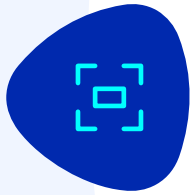
31/05/2018

ПРАКТИКА ЛОВЛИ ХАКЕРОВ НА БЛЕСНУ: ОПЫТ ПРИМЕНЕНИЯ DECEPTION-TOOLS

Анна Богданова

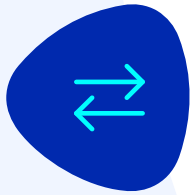
Руководитель направления SOC ЦИБ АО «Инфосистемы Джет»
av.bogdanova@jet.msk.su / +7 916 784-70-95

ПРОБЛЕМАТИКА



Периметровые средства не дают
100%-защиты от современных атак

С помощью SIEM-систем
сложно задетектировать APT-атаки

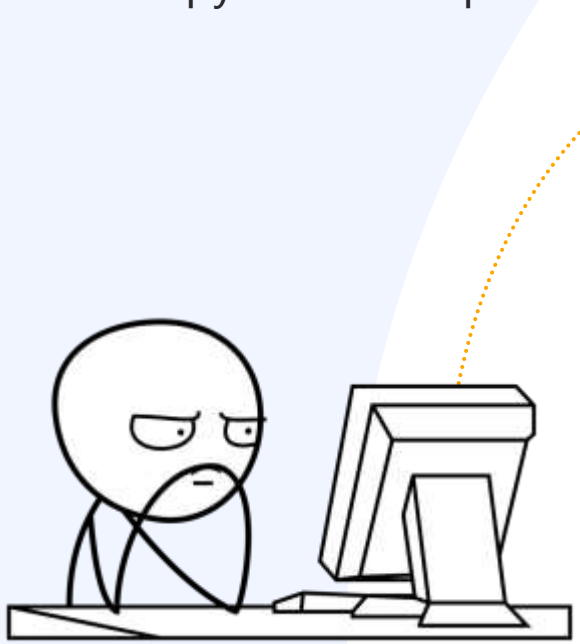


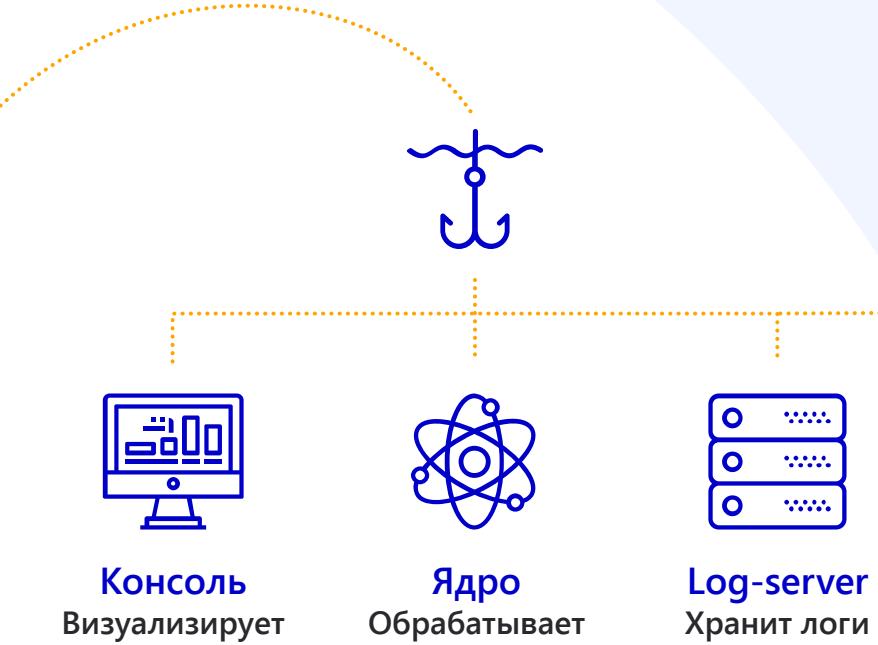
Зачастую горизонтальный трафик в сети
никак не контролируется

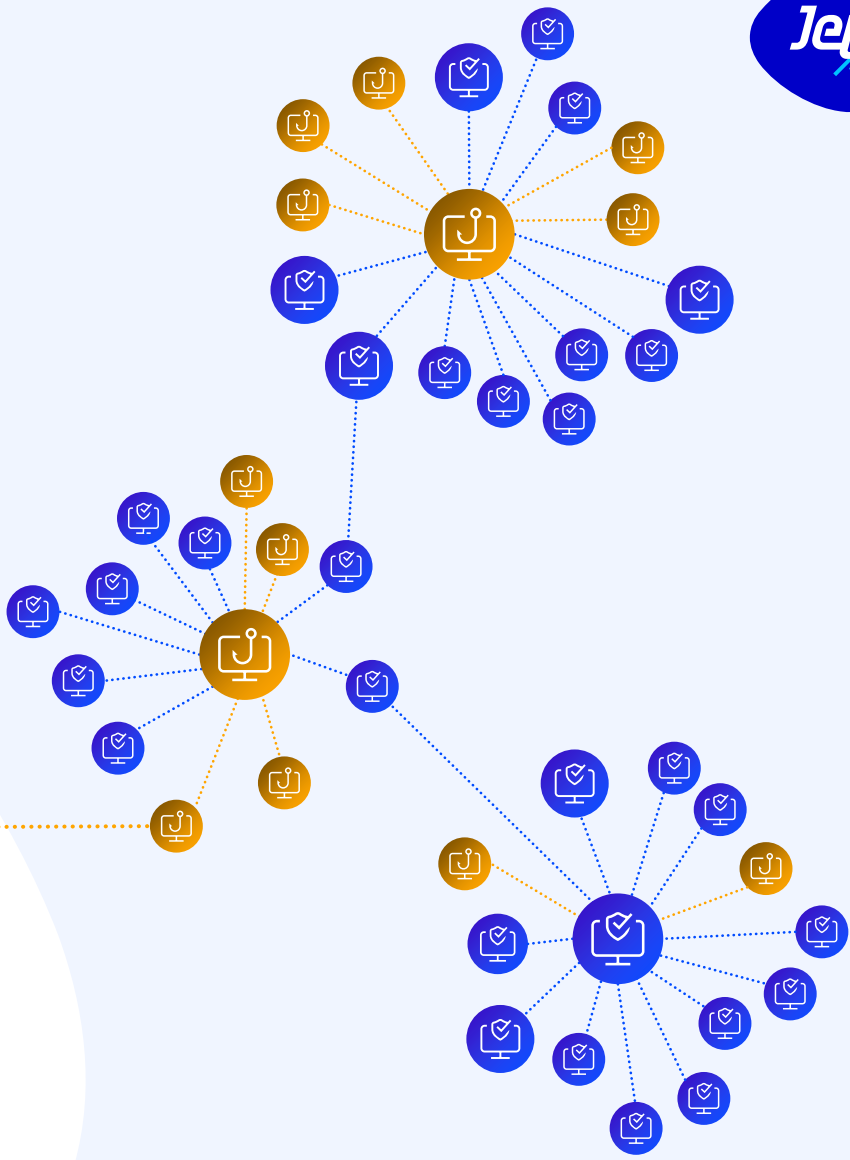
Shadow IT,
Bring Your Own Device

DECEPTION-РЕШЕНИЯ

- Потомки классических honey pot'ов
- Своего рода «сигнальные сети», состоящие из поддельных «условно уязвимых» узлов
- Распределенные системы обнаружения вторжений





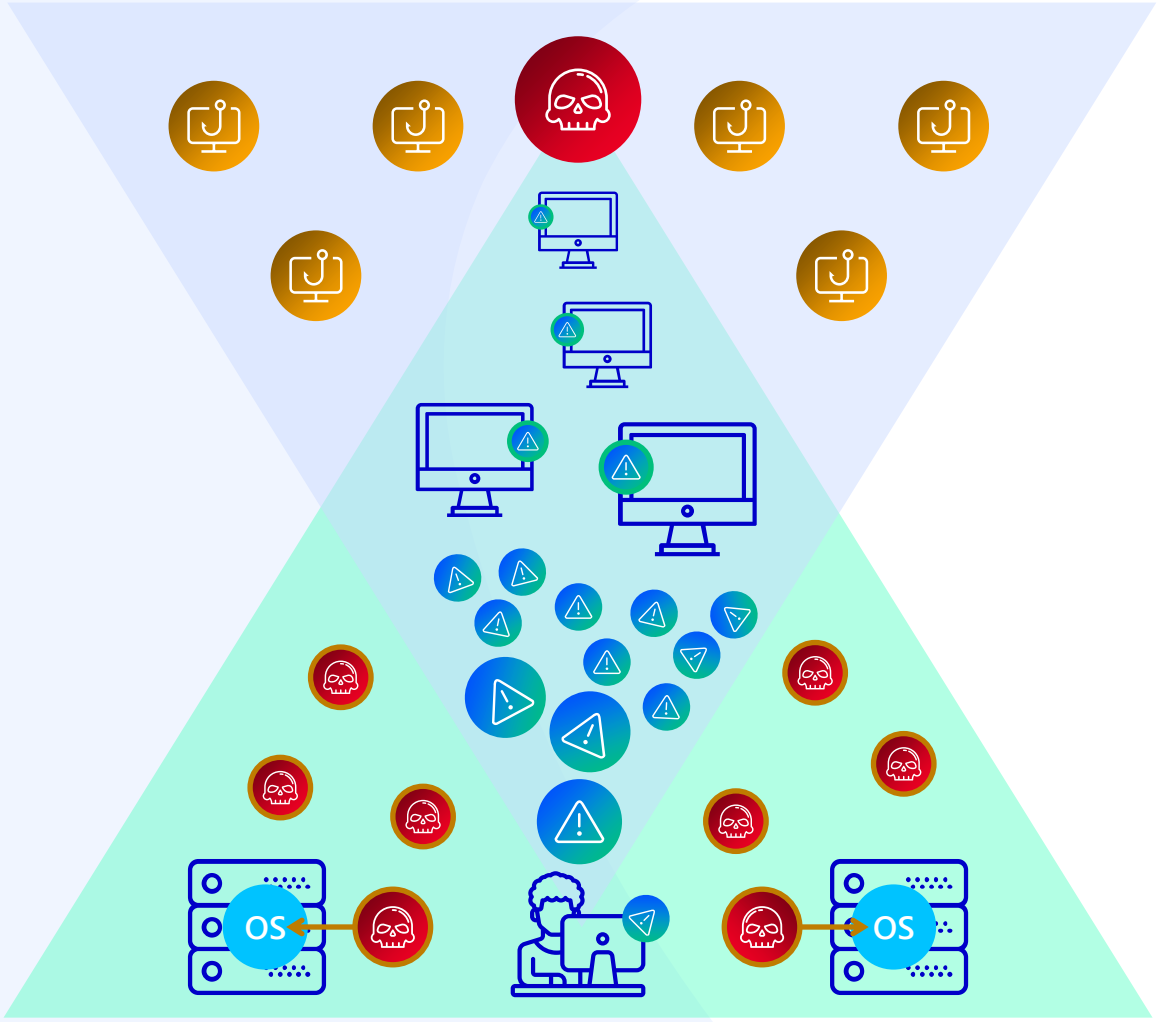


TRAPX DECEPTION GRID

Токены (приманки)

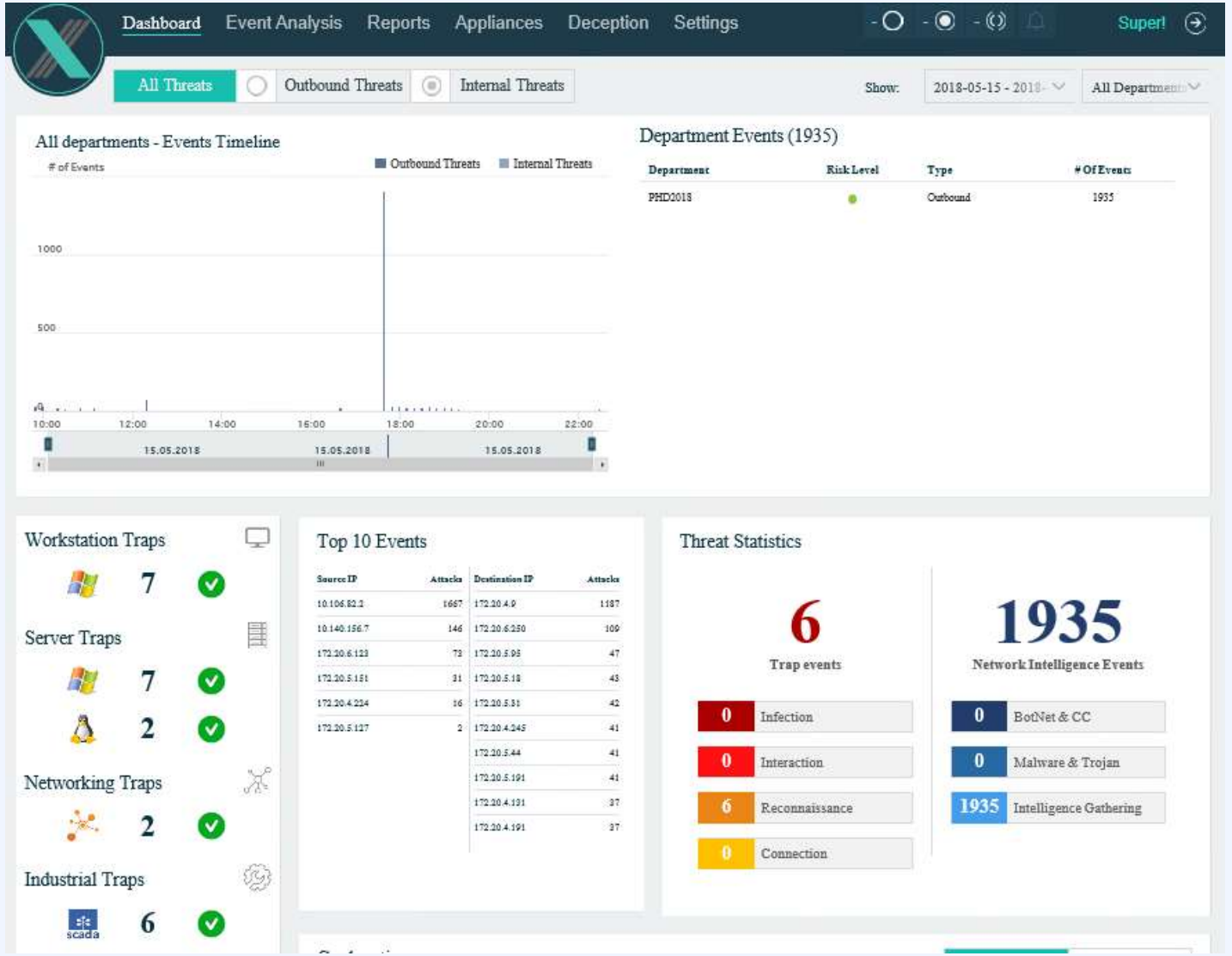
Сетевые сенсоры (ловушки)

Full OS Clones



TRAPX ДЛЯ ЗАЩИТЫ SCADA НА PHDAYS

TRAPX ДЛЯ ЗАЩИТЫ SCADA НА PHDAYS

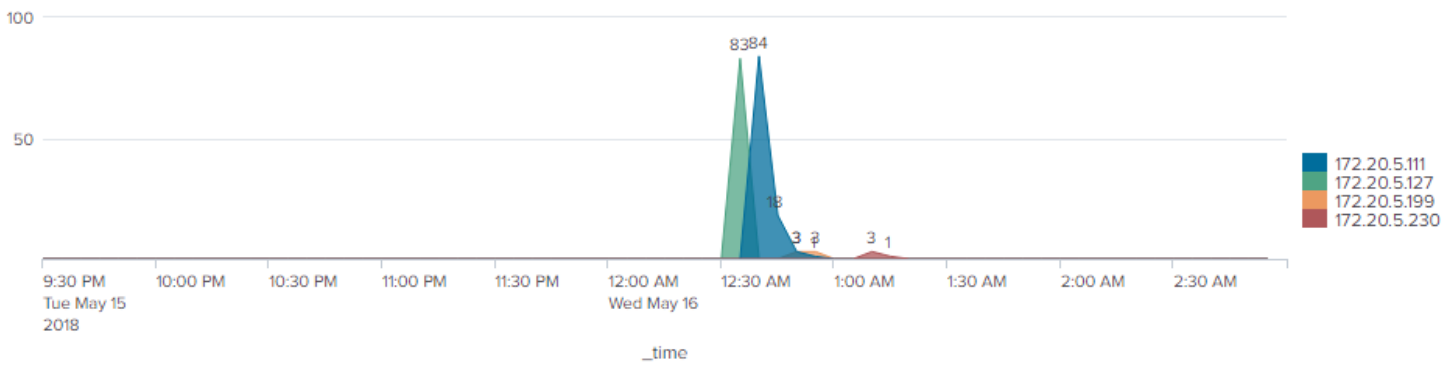


TRAPX ДЛЯ ЗАЩИТЫ SCADA НА PHDAYS

Network activity PHD

Edit | Export | ...

Активность между защищаемыми сетями. Сервисы



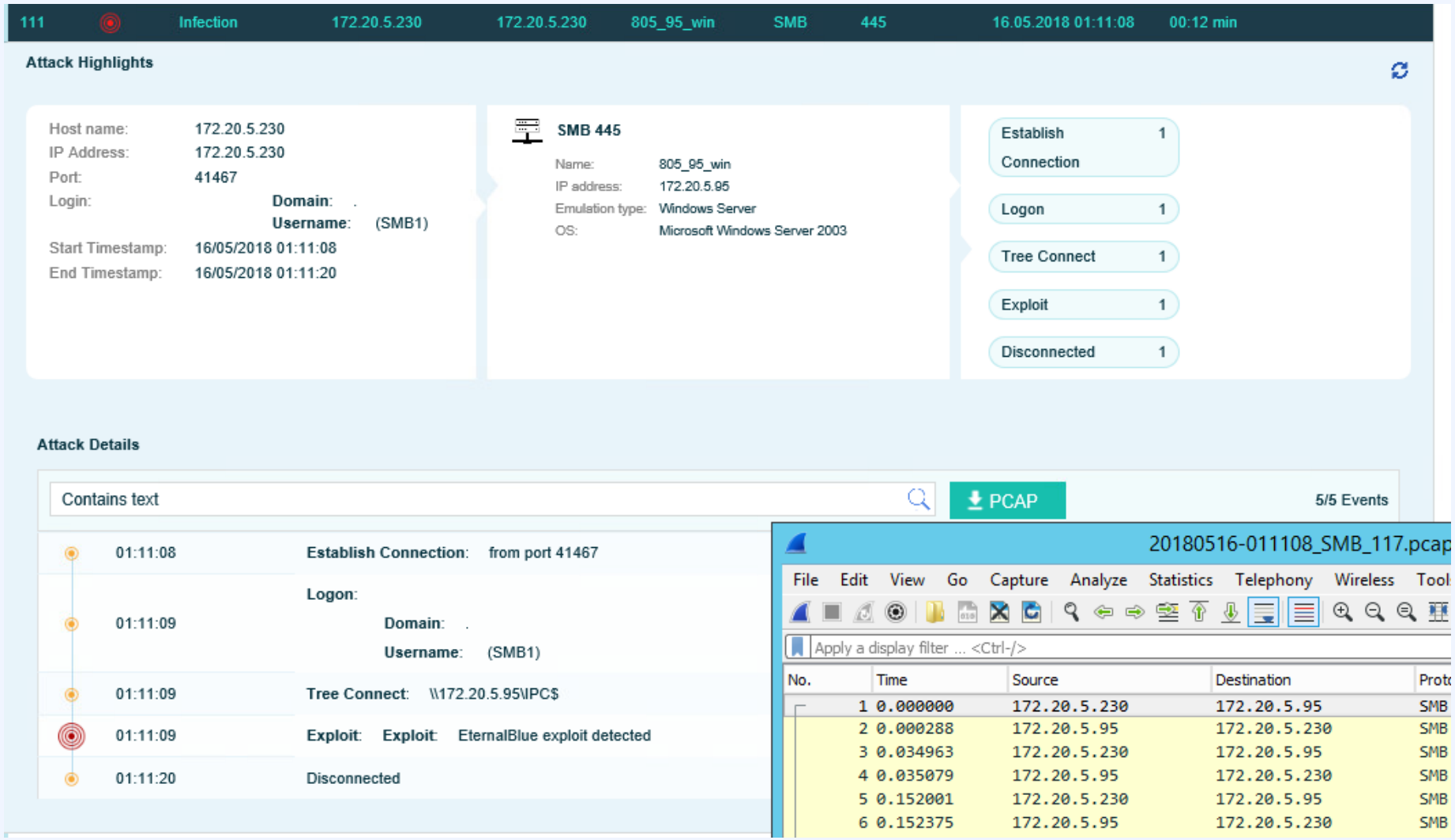
TrapX. Источники атак (1час)

src	dst count	count
172.20.5.230	3	44
172.20.5.111	3	41
172.20.5.199	4	38
172.20.5.127	4	20
172.20.4.224	5	16
172.20.5.133	1	1

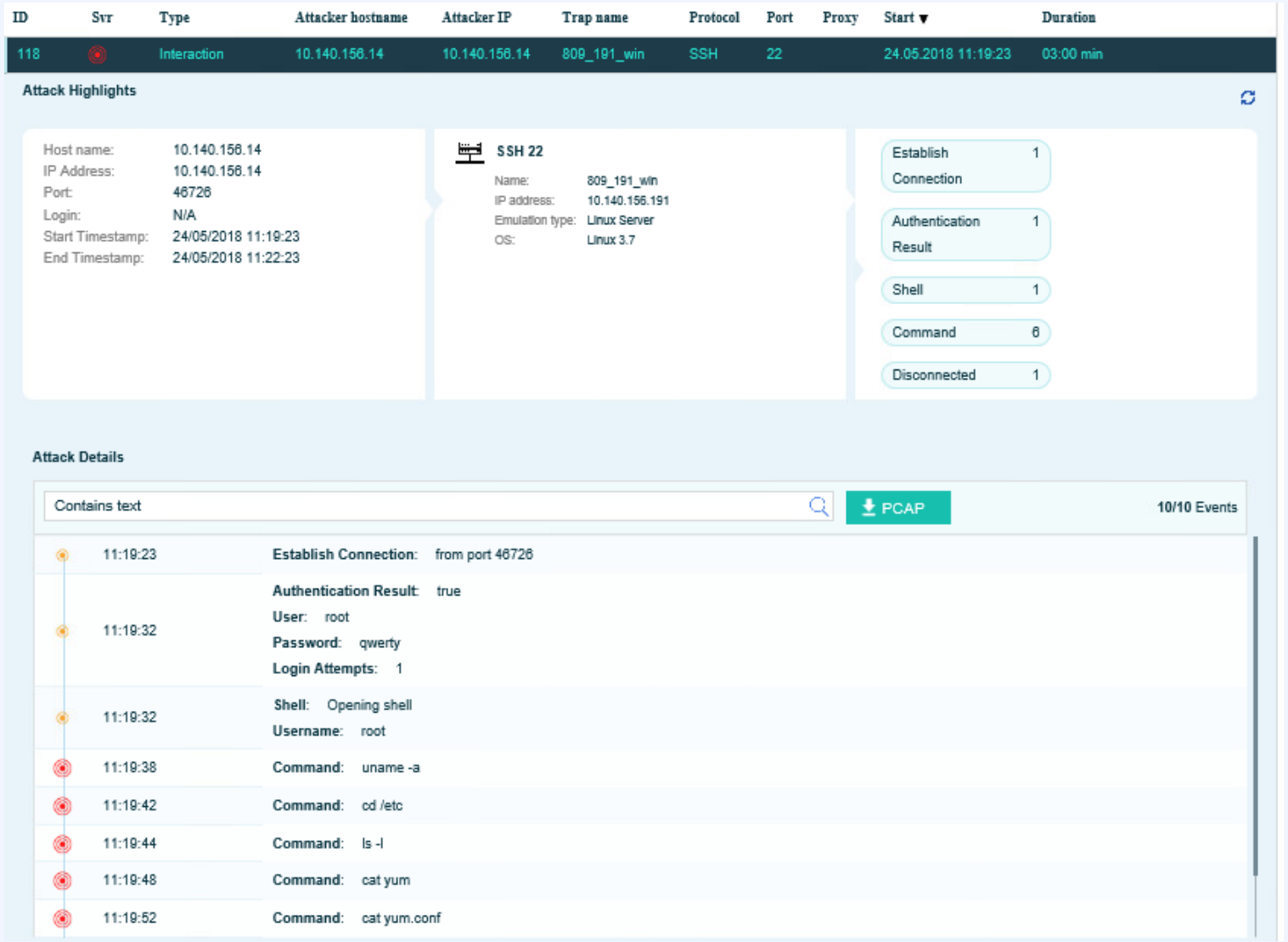
TrapX. Цели атак (1час)

dst	count
172.20.4.9	222
172.20.5.18	47
172.20.5.44	38
172.20.5.95	29
172.20.5.31	19
172.20.5.191	11

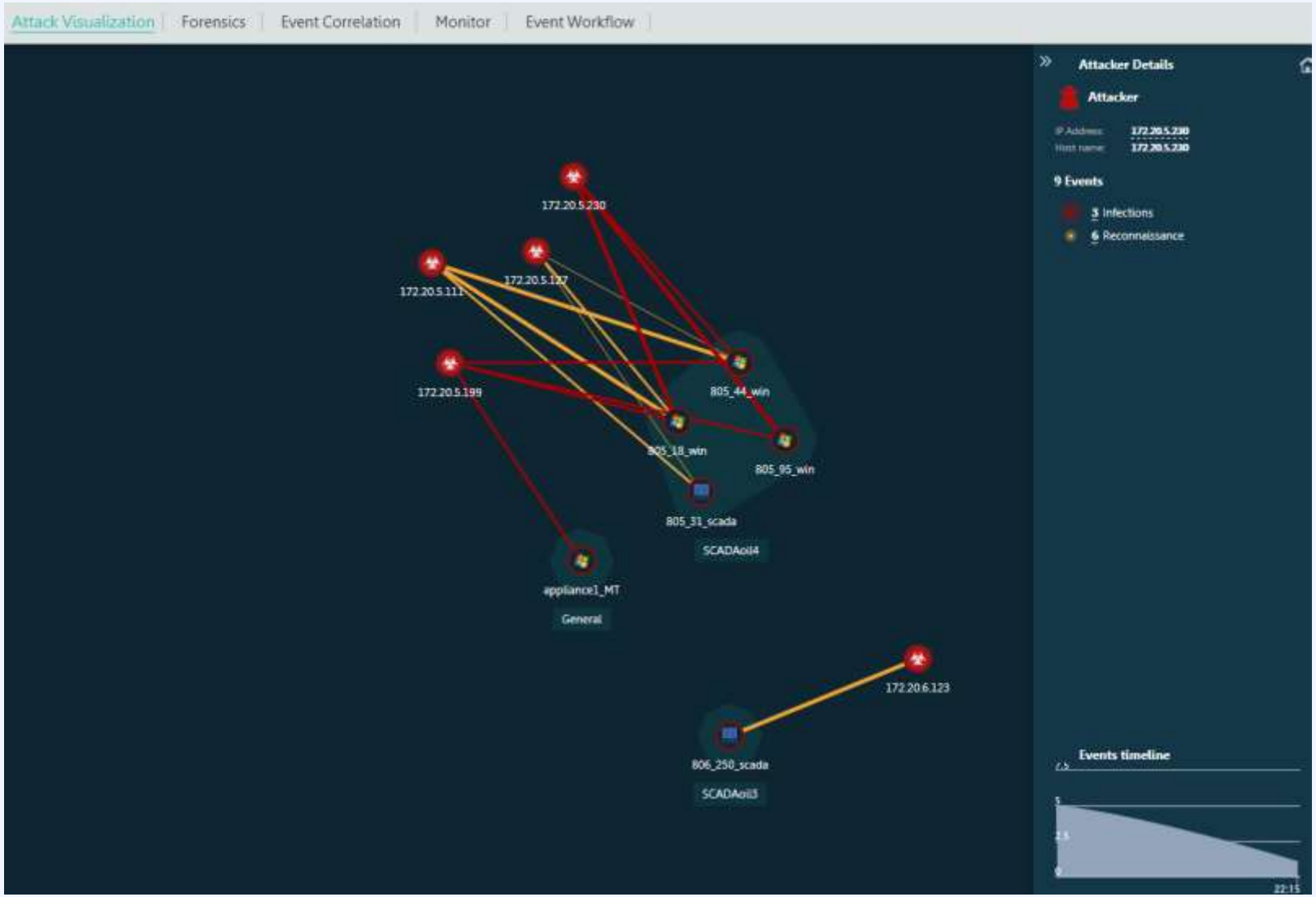
TRAPX ДЛЯ ЗАЩИТЫ SCADA НА PHDAYS



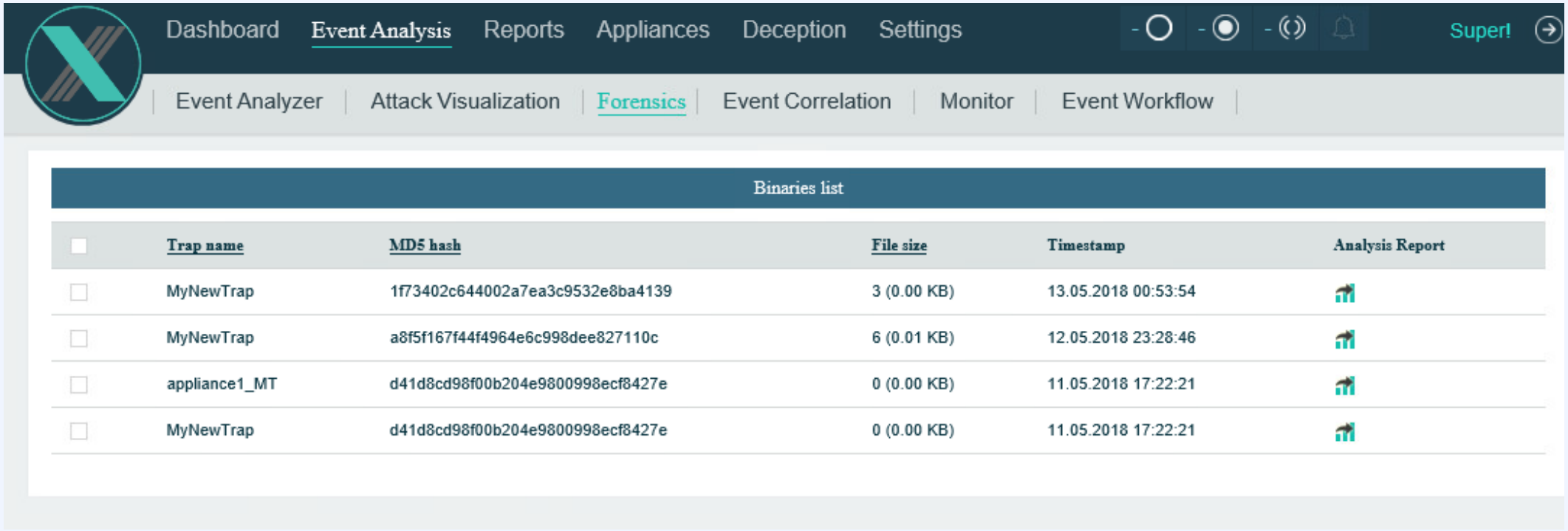
TRAPX ДЛЯ ЗАЩИТЫ SCADA НА PHDAYS



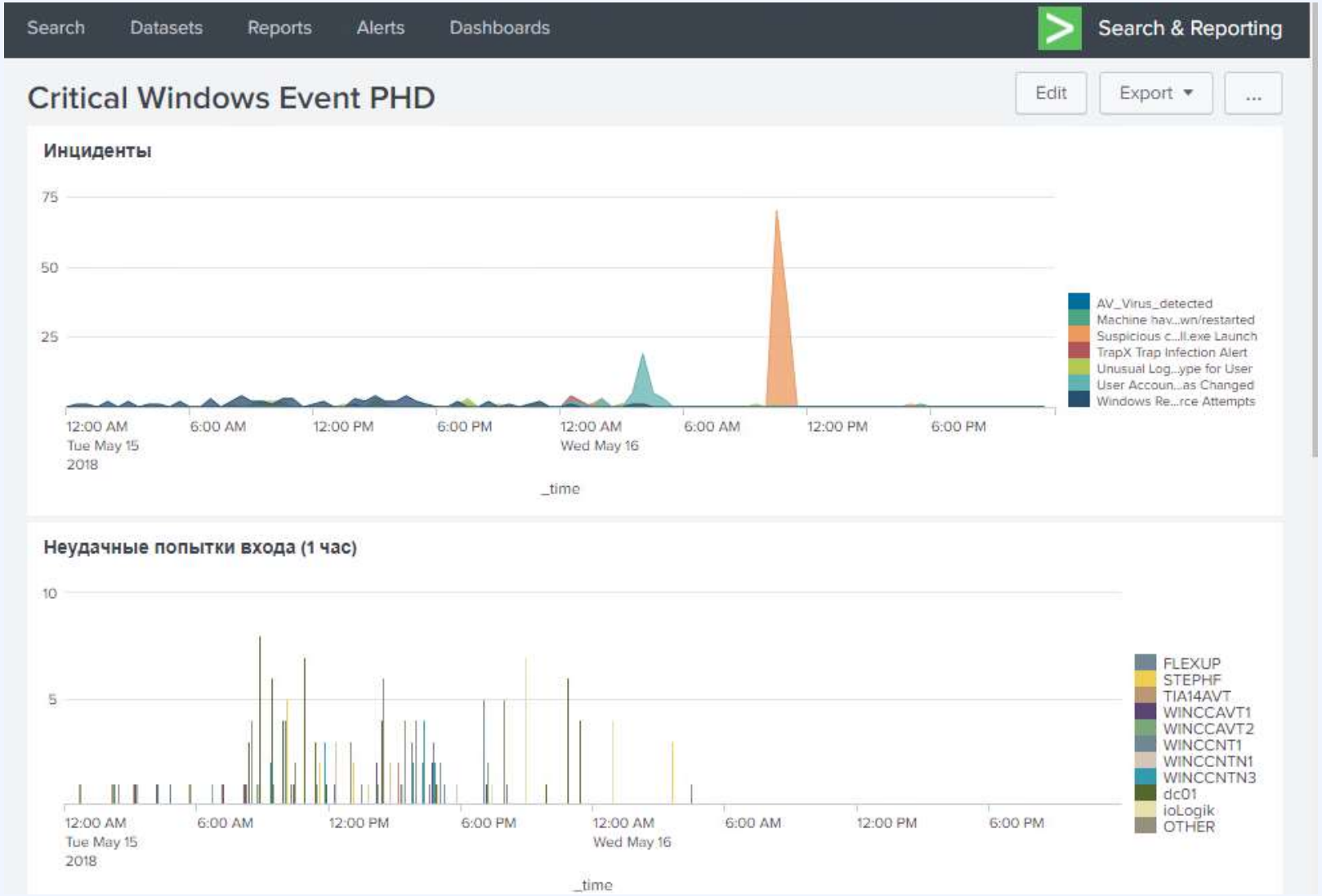
TRAPX ДЛЯ ЗАЩИТЫ SCADA НА PHDAYS



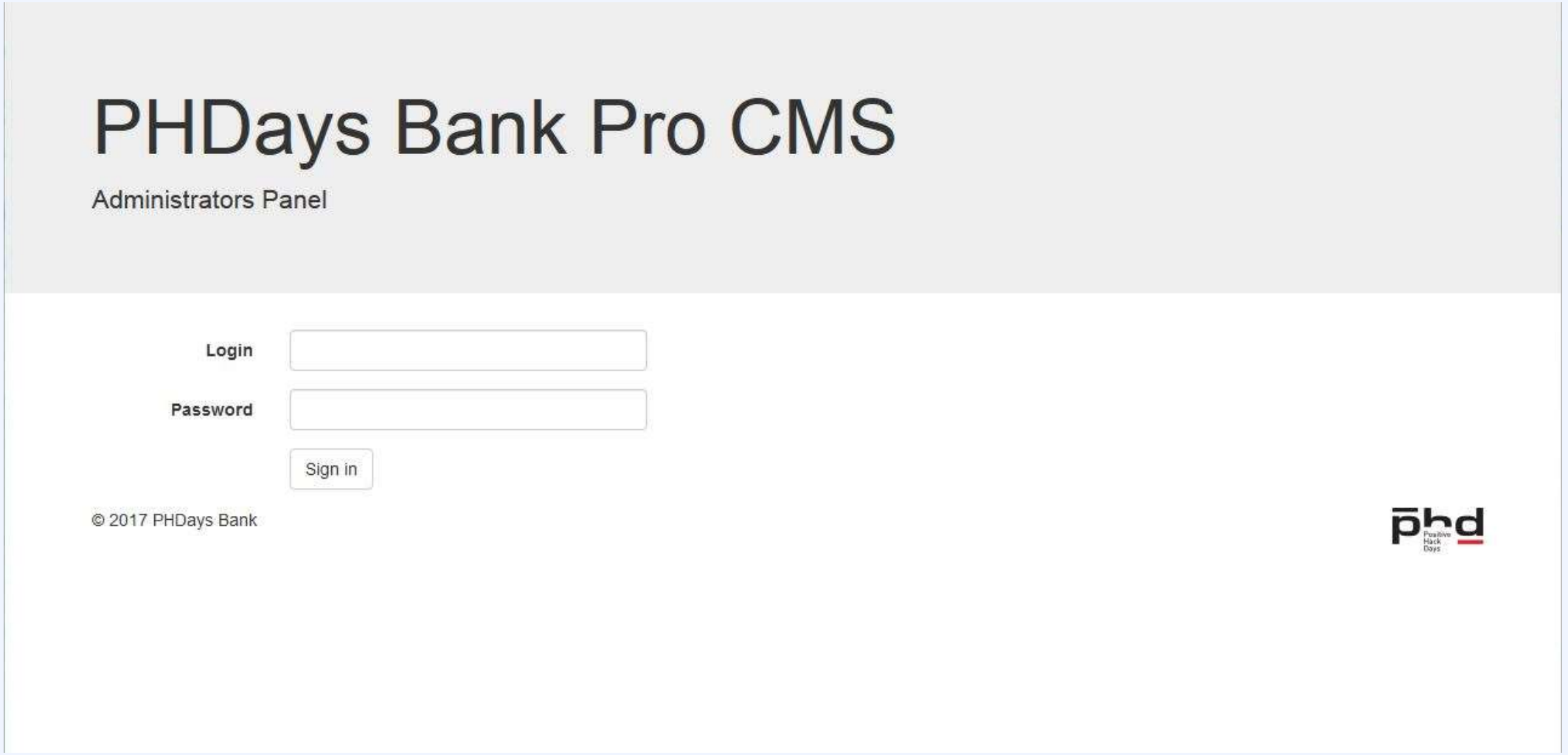
TRAPX ДЛЯ ЗАЩИТЫ SCADA НА PHDAYS



TRAPX ДЛЯ ЗАЩИТЫ SCADA НА PHDAYS



HONEY POT ДЛЯ ЗАЩИТЫ БАНКА НА PHDAYS



31/05/2018

СПАСИБО ЗА ВНИМАНИЕ!

Анна Богданова

Руководитель направления SOC ЦИБ АО «Инфосистемы Джет»
av.bogdanova@jet.msk.su / +7 916 784-70-95