КОД ИБ

ИТОГИ

ВАЖНЫЕ МЕТРИКИ ДЛЯ CISO

КУЛИЧКИН АРТЁМ
И. о. директора по ИБ ДЗО
АО «СОГАЗ»

КОД ИБ

ИТОГИ

Почему бизнесу важно знать свою инфру?

Лучше ничего не знать, чем знать многое наполовину!

Фридрих Ницше

КОД ИБ

ИТОГИ

Что важно ИТ/ИБ знать о сети?

- Понимать, какие порты на каждом IP
- Понимать, что именно это за устройство
- Отделять проприетарное оборудование
- Уметь фильтровать и исключать оборудование
- Сканировать безопасно для инфраструктуры
- Автоматизировать процесс
- Понять периметр сети и его уязвимости
- Делать все это в течение рабочего дня

КОД ИБ

ИТОГИ

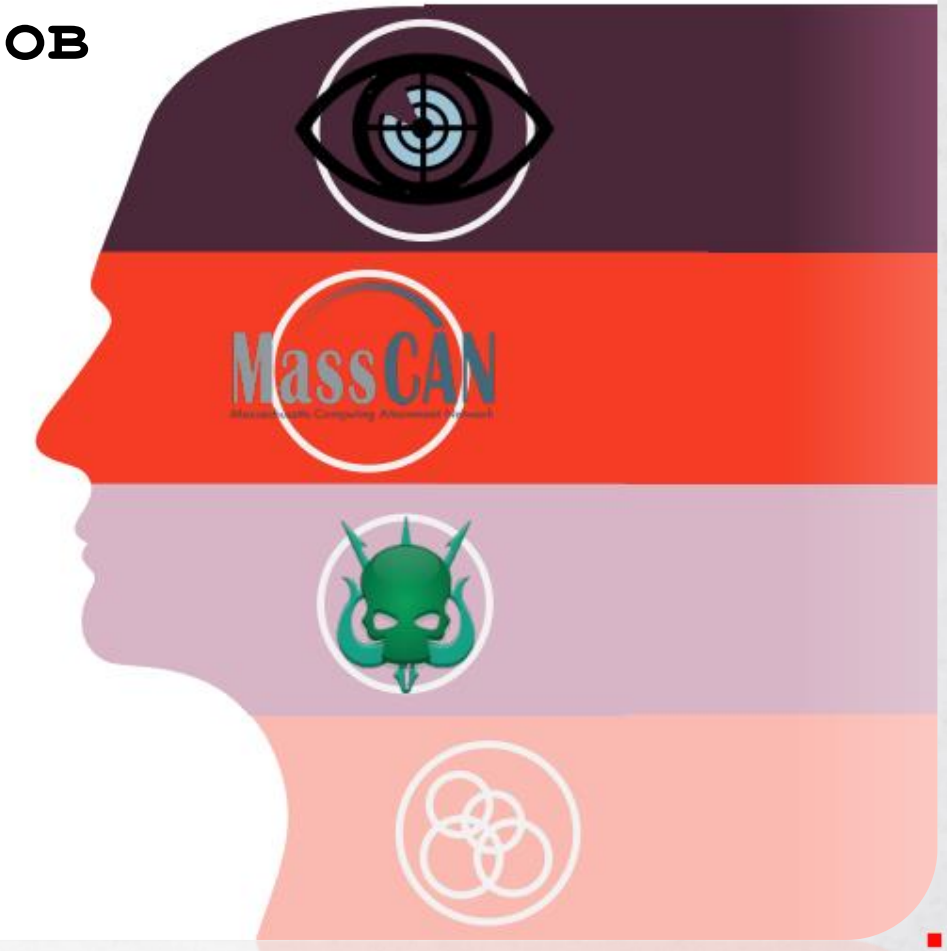
Нужно установить агент

- У нас 10 компьютеров
- Восемь из них в AD, два отдельно
- Что-то про VLAN’ы
- Как нам их найти и убедиться, что агент поставился на все?
- А если их не 10, а 100000?

IP	HOST	Комментарий	АВЗ	DLP	SOC	Скан
10.0.0.1	C831sd	Телефония				
10.0.0.2	ПК-001	АРМ	+	+	+	
10.0.0.3	P-001	Принтер				+

Мысли по выявлению хостов

- **Nmap** Сканируем 10.0.0.0\8.
  - •Сразу вопрос, а сколько это займёт даже с T5 (максимальная скорость)?
  - •Как понять, что я прохожу во все подсети?
  - •Как это выводить в читаемый вид, т.к хостов по предположению 25к+?
- **Masscan** Сканируем 10.0.0.0\8.
  - •Вопрос, как определить службу на порту, ведь masscan показывает только существование хоста.
  - •Тот же вопрос по подсетям, есть ли доступ на пограничных FW и локальных.
  - •Как работать с получившимся списком?
- **Crackmapexec**
  - CrackMapExec удобрый инструмент, который подключается к портам например SMB, SSH, WinRM и даёт точную информацию, что это за хост.
- **Остальные утилиты.**
  - Остальные различные утилиты коих много naabu, rustscan, umit, wireshark и др.



Скрестим NMAP и masscan?

1. Сканируем masscan в список.
2. Удаляем дубликаты IP.
3. Загружаем список в NMAP.
4. Сканируем по списку.

1 2 3 4 ?

КОД ИБ

ИТОГИ

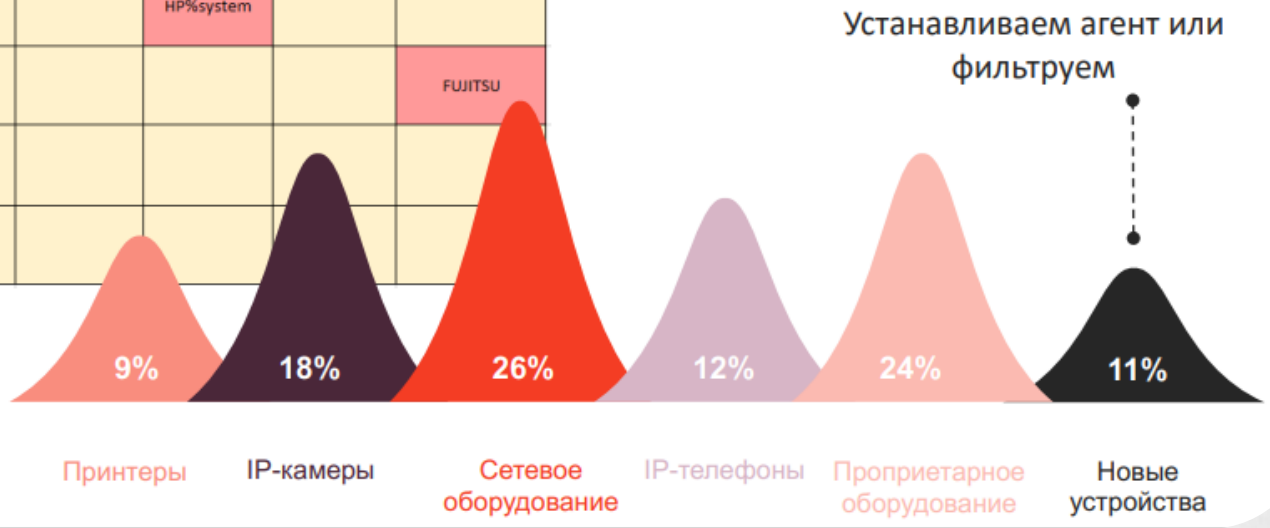
Анализ

IP	Hostname	OS	HostScript	135	135/Script	139	139/Script	443	443/Script	445	445/Script	5060	5060/Scrip	5061	5061/S
10.3	w00-0002-	Microsoft	[{"id": "sn	135/tcpwr	135/	139/tcpwr	139/			445/tcpwr	445/				
10.4	-	Digi AnywhereUSB network-attached USB hub/HP Laserjet CP1						443/tcpwrappec	443/{"http-title": "HP LaserJet 40		MFP M425dn 1		, "ssl-cert": "Subject: commonN		
10.2	w00-3700-	Microsoft	[{"id": "sn	135/msrp	135/	139/netbi	139/			445/micro	445/				
10.7	-	Cisco 2811 router (IOS 12.X)										5060/sip-proxy/Cisco SIP Gateway//cpe:/o:cisco:ios		5060/{"sip-methods": "INVI	
10.7	w00-1500-	Microsoft	[{"id": "sn	135/msrp	135/	139/netbi	139/			445/micro	445/				
10.1	-	Linux 2.6.32/Linux 2.6.32 or 3.10/Linux 4.4						443/http/nginx/	443/{"ssl-cert": "Subject: commonName=		/organizationName=JSC			eName=Mos	
10.2	p00-4200-	Linux 3.11 - 4.1/Linux 4.4/Linux 3.10 - 3.12						443/http/nginx/	443/{"ssl-date": "TLS randomness does not represent time", "http-title": "400 The plain HTTP request was sent t						
10.7	-	Digi AnywhereUSB/2 network-attached USB hub/Digi Anywhe						443/tcpwrappec	443/{"http-server-header": "gSOAP/2.7", "ssl-cert": "Subject: commonName=					anizationName=He	
10.0	p00-0000-	Linux 3.11 - 4.1						443/http/nginx/	443/{"http-title": "400 The plain HTTP request was sent to HTTPS port", "ssl-cert": "Subject: commonName=P00-						
10.1	-	Microsoft	[{"id": "sn	135/msrp	135/	139/netbi	139/	443/https///	443/	445/micro	445/				
10.7	w00-0000-	Microsoft	[{"id": "sn	135/msrp	135/	139/netbi	139/			445/micro	445/				
10.7	p00-0000-	HP iLO 4 remote management interface						443/tcpwrappec	443/{"ssl-cert": "Subject: commonName=P00-0		.ru/organizationName=HP\nNot valid before: 201				
10.0	w00-0000-	Microsoft	[{"id": "sn	135/msrp	135/	139/netbi	139/			445/micro	445/				
10.4	-	Microsoft	[{"id": "sn	135/msrp	135/	139/netbi	139/			445/micro	445/				
10.2	-	Microsoft	[{"id": "sn	135/msrp	135/	139/netbi	139/			445/micro	445/				
10.1	-	Cisco 2950, 2960, 3550, 3560, or 3750 switch (IOS 12.1 - 12.2)/Cisco 6509 switch (IOS 12.2)/Cisco 3550 switch (IOS 12.2)													
10.4	-	Linux 3.11 - 4.1/Linux 4.4/OpenWrt Designated Driver (Linux 4.						443/http/nginx/	443/{"http-title": "Site doesn't have a title (text/html).", "ssl-cert": "Subject: commonName=H						niz
10.5	-	Linksys BE	[{"id": "clock-skew", "output": "-6s"}]					443/https///	443/{"ssl-date": "2023-06-14T10:49:34+00:00; -6s from scanner time.", "ssl-cert": "Subject: commonName=CP-79						
10.3	w00-0002-	Microsoft	[{"id": "sn	135/msrp	135/	139/netbi	139/			445/micro	445/				
10.1	s00-0000-\	Microsoft	[{"id": "nb	135/msrp	135/	139/netbi	139/			445/micro	445/				
10.1	w00-3400-	Microsoft	[{"id": "sn	135/msrp	135/	139/netbi	139/			445/micro	445/				
10.7	p00-4000-	Axceint U	[{"id": "clock-skew", "output":			139/netbi	139/	443/https///	443/{"ssl-	445/route	445/				
10.1	s00-0000-s	Microsoft	[{"id": "sn	135/msrp	135/	139/netbi	139/			445/micro	445/				
10.5	-	Teradici 10ZiG V1200 thin client/HP Laserjet CP1515n printer/D						443/tcpwrappec	443/{"ssl-cert": "Subject: commonNa		:/organizationName=Hewlett-Packard Co.\nNot valid before				
10.4	-	Microsoft	[{"id": "sn	135/msrp	135/	139/netbi	139/			445/micro	445/				
10.0	p00-0000-	Digi AnywhereUSB network-attached USB hub/HP Laserjet CP1						443/tcpwrappec	443/{"ssl-date": "TLS randomness does not represent time", "http-server-header": "\n Virata-EmWeb/R6_2_1\r						
10.2	-	Cisco IP Phone 7941/Avaya 4000- or 5000-series Ethernet Routing switch/Konica Minolta bizhub C253 printer													
10.0	w00-0000-	Microsoft	[{"id": "sn	135/msrp	135/	139/netbi	139/			445/micro	445/				
10.3	p00-4600-	Linux 3.11 - 4.1/Linux 4.4/Linux 3.10 - 3.12						443/http/nginx/	443/{"http-title": "Site doesn't have a title (text/html).", "ssl-cert": "Subject: commonName=P						org

КОД ИБ

ИТОГИ

№ HOST	Port 23	Port 80	Port 443	Port 554	Port 8080	Port 2301	Port 9100	Port 5989
host #1				Hikvision				
host #2	Port 23	Port 80	Huawei					FUJITSU
host #3						ViPNet		
host #4		Port 80	Huawei					
host #5	Port 23	Hikvision		Hikvision				FUJITSU
host #6				Hikvision				
host #7						HP%system		
host #8								FUJITSU
host #9	Cisco Systems	Cisco Systems	Cisco Systems					
host #10		HP Storage						

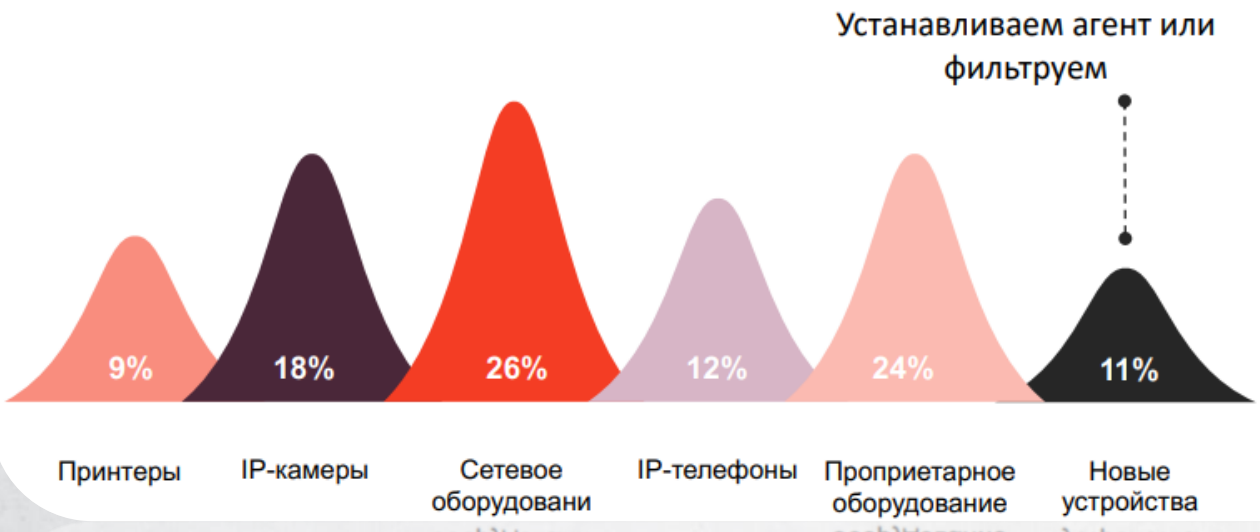


КОД ИБ

ИТОГИ

Нашли, куда поставить

- Отфильтровали, где агент есть
- Отфильтровали, куда агента поставить невозможно
- На оставшиеся в списке хосты его поставим




```
SELECT * FROM host_scan.table_2023_06_22_0
LEFT JOIN FLEET23 ON host_scan.table_2023_06_22_0.IP = Flt
WHERE FLEET23.primary_ip IS NULL and
port_80_ScriptOutput like '%80%' and

--Принтеры
port_80_ScriptOutput not like '%HP%Laser%JET%' and
port_443_ScriptOutput not like '%HP%Virtual%' and
port_443_ScriptOutput not like '%Hewlett%' and
port_443_ScriptOutput not like '%Laser%Jet%' and
port_80 not like '%Canon%' and
port_80 not like '%Xerox%' and
port_80 not like '%Lexmark%' and
port_80 not like '%MFP printer%' and
port_80 not like '%FUJITSU%' and
port_80 not like '%Printer%' and
port_80_ScriptOutput not like '%Canon%' and
port_80_ScriptOutput not like '%Xerox%' and
port_80_ScriptOutput not like '%Lexmark%' and
port_80_ScriptOutput not like '%MFP printer%' and
port_80_ScriptOutput not like '%Konica%' and
port_80_ScriptOutput not like '%Kyocera%' and

--IP-Камеры
port_80_ScriptOutput not like '%Hikvision%' and
port_21 not like '%Camera%' and
port_443_ScriptOutput not like '%Yealink%' and

--Сетевые устройства
port_80 not like '%Huawei switch%' and
port_443_ScriptOutput not like '%Huawei%' and
port_443 not like '%Huawei switch%' and
port_443 not like '%HP Integrated%' and
port_80 not like '%D-Link%' and
port_80 not like '%Switch%' and
port_22 not like '%Huawei%' and
port_17988 not like '%ilo%' and
port_80 not like '%Dell%' and
port_80 not like '%DD-WRT%' and

--IP Телефония
port_80 not like '%Phone%' and
port_80 not like '%VoIP%' and
port_80_ScriptOutput not like '%VoIP%' and

--Остальное
port_80_ScriptOutput not like '%APC | Log On%' and
port_443 not like '%VMware%' and
port_25 not like '%Exchange%' and
port_443_ScriptOutput not like '%Lenovo%' and
port_443_ScriptOutput not like '%Citrix%' and
port_443 not like '%Continent TLS%' and
port_256 not like '%Check%Point%' and
port_443_ScriptOutput not like '%HP BladeSystem%' and
```

Итоги:

- Знаем каждый IP в сети и его порты
- Есть понимание, что за хосты в сети
- Сразу отделяем проприетарное оборудование
- Легко фильтруем и исключаем нужное оборудование
- Производим сканирование безопасно
- Процесс полностью автоматизирован
- Интегрируемся с любыми источниками
- Сканируем за 9 часов всю сеть

IP	HOST	Комментарий	CMDB	FLEET	АВЗ	DLP	SOC	Скан
10.0.0.1	C831sd	Телефония						
10.0.0.2	ПК-001	АРМ	-	-	+	+	+	
10.0.0.3	P-001	Принтер						+

КОД ИБ

ИТОГИ

СПАСИБО ЗА ВНИМАНИЕ!

Куличкин Артём
+79171110055
@Kulichkin