

Netwrix Auditor for Network Devices

Знайте, что происходит в ваших сетевых устройствах

Netwrix Auditor for Network Devices обеспечивает полный контроль устройств Cisco, Fortinet, Palo Alto, SonicWall, Juniper, Cisco Meraki, HPE Aruba и Pulse Connect Secure. **Интеллектуальная система безопасности** позволяет быстро обнаруживать и исследовать **угрозы безопасности вашего периметра**, такие как несанкционированные изменения конфигураций, подозрительные попытки входа в систему и угрозы сканирования. Он также предоставляет подробную информацию о неисправностях оборудования и удаленном доступе к вашей сети.



ОБНАРУЖИВАЙТЕ УГРОЗЫ БЕЗОПАСНОСТИ

Выявляйте и исследуйте неправильные изменения конфигурации, подозрительные попытки входа в систему, угрозы сканирования и многое другое - до того, как они приведут к нарушениям безопасности сети или сбоям в работе.



ПРОХОДИТЕ АУДИТ С НАИМЕНЬШИМИ ЗАТРАТАМИ

Сократите время подготовки к аудиту, предоставив убедительные доказательства, подтверждающие, что ваши средства контроля безопасности работают должным образом, и с легкостью ответьте на специальные вопросы аудиторов.



ПОВЫШАЙТЕ ПРОДУКТИВНОСТЬ ИТ-КОМАНД

Сведите к минимуму время и усилия, затрачиваемые на регулярный мониторинг активности сетевых устройств, расследование инцидентов и регулярную отчетность перед руководством.



ОТЗЫВ КЛИЕНТА

«Мне нравятся отчеты! Продукт соответствует одному из моих требований DoD DFAR по мониторингу сеансов удаленного доступа. В журнале отображается вся активность VPN с моего Cisco ASA. Хорошая работа, ребята!»

Майкл Недбал, главный специалист по информационной безопасности,
Makai Ocean Engineering, Inc.

Основные возможности Netwrix Auditor for Network Devices



АУДИТ ВХОДОВ В СИСТЕМУ

Следите за успешными и неудачными входами в свои сетевые устройства, включая вход через VPN. Выявляйте подозрительную активность и своевременно реагируйте, чтобы предотвратить нарушения безопасности.



АУДИТ ИЗМЕНЕНИЙ КОНФИГУРАЦИИ

Легко обнаруживайте изменения в конфигурации ваших сетевых устройств и подозрительную активность, которая снижает безопасность периметра. Привлекайте людей к ответственности за их действия.



МОНИТОРИНГ ОБОРУДОВАНИЯ

Полный контроль работы оборудования позволяет быстро обнаружить неисправности, определить основную причину и принять соответствующие меры для обеспечения стабильной работы сети.



ОПОВЕЩЕНИЯ О КРИТИЧЕСКИ ВАЖНЫХ СОБЫТИЯХ

Получайте уведомления о необычных изменениях, подозрительных попытках входа в систему, высоком трафике данных, угрозах сканирования и проблемах с оборудованием.



ИНТЕРАКТИВНЫЙ ПОИСК

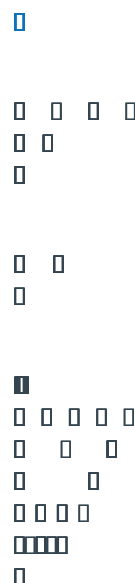
Быстро определяйте основную причину инцидента, такую как отключение сетевого устройства или несанкционированный сброс пароля на маршрутизаторе, путем сортировки вашего контрольного журнала и точной настройки запросов с помощью Google-подобного поиска.



ОТЧЕТЫ О СООТВЕТСТВИИ ТРЕБОВАНИЯМ ИБ

Сократите время, необходимое для подготовки к соблюдению нормативных требований, с помощью готовых отчетов. Быстро предоставляйте аудиторам доказательства того, что вы знаете, что происходит вокруг ваших сетевых устройств, и контролируете сеансы входа в систему.

NETWRIX AUDITOR FOR NETWORK DEVICES



RESTFUL API

