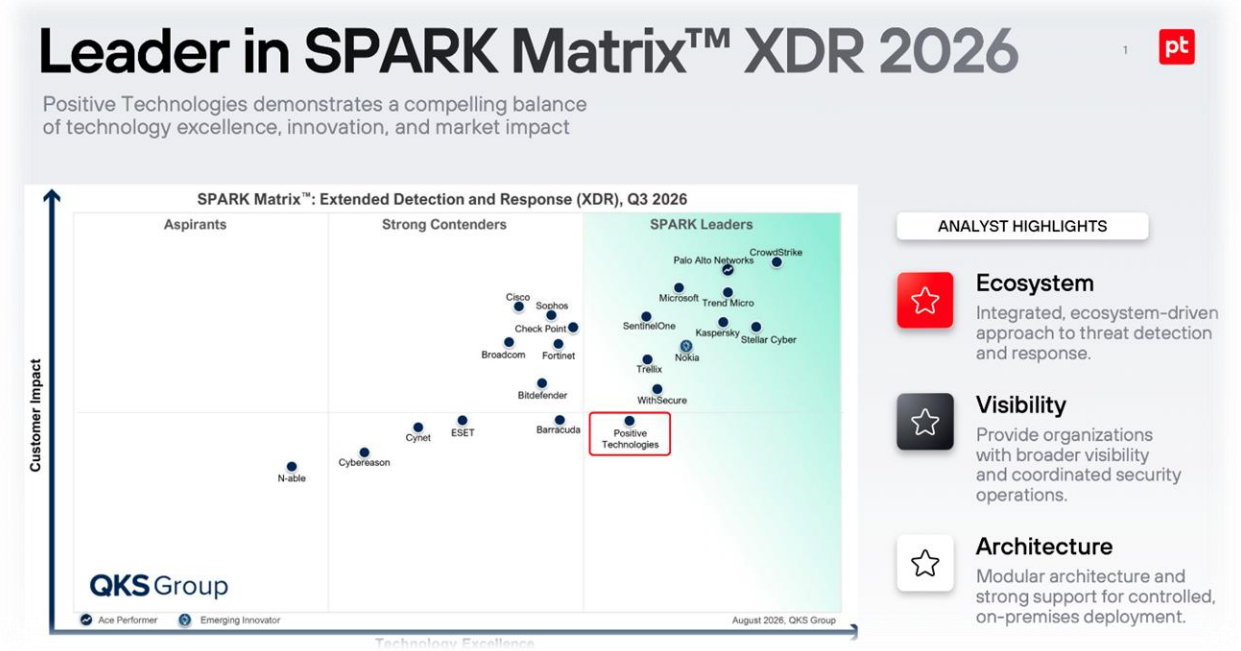
Positive Technologiesدر جمع رهبران جهانیXDR ؛

بررسی جایگاه PT در رتبه‌بندی SPARK Matrix سال ۲۰۲۶



شرکت تحقیقاتی و مشاوره‌ای QKS Group در تازه‌ترین ارزیابی خود از بازار جهانی Extended Detection and Response یا XDR ، شرکت Positive Technologies را در گروه رهبران این بازار قرار داده است. این ارزیابی اهمیت ویژه‌ای دارد، زیرا Positive Technologies در کنار مجموعه‌ای از بزرگ‌ترین شرکت‌های امنیت سایبری جهان از جملهMicrosoft ، CrowdStrike، Palo Alto Networks، SentinelOne، Cisco، Fortinetو Trend Micro بررسی شده است. در گزارش سال ۲۰۲۶، مجموعاً ۲۲ تأمین‌کننده راهکارهای XDR مورد ارزیابی قرار گرفته‌اند.

اما اهمیت این خبر صرفاً در دریافت عنوان «Leader» خلاصه نمی‌شود. نکته مهم‌تر این است کهQKS ، معماری XDR شرکت Positive Technologiesرا نه صرفاً به عنوان یک محصولEndpoint ، بلکه به عنوان یک اکوسیستم امنیتی متشکل ازEDR ، EPP، SIEM، NDR/NAD، Vulnerability Management، Sandbox، Threat Intelligenceو حتی امنیت زیرساخت‌های صنعتی مورد توجه قرار داده است.

https://qksgroup.com/newsroom/positive-technologies-positioned-as-a-leader-in-the-spark-matrix-extended-detection-and-response-xdr-2026-by-qks-group-1787

QKS Group چیست و SPARK Matrix چگونه کار می‌کند؟

QKS Groupیک شرکت بین‌المللی تحقیقاتی و مشاوره فناوری است که پیش‌تر با نام Quadrant Knowledge Solutions شناخته می‌شد. سابقه شکل‌گیری فعالیت این مجموعه به سال ۲۰۱۵ بازمی‌گردد و این شرکت بعدها چارچوب ارزیابی خود را با عنوان SPARK Matrix توسعه داد. این چارچوب از سال ۲۰۱۸ به یکی از محصولات اصلی تحقیقاتی این شرکت تبدیل شده است.

بر خلاف برندهای تجاری مانند گارتنر که شرکتهای امریکایی هستند و بر پایه تحریمهای امریکا و اتحادیه اروپا محصولات ایرانی و روسی و گاها چینی را تحریم کرده و از مقالات و بررسیها خارج کرده اند این شرکت همچنان به بررسی همه محصولات فعال در بازار بین المللی پایبند است .

SPARK مخفف Strategic Performance Assessment and Ranking است و هدف آن مقایسه شرکت‌های فعال در یک بازار فناوری بر اساس دو محور اصلی است:

- Technology Excellenceیا برتری فناوری، که عواملی مانند قابلیت‌های فنی محصول، معماری، نوآوری، سطح یکپارچگی و بلوغ فناوری را بررسی می‌کند؛
- Customer Impact یا تأثیر بر مشتری، که عواملی نظیر حضور در بازار، تجربه مشتری، میزان پذیرش محصول و ارزشی که راهکار برای سازمان‌ها ایجاد می‌کند را در نظر می‌گیرد.

برخلاف برخی مدل‌های سنتی ۲×۲، QKSاز یک ساختار ۳×۲ استفاده می‌کند و شرکت‌ها را در گروه‌هایی مانند Leaders & Emerging Leaders، Contenders & Strong Contendersو Aspirants قرار می‌دهد. بنابراین قرارگرفتن یک شرکت در بخش Leaders به معنی عبور همزمان آن از سطح بالایی از بلوغ فناوری و تأثیرگذاری بر مشتری است، اما الزاماً به معنی رتبه اول عددی در بازار نیست.

اطلاعات مورد استفاده برای رتبه‌بندی از کجا تأمین می‌شود؟

یکی از بخش‌های مهم روشQKS ، مدل تحقیقاتی Closed-Loop Research است.

طبق توضیحات رسمی این شرکت، اطلاعات مورد استفاده در ارزیابی‌ها می‌تواند از جلسات ۶۰ تا ۹۰ دقیقه‌ای باVendor ها، RFI، نمایش زنده محصولات، نظرسنجی ساختاریافته از مشتریان، تحقیقات بازار، منابع عمومی و بانک اطلاعاتی داخلی QKS به دست آید. نکته مهم این است که شرکت مورد ارزیابی الزاماً نباید در فرآیند تحقیق مشارکت داشته باشد؛ QKS اعلام می‌کندVendor های مرتبط را حتی در صورت عدم مشارکت مستقیم، بر اساس بهترین اطلاعات موجود بررسی می‌کند.

در نتیجه SPARK Matrix را نباید صرفاً یک مقایسه Feature-by-Feature دانست؛ عواملی مانند بلوغ محصول، معماری، نوآوری، Integration، تجربه مشتری و جایگاه Vendor نیز در نتیجه نهایی تأثیر دارند.

چرا Positive Technologies در حوزه XDR مورد توجه QKS قرار گرفته است؟

در مرکز معماری مورد ارزیابیPositive Technologies ، راهکار MaxPatrol Endpoint Security قرار دارد.

این راهکار در عمل دو لایه اصلی امنیت Endpoint شرکت را کنار یکدیگر قرار می‌دهد:

- MaxPatrol EPPبرای محافظت پیشگیرانه ازEndpoint ها در برابر بدافزارها، باج‌افزارها و تهدیدهای شناخته‌شده و عمومی؛
- MaxPatrol EDR برای شناسایی حملات پیچیده‌تر، تحلیل رفتار مهاجم، Incident Investigationو اجرای اقدامات.Response

بنابراین MaxPatrol Endpoint Security تنها یک Antivirus نیست؛ Endpoint به یکی از منابع اصلی Telemetry برای معماری گسترده‌تر Detection & Response تبدیل می‌شود.

اما نکته‌ای که QKS در ارزیابی Positive Technologies به آن اهمیت زیادی داده، قابلیت اتصال این Endpoint Security به سایر اجزای پلتفرم امنیتی PT است.

MaxPatrol SIEM ؛ مرکز جمع‌آوری و تحلیل رخدادها

MaxPatrol SIEMمسئول جمع‌آوری و Correlation رخدادهای امنیتی از منابع متعدد سازمان است.

ترکیب اطلاعات SIEM با داده‌های Endpoint باعث می‌شود یک Alert منفرد صرفاً به عنوان یک رویداد مستقل بررسی نشود، بلکه بتوان آن را در کنارLogin ها، رفتار کاربران، رخدادهای شبکه و سایر اطلاعات امنیتی تحلیل کرد.

در نتیجه SOC می‌تواند به جای مشاهده ده‌ها Alert جداگانه، تصویری نزدیک‌تر به زنجیره واقعی حمله ایجاد کند.

MaxPatrol VM ؛ اضافه‌شدن Context آسیب‌پذیری

MaxPatrol VMبخش Vulnerability Management اکوسیستم است.

ارزش Integration آن با XDR در این است که سیستم می‌تواند متوجه شود یک Endpoint یا Server که رفتار مشکوکی از آن مشاهده شده، چهVulnerability هایی نیز دارد , به این ترتیب اولویت یک Incident فقط بر اساس نوع Alert تعیین نمی‌شود، بلکه Exposure واقعی Asset نیز می‌تواند در تصمیم‌گیری دخالت داشته باشد.

PT Sandbox ؛ تحلیل عمیق فایل‌های مشکوک

یکی دیگر از اجزای این معماری PT Sandbox است. در صورتی که یک فایل یا Object مشکوک در Endpoint یا بخش دیگری از زیرساخت مشاهده شود، امکان ارسال آن برای تحلیل عمیق‌تر در یک محیط ایزوله وجود دارد. به این ترتیب نتیجه تحلیل Sandboxمی‌تواند دوباره وارد فرآیند Detection و Incident Investigation شود.

PT NAD ؛ اضافه‌شدن دید شبکه

یکی از تفاوت‌های مهم معماریPT ، حضور PT NAD – Network Attack Discovery است, EDR عمدتاً آنچه روی Endpointاتفاق می‌افتد را مشاهده می‌کند، اما همه مراحل حمله الزاماً روی Endpoint قابل مشاهده نیستند.

PT NAD با بررسی Network Traffic می‌تواند یک لایه مستقل از Visibility ایجاد کند و اطلاعات آن باEndpoint ، SIEM و سایر اجزا ترکیب شود , QKSنیز به صورت مشخص به نقش PT NAD در گسترش Visibility در سطح شبکه اشاره کرده است.

PT ISIM ؛ گسترش XDR به محیط‌های صنعتی

یکی از جالب‌ترین نقاط تمایز Positive Technologies ، PT ISIM است , PT ISIM برای Monitoring و Cybersecurity در زیرساخت‌های صنعتی و محیط‌های OT/ICS طراحی شده و باعث می‌شود اکوسیستم Detection & Response شرکت تنها محدود به IT ، Server و Endpoint نباشد, QKS به صورت مشخص به ترکیب PT NAD و PT ISIM به عنوان عاملی اشاره می‌کند که Visibility راهکار PT را به شبکه و محیط‌های صنعتی گسترش می‌دهد.

نقش PT Expert Security Center در این رتبه‌بندی

بخش دیگری که در ارزیابی QKS مورد توجه قرار گرفته، PT Expert Security Center یا PT ESC است.

تیم‌های تحقیقاتی PT به صورت مستمر کمپین‌های حمله، Malwareها، TTPهای مهاجمان و گروه‌های APT را بررسی می‌کنند و اطلاعات حاصل از این تحقیقات می‌تواند به Detection Logic و محصولات شرکت منتقل شود.

QKSاین موضوع را یکی از نقاط قوت Positive Technologies دانسته است؛ زیرا در یک XDR مدرن، داشتن تعداد زیادی Sensorبه تنهایی کافی نیست و کیفیت Detection تا حد زیادی به کیفیت Threat Research و دانش رفتار مهاجمان وابسته است. به بیان ساده‌تر، معماری PT تلاش می‌کند دو بخش را به هم متصل کند:

و همین چرخه یکی از دلایل مهم ارزیابی مثبت QKS بوده است.

رقبای Positive Technologies در بررسی XDR چه شرکت‌هایی بودند؟

طبق اطلاعات منتشرشده درباره SPARK Matrix سال ۲۰۲۶، در مجموع ۲۲ Vendor در این حوزه بررسی شده‌اند.

منابع عمومی مرتبط با گزارش حضور نام‌هایی مانندMicrosoft ، CrowdStrike، Palo Alto Networks، SentinelOne، Cisco، Fortinetو Trend Micro را تأیید می‌کنند.

بنابراین Positive Technologies در یک گروه محدود از تولیدکنندگان منطقه‌ای ارزیابی نشده است؛ بلکه وارد مقایسه با Vendorهایی شده که بخش قابل توجهی از بازار جهانیEndpoint Security ، EDR، SIEMو XDR را در اختیار دارند.

Microsoft Defender XDR

Microsoftمعماری XDR خود را حول اکوسیستم Defender توسعه داده است.

Microsoft Defender XDRاطلاعات Defender for Endpoint ، Defender for Identity، Defender for Office 365و Defender for Cloud Apps را در یک محیط مشترک جمع‌آوری کرده و قابلیت Investigation ، Threat Huntingو Automated Response ارائه می‌کند.

مزیت اصلی Microsoft عمق Integration با اکوسیستمMicrosoft ، Active Directory/Entra، Microsoft 365، Emailو Endpoint است.

در سازمان‌هایی که بخش بزرگی از زیرساخت آنها Microsoft است، این Integration یک مزیت بسیار جدی محسوب می‌شود.

CrowdStrike Falcon Insight XDR

CrowdStrikeیکی دیگر از مهمترین رقبای جهانی در این بازار است .

Falcon Insight XDRهسته EDR قدرتمند CrowdStrike را با Telemetry مربوط بهIdentity ، Cloud، Mobileو سایر منابع ترکیب کرده و از Threat Intelligence و AIنیز برای Detectionو Investigation استفاده می‌کند .

CrowdStrikeاز نظرCloud-native Architecture ، Threat Intelligenceو Endpoint Telemetryیکی از Benchmark های اصلی بازار محسوب می‌شود .

Palo Alto Networks Cortex XDR

Cortex XDRداده‌هایEndpoint ، Network، Cloud، Identityو منابع Third-party را کنار یکدیگر قرار می‌دهد .

Palo Altoهمچنین Cortex XDR را به عنوان یکی از پایه‌های معماری گسترده‌تر Cortex XSIAMتوسعه داده که هدف آن حرکت به سمت یک SOCیکپارچه و AI-driven است .

یکی از نقاط قوت Palo Alto ارتباط نزدیک میانXDR ، Firewall Telemetry، Cloud Securityو سایر اجزای اکوسیستم Cortex است .

SentinelOne Singularity XDR

SentinelOneنیز معماری Singularity XDR خود را بر پایه Endpoint ، Cloud و Identity Telemetryتوسعه داده است .

این پلتفرم می‌تواند Telemetry داخلی و اطلاعات Third-party را در یک Data Lake ترکیب، Correlate و Analyze کرده و Response های خودکار اجرا کند .

Cisco XDR

Cisco XDRنیز با هدف ترکیب Telemetry از Endpoint ، Network، Email، Cloud و سایر ابزارهای امنیتی توسعه یافته است .

برای سازمان‌هایی که زیرساخت شبکه و Security Stack گسترده Cisco دارند، یکی از مزیت‌های مهم این محصول استفاده از اطلاعات موجود در همین اکوسیستم است .

Fortinet FortiXDR

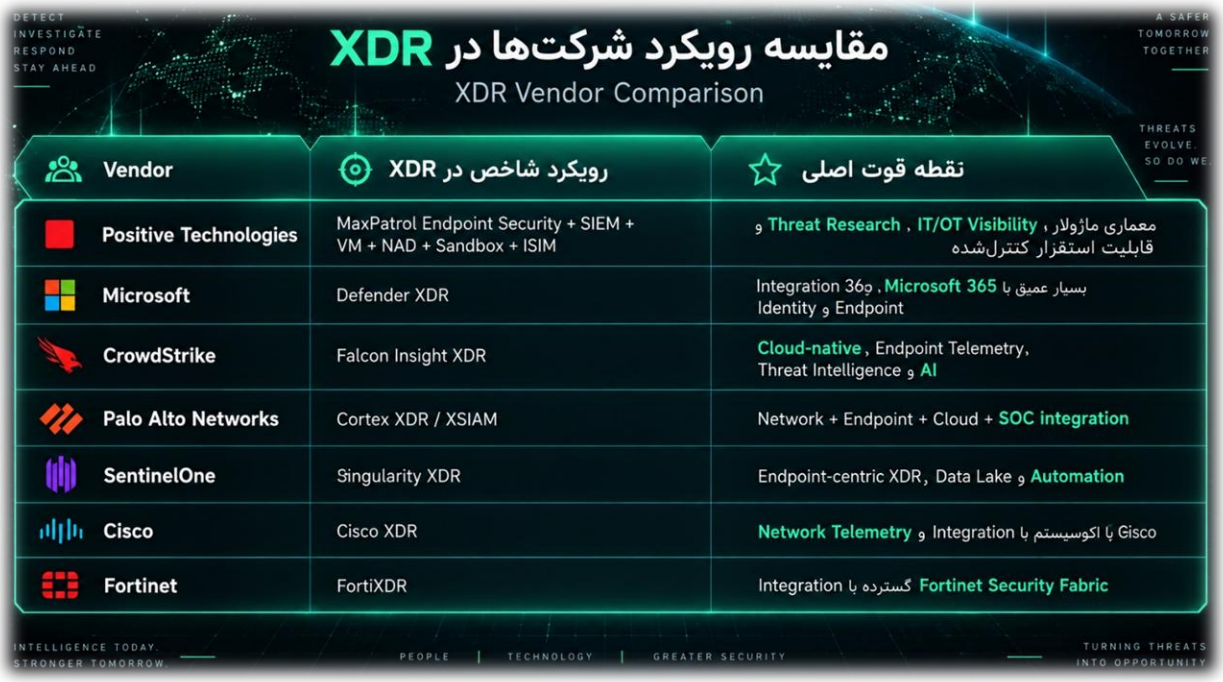
FortiXDRاطلاعات Endpoint ، Network، Cloud و سایر اجزای Fortinet Security Fabric را Correlate می‌کند و قابلیت Automated Response را نیز در اختیار SOC قرار می‌دهد .

Fortinetهمچنین بر استفاده از AI و Automation برای Investigation و Response تأکید دارد .

Positive Technologies در مقایسه با این رقبا در چه جایگاهی قرار می‌گیرد؟

مهم‌ترین نتیجه گزارش QKS این نیست که Positive Technologies از Microsoft ، CrowdStrike یا« Palo Alto بهتر» معرفی شده است. چنین نتیجه‌ای از اطلاعات عمومی گزارش قابل استخراج نیست.

آنچه با اطمینان می‌توان گفت این است که Positive Technologies توانسته وارد گروه Leaders در همان بازار جهانی شود که Vendor های بسیار بزرگ XDR در آن ارزیابی می‌شوند و این موضوع در کنار اینکه با توجه به شرایط ویژه جنگی در کشور و وابستگی بسیاری از برندهای فوق به شرکتهای امریکایی و اسراییلی و عدم اخذ مجوز رسمی فعالیت در ایران از مرکز افتا باعث شده هم از نظر فنی هم از نظر توانایی مزیت استفاده از محصولات پی تی در بازار امنیت سایبری در ایران بیش از پیش تثبیت شود همچنین این موضوع از منظر بلوغ فناوری اهمیت زیادی دارد و برای شرکتهای ایرانی این امکان را فراهم میکند تا به سمت ادغام یا هم افزایی محصولات بومی خود با محصولات پی تی قدم بردارند .



این مقایسه نشان می‌دهد که رقابت در XDR دیگر بر سر داشتن یک EDR قوی نیست.

رقابت اصلی بر سر این است که کدام Vendor می‌تواند بیشترین Context را از لایه‌های مختلف Infrastructure جمع‌آوری کرده و آن را سریع‌تر به یک Incident قابل فهم و یک Response مؤثر تبدیل کند.

مزیت متفاوت Positive Technologies چیست؟

از نگاه معماری، شاید مهم‌ترین نقطه تمایز PT در برابر بسیاری از رقبا ترکیب سه حوزه باشد:

Endpoint + Network + Industrial Infrastructure

در بسیاری از معماری‌های XDR مطرح جهانی، تمرکز بسیار زیادی برEndpoint ، Identity، Cloudو Email وجود دارد.

در مقابل، وجود PT NAD در کنار PT ISIM باعث شده Positive Technologies بتواند علاوه برIT ، شبکه و بخش‌هایی از OT/ICSرا نیز وارد معماری Detection & Response خود کند.

این ویژگی می‌تواند برای صنایع انرژی، نفت و گاز، نیروگاه‌ها، Utilities، Manufacturingو سایر سازمان‌هایی که IT و OT همزمان دارند، اهمیت بیشتری داشته باشد .QKS نیز دقیقاً به توسعه Visibility در Network و Industrial Environments از طریق PT NAD و PT ISIM اشاره کرده است.

معماری On-Premise و کنترل داده‌ها؛ مزیت دیگرPT

یکی دیگر از موضوعاتی که QKS در تحلیل Positive Technologies مورد توجه قرار داده، قابلیت استقرار کنترل‌شده محصولات در Infrastructure مشتری است , این موضوع در بازار XDR اهمیت زیادی پیدا کرده است.

بخش قابل توجهی از پلتفرم‌های بزرگ جهانی با معماری Cloud-first توسعه یافته‌اند؛ در حالی که بسیاری از سازمان‌های دولتی، دفاعی، بانکی، اپراتورها و زیرساخت‌های حیاتی نمی‌خواهند Telemetry امنیتی آنها خارج از Infrastructure تحت کنترلشان پردازش شود.

در چنین محیط‌هایی، انعطاف‌پذیری درOn-Premise Deployment ، Data Sovereigntyو کنترل محل نگهداری Telemetryمی‌تواند به یک مزیت رقابتی تبدیل شود.

آیا Leader شدن در SPARK Matrix به معنی برتری PT از Microsoft و CrowdStrike است؟

خیر. این نکته در تفسیر گزارش اهمیت زیادی دارد. قرار گرفتن Positive Technologies در ناحیه Leader نشان می‌دهد QKSترکیبی از Technology Excellence و Customer Impact شرکت را در سطح بالایی ارزیابی کرده است؛ اما از اعلامیه عمومی QKS نمی‌توان نتیجه گرفت که PT از نظر امتیاز عددی بالاتر ازMicrosoft ، CrowdStrikeیا Palo Alto قرار گرفته است , برای چنین ادعایی بایدScore ها و Coordinate دقیق تمام ۲۲ Vendor در نسخه کامل گزارش مقایسه شود.

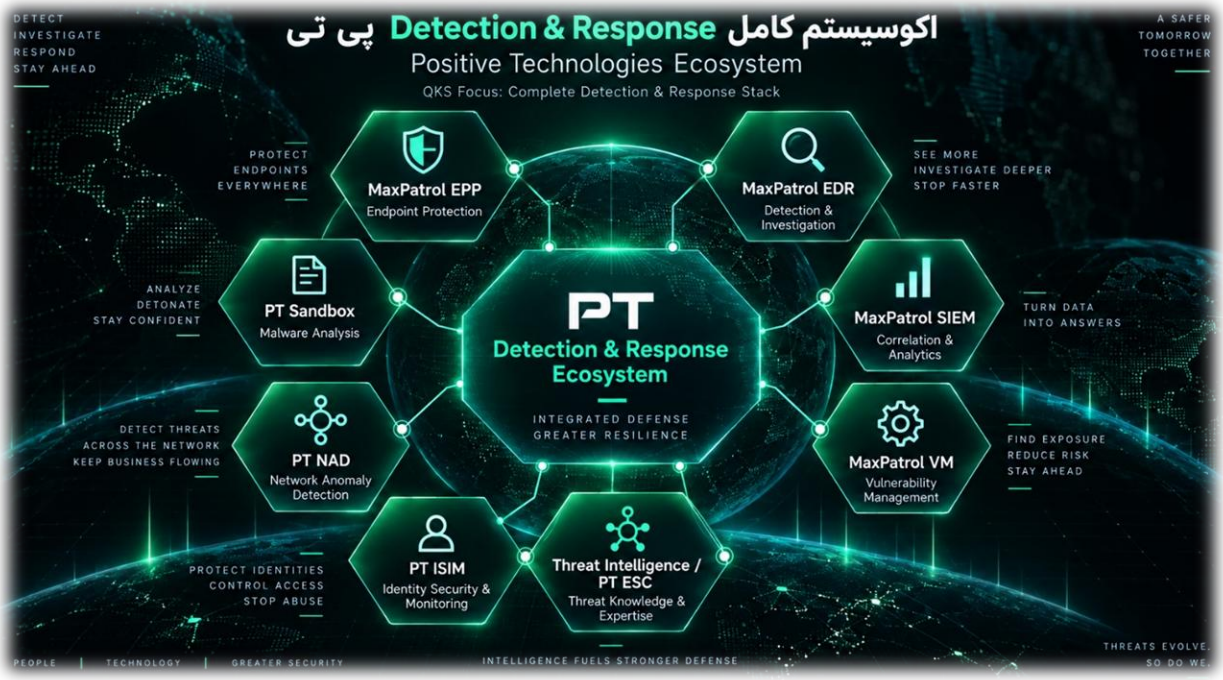
بنابراین عبارت صحیح‌تر این است:

Positive Technologiesاز سوی QKS Group به عنوان یکی از رهبران بازار جهانی XDR شناخته شده و در ارزیابی‌ای قرار گرفته که ۲۲ Vendor ، شامل تعدادی از بزرگ‌ترین شرکت‌های Cybersecurity جهان، در آن حضور داشته‌اند.

اهمیت این رتبه‌بندی برای Positive Technologies

قرار گرفتن PT در این بخش SPARK Matrix را می‌توان نشانه‌ای از تغییر جایگاه این شرکت از یک Vendor عمدتاً شناخته‌شده در بازار روسیه و کشورهای پیرامونی به یک بازیگر قابل مقایسه در بازار بین‌المللی Enterprise Cybersecurity دانست. در این ارزیابی، مزیت Positive Technologies صرفاً به MaxPatrol EDR محدود نشده است. در واقع آنچه QKS مورد توجه قرار داده، اکوسیستم کامل Detection & Response شامل:

MaxPatrol EPP + MaxPatrol EDR + MaxPatrol SIEM + MaxPatrol VM + PT Sandbox + PT NAD + PT ISIM + Threat Intelligence/PT ESC



این موضوع از نظر استراتژیک مهم است؛ زیرا بازار Cybersecurity به سرعت از خرید محصولات جزیره‌ای به سمت Platform Consolidationحرکت می‌کند.

مشتری دیگر صرفاً به دنبال بهترین EDR یا بهترین SIEM نیست؛ بلکه می‌خواهد بداند آیا محصولات مختلف می‌توانند اطلاعات یکدیگر را Contextualize کنند، یک Attack Chain واحد بسازند و عملیات SOC را از Detection تا Response کوتاه‌تر کنند یا خیر.

جمع‌بندی

ارزیابی SPARK Matrix سال ۲۰۲۶ نشان می‌دهد Positive Technologies توانسته از منظر QKS Group وارد گروه رهبران بازار Extended Detection and Response شود , نقطه قوت اصلی این شرکت در این ارزیابی را نمی‌توان به یک Feature یا حتی یک محصول خاص نسبت داد.

آنچه PT را در این رقابت قابل توجه کرده، ترکیبEndpoint Security ، SIEM، Vulnerability Management، Network Detection، Sandbox، Industrial Securityو Threat Research در یک اکوسیستم به‌هم‌پیوسته است.

رقبایی مانندMicrosoft ، CrowdStrike، Palo Alto Networks، SentinelOne، Ciscoو Fortinet هر یک مزیت‌های بسیار قدرتمندی دارند؛ Microsoft در اکوسیستم Identity وProductivity ، CrowdStrikeدر Cloud-native Endpoint Securityو Threat Intelligence ، Palo Altoدر یکپارچگیNetwork/Cloud/SOC ، Ciscoدر Network Visibilityو Fortinet در.Security Fabric

در مقابل، Positive Technologiesتلاش کرده مزیت رقابتی خود را بر روی معماری ماژولار، Integrationمیان محصولات، کنترل استقرار در زیرساخت مشتری، تحقیقات مستمر PT ESC و پوشش همزمانIT ، Networkو OT بنا کند.

بنابراین شاید مهم‌ترین پیام SPARK Matrix برای بازار این نباشد که» Positive Technologies از کدام Vendor بالاتر است»، بلکه این باشد که محصولات این شرکت اکنون از سوی یک مؤسسه تحقیقاتی بین‌المللی در همان طبقه رقابتی بررسی می‌شوند که بزرگ‌ترین بازیگران جهانی XDR در آن حضور دارند.

و برای سازمان‌هایی که به دنبال یک معماری مستقل و یکپارچهDetection & Response ، خصوصاً در محیط‌های دارای ترکیب ITو OT هستند، این جایگاه می‌تواند Positive Technologies را به یک گزینه جدی‌تر برای مقایسه با پلتفرم‌های شناخته‌شده جهانی تبدیل کند.