Экспертный дистрибьютор ИБ

Валерий Филин
Технический директор CITUM

Pentera Ransomware Ready

PENTERA

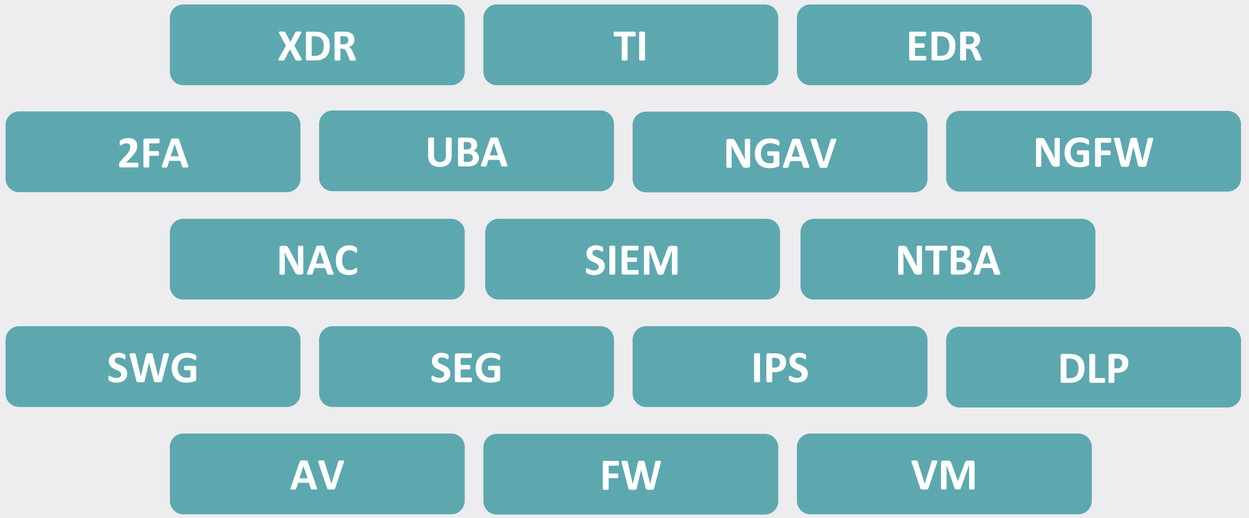
Как подтвердить готовность к отражению атак шифровальщиков?

https://www.pentera.io

Гонка вооружений

На протяжении последних десятилетий мы устанавливаем все больше и больше новых эшелонов защиты

Остановились ли мы хоть раз для проверки?



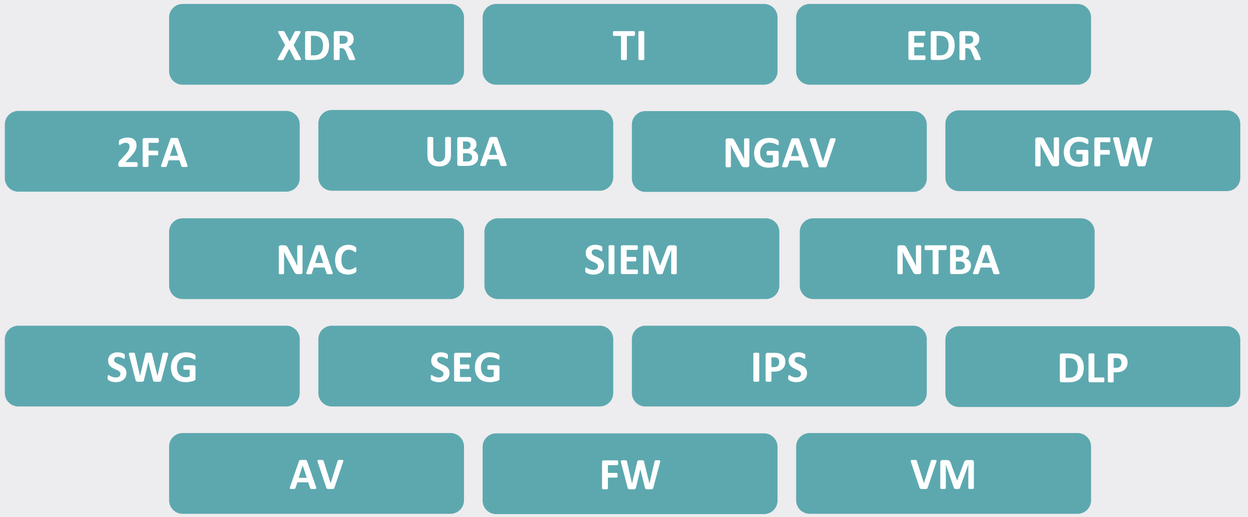
Вымогатели-шифровальщики

Серьезная угроза

- За 2020 год сумма выплаченных выкупов – более $ 300 млн[1]
- За первые 4 месяца 2021 года сумма выплаченных выкупов – более $ 81 млн[1]
- Средний размер выкупа – $ 220 298[2]
- Средняя стоимость восстановления после атаки Ransomware в 2021 году – $ 1.85 млн[2]
- Почти половина всех атак в 2020 году пришлась на 3 семейства – Maze, REvil, Ryuk[3]

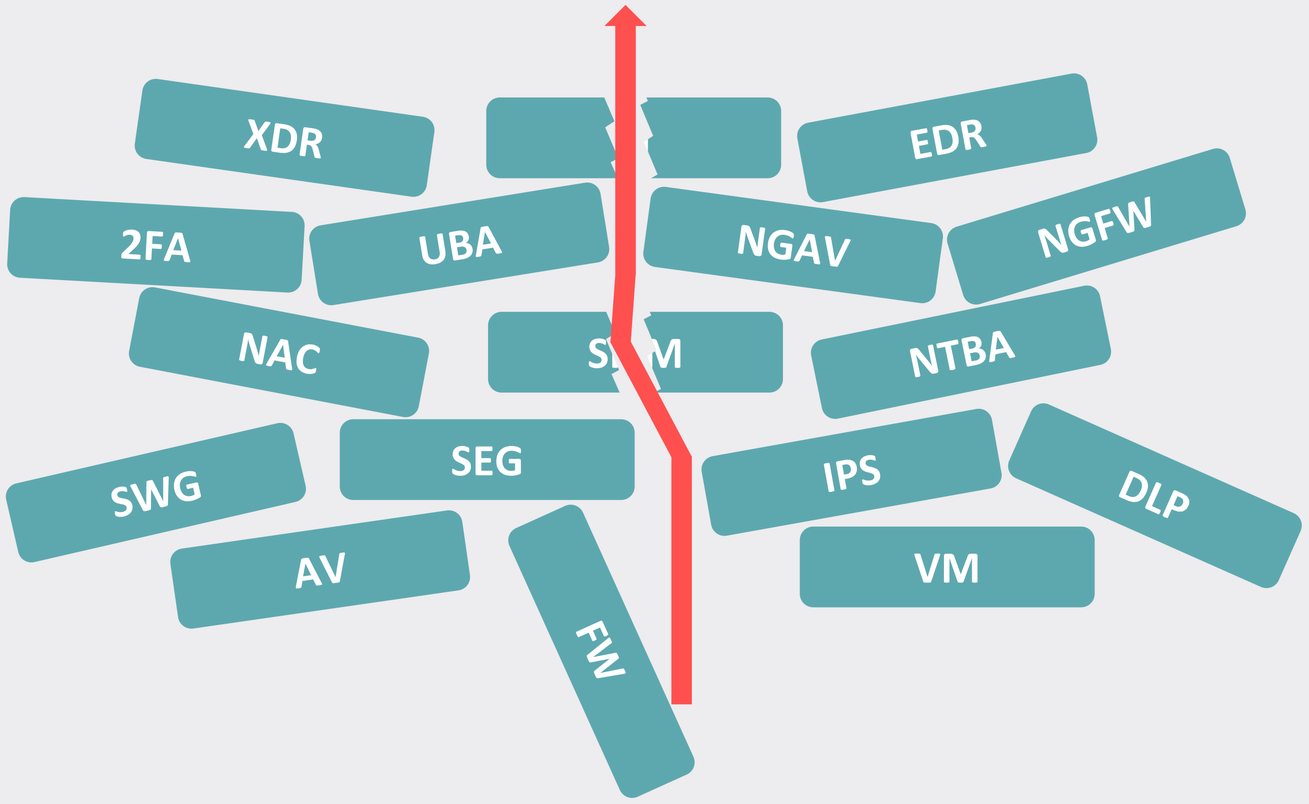
[1]Chainalysis, 2021 [2]Cloudwards, 2021 [3]Group-IB, 2021

Готовы ли мы к атаке?



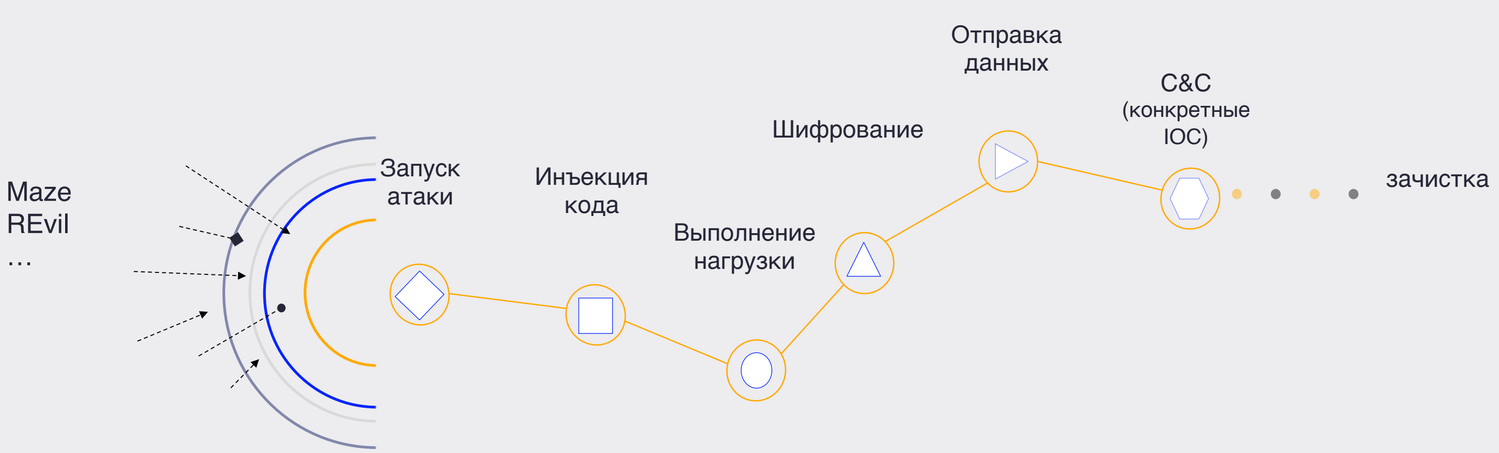
Готовы ли мы к атаке?

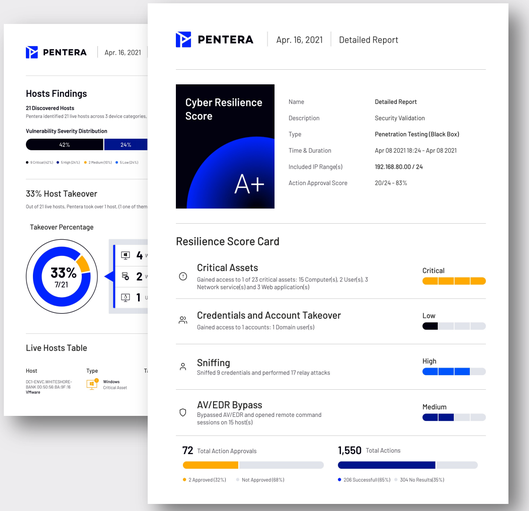
Предположения ≠ реальность



Специальный модуль Pentera ASV

Проверка в боевых условиях

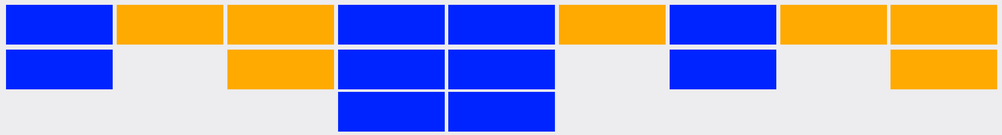




Обход AV/EDR

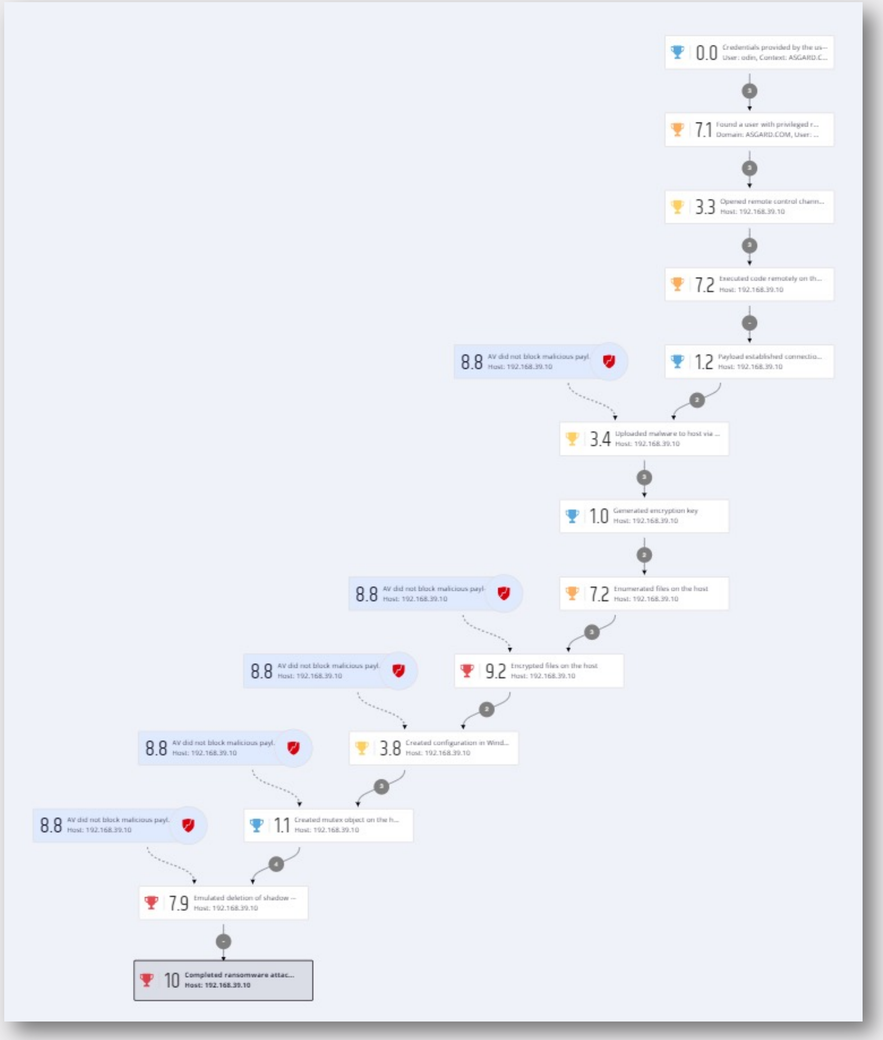
Уязвимости и достижения

Рекомендации по улучшению защиты



Интеграция с MITRE ATT&CK Framework

Новый шаблон тестирования



Запуск атаки
ATT&CK | T1047

Инъекция кода
ATT&CK | T1105

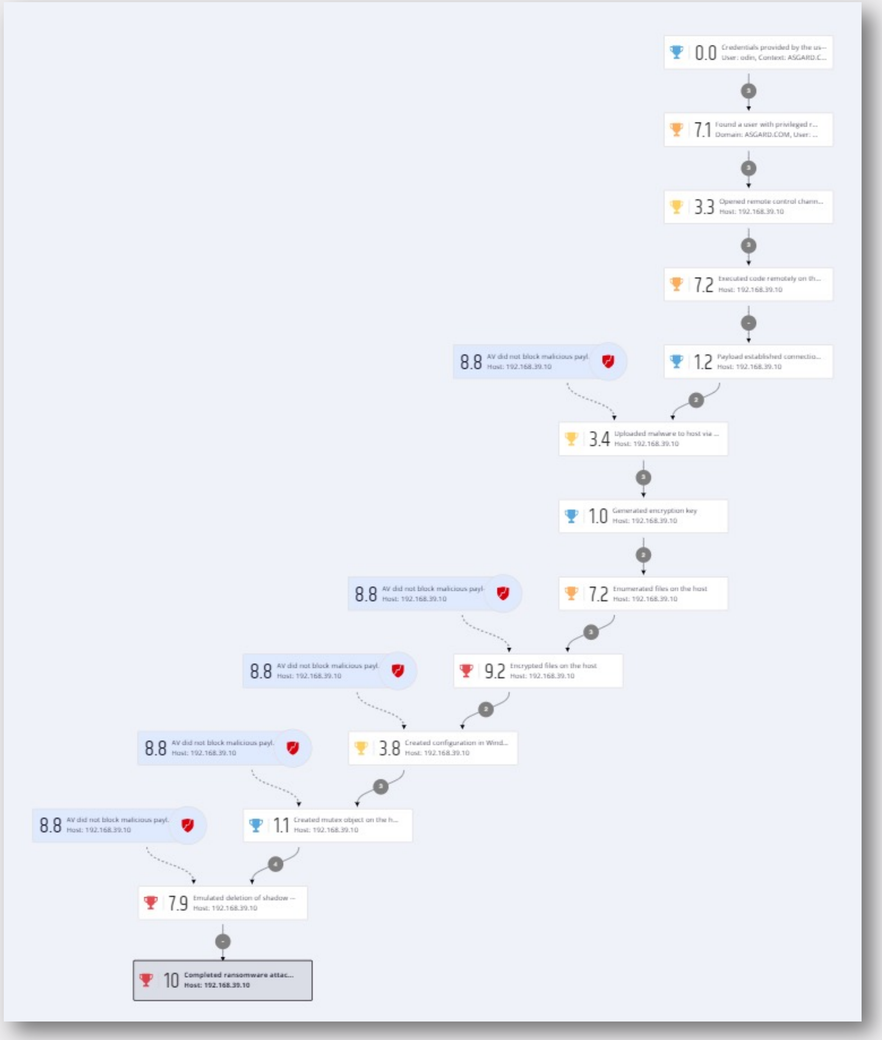
Выполнение нагрузки
ATT&CK | T1496

Шифрование
ATT&CK | T1083

Отправка данных
ATT&CK | T1490

C&C (конкретные IOC)
ATT&CK | T1005

Новый шаблон тестирования



Полный цикл атаки

Шифрование алгоритмом Salsa20

Проверка доступа к теневым копиям

Связь каждого действия с матрицей MITRE

Запуск атаки
ATT&CK | T1047

Инъекция кода
ATT&CK | T1105

Выполнение нагрузки
ATT&CK | T1496

Шифрование
ATT&CK | T1083

Отправка данных
ATT&CK | T1490

C&C (конкретные IOC)
ATT&CK | T1005

Гибкий выбор типов файлов

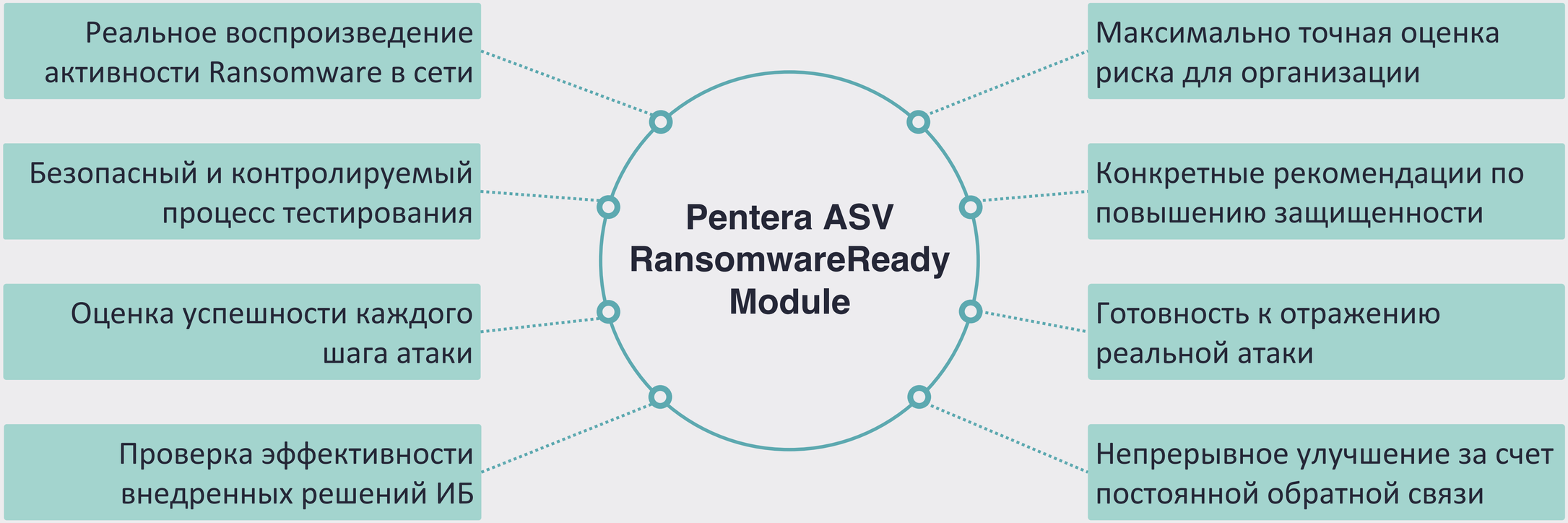
Характерные IOC на хосте

Отправка данных
- На собственный сервер
- На реальные адреса кампаний

Проверка контрмер

Что это дает заказчику?

Возможности и преимущества системы



Модуль Ransomware Ready

Демонстрация системы

Платформа Pentera ASV

Пилотный проект

У Вас остались вопросы?

БУДЕМ РАДЫХ ОТВЕТИТЬ!

Валерий Филин, CITUM
vfilin@citum.ru

marketing@dialognauka.ru