



ОПТИМИЗАЦИЯ ЗАТРАТ НА ИБ

ЦЕНА \ КАЧЕСТВО

ПОВЫШАЕМ ЗРЕЛОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Куличкин Артём Александрович

CISM, CISA, CEH, CND.

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

Введение

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

Используй лучшие практики с простым контролем.



AD

Аудит + доработка AD:

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

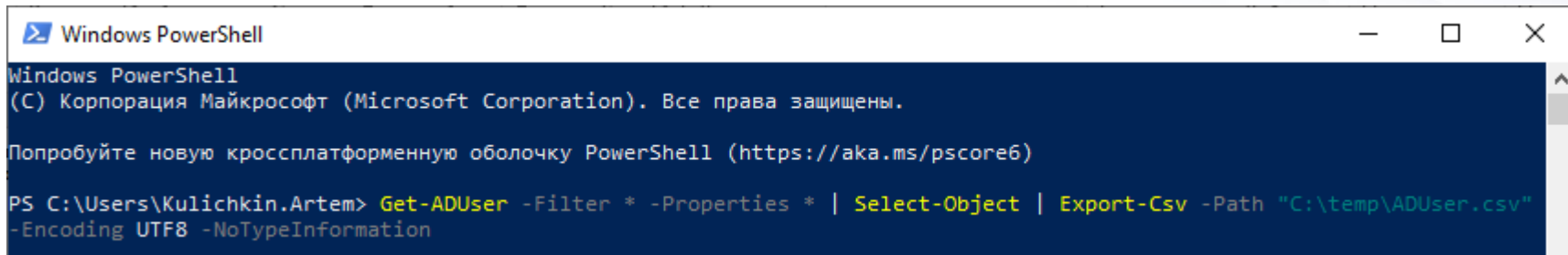


Active Directory

AD

Аудит + доработка AD:

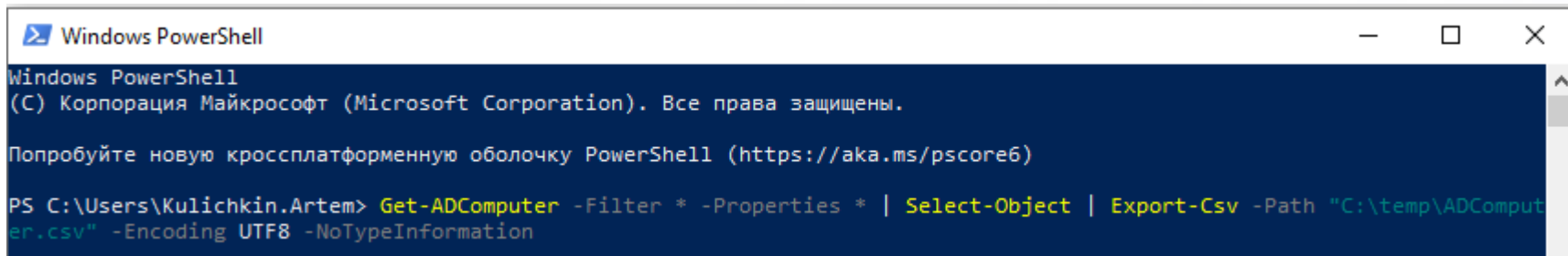
- **Учётные записи** (Password ,Password never expires, last logon)



```
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Попробуйте новую кроссплатформенную оболочку PowerShell (https://aka.ms/pscore6)

PS C:\Users\Kulichkin.Artem> Get-ADUser -Filter * -Properties * | Select-Object | Export-Csv -Path "C:\temp\ADUser.csv"
-Encoding UTF8 -NoTypeInfoInformation
```



```
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Попробуйте новую кроссплатформенную оболочку PowerShell (https://aka.ms/pscore6)

PS C:\Users\Kulichkin.Artem> Get-ADComputer -Filter * -Properties * | Select-Object | Export-Csv -Path "C:\temp\ADComputer.csv" -Encoding UTF8 -NoTypeInfoInformation
```

[Аудит пользователей AD с помощью Powershell / Хабр](#)



AD

Admin Accounts With SPN



0.22%

3 Admin Accounts With SPN



Accounts With Passwords That Never Expire

1,158

Users

84% Accounts With Passwords That Never Expire



Accounts That Do Not Require Kerberos Pre-Authentication

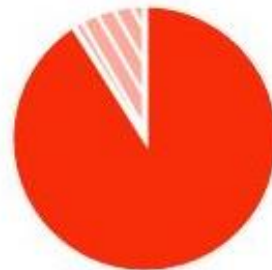


0.43%

6 Accounts That Do Not Require Kerberos Pre-Authentication



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
```

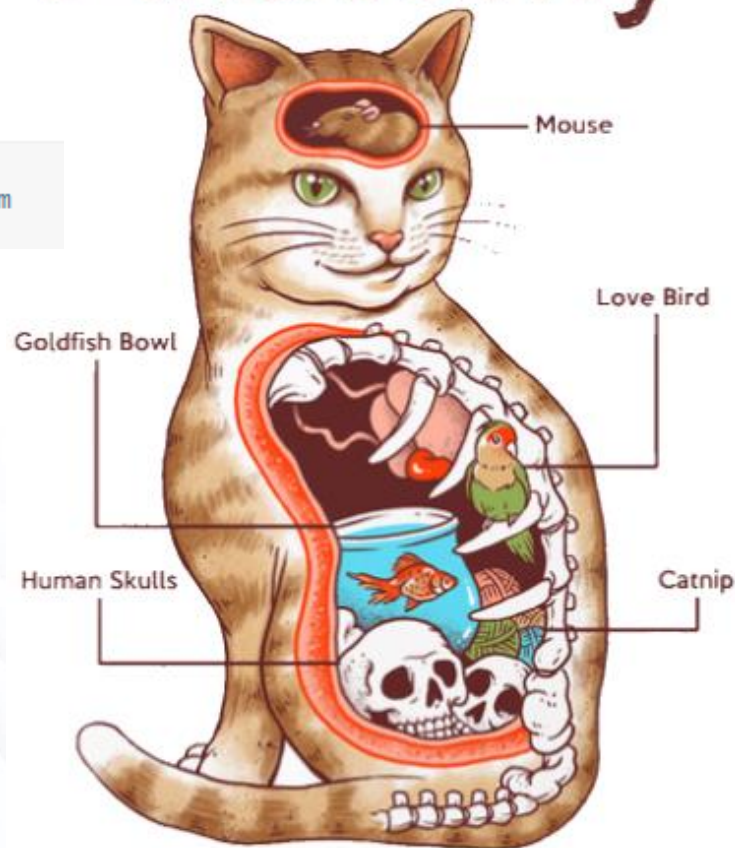
```
hashcat.exe -m 1000 E:\hashs.txt --show
```

```
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](#)

Guide to Cat^{HASH} Anatomy



AD

Аудит + доработка AD:

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



 Lithnet

Password Protection for Active Directory

Password93.]

Password93.



ооPS!

Ой! Ваш пароль взламывают быстрее, чем вы скажете «Ой!»



Пароль пора срочно менять!

- Плохая новость
 - ⚠ Часто используемое слово
- Этот пароль засветился в базах утекших паролей 12 раз.

[Weakpass: biggest wordlists collection](#)

[HashMob | Resources | HashMob Wordlists](#)

[Защита паролем AD — Lithnet](#)

AD

Аудит + доработка AD:

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

Y	Z	AA	AB
Enabled	LastLogonDate	HomePage	instanceType
True	22.02.2024 1:	Сортировка от старых к новым	
True	11.03.2024 20:	Сортировка от новых к старым	
True	08.03.2024 3:	Сортировка по цвету	
True	07.03.2024 3:	Удалить фильтр из столбца "LastLogonDate"	
True	06.03.2024 9:	Фильтр по цвету	
True	10.03.2024 7:	Фильтры по дате	
True	04.03.2024 20:	Область поиска: (Все)	
True	08.03.2024 1:	☒ 2019	
True	11.03.2024 22:	☒ 2018	
True	06.03.2024 15:	☒ 2017	
True	04.03.2024 19:	☒ 2016	
True	09.03.2024 0:	☒ 2014	
True	08.03.2024 23:	☒ 2013	
True	06.03.2024 16:	☒ 2012	
True	13.11.2023 18:	☒ 2011	
		☒ 2009	
		☒ (Пустые)	

Показаны не все элементы

OK Отмена

Было

Y	Z
Enabled	LastLogonDate
True	17.07.2009 17:15
True	19.04.2011 22:05
True	22.05.2012 15:04
True	13.02.2013 8:17
True	11.03.2014 12:36
True	25.06.2014 9:30
True	24.08.2014 13:24
True	07.09.2014 12:10
True	09.03.2016 9:15
True	15.04.2016 14:22
True	20.07.2016 17:51
True	15.08.2016 15:59
True	12.09.2016 15:19
True	16.09.2016 17:27
True	24.09.2016 16:06
True	26.09.2016 15:39
True	21.10.2016 10:38
True	01.11.2016 15:40
True	14.11.2016 16:04
True	23.11.2016 13:16
True	18.01.2017 21:25

Y	Z	AA	AB
Enabled	LastLogonDate	HomePage	instanceType
True	12.10.2023 7:	Сортировка от старых	
True	03.10.2023 2:	Сортировка от новых к	
True	09.10.2023 13:	Сортировка по цвету	
True	08.10.2023 10:	Удалить фильтр из сто	
True	07.10.2023 15:	Фильтр по цвету	
True	05.10.2023 17:	Фильтры по дате	
True	06.10.2023 4:	Область поиска: (Все)	
True	08.10.2023 9:	☒ (Выделить все)	
True	05.10.2023 18:	☒ 2023	
True	08.10.2023 17:	☒ Август	
True	10.10.2023 18:	☒ Сентябрь	
True	08.10.2023 11:	☒ Октябрь	
True	04.10.2023 14:		
True	03.10.2023 11:		
True	08.10.2023 11:		
True	09.10.2023 10:		

Стало

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.local\...	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.local\...	Для этой папки, ее подп...	пользователи@builtin	✗ Права преобразованы	F M X W R L S	F M X W R L S
ts.sus.local	\\ts.sus.local\...	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.local\...	Для этой папки, ее подп...	пользователи@builtin	✗ Права удалены		F M X W R L S
ts.sus.local	\\ts.sus.local\...	Для этой папки, ее подп...	все	✗ Права удалены		F M X W R L S
ts.sus.local	\\ts.sus.local\...	Для этой папки, ее подп...	пользователи@builtin	⚠ Неверные флаги наследования	F M X W R L S	F M X W R L S
ts.sus.local	\\ts.sus.local\...	Для этой папки, ее подп...	пользователи@builtin	⚠ Наследование без родителя	F M X W R L S	
ts.sus.local	\\ts.sus.local\...	Для этой папки, ее подп...	пользователи@builtin	⚠ Ложное наследование		F M X W R L S
ts.sus.local	\\ts.sus.local\...	Для этой папки, ее подп...	все	⚠ Добавлен пользователь	F M X W R L S	
ts.sus.local	\\ts.sus.local\...	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

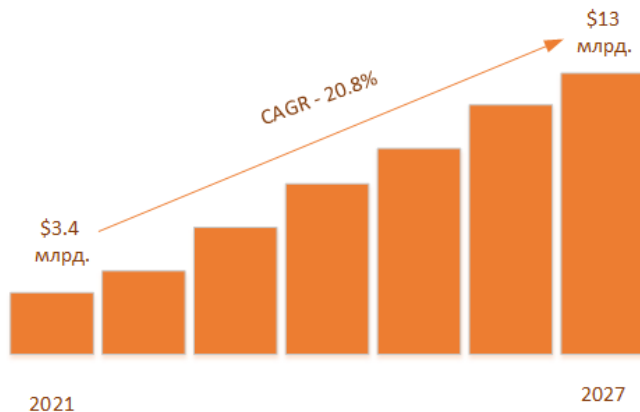
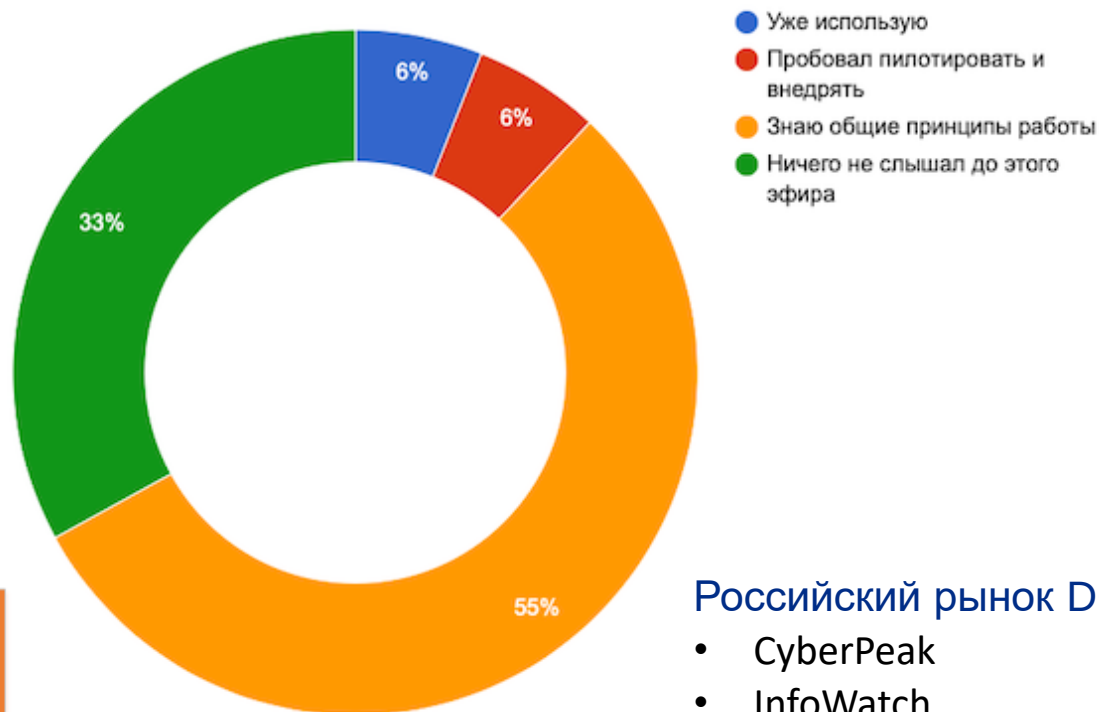


Рисунок 1. Насколько хорошо вы знакомы с решениями DCAP?



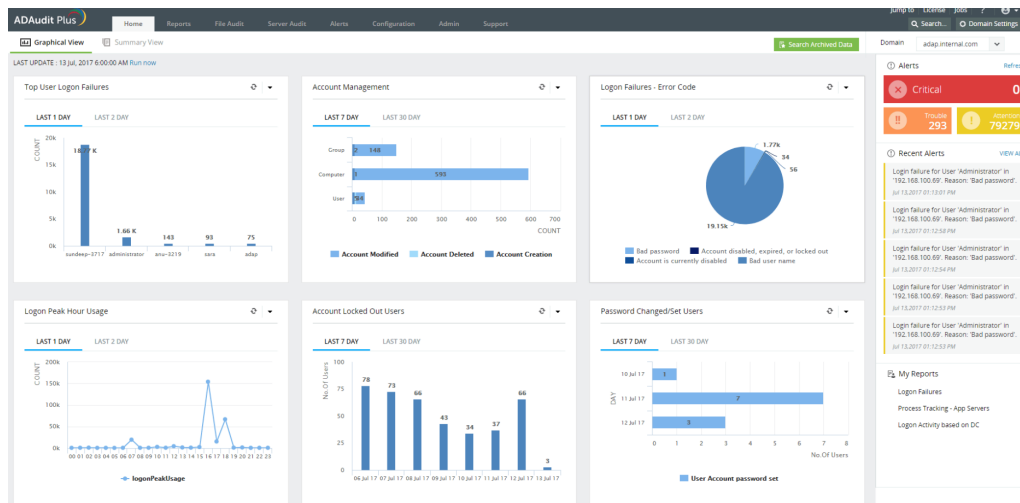
Российский рынок DCAP

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

AD

Аудит + доработка AD:

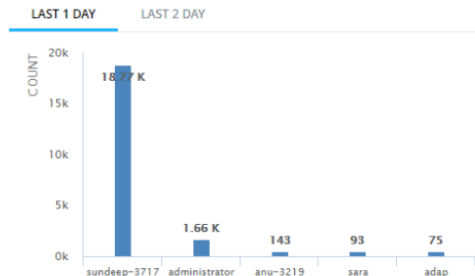
- Учётные записи
- Брут паролей
- Lithnet Password Protection
- Хосты
- Неправильное наследование
- Пилоты DCAP
- **AD Audit Plus**



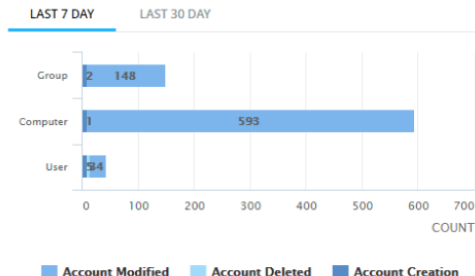
AD Audit plus

LAST UPDATE : 13 Jul, 2017 6:00:00 AM [Run now](#)

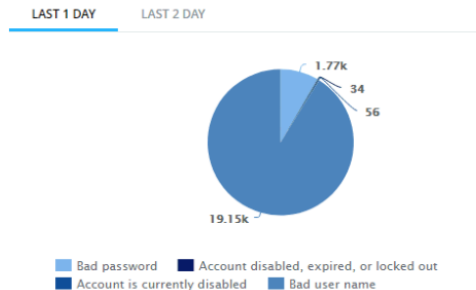
Top User Logon Failures



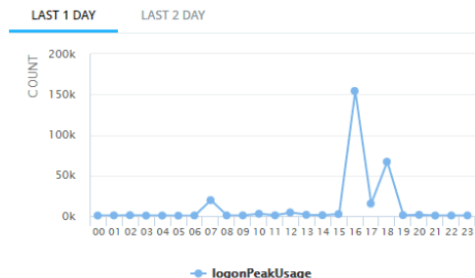
Account Management



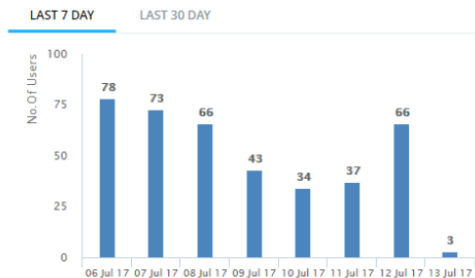
Logon Failures - Error Code



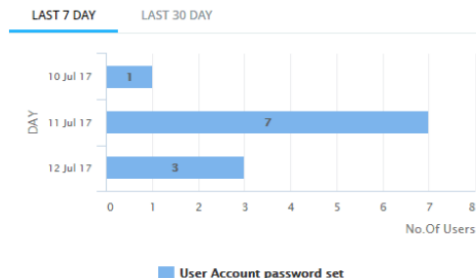
Logon Peak Hour Usage



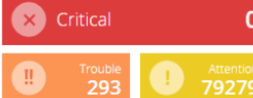
Account Locked Out Users



Password Changed/Set Users



Alerts



Recent Alerts

- Logon failure for User 'Administrator' in '192.168.100.69'. Reason: 'Bad password'.
Jul 13, 2017 01:13:01 PM
- Logon failure for User 'Administrator' in '192.168.100.69'. Reason: 'Bad password'.
Jul 13, 2017 01:12:58 PM
- Logon failure for User 'Administrator' in '192.168.100.69'. Reason: 'Bad password'.
Jul 13, 2017 01:12:54 PM
- Logon failure for User 'Administrator' in '192.168.100.69'. Reason: 'Bad password'.
Jul 13, 2017 01:12:53 PM
- Logon failure for User 'Administrator' in '192.168.100.69'. Reason: 'Bad password'.
Jul 13, 2017 01:12:53 PM

My Reports

- Logon Failures
- Process Tracking - App Servers
- Logon Activity based on DC

Анализ инфраструктуры

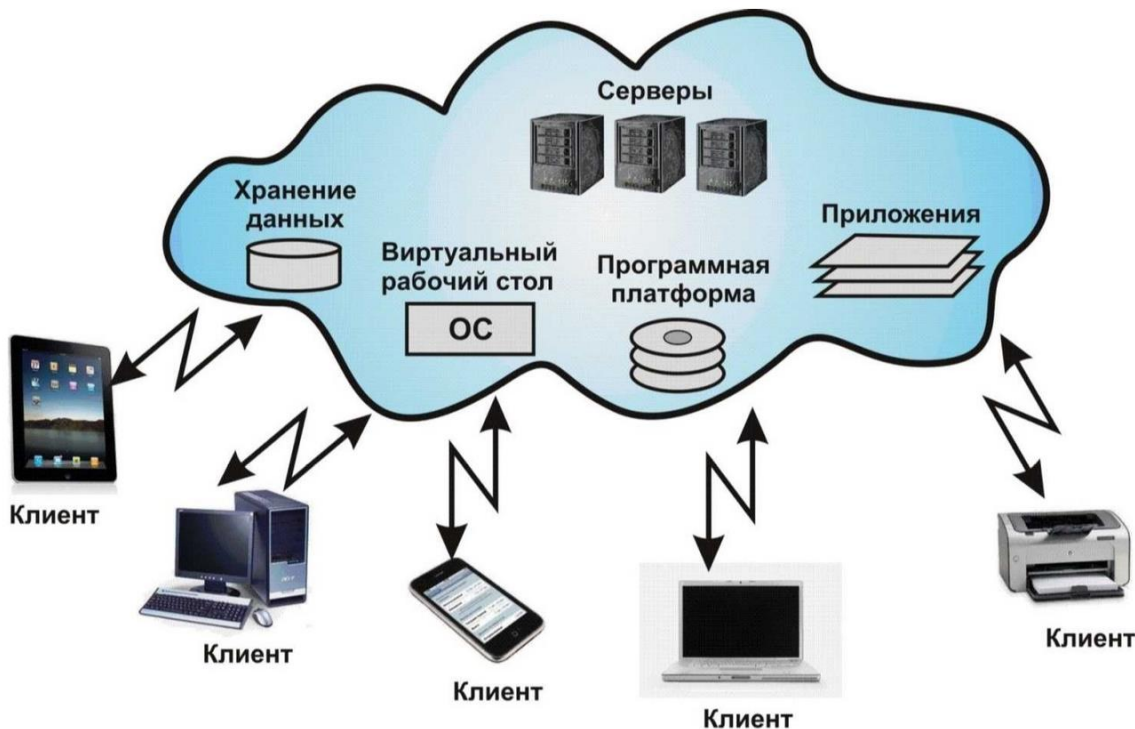
Аудит + доработка инфраструктуры:

- 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)



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				

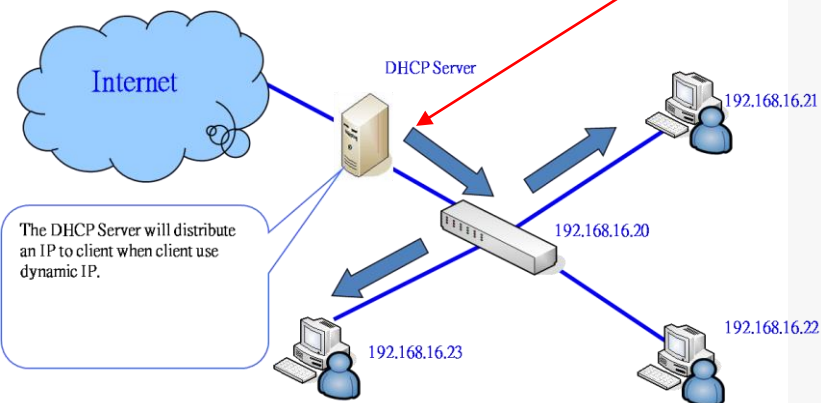
10.22.11.18	FLEET	
10.22.11.18	PORT	21/ftp/vsftpd/2.0.5/cpe:/a:vsftpd:vsftpd:2.0.5 21/
10.22.11.18	PORT	23/telnet/Linux telnetd//cpe:/o:linux:linux_kernel 23/
10.22.11.18	PORT	80/http/mini_httpd/1.19_19dec2003/cpe:/a:acme:mini_httpd:1.19_19dec2003 80/{"http-server-header": "mini_httpd/1.19_19dec2003", "http-title": "Site doesn't have a valid SSL certificate"}
10.22.11.18	PORT	427/svrlloc/// 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 http://cpe:/o:linux:linux_kernel 5988/{"http-title": "Site doesn't have a valid SSL certificate"}
10.22.11.18	MAIN_DATA	
10.22.11.18	KSC	
10.22.11.18	FLEET	
10.0.55.112	IT	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/sentinelism/// 1947/{"fingerprint-strings": "\n FourOhFourRequest:\n HTTP/1.0 403 Forbidden\n Server: HASP LM/24.00\n Date: Sat, 02 Nov 2019 12:00:00 GMT"}
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\n"}
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/

Анализ инфраструктуры

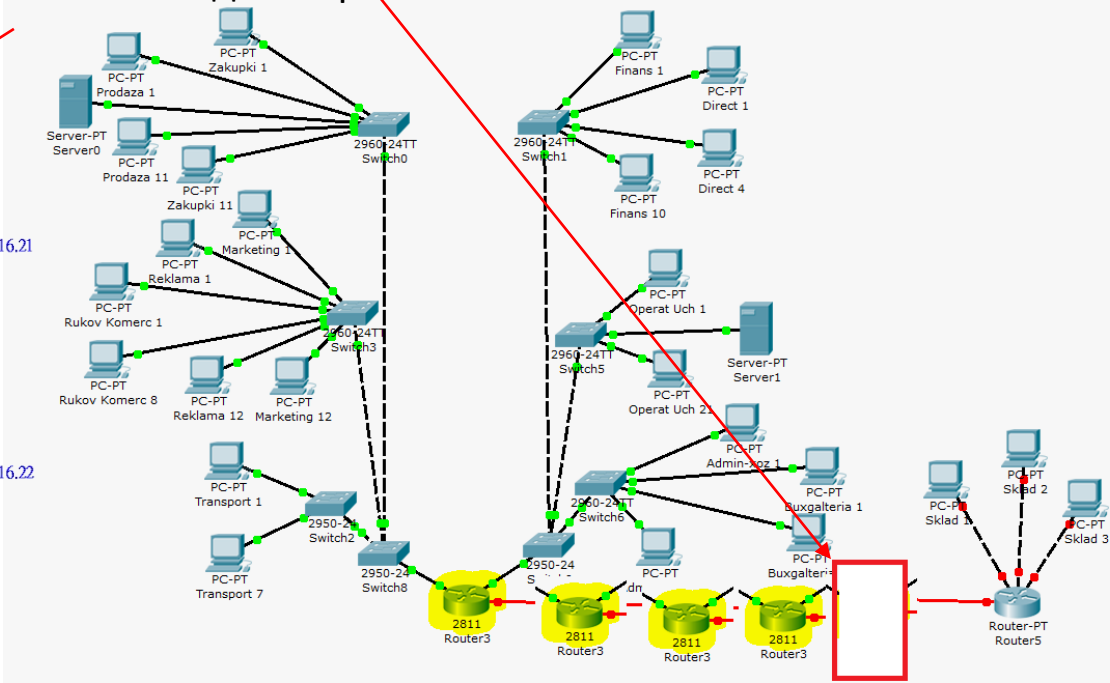
Аудит + доработка инфраструктуры:

- 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

77.222.61.88

As of: Nov 06, 2024 6:58am UTC | Latest

Summary

History

WHOIS

Basic Information

Forward DNSwww.mpzmr.ru, xn--vip42.web.ru, online:...

Routing77.222.32.0/24 via SV

Services (1)3306/MYSQL

LabelsDATABASE

MYSQL 3306/TCP

DATABASE

Software

Oracle MySQL

Details

Error Code1130

Error IDER_HOST_NOT_PRIVILEGED

Error MessageHost '66.132.153.63' is not allowed to connect to this MySQL server

myasnackj

5/24

178.159.43.197

178-159-43-197.netherlands-2.vps.ac

Ubuntu Linux

PODAON (211381)

North Holland, Netherlands

jquery

click

default-handling-page

remote-access

22/SSH

80/HTTP

443/HTTP

188.124.39.78

SELECTEL (49505)

St.-Petersburg, Russia

remote-access

database

angularajs

22/SSH

5432/POSTGRES

80/HTTP

7946/UNKNOWN

443/HTTP

8000/HTTP

9443/HTTP

Hosts

Results: 2 Time: 0.01s

Host Filters

Labels:

2 remote-access

1 angularajs

1 database

1 default-handling-page

1 jquery

More

Autonomous System:

1 PODAON

1 SELECTEL

Location:

1 Netherlands

1 Russia

Service Filters

Service Names:

9 HTTP

2 SSH

2 UNKNOWN

1 POSTGRES

Report

Docs

Subscriptions

Register

Log In

Register or Log In

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

← ↻ 📄 <https://kolbasa.ru/bitrix/admin/#authorize>

kolbasa.ru

Авторизация

Пожалуйста, авторизуйтесь

Логин

Пароль

☐ Запомнить меня на этом компьютере

[Забыли свой пароль?](#)

или войдите через

Битрикс24

1С-Битрикс: Управление сайтом 22.0.300. © Битрикс, 2002-2022



Банк данных угроз безопасности

Федеральная служба по техническому и экспортному контролю

ФСТЭК России

Угрозы

Уязвимости

Тестирование обновлений

Документы

Обратная связь

Обновления

Участники

Обучение

[Главная](#) / [Список уязвимостей](#) / BDU:2023-05857

BDU:2023-05857: Уязвимость модуля landing системы управления содержимым сайтов (CMS) 1С-Битрикс: Управление сайтом вызвана нарушением выполнения команд ОС на уязвимом узле, получить контроль над ресурсами и проникнуть во внутреннюю сеть

Описание уязвимости	Уязвимость модуля landing системы управления содержимым сайтов (CMS) 1С-Битрикс: Управление сайтом вызвана нарушением выполнения команд ОС на уязвимом узле, получить контроль над ресурсами и проникнуть во внутреннюю сеть
Вендор	ООО «1С-Битрикс»
Наименование ПО	1С-Битрикс: Управление сайтом (запись в едином реестре российских программ №35)
Версия ПО	до 23.850.0 (1С-Битрикс: Управление сайтом)
Тип ПО	Прикладное ПО информационных систем
Уровень опасности уязвимости	Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10) Критический уровень опасности (базовая оценка CVSS 3.0 составляет 10)
Дата выявления	13.09.2023
Идентификатор типа	CWE-362

Subject Name	
Country	RU
State/Province	Moscow Oblast
Locality	Odintsovo
Organization	OOO Mpz Myasnitskiy Ryad
Common Name	*.kolbasa.ru
Issuer Name	
Country	BE
Organization	GlobalSign nv-sa
Common Name	GlobalSign RSA OV SSL CA 2018
Validity	
Not Before	Mon, 22 Jan 2024 08:58:39 GMT
Not After	Sat, 22 Feb 2025 08:58:38 GMT
Subject Alt Names	
DNS Name	*.kolbasa.ru
DNS Name	kolbasa.ru

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**



AnyDesk



TeamViewer



Chrome
Remote
Desktop



TightVNC



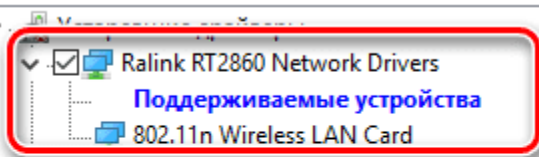
Virtual
Network
Computing



UltraVNC



Н



[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](#)

[ОСПБ «МАКС»](#)

[Учетные системы](#)

[Складские системы](#)

[Логистическое ПО](#)

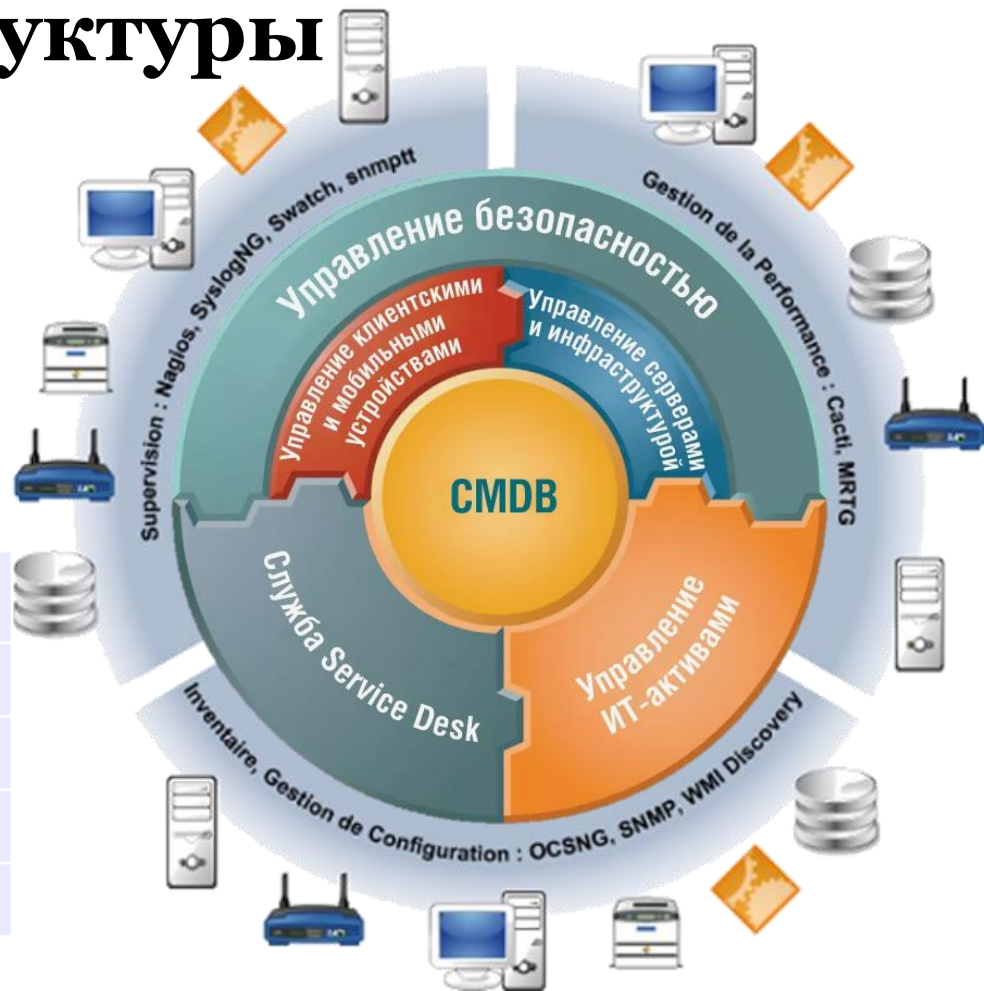
[Склад-15](#)

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.jspa?id=92004	Игорь Игоревич Игорев
90.90.48.39	G-0000-5202	https://ShowObject.jspa?id=92699	Игорь Игоревич Игорев
90.86.4.2	G2800-SQ01	https://ShowObject.jspa?id=99942	Иванов Иван Иванович
90.46.0.57	G6400-DP01	https://ShowObject.jspa?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)

ZABBIX



Network and server infrastructure



Cloud deployments



APIs and websites



Services and applications



IoT devices and sensors



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
- 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

Начальные телодвижения

Установка, настройка, доработка:

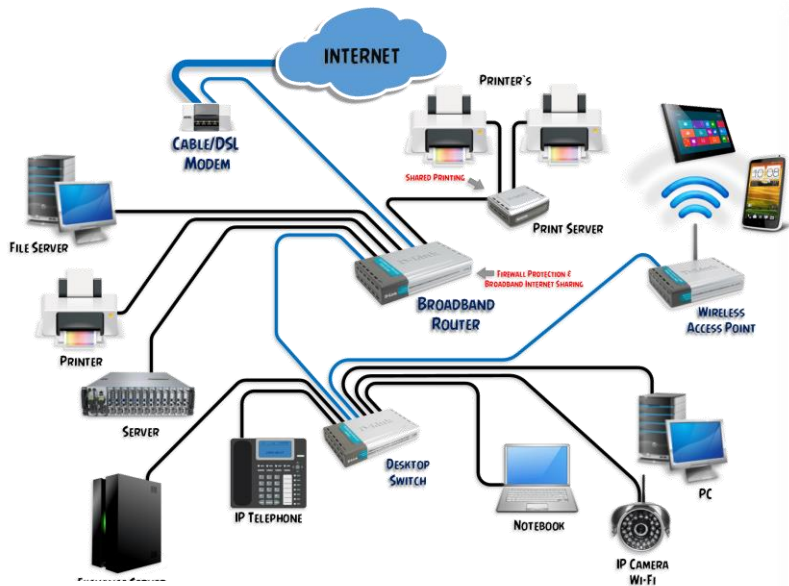
- Ограничение физического доступа к инфраструктуре.



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**

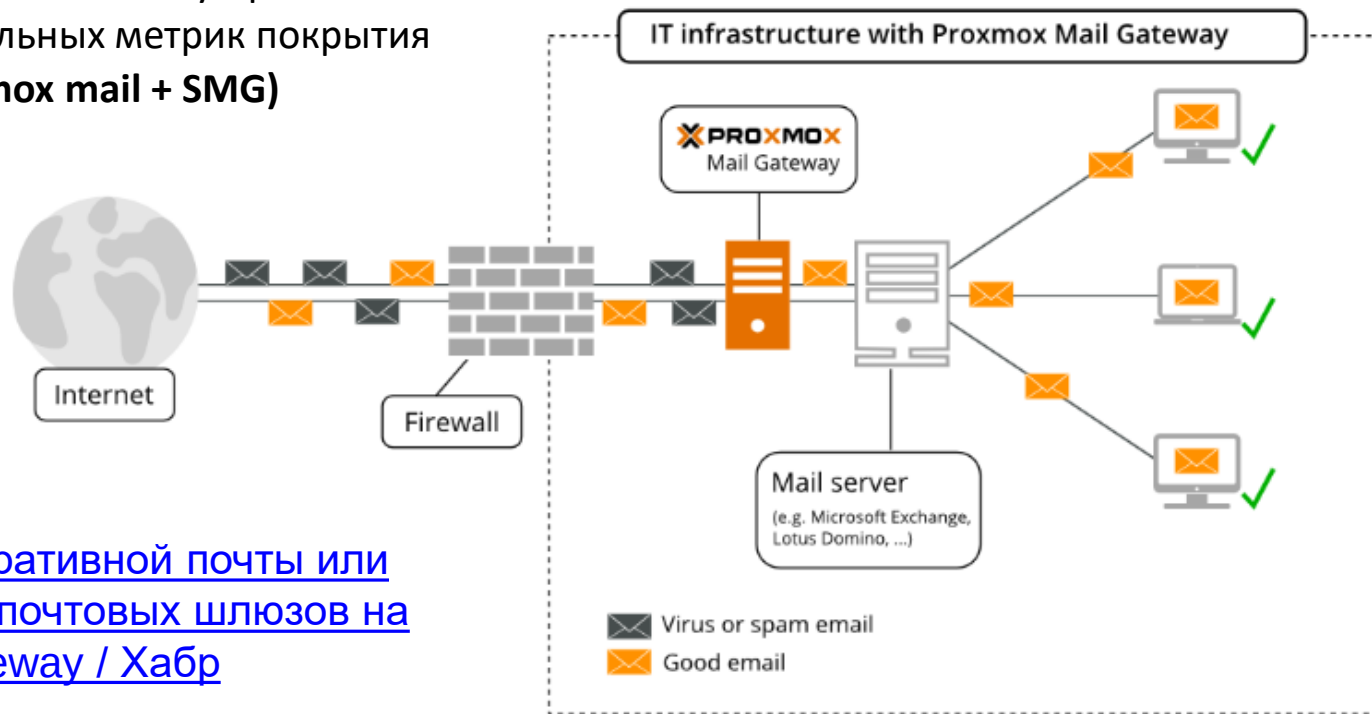
AB3 EDR SOC IDS DLP ...

	Кол-во	AB3	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

Начальные телодвижения

Установка, настройка, доработка:

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

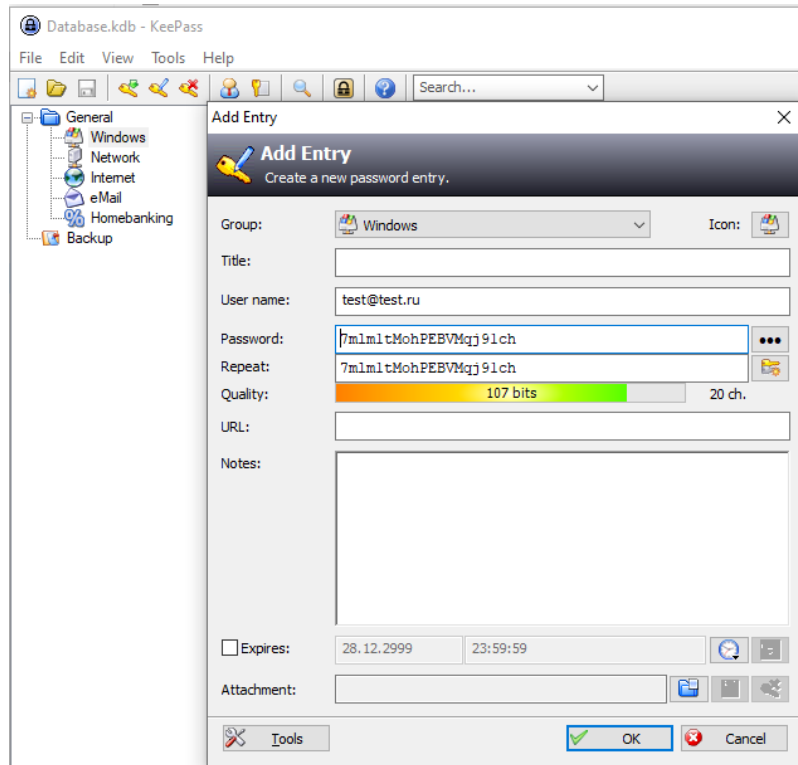


[ЧудЕСА защиты корпоративной почты или внедрение свободных почтовых шлюзов на базе Proxmox Mail Gateway / Хабр](#)

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
- **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)**

A screenshot of the LAPS UI window. The window title is "LAPS UI". It contains several fields: "Computer name:" with the value "SRV01" and a "Search" button; "Password:" with the value "oGYV+dRZ ([} 47-"; "Password expires:" with the value "8/7/2021 10:54:21 PM"; and "New expiration time (leave as is for immediate expiration):" with a date picker showing "Thursday, July 8, 2021 10:54:50 PM". There are "Set" and "Exit" buttons at the bottom right.

[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

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**

Русский v

Kulichkin.artem@kulichkin.ru

Одноразовый код

Вход

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**



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, обновление ОС, ПО.
- Бэкап и восстановление + проверка.
- Запретить вход через рут по ssh

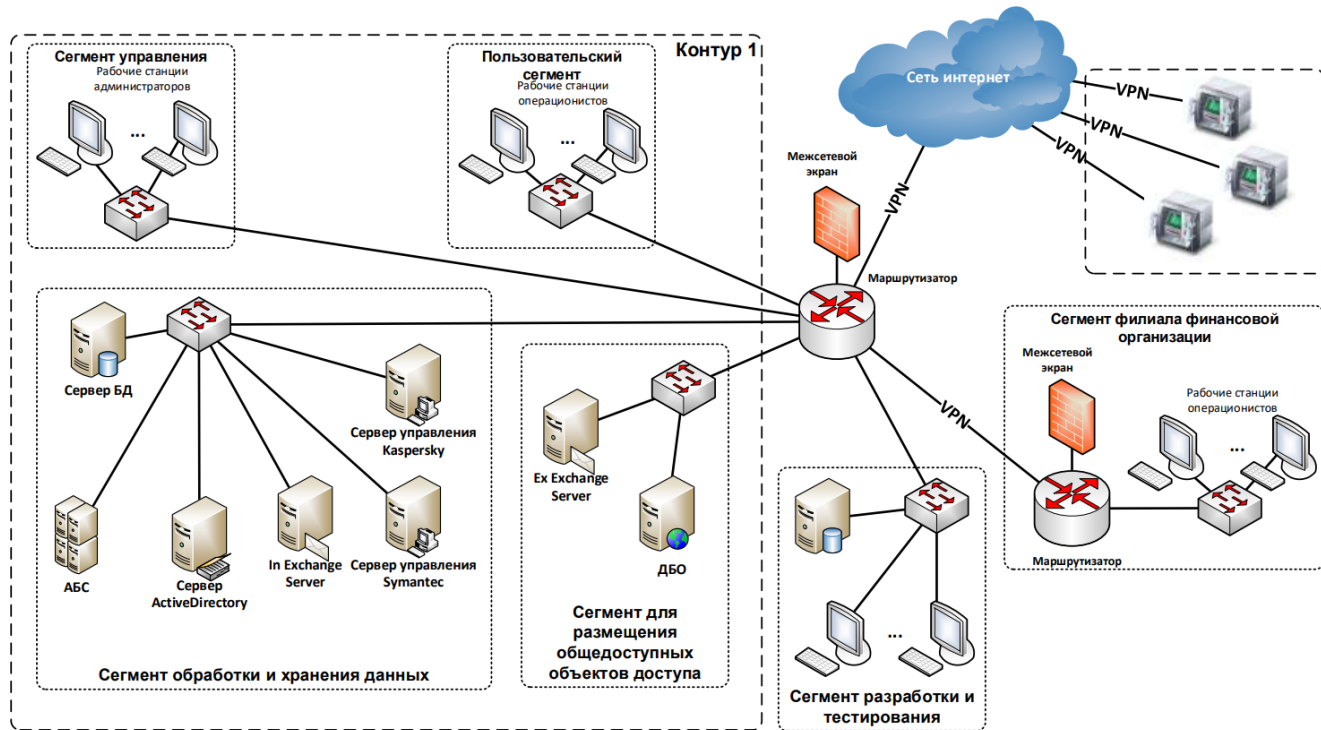
Прописать в ОРД

Администрирование

Установка, настройка, доработка:

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

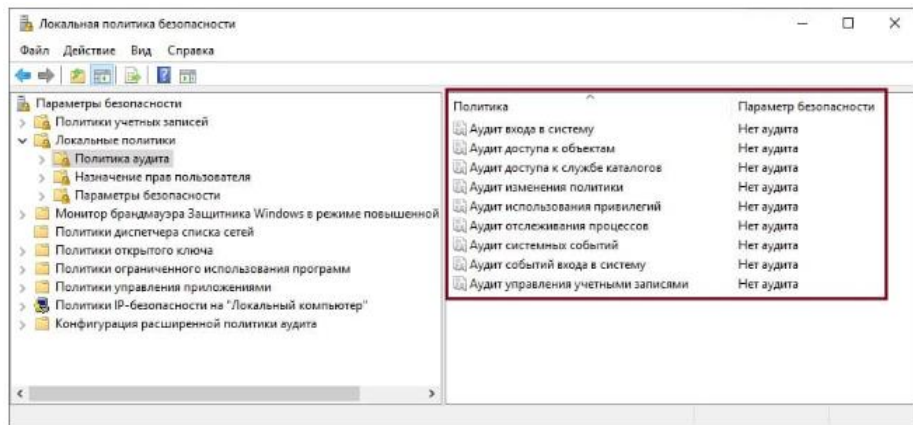
- ✓ Сегментирование сети
- ✓ Разделять прод, тест, деф.
- ✓ Запретить выход в интернет из серверного сегмента
- ✓ Выход в интернет через единый прокси с авторизацией



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**



KeePass

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**



Администрирование

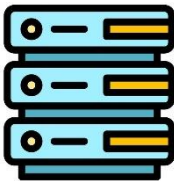
Установка, настройка, доработка:

- 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



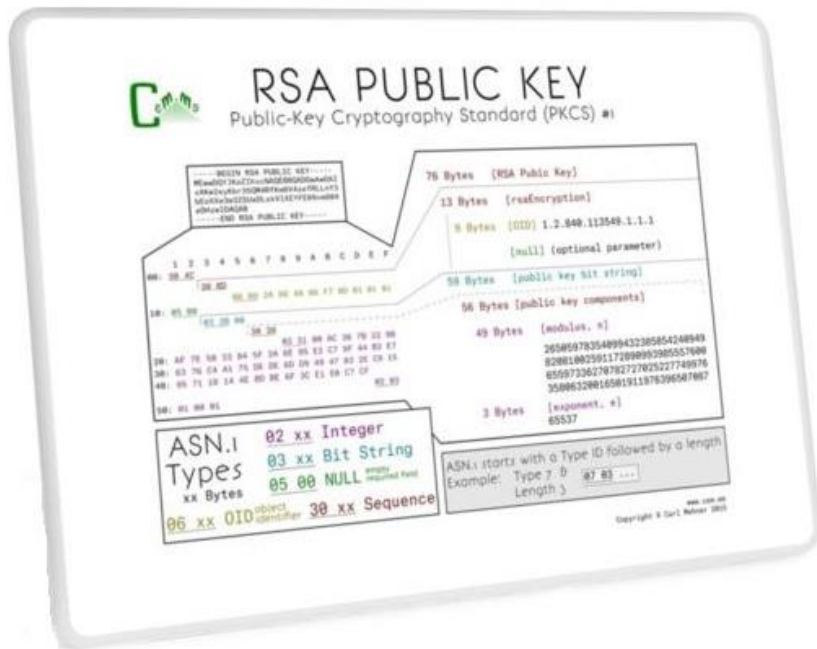
Tier 3



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 менеджмент**



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.**



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.
- **Запретить вход через рут по ssh**

Прописать в ОРД

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, эниран.
- Wazuh
- Пилоты! DCAP и тд...

Заключение

Не усложняйте простое, а упрощайте сложное...



**Спасибо
за внимание**