

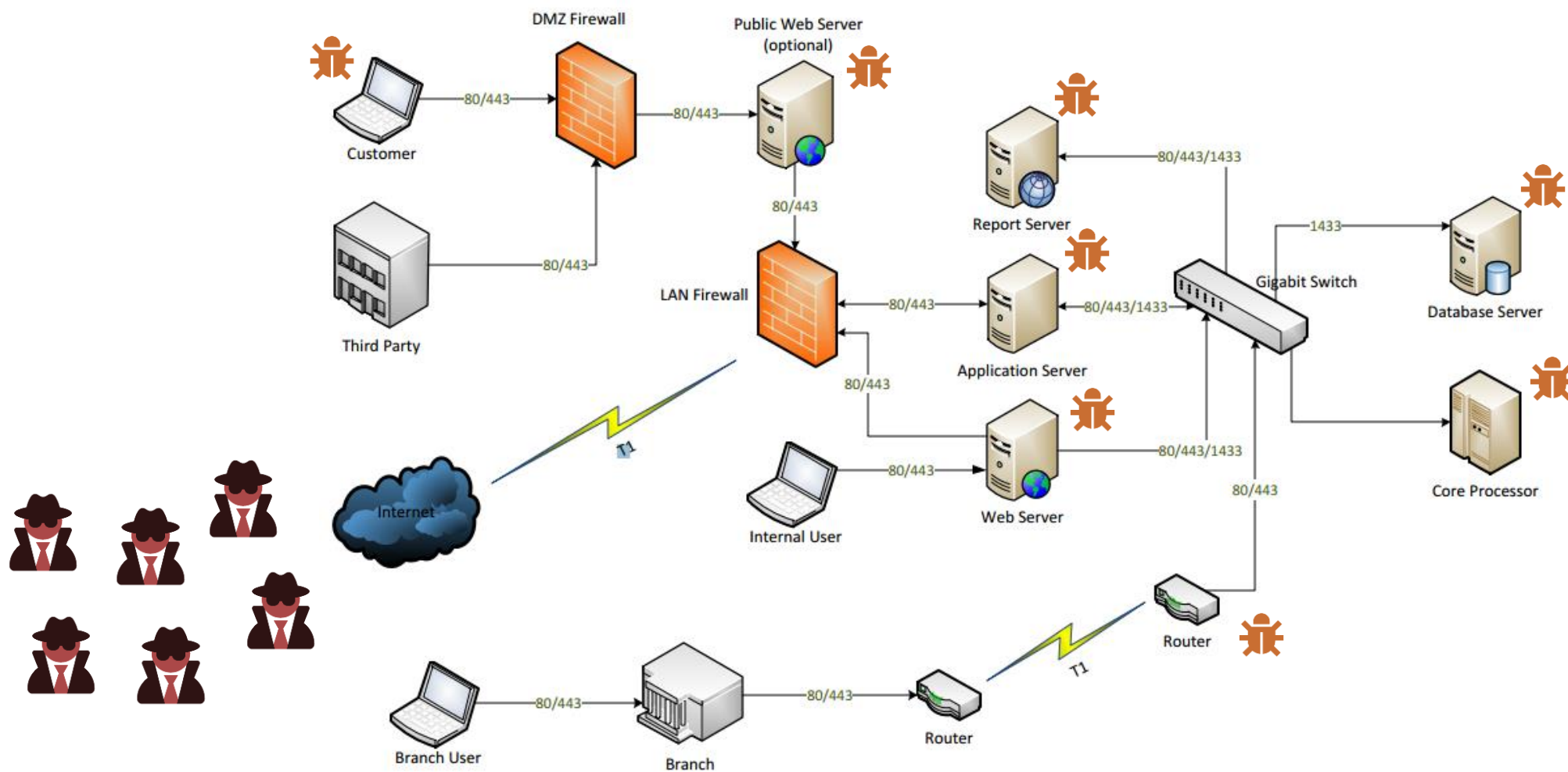


Гонка со злоумышленником

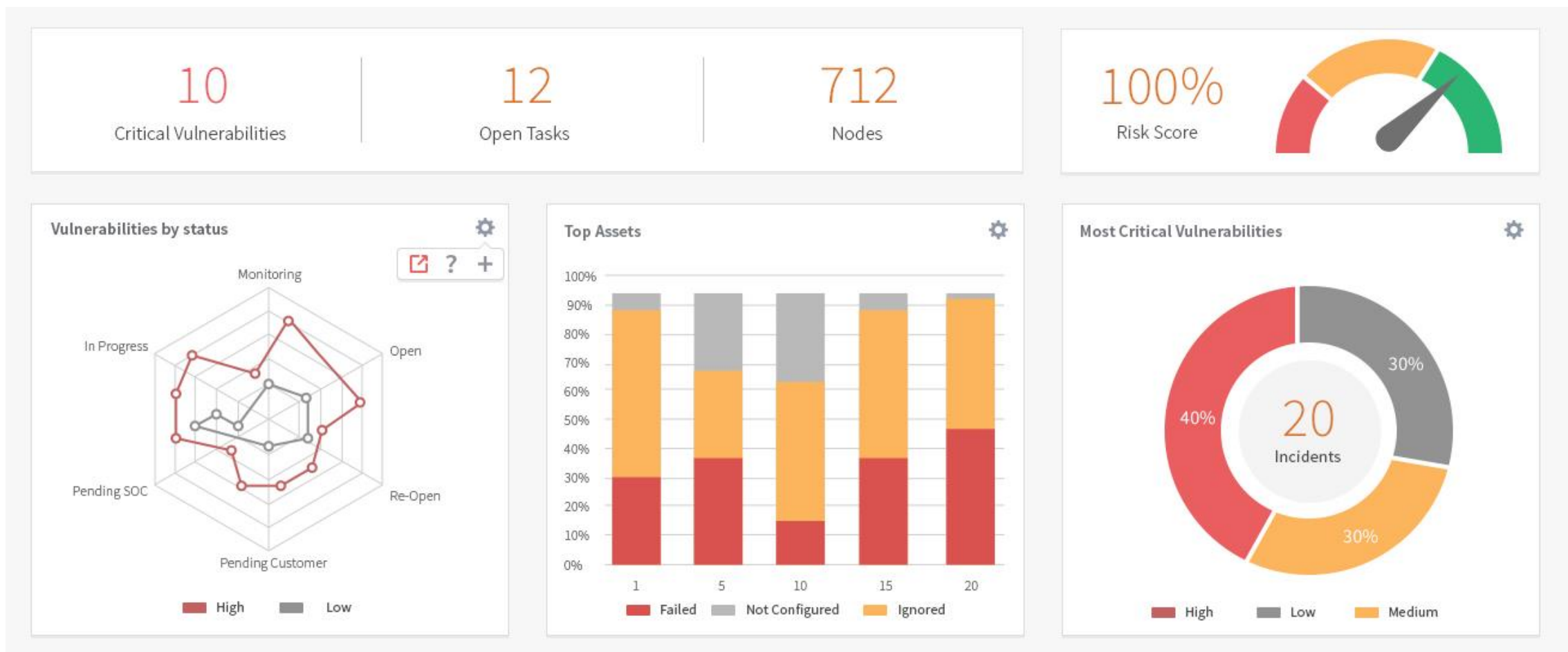
Реагирование на новые уязвимости

Vulns.io VM

Злоумышленник где-то рядом



Мы спокойны – у нас же VM-решение



Появляется новая уязвимость

CVE-2022-9876

CVSS Score **10**, Severity: **High**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam tincidunt feugiat feugiat. Etiam nulla odio, lobortis ac lectus sed, pretium faucibus dolor. Phasellus sapien tortor, ornare sed erat ut, commodo laoreet libero. Integer a facilisis magna. Etiam malesuada mauris non libero accumsan volutpat. Integer condimentum est erat, at hendrerit justo auctor eu.

Кто первый?



Вендор VM



Офицер ИБ



Служба ИТ

Закроют уязвимость



Злоумышленник

Реализует уязвимость

Вендор VM



1. Получает информацию об уязвимости
2. Обрабатывает, тестирует
3. Публикует обновление БДУ
4. Решение VM обновляет локальную БДУ

Вендор VM



1. Получает информацию об уязвимости
2. Обрабатывает, тестирует

✗ Медленно:

- ручной сбор и обработка

✓ Быстро:

- автоматизированный сбор и обработка

Вендор VM



3. Публикует обновление БДУ
4. Решение VM обновляет локальную БДУ

✗ Медленно:

- обновления БДУ публикуются раз в месяц/неделю/день
- VM-решение периодически проверяет обновления БДУ

✓ Быстро:

- обновления БДУ публикуются сразу по мере появления новых уязвимостей
- VM-решение получает оповещение о необходимости обновить БДУ и сразу обновляется (PUSH)

Офицер ИБ



1. Обновляет локальную БДУ VM
2. Проводит сканирование активов
3. Передает информацию в IT

Офицер ИБ



1. Обновляет локальную БДУ VM

✗ Медленно:

- Периодически проверяет нет ли обновлений БДУ
- Планирует установку обновлений БДУ
- Проводит обновление БДУ автоматизировано по расписанию

✓ Быстро:

- VM-решение получает оповещение о необходимости обновить БДУ
- БДУ VM сразу обновляется (PUSH)

Офицер ИБ

2. Проводит сканирование активов



✗ Медленно:

- Планирует и проводит сканирование после обновления БДУ
- Полагается на запланированное сканирование по расписанию
- Актив сканируется несколько минут

✓ Быстро:

- Автоматическое пересканирование тех активов, для которых обновилась БДУ
- Актив сканируется несколько секунд

Офицер ИБ



3. Передает информацию в IT

✗ Медленно:

- В сторонней системе вручную формирует тикет на обновление активов

✓ Быстро:

- Формирует тикет напрямую из VM-решения
- Тикет формируется автоматически по заданным правилам

Служба ИТ



1. Планирует обновление активов
2. Обновляет тестовое окружение
3. Обновляет боевое окружение

Служба ИТ



1. Планирует обновление активов
2. Обновляет тестовое окружение
3. Обновляет боевое окружение

✗ Медленно:

- Делает это вручную, без средств автоматизации

✓ Быстро:

- Делает это в «одном окне» с офицером ИБ с помощью инструментов VM-решения

Проигрываем гонку

Когда всё делаем **медленно**

Проигрываем гонку:

- Вендор VM вручную собирает и обрабатывает новые уязвимости
- Обновления БДУ публикуются раз в месяц/неделю/день
- Со стороны VM-решения обновления проверяется вручную
 - или решение периодически само проверяет обновления БДУ
- Планируется установка обновлений БДУ
 - или обновление автоматизировано по расписанию
- После обновления БДУ планируется и проводится сканирование активов
- Каждый актив сканируется по несколько минут
- В сторонней системе вручную формируется тикет на обновление активов
- Обновление устанавливается вручную, без средств автоматизации

Выигрываем гонку

Когда всё делаем **быстро**

Vulns.io VM

Выигрываем гонку:

- Вендор VM автоматизировано собирает и обрабатывает новые уязвимости
- Обновления БДУ публикуются сразу по мере появления новых уязвимостей
- VM-решение получает оповещение о необходимости обновить БДУ и сразу обновляется (PUSH)
- Автоматически пересканируются те активы, для которых обновилась БДУ
- Актив сканируется ~1-3 секунды
- Автоматически или вручную из VM-решения формируется тикет на обновление активов
- С помощью инструментов VM-решения обновляется тестовое, а затем и боевое окружение

Вопросы вендору VM-решения

- Как быстро новые уязвимости становятся доступны в виде обновления БДУ для VM-решения?
- Насколько быстро VM-решение получает обновления БДУ?
- Можно ли автоматически пересканировать активы после обновления БДУ?
- Как быстро сканируется актив?
- Можно ли автоматизировать создание тикетов на обновление активов?
- Можно ли провести обновление активов с помощью VM-решения?



Владимир Михайлов

Руководитель департамента
перспективных проектов



v.mikhailov@frodex.ru



+7(495) 967 65 19



https://t.me/vladimir_mikhailov

