Эшелон
комплексная безопасность

Мониторинг событий информационной безопасности на объектах КИИ с помощью KOMRAD Enterprise SIEM

Дорофеев Александр, CISSP, CISA, CISM

План

1. Ключевые требования ФСТЭК России и ФСБ России к мониторингу КИИ
2. Принцип работы SIEM-систем
3. KOMRAD Enterprise SIEM

Приказ ФСТЭК России от 25 декабря 2017 г. N 239

- АУД.4 Регистрация событий безопасности
- АУД.7 Мониторинг безопасности
- ИНЦ.0 Регламентация правил и процедур
- ИНЦ.1 Выявление компьютерных инцидентов
- ИНЦ.2 Информирование о компьютерных инцидентах
- ИНЦ.3 Анализ компьютерных инцидентов
- ИНЦ.4 Устранение последствий компьютерных инцидентов
- ИНЦ.5 Принятие мер по предотвращению повторного возникновения
- компьютерных инцидентов
- ИНЦ.6 Хранение и защита информации о компьютерных инцидентах

Приказ ФСБ РОССИИ от 24 июля 2018 года N 367

5. Информация, указанная в пункте 5 Перечня, направляется субъектом критической информационной инфраструктуры в НКЦКИ не позднее 24 часов с момента обнаружения компьютерного инцидента.

Перечень:

5. Информация о компьютерных инцидентах, связанных с функционированием объектов критической информационной инфраструктуры:

- дата, время, место нахождения или географическое местоположение объекта критической информационной инфраструктуры, на котором произошел компьютерный инцидент;
- наличие причинно-следственной связи между компьютерным инцидентом и компьютерной атакой;
- связь с другими компьютерными инцидентами (при наличии);
- состав технических параметров компьютерного инцидента;
- последствия компьютерного инцидента.

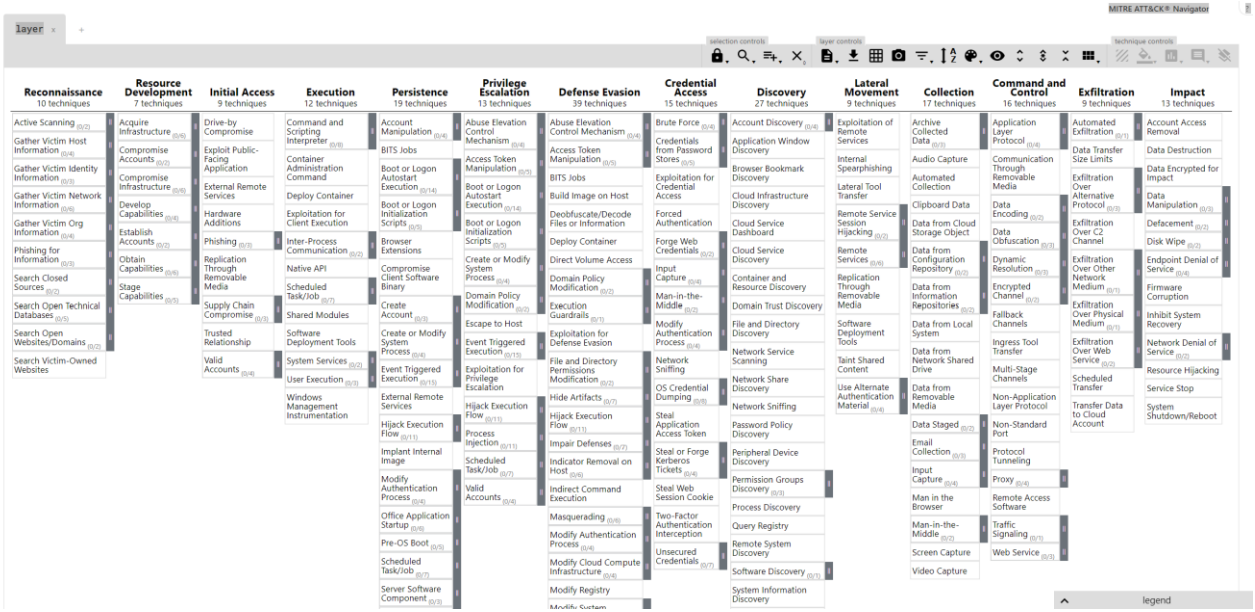
Центр мониторинга информационной безопасности (Security Operations Center)

подразделение организации, осуществляющее мониторинг информационной безопасности и улучшающее защищенность организации путем предотвращения, обнаружения, анализа и реагирования на инциденты кибербезопасности.

SOC выступает в роли центрального командного пункта, в который стекаются события со всей ИТ-инфраструктуры.

MITRE ATT@CK (1)

1. Reconnaissance – сбор информации о цели снаружи
2. Resource Development – подготовка ресурсов для нападения
3. Initial Access – первоначальный доступ
4. Execution – попытка запуска вредоносного ПО
5. Persistence – организация постоянного доступа к целевой инфраструктуре
6. Privilege Escalation – повышение уровня доступа
7. Defense Evasion – обход средств защиты информации

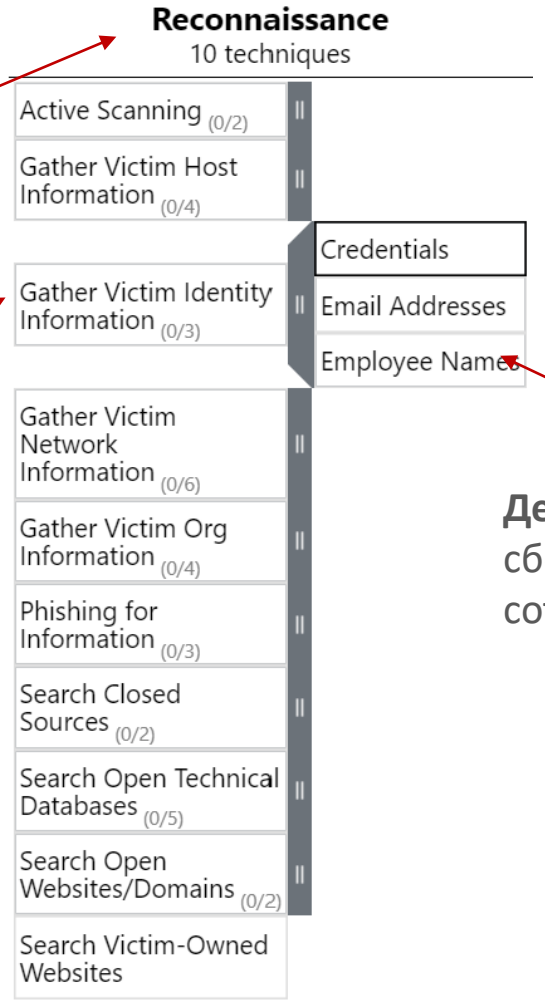


MITRE ATT@CK (2)

8. Credential Access – получение доступа с помощью действующих учетных записей
9. Discovery – сбор информации о цели изнутри
10. Lateral Movement – перемещение внутри целевой ИТ-инфраструктуры
11. Collection – сбор интересующих данных
12. Command and Control – организация внешнего управления
13. Exfiltration – передача интересующих данных вовне
14. Impact – разрушающее воздействие на ИТ-инфраструктуру

Задача: разведка

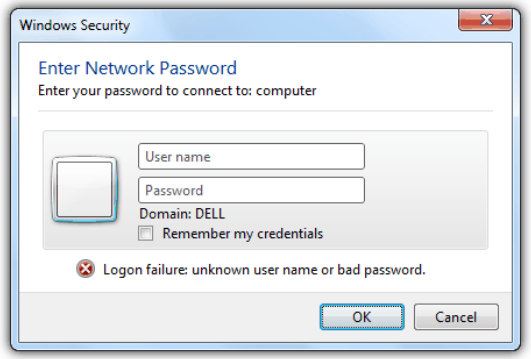
Набор действий: сбор данных, идентифицирующих цель



Действие: сбор имен сотрудников

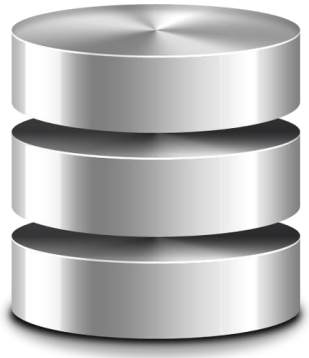
Как своевременно обнаруживать таргетированные атаки?

Необходимо отслеживать признаки нарушения ИБ



Авторизация: как успешная, так и неуспешная

Срабатывания антивирусного ПО, СОВ



Подозрительные запросы к СУБД

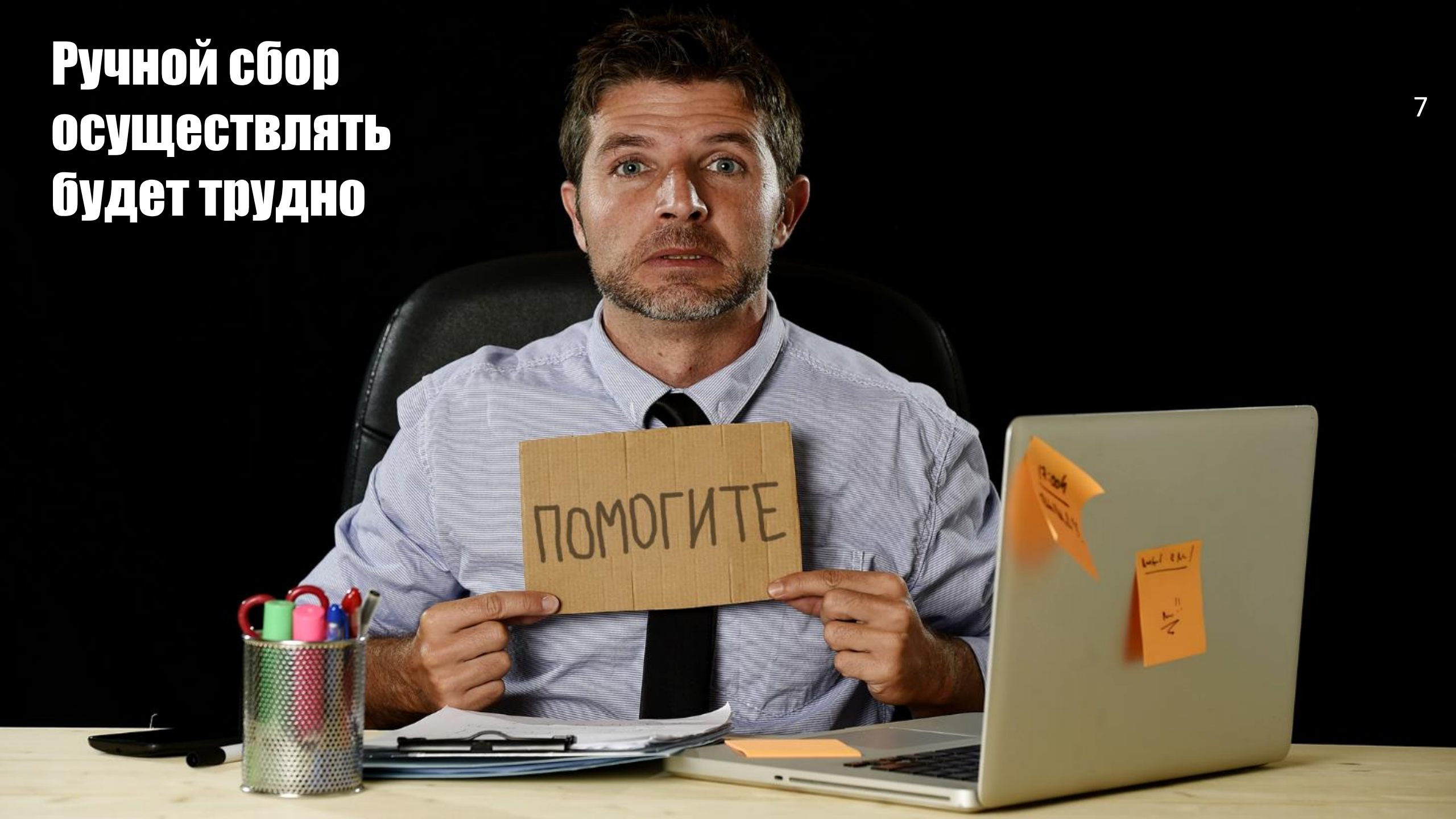
Нетипичное поведение пользователя

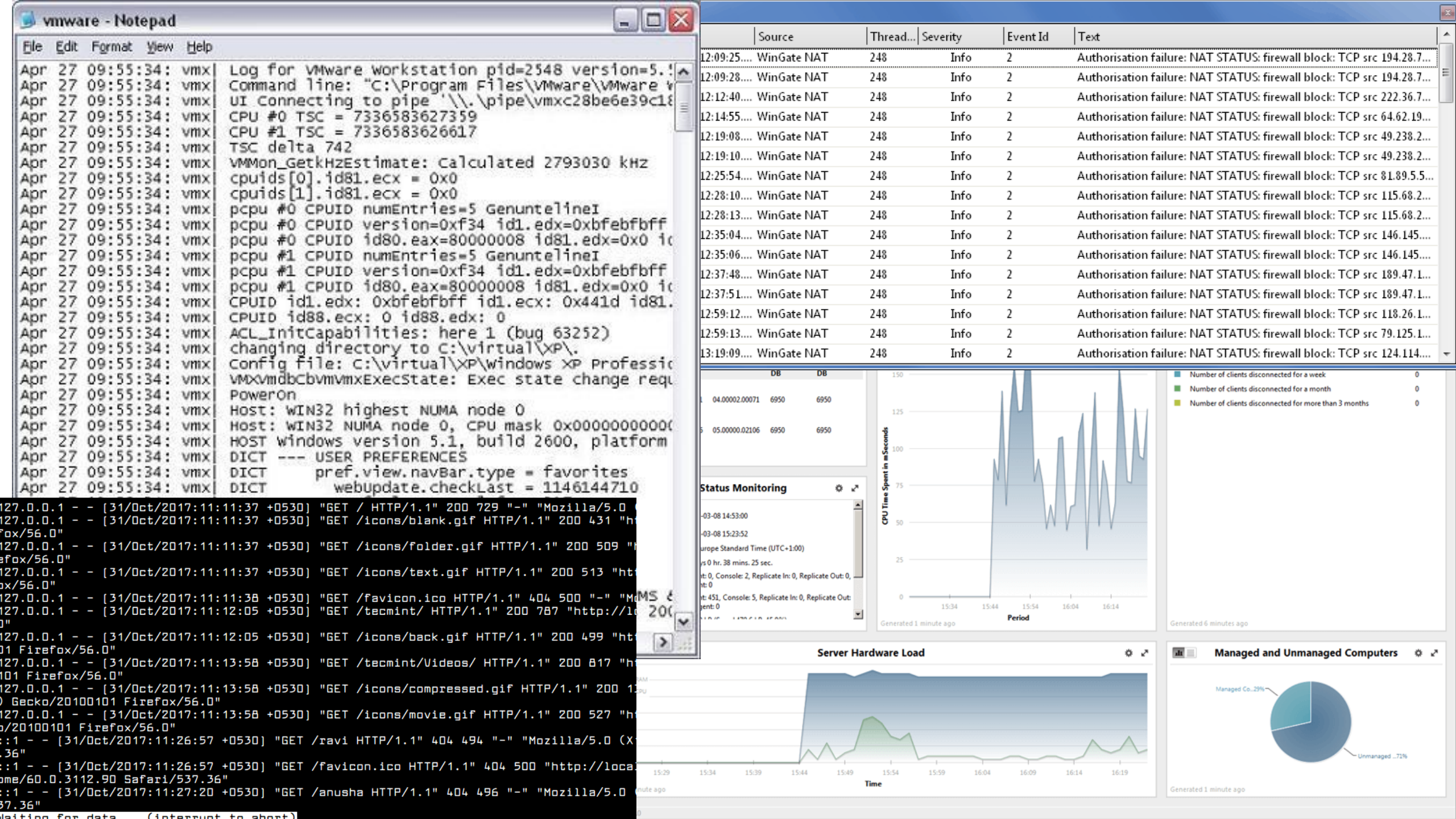
Для этого надо осуществлять мониторинг критичных сегментов инфраструктуры

Соответствующее требование включено в:

Приказ ФСТЭК России N 17
Приказ ФСТЭК России N 21
Приказ ФСТЭК России N 31
Приказ ФСТЭК России N 239

Ручной сбор осуществлять будет трудно




vmware - Notepad
File Edit Format View Help
Apr 27 09:55:34: vmx| Log for VMware Workstation pid=2548 version=5.
Apr 27 09:55:34: vmx| Command line: "C:\Program Files\VMware\VMware
Apr 27 09:55:34: vmx| UI Connecting to pipe '\\.\pipe\vmxc28be6e39c1
Apr 27 09:55:34: vmx| CPU #0 TSC = 7336583627359
Apr 27 09:55:34: vmx| CPU #1 TSC = 7336583626617
Apr 27 09:55:34: vmx| TSC delta 742
Apr 27 09:55:34: vmx| VMMon_GetkHzEstimate: Calculated 2793030 kHz
Apr 27 09:55:34: vmx| cpuids[0].id81.ecx = 0x0
Apr 27 09:55:34: vmx| cpuids[1].id81.ecx = 0x0
Apr 27 09:55:34: vmx| pcpu #0 CPUID numEntries=5 GenuntelineI
Apr 27 09:55:34: vmx| pcpu #0 CPUID version=0xf34 id1.edx=0xbfebfbff
Apr 27 09:55:34: vmx| pcpu #0 CPUID id80.eax=80000008 id81.edx=0x0 ic
Apr 27 09:55:34: vmx| pcpu #1 CPUID numEntries=5 GenuntelineI
Apr 27 09:55:34: vmx| pcpu #1 CPUID version=0xf34 id1.edx=0xbfebfbff
Apr 27 09:55:34: vmx| pcpu #1 CPUID id80.eax=80000008 id81.edx=0x0 ic
Apr 27 09:55:34: vmx| CPUID id1.edx: 0xbfebfbff id1.ecx: 0x441d id81.
Apr 27 09:55:34: vmx| CPUID id88.ecx: 0 id88.edx: 0
Apr 27 09:55:34: vmx| ACL_InitCapabilities: here 1 (bug 63252)
Apr 27 09:55:34: vmx| changing directory to C:\virtual\XP\.
Apr 27 09:55:34: vmx| Config file: C:\virtual\XP\Windows XP Professic
Apr 27 09:55:34: vmx| VMXVmdbCbVmVmxExecState: Exec state change requ
Apr 27 09:55:34: vmx| PowerOn
Apr 27 09:55:34: vmx| Host: WIN32 highest NUMA node 0
Apr 27 09:55:34: vmx| Host: WIN32 NUMA node 0, CPU mask 0x00000000000
Apr 27 09:55:34: vmx| HOST Windows version 5.1, build 2600, platform
Apr 27 09:55:34: vmx| DICT --- USER PREFERENCES
Apr 27 09:55:34: vmx| DICT pref.view.navBar.type = favorites
Apr 27 09:55:34: vmx| DICT webupdate.checkLast = 1146144710
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET / HTTP/1.1" 200 729 "-" "Mozilla/5.0
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/blank.gif HTTP/1.1" 200 431 "h
fox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/folder.gif HTTP/1.1" 200 509 "
efox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/text.gif HTTP/1.1" 200 513 "ht
ox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:38 +0530] "GET /favicon.ico HTTP/1.1" 404 500 "-" "M
127.0.0.1 - - [31/Oct/2017:11:12:05 +0530] "GET /tecmint/ HTTP/1.1" 200 787 "http://l
0"
127.0.0.1 - - [31/Oct/2017:11:12:05 +0530] "GET /icons/back.gif HTTP/1.1" 200 499 "ht
01 Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:13:58 +0530] "GET /tecmint/Videos/ HTTP/1.1" 200 817 "h
101 Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:13:58 +0530] "GET /icons/compressed.gif HTTP/1.1" 200 1
) Gecko/20100101 Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:13:58 +0530] "GET /icons/movie.gif HTTP/1.1" 200 527 "h
0/20100101 Firefox/56.0"
::1 - - [31/Oct/2017:11:26:57 +0530] "GET /ravi HTTP/1.1" 404 494 "-" "Mozilla/5.0 (X
.36"
::1 - - [31/Oct/2017:11:26:57 +0530] "GET /favicon.ico HTTP/1.1" 404 500 "http://loca
ome/60.0.3112.90 Safari/537.36"
::1 - - [31/Oct/2017:11:27:20 +0530] "GET /anusha HTTP/1.1" 404 496 "-" "Mozilla/5.0
37.36"
Waiting for data... (interrupt to abort)
Source
Thread...
Severity
Event Id
Text
12:09:25.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 194.28.7...
12:09:28.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 194.28.7...
12:12:40.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 222.36.7...
12:14:55.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 64.62.19...
12:19:08.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 49.238.2...
12:19:10.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 49.238.2...
12:25:54.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 81.89.5.5...
12:28:10.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 115.68.2...
12:28:13.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 115.68.2...
12:35:04.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 146.145....
12:35:06.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 146.145....
12:37:48.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 189.47.1...
12:37:51.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 189.47.1...
12:59:12.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 118.26.1...
12:59:13.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 79.125.1...
13:19:09.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 124.114....
DB DB
04.00002.00071 6950 6950
05.00000.02106 6950 6950
Status Monitoring
-03-08 14:53:00
-03-08 15:23:52
urope Standard Time (UTC+1:00)
ys 0 hr. 38 mins. 25 sec.
nt: 0, Console: 2, Replicate In: 0, Replicate Out: 0,
nt: 0
nt: 451, Console: 5, Replicate In: 0, Replicate Out:
gent: 0
CPU Time Spent in mSeconds
150
125
100
75
50
25
0
15:34
15:44
15:54
16:04
16:14
Period
Generated 1 minute ago
Number of clients disconnected for a week 0
Number of clients disconnected for a month 0
Number of clients disconnected for more than 3 months 0
Generated 6 minutes ago
Server Hardware Load
15:29
15:34
15:39
15:44
15:49
15:54
15:59
16:04
16:09
16:14
16:19
Time
Managed and Unmanaged Computers
Managed Co...29%
Unmanaged ...71%
Generated 1 minute ago

Решение: применение SIEM-системы

KOMRAD Enterprise SIEM 4.0

Гибкая и производительная система централизованного управления событиями информационной безопасности, совместимая с отечественными средствами защиты информации.

Принцип работы SIEM-системы

LOG

LOG

LOG

LOG

LOG

Нормализация

Фильтрация

Корреляция

Реакция

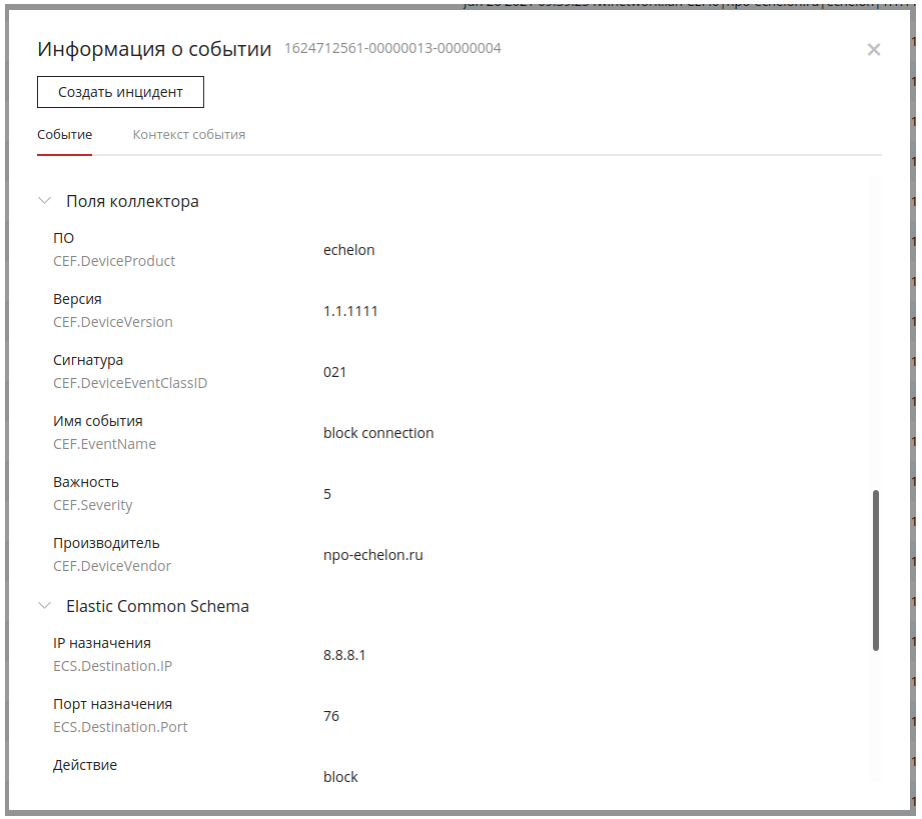
Уведомление

Нормализация (разбор) событий

Сырое событие:

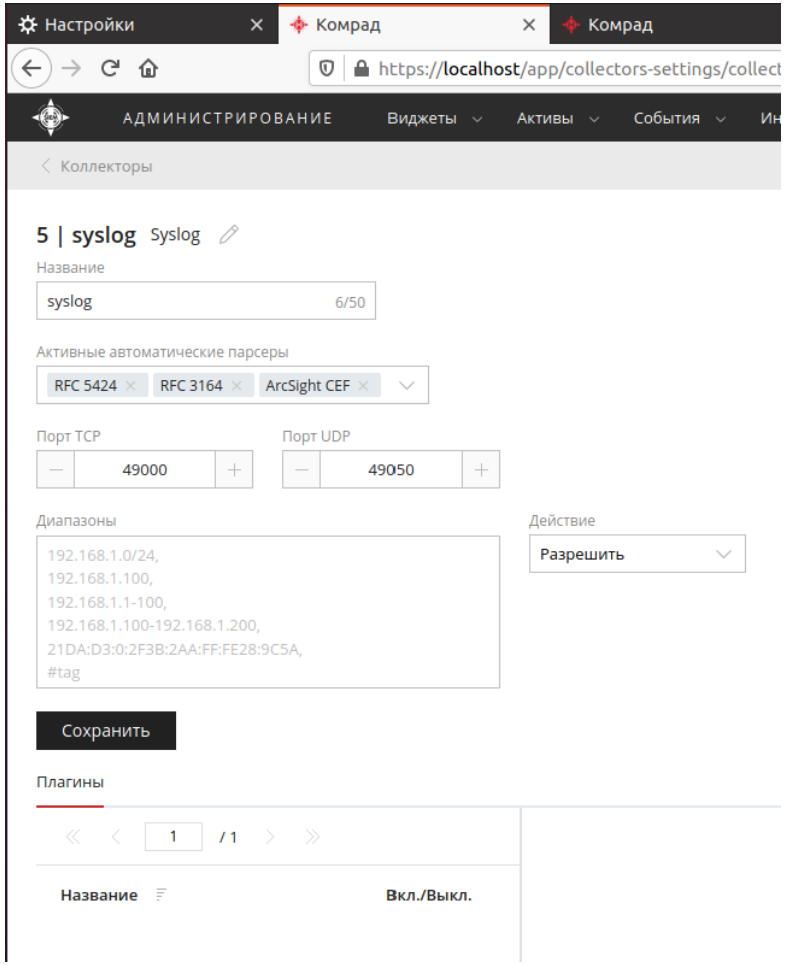
Jun 26 2021 09:02:35 fw.network.lan CEF:0
npo-echelon.ru|echelon|
1.1.1111|021|block connection|5|
src=8.8.8.10 spt=56117 dst=8.8.8.1 dpt=76
act=block

Разобранное событие:



Поддерживаемые стандарты и технологии разбора событий

- Поддержка стандартов:
  - RFC 5424
  - RFC 3164
  - ArcSight CEF
- Поддержка возможности разработки плагинов с помощью регулярных выражений (реализован стандат RE2)
- Поддержка стандарта структурирования события: Elastic Common Schema

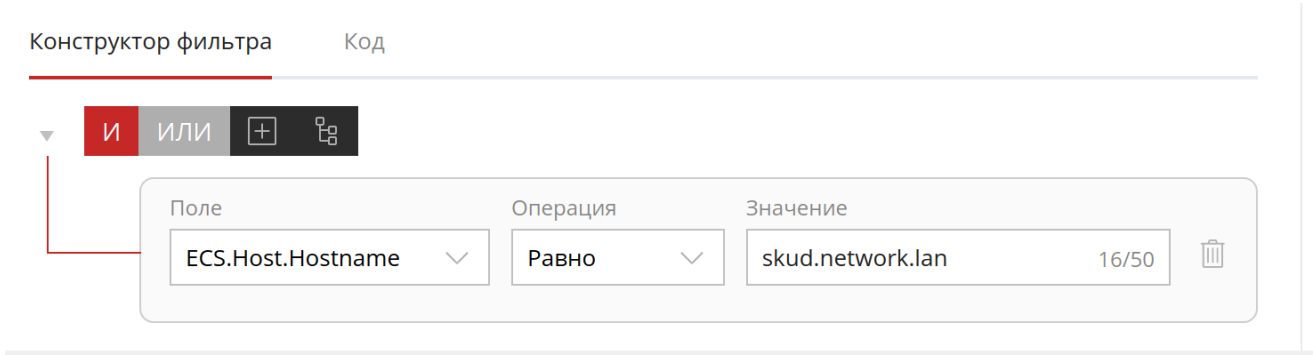


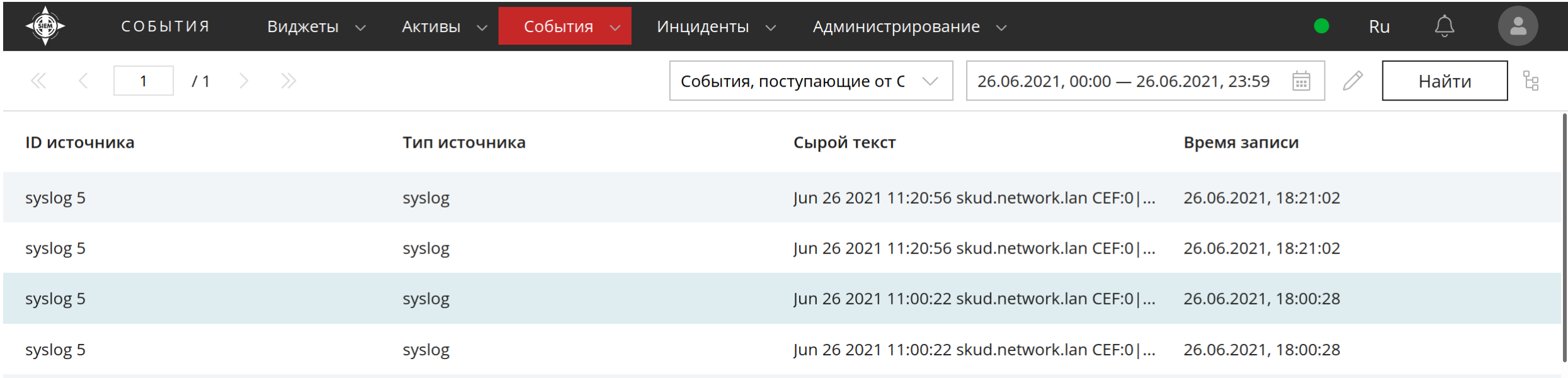
Хранение событий

- Подсистема сохраняет нормализованные события в СУБД ClickHouse, также возможна интеграция с PostgreSQL с расширением TimescaleDB для работы с временными рядами.

ClickHouse
не тормозит

Фильтры событий

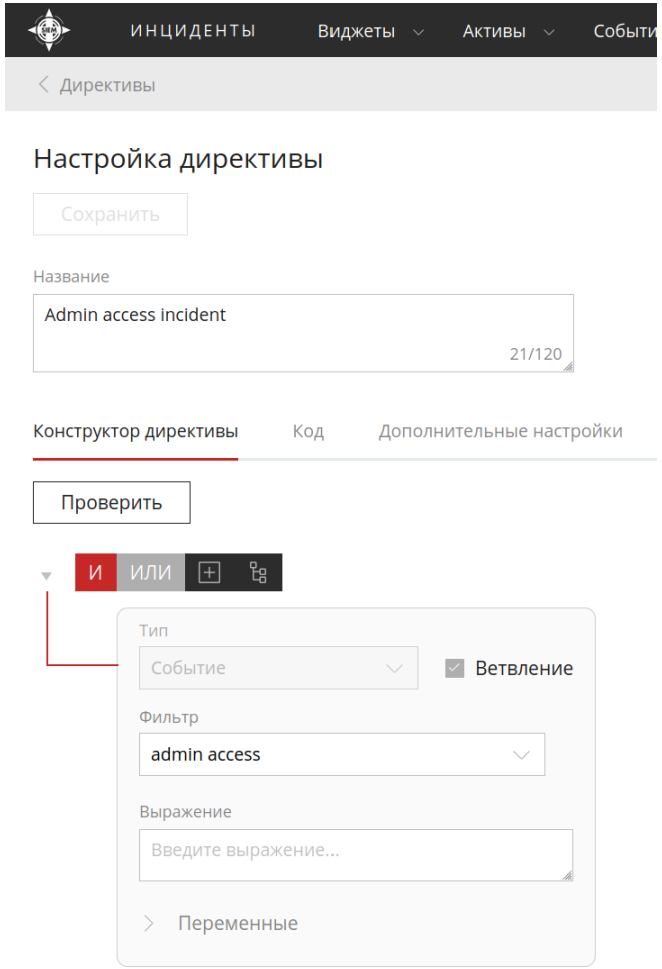




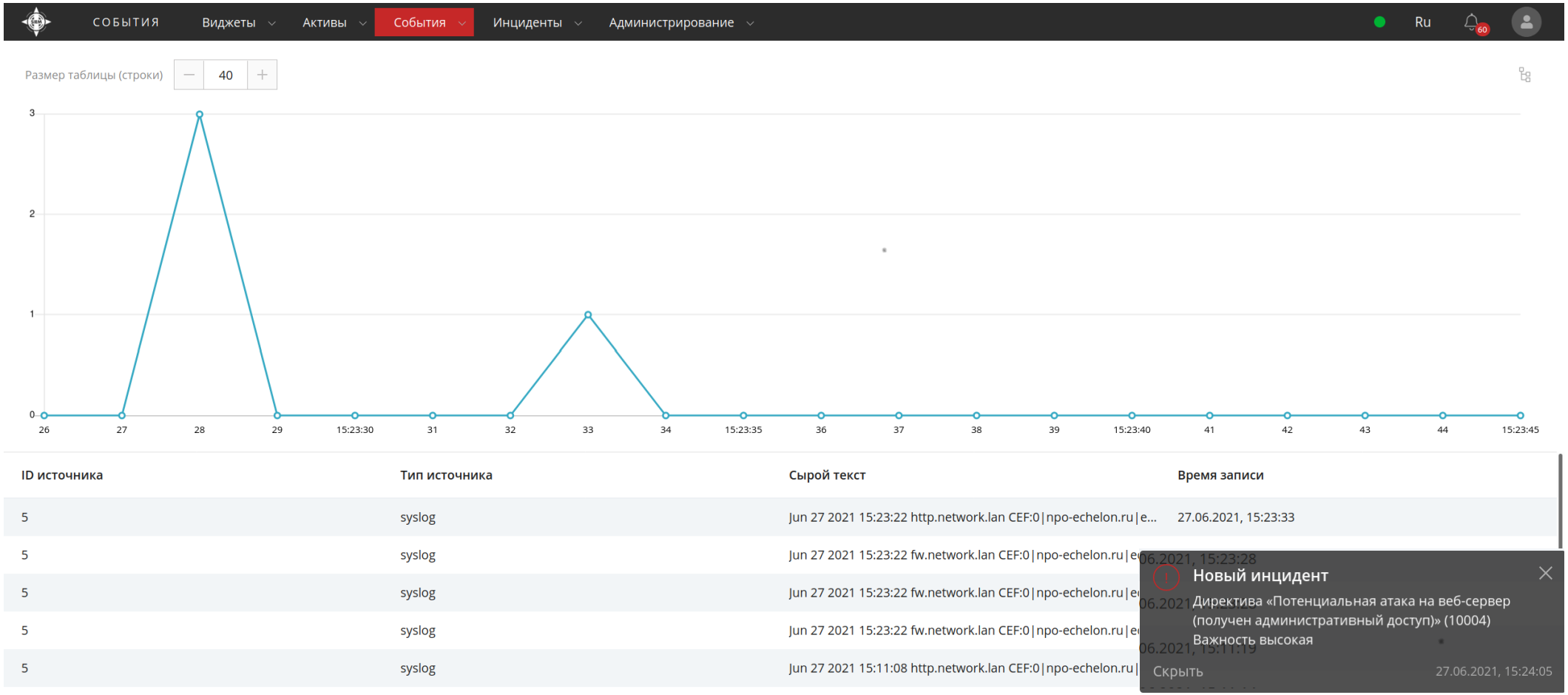
ID источника	Тип источника	Сырой текст	Время записи
syslog 5	syslog	Jun 26 2021 11:20:56 skud.network.lan CEF:0|...	26.06.2021, 18:21:02
syslog 5	syslog	Jun 26 2021 11:20:56 skud.network.lan CEF:0|...	26.06.2021, 18:21:02
syslog 5	syslog	Jun 26 2021 11:00:22 skud.network.lan CEF:0|...	26.06.2021, 18:00:28
syslog 5	syslog	Jun 26 2021 11:00:22 skud.network.lan CEF:0|...	26.06.2021, 18:00:28

Директивы корреляции

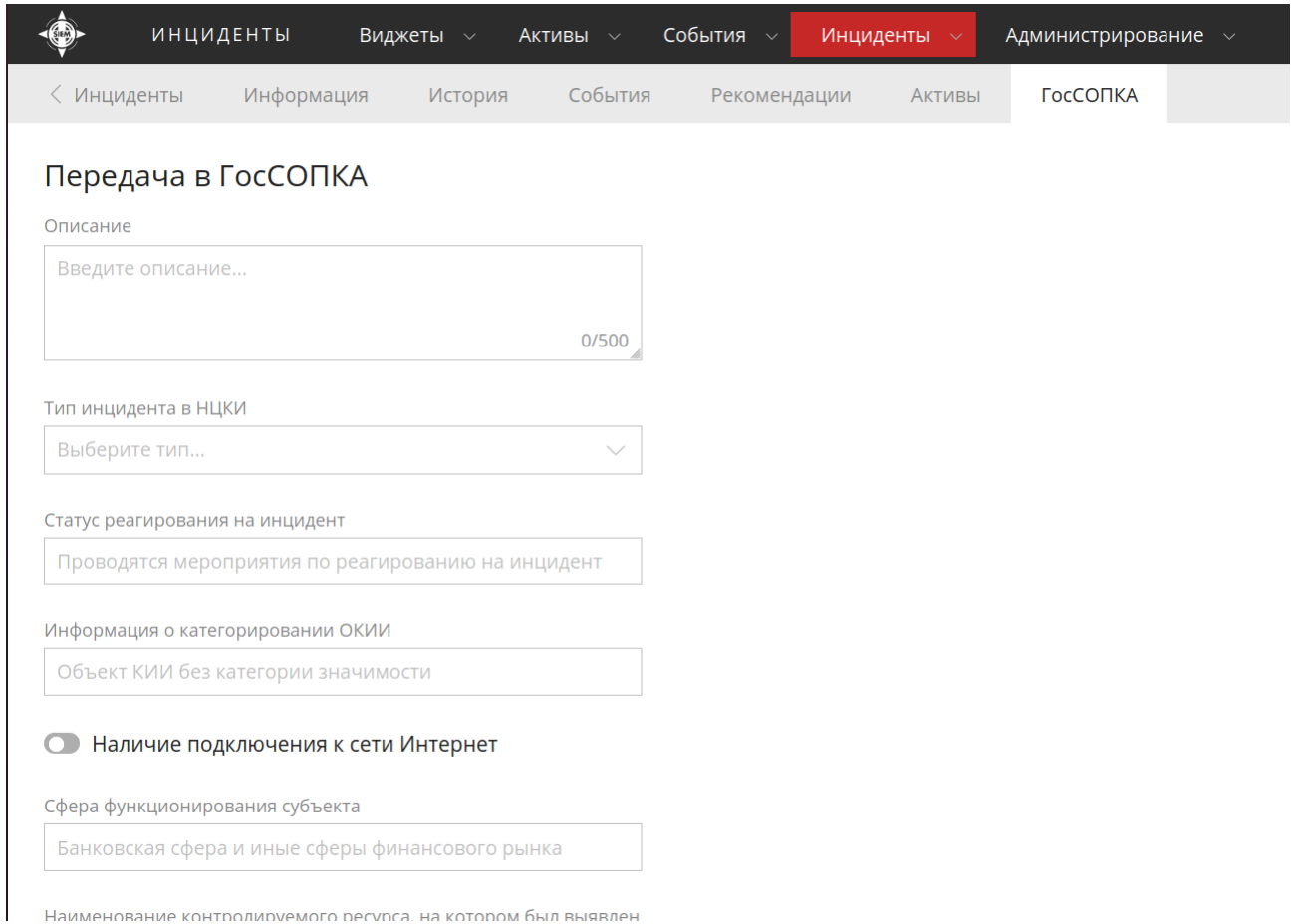
- Простой вариант: ссылка на директиву
- Продвинутый:
  - Определение последовательности событий с временными окнами
  - Работа с переменными
  - Проверка отсутствия события



Уведомление: в интерфейсе и по SMTP

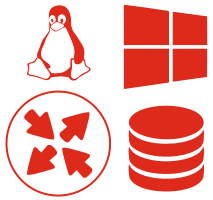


Инцидент может быть передан в ГОССОПКА автоматически или в ручном режиме



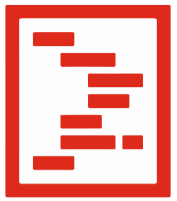
Отличительные особенности

Высокая производительность



Широкий спектр поддерживаемых источников событий «из коробки»

Возможность подключения любого источника событий



Гибкость при создании фильтров и директив корреляции

Оперативное оповещение об инциденте

Возможность автоматического реагирования на инциденты

ГОССОПКА

Обнаружение. Предупреждение. Ликвидация.

Возможность передачи инцидентов в систему ГОССОПКА

ASTRA LINUX

Дистрибутив под Astra Linux

KOMRAD Enterprise SIEM предъявляет минимальные требования к аппаратному обеспечению

- ОЗУ: 4 GB
- CPU: 2 ядра
- SSD: 100 GB

Полезные ссылки

- getkomrad@npo-echelon.ru – email для получения демо-лицензии KOMRAD Enterprise SIEM;
- https://t.me/komrad4 - чат пользователей продукта
- https://www.youtube.com/channel/UCIwZEG8EcL7tnZN4Qzjt13w

канал учебного центра «Эшелон» с обучающими видео


Эшелон
комплексная безопасность