Позитивная карта импортозамещения

Какие продукты Positive Technologies помогут успешно заменить продукты зарубежных вендоров

Класс решений	Vulnerability Management	SIEM	NTA	Sandbox	SCADA Security	OT Security	WAF	AST	XDR	DAST
	Системы анализа защищенности и сканеры уязвимостей	Системы выявления инцидентов ИБ	Системы глубокого анализа сетевого трафика	Песочницы, системы динамического анализа файлов	Системы выявления атак в сетях АСУ ТП и нарушений регламентов ИБ	Решения для защиты промышленных сетей от угроз	Межсетевые экраны уровня веб-приложений	Анализаторы кода	Extended Detection and Response	Динамические анализаторы приложений
Зарубежные вендоры	VM-решения: Rapid7 InsightVM Qualys VMDR Tenable.sc Tenable.io Сканеры уязвимостей: Nexpose Vulnerability Scanner Tenable Nessus Pro GFI LanGuard Tripwire IP360	IBM QRadar SIEM Micro Focus ArcSight ESM Splunk Enterprise FortiSIEM McAfee ESM Exabeam Fusion LogRhythm NextGen SIEM Platform Securonix Next-Gen SIEM Elastic (ELK) Stack	Cisco Stealthwatch Trend Micro Deep Discovery Darktrace Enterprise Immune System Plixer Scrutinizer Flowmon Vectra AI Awake Security Platform IBM QRadar Incident Forensics RSA NetWitness Network ExtraHop Reveal(x) Palo Alto Cortex XDR	FortiSandbox Trend Micro Deep Discovery FireEye NX, EX, FX Check Point SandBlast McAfee Advanced Threat Defense Palo Alto WildFire ESET Dynamic Threat Defense CrowdStrike (Falcon Sandbox)	Dragos Platform Nozomi Networks Platform Claroty Platform	Dragos Platform (все продукты) Nozomi Networks Platform (все продукты) Claroty Platform (все продукты)	Imperva WAF Radware AppWall Akamai Kona Site Defender Akamai Web Protection F5 Advanced WAF FortiWeb WAF Barracuda WAF	Micro Focus Fortify Checkmarx Snyk.io AppScan (HCL)	Palo Alto Cortex XDR Qualys EDR Check Point Harmony Endpoint Fortinet FortiXDR Sangfor XDDR McAfee MVISION XDR SentinelOne EDR VMware Carbon Black EDR CrowdStrike Falcon Insight EDR Cisco AMP for Endpoints Trend Micro Vision One XDR Percept XDR Symantec EDR	Acunetix Invicti (Netsparker) Burp Pro

Продукт PT	MaxPatrol VM	MaxPatrol SIEM	PT NAD	PT Sandbox	PT ISIM	PT ICS	PT Application Firewall	PT Application Inspector	PT XDR	PT BlackBox
Сертификация	**Плановая дата получения: Q4 2023**	**ФСТЭК 3734**	**ФСТЭК 4042, ФСБ 0462**	**ФСТЭК 4604**	**ФСТЭК 4182**	**Отдельно по продуктам**	**ФСТЭК 3455**	**ФСТЭК 4000**	**Плановая дата получения: Q4 2023**	
	► Помогает выстроить полноценный процесс управления уязвимостями и отслеживать повышение уровня защищенности ► Выявляет уязвимости IT-инфраструктуры и позволяет приоритизировать их по уровню опасности для бизнеса ► Сообщает о трендовых уязвимостях, которые, согласно данным экспертного центра безопасности PositiveTechnologies (PT ESC), злоумышленники эксплуатируют прямо сейчас ► Автоматически пересчитывает уязвимости при изменении базы знаний без активного сканирования ► Собирает полную информацию об активах сети и следит за изменениями IT-инфраструктуры ► Сделан на единой платформе MaxPatrol 10	► Дает полную видимость IT-инфраструктуры и выявляет инциденты информационной безопасности ► Упрощает выявление и работу с инцидентами за счет пакетов экспертизы, содержащих правила выявления угроз и рекомендации по реагированию ► Приоритизирует инциденты по значимости активов ► Позволяет снизить затраты экспертов на расследование инцидентов ► Масштабируется для соответствия требованиям высокой нагрузки и географически распределенных IT-инфраструктур ► Содержит все средства для самостоятельной разработки контента и интеграций с внешними системами для построения полноценного SOC	► Выявляет внешних и внутренних злоумышленников в сети ► Выявляет атаки и индикаторы даже в зашифрованном трафике без расшифровки ► Определяет использование теневой инфраструктуры, сторонних сервисов, средств удаленного администрирования в туннелях ► Выявляет нарушения регламентов ИБ. Делает сеть прозрачной для отделов ИТ и ИБ ► Выявляет скрытые угрозы в сети за счет комбинации модулей обнаружения угроз: поведенческий анализ трафика, статистический анализ сессий, правила обнаружения угроз, ретроспективный анализ	► Позволяет максимально точно имитировать реальную инфраструктуру благодаря гибкой кастомизации виртуальных сред ► Обеспечивает комплексную проверку файлов: статический и динамический анализ с помощью уникальных правил PT ESC и проверка антивирусами ► Выявляет угрозы не только в файлах, но и в сетевом трафике, включая шифрованный ► Безопасно провоцирует хакеров выдать себя (decep-tion-технологии, «приманки») ► Выявляет скрытые угрозы в сети с помощью ретроспективного анализа	► Обнаруживает атаки и нарушения регламентов ИБ в промышленных сетях (самая большая и пополняемая база экспертных знаний PT ISTI) ► Полный разбор и нормализация трафика АСУ ТП для целей threat hunting ► Продукт является частью комплексной платформы для защиты промышленности от киберугроз — PT ICS ► Классифицирует угрозы в соответствии с матрицей MITRE ATT&CK и приказом ФСТЭК № 239 ► Автоматически обучается и подстраивается под любую инфраструктуру	► Состоит из пяти ключевых продуктов Positive Technologies: MaxPatrol SIEM, MaxPatrol VM, PT ISIM, PT Sandbox и агентов PT XDR ► Все продукты в составе платформы содержат промышленную экспертизу PT ESC ► Помогает обнаружить злоумышленника на ранних этапах развития атак в промышленных средах и своевременно на них отреагировать ► Позволяет реализовать единый корпоративный и технологический SOC на универсальном стеке продуктов (не требуется сложное обучение персонала) ► Расширяет возможности SOC для предотвращения инцидентов в технологических системах ► Помогает выполнить максимум требований приказа ФСТЭК № 239, связанных с наложенными средствами защиты	► Блокирует массовые и целевые атаки ► Выявляет атаки, распределенные во времени ► Быстро встраивается в инфраструктуру ► Дополнительные модули: M-Scan (мультивендорная антивирусная проверка загружаемых и скачиваемых файлов); P-Code (поиск уязвимостей в защищаемых приложениях и формирование виртуальных патчей)	► Минимум ложных срабатываний ► Эффективно встраивается в процессы компании: интеграция с Jenkins, TeamCity, GitLab CI, Azure ► Умеет анализировать код, готовые развернутые приложения, сторонние компоненты (библиотеки)	► Связывает события и контекст из разных инструментов ИБ ► Верифицирует факты атак, выявляет причины заражения или компрометации, отсеивает ложные срабатывания ► Сокращает время устранения угрозы: дает необходимые данные для реагирования и расследования, автоматизирует реагирование, снижает требования к квалификации специалистов и их количеству ► Позволяет выявлять атаки как в сети, так и на конечных точках, останавливает атаки на конечные точки ► Позволяет распространять знания об угрозах (IoC, IoA) по всей сети агентов, обеспечивает поиск схожего поведения в сети	► Дает рекомендации по устранению проблем не только в приложении, но и в его эксплуатационной среде ► Находит то, что скрыто. Использует комбинацию эвристического и сигнатурного анализа, непрерывно обновляя данные об уязвимостях ► Экономит ресурсы сканирования, определяя шаблонные повторяющиеся страницы и не тратя на них время ► Быстро встраивается в текущие процессы разработки и релизный цикл. За счет этого позволяет быстрее обнаруживать и исправлять уязвимости ► Тонкая настройка сканирования и авторизации позволяет пользователю задавать параметры анализа, добавлять профили сканирования