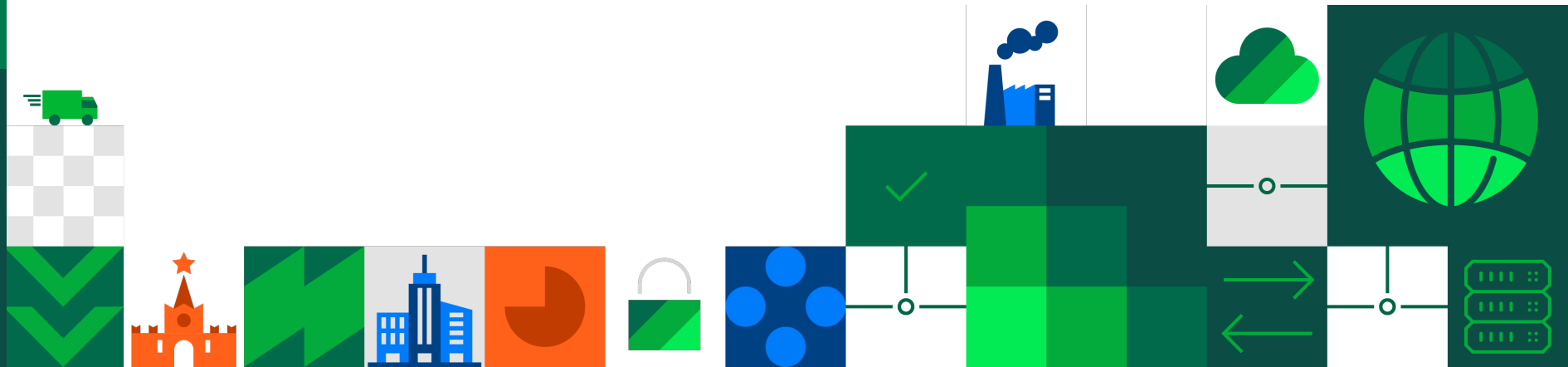
КОД безопасности

Технологические партнерства, или как получить максимум от NGFW



КОД безопасности

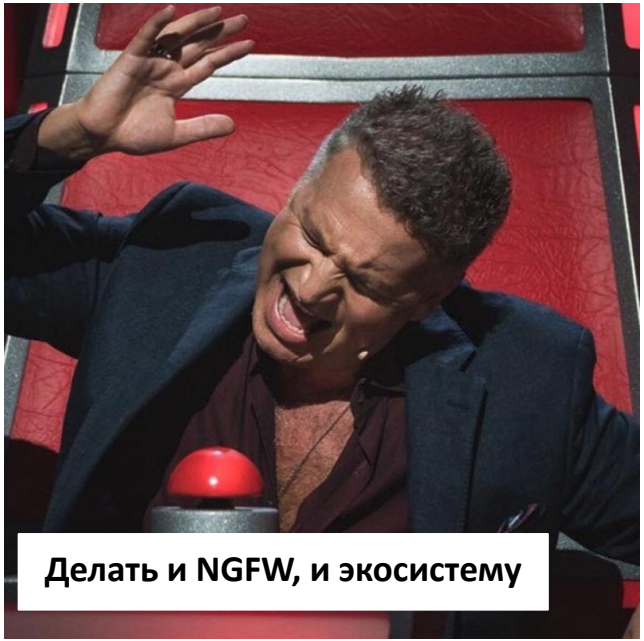
После ухода иностранных вендоров есть два тренда

Вендоры по ИБ

КОД безопасности

После ухода иностранных вендоров есть два тренда

Вендоры по ИБ



КОД безопасности

Выбор российских вендоров

Развитие продуктов вне NGFW

Недостаток – оттягивание ресурсов от развития NGFW

Концентрация только на NGFW

Недостаток – слабая зрелость для крупных заказчиков

Поиск технологических партнерств

Использование продуктов и сервисов партнеров в совокупности с NGFW позволяет получить набор функций, к которому привыкли крупные заказчики

КОД безопасности

КиберАльянс

Многофакторная аутентификация

MULTIFACTOR
Avanpost
Аладдин
КОМПАНИЯ ИНДИД
КОМПАНИЯ АКТИВ

Удаленный доступ

iOS
MacOS
АВРОРА

Комплаенс-контроль

Континент ZTN клиент
Сакура

Защита виртуализации

vGate

Планируются в ближайшее время

Анализ правил

EFROS DEFENCE OPERATIONS
Нетхаб
SPACE-BIT

Балансировка нагрузки

ЦИФРОВЫЕ РЕШЕНИЯ

Песочницы

positive technologies
AVSOFT
kaspersky

Индикаторы компрометации

kaspersky
Security Vision
CyberThreatTech
R-Vision
BI.ZONE

КОД безопасности

Многофакторная аутентификация

Многофакторная аутентификация

MULTIFACTOR Avanpost Аладдин КОМПАНИЯ ИНДИД КОМПАНИЯ АКТИВ

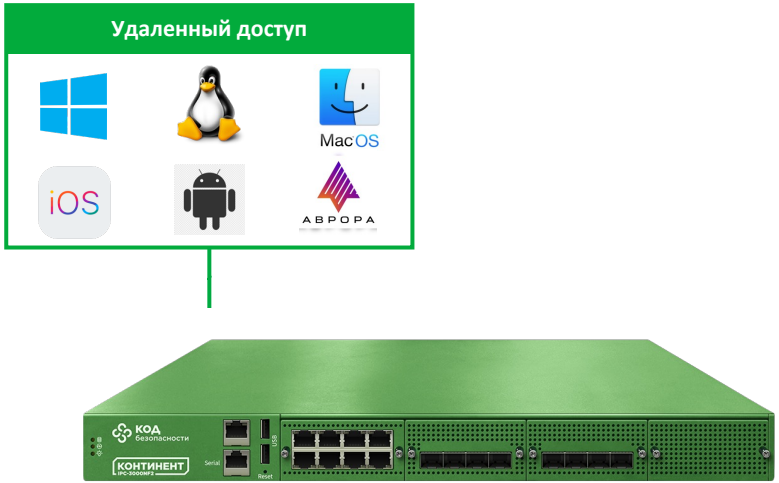
Взлом пароля – один из основных методов хакеров для проникновения в сеть. MFA значительно усложняет этот процесс

Результат:

- Снижение вероятности инцидентов ИБ, связанных с проникновением злоумышленника в корпоративную сеть через удаленных пользователей

Пример реализации интеграции NGFW с MFA

Удаленный доступ



Пример реализации удаленного доступа

Результат:

- Безопасная удаленная работа пользователей

Преимущества:

- Шифрование ГОСТ VPN
- Возможность проверки трафика удаленных пользователей механизмами NGFW
- Мультиплатформенные VPN клиенты
- Управление пользовательским соединением

Комплаенс-контроль

Пример реализации интеграции с САКУРА

Комплаенс-контроль

Континент ZTN клиент

Сакура

ПК соответствуют установленной политике безопасности → Доступ разрешен

ПК НЕ соответствуют установленной политике безопасности → Доступ запрещен или прерывается

Результат:

- Снижение инцидентов ИБ, связанных с компрометацией удаленных пользователей
- Реализация архитектуры ZTNA

Защита виртуализации

Результат:

- Снижение инцидентов ИБ, связанных с проникновением злоумышленника через виртуальные сети

Преимущества:

- Отсутствие зависимости от производительности в виртуальных средах
- Микросегментация сервисов
- Интеграция со средой виртуализации
- Гибкость миграции в виртуальных сетях

Интеграция vGate и Континент 4 – распределенный NGFW

Анализ правил

Результат:

- Сокращение трудозатрат администратора
- Снижение инцидентов ИБ, связанных с неправильной настройкой политик
- Оптимизация производительности NGFW

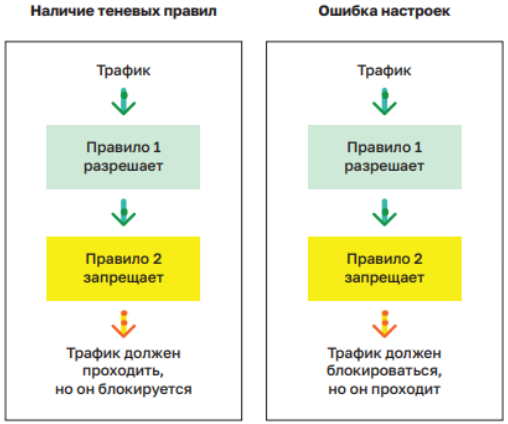
Пример реализации интеграции с Efros Defense Operations

Анализ правил

EFROS DEFENCE OPERATIONS

Нетхаб

SPACE-BIT



Балансировка нагрузки

Цифры:

- До 32 NGFW на 1 брокер сетевых пакетов
- До 288 Гбит/сек в режиме NGFW
- До 1 Тбит/сек в режиме МСЭ
- До 256 Гбит/сек в режиме VPN

Результат:

- Снижение вероятности распространения злоумышленника в сети высоконагруженного ЦОД

Балансировка нагрузки

ЦИФРОВЫЕ РЕШЕНИЯ

Пример реализации интеграции с DS Integrity

КОД безопасности

Песочницы

Результат:

- Повышение вероятности инцидентов, связанных с распространением вредоносного программного обеспечения

Преимущества:

- Построение эшелонированной защиты компаний от сложных киберугроз
- Снижение нагрузки на NGFW и как следствие рост производительности на потоке
- Использование технологий искусственного интеллекта
- Замещение иностранных связок

Пример интеграции NGFW и Sandbox

Песочницы

positive technologies

AVSOFT

kaspersky

КОД безопасности

Индикаторы компрометации

Преимущества:

- Предупреждение, мониторинг и предотвращение современных киберугроз
- Использование IoC, релевантных для защиты конкретной инфраструктуры
- Повышение производительности NGFW

IoC:

- IP-адреса вредоносных ресурсов
- Хэши вредоносных файлов
- URL-вредоносных сайтов
- Вредоносные домены

Результат:

- Своевременная блокировка известных атак на уровне сети
- Повышение прозрачности сетевой инфраструктуры с точки зрения обнаружения атак

Пример реализации интеграции NGFW и TIP

Индикаторы компрометации

kaspersky
Security Vision
CyberThreatTech
R-Vision
BI.ZONE

КОД безопасности

Основные тезисы

- КиберАльянс – союзы с наиболее сильными вендорами на российском рынке ИБ – подход, позволяющий сфокусировать основное внимание на **ядре безопасности**
- Три направления интеграций:
  1. Защищенный удаленный доступ (VPN-клиенты, многофакторная аутентификация, комплаенс)
  2. Интеграция с инфраструктурой (балансировка нагрузки, анализ конфигураций, защита виртуализации)
  3. Расширенная безопасность (песочницы, индикаторы компрометации)
- Не все компоненты КиберАльянса нужны вам прямо сейчас

КиберАльянс – подход, который позволяет **наращивать безопасность по мере необходимости**

КОД безопасности

Основа КиберАльянса - API

Экспорт конфигурации всех или выбранных Континент 4 под управлением отдельного ЦУС через API	▪ Политика безопасности и журналирование ▪ Настройки времени ▪ Сетевые функции
Миграции со сторонних NGFW (UserGate, FortiGate, Check Point, Palo Alto, Cisco)	▪ Правила фильтрации и трансляции ▪ Связанные с правилами сетевые объекты и группы ▪ Связанные с правилами сервисы и группы
Импорт индикаторов компрометации (IoC) в Континент 4	▪ IP-адреса вредоносных ресурсов ▪ FQDN вредоносных ресурсов ▪ URL-адреса вредоносных сайтов ▪ Hash ВПО
Создание политик безопасности	▪ Из SOAR-систем ▪ Из систем управления политиками безопасности

Приглашаем принять участие в Исследовательской группе Кода Безопасности

Давайте вместе развивать российский рынок информационной безопасности!

КОД безопасности

Социальные сети

КОД безопасности

Спасибо за внимание!

Лебедев Дмитрий – Ведущий эксперт
d.lebedev@securitycode.ru

info@securitycode.ru

www.securitycode.ru