GIS ГАЗИНФОРМ СЕРВИС

Проблематика контроля АСУ ТП

Ведущий инженер
Максимов Александр

GIS ГАЗИНФОРМ СЕРВИС

Как связаны данные картинки ?

+

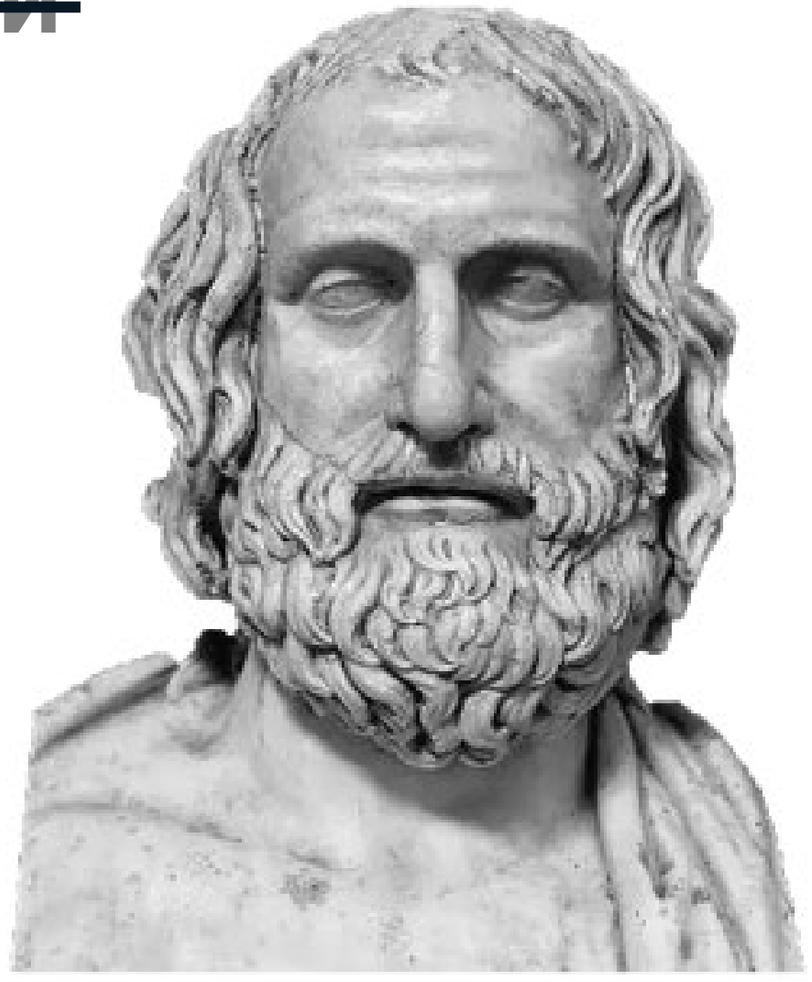
+

GIS ГАЗИНФОРМ СЕРВИС

Из-за чего такое могло произойти ?

«Человек есть мера всех ~~вещей~~ проблем» *Протагор©*

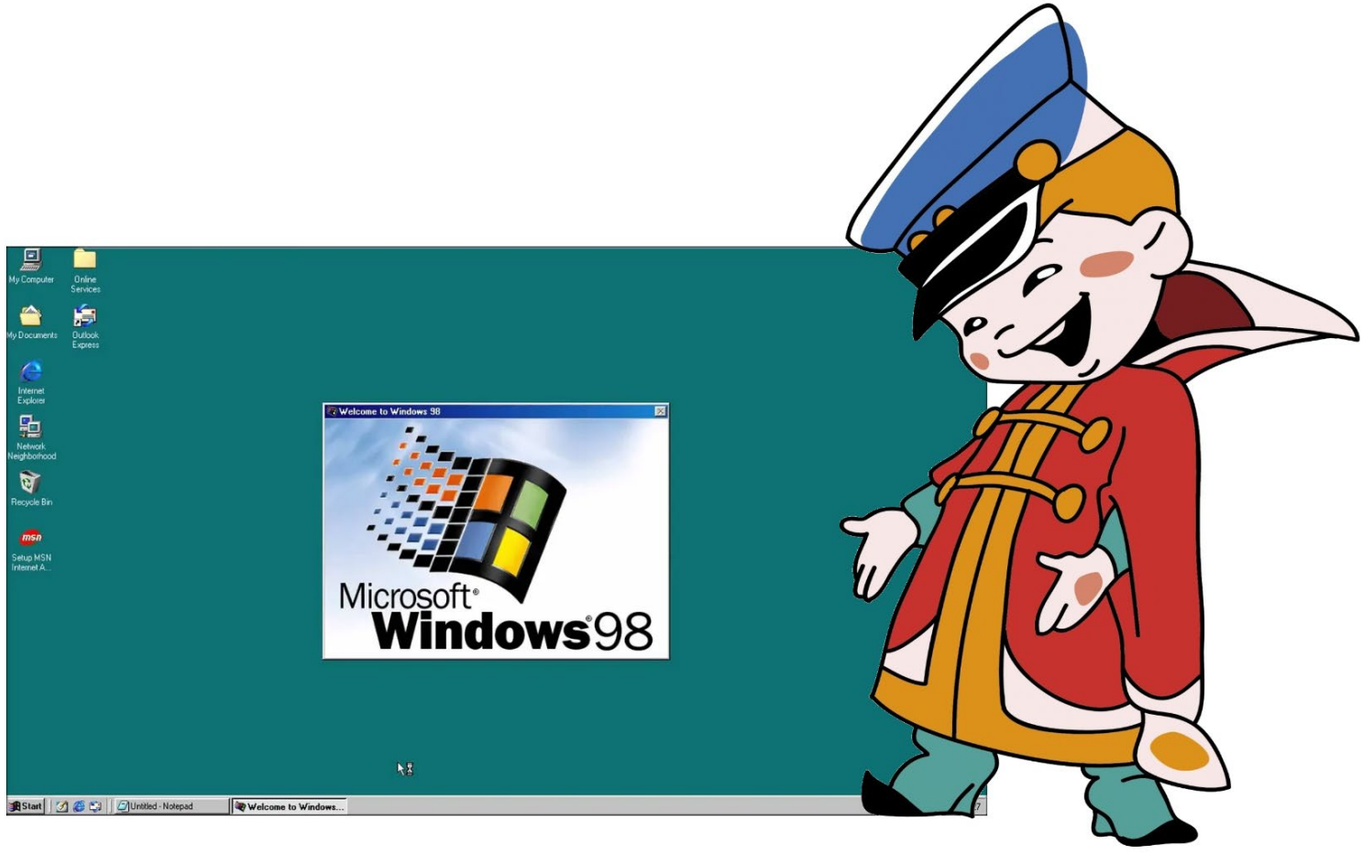
– Использование паролей по умолчанию или слабых паролей
– Несоблюдение правил пользования АРМ
– Групповая учетная запись
– Использование нелегитимного софта



Из-за чего такое могло произойти ?

«Все новое – хорошо забытое старое»

– Отсутствие обновления ОС и ПО
– Отсутствует регулярное сканирование состояния оборудования
– Зависимость от разработчиков ПО для АСУ ТП



Из-за чего такое могло произойти ?

«В здоровом теле – СЗИ не нужны»

– Отсутствие обновления ОС и ПО
– Отсутствует регулярное сканирование состояния оборудования
– Зависимость от разработчиков ПО для АСУ ТП

GIS ГАЗИНФОРМ СЕРВИС

Из-за чего такое могло произойти ?

«Не пей, не ешь, а держи святой рубеж»

– Не настроена сеть
– Сеть не сегментирована
– Сотрудники не знают устройство сети
– Небезопасный удаленный доступ

GIS ГАЗИНФОРМ СЕРВИС

«Знай своего врага в лицо»

10

Каждая успешная атака на промышленный сектор.

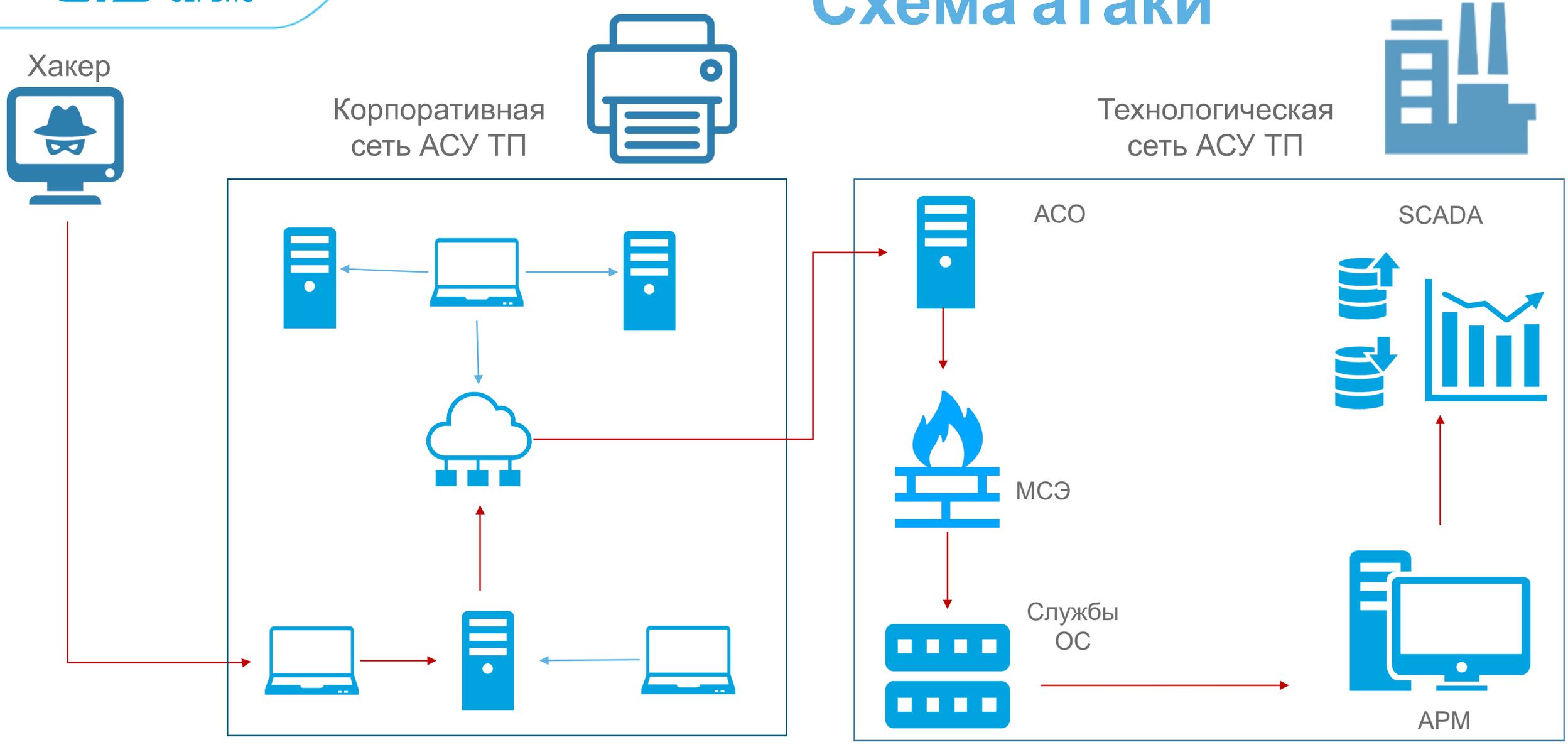
80%

Рост числа атак в России на КИИ и АСУ.

В большинстве атак применялось вредоносное ПО, которое распространялось преимущественно через компрометацию ресурсов на периметре организаций (49%) и электронную почту (43%).

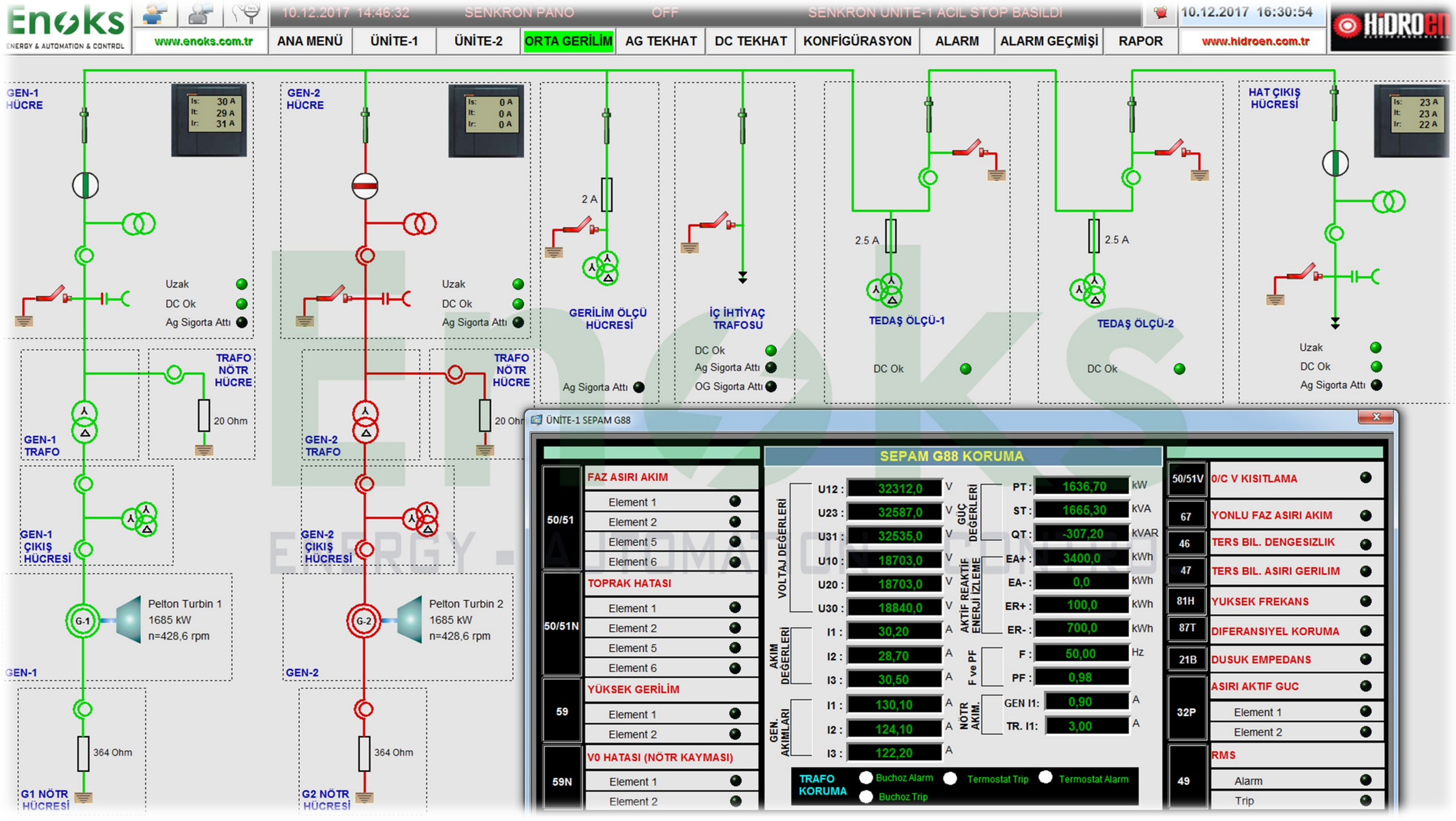
GIS ГАЗИНФОРМ СЕРВИС

Схема атаки



GIS ГАЗИНФОРМ СЕРВИС

Схема атаки



EFROS

CONFIG INSPECTOR

Контроль безопасности конфигураций и состояний сетевого оборудования, сред виртуализации, операционных систем, SCADA- и RPA-решений.

GIS ТАВИНФОРМ СЕРВИС

Основные возможности Efros Config Inspector

Контроль изменений в конфигурациях

Аудит межсетевых экранов

Обнаружение уязвимостей

Проверка безопасности устройств

GIS ГАЗИНФОРМ СЕРВИС

Спасибо за внимание!

+7 (812) 677-20-53

sales@gaz-is.ru