



Kaspersky Industrial
Cybersecurity
Conference

Пассивное обнаружение активов в технологических сетях

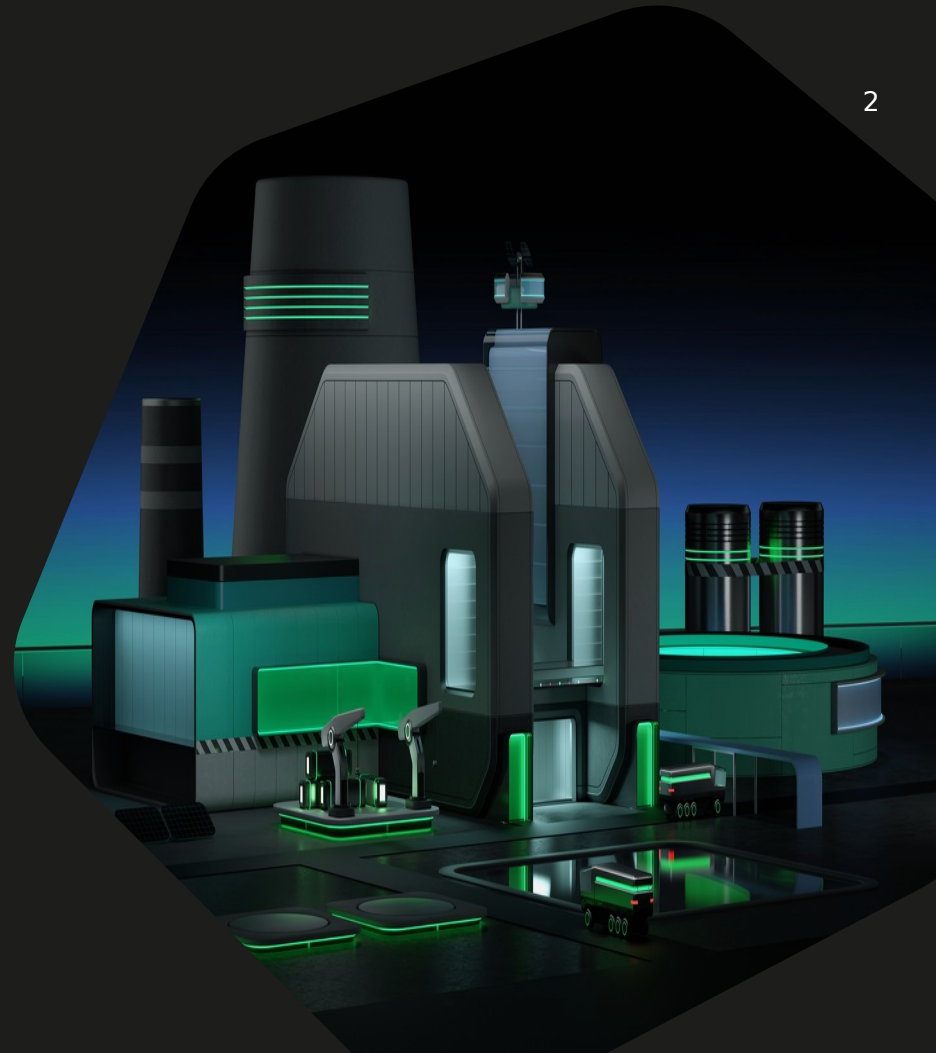


Ежов Роман

kaspersky

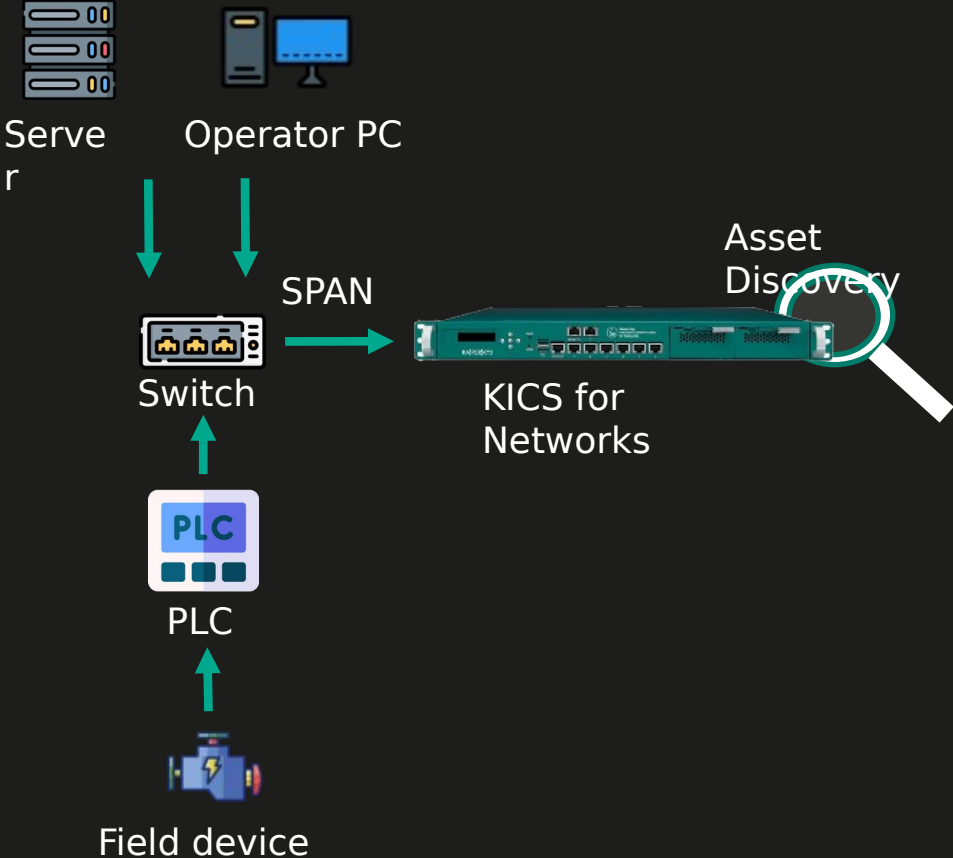
Почему это важно?

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





Kaspersky Industrial CyberSecurity **for Networks**



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

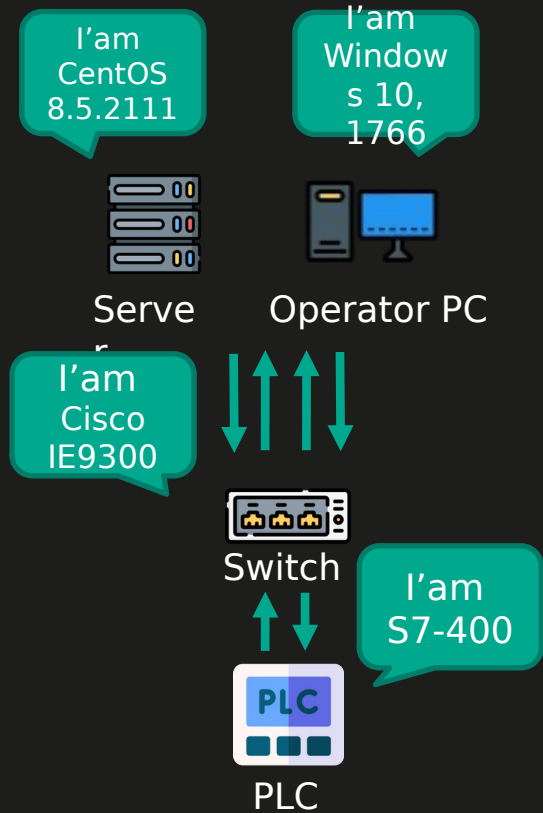


- Инвентаризация технологической сети:
 - Тип устройства
 - Производитель устройства
 - Операционная система
 - Модель устройства
 - Версии аппаратных элементов устройства
 - Версия прошивки
- Определение уязвимостей на устройствах
- Выявление нежелательной активности
- Расследование инцидентов



Устройства рассказывают о себе

7



Сигнатурные правила

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

Фингерпринт правила

8

- Устройства
- Операционные системы

Формат правила Asset Discovery

9

```
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\\V[\\d\\.]*|Linux\\V[\\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 c1x..
0060	01 00 00 00 01 02 01 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 30FCS010
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 00 c8 78 60 39x`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 00SB301.
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

Контролле
р

Потенциальное
обозначение
контроллера в
проекте

Системное ПО
Centum VP

Коммуникационн
ый модуль шины
ESB

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.....<>. #00. 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 32BMX 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	...>.	

Версия
прошивки

Процессорный
модуль

Kaspersky Industrial CyberSecurity **for Networks**

14

The screenshot displays the Rapid7 Industrial CyberSecurity for Networks interface. On the left is a sidebar with navigation options: Dashboard, Assets, Network map, Events, Process Control, Allow rules, Intrusion Detection, Vulnerabilities, Settings, and About. The main panel shows a 'Devices' table with columns: Name, Status, Address, Category, Security status, and Last seen. The table lists several devices, including 'ModiconM340' which is highlighted in green and marked as 'Authorized' with a 'OK' security status. On the right, a detailed view for 'ModiconM340' is shown, including its address (192.168.0.8) and settings (Router: No, Status: Authorized, Network name: M340, Hardware vendor: Schneider Electric, Hardware version: BMX P34 2020, Software vendor: Schneider Electric, Software version: 2.1). A red box highlights the 'Network name', 'Hardware vendor', 'Hardware version', 'Software vendor', and 'Software version' fields, with arrows pointing to the corresponding fields in the detailed view on the right.

Name	Status	Address	Category	Security status	Last seen
ModiconM340	Authorized	192.168.0.8	PLC	OK	2022-09-01
OS2-11391419	Unauthorized	192.168.0.8	HW / SCADA	Critical	2022-09-01
OS2-11391419	Unauthorized	192.168.0.8	Other	Critical	2022-09-01
Siemens AG SIMATIC S7 MULTIPORT SCALANCE X 200	Unauthorized	192.168.0.8	PLC	Critical	2022-09-01
Siemens AG SIMATIC S7 MULTIPORT SCALANCE X 200	Unauthorized	192.168.0.8	PLC	Critical	2022-09-01
Siemens AG SIMATIC S7 MULTIPORT SCALANCE X 200	Unauthorized	192.168.0.8	PLC	Critical	2022-09-01
Siemens AG SIMATIC S7 MULTIPORT SCALANCE X 200	Unauthorized	192.168.0.8	PLC	Critical	2022-09-01
Siemens AG SIMATIC S7 MULTIPORT SCALANCE X 200	Unauthorized	192.168.0.8	PLC	Critical	2022-09-01
Siemens AG SIMATIC S7 MULTIPORT SCALANCE X 200	Unauthorized	192.168.0.8	PLC	Critical	2022-09-01
Siemens AG SIMATIC S7-400	Unauthorized	192.168.0.8	PLC	Critical	2022-09-01
Siemens AG SIMATIC S7-400 (S)	Unauthorized	192.168.0.8	PLC	Critical	2022-09-01

Network name M340

Hardware vendor Schneider Electric

Hardware version BMX P34 2020

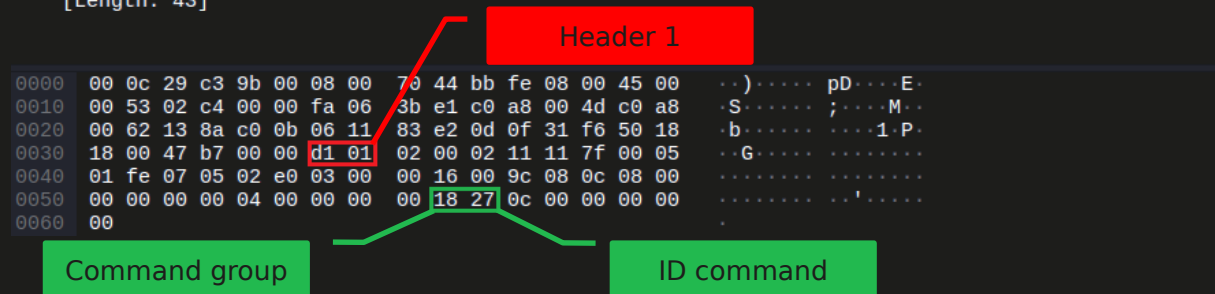
Software vendor Schneider Electric

Software version 2.1

```

> 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: d10102000211117f000501fe070502e003000016009c080c08000000000040000000018...
  [Length: 43]

```



```
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|\\
      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"
  }
```

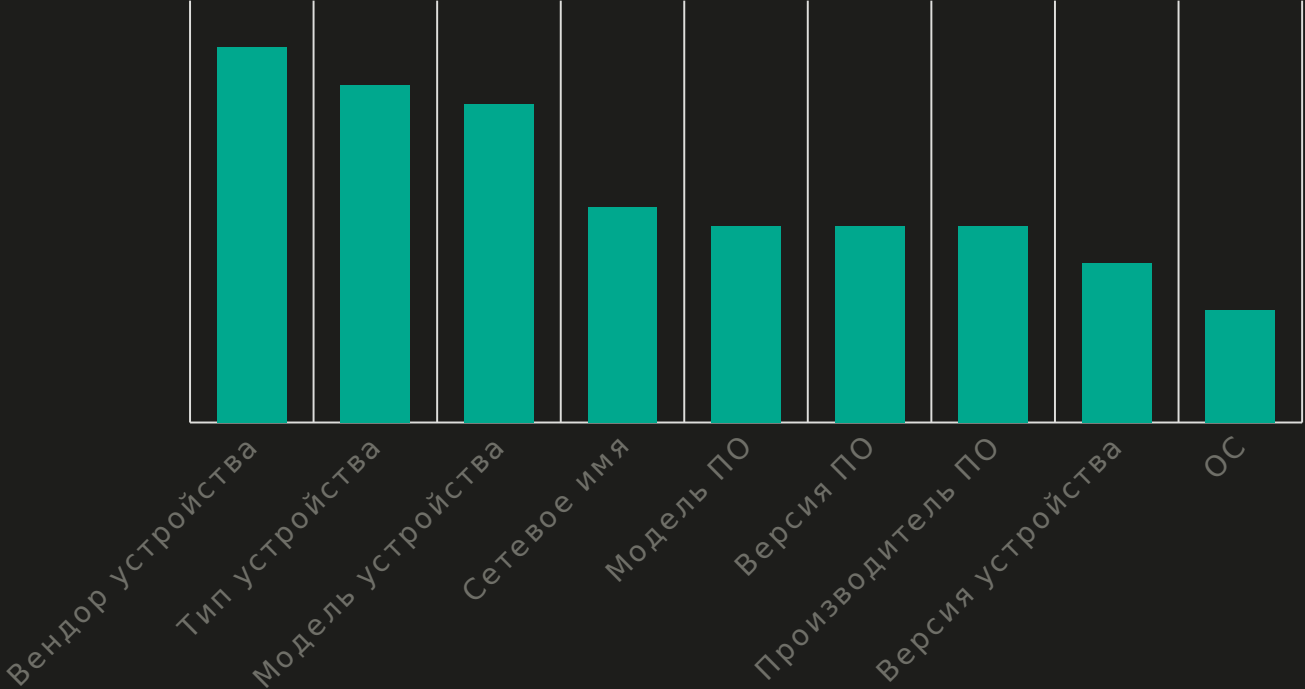

ip_flags
ttl
tcp_flags
tcp_win_size
e
tcp_options

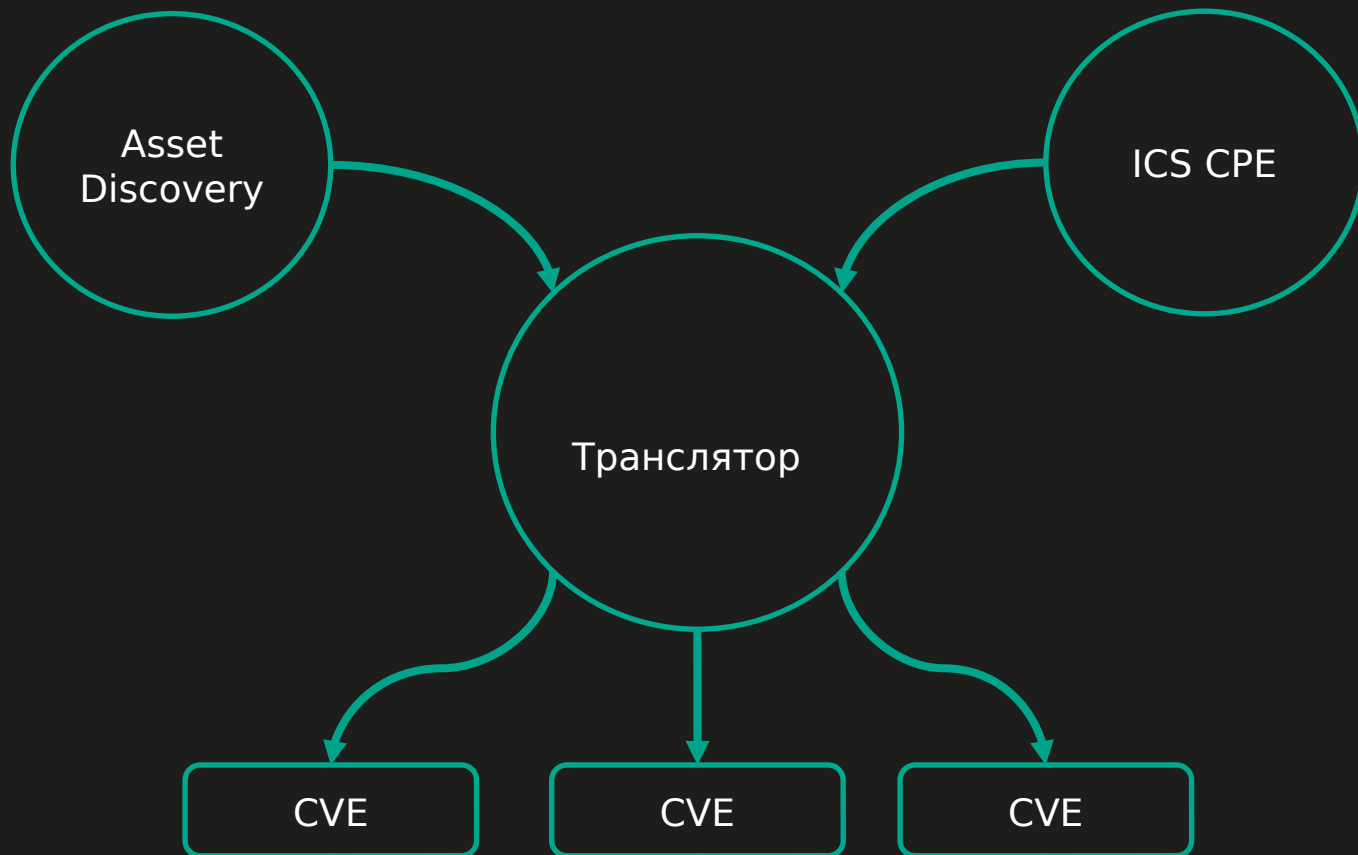
```
ip_flags = df
ttl = 64
tcp_flags = syn, ack
tcp_win_size = 8192
tcp_options = mss 1460, nop,
ws 0
```

19

	MBAP Header																Id			
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





The screenshot displays the Ekipernity Industrial CyberSecurity for Networks interface. On the left is a sidebar with navigation options: Dashboard, Assets, Network map, Events, Process Control, Allow rules, Intrusion Detection, Vulnerabilities, Settings, and About. The main area is titled 'Devices' and shows a table of network devices. A modal window is open, displaying details for a selected Siemens SIMATIC S7-400 PLC.

Name	Status	Address	Category	Security	Last seen
ModiconM340	Authorized	80:80:F4:8F:01:...	PLC	OK	2022-09-01
OS2-11191419	Unauthorized	F8:76:62:80:28:...	Workstation	Critical	2022-09-01
OS2-11191419	Unauthorized	F8:76:62:80:28:...	Workstation	Critical	2022-09-01
Siemens AG SIMATIC S7 MULTIPORT SCALANCE X 200 FA...	Unauthorized				2022-09-01
Siemens AG SIMATIC S7 MULTIPORT SCALANCE X 200 FA...	Unauthorized				2022-09-01
Siemens AG SIMATIC S7 MULTIPORT SCALANCE X 200 FA...	Unauthorized				2022-09-01
Siemens AG SIMATIC S7 MULTIPORT SCALANCE X 200 FA...	Unauthorized				2022-09-01
Siemens AG SIMATIC S7 MULTIPORT SCALANCE X 200 FA...	Unauthorized				2022-09-01
Siemens AG SIMATIC S7 MULTIPORT SCALANCE X 200 FA...	Unauthorized				2022-09-01
Siemens AG SIMATIC S7 MULTIPORT SCALANCE X 200 FA...	Unauthorized				2022-09-01
Siemens SIMATIC S7-400	Authorized				2022-09-01
SIMATIC S7-400	Unauthorized	80:1B:1B:06:16:...	PLC	Critical	2022-09-01
SIMATIC S7-400 (S)	Unauthorized	80:1B:1B:06:16:...	PLC	Critical	2022-09-01
TR-11191419	Unauthorized	80:1B:1B:06:16:...	Workstation	Critical	2022-09-01

Device Details: Siemens SIMATIC S7-400 PLC

- IP address: 192.168.0.20
- Settings:
 - Router: No
 - Status: Authorized
 - Network name: S7-400
 - Hardware vendor: Siemens
 - Hardware model: SIMATIC S7-400
 - Hardware version: 6es7414-3em05-0ab0
- Vulnerabilities:
 - CVE-2018-16557
 - CVE-2016-9158
 - CVE-2017-12741
 - CVE-2018-16556
 - CVE-2019-10936
 - CVE-2019-6568
- Actions:
 - Edit
 - Change status to Unauthorized
 - Show events
 - Show tags
 - Show vulnerabilities
 - Move to group
 - Delete device

Идентификация устаревших ОС и нежелательные протоколы

23

Obsolete OS on device

Risk ID: 47
Risk type: 5000005034
Category: Configuration problems
Score: 9.8
Status: Active
Description: Obsolete operating system Windows 8.1 is installed on the device.
Potential impact: The obsolete OS contains a multitude of public vulnerabilities that have not been patched by the developer, thereby providing opportunities to breach the confidentiality, integrity, and availability of the infrastructure. *Threat elimination measures:*

- update the OS.

Device: [Eng_station \(192.168.0.25\)](#)

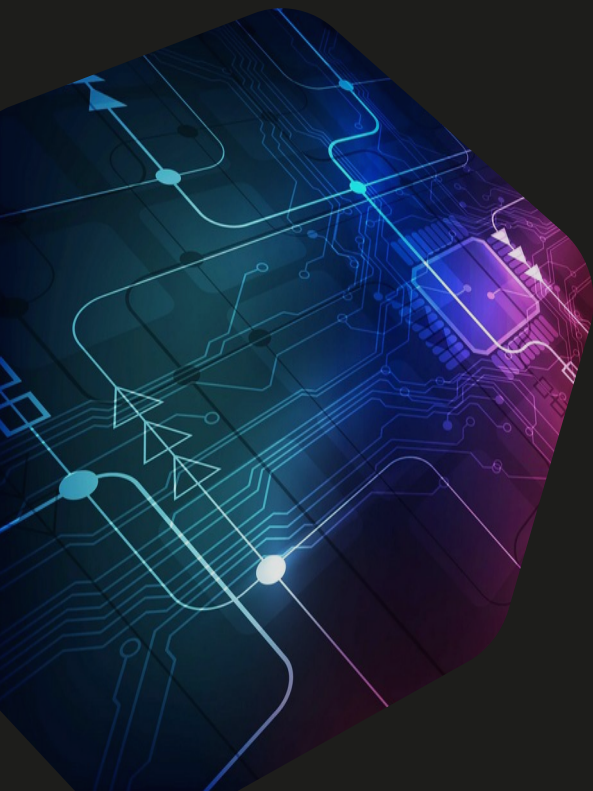
Interaction over unwanted Ethernet II / IP / TCP / Bitcoin over TCP protocol in OT subnet

Risk ID: 3
Risk type: 5000009104
Category: Insecure network architecture
Score: 7.5
Status: Active
Description: Detected interaction over an unwanted protocol in a subnet categorized as Private, OT.
Potential impact: Use of unwanted protocols in industrial networks enables a potential cybercriminal to implement various threat vectors associated with these protocols. Use of these protocols may also indicate security policy violations, incorrect configuration of network equipment, or improper design of the network architecture. *Elimination measures:*

Name	Score
Unauthorized device with address 192.168.5.100	6.5
Unauthorized device with address 192.168.77.77	6.5
Insufficient filtering of DNS traffic in OT network	6.5
Interaction over insecure protocol Ethernet II / IP / UDP / mDNS over UDP	6
Unauthorized device with address 192.168.77.77	6.5
Authorized device inactive	6.5
Authorized device inactive	6.5
Obsolete OS on device	9.8
IPv6 protocol is in use	6.5
Unauthorized device with address 192.168.1.222	6.5
Interaction over insecure protocol Ethernet II / IP / TCP / TLS v1.0	6
Interactions with external networks	6.5
Interaction over unwanted Ethernet II / IP / TCP / Bitcoin over TCP protocol in OT subnet	7.5
Interaction over insecure protocol Ethernet II / IP / TCP / SMB	6

Методы улучшения детектирования

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



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

**Kaspersky Industrial Cybersecurity Conference
2022**

Спасибо за внимание!

**Roman.Ezhov@kaspersky.
com**

kaspersky