УЦСБ

USSC.RU

ZERO TRUST
Современное прочтение правила «доверяй, но проверяй»

Алексей Брыляков
Менеджер по развитию решения по сетевой безопасности

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ

Содержание

- Контроль доступа к сети – Efros DO - модуль NAC
- Харденинг и регулярный аудит настроек оборудования и ПО
- Автоматизация аудита и харденинга – Efros DO модули NA и ICC
- Аудит политик межсетевого экранирования – Efros DO модуль FA

Предпосылки к NAC



Увеличение числа удаленных подключений и некорпоративных пользователей



Работа на собственных устройствах при подключении к сети

Рост числа подключенных IoT устройств



Shadow IT

ВОЗМОЖНОСТИ EDO NAC

- RADUIS сервер с поддержкой различных типов EAP
- Гибкие политики авторизации
- Интеграция с Microsoft AD и LDAP
- TACACS+ сервер
- Профилирование
- Учет состояния защищенности

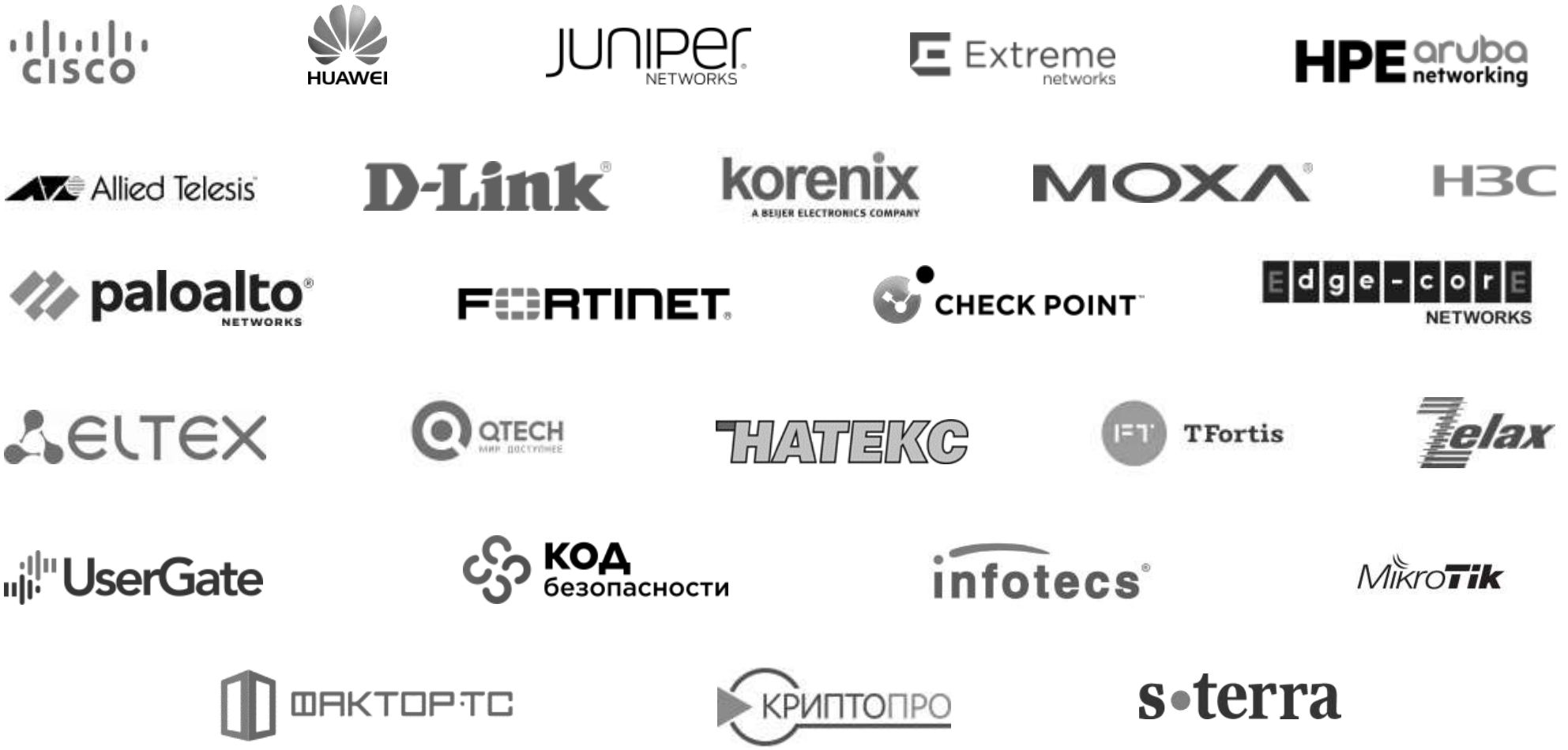
Харденинг и регулярный аудит

- Отключение неиспользуемых функций и сервисов
- Изменения настроек по умолчанию
- Внесение изменений в настройки
- Регулярное обновление ПО и аудит настроек

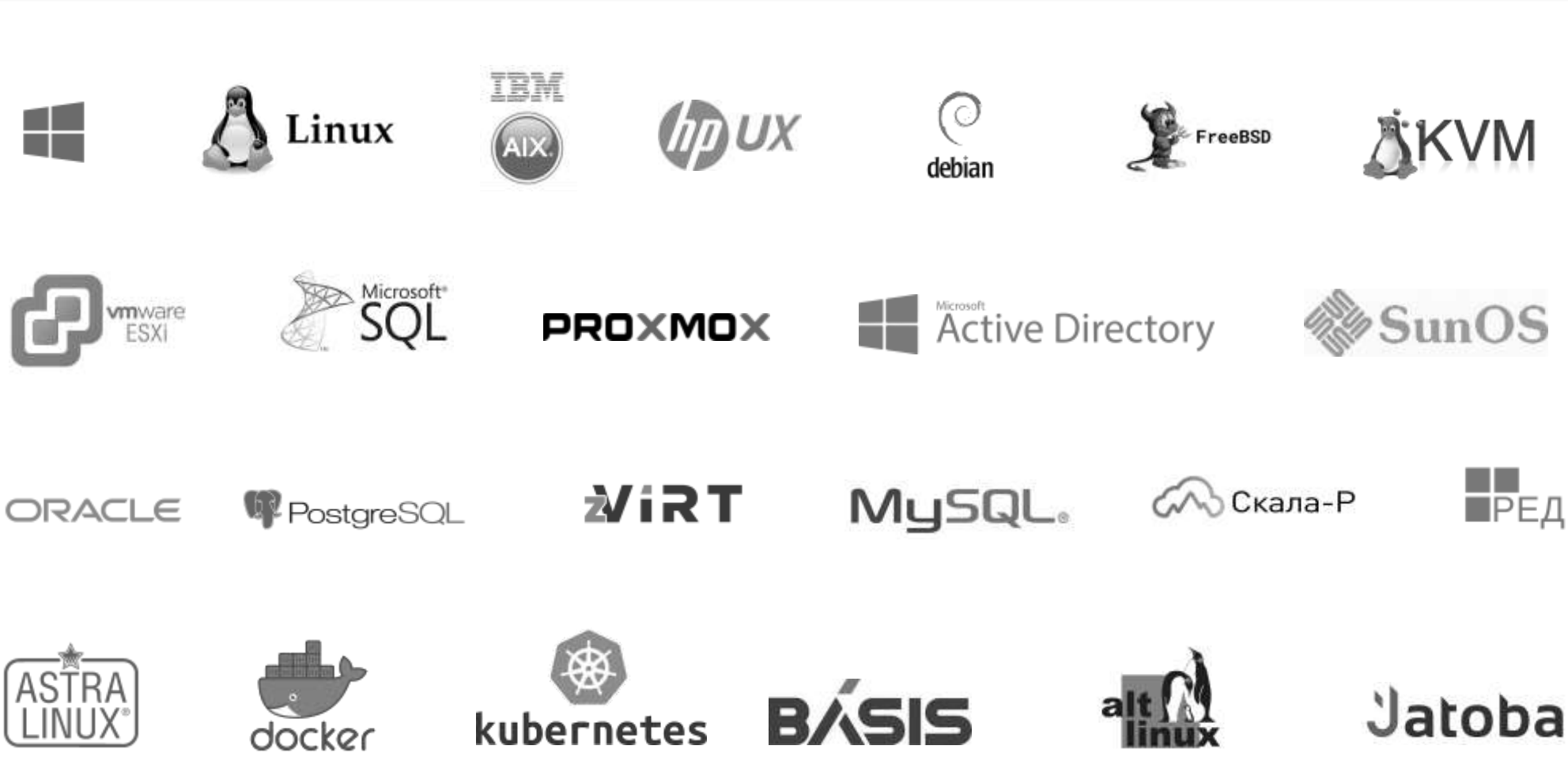
Efros DO модули NA и ICC

- Сбор конфигураций/настроек
- Инвентаризация, ведение архива и отслеживание изменений
- Выявление известных уязвимостей на основе версии ОС
- Анализ соответствия настроек
- Построение карты сети / Контроль целостности

Поддерживаемое оборудование



Поддерживаемое ПО



МОДУЛЬ EDO Firewall Assurance

- Сбор политик межсетевого экранирования
- Инвентаризация и архив политик
- Оптимизация политик межсетевого экранирования
- Аудит правил межсетевого экранирования на соответствие

Поддерживаемые межсетевые экраны

paloalto NETWORKS
FORTINET
CHECK POINT
HUAWEI
JUNIPER NETWORKS
MikroTik
CISCO
UserGate
КОД безопасности
infotecs
ФАКТОР-ТС
ELTEX
s•terra

УЦСБ

USSC.RU

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ

Спасибо за внимание!

Вопросы?

Алексей Брыляков
Менеджер по развитию решения по сетевой безопасности

abrylyakov@ussc.ru