Kaspersky Industrial Cybersecurity Conference

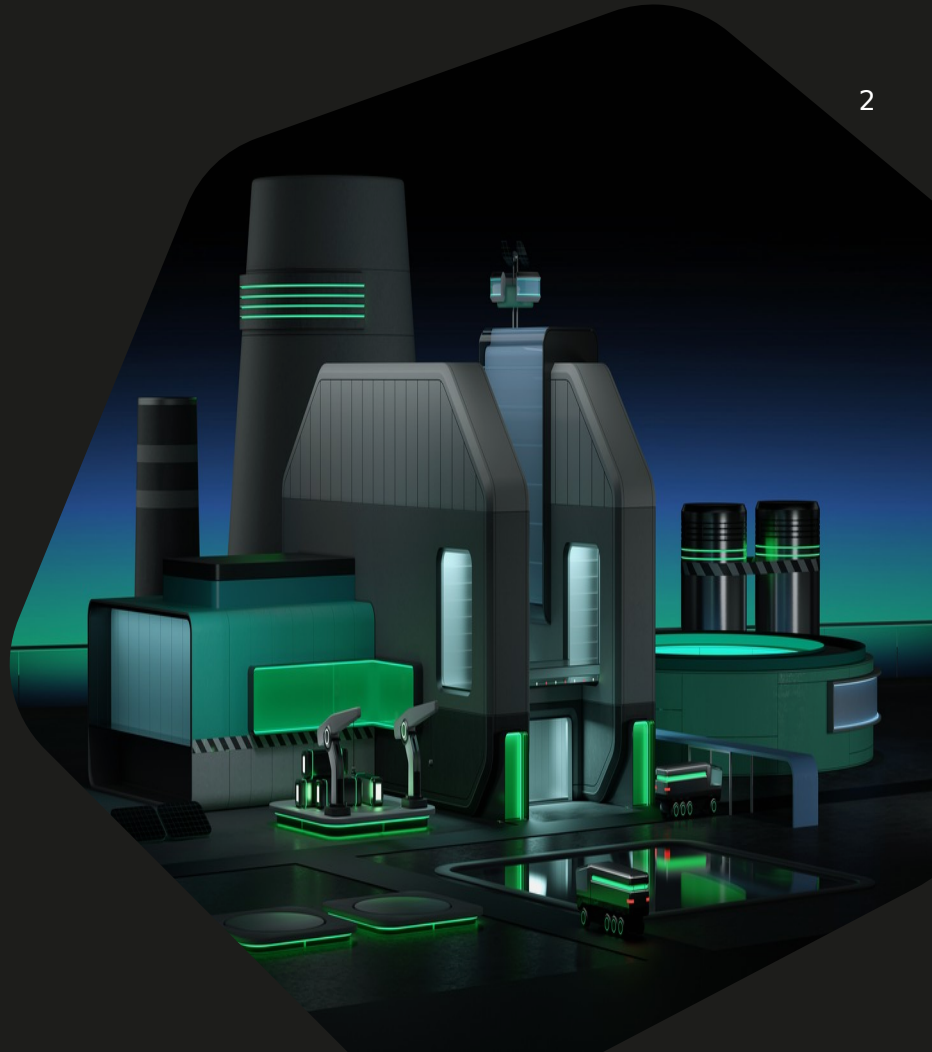
Пассивное обнаружение активов в технологических сетях

Ежов Роман

kaspersky

Почему это важно?

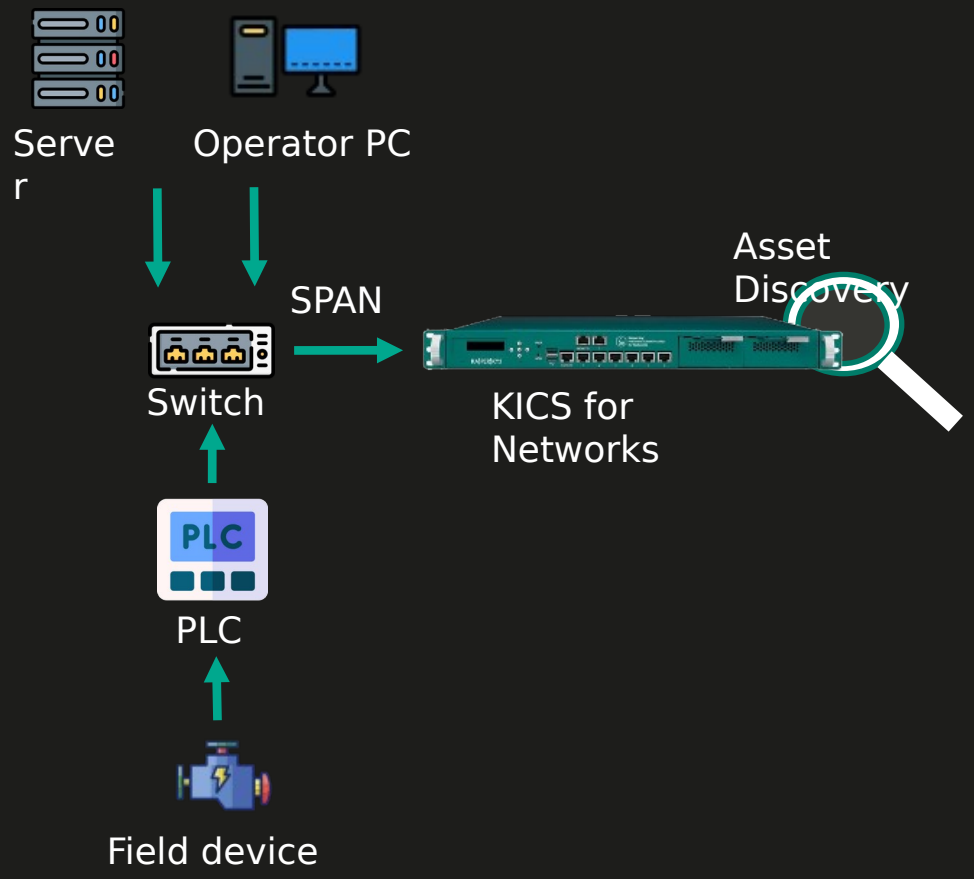
- Сетевая архитектура, какая она есть
- Отслеживание состояния активов
- Новые устройства в сети
- Уязвимые устройства
- Аномальные коммуникации активов



CONTROL 01 Inventory and Control of Enterprise Assets	5 Safeguards	IG1 2/5	IG2 4/5	IG3 5/5
CONTROL 02 Inventory and Control of Software Assets	7 Safeguards	IG1 3/7	IG2 6/7	IG3 7/7
CONTROL 03 Data Protection	14 Safeguards	IG1 6/14	IG2 12/14	IG3 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software	12 Safeguards	IG1 7/12	IG2 11/12	IG3 12/12
CONTROL 05 Account Management	6 Safeguards	IG1 4/6	IG2 6/6	IG3 6/6
CONTROL 06 Access Control Management	8 Safeguards	IG1 5/8	IG2 7/8	IG3 8/8
CONTROL 07 Continuous Vulnerability Management	7 Safeguards	IG1 4/7	IG2 7/7	IG3 7/7
CONTROL 08 Audit Log Management	12 Safeguards	IG1 3/12	IG2 11/12	IG3 12/12
CONTROL 09 Email and Web Browser Protections	7 Safeguards	IG1 2/7	IG2 6/7	IG3 7/7
CONTROL 10 Malware Defenses	7 Safeguards	IG1 3/7	IG2 7/7	IG3 7/7
CONTROL 11 Data Recovery	5 Safeguards	IG1 4/5	IG2 5/5	IG3 5/5
CONTROL 12 Network Infrastructure Management	8 Safeguards	IG1 1/8	IG2 7/8	IG3 8/8
CONTROL 13 Network Monitoring and Defense	11 Safeguards	IG1 0/11	IG2 6/11	IG3 11/11
CONTROL 14 Security Awareness and Skills Training	9 Safeguards	IG1 8/9	IG2 9/9	IG3 9/9
CONTROL 15 Service Provider Management	7 Safeguards	IG1 1/7	IG2 4/7	IG3 7/7
CONTROL 16 Applications Software Security	14 Safeguards	IG1 0/14	IG2 11/14	IG3 14/14
CONTROL 17 Incident Response Management	9 Safeguards	IG1 3/9	IG2 8/9	IG3 9/9
CONTROL 18 Penetration Testing	5 Safeguards	IG1 0/5	IG2 3/5	IG3 5/5

https://www.cisecurity.org/controls/v8

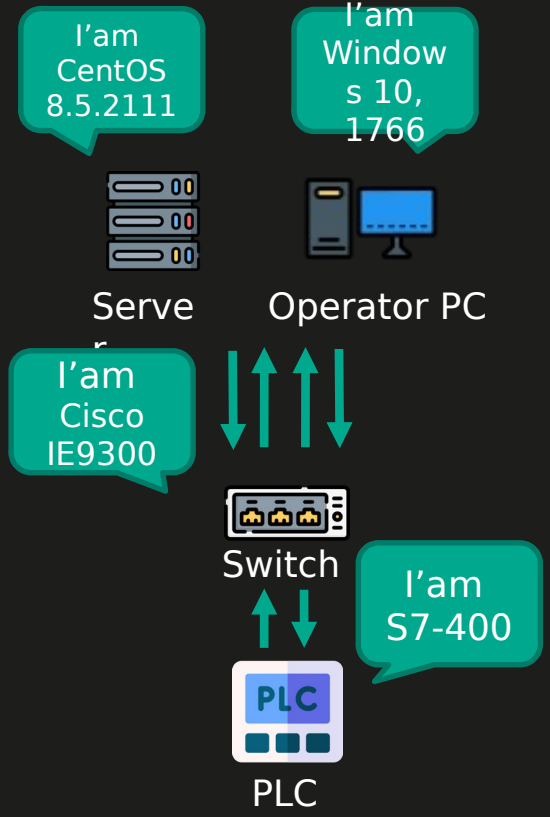
Kaspersky Industrial CyberSecurity **for Networks**



Не генерирует дополнительный трафик
Не провоцирует СОВ
Нет рисков негативно повлиять на устройство

- Инвентаризация технологической сети:
  - Тип устройства
  - Производитель устройства
  - Операционная система
  - Модель устройства
  - Версии аппаратных элементов устройств
  - Версия прошивки
- Определение уязвимостей на устройствах
- Выявление нежелательной активности
- Расследование инцидентов

Устройства рассказывают о себе



Сигнатурные правила

- Устройства
- Операционные системы
- Протоколы
- Сервисы
- Производитель устройства

Фингерпринт правила

- Устройства
- Операционные системы

Формат правила Asset Discovery


```
asset_rule:
    id:
    confidence: 1-100
    message: "Name rule"
    protocols: [ ]
    ports: {}
    prefilter: {
        pattern: "regex",
        flags: "Hsi"
    }
    host:  {vendor: , key: src_ip}
    asset: {type: hardware, key: AssetKey_Cpu, pattern: "regex"}
    asset: {type: hardware, key: AssetKey_HwVer, pattern: "regex"}
    asset: {type: hardware, key: AssetKey_Model, pattern:  "regex"}
    asset: {type: hardware, key: AssetKey_HardwareVersion, pattern: "regex"}
    asset: {type: software, key: AssetKey_SoftwareVendor, description: local_key}
    asset: {type: software, key: AssetKey_SoftwareModel, pattern: "regex"}
    asset: {type: software, key: AssetKey_SoftwareVersion, pattern: "regex"}
    asset: {type: software, key: AssetKey_SoftwareVersion, pattern: "regex", post_processor: convert_to_hex}
```

Определение производителя устройства

00:00:54: ff:ac:
44:0f

Schneider Electric

https://gist.github.com/aallan/b4bb86db86079509e6159810ae9bd3e4

DHCP : \\x35.+\\x3d.+\\x0c.+\\x3c.MSFT5\\.0.*\\x37.\\x01\\x0f\\x03\\x06\\x2c\\x2e\\x2f\\x1f\\x21\\x79\\xf9\\x2b

MAILSLOT : ^\\x11.{7}\\x00\\x8a..\\x00\\x00.+\\\\MAILSLOT\\\\BROWSE.{23}\\x04\\x00

SSDP : SERVER:\\s*(Microsoft\\-Windows\\/[\\d\\.]*|Linux\\/[\\d\\.]*)

MDNS : [^\\w\\-\\.]{2}([\\w\\-\\.]{3,})[^\\w\\-\\.]local

LLMNR : ^.{13}[^\\x00]+\\x00.{5}([\\w_\\-\\.]{3,})\\x00

HTTP User-Agent : ^(GET|CONNECT).+HTTP/(0\\.9|1\\.0|1\\.1).+User-Agent:.+Windows\\sNT\\s6\\.0

NTLMSSP : NTLMSSP\\x00\\x02\\x00\\x00\\x00.{8}.{4}.{8}\\x00{8}.{8}\\x04\\x5a\\xb8\\x0b

Дамп Vnet\IP


```
0000   00 15 5d 05 ca 14 00 00 64 95 56 dc 08 00 45 62   ..]....d.V...Eb
0010   02 54 01 2f 00 00 01 11 32 61 c0 a8 01 03 c0 a8   .T./....2a......
0020   01 54 85 46 26 d4 02 40 7f 1d 02 21 00 30 00 00   .T.F&..@...!.0..
0030   02 38 80 00 b6 e4 c4 91 00 00 00 00 00 00 00 00   .8..............
0040   00 00 00 00 00 00 21 10 00 07 00 00 02 14 01 2a   ..*
0050   01 01 02 0e 90 78 94 b1 22 32 0c 00 81 78 02 c1   x..
0060   01 00 00 01 02 01 00 00 00 00 00 00 00 00 00 00   ................
0070   00 00 00 00 00 00 01 e8 00 01 00 00 00 00 00 00   ................
0080   00 00 00 00 00 00 00 00 00 00 46 43 53 30 31 30   ..........FCS010
0090   31 00 41 46 56 31 30 44 2d 33 52 36 2e 30 37 2e   1.AFV10D-3R6.07.
00a0   30 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00   00..............
00b0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00c0   00 00 00 01 00 02 00 0f 00 00 00 00 c8 78 60 39   .............x`9
00d0   8c f7 00 00 00 00 00 03 00 00 00 00 00 00 00 00   ................
00e0   00 00 00 00 00 00 00 00 30 31 60 39 8c f7 00 00   ................
00f0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0100   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0110   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0120   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0130   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0140   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0150   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0160   00 00 00 04 ff ff 53 42 33 30 31 00 00 00 00 00   ......SB301.....
0170   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0180   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0190   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
01a0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
01b0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

Контроллер

Потенциальное обозначение контроллера в проекте

Системное ПО Centum VP

Коммуникационный модуль шины ESB

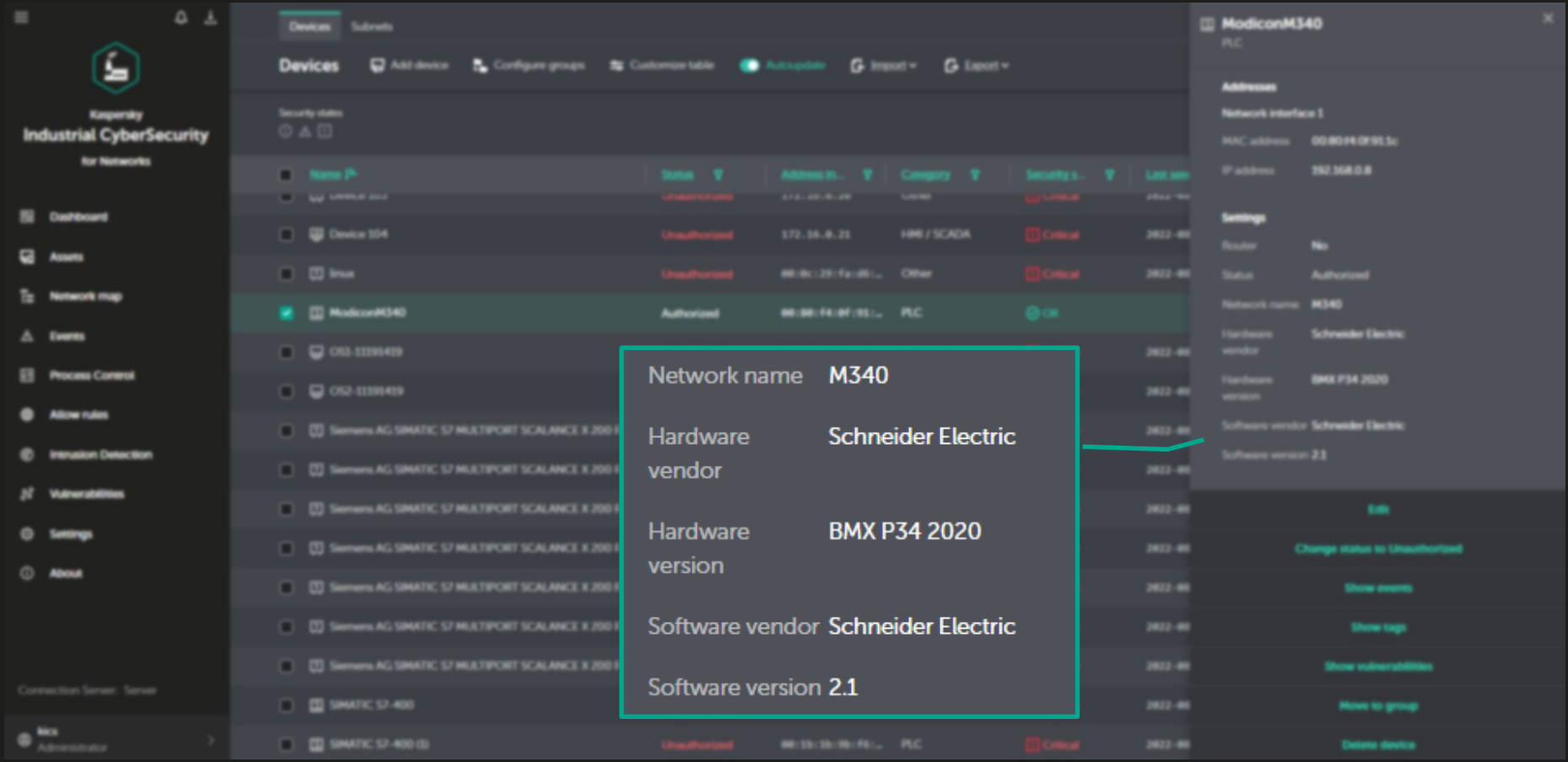
Дамп Umas

Версия прошивки

Процессорный модуль

```
0000   a0 d3 c1 27 7d 71 f4 0f 1b 76 e3 9d 08 00 45 00   ...'}q...v....E.
0010   00 66 00 48 40 00 40 06 30 78 0a e2 7a 8a 0a e2   .f.H@.@.0x..z...
0020   79 84 01 f6 ef 95 3c 3e 89 23 30 4f f2 c3 50 18   y.....<>.#0O..P.
0030   20 58 d0 e5 00 00 00 2a 00 00 00 38 00 5a 00 fe    X.....*...8.Z..
0040   06 30 01 03 00 00 00 00 10 02 00 00 08 00 06 01   .0..............
0050   03 01 00 00 00 00 0c 42 4d 58 20 50 33 34 20 32   .......BMX P34 2
0060   30 32 30 02 01 01 00 00 00 00 40 00 04 01 00 00   020......@.....
0070   00 00 3e 05                                       ..>.
```

Kaspersky Industrial CyberSecurity **for Networks**



Дамп Melsec System -Q


```
▸ Frame 2: 97 bytes on wire (776 bits), 97 bytes captured (776 bits)
▸ Ethernet II, Src: Mitsubis_44:bb:fe (08:00:70:44:bb:fe), Dst: VMware_c3:9b:00 (00:0c:29:c3:9b:00)
▸ Internet Protocol Version 4, Src:                Dst:
▸ Transmission Control Protocol, Src Port: 5002  Dst Port: 49163, Seq: 1, Ack: 60, Len: 43
▾ Data (43 bytes)
    Data: d10102000211117f000501fe070502e003000016009c080c080000000000040000000018…
    [Length: 43]
```

Header 1

```
0000  00 0c 29 c3 9b 00 08 00  70 44 bb fe 08 00 45 00   ··)····· pD····E·
0010  00 53 02 c4 00 00 fa 06  3b e1 c0 a8 00 4d c0 a8   ·S····· ;····M··
0020  00 62 13 8a c0 0b 06 11  83 e2 0d 0f 31 f6 50 18   ·b····· ····1·P·
0030  18 00 47 b7 00 00 d1 01  02 00 02 11 11 7f 00 05   ··G····· ........
0040  01 fe 07 05 02 e0 03 00  00 16 00 9c 08 0c 08 00   ........ ........
0050  00 00 00 00 04 00 00 00  00 18 27 0c 00 00 00 00   ........ ..'·····
0060  00                                                 ·
```

Command group

ID command

```
protocol_rule:
    id: 1000006
    confidence: 75
    message: "Melsec-Q Industrial Protocol"
    protocols: [tcp]
    prefilter: {
        pattern: "^\\xd1.{34}(\\x18\\x10|\\x18\\x11|\\x18\\x20|\\x18\\x22|\
                \\x18\\x24|\\x18\\x25|\\x18\\x26|\\x18\\x27|\\x18\\x28|\\x18\\x29|\\x18\\x2a|\\x04\\
x06|\
                \\x14\\x06|\\x04\\x03|\\x14\\x02|\\x04\\x01|\\x14\\x01|\\x08\\x01|\\x08\\x02|\\x06\\
x13|\
                \\x16\\x13|\\x06\\x01|\\x16\\x01|\\x10\\x01|\\x10\\x02|\\x10\\x03|\\x10\\x05|\\x10\\
x06|\
                \\x01\\x01|\\x14\\x05|\\x02\\x05|\\x12\\x07|\\x06\\x10|\\x16\\x10|\\x16\\x17|\\x06\\
x19|\
                \\x16\\x30|\\x16\\x31|\\x00\\x14|\\x0b\\x05|\\x00\\x16|\\x18\\x05|\\x18\\x18|\\x07\\
x01|\
                \\x18\\x2c)",
        flags: "Hsi"
    }
```

Фингерпринт стека TCP IP

ip_flags
ttl
tcp_flags
tcp_win_size
tcp_options

https://lcamtuf.coredump.cx/p0f3/

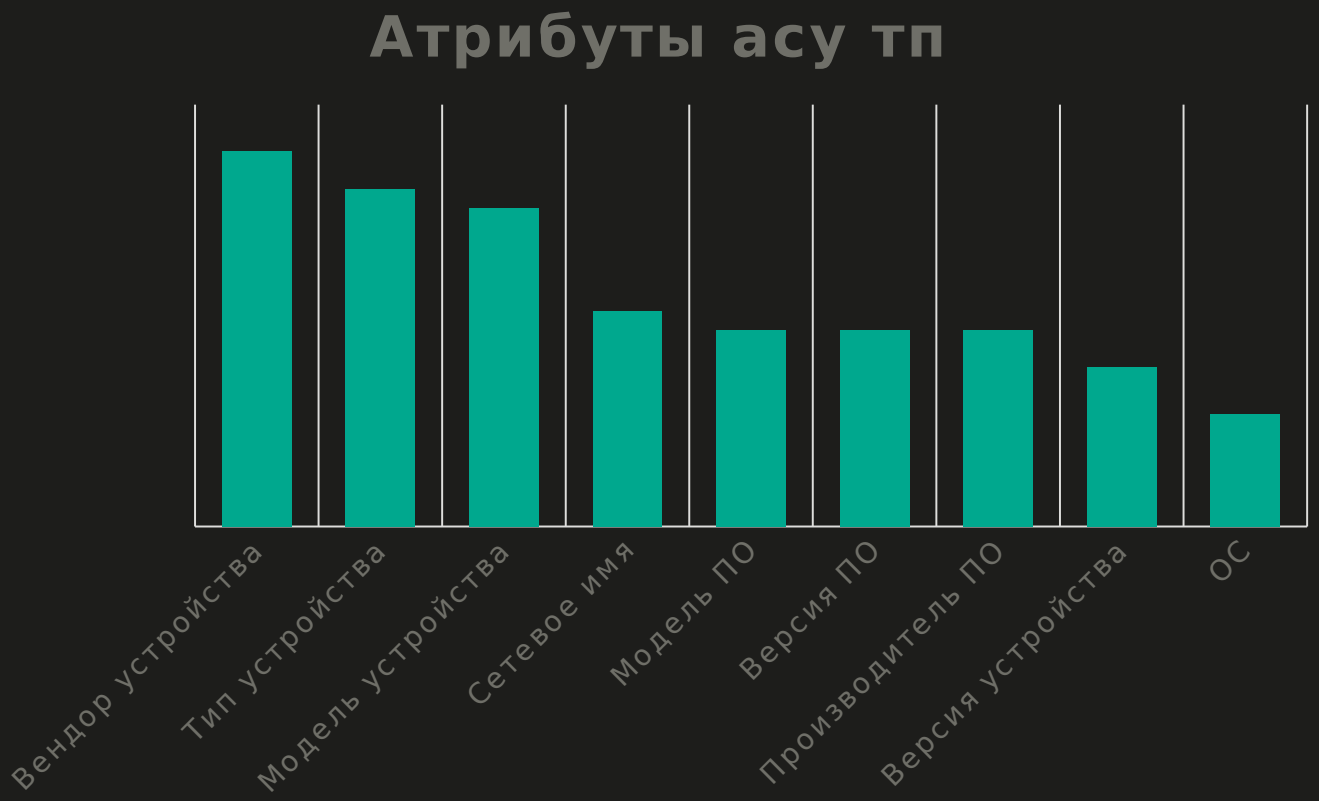
ip_flags = df
ttl = 64
tcp_flags = syn, ack
tcp_win_size = 8192
tcp_options = mss 1460, nop, ws 0

Дамп Modbus TCP

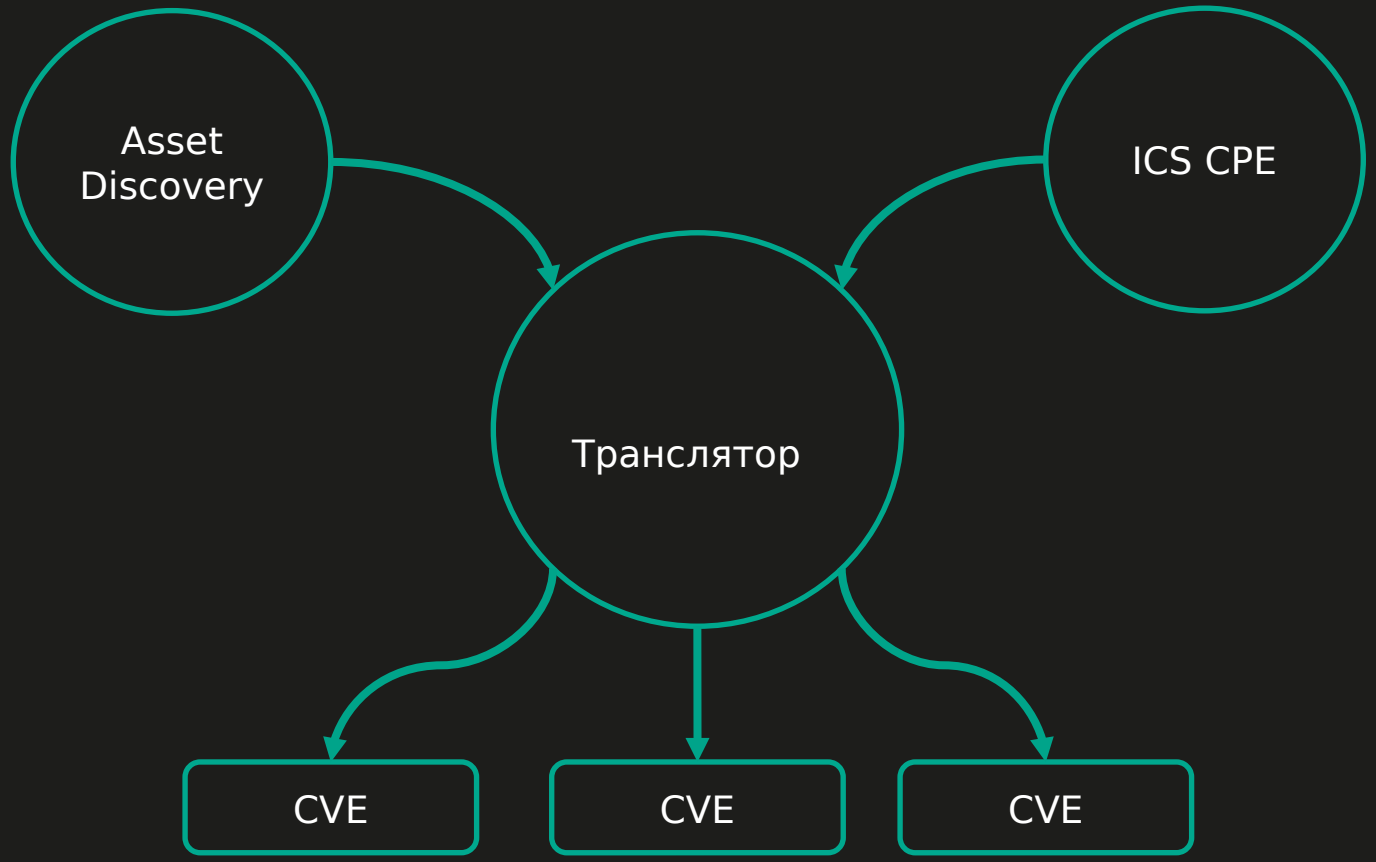
MBAP Header

Unit Identifier

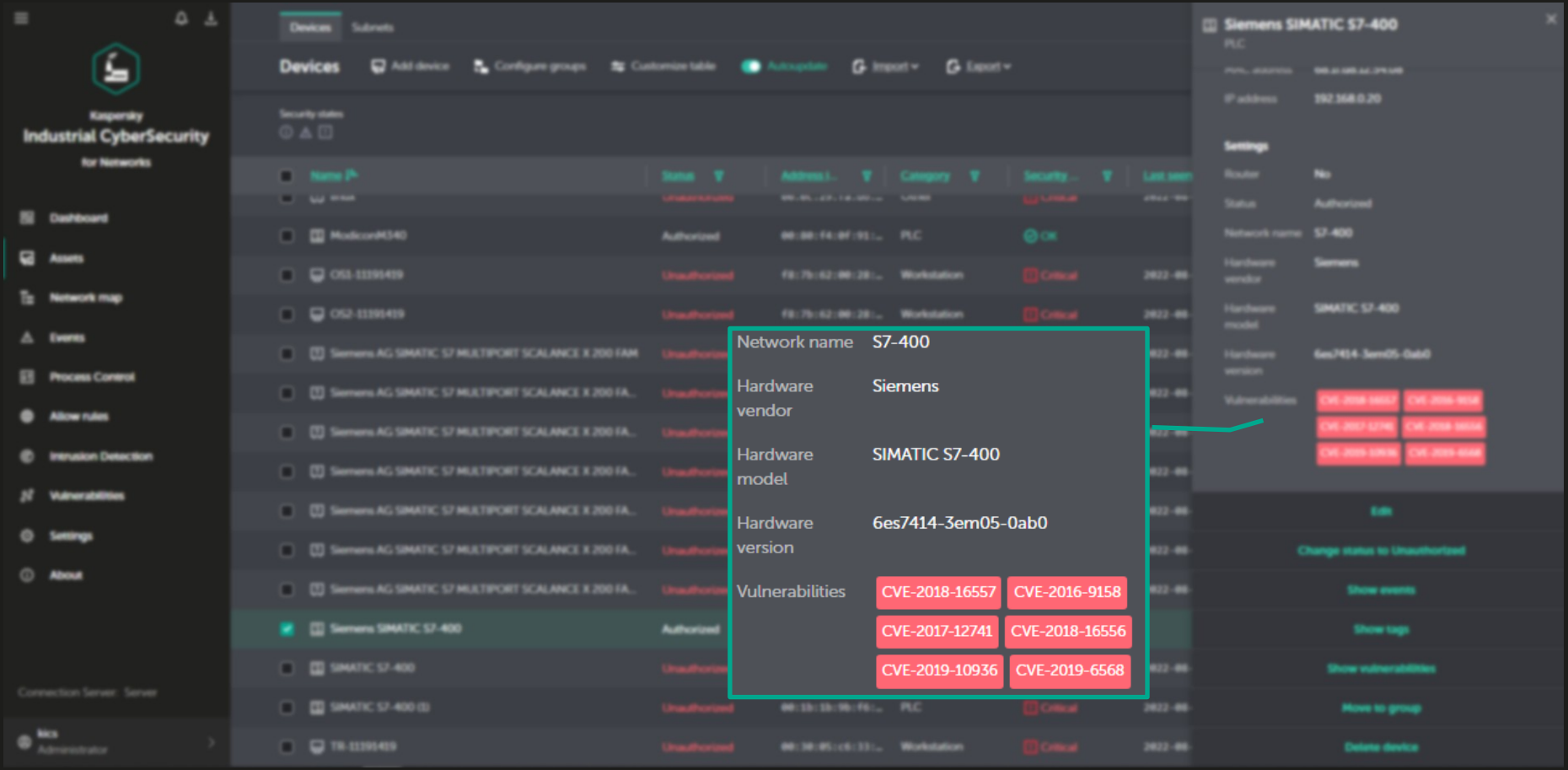
```
0000   00 0a 8d 02 1b 1a 00 ee 22 33 44 34 08 00 45 00
0010   00 34 26 83 40 00 80 06 52 ab c0 a8 00 22 c0 a8
0020   00 23 ce bc 01 f6 00 00 00 15 00 0c b8 74 50 18
0030   ff f0 a3 e5 00 00 00 00 00 00 00 06 01 04 00 01
0040   00 01
```


Атрибуты асу тп
Вендор устройства
Тип устройства
Модель устройства
Сетевое имя
Модель ПО
Версия ПО
Производитель ПО
Версия устройства
ОС

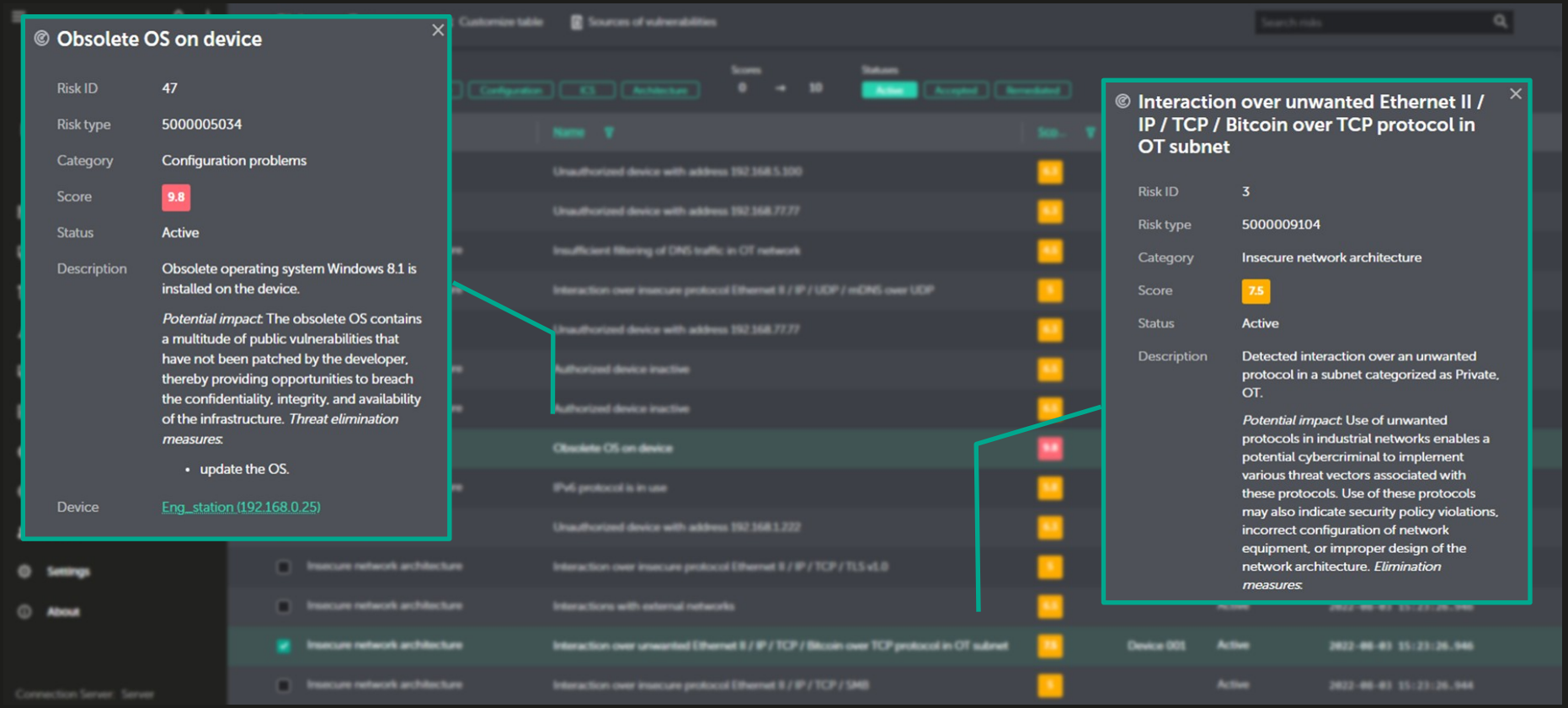
Vulnerability assessment



Vulnerability assessment

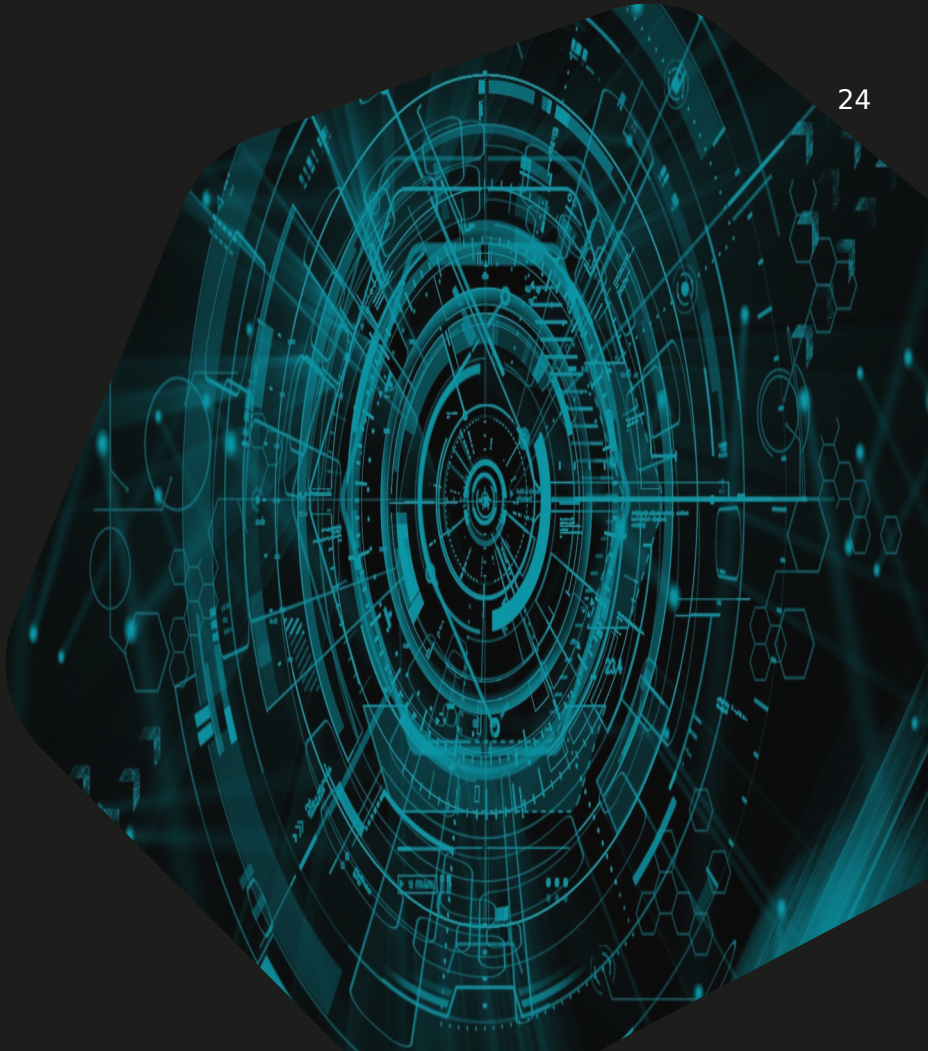


Идентификация устаревших ОС и нежелательные протоколы

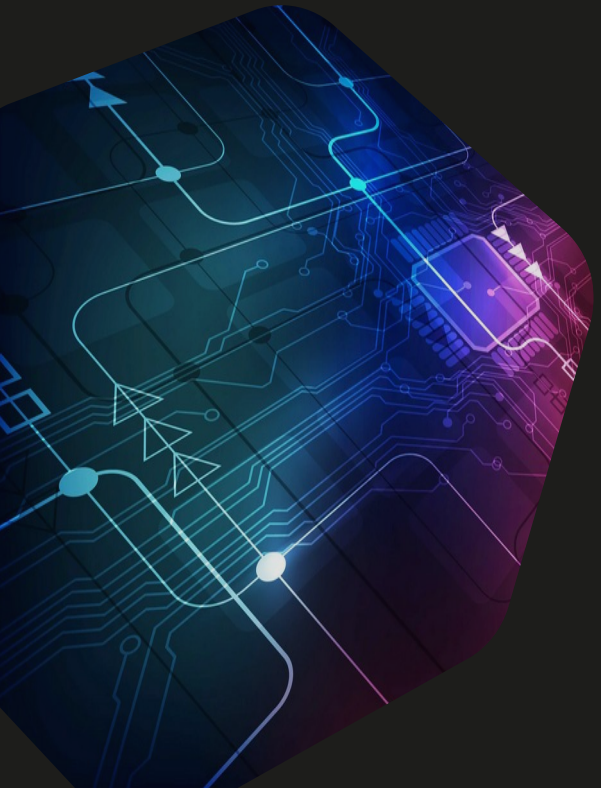


Методы улучшения детектирования

- Фингерпринт + 3 байта MAC адреса
- Агрегация атрибутов
- Уровень достоверности правила
- Взаимоисключение атрибутов



Куда двигаемся дальше ?



- Взаимодействие с конечными устройства средствами коннекторов KICS for Nodes
- Больше постпроцессоров
- Зависимости MAC адреса от серии и линейки оборудования
- Поведенческий метод
- Активное сканирование

Спасибо за внимание!

Roman.Ezhov@kaspersky.com

kaspersky