WithSecure™ Elements

Больше гибкости — меньше сложности.

Единственная платформа для кибербезопасности, которая вам нужна.

WITHSECURE ELEMENTS — ЭТО УНИВЕРСАЛЬНАЯ ПЛАТФОРМА, В КОТОРОЙ ВСЕ РАБОТАЕТ ВМЕСТЕ:

Endpoint Protection

Защита конечных точек от высоко-уровневых программ-вымогателей, вредоносных программ и угроз "нулевого дня".

Vulnerability Management

Выявление уязвимостей и критических слабых мест в ваших активах.

Collaboration Protection

Дополнительный слой защиты для экосистемы Microsoft Office365.

Endpoint Detection and Response

Мощный автоматизированный инструмент детектирования, расследования и реагирования на сложные атаки на конечные точки.

Cloud Security Posture Management

Надежная защита облачных сервисов путем автоматического обнаружения неправильной конфигурации и рекомендаций по ее исправлению.

ОСОБЕННОСТИ ПЛАТФОРМЫ:

- **Защита ваших конечных устройств и облачных сервисов**
- **Обнаружение и уничтожение угроз**
- **Предотвращение атак вредоносного ПО и программ-вымогателей**
- **Предотвращение фишинга и спам-атак**
- **Выявление уязвимостей и управление ими**
- **Обнаружение взломанных учетных записей Office 365**
- **Быстрое реагирование на атаки с помощью автоматизации, рекомендаций и круглосуточной поддержки**

WITHSECURE ELEMENTS
ENDPOINT PROTECTION

Новаторская защита от современных вредоносных программ и программ-вымогателей.
Elements Endpoint Protection обеспечивает автономную защиту, способную противостоять современным угрозам, к которым относятся программы-вымогатели, неизвестные вредоносные программы, эксплойты и уязвимости Zero Day. Получите комплексную защиту для мобильных телефонов, ПК, ноутбуков и серверов. Отфильтрованные оповещения и высокий уровень автоматизации обеспечивают максимальную эффективность.

- **Автономная круглосуточная защита** не требовательна к опыту специалистов и количеству времени, которое выделяется на управление ею.
- **Защита от угроз,** реализованная эвристическим и поведенческим анализом, расширенным машинным обучением и анализом угроз в реальном времени.
- **Применяйте обновленные патчи** безопасности по мере их выпуска с полностью автоматизированным управлением обновлениями.
- **Блокируйте выполнение программ** и скриптов в соответствии с правилами, созданными WithSecure или вашими администраторами.
- **Предотвращайте попадание пользователей** на вредоносные веб-сайты и другие онлайн-ресурсы.
- **Выявляйте программы-вымогатели** и предотвращайте уничтожение и подделку данных с помощью технологий DeepGuard и DataGuard.
- **Предотвращайте проникновение угроз или утечку данных** из вашей системы через контроль сменных носителей информации.
- **Запрещайте доступ несанкционированным программам** к файлам и системным ресурсам.

WITHSECURE ELEMENTS
ENDPOINT DETECTION AND RESPONSES

Будьте на шаг впереди злоумышленников.
Elements Endpoint Detection and Response защитит вас от сложных и целенаправленных кибератак с помощью передовых возможностей обнаружения. Оставайтесь устойчивыми и быстро возвращайте контроль над вашей инфраструктурой с помощью полезных идей и простых инструкций.

- **Получайте информацию о процессах** на конечных точках с помощью телеметрии в Windows, macOS и Linux.
- **Замечайте угрозы быстро** и точно с помощью функции Broad Context Detection™. Выявите все подозрительное поведение, даже если оно кажется безобидным.
- **Эффективно отслеживайте угрозы** с помощью поиска и фильтрации событий.
- **Разбирайте коррелирующие цепочки событий** с помощью упрощенных визуализаций.
- **Мгновенно реагируйте на угрозы** с помощью automatic response, включая сетевую изоляцию хоста на основе рисковой модели.
- **Контролируйте атаки с четким практическим руководством** и возможностью эскалации сложных кейсов к экспертам WithSecure.
- **Соблюдайте нормативные требования** PCI, HIPAA и GDPR по уведомлению о нарушениях в течение 72 часов.

WITHSECURE ELEMENTS
COLLABORATION PROTECTION

Многоуровневая защита для обнаружения и предотвращения сложных угроз и фишинговых атак, нацеленных на облачную инфраструктуру.
Укрепляет возможности Microsoft по защите от более изощренных фишинговых атак и вредоносного контента в электронной почте, календаре, Teams и SharePoint. Расширенные возможности обнаружения охватывают детекцию аномалий в сервисах M365 и обнаружение скомпрометированных учетных записей Office 365.

- **Обеспечивайте непрерывность бизнеса** с помощью многоуровневого подхода.
- **Сохраняйте постоянную защиту** независимо от устройства доступа или пользователя.
- **Упрощайте рабочие процессы** с помощью унифицированного управления безопасностью конечных точек и облачных сервисов.
- **Развертывайте решение легко** благодаря бесшовной интеграции из облака в облако. Нет необходимости в промежуточном программном обеспечении или настройке.
- **Блокируйте вредоносный контент,** включая вредоносное программное обеспечение, программы-вымогатели и попытки фишинга.
- **Выявляйте даже самое сложное вредоносное ПО** путем запуска и анализа подозрительных файлов в "песочнице".
- **Отслеживайте, были ли взломаны учетные записи вашей компании.**

WITHSECURE ELEMENTS
VULNERABILITY MANAGEMENT

Отслеживайте и управляйте уязвимостями информационных активов.
Vulnerability Management идентифицирует активы вашей организации, точно определяет их уязвимые места. Сведите к минимуму поверхность атаки и риск. Найдите свои внутренние и внешние слабые места раньше, чем кто-либо другой.

- **Следите за полной картиной** и точным отображением всех информационных активов, а также теневых IT-систем.
- **Уменьшайте поверхность атаки** путем выявления уязвимостей в системах, программном обеспечении и неправильной конфигурации.
- **Минимизируйте риск** вследствие применения превентивных мер до возникновения любых инцидентов.
- **Оптимизируйте рабочие процессы** с помощью автоматического сканирования по расписанию. Расставляйте приоритеты обновления с помощью встроенной системы оценки рисков.
- **Расширяйте возможности сканирования уязвимостей** на удаленных устройствах вне вашей сети с помощью агента на конечной точке Windows.
- **Поддерживайте непрерывность бизнеса** с помощью стандартных и кастомизированных отчетов о состоянии вашей безопасности и рисках.
- **Обеспечивайте соответствие требованиям PSI DSS, GDPR** и другим стандартам с помощью автоматического сканирования информационных активов на соответствие этим стандартам.

WITHSECURE ELEMENTS
CLOUD SECURITY POSTURE MANAGEMENT

Поймите и защитите свою облачную инфраструктуру.
Cloud Security Posture Management сканирует среды AWS и Azure на соответствие настроек лучшим отраслевым практикам. Вдобавок решение предоставляет указания по устранению выявленных проблем безопасности. Благодаря уже имеющемуся набору Elements вы можете защитить свои гибридные и облачные среды, установить защиту 24/7, закрывать проблемы безопасности в нескольких облаках и практиковать управление рисками.

- **Эффективно выявляйте неправильные конфигурации** и получайте указания по их устранению.
- **Получайте различные взгляды на вашу систему безопасности:** просматривайте результаты, сгруппированные по отдельным сканированиям, учетным записям или правилам.
- **Наслаждайтесь комплексным решением для кибербезопасности,** где вы можете прогнозировать, предотвращать, выявлять и реагировать на угрозы на одной платформе.
- Предоставьте аудиторам и регуляторным органам **гарантии надлежащего уровня рисков облачной безопасности и средств контроля управления.**
- **Отслеживайте и проактивно реагируйте** на уязвимости облачной конфигурации и возникающие риски.
- **Предотвращайте атаки** с помощью правил CSPM, основанных на методах злоупотребления неправильной конфигурацией, которые консультанты WithSecure видели и исправили во многих средах клиентов.

WITH secure | bakotech

+380 44 273 3333

www.bakotech.com

withsecure@bakotech.com

Бульвар В. Гавела, 6з, 6 этаж,
Киев, 03124, Украина