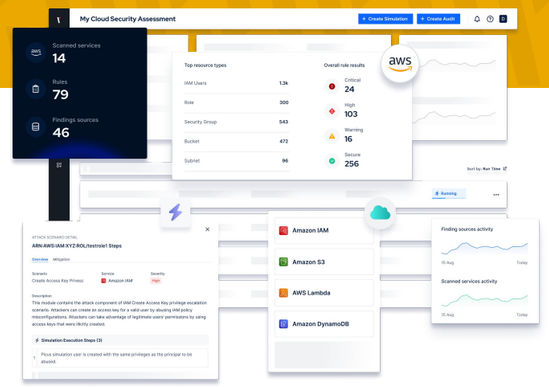
CLOUD SECURITY VALIDATION

Picus Cloud Security Validation (CSV) допомагає командам безпеки полегшити управління безпекою хмарних середовищ. Він виявляє в активах, що наражаються на ризик, поширені неправильні конфігурації та моделює реальні атаки для оцінки ефективності засобів контролю та наслідків порушень.



PICUS CLOUD SECURITY VALIDATION ДЛЯ AWS ДОПОМАГАЄ ШВИДКО ВИЯВЛЯТИ Й УСУВАТИ ВРАЗЛИВОСТІ В ПРОАКТИВНОМУ РЕЖИМІ ЗАВДЯКИ:

Аудиту основних служб AWS

Скануючи чотирнадцять основних сервісів AWS, Picus CSV виявляє критичні помилки в конфігурації, як-от надмірні привілеї, відкриті бакети S3, невикористовувані ресурси, криптографічні збої та багато іншого.

Моделюванню атак у вашому середовищі

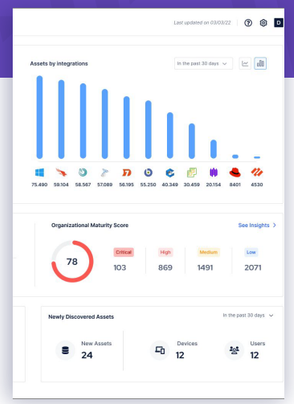
Щоб перевірити вплив будь-яких виявлених сценаріїв підвищення привілеїв, Picus CSV надає можливість моделювати атаки в середовищі AWS. Усі дії виконуються з використанням новостворених користувачів і відкочуються після завершення оцінювання.

Виявленню сценаріїв підвищення привілеїв

Якщо зловмисникам вдасться отримати доступ до вашого середовища AWS, вони, найімовірніше, спробують отримати доступ до критично важливих систем шляхом підвищення привілеїв. Щоб виявити надмірно відкриті політики IAM, Picus CSV збирає ресурси AWS і моделює атаки в симуляторі локальних політик.

ATTACK SURFACE VALIDATION

Picus Attack Surface Validation (ASV) покращує видимість користувачів, вузлів, систем і додатків у вашій мережі, допомагаючи підвищити обізнаність про безпеку та визначити пріоритетність ризиків.



ЗБИРАЮЧИ ДАНІ ПРО АКТИВИ З РІЗНИХ ДЖЕРЕЛ І НАДАЮЧИ ЇХ ДЛЯ АНАЛІЗУ ЧЕРЕЗ ЄДИНИЙ ПРОСТІР, PICUS ASV ЗАБЕЗПЕЧУЄ РОЗУМІННЯ І БАГАТИЙ КОНТЕКСТ, НЕОБХІДНІ ДЛЯ:

- **Отримання більш повного уявлення про інвентаризацію активів**
- **Виявлення прогалин у політиці та неправильної конфігурації**
- **Виявлення невідповідних пристроїв із недостатнім рівнем захисту**
- **Визначення пріоритетності управління вразливостями залежно від важливості активів**
- **Прискорення аналізу повідомлень безпеки**

ЗВ'ЯЖІТЬСЯ З НАМИ, ЩОБ ОТРИМАТИ ДОДАТКОВУ ІНФОРМАЦІЮ ПРО РІШЕННЯ:

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

PICUS | bako tech®

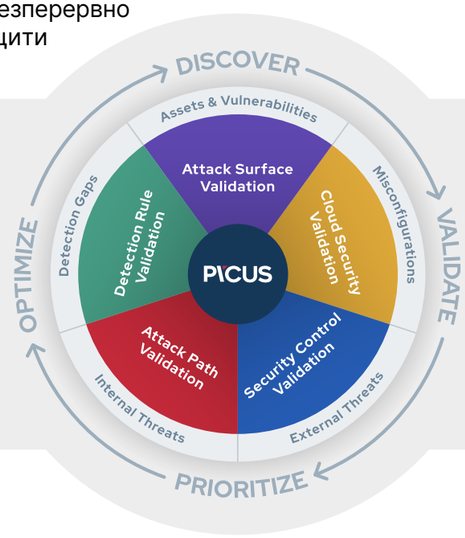
PICUS COMPLETE SECURITY VALIDATION PLATFORM

THE PICUS COMPLETE SECURITY CONTROL VALIDATION PLATFORM

Платформа Picus Complete Security Control Validation Platform — це рішення для моделювання злому й атаки (BAS), що автоматично, безперервно та послідовно перевіряє, вимірює та допомагає підвищити кіберстійкість у режимі 24/7.

ОСНОВНІ ФУНКЦІЇ:

- Вимірювання та оптимізація захисту, що забезпечується наявними засобами контролю безпеки;
- Виявлення та усунення шляхів атак на критично важливі системи і користувачів;
- Оптимізація можливостей виявлення і реагування для якнайшвидшого усунення атак.



ЯК ПЛАТФОРМА PICUS ЗМІЦНЮЄ ВАШУ БЕЗПЕКУ

Забезпечує цілісну і безперервну картину

У будь-який момент ви можете зрозуміти, наскільки ваша організація готова до захисту від новітніх загроз, перевіривши ефективність захисту в ключових сферах.

Прискорює усунення прогалин у системі безпеки

Отримайте інформацію, необхідну не тільки для проактивного виявлення прогалин у системі безпеки, а й для їх усунення до того, як ними скористаються противники.

Автоматизує ручні процеси перевірки

Усунення ризиків безпеки на більш ранніх етапах завдяки автоматизації процесів ручного оцінювання та наданню команді можливості зосередитися на усуненні недоліків, а не на їх виявленні.

Підтверджує готовність до загроз і окупність інвестицій

Отримайте метрики та дані, необхідні для ухвалення орієнтованих на загрози рішень на їх основі, а також для демонстрації гарантій і цінності керівникам компаній та аудиторам.

Платформа Picus Complete Security Validation Platform надає можливості, необхідні для автоматичного, безперервного та послідовного оцінювання рівня безпеки вашої організації.

Інтеграція трьох продуктів, що ліцензуються окремо, — Security Control Validation, Attack Path Validation і Detection Rule Validation — дає змогу проактивно виявляти невідомі ризики, перевіряти ефективність засобів контролю та процесів, визначати пріоритети прогалин і оптимізувати захист у режимі 24/7.

SECURITY CONTROL VALIDATION

Моделюйте реальні кіберзагрози, щоб виявити недоліки в запобіганні та виявленні й отримати дієві рекомендації щодо їх швидкого та ефективного усунення.

ЯК SECURITY CONTROL VALIDATION ПІДВИЩУЄ РІВЕНЬ БЕЗПЕКИ

Тестує засоби контролю безпеки безперервно, 24/7

Picus виявляє слабкі місця в запобіганні загрозам та їх виявленні, оцінюючи ефективність ваших засобів захисту за допомогою постійно запланованих симуляцій.

Перевіряє готовність до боротьби з новітніми загрозами

Завдяки багатій бібліотеці загроз, щодня оновлюваній експертами з наступальної безпеки, Picus перевіряє ваш захист від поточних і нових методів атак.

Оптимізує можливості запобігання та виявлення

Для досягнення оптимального захисту за допомогою ваших засобів безпеки Picus надає прості в застосуванні сигнатури запобігання і правила виявлення.

Працює з MITRE ATT&CK

Picus зіставляє результати оцінки з MITRE ATT&CK Framework, що дає змогу візуалізувати охоплення загроз і визначити пріоритетність усунення прогалин.

Підтверджує цінність інвестицій

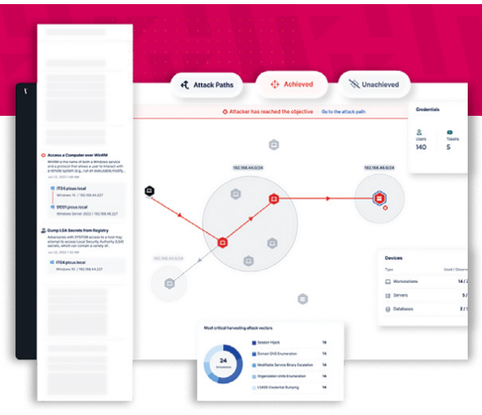
Надаючи метрики в режимі реального часу разом із загальним балом безпеки для вашої організації, Picus допомагає вам виміряти ефективність і довести цінність інвестицій.

Підвищує ефективність і результативність SOC

Picus автоматизує ручні процеси оцінювання і проєктування, знижуючи втому і допомагаючи командам безпеки працювати більш злагоджено.

ATTACK PATH VALIDATION

Picus Attack Path Validation (APV) дає змогу командам безпеки автоматично виявляти та візуалізувати кроки, які може зробити зловмисник, що ухиляється, з початковим доступом до внутрішньої мережі, щоб скомпрометувати критично важливі системи та користувачів. Моделюючи дії реального противника, цей інструмент виявляє шляхи атак, що становлять найбільший ризик, і дає інформацію для їхнього усунення.



Цей простий у використанні інструмент, заснований на Picus Intelligent Adversary Decision Engine, моделює дії реального супротивника, щоб визначити найкоротші шляхи атаки та підтвердити, що вони становлять реальний ризик.

ЯК ATTACK PATH VALIDATION ПІДВИЩУЄ БЕЗПЕКУ ВАШОЇ ВНУТРІШНЬОЇ МЕРЕЖІ

Виявляє та перевіряє шляхи до критичних ресурсів

Picus APV визначає найкоротший шлях, яким зловмисники можуть пройти для компрометації вашої Active Directory. Після цього він моделює дії реальних супротивників, щоб переконатися в актуальності загрози.

Забезпечує цілісне уявлення про внутрішню поверхню атаки

На відміну від ручних тестів «червоної команди», які проводяться з однієї початкової точки доступу, Picus APV забезпечує ширшу перспективу, даючи змогу проводити моделювання з декількох ділянок вашої мережі й отримувати результати за лічені хвилини, а не тижні.

Допомагає визначити пріоритетність вразливостей і неправильних конфігурацій

Визначте об'єкти в мережі, де сходяться численні шляхи атак, і визначте пріоритети для усунення вразливостей і неправильних конфігурацій у цих точках, щоб забезпечити максимальний ефект для безпеки.

Перевіряє ефективність засобів контролю безпеки

Використовуйте Picus APV, щоб визначити, чи налаштована система безпеки кінцевих точок вашої організації на виявлення і запобігання мережевим латеральним переміщенням та іншим методам ухилення, які використовують противники.

Автоматизує ручний аналіз

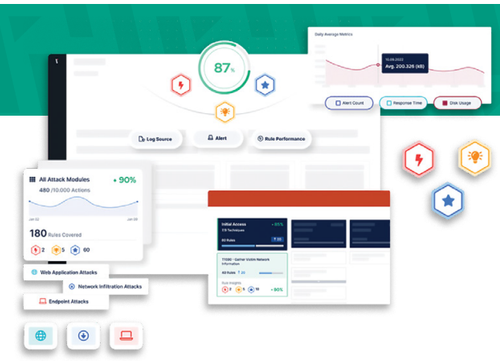
Заощаджуйте час і гроші, автоматизувавши тестування безпеки, і переконайтеся, що під час проведення ручного тестування воно принесе кращі результати та вигоду.

Посилює безпеку Active Directory

APV усуває слабкі місця, які можуть дозволити зловмиснику отримати привілеї адміністратора домену та мати контроль над усіма користувачами, системами та даними у вашому середовищі.

DETECTION RULE VALIDATION

Picus Detection Rule Validation оптимізує можливості виявлення загроз і реагування на них, а також зменшує зусилля, необхідні для підтримки та оптимізації роботи правил виявлення.



ЯК DETECTION RULE VALIDATION ЗМІЦНЮЄ ВАШУ БАЗУ ПРАВИЛ

Підвищує ефективність SOC

Підвищте упевненість команди SOC у тому, що потрібні правила встановлено, а сповіщення про критичні інциденти безпеки спрацьовують.

Перевіряє ефективність правил виявлення

Підтвердження ефективності наявних і нових правил на основі охоплення журналів, частоти сповіщень і показників продуктивності.

Забезпечує проактивну перевірку правил

Отримайте інформацію про охоплення загроз, точність і продуктивність правил виявлення SIEM і EDR і дайте можливість командам SOC виконувати проактивну перевірку правил.

Зосереджується на головному

Виділіть покриття виявлення на основі важливих для організації реальних загроз і звільніть інженерів SOC від виснажливих завдань, щоб вони могли зосередитися на головному.

Зменшує зусилля з підтримки та оптимізації

Скоротіть час розробки системи виявлення загроз, що знову з'являються, з декількох один до декількох хвилин.

Оптимізує виявлення загроз і реагування на них

Отримайте цілісне уявлення про можливості виявлення загроз і реагування на них та прискорте впровадження MITRE ATT&CK Framework.