PICUS | bako tech

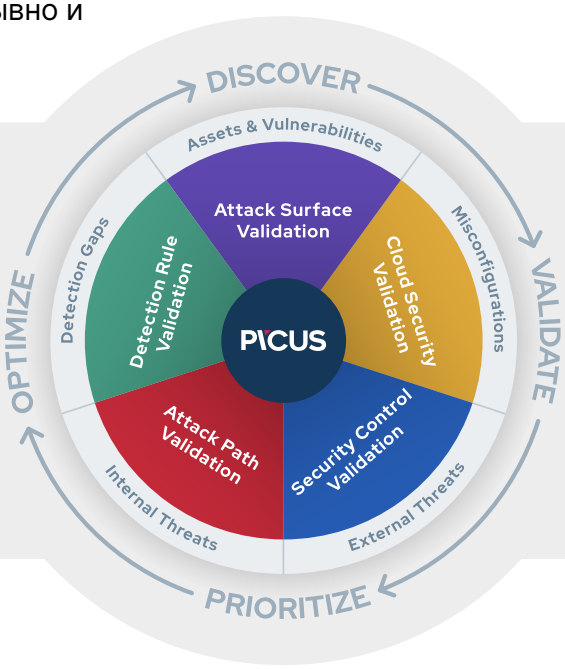
PICUS COMPLETE SECURITY VALIDATION PLATFORM

THE PICUS COMPLETE SECURITY CONTROL VALIDATION PLATFORM

Платформа Picus Complete Security Control Validation Platform — это решение для моделирования взлома и атаки (BAS), которое автоматически, непрерывно и последовательно проверяет, измеряет и помогает повысить киберустойчивость в режиме 24/7.

ОСНОВНЫЕ ФУНКЦИИ:

- Измерение и оптимизация защиты, обеспечиваемой существующими средствами контроля безопасности;
- Обнаружение и устранение путей атак на критически важные системы и пользователей;
- Оптимизация возможностей обнаружения и реагирования для скорейшего устранения атак.



КАК ПЛАТФОРМА PICUS УКРЕПЛЯЕТ ВАШУ БЕЗОПАСНОСТЬ

Обеспечивает целостную и непрерывную картину

В любой момент вы можете понять, насколько ваша организация готова к защите от новейших угроз, проверив эффективность защиты в ключевых областях.

Ускоряет устранение пробелов в системе безопасности

Получите информацию, необходимую не только для проактивного выявления пробелов в системе безопасности, но и для их устранения до того, как ими воспользуются противники.

Автоматизирует ручные процессы проверки

Устранение рисков безопасности на более ранних этапах благодаря автоматизации процессов ручной оценки и предоставлению команде возможности сосредоточиться на устранении недостатков, а не на их обнаружении.

Подтверждает готовность к угрозам и окупаемость инвестиций

Получите метрики и данные, необходимые для принятия ориентированных на угрозы решений на их основе, а также для демонстрации гарантий и ценности руководителям компаний и аудиторам.

Платформа Picus Complete Security Validation Platform предоставляет возможности, необходимые для автоматической, непрерывной и последовательной оценки уровня безопасности вашей организации.

Интеграция трех лицензируемых по отдельности продуктов — Security Control Validation, Attack Path Validation и Detection Rule Validation — позволяет проактивно обнаруживать неизвестные риски, проверять эффективность средств контроля и процессов, определять приоритеты пробелов и оптимизировать защиту в режиме 24/7.

SECURITY CONTROL VALIDATION

Моделируйте реальные киберугрозы, чтобы выявить недостатки в предотвращении и обнаружении и получить действенные рекомендации по их быстрому и эффективному устранению.

КАК SECURITY CONTROL VALIDATION ПОВЫШАЕТ УРОВЕНЬ БЕЗОПАСНОСТИ

Тестирует средства контроля безопасности непрерывно, 24/7

Picus выявляет слабые места в предотвращении и обнаружении угроз, оценивая эффективность ваших средств защиты с помощью постоянно запланированных симуляций.

Проверяет готовность к борьбе с новейшими угрозами

Благодаря богатой библиотеке угроз, ежедневно обновляемой экспертами по наступательной безопасности, Picus проверяет вашу защиту от текущих и новых методов атак.

Оптимизирует возможности предотвращения и обнаружения

Для достижения оптимальной защиты с помощью ваших средств безопасности Picus предоставляет простые в применении сигнатуры предотвращения и правила обнаружения.

Работает с MITRE ATT&CK

Picus сопоставляет результаты оценки с MITRE ATT&CK Framework, что позволяет визуализировать охват угроз и определить приоритетность устранения пробелов.

Подтверждает ценность инвестиций

Предоставляя метрики в режиме реального времени вместе с общим баллом безопасности для вашей организации, Picus помогает вам измерить эффективность и доказать ценность инвестиций.

Повышает эффективность и результативность SOC

Picus автоматизирует ручные процессы оценки и проектирования, снижая усталость и помогая командам безопасности работать более слаженно.

ATTACK PATH VALIDATION

Picus Attack Path Validation (APV) позволяет командам безопасности автоматически обнаруживать и визуализировать шаги, которые может предпринять уклоняющийся злоумышленник с первоначальным доступом ко внутренней сети, чтобы скомпрометировать критически важные системы и пользователей. Моделируя действия реального противника, этот инструмент выявляет пути атак, представляющие наибольший риск, и дает информацию для их устранения.

Этот простой в использовании инструмент, основанный на Picus Intelligent Adversary Decision Engine, моделирует действия реального противника, чтобы определить кратчайшие пути атаки и подтвердить, что они представляют реальный риск.

КАК ATTACK PATH VALIDATION ПОВЫШАЕТ БЕЗОПАСНОСТЬ ВАШЕЙ ВНУТРЕННЕЙ СЕТИ

Выявляет и проверяет пути к критическим ресурсам

Picus APV определяет кратчайший путь, по которому злоумышленники могут пройти для компрометации вашей Active Directory. После этого он моделирует действия реальных противников, чтобы убедиться в актуальности угрозы.

Обеспечивает целостное представление о внутренней поверхности атаки

В отличие от ручных тестов «красной команды», которые проводятся с одной начальной точки доступа, Picus APV обеспечивает более широкую перспективу, позволяя проводить моделирование из нескольких областей вашей сети и получать результаты за считанные минуты, а не недели.

Помогает определить приоритетность уязвимостей и неправильных конфигураций

Определите объекты в сети, где сходятся многочисленные пути атак, и определите приоритеты для устранения уязвимостей и неправильных конфигураций в этих точках, чтобы обеспечить максимальный эффект для безопасности.

Проверяет эффективность средств контроля безопасности

Используйте Picus APV, чтобы определить, настроена ли система безопасности конечных точек вашей организации на обнаружение и предотвращение сетевых латеральных перемещений и других методов уклонения, используемых противниками.

Автоматизирует ручной анализ

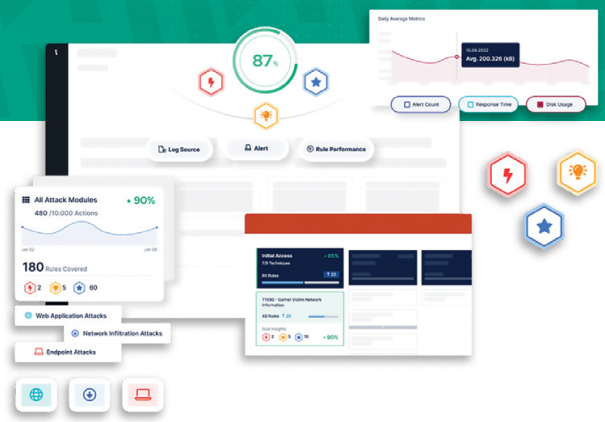
Сэкономьте время и деньги, автоматизировав тестирование безопасности, и убедитесь, что при проведении ручного тестирования оно принесет лучшие результаты и выгоду.

Усиливает безопасность Active Directory

APV устраняет слабые места, которые могут позволить злоумышленнику получить привилегии администратора домена и получить контроль над всеми пользователями, системами и данными в вашей среде.

DETECTION RULE VALIDATION

Picus Detection Rule Validation оптимизирует возможности обнаружения угроз и реагирования на них, а также сокращает усилия, необходимые для поддержания и оптимизации работы правил обнаружения.



КАК DETECTION RULE VALIDATION УКРЕПЛЯЕТ ВАШУ БАЗУ ПРАВИЛ

Повышает эффективность SOC

Повысьте уверенность команды SOC в том, что нужные правила установлены и что оповещения о критических инцидентах безопасности срабатывают.

Проверяет эффективность правил обнаружения

Подтверждение эффективности существующих и новых правил на основе охвата журналов, частоты оповещений и показателей производительности.

Обеспечивает проактивную проверку правил

Получите информацию об охвате угроз, точности и производительности правил обнаружения SIEM и EDR и дайте возможность командам SOC выполнять проактивную проверку правил.

Сосредотачивается на главном

Выделите покрытие обнаружения на основе важных для организации реальных угроз и освободите инженеров SOC от утомительных задач, чтобы они могли сосредоточиться на главном.

Сокращает усилия по поддержке и оптимизации

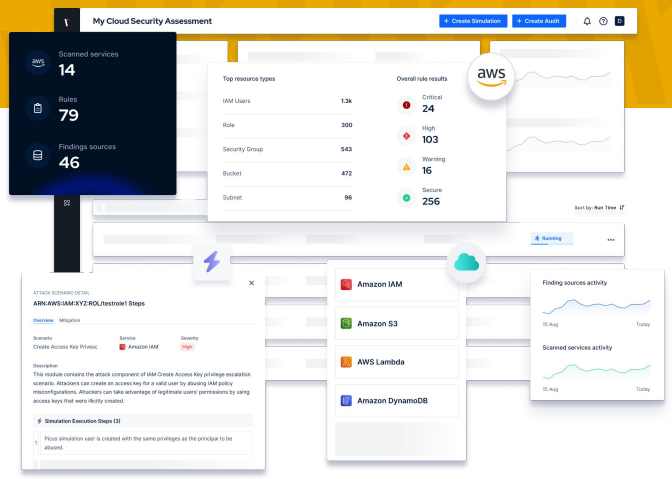
Сократите время разработки системы обнаружения вновь появляющихся угроз с нескольких часов до нескольких минут.

Оптимизирует обнаружение угроз и реагирование на них

Получите целостное представление о возможностях обнаружения угроз и реагирования на них и ускорьте внедрение MITRE ATT&CK Framework.

CLOUD SECURITY VALIDATION

Picus Cloud Security Validation (CSV) помогает командам безопасности облегчить управление безопасностью облачных сред. Он выявляет в подвергающихся риску активах распространенные неправильные конфигурации и моделирует реальные атаки для оценки эффективности средств контроля и последствий нарушений.



PICUS CLOUD SECURITY VALIDATION ДЛЯ AWS ПОМОГАЕТ БЫСТРО ВЫЯВЛЯТЬ И УСТРАНЯТЬ УЯЗВИМОСТИ В ПРОАКТИВНОМ РЕЖИМЕ БЛАГОДАРЯ:

Аудиту основных служб AWS

Сканируя четырнадцать основных сервисов AWS, Picus CSV выявляет критические ошибки в конфигурации, такие как чрезмерные привилегии, открытые бакеты S3, неиспользуемые ресурсы, криптографические сбои и многое другое.

Моделированию атак в вашей среде

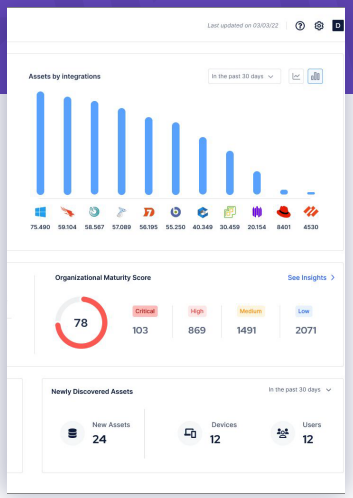
Чтобы проверить влияние любых выявленных сценариев повышения привилегий, Picus CSV предоставляет возможность моделировать атаки в среде AWS. Все действия выполняются с использованием вновь созданных пользователей и откатываются по завершении оценки.

Обнаружению сценариев повышения привилегий

Если злоумышленникам удастся получить доступ к вашей среде AWS, они, скорее всего, попытаются получить доступ к критически важным системам путем повышения привилегий. Чтобы выявить чрезмерно открытые политики IAM, Picus CSV собирает ресурсы AWS и моделирует атаки в симуляторе локальных политик.

ATTACK SURFACE VALIDATION

Picus Attack Surface Validation (ASV) улучшает видимость пользователей, узлов, систем и приложений в вашей сети, помогая повысить осведомленность о безопасности и определить приоритетность рисков.



СОБИРАЯ ДАННЫЕ ОБ АКТИВАХ ИЗ РАЗЛИЧНЫХ ИСТОЧНИКОВ И ПРЕДСТАВЛЯЯ ИХ ДЛЯ АНАЛИЗА ЧЕРЕЗ ЕДИНОЕ ПРОСТРАНСТВО, PICUS ASV ОБЕСПЕЧИВАЕТ ПОНИМАНИЕ И БОГАТЫЙКОНТЕКСТ, НЕОБХОДИМЫЕ ДЛЯ:

- **Получения более полного представление об инвентаризации активов**
- **Выявления пробелов в политике и неправильной конфигурации**
- **Обнаружения несоответствующих устройств с недостаточным уровнем защиты**
- **Определения приоритетности управления уязвимостями в зависимости от важности активов**
- **Ускорения анализа уведомлений безопасности**

СВЯЖИТЕСЬ С НАМИ, ЧТОБЫ ПОЛУЧИТЬ ДОПОЛНИТЕЛЬНУЮ ИНФОРМАЦИЮ О РЕШЕНИЯХ:

picus@bakotech.com || picussecurity.bakotech.com