ЕВРАЗ

Нужен ли EDR?
Или качественно зафиксированный пациент в анестезии не нуждается

Нуйкин Андрей

2024

О чем поговорим

ЕВРАЗ

Многие компании активно продвигают решения EDR\XDR как панацею

Стоимость решений EDR\XDR высока по сравнению с другими средствами

На компьютер ложится дополнительная нагрузка от агента

Контекст

ЕВРАЗ

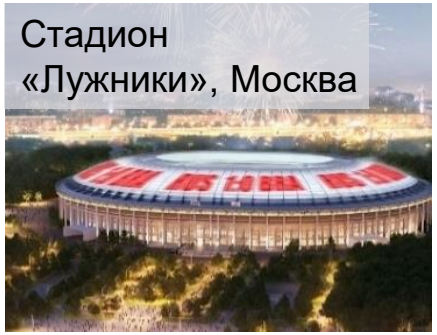
- Данная презентация является частным мнением и может не совпадать с мнением других организаций и экспертов.
- Данное исследование не является окончательным и не ставит целью дискредитацию решений или подходов.
- Исследование не охватывает всех продуктов и методик.
- Полученные результаты являются не окончательными и требуют дальнейшего всестороннего изучения и сравнения с другими решениями.

Что такое ЕВРАЗ?

ЕВРАЗ


Олимпийские объекты, Сочи


Лахта центр, Санкт-Петербург

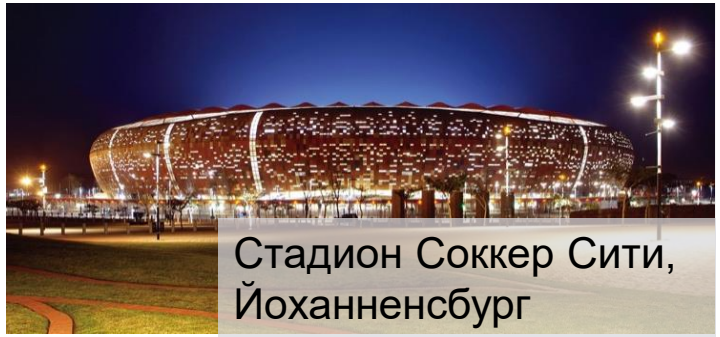

Стадион «Лужники», Москва


Амурский ГПЗ, Дальний Восток


Burj Al Arab Jumeirah, Дубай


Нефтегазовый комплекс Ямал СПГ


Спортивные объекты, Казань


Стадион Соккер Сити, Йоханненсбург


Красноярская ГЭС и Саяно-Шушенская ГЭС

Кто мы

ЕВРАЗ

- Три больших локации – Москва, Сибирь, Урал
- Порядка 150 проектов цифровизации в год
- Более 15 000 пользователей
- Порядка 3 000 000 писем в месяц
- В среднем 5 000 фишинговых писем
- Порядка 1000 вирусов и 18 000 подозрительных URL

Кто мы

ЕВРАЗ

- Более 20 лет в ИБ.
- Член (АРСИБ), БИП-Клуба, КУБИТ.
- Работал в различных крупных компаниях: «Евроцемент», «Промсвязьбанк», SELA и др.
- С 2014 г. — начальник отдела обеспечения безопасности информационных систем в ЕВРАЗе.

Андрей Нуйкин
CISA, CISM, CRISK
АРСИБ
RuSCADASec Coin #29

ЕВРАЗ

- Количество атак неуклонно растет.
- Атаки усложняются.
- Защищаться сложнее.

Текущая реальность

ЕВРАЗ

Решили проверить:

- А так ли хороши EDR\XDR?
- В какой инфраструктуре они более эффективны?
- Насколько они повышают общую защищенность?

Что сделали?

ЕВРАЗ

Подготовили стенд:

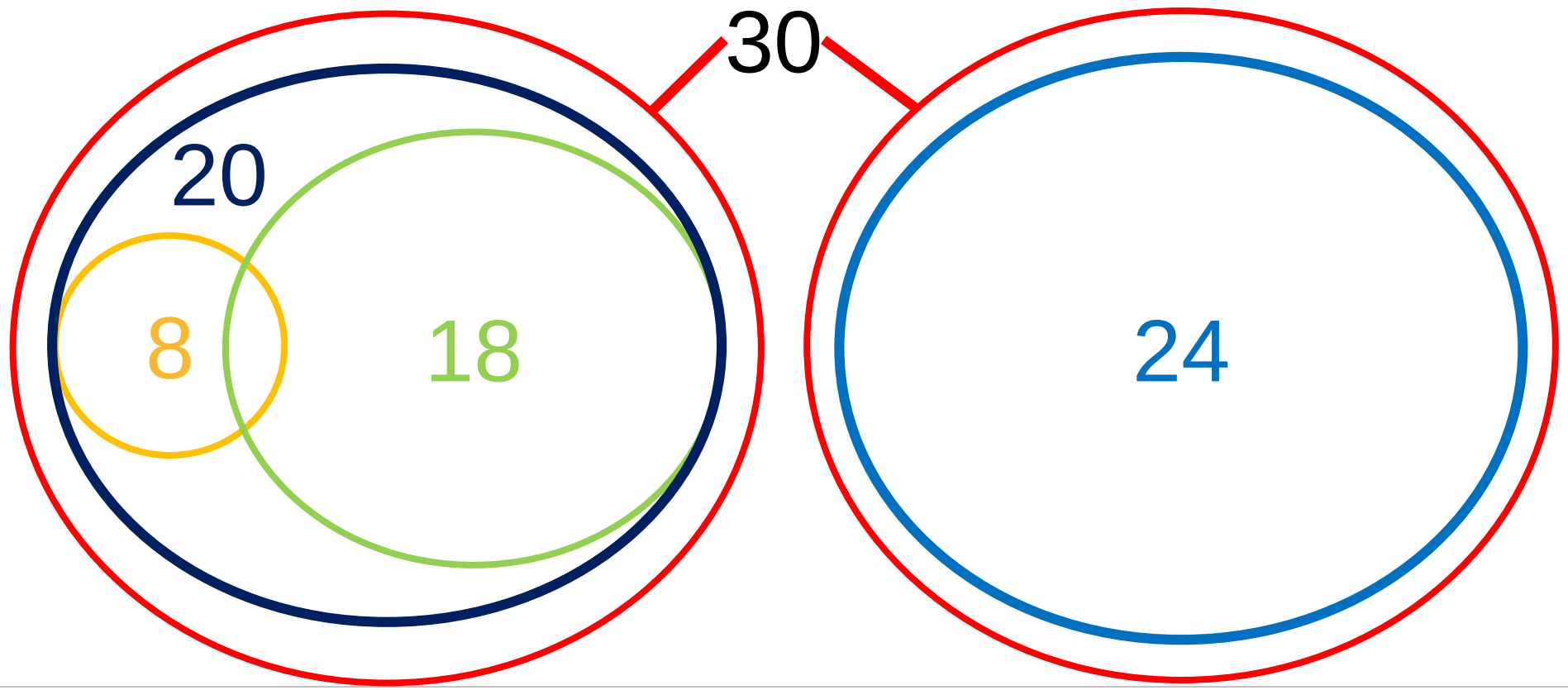
- Default Windows + KES
- Default Windows + KEDR
- Windows Hardening Admin
- Windows Hardening NoAdmin

К настроенным компьютерам применили 30 различных хакерских техник.

Результат

ЕВРАЗ

Hardening KES KES+Hard KEDR



ЕВРАЗ

Ожидали

большего эффекта

- Попробовать решения от других производителей EDR\XDR
- Расширить перечень атакующих техник
- Установить дополнительно прикладное ПО

ЕВРАЗ

Больше тестируйте и проверяйте

+7(495) 363-19-60

Andrey.nuykin@evraz.com

www.evraz.com

Андрей Нуйкин
CISA, CISM
АРСИБ
RuSCADASec Coin #29