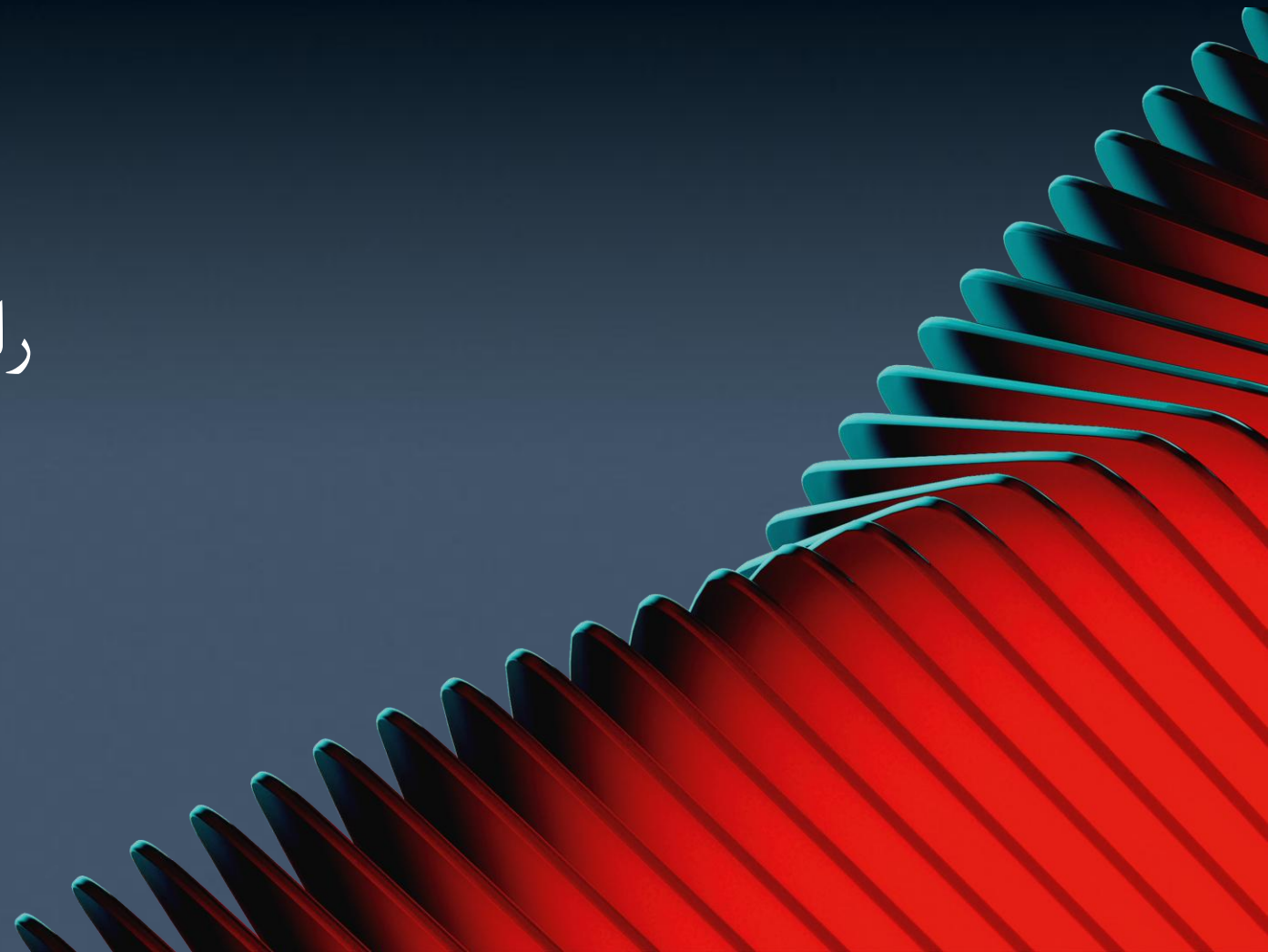
positive technologies

شرکت فناوری ارتباطات
آشیانه امن

AppSec

راهبرد پیرامون فرایندهای توسعه امن



درباره چه چیزهایی صحبت خواهیم کرد

- درباره ما
- AppSec چیست
- ارائه ما
- سناریوهای کاربردی
- خروجی نهایی برای شما
- چگونه می‌توانیم شروع کنیم

POSITIVE TECHNOLOGIES

حفاظت از جهان در برابر رویدادهای غیرقابل‌تحمل با
بهره‌گیری از جدیدترین فناوری‌ها

شرکت سهامی عام

MOEX:
POSI

22+
R&D در حوزه امنیت سایبری، سال‌ها

4k
مشتریان سازمانی در سراسر جهان

2.8k
محیط خلاقانه با حضور متخصصان و کارشناسان

2

تجربه و تخصص جهانی شرکت Positive Technologies تقریباً تمامی قاره‌ها و مناطق جهان را پوشش می‌دهد، از جمله خاورمیانه و شمال آفریقا، آمریکای لاتین، آسیای جنوب‌شرقی، هند، چین و آفریقا.

300+
شرکای پیشرو در حوزه یکپارچه‌سازی

1

Positive Technologies یکی از رهبران صنعت امنیت سایبری مبتنی بر نتیجه‌محوری و یکی از تأمین‌کنندگان بزرگ جهانی محصولات و راهکارهای امنیت اطلاعات است. **مأموریت ما** محافظت از کسب‌وکارها و صنایع مختلف در برابر تهدید حملات سایبری است.

حوزه‌های تحت حفاظت ما

positive technologies

شرکت فناوری ارتباطات
آشیانه امن

AppSec چیست

AppSec همواره نادیده گرفته می‌شد

AppSec در خط لوله توسعه به‌طور یکپارچه ادغام می‌شود

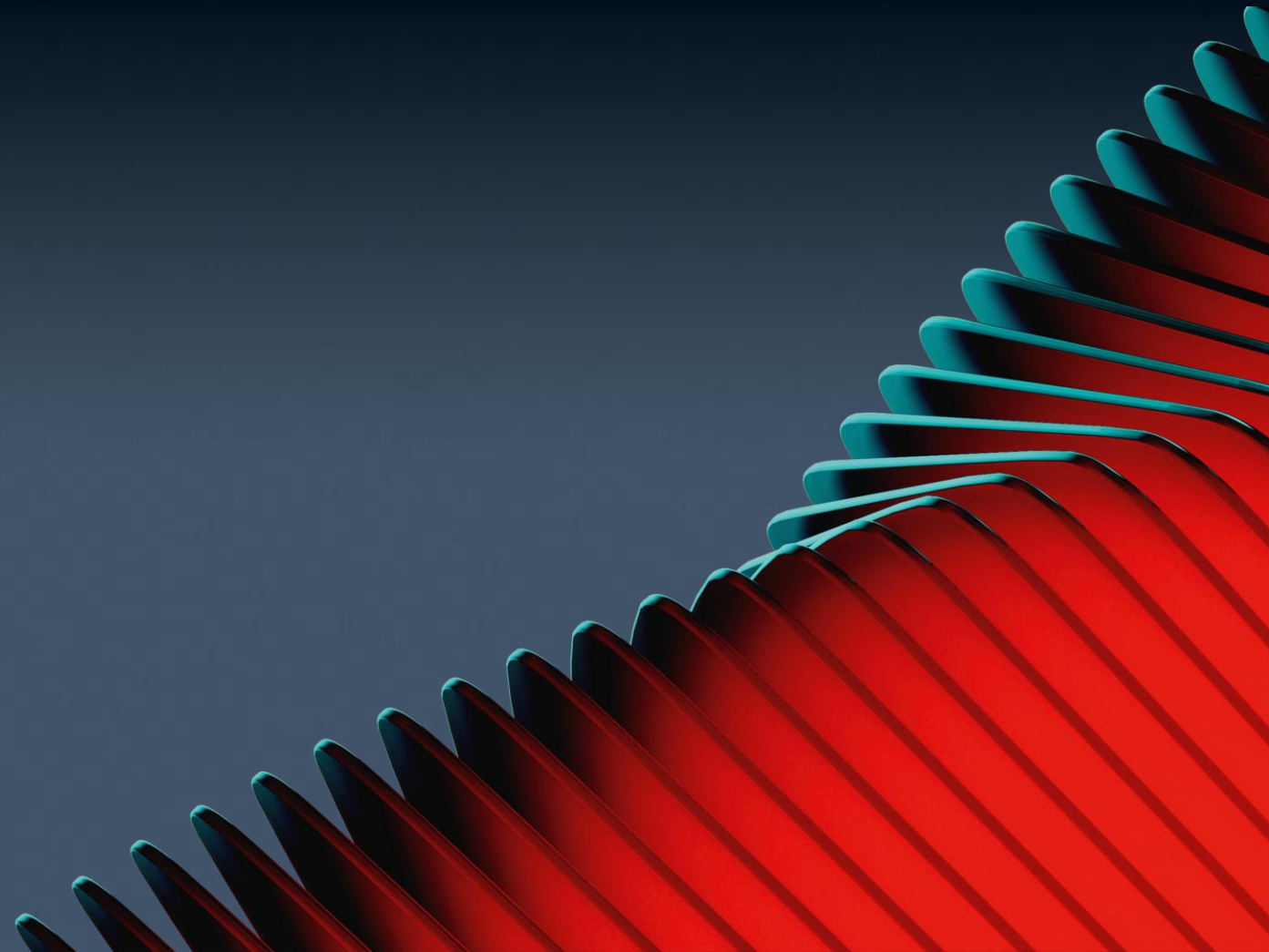
شیوه‌های AppSec در هر مرحله از چرخه عمر توسعه استفاده می‌شوند: برنامه‌ریزی، تحلیل، طراحی، توسعه، تست، پیاده‌سازی و بهره‌برداری

مجموعه‌ای از فرایندها و شیوه‌ها که برای کمک به توسعه نرم‌افزار امن استفاده می‌شوند

positive technologies

شرکت فناوری ارتباطات
آشیانه امن

ارائه ما



مجموعه‌ای کامل از محصولات و خدمات

برای تضمین توسعه امن نرم‌افزار طراحی شده‌اند

محصولات

PT Application Inspector SAST/SCA

PT Container Security

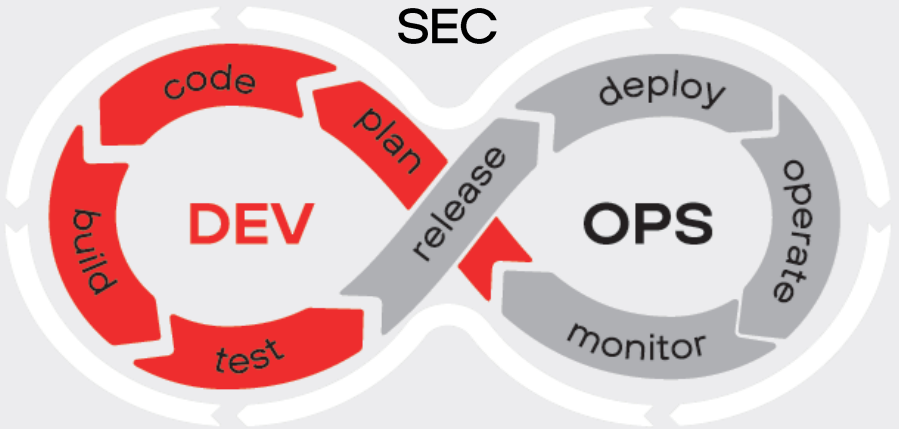
PT BlackBox DAST

PT Application Firewall PRO

PT MAZE

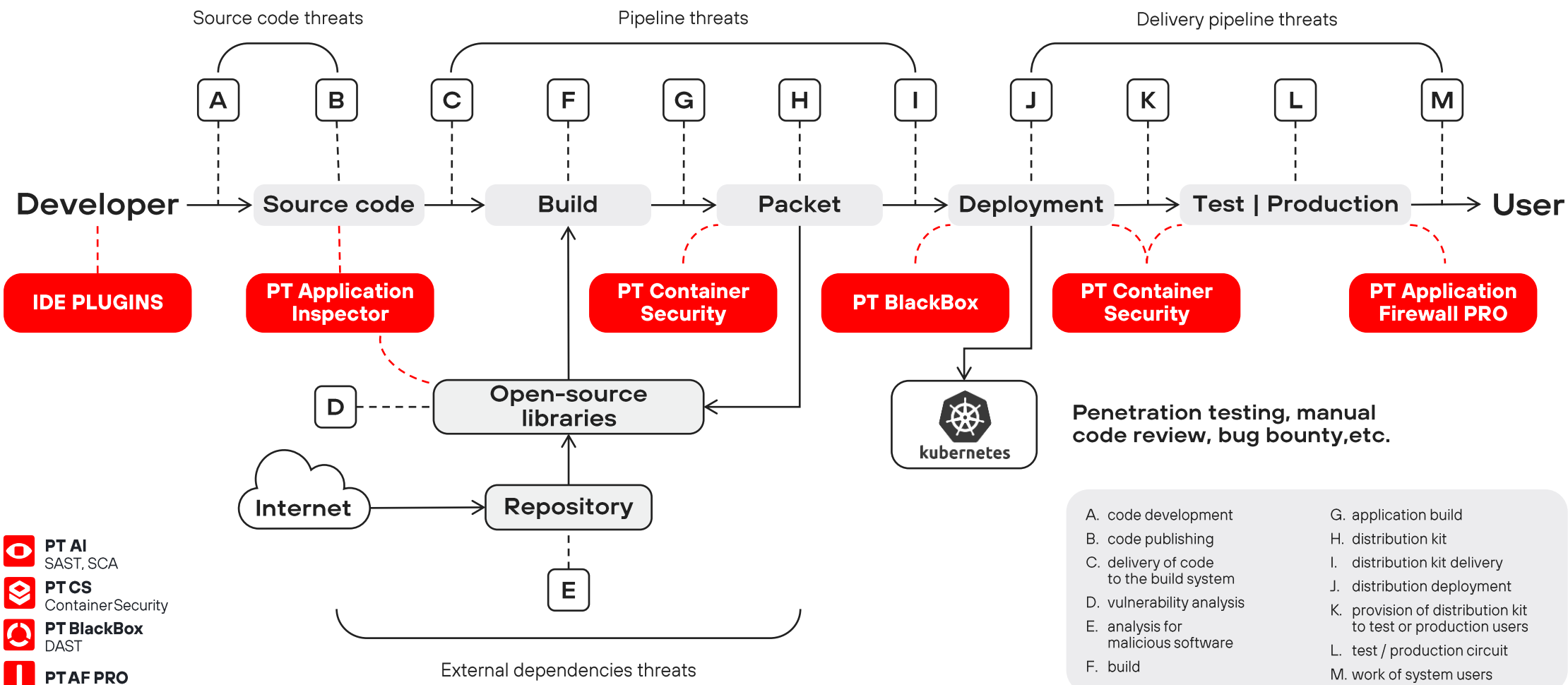
محافظت از برنامه‌های موبایل در برابر مهندسی معکوس

خدمات



- SSDLC assessment and automation review
- AppSec tool integration and automation within the CI/CD pipeline
- Reusable pipeline components
- AppSec operationalization

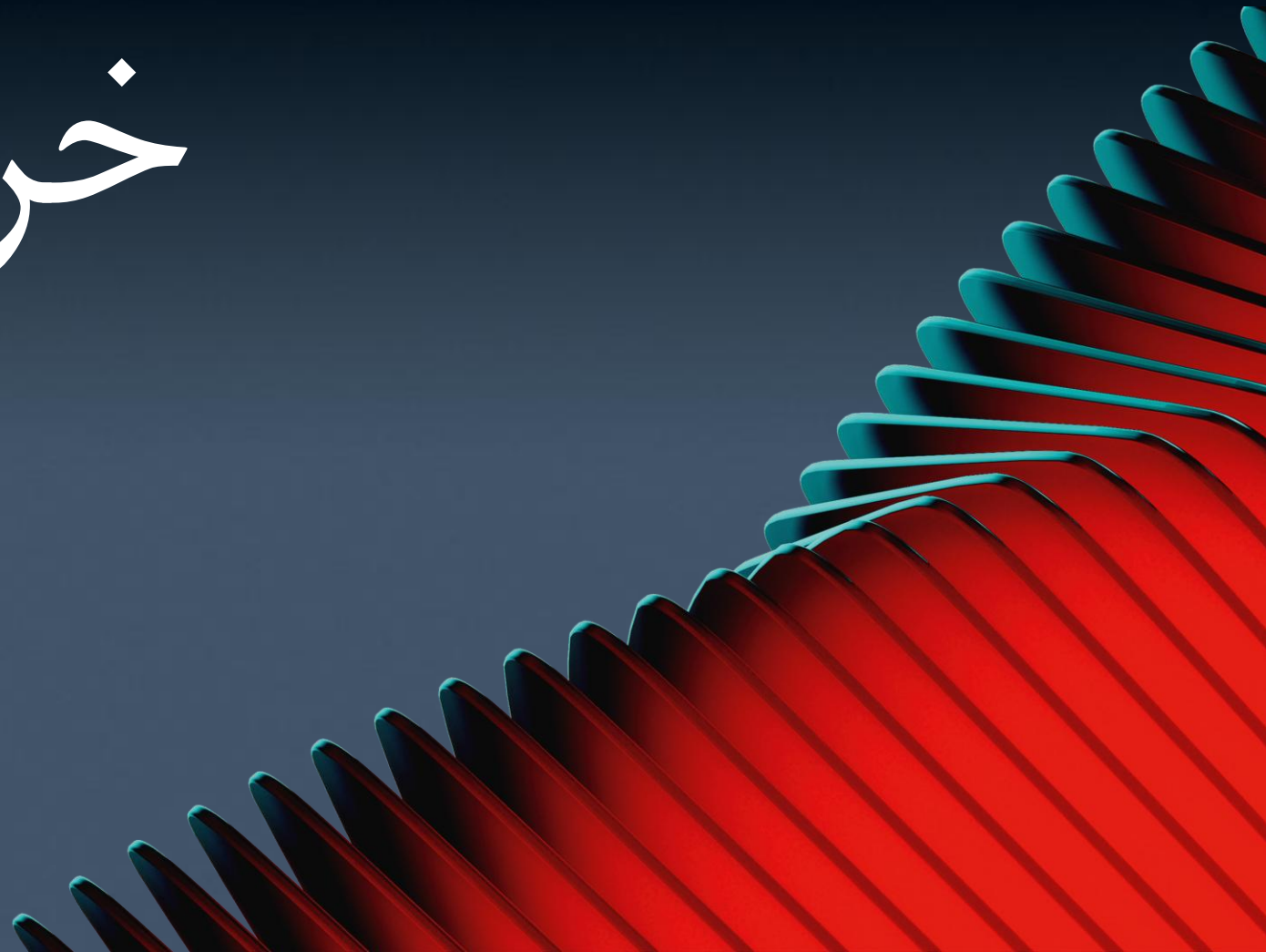
مجموعه محصولات



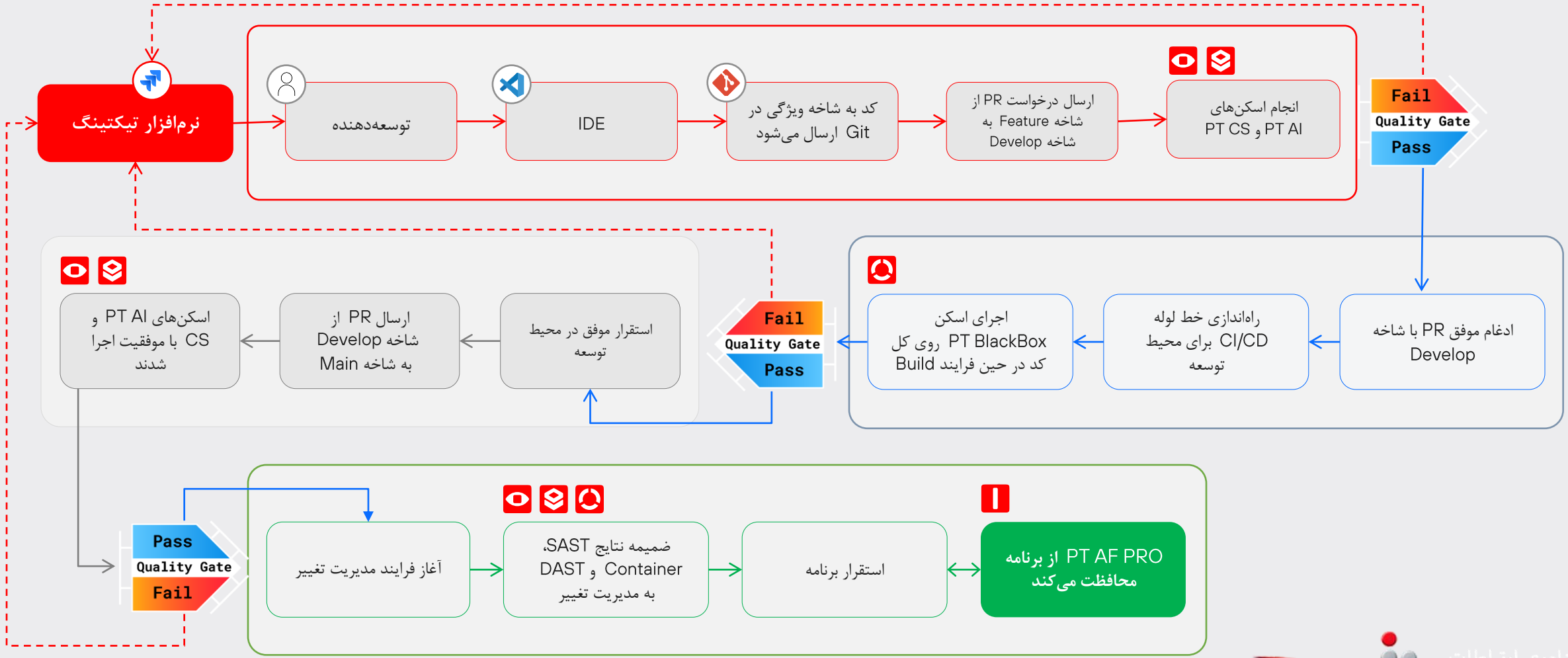
positive technologies

شرکت فناوری ارتباطات
آشیانه امن

خروجی نهایی برای شما



DEVSECOPS FRAMEWORK



برنامه موفق APPSEC

مدیریت آسیب‌پذیری‌ها

- عملیاتی کردن امنیت برنامه‌های کاربردی
- رفع و پاک‌سازی آسیب‌پذیری‌ها

Quality Gates

- اتوماسیون در تصمیم‌گیری‌های امنیتی
- پذیرش رویکرد امنیت محور Security First

تجربه توسعه‌دهنده

- افزایش کارایی توسعه‌دهندگان
- اگر امنیت مدیریت‌ناپذیر باشد، توسعه‌دهندگان آن را نادیده می‌گیرند

"Shift Left"

- انتقال مسئولیت به توسعه‌دهندگان
- ارزانترین زمان برای رفع آسیب‌پذیری‌ها

راهکارهای ما

برای پاسخگویی به نیازهای AppSec

- مجموعه‌ای از ابزارها برای پوشش کامل AppSec: SAST، SCA، DAST و امنیت کانتینر
- پلتفرم یکپارچه برای همبستگی، حذف تکراری و تحلیل هشدارها (به‌زودی)
- امکان مدیریت پیشگیرانه ریسک مطابق با روندهای AppSec

چشم‌انداز AppSec

افزایش تقاضا برای راهکارهای امنیتی خودکار و یکپارچه

- افزایش پیچیدگی برنامه‌ها و چشم‌انداز تهدیدات
- تقاضای بالای ابزارها با پوشش کامل: SAST، SCA، DAST و امنیت کانتینر
- پلتفرم‌های یکپارچه کارایی را افزایش می‌دهند: همبستگی و حذف تکراری هشدارها به‌صورت ساده‌سازی‌شده

روندهای فعلی در AppSec و یکپارچه‌سازی SDLC امن

- افزایش ادغام امنیت در سراسر SDLC شناسایی زودهنگام آسیب‌پذیری‌ها و کاهش ریسک و هزینه
- پذیرش DevSecOps برای تعبیه امنیت در فرایند توسعه
- روند رو به رشد شیوه‌های امنیتی پیشگیرانه و مداوم

ارزش ما

ساخت محصولات AppSec مستحکم بر اساس بالاترین استانداردها

تضمین نرخ خطای پایین در شناسایی آسیب‌پذیری‌ها

رشد و رهبری صنعت AppSec با تکیه بر تخصص و تجربه

چگونه می‌توانیم شروع کنیم

آماده ارائه مطالعات موردی در جلسه هستیم

با ما تماس بگیرید

1 ارزیابی

تحلیل وضعیت فعلی امنیت
توسعه برنامه‌های کاربردی

2 راهبرد

تدوین استراتژی برای فرایند
توسعه امن نرم‌افزار

3 پایلوت

جرای آزمایشی ابزارها و
راهکارهای اسکن برای توسعه
امن

positive technologies

شرکت فناوری ارتباطات
آشیانه امن

Protect your business from cyberattacks with a measurable and result-driven approach. The Olympic Games and FIFA World Cup already have.

global.ptsecurity.com
www.safenest.ir

چرا AppSec مهم است

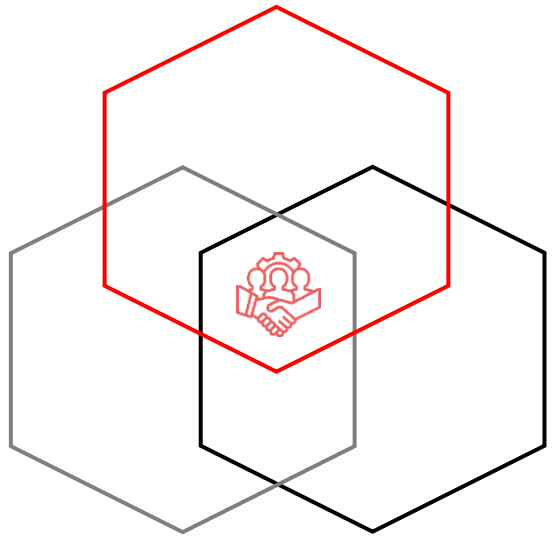
- کمک به توسعه‌دهندگان برای ارائه برنامه‌های امن
- تضمین وجود کنترل‌های امنیتی و حفظ سرعت عرضه به بازار
- علاوه بر ارتقای تخصص فنی داخلی، به ایجاد فرایندهای کارآمد نیز کمک می‌کند

افراد

با پشتیبانی هدفمند، نیازهای امنیتی خود را برطرف کرده و بدهی فنی را کاهش دهید.

فرایندها

تدوین استانداردها و سیاست‌های داخلی امنیت توسعه برنامه‌ها، مدیریت نقص‌ها و ارائه آموزش‌های امنیتی.



فناوری‌ها

شناسایی آسیب‌پذیری‌ها در تمام مراحل چرخه عمر توسعه نرم‌افزار و اطمینان از ادغام امنیت در کل فرایند.

و چگونه یک ابتکار مؤثر در حوزه امنیت برنامه‌های کاربردی ایجاد کنیم

APPLICATION
SECURITY

PT APPLICATION INSPECTOR

COMPREHENSIVE SAST/SCA SCANNER

نمای کلی محصول

راهکار جامع تست امنیت ایستا برنامه‌های کاربردی SAST و تحلیل ترکیب نرم‌افزار SCA است که تحلیل باکیفیت و ابزارهای کاربردی برای تأیید خودکار آسیب‌پذیری‌ها ارائه می‌دهد، روند کار با گزارش‌ها را به‌طور چشمگیر سرعت می‌بخشد و همکاری بین متخصصان امنیت و توسعه‌دهندگان را ساده می‌کند.

مزایا

1	**شناسایی زودهنگام**	PT AI در خطوط لوله CI/CD شما ادغام می‌شود و امکان اجرای اسکن‌های امنیتی در مراحل ابتدایی SSDLC را فراهم می‌کند.
2	**پوشش امنیتی جامع**	پشتیبانی از تست امنیت ایستا SAST و تحلیل ترکیب نرم‌افزارSCA برای محافظت از کدهای سفارشی و وابستگی‌های متن‌باز.
3	**Quality Gates متمرکز**	قابلیت‌های داخلی برای اعمال Quality Gates در سراسر سیستم‌های CI/CD، تضمین‌کننده اجرای یکنواخت سیاست‌های امنیتی.
4	**مقیاس‌پذیر و کاربرپسند**	فرایندهای خودکار و یکپارچه‌سازی، کارهای دستی را کاهش می‌دهند و پذیرش شیوه‌های امنیتی توسط توسعه‌دهندگان را آسان‌تر می‌کنند.

72%

از آسیب‌پذیری‌ها ناشی از خطاهای کدنویسی هستند

85%

از برنامه‌ها دارای آسیب‌پذیری‌هایی هستند که امکان حمله به کاربران را فراهم می‌کنند

99%

از برنامه‌های مالی ممکن است دارای آسیب‌پذیری‌های پرریسک باشند

APPLICATION
SECURITY

PT CONTAINER SECURITY

CONTAINER LIFECYCLE PROTECTION

نمای کلی محصول

PT Container Security حفاظت کامل از محیط‌های کانتینری را فراهم می‌کند. این ابزار Dockerfileها و Kubernetes Manifestها را برای یافتن پیکربندی‌های نادرست اسکن می‌کند، Images را برای آسیب‌پذیری‌ها تحلیل می‌کند و کلاسترهای در حال اجرا را به‌صورت Real-Time مانیتور می‌کند.این کار، یک چارچوب امنیتی یکپارچه برای کل چرخه عمر کانتینر، از Build تا Runtime ایجاد می‌کند.

مزایا

1	**پشتیبانی چندکلاستری**	مدیریت متمرکز چندین کلاستر Kubernetes — بدون توجه به موقعیت مکانی — زمان صرف شده توسط تیم‌های امنیتی را کاهش می‌دهد. این راهکار به‌راحتی قابل پیاده‌سازی است و امکان تنظیم مصرف منابع مطابق با حجم رویدادهای پردازش‌شده را فراهم می‌کند.
2	**پوشش کامل چرخه عمر برنامه**	امنیت در هر مرحله اعمال می‌شود — از تحلیل تصاویر ابزارهای اسمبلی کد تا مانیتورینگ فراخوان‌های API و رویدادهای رخداده در زمان اجرا
3	**موتور تشخیص ناهنجاری**	موتور اختصاصی و پرقدرت برای نظارت بر انطباق با سیاست‌ها و تشخیص ناهنجاری‌ها در زمان اجرای کانتینر، امکان مانیتورینگ منعطف رویدادها را فراهم می‌کند. همچنین مجموعه قوانین تشخیص از پیش ساخته‌شده، کمک می‌کند تهدیدها بلافاصله شناسایی شوند.
4	**شروع سریع**	قوانین از پیش ساخته‌شده برای محافظت از APIها و بررسی امنیت Kubernetes Manifestها، به شما امکان می‌دهد کلاستر را بلافاصله پس از نصب محصول محافظت کنید.

65%

از شرکت‌ها از کانتینرها برای استقرار برنامه‌ها به‌طور گسترده استفاده می‌کنند

92%

از سازمان‌ها منابع لازم برای شناسایی حوادث امنیتی جدی در کانتینرها را ندارند

83%

از شرکت‌ها به فرایندهای توسعه امن اهمیت می‌دهند

منبع: تحقیقات Positive Technologies و K2 Cybersecurity

APPLICATION
SECURITY

PT BLACKBOX

DYNAMIC APPLICATION SECURITY TESTING TOOL

نمای کلی محصول

PT BlackBox اقدامات یک مهاجم را شبیه‌سازی می‌کند که قصد نفوذ از راه دور به یک وب‌سایت یا سرویس را دارد.این محصول نه‌تنها کامپوننت‌های شخص ثالث دارای آسیب‌پذیری شناخته‌شده را شناسایی می‌کند، بلکه با ترکیب چندین روش تحلیل، مشکلات خاص برنامه تحت آزمایش را نیز کشف می‌کند.این ویژگی‌ها PT BlackBox را هم به‌عنوان یک ابزار مستقل و هم به‌عنوان یک تحلیل‌گر پویا Dynamic Analyzer که در خط لوله توسعه شما ادغام می‌شود، ضروری می‌سازد.

مزایا

1	**تحلیل چندبعدی آسیب‌پذیری‌ها**	روش‌های تحلیل که در همکاری نزدیک با متخصصان برجسته امنیت سایبری توسعه یافته‌اند، امکان شناسایی ده‌ها کلاس آسیب‌پذیری مانند SQLi، RCE، XSS، XXE و غیره را فراهم می‌کنند.
2	**اسکن کارآمد**	با نادیده گرفتن صفحات تکراری در حین اسکن، مصرف منابع کاهش یافته و عملکرد بهینه می‌شود.
3	**تحلیل خودکار و انعطاف‌پذیر**	اسکن و فرآیند احراز هویت را می‌توان برای هر برنامه خاص تنظیم کرد، در حالی که تحلیل به‌صورت خودکار انجام می‌شود و نیاز به بررسی دستی از بین می‌رود.
4	**پوشش آسیب‌پذیری API**	اسکن مستقیم API امکان شناسایی آسیب‌پذیری‌های بالقوه در سیستم‌های حیاتی Backend را فراهم می‌کند.

84%

از برنامه‌ها امکان دسترسی هکرها به منابع وب را فراهم می‌کنند

91%

از برنامه‌ها به هکرها اجازه می‌دهند داده‌های حساس را سرقت کنند

98%

از برنامه‌های IT دارای آسیب‌پذیری هستند

APPLICATION
SECURITY

PT APPLICATION FIREWALL PRO

ZERO-DAY THREAT PROTECTION

نمای کلی محصول

فایروال برنامه‌های وب WAF با کارایی بالااز برنامه‌های وب — از صفحات فرود ساده تا پورتال‌های سازمانی با بار بالا — و APIهای آن‌ها در برابر تهدیدات سایبری خارجی محافظت می‌کند.

مزایا

1	**پشتیبانی چندمستاجری**	محیط‌های ایزوله (Tenantها) امکان پیکربندی و دسترسی مستقل برای چندین برنامه در همان پلتفرم را فراهم می‌کنند. هر Tenant دارای پردازنده‌های ترافیک اختصاصی و جداسازی فیزیکی کلاستر است — که ایزوله‌سازی قوی‌تری نسبت به جداسازی منطقی ارائه می‌دهد.
2	**پشتیبانی کامل از HTTP/2 Proxy**	پشتیبانی کامل از پروتکل مدرن HTTP/2 سرعت انتقال داده را به‌طور قابل توجهی افزایش داده، تأخیر را به حداقل می‌رساند و عملکرد بالای برنامه را حفظ می‌کند.
3	**قابلیت‌های مقیاس‌گذاری خودکار**	افزایش ناگهانی ترافیک (مثلاً در حملات DDoS یا فروش‌های بزرگ مانند Black Friday) با اضافه شدن خودکار پردازنده‌های ترافیک مدیریت می‌شود. معماری مبتنی بر کانتینر اجازه مقیاس‌گذاری پویا نودهای کلاستر را بر اساس منابع موجود می‌دهد.
4	**گزینه‌های انعطاف‌پذیر استقرار**	چند سناریوی استقرار قابل انتخاب است: ▪ On-Premises — کنترل کامل داده‌ها بدون اتصال به اینترنت ▪ Multi-Site — از طریق Agentها یا سرورهای پردازش ترافیک اضافی. ▪ Hybrid/Cloud — ماژول سبک‌وزن که با نسخه ابری PT AF ارتباط برقرار می‌کند تا هزینه‌های زیرساخت کاهش یابد.

محافظت در برابر **OWASP Top 10**
و **OWASP API Security Top 10***

2000+
مشتری در طول بیش از ۱۰ سال

محافظت در برابر
5000+
آسیب‌پذیری شناخته‌شده

150 k RPS
عملکرد پایدار

*فهرست دقیق تهدیدات بنا به درخواست قابل ارائه است

APPLICATION
SECURITY

PT MAZE

A SERVICE FOR PROTECTING MOBILE APPLICATIONS FROM REVERSE ENGINEERING

نمای کلی محصول

از کلون‌سازی، دستکاری، فعال‌سازی غیرمجاز قابلیت‌های پولی و اسکن آسیب‌پذیری‌ها جلوگیری می‌کند و همچنین تلاش‌های اشخاص ثالث برای تحلیل سازوکار داخلی برنامه را مسدود می‌سازد.

در هسته PT MAZE ، سال‌ها تجربه شرکت Positive Technologies در حوزه هک اخلاقی و ارزیابی امنیت برنامه‌های موبایل قرار دارد.

عدم نیاز به دسترسی به کد منبع

PT MAZE بدون نیاز به دسترسی به کد منبع برنامه شما کار می‌کند.

اصلاح به‌جای افزودن

مکانیزم‌های امنیتی مستقیماً در فایل‌های اجرایی برنامه تعبیه می‌شوند.

غیرمتمرکزسازی

هر ماژول به‌صورت مستقل اجرا شده و قابل سفارشی‌سازی است، که امکان توزیع حفاظت در سراسر برنامه را فراهم می‌کند.

SaaS

برنامه خود را بارگذاری می‌کنید؛ PT MAZE آن را روی سرور اصلاح کرده و نسخه‌های محافظت‌شده با دفاع‌های تعبیه‌شده را در اختیار شما قرار می‌دهد.

بدون نیاز به پیکربندی

با استفاده از تنظیمات از پیش پیکربندی‌شده، حفاظت تنها با یک کلیک فعال می‌شود— بدون نیاز به راه‌اندازی یا تنظیمات دستی.

قابل ارائه بر روی

Android iOS

رویکرد ما

1

آماده‌سازی

- ارزیابی وضعیت فعلی امنیت برنامه‌های کاربردی
- شناسایی حوزه‌های قابل بهبود
- تدوین استراتژی و نقشه راه AppSec
- تهیه قالب‌های سیاست‌های داخلی
- مطالعه امکان‌سنجی کنترل‌های امنیتی
- آماده‌سازی مستندات لازم برای آغاز پروژه

2

پیاده‌سازی

- پیاده‌سازی فرایندها
- پیاده‌سازی کنترل‌های فنی
- پیکربندی و یکپارچه‌سازی
- بازبینی و اصلاح سیاست‌های داخلی
- آن‌بوردینگ تیم‌های توسعه منتخب

3

پشتیبانی

- آن‌بوردینگ سایر تیم‌ها
- رفع بدهی فنی
- بهینه‌سازی ابزارهای اسکن
- به‌روزرسانی سیاست‌های داخلی