزهای برنامه، حافظه داخلی، پایگاه‌داده‌ها، حافظه جانبی و...
- بررسی و تست نفوذ لینک‌های داخلی و APIها
- بررسی وجود آسیب‌پذیری‌های متداول مطابق با استاندارد MASVS

آزمایشگاه امنیت تلفن همراه

Mobile Security Lab



https://mobsl.cyberno.ir

- شناسایی آسیب‌پذیری‌های برنامه به صورت ایستا و پویا
- تحلیل پیکربندی
- پشتیبانی از زبان‌های برنامه‌نویسی و چارچوب‌های مختلف
- ارائه راهکار برای مشکلات امنیتی
- تولید خروجی PDF و HTML
- پشتیبانی از Restful API

سایبرنو
Cyberno

درایو امن سایبرنو

Cyberno Secure Drive

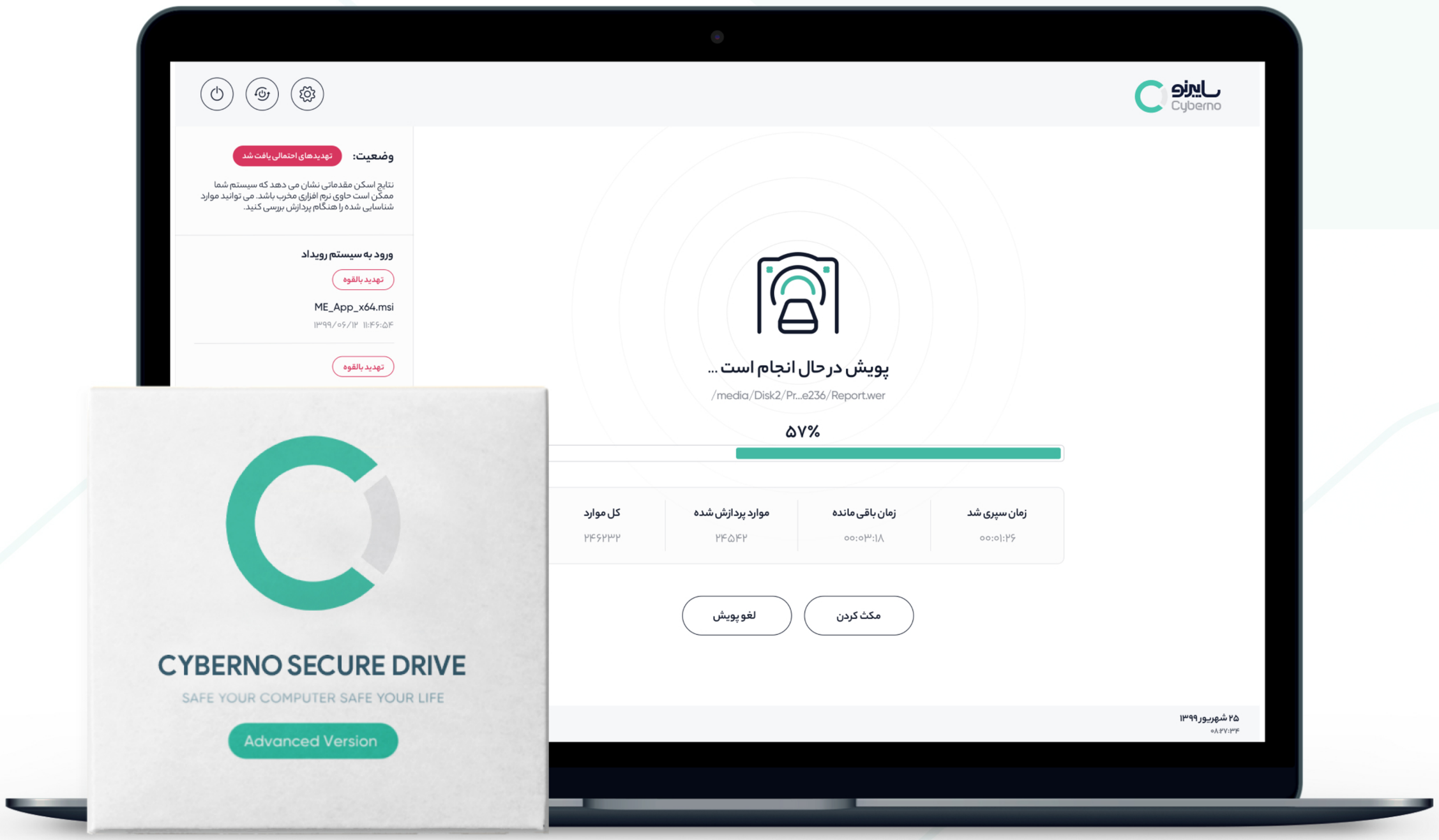
امروزه تقریبا هر دستگاه الکترونیکی همانند یک لپتاپ می‌تواند آلوده به بدافزار یا هدفی برای نفوذ باشد. درایو امن سایبرنو یک درایو USB است که می‌تواند قبل از ورود لپتاپ یا سایر تجهیزات ذخیره‌سازی اطلاعات به درون سازمان آنها را مورد بررسی قرار دهد تا حاوی بدافزار یا نرم‌افزار آسیب‌پذیر نباشند. همچنین این دستگاه می‌تواند به عنوان یک درایو نجات رایانه عمل کند. زمانی که رایانه شما آلوده به بدافزار شده باشد، ممکن است نتوانید سیستم عامل خود را اجرا نمایید، یا از ضدویروس موجود در سیستم عامل برای حذف بدافزار استفاده کنید. در این موارد رایانه را با این درایو امن بوت کرده و اقدام به حذف بدافزار و نرم‌افزارهای آسیب‌پذیر نمایید.

قابلیت‌های درایو امن سایبرنو

- قابلیت حمل
- استفاده از ۸ موتور ضدبدافزار
- استفاده در سازمان‌های حساس
- حفظ حریم خصوصی و سازگار با قوانین
- ضریب اطمینان بالا
- پشتیبانی از فایل سیستم‌های مختلف
- پشتیبانی از BitLocker
- پشتیبانی از امضاهای شخصی (در نسخه‌های حرفه‌ای)
- شناسایی آسیب‌پذیری (در نسخه‌های حرفه‌ای)

درایو امن سایبرنو

Cyberno Secure Drive



COMMUNITY

ESET

F-Secure

Dr.WEB®

PROFESSIONAL

McAfee

F-Secure

SOPHOS
Security made simple.

ESET

COMODO SSL CERTIFICATE

Dr.WEB®

ADVANCED

McAfee

F-Secure

SOPHOS
Security made simple.

ESET

COMODO

Dr.WEB®

F-PROT ANTIVIRUS

ClamAV

yara

NSRL

ULTIMATE

McAfee

F-Secure

SOPHOS
Security made simple.

ESET

COMODO SSL CERTIFICATE

Dr.WEB®

F-PROT ANTIVIRUS

ClamAV

yara

NSRL

vulnerability


Cyberno
smart security for smart people