

УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ В ЛОКАЛЬНОЙ ИНФРАСТРУКТУРЕ

*Всеохватывающий мониторинг.
Актуальное прогнозирование. Локальное управление.*

«Это локальное и универсальное решение Tenable позволяет мне в любое время приоритизировать киберриски и оценивать состояние корпоративной системы безопасности в соответствии с бизнес-целями»

— сотрудник ИБ медицинского учреждения

Из-за меняющегося ИТ-ландшафта и развивающихся киберугроз периодические сканирования и аудиты соответствия перестали эффективно защищать организации от современных кибератак. Для обеспечения корпоративной безопасности нужно решение для управления уязвимостями, которое позволит отслеживать всю поверхность атаки, измерять киберриски и эффективно управлять ими.

Tenable.sc+ — это лидирующая на рынке платформа управления уязвимостями нового поколения, предназначенная для локального развертывания и основанная на ведущей технологии Nessus. Благодаря продвинутой аналитике, настраиваемым дашбордам, отчетам и процессам Tenable.sc+ помогает эффективно управлять уязвимостями и сокращать риски для компании.

Функционал предсказательной приоритизации объединяет данные об уязвимостях и угрозах из множества источников, прогнозируя вероятность эксплойта той или иной уязвимости. Одновременно с этим оценивается критичность динамических активов в постоянно меняющейся среде. В результате можно видеть и приоритизировать уязвимости и связанные с ними наиболее важные активы. Эта полезная информация помогает защитить организацию от реальных атак, сказывающихся на бизнесе.

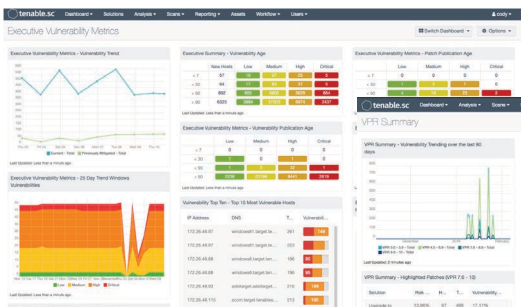


Рисунок 1: дашборды, отчеты, процессы и политики безопасности, которые тонко настраиваются в соответствии с конкретными потребностями бизнеса.

В Tenable.sc+ входят 350 готовых, но тонко настраиваемых дашбордов и шаблонов отчетов, которые позволяют мгновенно оценить соответствие требованиям ИБ, эффективность защиты и риски. Вы можете непрерывно измерять, анализировать и визуализировать эффективность программы ИБ с учетом важных для руководства приоритетных бизнес-целей и соответствующих настраиваемых политик безопасности.

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

- Непрерывный мониторинг**
 Непрерывно отслеживайте известные и выявляйте неизвестные активы и их уязвимости. Обнаруживайте угрозы и подозрительные изменения в сети до того, как они перерастут в атаку.
- Приоритизация активов и уязвимостей**
 Объединяйте данные об активах, их уязвимостях, киберразведку и аналитику и легко оценивайте риски. Это позволит быстро обнаруживать уязвимости и подверженные им критические активы, представляющие наибольший риск для бизнеса.
- Широкое и глубокое покрытие**
 Команда аналитиков Tenable Research тесно сотрудничает с ИБ-сообществом для выявления новейших уязвимостей и предоставления полезных сведений о них. Это помогает организациям оптимизировать свои процессы по оценке уязвимостей. Tenable обеспечивает самую обширную в отрасли поддержку базы CVE (более 67 тысяч уязвимостей) и настроек безопасности, что позволяет видеть все киберриски.
- Автоматизация процессов**
 Используйте задокументированный API и встроенные интеграции для импорта данных сторонних решений, автоматизации сканирования и распространения данных по ИТ-системам.

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

Управляйте своими данными по-своему

Tenable.sc+ — это одно из лучших решений для управления уязвимостями. Его можно развернуть в локальной или гибридной среде, что позволит компании управлять данными нужным для нее способом в соответствии с самыми жесткими требованиями к развертыванию и сокращать при этом киберриски.

Комплексная оценка уязвимостей

Tenable.sc+ обеспечивает комплексный мониторинг всей поверхности атаки. Решение использует сенсоры Nessus — комбинацию активных сканеров, агентов, пассивного мониторинга сети и интеграций с CMDB — для максимального охвата при сканировании инфраструктуры и устранения «слепых пятен». Сочетания разных сенсоров данных позволяет отслеживать и оценивать как известные, так и неизвестные активы и уязвимости.

Пассивное обнаружение уязвимостей

Выйдете за рамки сканирования в определенный момент времени и устраняйте слепые пятна с помощью пассивного обнаружения уязвимостей. Этот функционал выявляет активы и анализирует сетевой трафик, обеспечивая комплексный мониторинг.

Приоритизация уязвимостей с учетом их реального риска

Tenable.sc+ объединяет данные об уязвимостях, угрозах и их аналитику для простой оценки рисков. Благодаря этому можно приоритизировать уязвимости и порядок их исправления. Вы можете быстро оценивать риски и выявлять уязвимости, которые представляют наибольшую угрозу кибербезопасности вашей организации.

Упрощенное управление уязвимостями

Интуитивно понятные отчеты, визуализация данных на дашбордах, простой интерфейс Tenable.sc+ — все это значительно упрощает выполнение стандартных задач, таких как настройка сканирования, запуск оценки уязвимостей и анализ полученных результатов. Готовые шаблоны сканирования, проверки конфигурации и соответствия на основе лучших практик аудита помогут защитить организацию, прилагая меньше усилий, чем когда либо. Настройте отчетность и аналитику с помощью встроенных дашбордов, или с чистого листа создайте свой собственный, который бы отвечал потребностям организации.

Оценка критичности активов

Оценка критичности активов (Asset Criticality Rating, ACR), доступная в Tenable.sc+, позволяет определить их приоритетность с помощью индикаторов ценности и значимости для бизнеса. Вместе оценка критичности активов и предсказательная приоритизация обеспечивают индивидуальный подход к управлению уязвимостями, показывая, на какие уязвимости и активы следует обратить первостепенное внимание.

Оптимизированная проверка соответствия

Оцените соответствие отраслевым и регуляторным требованиям, а также сформируйте соответствующие отчеты с помощью готовых проверок, метрик и проактивных алертов о нарушении стандартов ИБ, таких как CERT, NIST, DISA STIG, DHS CDM, FISMA, PCI DSS, HIPAA/HITECH и др.

Команда аналитиков Tenable Research

За Tenable.sc+ стоит команда Tenable Research, которая предоставляет первоклассный анализ киберрисков, аналитические инсайты, алерты и рекомендации. Tenable Research часто выпускает проверки на наличие уязвимостей, исследования 0-day угроз и рекомендации по безопасной настройке систем, которые сразу же доступны для усиления защиты вашей организации.

Tenable.sc Director

Tenable.sc Director — дополнение, которое позволяет централизованно, а значит проще просматривать и контролировать риски и получить широкомасштабный мониторинг по всем консолям Tenable.sc.

Встроенные интеграции, задокументированный API и интегрированный SDK

Tenable.sc+ предлагает встроенные интеграции для сканирования с использованием учетных данных, а также с SIEM-, SOAR-, тикет-, патчинг-системами и другими дополнительными решениями. Это помогает легко оптимизировать процесс управления уязвимостями. Полный список интеграций можно найти здесь. Кроме того, вы можете легко создавать собственные интеграции с Tenable.sc+ благодаря его полностью задокументированному API. Использование этих инструментов не требует дополнительной платы — так вы сможете извлечь максимальную ценность из ваших конкретных сценариев управления уязвимостями.

Тайгер Оптикс — авторизованный дистрибьютор Tenable в России и СНГ

Свяжитесь с нами: sales@tiger-optics.ru

<https://www.tiger-optics.ru/>

