РАБОТАЙ РУКАМИ,

НЕ ВСЁ РЕШАЕТСЯ ДЕНЬГАМИ.

согаз

РАБОТАЙ РУКАМИ,
НЕ ВСЁ РЕШАЕТСЯ ДЕНЬГАМИ.

Куличкин Артём Александрович

CISA, CEH, CND.

И.о. Директора по информационной безопасности
дочерних компаний, АО «СОГАЗ»

согаз

Введение

Информационная безопасность – это не роскошь, а необходимость. Данный доклад предложит некоторые практические шаги по обеспечению безопасности вашей компании.

Используй лучшие практики с простым контролем.

[Модель Кеневин]

согаз

AD

Аудит + доработка AD:

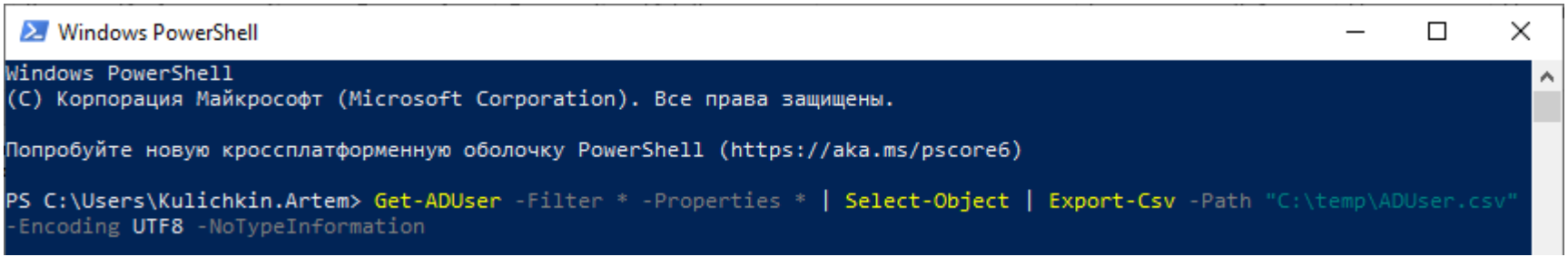
- Учётные записи
- Брут паролей
- Lithnet Password Protection
- Хосты
- Неправильное наследование
- Пилоты DCAP
- AD Audit Plus

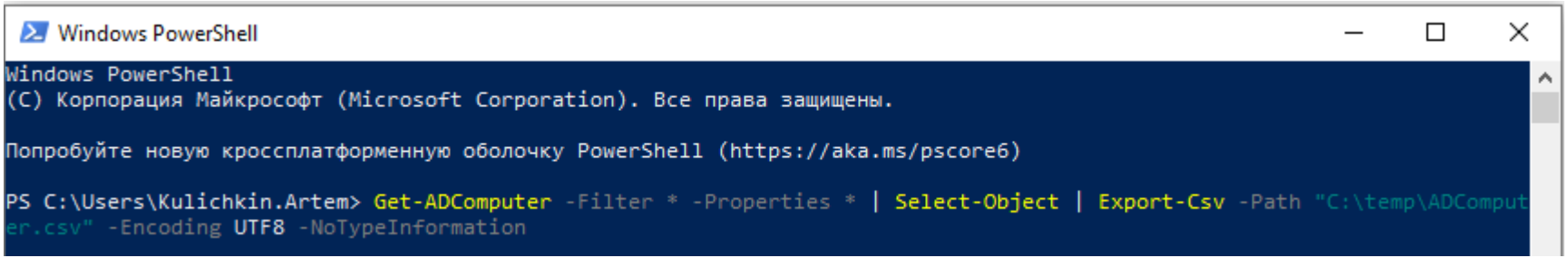
согаз

AD

Аудит + доработка AD:

- **Учётные записи** (Password ,Password never expires, last logon)





[Аудит пользователей AD с помощью Powershell / Хабр]

AD

Admin Accounts With SPN

0.22%

3 Admin Accounts With SPN

Accounts That Do Not Require Kerberos Pre-Authentication

0.43%

6 Accounts That Do Not Require Kerberos Pre-Authentication

Accounts With Passwords That Never Expire

1,158

Users

84% Accounts With Passwords That Never Expire

Accounts With No Password Policy

91%

1,255 Accounts With No Password Policy

AD

Аудит + доработка AD:

- Учётные записи
- **Брут паролей**

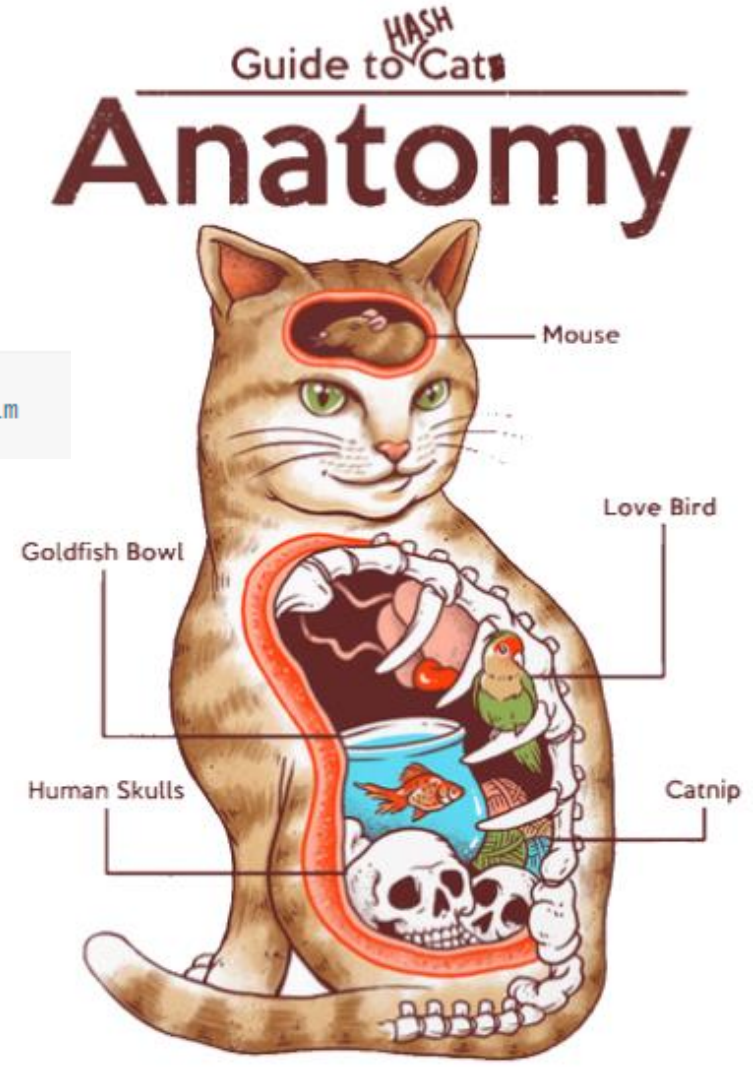
```
secretsdump.exe deiteriy.local/Administrator@192.168.88.32 -just-dc-ntlm
```

```
hashcat.exe -m 1000 E:\hashs.txt --show
```

```
E:\hashcat>hashcat.exe -m 1000 E:\hashs.txt --show
31d6cfe0d16ae931b73c59d7e0c089c0:
70b209a9e0b3739ed78b1fff628723a6:liverpool_fc5
5623bc6dcf13012f77f1bc6e867e4f9f:fr!3ndss
```

Поиск хэшей в pot-файле

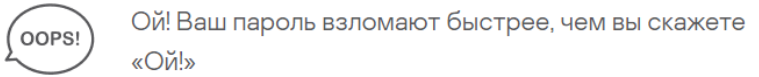
[Брутфорс хэшей в Active Directory / Хабр]

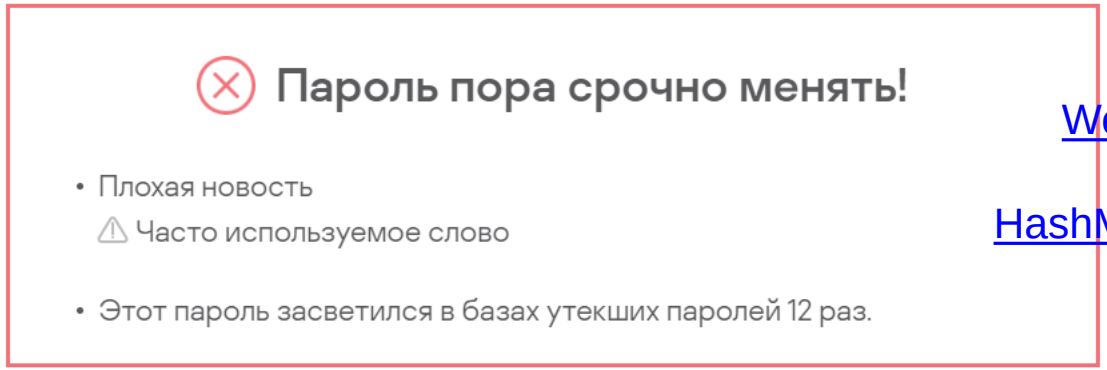


AD

Аудит + доработка AD:

- Учётные записи
- Брут паролей
- **Lithnet Password Protection**





[Weakpass: biggest wordlists collection]

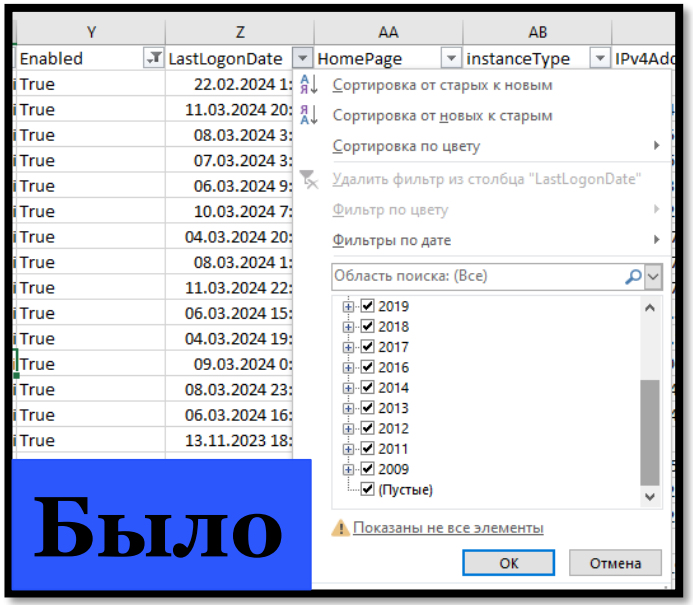
[HashMob | Resources | HashMob Wordlists]

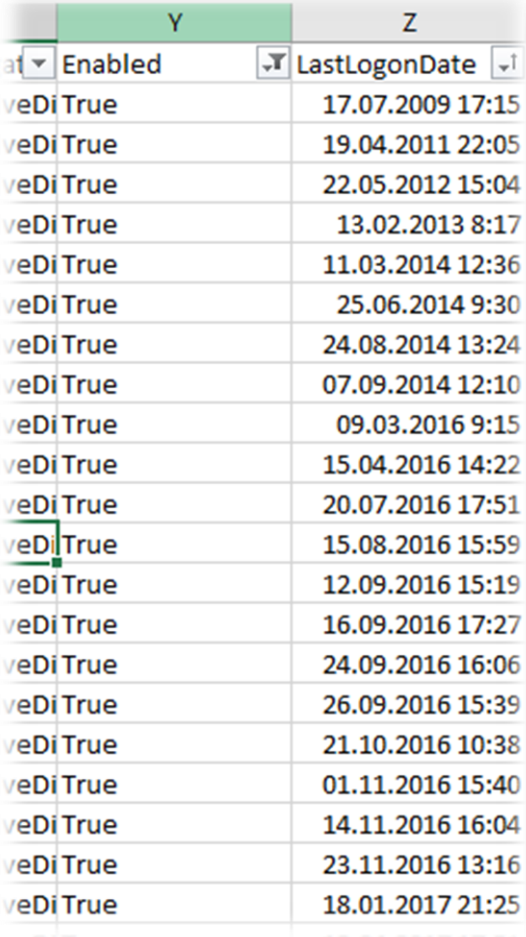
[Защита паролем AD — Lithnet]

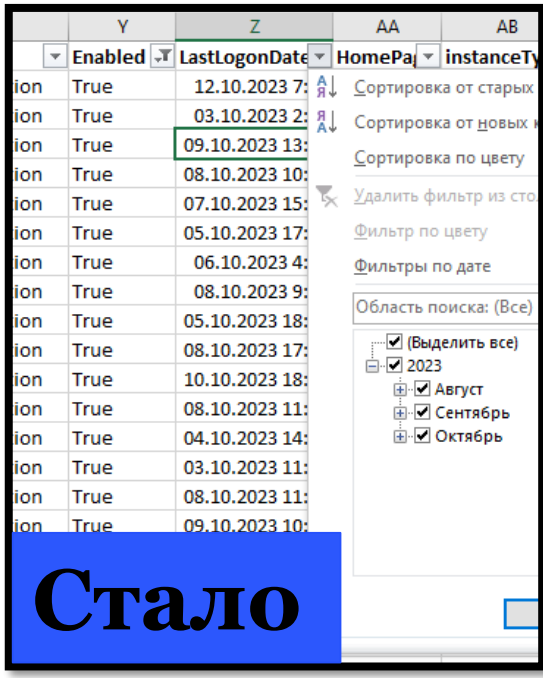
AD

Аудит + доработка AD:

- Учётные записи
- Брут паролей
- Lithnet Password Protection
- **Хосты**







AD

Аудит + доработка AD:

- Учётные записи
- Брут паролей
- Lithnet Password Protection
- Хосты
- **Неправильное наследование**

Компьютер	Путь	Применяется к	Пользователь/группа	Состояние наследования	Права объекта	Права родителя
ts.sus.local	\\ts.sus.loc	Для этой папки, ее подп	пользователи@builtin	Наследуется	F M X W R L S	F M X W R L S
ts.sus.local	\\ts.sus.loc	Для этой папки, ее подп	пользователи@builtin	Права преобразованы	F M X W R L S	F M X W R L S
		Для этой папки, ее подп	все	Права преобразованы	F M X W R L S	F M X W R L S
ts.sus.local	\\ts.sus.loc	Для этой папки, ее подп	пользователи@builtin	Права удалены		F M X W R L S
		Для этой папки, ее подп	все	Права удалены		F M X W R L S
ts.sus.local	\\ts.sus.loc	Для этой папки, ее подп	пользователи@builtin	Неверные флаги наследования	F M X W R L S	F M X W R L S
		Для этой папки, ее подп	пользователи@builtin	Наследование без родителя	F M X W R L S	
ts.sus.local	\\ts.sus.loc	Для этой папки, ее подп	пользователи@builtin	Ложное наследование		F M X W R L S
		Для этой папки, ее подп	все	Добавлен пользователь	F M X W R L S	
		Для этой папки, ее подп	служба@nt authority	Наследуется	F M X W R L S	F M X W R L S

AD

Аудит + доработка AD:

- Учётные записи
- Брут паролей
- Lithnet Password Protection
- Хосты
- Неправильное наследование
- **Пилоты DCAP**

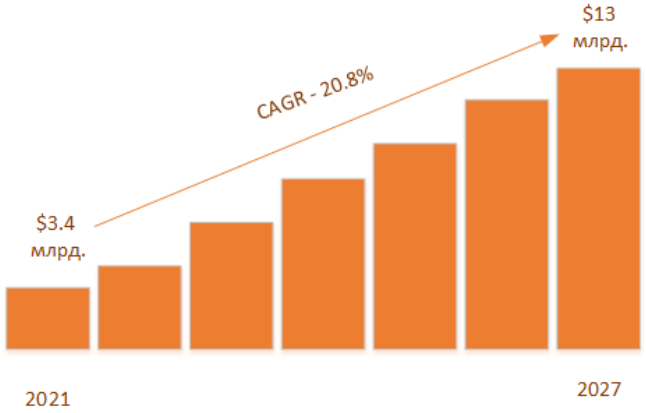


Рисунок 1. Насколько хорошо вы знакомы с решениями DCAP?

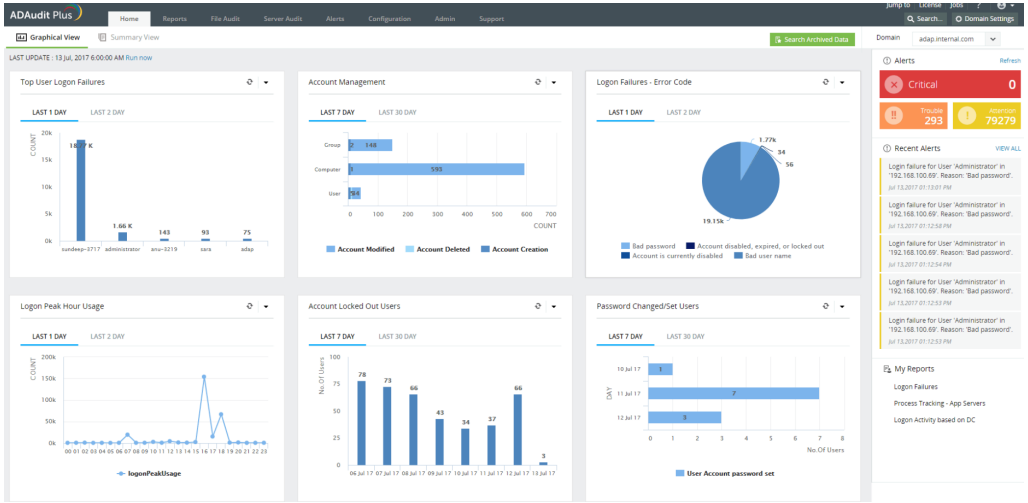
Российский рынок DCAP

- CyberPeak
- InfoWatch
- MAKVES
- Zecurion
- Орлан
- СёрчИнформ

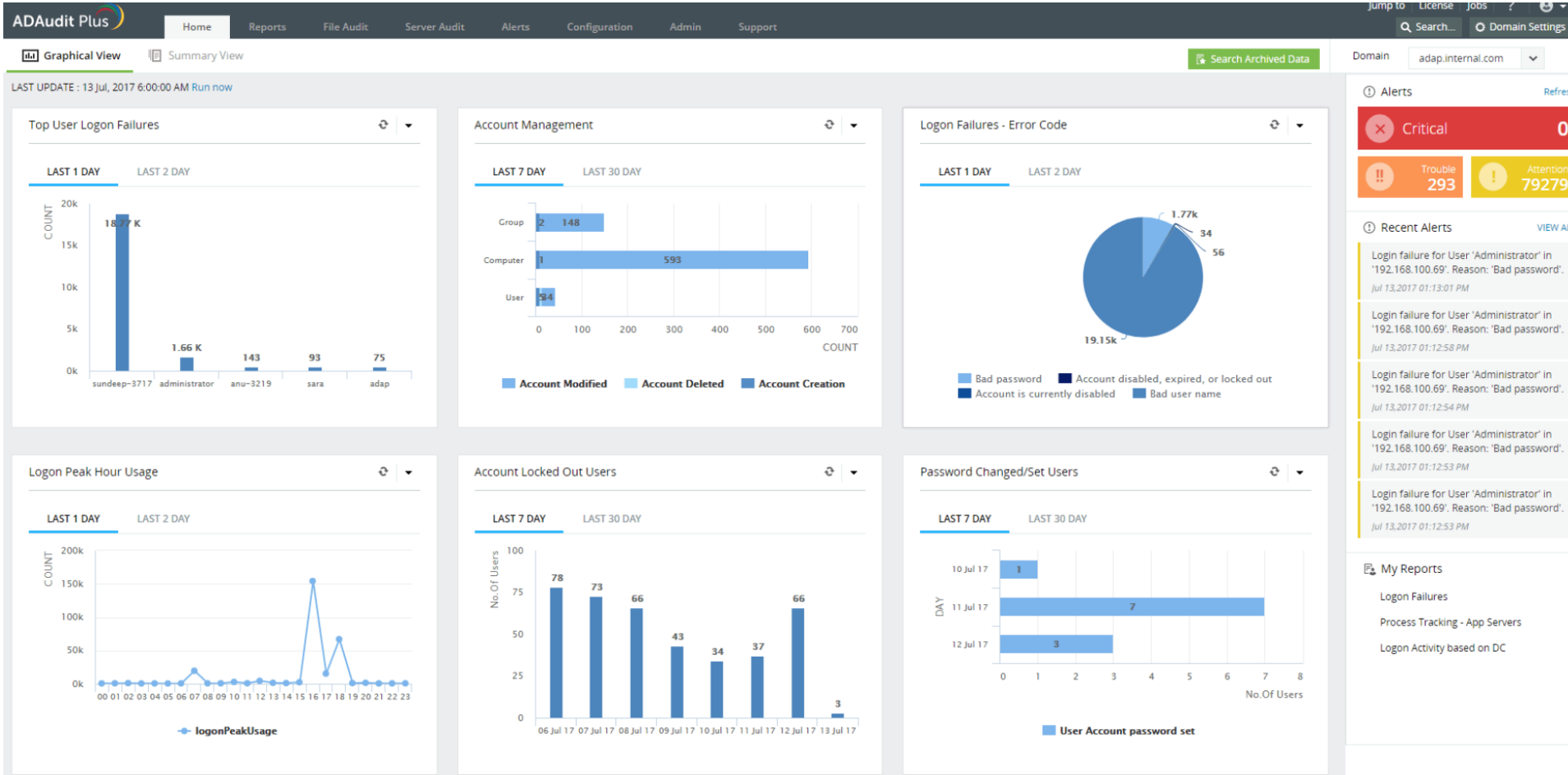
AD

Аудит + доработка AD:

- Учётные записи
- Брут паролей
- Lithnet Password Protection
- Хосты
- Неправильное наследование
- Пилоты DCAP
- **AD Audit Plus**



AD Audit plus



Анализ инфраструктуры

Аудит + доработка инфраструктуры:

- Аудит всех хостов в сети (Masscan + Nmap)
- Аудит всех портов в сети
- Аудит того, что торчит в интернет
- Аудит установленного ПО на хостах, каталог разрешённого
- IT CMDB актуальность
- Мониторинг инфраструктуры + аномальное поведение (Zabbix)

Анализ инфраструктуры

Аудит + доработка инфраструктуры:

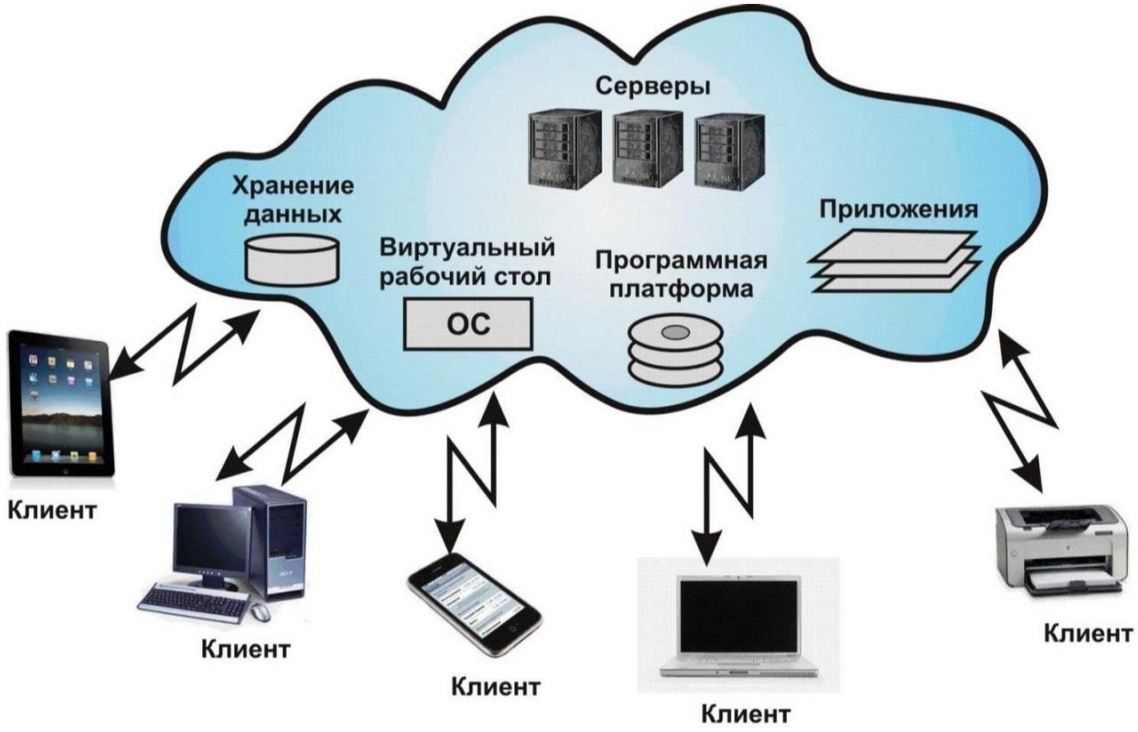
- **Аудит всех хостов в сети** (Masscan + Nmap)

MassCAN
Massachusetts Computing Attainment Network

+

NMAP

=



Анализ инфраструктуры

Аудит + доработка инфраструктуры:

- Аудит всех хостов в сети (Masscan + Nmap)
- **Аудит всех портов в сети**

		AB3	SOC	FLEET	EDR
ПК	200	200 (100%)	180 (90%)	160 (80%)	160 (80%)
Сервера	20				
?					
Всего	220				

10.22.11.18	FLEET		
10.22.11.18	PORT		21/ftp/vsftpd/2.0.5/cpe:/a:vsftpd:vsftpd:2.0.5 | 21/
10.22.11.18	PORT		23/telnet/Linux telnetd//cpe:/o:linux:linux_kernel | 23/
10.22.11.18	PORT		80/http/mini_httpd/1.19 19dec2003/cpe:/a:acme:mini_httpd:1.19_19dec2003 | 80/{"http-server-header": "mini_httpd/1.19 19dec2003", "http-title": "Site
10.22.11.18	PORT		427/svrloc/// | 427/
10.22.11.18	PORT		1720/h323q931/// | 1720/
10.22.11.18	PORT		5000/reverse-ssl/SSL/TLS ClientHello// | 5000/{"fingerprint-strings": "\n ZendJavaBridge: \n GetClassName"}
10.22.11.18	PORT		5988/http/Web-Based Enterprise Management CIM serverOpenPegasus WBEM httpd//cpe:/o:linux:linux_kernel | 5988/{"http-title": "Site doesn't have
10.22.11.18	MAIN_DATA		
10.22.11.18	KSC		
10.22.11.18	FLEET		
10.0.55.112	PORT		135/msrpc/// | 135/
10.0.55.112	PORT		139/netbios-ssn/Microsoft Windows netbios-ssn//cpe:/o:microsoft:windows | 139/
10.0.55.112	PORT		445/microsoft-ds/// | 445/
10.0.55.112	PORT		1720/h323q931/// | 1720/
10.0.55.112	PORT		1947/sentinelsrm/// | 1947/{"fingerprint-strings": "\n FourOhFourRequest: \n HTTP/1.0 403 Forbidden\n Server: HASP LM/24.00\n Date: Sat, 02 No
10.0.55.112	PORT		2701/cmrcservice/Microsoft Configuration Manager Remote Control service//cpe:/o:microsoft:windows | 2701/
10.0.55.112	PORT		3389/ms-wbt-server/Microsoft Terminal Services//cpe:/o:microsoft:windows | 3389/{"ssl-cert": "Subject: commonName=OLEG-VOLKOV.domen.local\nN
10.0.55.112	PORT		5040/unknown/// | 5040/
10.0.55.112	PORT		5357/http/Microsoft HTTPAPI httpd/2.0/cpe:/o:microsoft:windows | 5357/{"http-title": "Service Unavailable"}
10.0.55.112	PORT		7680/pando-pub/// | 7680/
10.0.55.112	PORT		8005/http/Microsoft HTTPAPI httpd/2.0/cpe:/o:microsoft:windows | 8005/{"http-title": "Bad Request"}
10.0.55.112	PORT		47001/http/Microsoft HTTPAPI httpd/2.0/cpe:/o:microsoft:windows | 47001/{"http-title": "Not Found"}
10.0.55.112	PORT		47546/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 47546/
10.0.55.112	PORT		49664/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 49664/
10.0.55.112	PORT		49665/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 49665/
10.0.55.112	PORT		49666/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 49666/
10.0.55.112	PORT		49667/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 49667/
10.0.55.112	PORT		49669/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 49669/
10.0.55.112	PORT		49672/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 49672/
10.0.55.112	PORT		49673/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 49673/
10.0.55.112	PORT		49674/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 49674/
10.0.55.112	PORT		49708/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 49708/

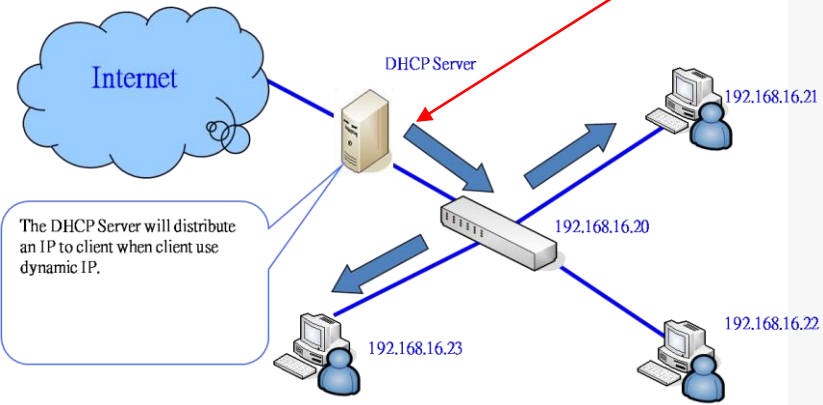
согаз

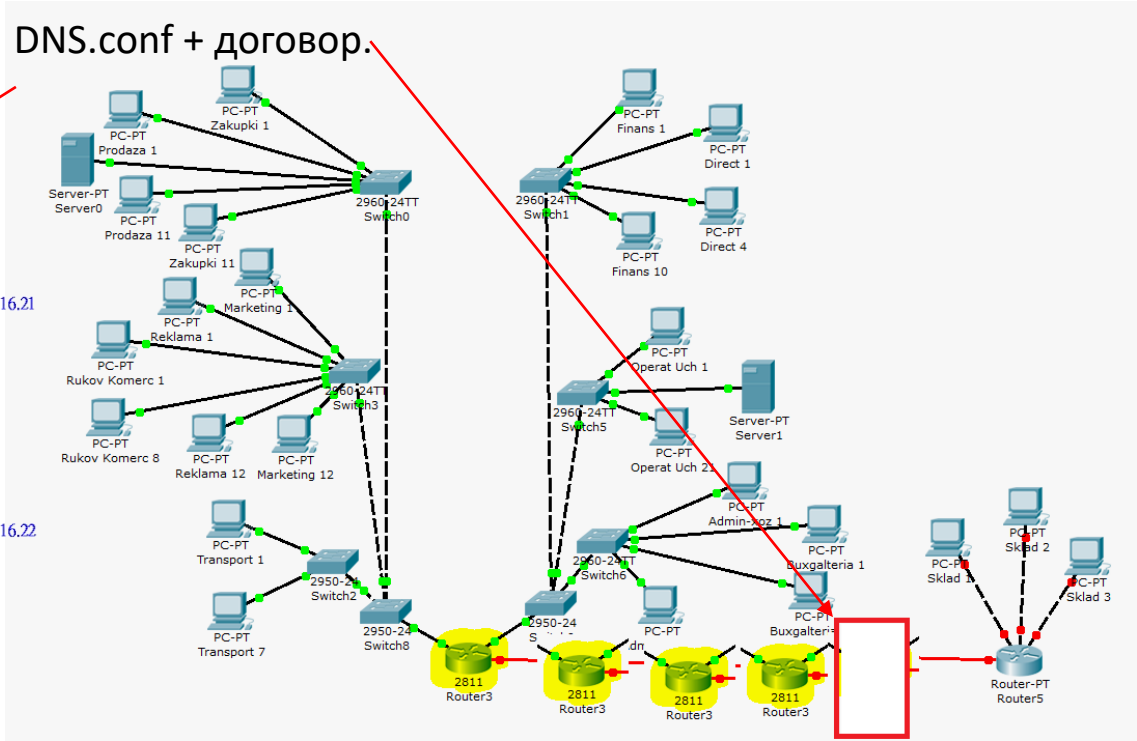
Анализ инфраструктуры

Аудит + доработка инфраструктуры:

- Аудит всех хостов в сети (Masscan + Nmap)
- Аудит всех портов в сети
- **Аудит того, что торчит в интернет**

DNS.conf + договор.



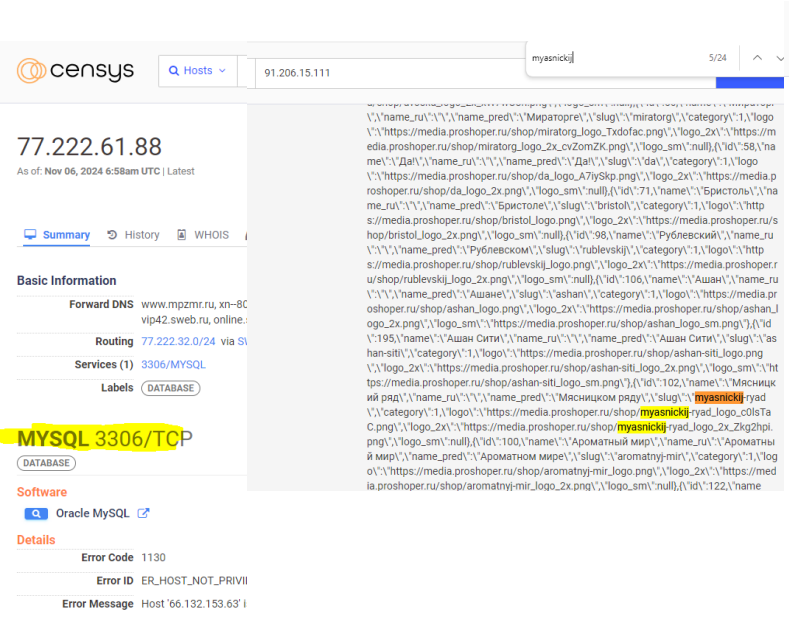


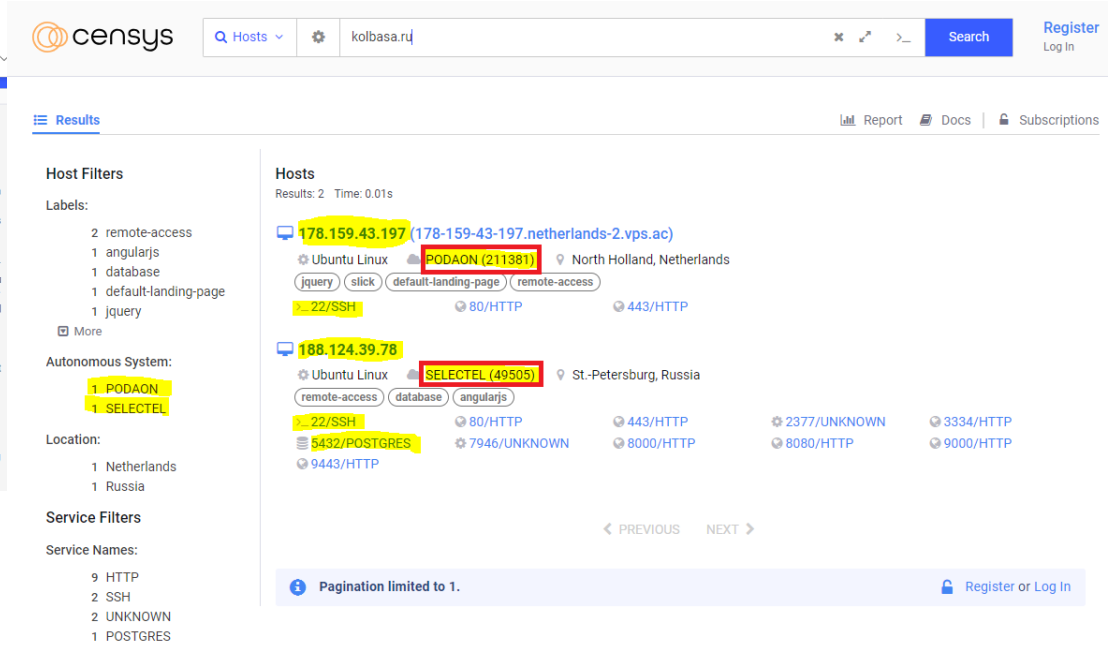
согаз

Анализ инфраструктуры

Аудит + доработка инфраструктуры:

- Аудит всех хостов в сети (Masscan + Nmap)
- Аудит всех портов в сети
- **Аудит того, что торчит в интернет** Посмотреть OSINT + Scanner

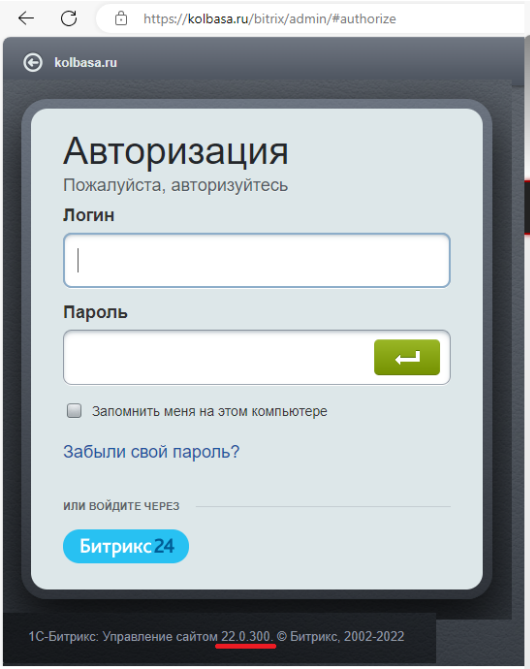


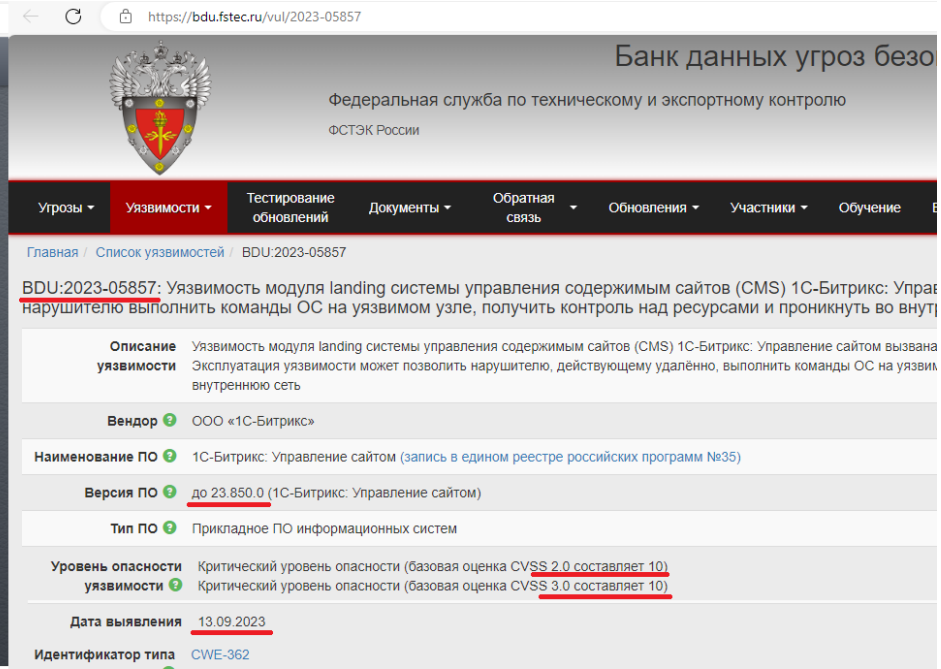


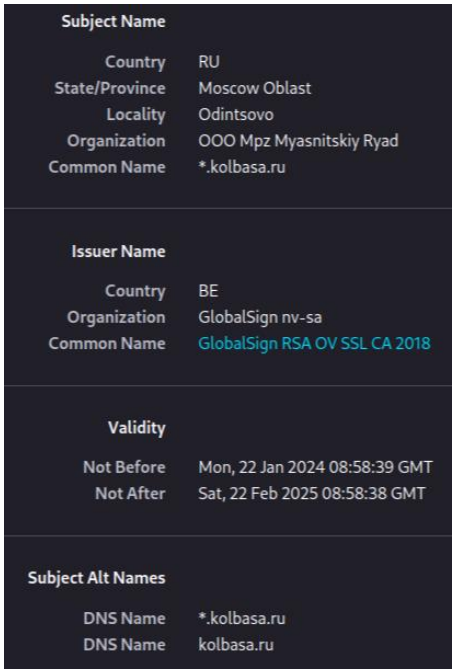
Анализ инфраструктуры

Аудит + доработка инфраструктуры:

- Аудит всех хостов в сети (Masscan + Nmap)
- Аудит всех портов в сети
- **Аудит того, что торчит в интернет** Посмотреть OSINT + Scanner



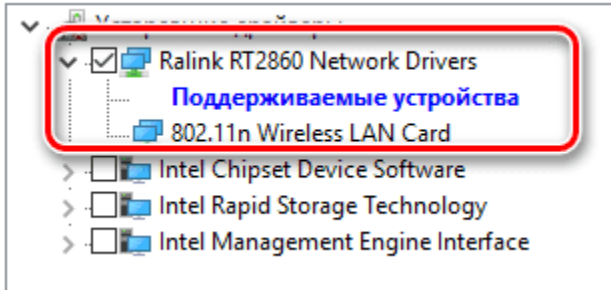




Анализ инфраструктуры

Аудит + доработка инфраструктуры:

- Аудит всех хостов в сети (Masscan + Nmap)
- Аудит всех портов в сети
- Аудит того, что торчит в интернет
- **Аудит установленного ПО на хостах, каталог разрешённого**



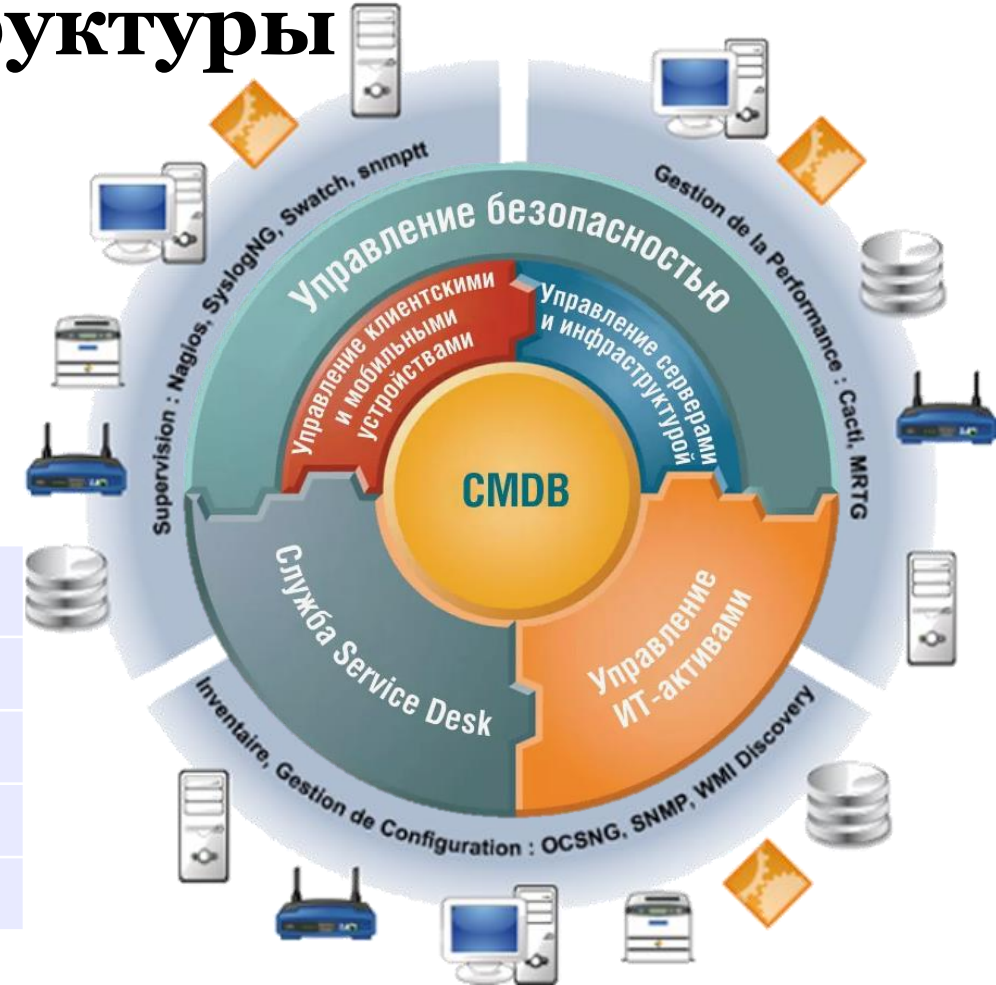
Альт Линукс СПТ
Альт
ОСь
Astra Linux
ROSA Linux
Calculate Linux
Ульяновск BSD
ICLinux
Альфа ОС
Эльбрус
Ред ОС
GosLinux
AlterOS
Мобильная система Вооружённых Сил
Заря
RAIDIX
Kraftway Terminal Linux
WTware
KasperskyOS
ОСРВ «МАКС»
Учетные системы
Складские системы
Логистическое ПО
Склад-15

Анализ инфраструктуры

Аудит + доработка инфраструктуры:

- Аудит всех хостов в сети (Masscan + Nmap)
- Аудит всех портов в сети
- Аудит того, что торчит в интернет
- Аудит установленного ПО на хостах
- **IT CMDB актуальность**

(Покрытие, реагирование на инциденты и др.)

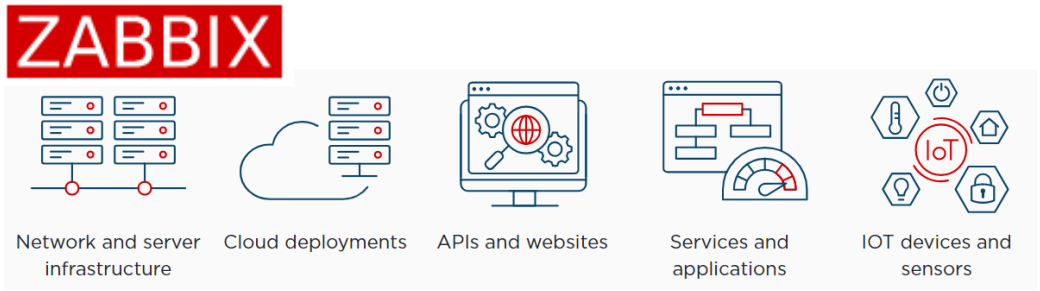


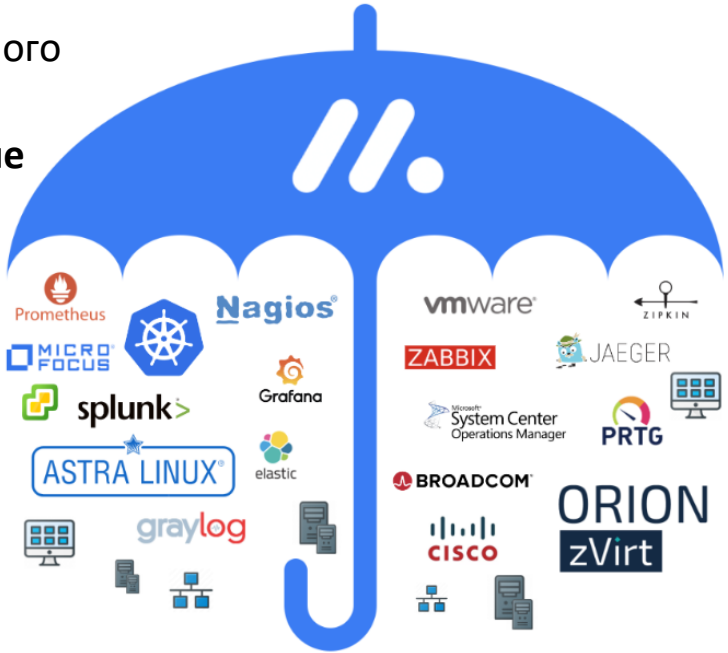
IP	NAME	ССЫЛКА	Владелец
90.90.72.39	G0000-EX31	https://ShowObject.jsp a?id=92004	Игорь Игоревич Игорев
90.90.48.39	G-0000-5202	https://ShowObject.jsp a?id=92699	Игорь Игоревич Игорев
90.86.4.2	G2800-SQ01	https://ShowObject.jsp a?id=99942	Иванов Иван Иванович
90.46.0.57	G6400-DP01	https://ShowObject.jsp a?id=92969	Иванов Иван Иванович

Анализ инфраструктуры

Аудит + доработка инфраструктуры:

- Аудит всех хостов в сети (Masscan + Nmap)
- Аудит всех портов в сети
- Аудит того, что торчит в интернет
- Аудит установленного ПО на хостах, каталог разрешённого
- IT CMDB актуальность
- **Мониторинг инфраструктуры + аномальное поведение (история про Zabbix)**





Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- Менеджеры паролей
- Минимальные права у юзера
- Запрет работать из под администратора администраторам
- Внедрение Local Administrator Password Solution (LAPS)
- VPN + 2ФА - удалённая работа
- 2ФА везде где возможно, 100% внешка.
- Пром данные только в проме

СОГАЗ

Начальные телодвижения

Установка, настройка, доработка:

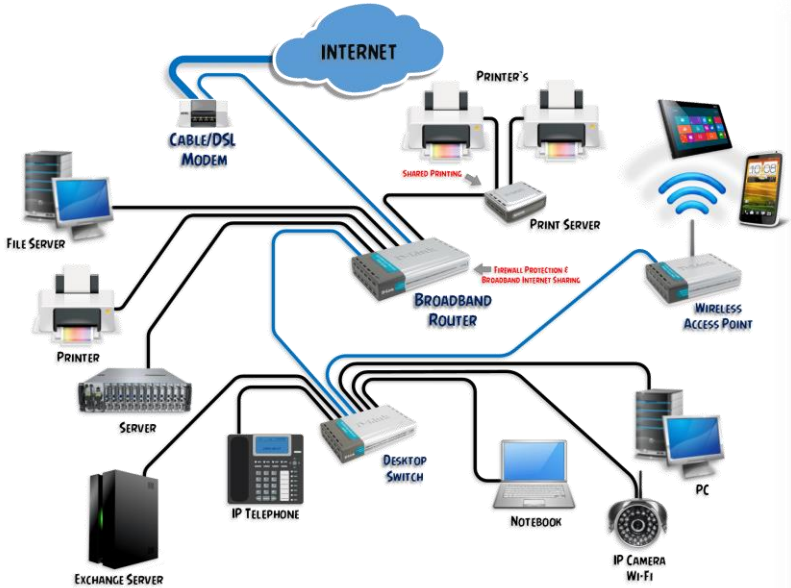
- **Ограничение физического доступа к инфраструктуре.**

СОГАЗ

Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- **Покрытие СЗИ всех возможных устройств**



согаз

Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- **Выстраивание правильных метрик покрытия**

АВЗ EDR SOC IDS DLP …

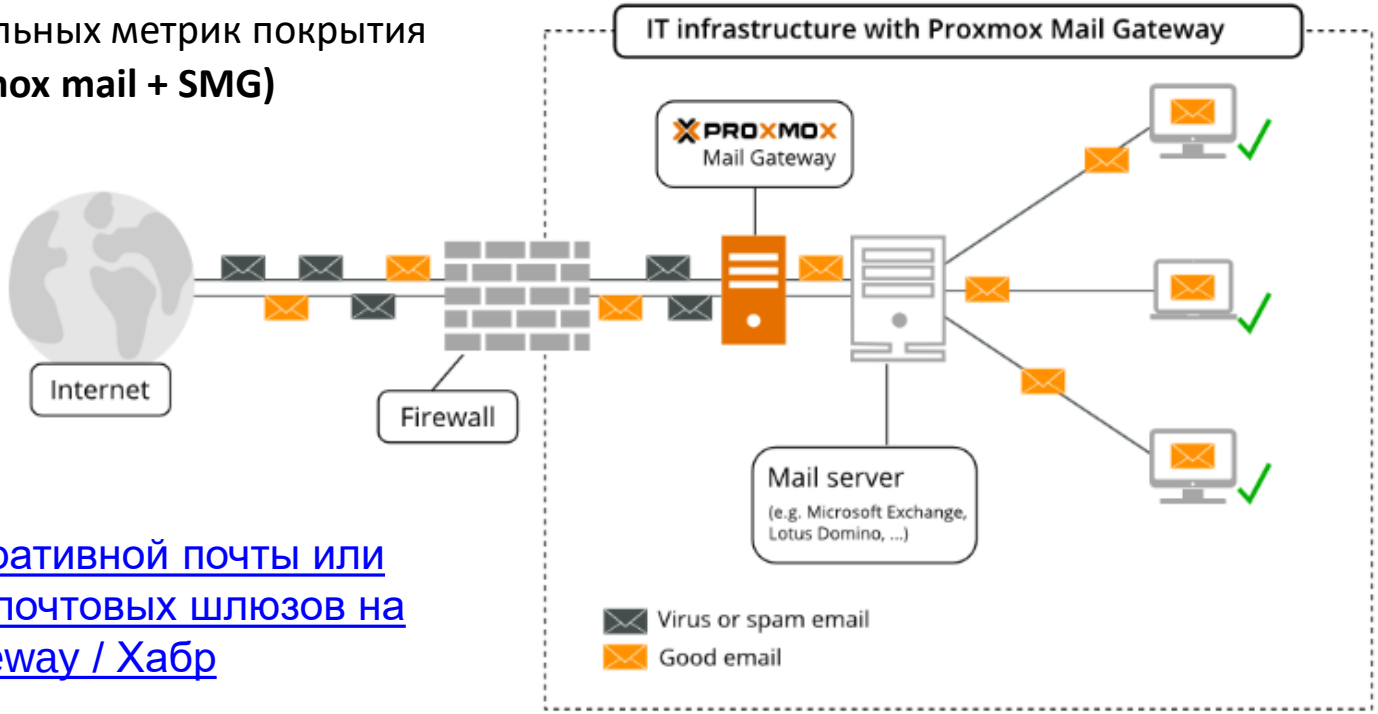
	Кол-во	АВЗ	SOC	FLEET	EDR
ПК	177	173 (98.3%) Из 176	None	165 (93.75%) Из 176	158 (89.77%) Из 176
Сервера	54	50 (96.15%) Из 52	14 (26.92%) Из 52	38 (73.08%) Из 52	51 (98.08%) Из 52
Прочее	392	None	4	None	None
Всего	624	223, (97.81%) Из 228	14, (8.0%) Из 225	203, (89.04%) Из 228	209, (91.67%) Из 228

согаз

Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- **Защита почты (Proxmox mail + SMG)**

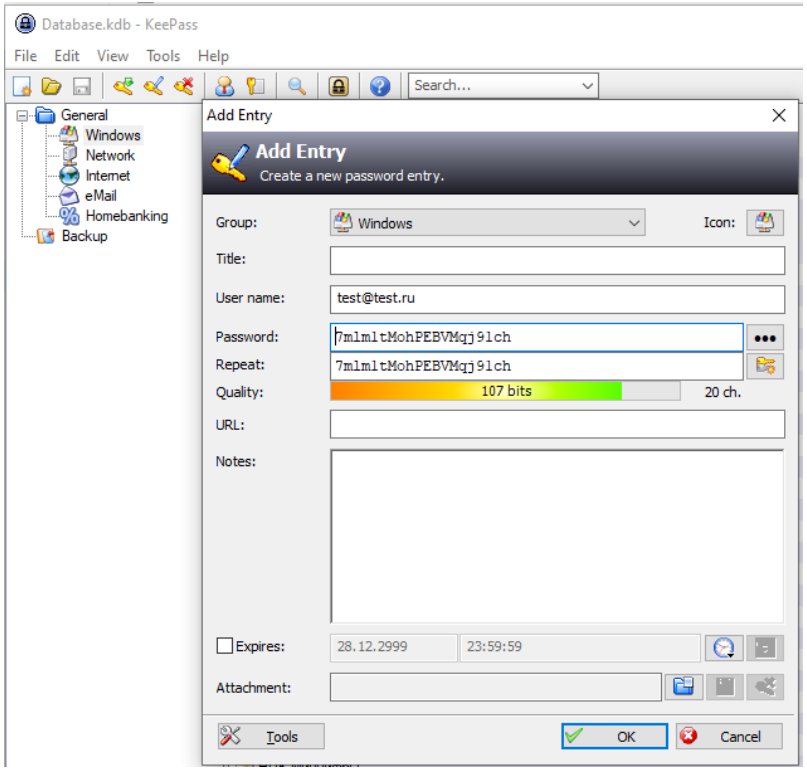


[ЧудESA защиты корпоративной почты или внедрение свободных почтовых шлюзов на базе Proxmox Mail Gateway / Хабр]

Начальные телодвижения

Установка, настройка, доработка:

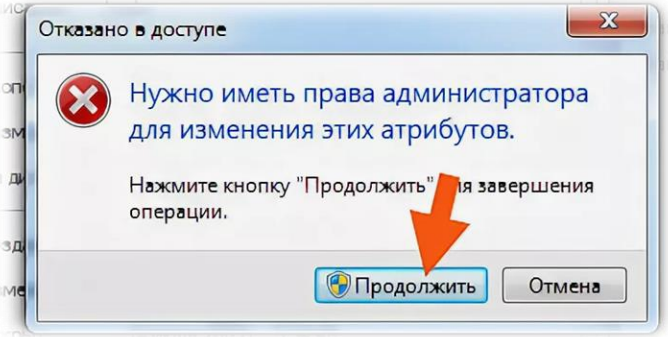
- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- **Менеджеры паролей**



Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- Менеджеры паролей
- **Минимальные права у юзера**



СОГАЗ

Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- Менеджеры паролей
- Минимальные права у юзера
- **Запрет работать из под администратора администраторам**

[конспект админа] Меньше администраторов всем / Хабр

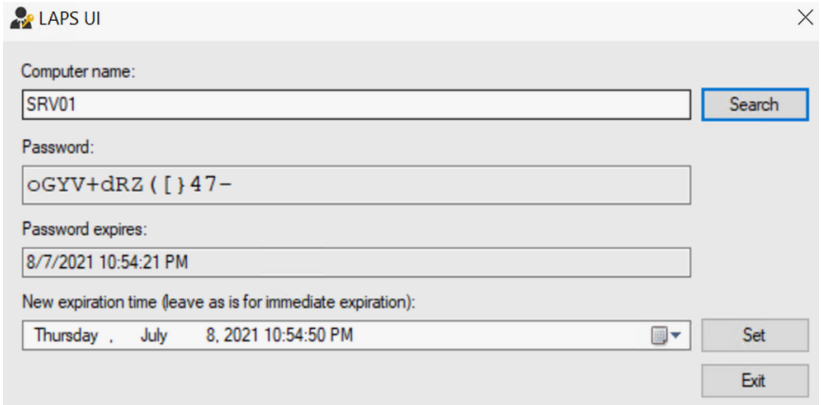
Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- Менеджеры паролей
- Минимальные права у юзера
- Запрет работать из под администратора администраторам
- **Внедрение Local Administrator Password Solution (LAPS)**

Microsoft LAPS

Local Administrator Password Solution



[Управляем паролем локального администратора с помощью LAPS / Хабр]

Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- Менеджеры паролей
- Минимальные права у юзера
- Запрет работать из под администратора администраторам
- Внедрение Local Administrator Password Solution (LAPS)
- **VPN + 2ФА - удалённая работа**

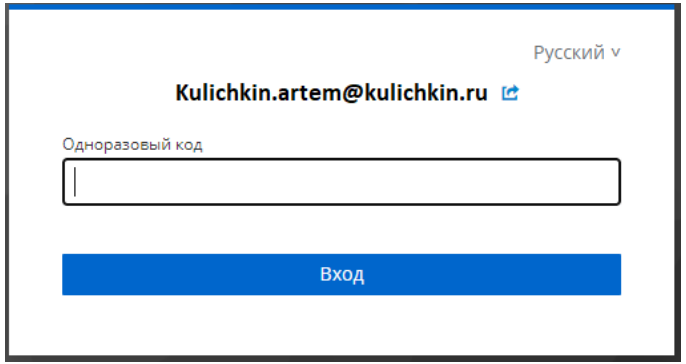
VPN (**RRAS, CISCO, др.**) + Radius + любой OTP

согаз

Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- Менеджеры паролей
- Минимальные права у юзера
- Запрет работать из под администратора администраторам
- Внедрение Local Administrator Password Solution (LAPS)
- VPN + 2ФА - удалённая работа
- **2ФА везде где возможно, 100% внешка**



согаз

Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- Менеджеры паролей
- Минимальные права у юзера
- Запрет работать из под администратора администраторам
- Внедрение Local Administrator Password Solution (LAPS)
- VPN + 2ФА - удалённая работа
- 2ФА везде где возможно, 100% внешка
- **Пром. данные только в проме**

согаз

Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- Менеджер паролей KeePass
- Минимальные права доступа
- Tier 1, Tier 2, Tier 3, Tier 4
- SSH авторизация по ключам
- Патч менеджемент, обновление ОС, ПО.
- Бекап и восстановление + проверка.
- Запретить вход через рут по ssh

Прописать в ОРД спина болеть не будет

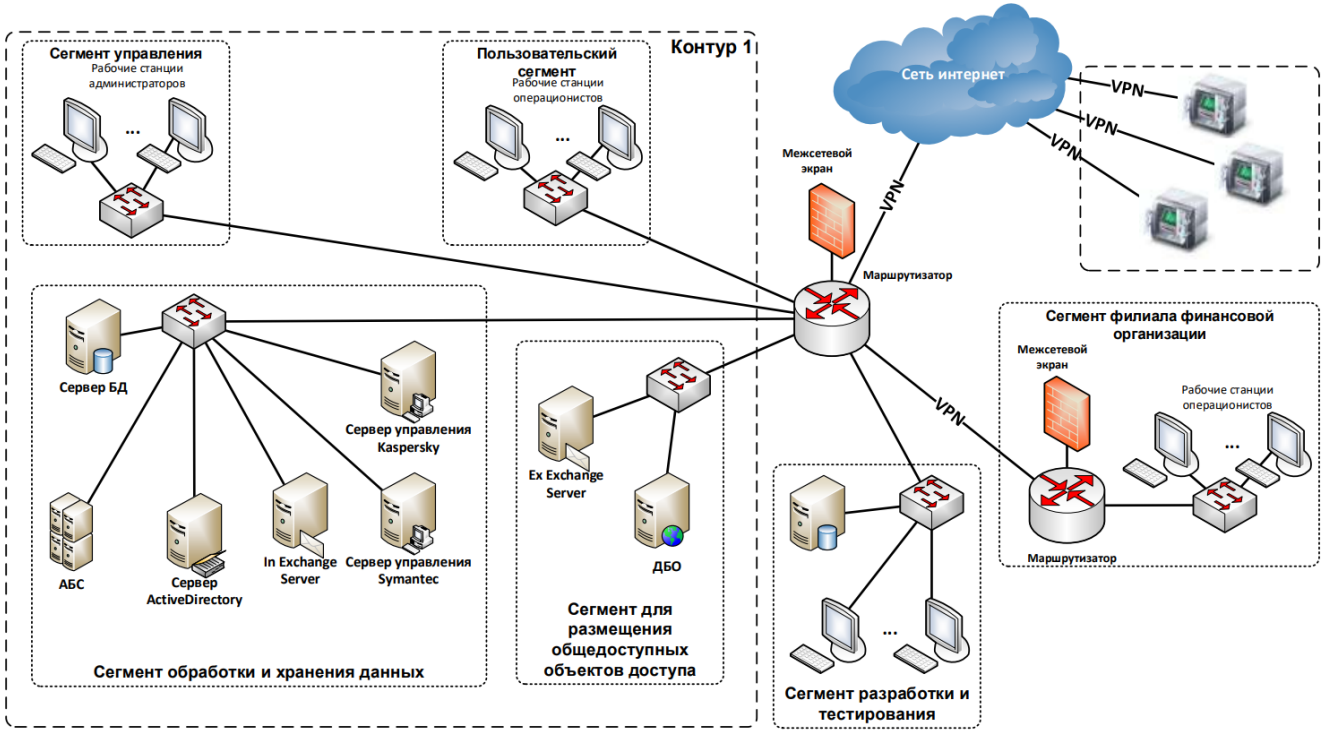
СОГАЗ

Администрирование

Установка, настройка, доработка:

- **Администрирование только из специального сегмента с отдельными учётками и правами**

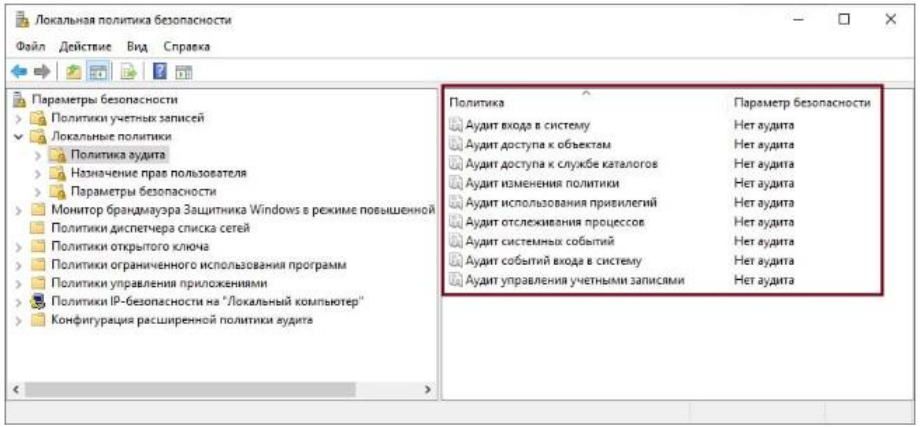
- ✓ Сегментирование сети
- ✓ Разделять прод, тест, деф.
- ✓ Запретить выход в интернет из серверного сегмента
- ✓ Выход в интернет через единый прокси с авторизацией



Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- **Включить расширенный аудит eventlog, Symon, auditd.**



Настройка аудита в Windows для полноценного SOC-мониторинга

Основы аудита. Настраиваем журналирование важных событий в Linux — Хакер

Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- **Менеджер паролей KeePass**

согаз

Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- Менеджер паролей KeePass
- **Минимальные права доступа**

СОГАЗ

Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- Менеджер паролей KeePass
- Минимальные права доступа
- **Tier 0, Tier 1, Tier 2, Tier 3**

Tier 0 **Tier 1** **Tier 2** **Tier 3**

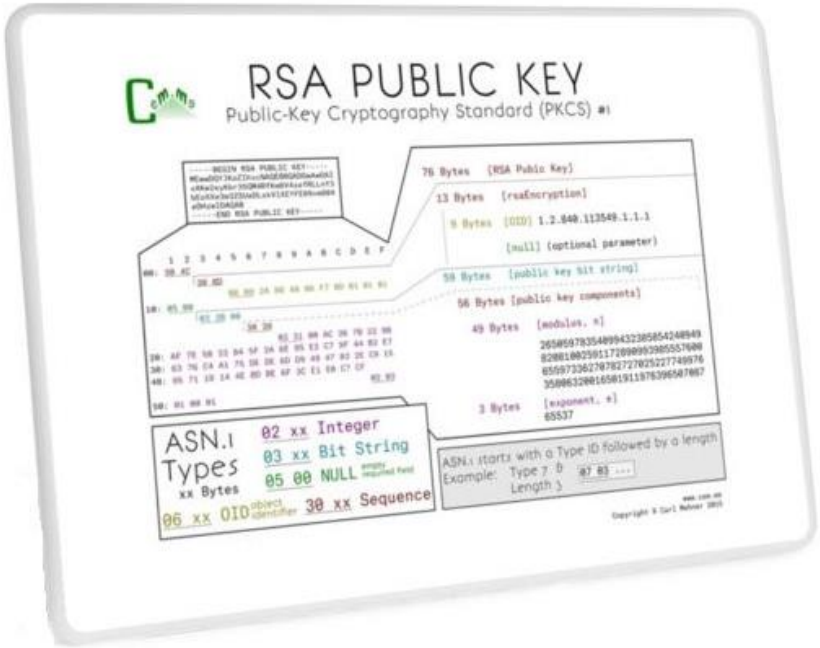
[Многоуровневая модель среды PAM | Microsoft Learn]

согаз

Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- Менеджер паролей KeePass
- Минимальные права доступа
- Tier 1, Tier 2, Tier 3, Tier 4
- **SSH авторизация по ключам**



Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- Менеджер паролей KeePass
- Минимальные права доступа
- Tier 1, Tier 2, Tier 3, Tier 4
- SSH авторизация по ключам
- **Патч менеджемент**

согаз

Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- Менеджер паролей KeePass
- Минимальные права доступа
- Tier 1, Tier 2, Tier 3, Tier 4
- SSH авторизация по ключам
- Патч менеджмент
- **Бекап и восстановление + проверка.**

СОГАЗ

Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- Менеджер паролей KeePass
- Минимальные права доступа
- Tier 1, Tier 2, Tier 3, Tier 4
- SSH авторизация по ключам
- Патч менеджемент
- Бекап и восстановление + проверка.
- **Запретить вход через рут по ssh**

Прописать в ОРД спина болеть не будет

СОГАЗ

Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- Менеджер паролей KeePass
- Минимальные права доступа
- Tier 1, Tier 2, Tier 3, Tier 4
- SSH авторизация по ключам
- Патч менеджемент
- Бекап и восстановление + проверка.
- Запретить вход через рут по ssh

Прописать в ОРД спина болеть не будет

СОГАЗ

Немного допов

Установка, настройка, доработка:

- Процесс безопасной разработки opensource решениями. (metodologiya-appsec-table-top.pdf)
- Запрет запуска из “Download”
- Нет секретов в коде
- Hardening fleet
- AntiDDos на уровне провайдера
- Обучение работников, тестовый фишинг (Используйте доступные онлайн-ресурсы и руководства, пилоты)
- Анализ утечек «haveibeenpwned.com»
- Проверка ПО в песочнице: кукушка, энiран.
- Wazuh
- Пилоты! DCAP и тд…

Заключение

Работай руками, не всё решается деньгами.

СОГАЗ

Спасибо
за внимание