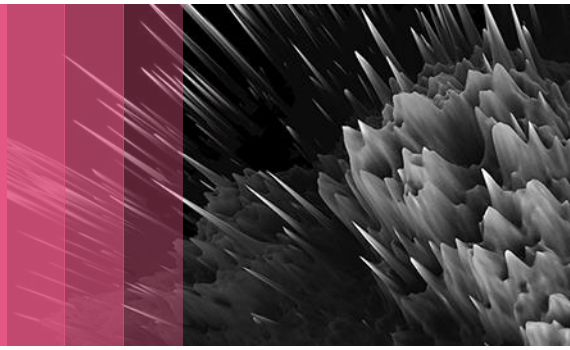
SECURITY CHECKUP

THREAT ANALYSIS REPORT



Корпоративная сеть открывает доступ к ценной конфиденциальной информации компании. Информации, которая ни в коем случае не должна попасть в чужие руки. Но можете ли вы быть уверены, что нет никаких скрытых опасностей и сюрпризов, угрожающих целостности и безопасности ценных ресурсов вашей компании? Особенно в отсутствии необнаруживаемого вредоносного ПО, бэкдоров, утечек данных и других дыр в безопасности. Раннее обнаружение скрытых угроз позволит вам немедленно отреагировать на возникающие риски и повысить безопасность корпоративных данных. С Check Point вы можете легко выявить риски, угрожающие вашей организации.

Check Point Security Checkup — это инструмент, позволяющий обнаружить риски и угрозы во всей вашей сети. По итогам обследования мы предоставим вам подробный отчет с анализом обнаруженных угроз. Наши эксперты будут вашими советниками и помогут проанализировать обнаруженные инциденты, а также дадут рекомендации по защите от подобных угроз.

ПОЛНЫЙ НАБОР РИСКОВ БЕЗОПАСНОСТИ

Check Point Security Checkup покрывает весь спектр рисков безопасности:

- Веб-приложения и веб-сайты сомнительного характера, используемые сотрудниками: пиринговые сети, облачные файловые хранилища, прокси и анонимайзеры, вредоносные сайты и многое другое.
- Анализ угроз, включающий компьютеры, инфицированные ботами, вирусами, неизвестным вредоносным ПО (атаки «нулевого дня» и атаки, не обнаруживаемые традиционными антивирусными решениями).
- Эксплуатацию уязвимостей серверов и компьютеров компании, являющиеся целью возможных атак.
- Конфиденциальные данные, отправленные за пределы организации по email или через веб.
- Анализ полосы пропускания и идентификацию наиболее ресурсоемких приложений и веб-сайтов: кто и каким образом более всего загружал сеть.
- *Для существующих заказчиков Check Point, использующих централизованное управление:* Проверка политики безопасности на соответствие требованиям регуляторов и лучшим практикам, включая индустриальные стандарты PCI, HIPAA, ISO, и другие.

Отчет Security Checkup включает рекомендации, помогающие понять риски и способы защиты от них.

ОЦЕНИТЕ РИСКИ БЕЗОПАСНОСТИ ВАШЕЙ ОРГАНИЗАЦИИ

ОТЧЕТ ВКЛЮЧАЕТ:

- **Компьютеры, инфицированные вредоносным ПО**
- **Доступ к высокорисковым приложениям и веб-сайтам**
- **Эксплуатацию уязвимостей и атаки на вашу сеть**
- **Инциденты с утечкой данных**
- **Рекомендации по защите сети от рисков**

НИКАКОГО РИСКА ДЛЯ СЕТИ

Обследование сети посредством Security Checkup предусматривает установку шлюза безопасности Check Point внутри сети для инспекции проходящего трафика. При этом шлюз не устанавливается «в разрыв», что не требует изменения конфигурации сети и позволяет избежать сбоев и простоев в работе сети. Вместо этого инспектируется копия трафика за счет подключения к соответствующему устройству Test Access Point (TAP) или порту зеркалирования (Mirror Port, так же известен как Span Port) на сетевом коммутаторе. Подобный подход полностью исключает проблемы, характерные для подключения «в разрыв», поскольку инспектируется только копия трафика. Поскольку через порт зеркалирования трафик в сеть не отправляется, такое подключение легко настраивается и не несет угрозу простоя или отказа в работе сети.

ОБСЛЕДОВАНИЕ РЕАЛЬНОЙ СЕТИ

Любая организация может участвовать в программе Security Checkup независимо от того, использует ли она решения Check Point или нет. Наши эксперты по безопасности проводят анализ у вас на сайте. Он состоит из 4 основных шагов:

1. **Установка шлюза безопасности Check Point** — Эксперт по безопасности настраивает шлюз для проведения обследования. Затем активируются необходимые программные блейды. Могут быть включены Application Control (контроль приложений), URL Filtering (URL фильтрация), IPS (предотвращение атак), Anti-Bot (антибот), Anti-Virus (антивирус), Threat Emulation (эмуляция угроз), DLP, (утечка данных), Identity Awareness (идентификация пользователей), SmartEvent (корреляция событий) и другие.
2. **Инспекция сетевого трафика** — Устройство устанавливается у вас в компании. Будучи подключенным к сети оно начинает анализировать сетевой трафик. Для сбора достаточного количества информации мы рекомендуем дать ему поработать как минимум неделю. Более длительный срок анализа даст еще более хорошие результаты.
3. **Анализ результатов** — После отключения устройства от сети эксперт анализирует результаты и формирует отчет Security Checkup.
4. **Отчет об обнаруженных рисках** — Эксперт по безопасности представит вам важные моменты, идентифицирующие слабые места вашей сети, обнаруженные во время тестирования. Затем вы узнаете о современных технологиях и решениях, которые наилучшим образом подойдут для защиты вашей сети от обнаруженных угроз.

ЧТО ЭТО ДАЕТ ВАМ?

- Лучшая осведомленность о рисках в вашей сети.
- Идентификация и приоритизация узких мест в безопасности, требующих улучшений.
- Представление о последних технологических новинках, покрывающих все аспекты информационной безопасности

ЗАРЕГИСТРИРУЙТЕСЬ НА SECURITY CHECKUP

Для проведения обследования Security Checkup, обратитесь к вашему локальному представителю Check Point или зарегистрируйтесь на:

checkpoint.com/securitycheckup

ИНСПЕКЦИЯ ЗЕРКАЛИРУЕМОГО ТРАФИКА ГАРАНТИРУЕТ НЕВМЕШАТЕЛЬСТВО В РАБОТУ СЕТИ