Позитивная карта импортозамещения

Какие продукты Positive Technologies помогут успешно заменить продукты зарубежных вендоров

Мониторинг безопасности

Класс решений	SIEM	Vulnerability Management	NTA	Sandbox	XDR
	Система выявления инцидентов ИБ	Системы анализа защищенности и сканеры уязвимостей	Система глубокого анализа сетевого трафика	Песочница, система динамического анализа файлов	Extended Detection and Response
Зарубежные вендоры	— 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	VM-решения: — Rapid7 InsightVM — Qualys VMDR — Tenable.sc — Tenable.io Сканеры уязвимостей: — Nexpose Vulnerability Scanner — Tenable Nessus Pro — GFI LanGuard — Tripwire IP360	— Cisco Stealthwatch — Trendmicro 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 — CheckPoint Sandblast — McAfee Advanced Threat Defense — Palo Alto WildFire — ESET Dynamic Threat Defense — CrowdStrike (Falcon Sandbox)	— Palo Alto Cortex XDR — Qualys EDR — Checkpoint 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
Продукт PT	MaxPatrol SIEM	MaxPatrol VM	PT Network Attack Discovery	PT Sandbox	PT XDR
Сертификация	**ФСТЭК 3734** Дает полную видимость IT-инфраструктуры и выявляет инциденты информационной безопасности Упрощает выявление и работу с инцидентами за счет пакетов экспертизы, содержащих правила выявления и рекомендации по реагированию Приоритизирует инциденты для значимых активов Позволяет снизить затраты экспертов на расследование инцидентов Масштабируется для соответствия требованиям высокой нагрузки и геораспределенных IT-инфраструктур Содержит все средства для самостоятельной разработки контента и интеграций с внешними системами для построения полноценного SOC	**Плановая дата получения: Q4 2023** Помогает выстроить полноценный процесс управления уязвимостями в компании и отслеживать повышение уровня защищенности Выявляет уязвимости IT-инфраструктуры и позволяет приоритизировать их по уровню опасности для бизнеса Сообщает о трендовых уязвимостях, которые злоумышленники эксплуатируют прямо сейчас, по данным экспертного центра безопасности Positive Technologies (PT Expert Security Center, PT ESC) 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	**ФСТЭК 4042, ФСБ 0462** Выявляет внешних и внутренних злоумышленников в сети Выявляет атаки и индикаторы даже в зашифрованном трафике без расшифрования Определяет использование теневой инфраструктуры, сторонних сервисов, средств удаленного администрирования в туннелях Выявляет нарушения регламентов ИБ. Делает сеть прозрачной для ИТ и ИБ отделов Выявляет скрытые угрозы в сети за счет комбинации модулей обнаружения угроз: поведенческий анализ трафика, статистический анализ сессий, правила обнаружения угроз, ретроспективный анализ	**ФСТЭК 4604** Позволяет максимально точно имитировать реальную инфраструктуру заказчика благодаря гибкой кастомизации виртуальных сред. Обеспечивает комплексную проверку файлов: проводит статический и динамический анализ с помощью уникальных правил PT ESC и проверку антивирусами. Выявляет угрозы не только в файлах, но и в сетевом трафике, включая шифрованный Безопасно провоцирует хакеров выдать себя (deception-технологии,«приманки») Выявляет скрытые угрозы в сети с помощью ретро-спективного анализа	**Плановая дата получения: Q4 2023** 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

AppSec

Класс решений	SAST	WAF	DAST
	Анализатор кода	Межсетевой экран уровня приложений	Динамический анализатор приложений
Зарубежные вендоры	— Micro Focus Fortify — Checkmarx — Snyk.io — AppScan (HCL)	— Imperva WAF — Radware AppWall — Akamai Kona Site Defender — Akamai Web Protection — F5 Advanced WAF — FortiWeb WAF — Barracuda WAF	— Acunetix — Netsparker (Invicti) — Burp Pro
Продукт PT	PT Application Inspector	PT Application Firewall	PT BlackBox
Сертификация	**ФСТЭК 4000** Минимум ложных срабатываний Эффективно встраивается в процессы компании: интеграции с Jenkins, TeamCity, GitLab CI, Azure Умеет анализировать: Код Готовое развернутое приложение Сторонние компоненты (библиотеки)	**ФСТЭК 3455** Блокирует массовые и целевые атаки Выявляет атаки, распре-деленные во времени Быстро встраивается в инфраструктуру Дополнительные модули: M-Scan (мультивендорная анти-вирусная проверка загружаемого на приложения контента); P-Code (поиск уязвимостей — в защищаемых приложениях и формирование виртуальных патчей).	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 на сканирование за счет определения шаблонных повторяющихся страниц и не тратит 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

Промышленная безопасность

	SCADA Security	OT Security
	Система выявления атак в сетях АСУ ТП и нарушений регламентов ИБ	Решение для защиты промышленных сетей от угроз
	— Dragos Platform — Nozomi Networks Platform — Claroty Platform	— Dragos Platform (все продукты) — Nozomi Networks Platform (все продукты) — Claroty Platform (все продукты)
	PT ISIM	PT ICS
	ФСТЭК 4182 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 предприятия	**Отдельно по продуктам** 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 атаки в промышленных средах и своевременно на них отреагировать Позволяет реализовать единый корпоративный и технологический SOC на универсальном стеке продуктов (не требуется сложное доп. обучение) Расширяет возможности SOC для предотвращения инцидентов в технологических системах Помогает выполнить максимум требований приказа ФСТЭК №239, связанных с наложенными средствами защиты