10 YEARS JETSECURITY CONFERENCE 2019

ALL-IN-ONE: КАК СДЕЛАТЬ ПРОЕКТ ПО СЕТЕВОЙ БЕЗОПАСНОСТИ

Дмитрий Борисов

Инженер-проектировщик по ИБ
dp.borisov@jet.su

ЗАКАЗЧИК И ОТНОШЕНИЯ С ДЖЕТ

- Один из крупных региональных банков (ТОП-50)
- Почти 4000 сотрудников,
  более 700 000 клиентов-физических лиц
  и 15 000 корпоративных клиентов
- Более 10 совместных проектов:
  - Внедрение HP Arcsight (2014 г.)
  - Внедрение McAfee Web | Mail Gateway и McAfee Network DLP (2014 г.)
  - Внедрение Imperva DAM (2015 г.) и модернизация (2017 г.)
  - Аудиты на соответствие PCI DSS (2014 - 2017 г.)

НА ИСХОДНУЮ!

- **Цели Заказчика**
  - обновление текущих решений по ИБ
  - возможность администрирования малыми ресурсами
  - противодействие целенаправленным атакам и «zero-day»-угрозам

- **Три гео-распределенные площадки:**
  - Центральный офис/ЦОД
  - Резервный ЦОД
  - Процессинговый центр

У ВАС ЕСТЬ ПРОБЛЕМА? У НАС ЕСТЬ РЕШЕНИЕ

ЦЕНТРАЛЬНЫЙ ОФИС/ЦОД

РЕЗЕРВНЫЙ ЦОД

ПРОЦЕССИНГОВЫЙ ЦЕНТР

МОНОВЕНДОРНОСТЬ ХОРОШО ИЛИ ПЛОХО?

КОНФИДЕНТ®
CONFIDENT

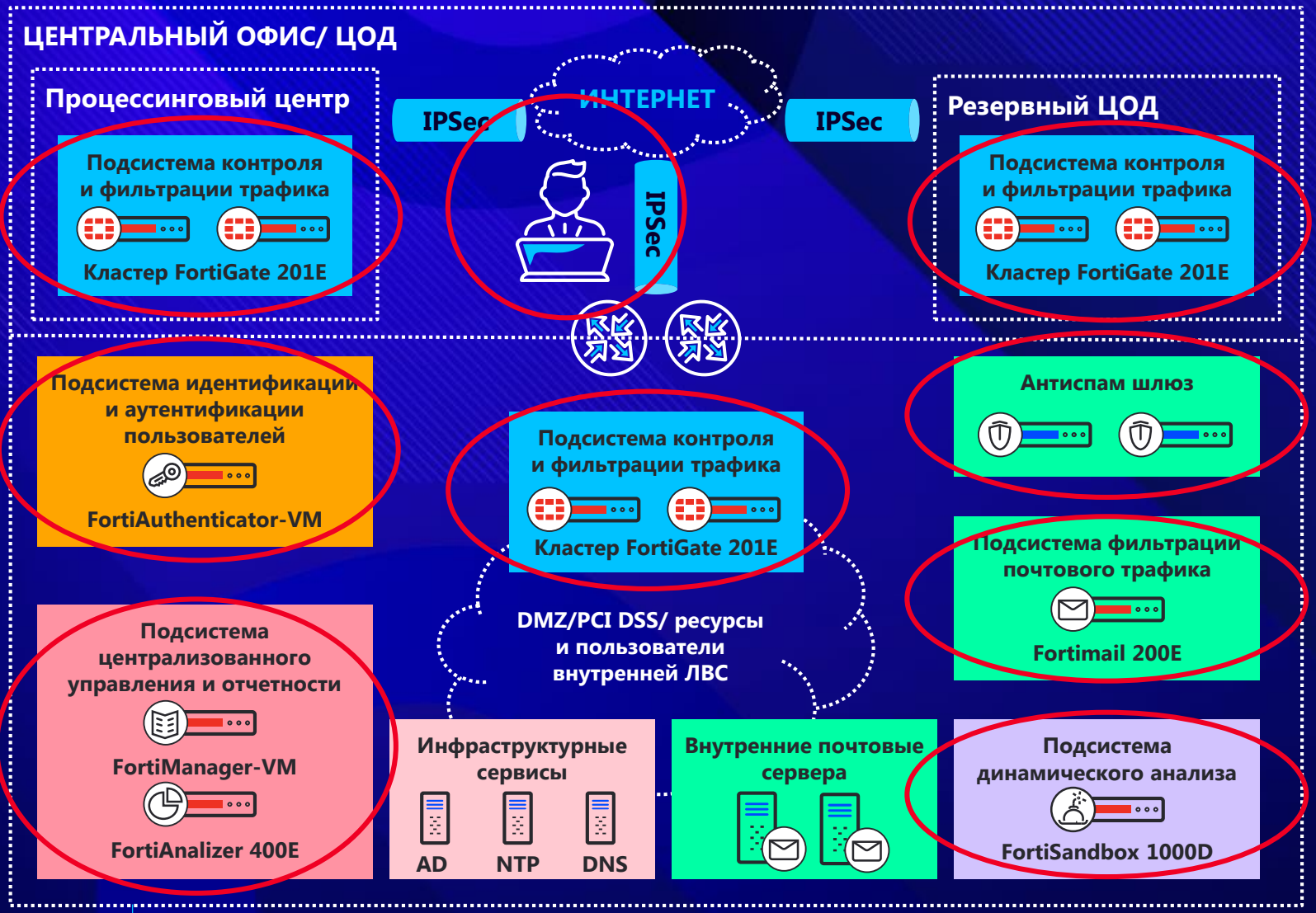
КОД БЕЗОПАСНОСТИ

ОКБ АПР

FORTINET®

s•terra

#АРХИТЕКТУРА ПРОЕКТА

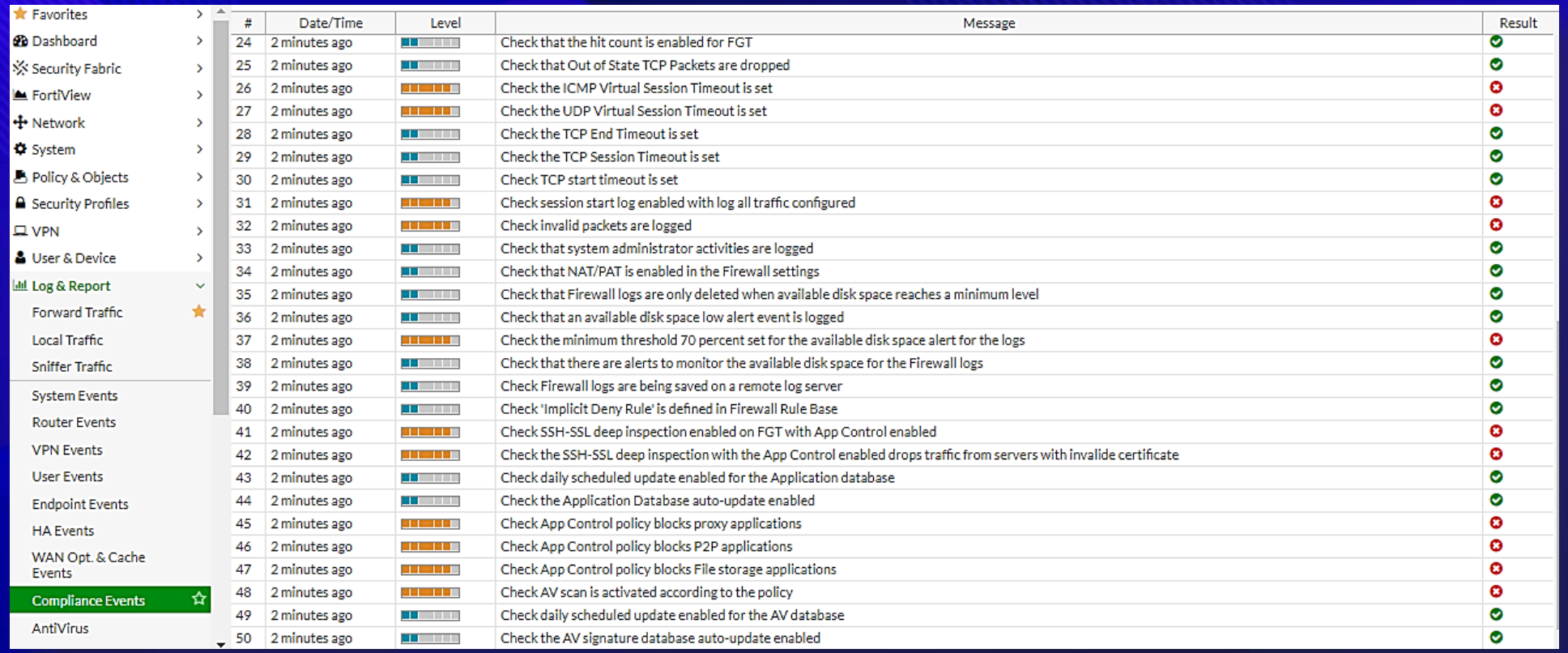


ОСТАВИМ ТЕХНИЧЕСКИЕ ПОДРОБНОСТИ — У НАС ЖЕ СТЕНД-АП!

ИНСТРУМЕНТОВ, КОТОРЫЕ ПОЯВИЛИСЬ У ЗАКАЗЧИКА

5 МЕСТО

ВСТРОЕННЫЙ АУДИТ НА СООТВЕТСТВИЕ PCI DSS



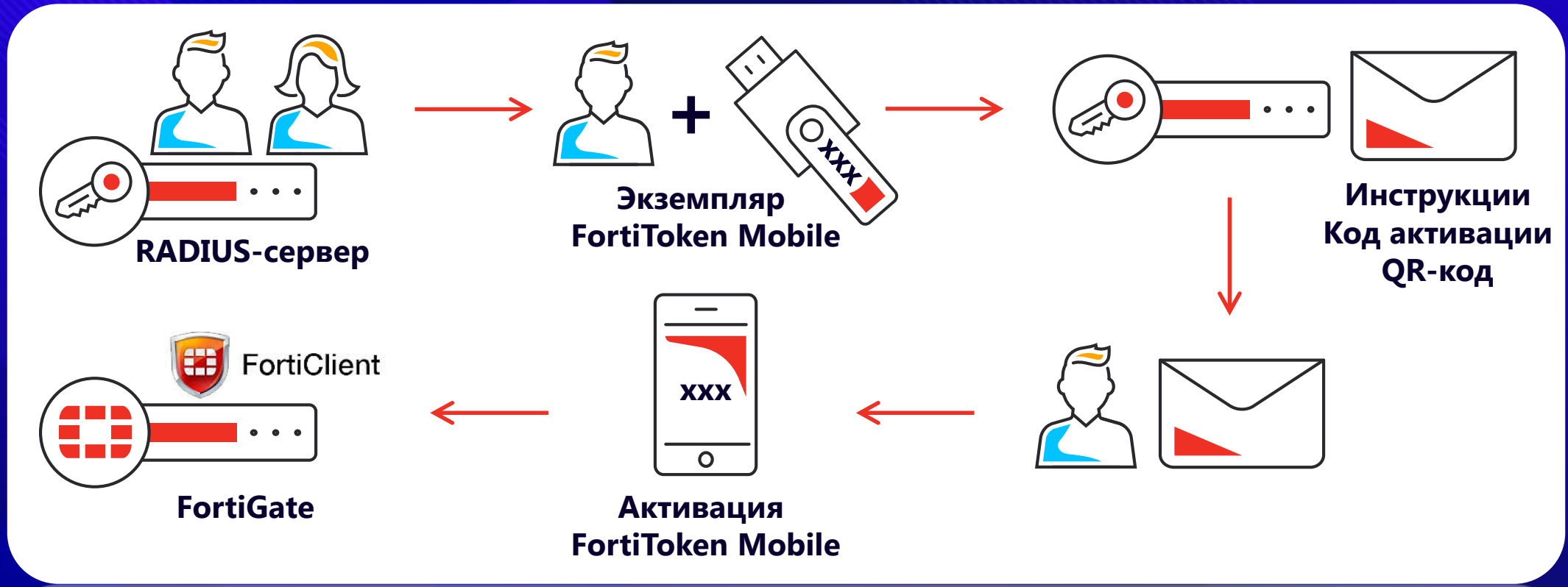
#	Date/Time	Level	Message	Result
24	2 minutes ago		Check that the hit count is enabled for FGT	✓
25	2 minutes ago		Check that Out of State TCP Packets are dropped	✓
26	2 minutes ago		Check the ICMP Virtual Session Timeout is set	✗
27	2 minutes ago		Check the UDP Virtual Session Timeout is set	✗
28	2 minutes ago		Check the TCP End Timeout is set	✓
29	2 minutes ago		Check the TCP Session Timeout is set	✓
30	2 minutes ago		Check TCP start timeout is set	✓
31	2 minutes ago		Check session start log enabled with log all traffic configured	✗
32	2 minutes ago		Check invalid packets are logged	✗
33	2 minutes ago		Check that system administrator activities are logged	✓
34	2 minutes ago		Check that NAT/PAT is enabled in the Firewall settings	✓
35	2 minutes ago		Check that Firewall logs are only deleted when available disk space reaches a minimum level	✓
36	2 minutes ago		Check that an available disk space low alert event is logged	✓
37	2 minutes ago		Check the minimum threshold 70 percent set for the available disk space alert for the logs	✗
38	2 minutes ago		Check that there are alerts to monitor the available disk space for the Firewall logs	✓
39	2 minutes ago		Check Firewall logs are being saved on a remote log server	✓
40	2 minutes ago		Check 'Implicit Deny Rule' is defined in Firewall Rule Base	✓
41	2 minutes ago		Check SSH-SSL deep inspection enabled on FGT with App Control enabled	✗
42	2 minutes ago		Check the SSH-SSL deep inspection with the App Control enabled drops traffic from servers with invalide certificate	✗
43	2 minutes ago		Check daily scheduled update enabled for the Application database	✓
44	2 minutes ago		Check the Application Database auto-update enabled	✓
45	2 minutes ago		Check App Control policy blocks proxy applications	✗
46	2 minutes ago		Check App Control policy blocks P2P applications	✗
47	2 minutes ago		Check App Control policy blocks File storage applications	✗
48	2 minutes ago		Check AV scan is activated according to the policy	✗
49	2 minutes ago		Check daily scheduled update enabled for the AV database	✓
50	2 minutes ago		Check the AV signature database auto-update enabled	✓

4 МЕСТО

УПРАВЛЕНИЕ ВСЕМ ИЗ ОДНОЙ КОНСОЛИ

3 МЕСТО

2FA ПРИ УДАЛЕННОМ ДОСТУПЕ

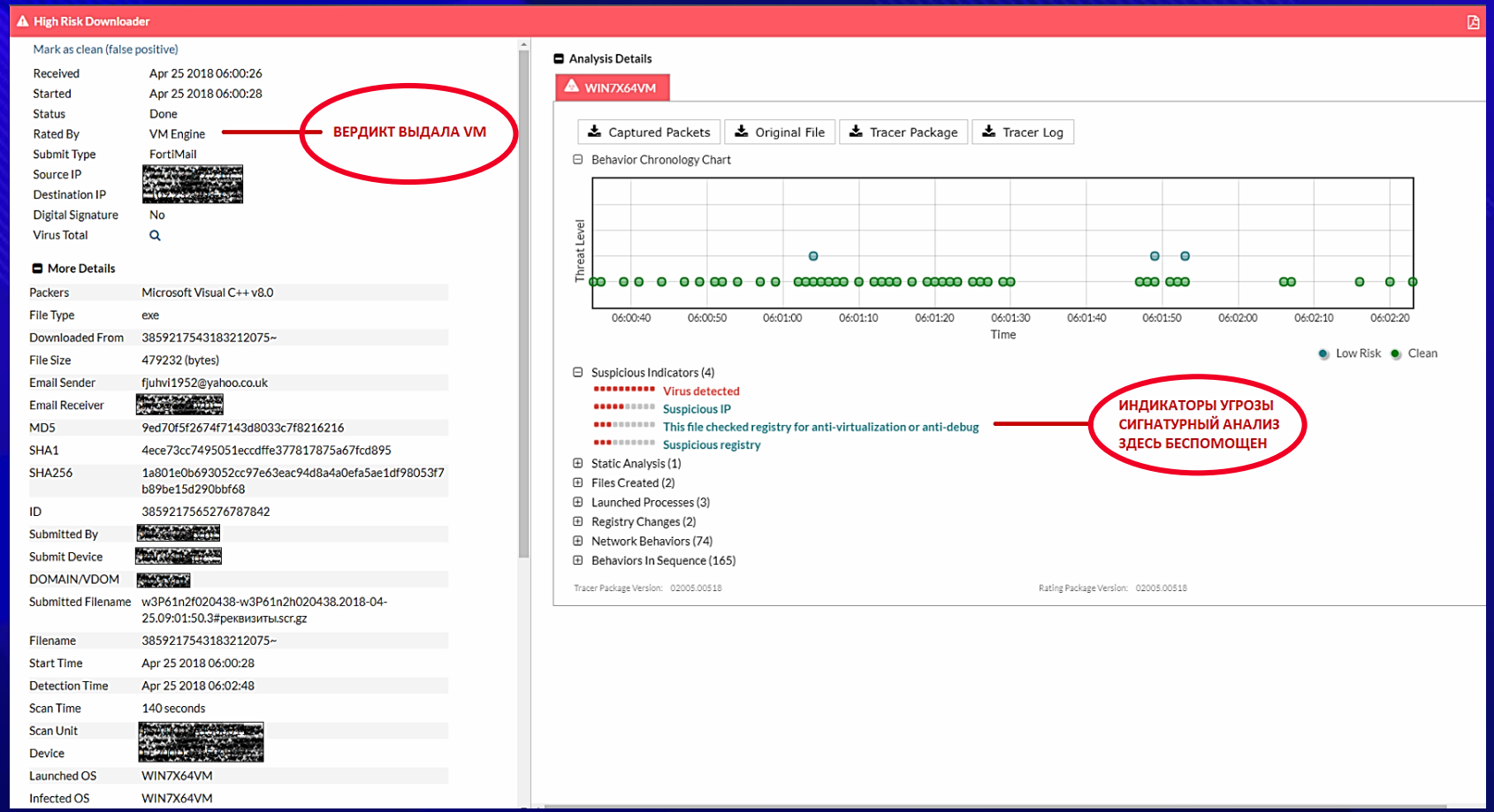


2 МЕСТО

А ДЛЯ ТЕХ КТО ЛЮБИТ ОЛДСКУЛ И ПРЕДАННЫХ ФАНАТОВ ЗМЕЙКИ…ПРИХОДЯТ СМС

1 МЕСТО

ГДЕ АТАКА? ВОТ ЖЕ ОНА…



ПОДВОДИМ ИТОГИ

- ## В НОГУ СО ВРЕМЕНЕМ

  ПОЛНОЦЕННЫЕ NGFW С SSL-ИНСПЕКЦИЕЙ,
  КОНТРОЛЕМ ПРИЛОЖЕНИЙ И МНОГИМ ДРУГИМ

- ## С РАСЧЕТОМ НА БУДУЩЕЕ

  EOL ТЕПЕРЬ НЕ СТРАШЕН

- ## БЕЗОПАСНЕЕ

  ЗАЩИТА ОТ ЦЕЛЕНАПРАВЛЕННЫХ АТАК И 2FA

10 YEARS JETSECURITY CONFERENCE 2019

СПАСИБО ЗА ВНИМАНИЕ!

Дмитрий Борисов

Инженер-проектировщик по ИБ
dp.borisov@jet.su