{KOMRAD}
Enterprise SIEM

Эшелон
комплексная безопасность

Технологии SOC и роль SIEM
KOMRAD Enterprise SIEM

Каменский Станислав
Специалист группы внедрения СЗИ

Оставайтесь на связи

Группа пользователей KOMRAD 4

- Ссылки на дистрибутивы и документацию
- Оперативная помощь по применению продукта
- https://t.me/komrad4

Новостной telegram-канал Echelon Eyes

- Материалы вебинара: презентации, видео
- Новости об уязвимостях, инцидентах, эксплойтах, изменениях в нормативной базе
- https://t.me/EchelonEyes

{KOMRAD}
Enterprise SIEM

Эшелон
комплексная безопасность

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.

Основные функции центра мониторинга

- инвентаризация информационных ресурсов;
- выявление уязвимостей информационных систем;
- анализ угроз информационной безопасности;
- повышение квалификации персонала информационных ресурсов;
- прием сообщений о возможных инцидентах от персонала и пользователей
- информационных ресурсов;
- обнаружение компьютерных атак;
- анализ данных о событиях безопасности;
- регистрация инцидентов;
- реагирование на инциденты и ликвидация их последствий;
- установление причин инцидентов;
- анализ результатов устранения последствий инцидентов.

Центр мониторинга информационной безопасности

- Люди
- Процессы
- Технологии

Люди

- Аналитик информационной безопасности
- Архитектор информационной безопасности
- Руководитель центра мониторинга
- Руководитель службы информационной безопасности (CISO)

Аналитики информационной безопасности

- Аналитик 1-й линии — анализирует последние оповещения о событиях информационной безопасности для определения их срочности и актуальности. Создает карточки инцидента, требующие участия аналитика информационной безопасности 2-й линии. Проводит анализ защищенности, анализирует получаемые отчеты. Конфигурирует инструменты мониторинга безопасности (СОВ, SIEM и т.п.)
- Аналитик 2-й линии — анализирует карточки инцидентов, созданные аналитиками 1-й линии. Использует данные об угрозах (индикаторы компрометации, правила, сигнатуры) для идентификации скомпрометированных систем и определения границ атаки. Собирает и анализирует данные активов (настройки систем, запущенные процессы, и др.) для дальнейшего расследования.

Аналитики информационной безопасности

- Аналитик 3-й линии — анализирует критические инциденты. Проводит тестирование на проникновение и оценку защищенности инфраструктуры. Проводит ревью срабатываний систем мониторинга, осуществляет анализ угроз.
- Менеджер по реагированию на инцидент — управляет действиями во время анализа и ограничения последствий инцидента. Отвечает за коммуникацию специальных требований относительно критичных инцидентов.

Архитектор информационной безопасности

- Архитектор информационной безопасности поддерживает и предлагает инструменты мониторинга и анализа. Создает инфраструктуру информационной безопасности в организации.
- Принимает активное участие в ходе разработки и внедрения информационных систем в части формирования и контроля выполнения требований по информационной безопасности. Документирует процедуры, требования и протоколы.

Руководитель центра мониторинга

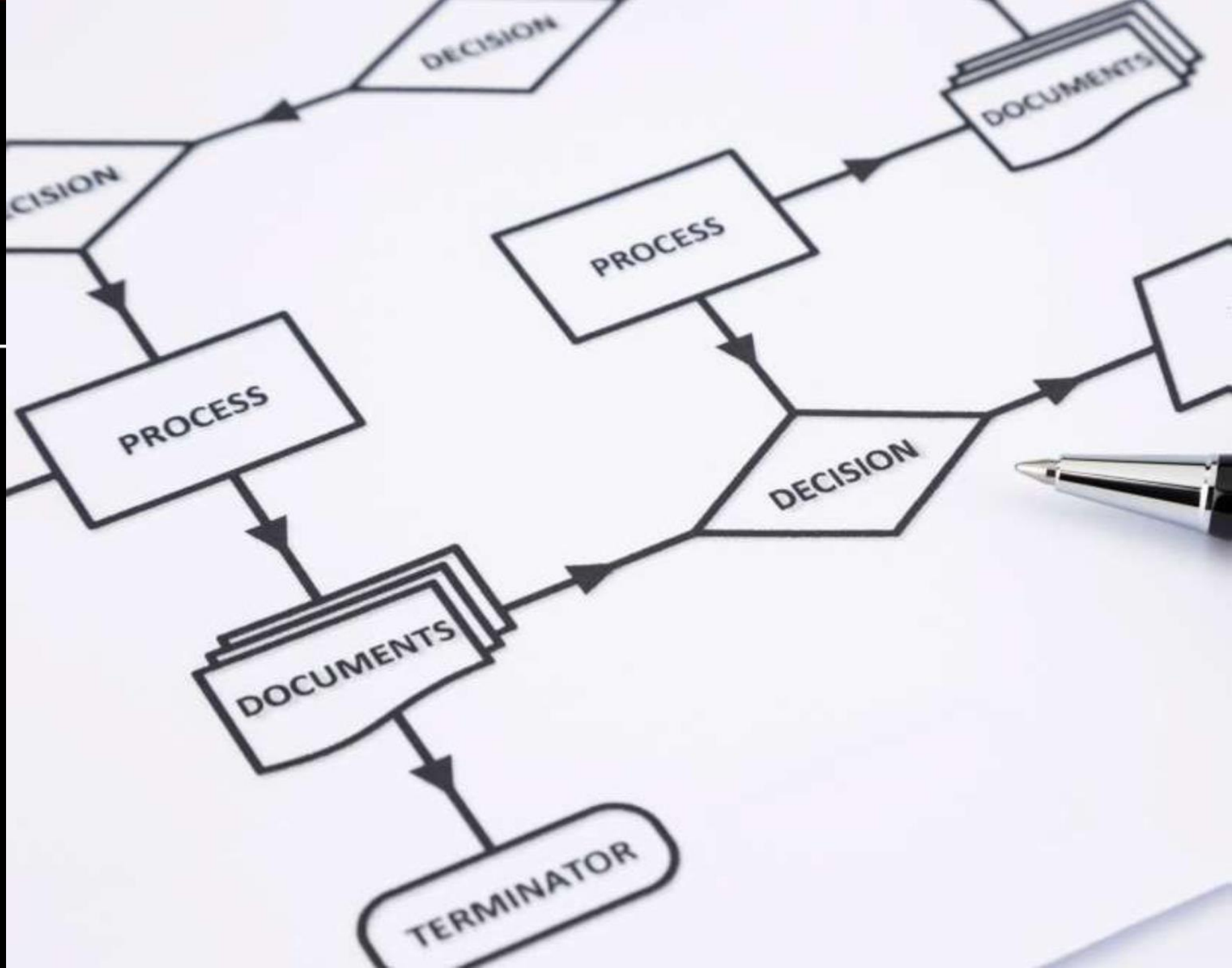
- Руководитель центра мониторинга управляет действиями команды центра мониторинга и отчитывается перед руководителем службы информационной безопасности.
- Обеспечивает техническое руководство, а также управляет финансовым бюджетом. Отвечает за подбор, обучение и оценку персонала центра мониторинга. Внедряет процессы, проводит оценку отчетов по инцидентам, разрабатывает и исполняет планы по кризисным коммуникациям. Поддерживает процесс аудита, отслеживает результативность центра мониторинга.

Руководитель службы информационной безопасности

- Руководитель службы информационной безопасности (CISO) является руководителем высшего звена в организации отвечает за создание и поддержание корпоративного видения, стратегии и программы для обеспечения информационной безопасности информационных активов.

Процессы

- Мониторинг
- Реагирование на инциденты
- Анализ угроз



Мониторинг

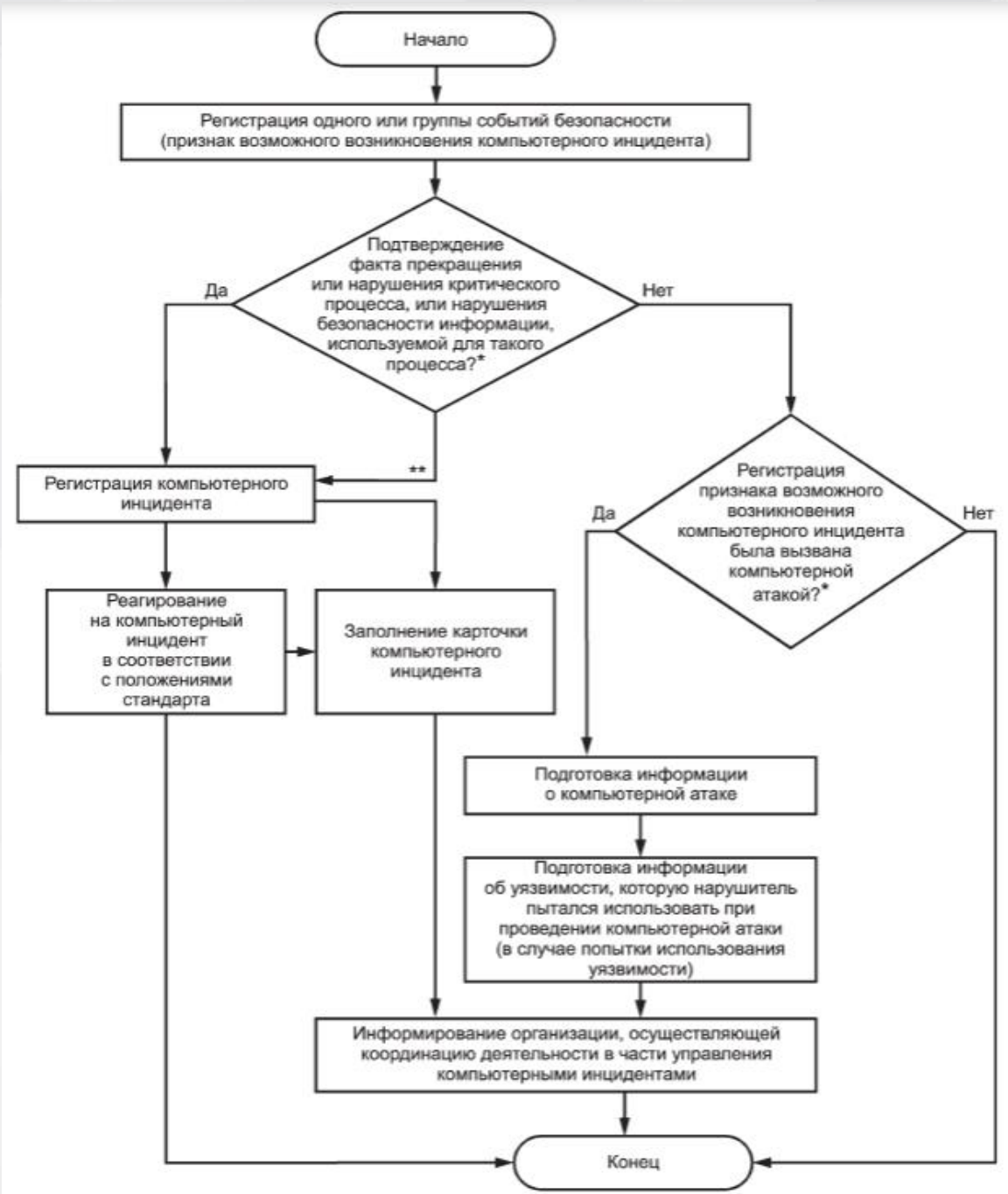
- Идентификация источников
- Сбор
- Корреляция
- Агрегация
- Хранение
- Контроль защищенности

Основные понятия

- Событие (информационной) безопасности: зафиксированное состояние информационной (автоматизированной) системы, сетевого, телекоммуникационного, коммуникационного, иного прикладного сервиса или информационно телекоммуникационной сети, указывающее на возможное нарушение безопасности информации, сбой средств ЗИ, или ситуацию, которая может быть значимой для безопасности информации. **ГОСТ Р 59709—2022**
- Корреляция событий ИБ — взаимосвязь двух или более событий безопасности.
- Нормализация событий безопасности — приведение сообщений о событиях безопасности к единому формату.

Новые ГОСТы

- ГОСТ Р 59709 — 2022 Защита информации. Управление компьютерными инцидентами. Термины и определения
- ГОСТ Р 59710 — 2022 Защита информации. Управление компьютерными инцидентами. Общие положения
- ГОСТ Р 59711 — 2022 Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами
- ГОСТ Р 59712 — 2022 Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты



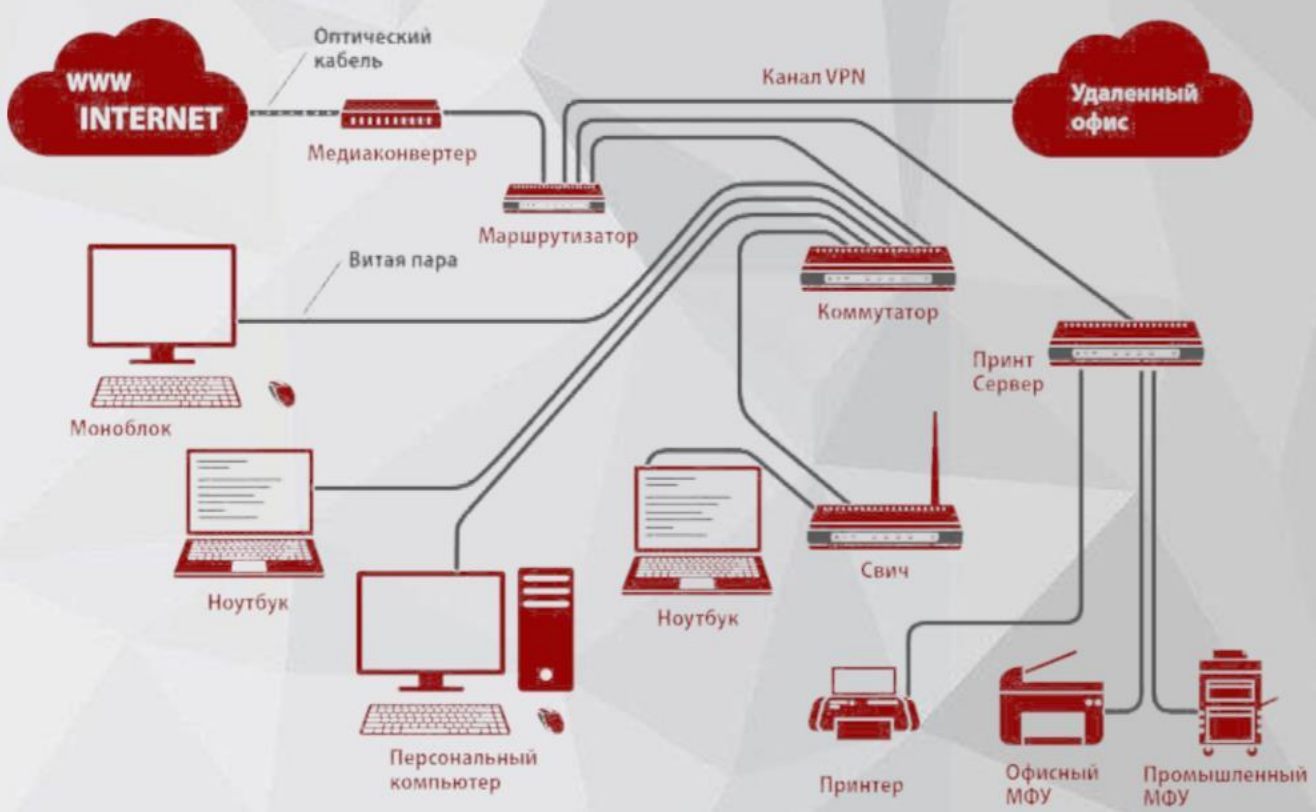
* Проверка факта возникновения компьютерного инцидента.

** Отсутствие факта возникновения компьютерного инцидента не может быть однозначно подтверждено.

Рисунок 1 — Общий подход к обнаружению и регистрации компьютерных инцидентов, реагированию на них и информированию организации, осуществляющей координацию деятельности в части управления компьютерными инцидентами

Какие источники необходимо подключать

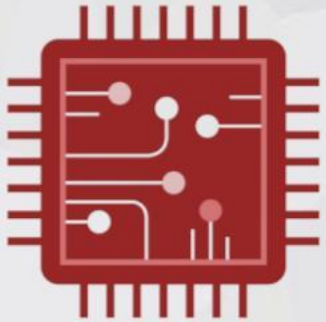
- Межсетевые экраны, системы обнаружения и предотвращения вторжений
- Контроллер домена
- Сканеры уязвимостей
- Антивирусные средства
- Серверы
- Рабочие станции



СБОР ВСЕЙ ИНФРАСТРУКТУРЫ

Syslog (сетевое оборудование, ОС Linux, информационные системы)

WMI (ОС Windows и Windows-приложения)



Коллекторы

FTP (приложения с локальным журналом в виде файла)

SNMP (сетевое оборудование)

SSH (приложения с локальным журналом в виде файла)

SQL (СУБД и системы, ведущие журналы в СУБД)

xFlow (сетевое оборудование)

Корреляция событий

Хранение

7. При осуществлении автоматического анализа событий ИБ и выявления компьютерных инцидентов средства обнаружения должны обеспечивать:

- хранение агрегированных событий ИБ не менее шести месяцев.

Приказ № 196 ФСБ России от 06.05.2019

Контроль защищенности

Реагирование на инциденты

Управление инцидентами

- Фиксация состояния и анализ объектов информационных ресурсов, вовлеченных в инцидент.
- Координация деятельности по прекращению воздействия компьютерных атак, проведение которых вызвало возникновение инцидента.
- Фиксация и анализ сетевого трафика, циркулирующего в информационном ресурсе, вовлеченном в инцидент.
- Определение причин инцидента и возможных его последствий для информационного ресурса.
- Локализация инцидента.
- Сбор сведений для последующего установления причин инцидента.
- Планирование мер по ликвидации последствий инцидента.
- Ликвидация последствий инцидента.
- Контроль ликвидации последствий.
- Формирование рекомендаций для совершенствования.

Методические рекомендации по созданию ведомственных и корпоративных центров ГОССОПКА

Основные руководства по управлению инцидентами

- Методические рекомендации по созданию ведомственных и корпоративных центров ГОССОПКА
- ISO 27035, “ Information Security Incident Management”
- NIST SP 800-61, “ Computer Security Incident Handling Guide”
- ENISA, “ CSIRT Setting Up Guide”
- ISACA, “ Incident Management and Response”

Анализ угроз

Основные понятия

- Анализ угроз — процесс определения возможных способов реализации угроз безопасности информации, включая определение возможных способов проведения компьютерных атак на информационную систему с учетом особенностей реализованных в ней информационных технологий, а также состава ее технических средств и программного обеспечения.

Три уровня данных об угрозах

- Операционный или технический уровень: индикаторы компрометации, т.е. признаки, по которым можно распознать потенциальную угрозу (например, хэши вредоносных файлов, IP-адреса, домены, связанные с киберпреступниками).
- Тактический уровень: техника, тактика и процедуры злоумышленников (TTP), понимание того, кто может выступить источником киберугроз для конкретной организации.
- Стратегический уровень. аналитические данные о тенденциях угроз в мире с целью выработки дальнейшей стратегии развития системы информационной безопасности организации. Опираясь на информацию из предыдущих уровней, осуществляется представление актуальных угроз и необходимых мер перед топ- менеджментом организации, планирование задач и потребностей (в новых людях, процессах, инструментах).

Реализация процесса в SOC

- Сбор данных из разных источников. Это могут быть любые источники об угрозах, поступающие в SOC: внешние данные от провайдеров, открытые источники, от партнеров, регуляторов (к примеру, ФинЦЕРТ), данные средств защиты информации.
- Обработка собранных данных предполагает их нормализацию и стандартизацию для того, чтобы все они были приведены к единому формату, к единой карточке.
- Обогащение дополнительным контекстом, если данных недостаточно. Для обогащения данных существуют универсальные сервисы (например, VirusTotal, whois и другие) и узкоспециализированные источники.
- Распространение индикаторов и правил на средства защиты и мониторинга.

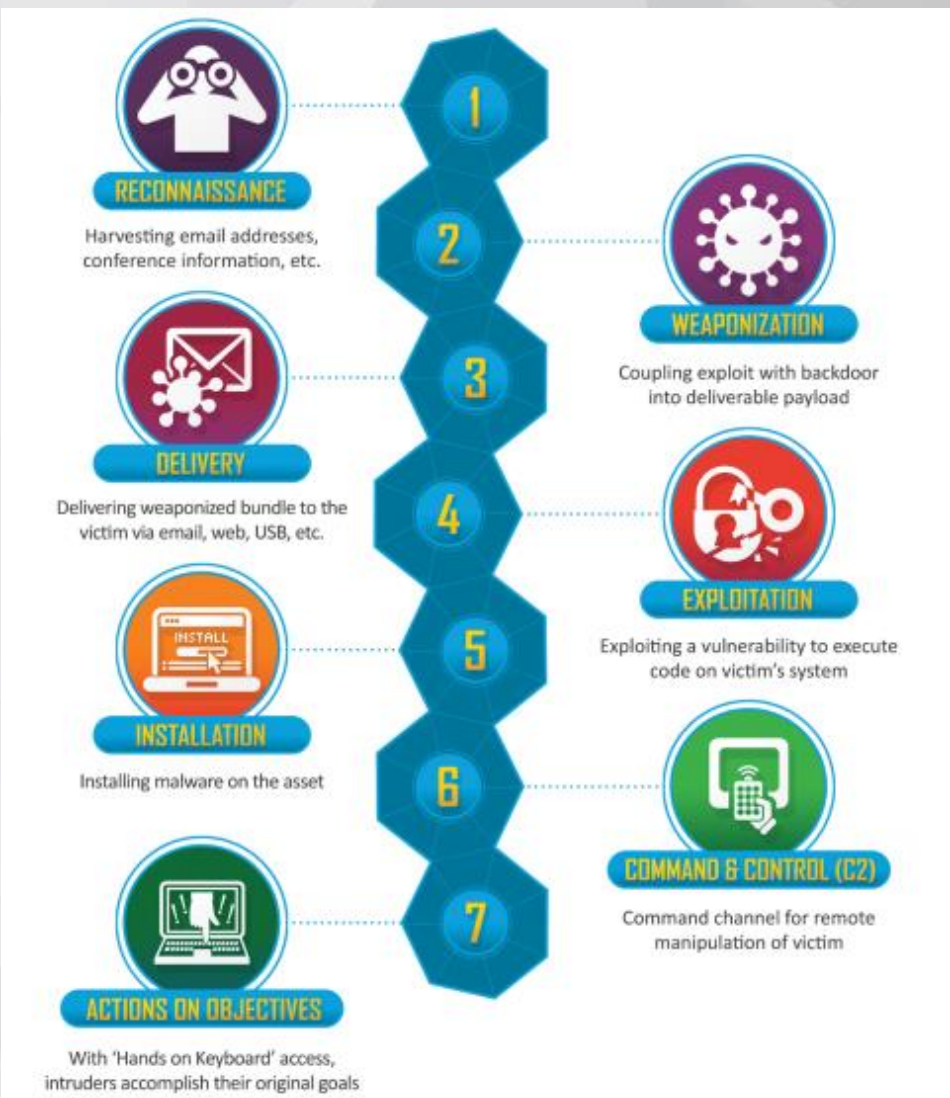
Технологии

- SIEM
- VA
- IDS

Современная таргетированная атака

Cyber Kill Chain от Lockheed Martin

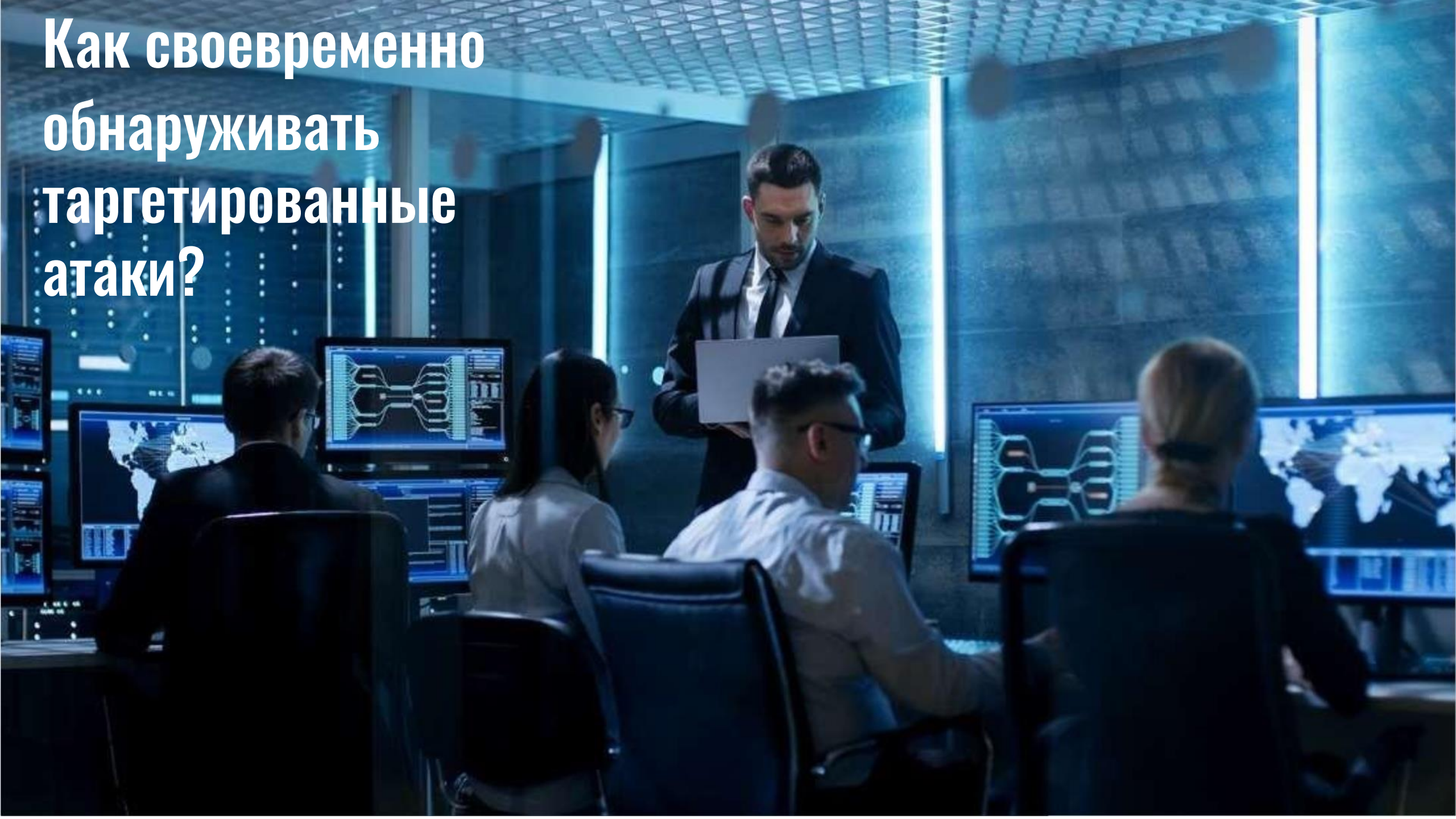
- Разведка
- Выбор средств нападения
- Доставка
- Эксплуатация
- Установка вредоносного ПО
- Организация управления
- Реализация поставленных задач



MITRE ATT&CK

1. Разведка
2. Получение полезных ресурсов
3. Первоначальный доступ
4. Атака
5. Закрепление
6. Эскалация привилегий
7. Обход средств защиты
8. Доступ с учетными записями
9. Внутренняя разведка
10. Перемещение внутри инфраструктуры
11. Сбор данных
12. Управление и контроль
13. Передача данных вовне
14. Деструктивное воздействие

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

{KOMRAD}
Enterprise SIEM

Эшелон
комплексная безопасность

vmware - Notepad

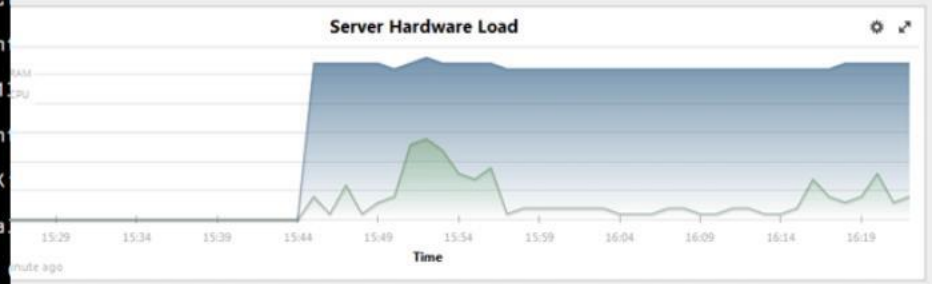
File Edit Format View Help

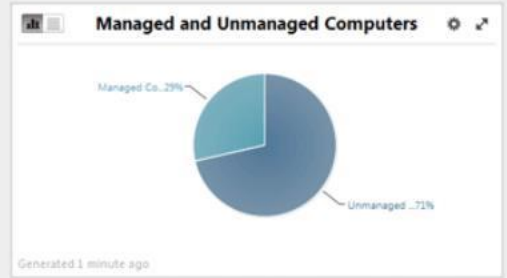
```
Apr 27 09:55:34: vmx| Log for VMware Workstation pid=2548 version=5.
Apr 27 09:55:34: vmx| Command line: "C:\Program Files\VMware\VMware
Apr 27 09:55:34: vmx| UI Connecting to pipe '\\.\pipe\vmxc28be6e39c1
Apr 27 09:55:34: vmx| CPU #0 TSC = 7336583627359
Apr 27 09:55:34: vmx| CPU #1 TSC = 7336583626617
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
```

```
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"
```

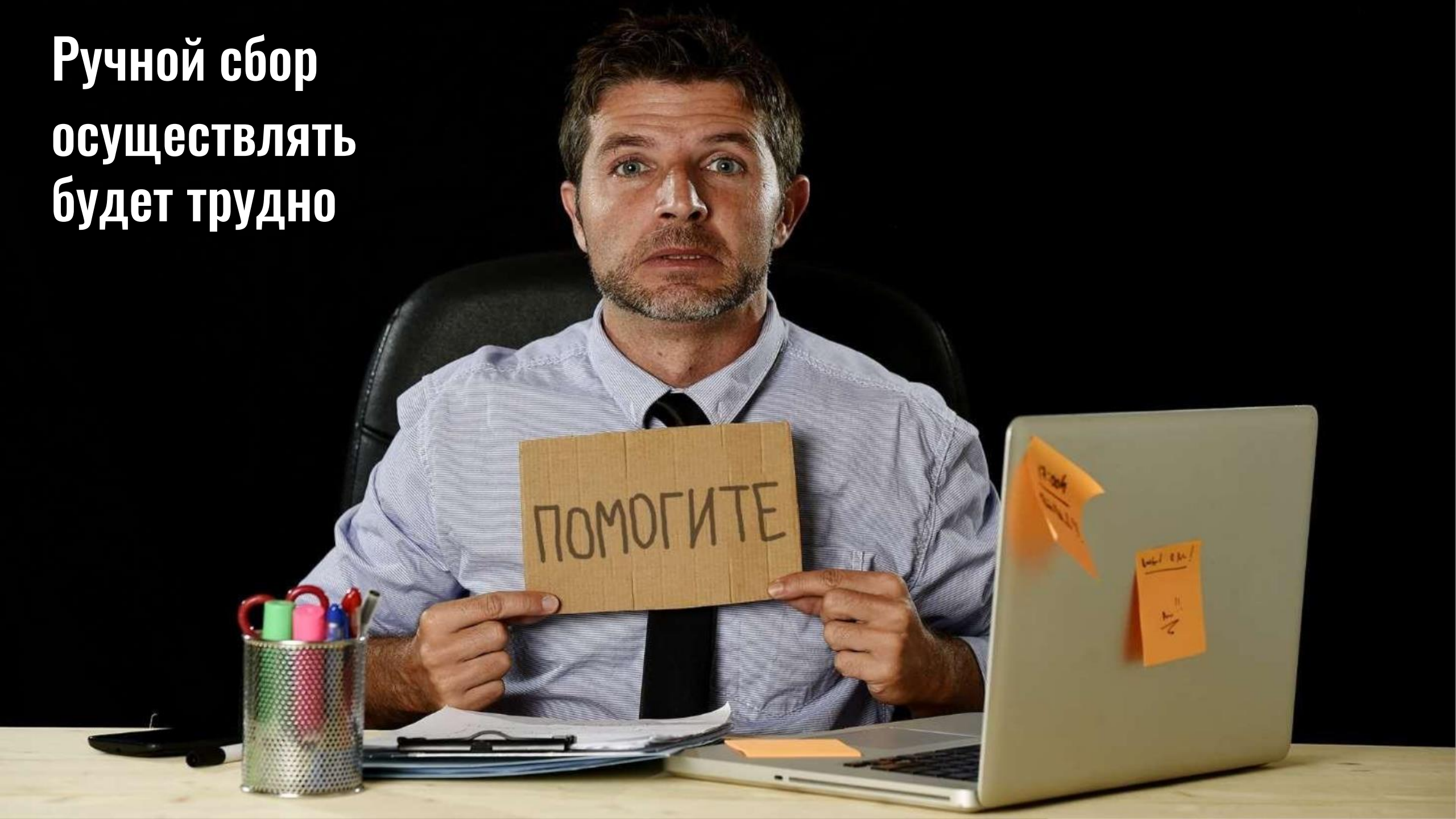
File Detail

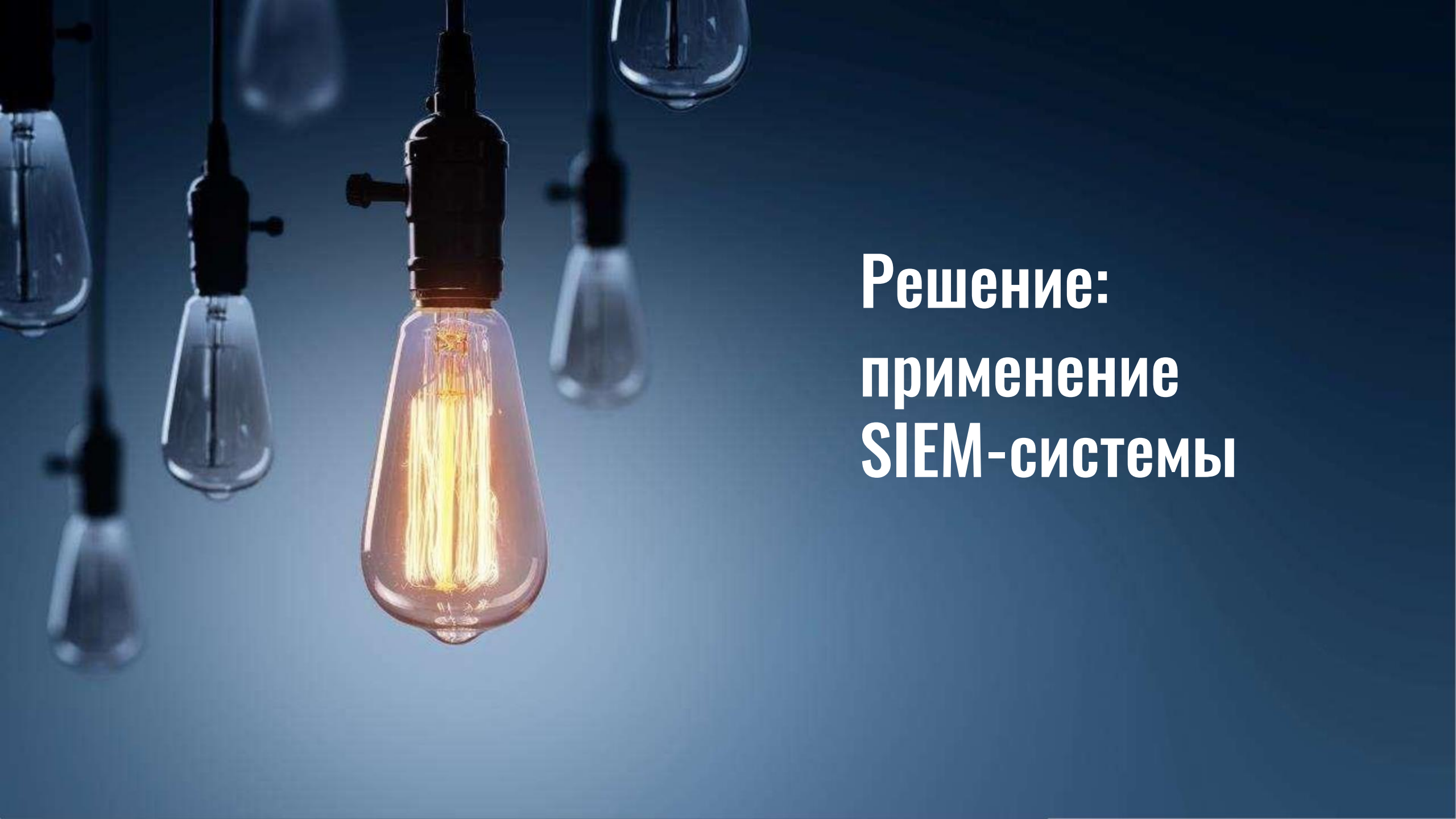
Seq No.	Date	Source	Thread...	Severity	Event Id	Text
8	5/09/2011 12:09:25....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 194.28.7...
10	5/09/2011 12:09:28....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 194.28.7...
12	5/09/2011 12:12:40....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 222.36.7...
14	5/09/2011 12:14:55....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 64.62.19...
16	5/09/2011 12:19:08....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 49.238.2...
18	5/09/2011 12:19:10....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 49.238.2...
20	5/09/2011 12:25:54....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 81.89.5.5...
22	5/09/2011 12:28:10....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 115.68.2...
24	5/09/2011 12:28:13....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 115.68.2...
26	5/09/2011 12:35:04....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 146.145....
28	5/09/2011 12:35:06....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 146.145....
30	5/09/2011 12:37:48....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 189.47.1...
32	5/09/2011 12:37:51....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 189.47.1...
34	5/09/2011 12:59:12....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 118.26.1...
36	5/09/2011 12:59:13....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 79.125.1...
38	5/09/2011 13:19:09....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 124.114....





Ручной сбор осуществлять будет трудно





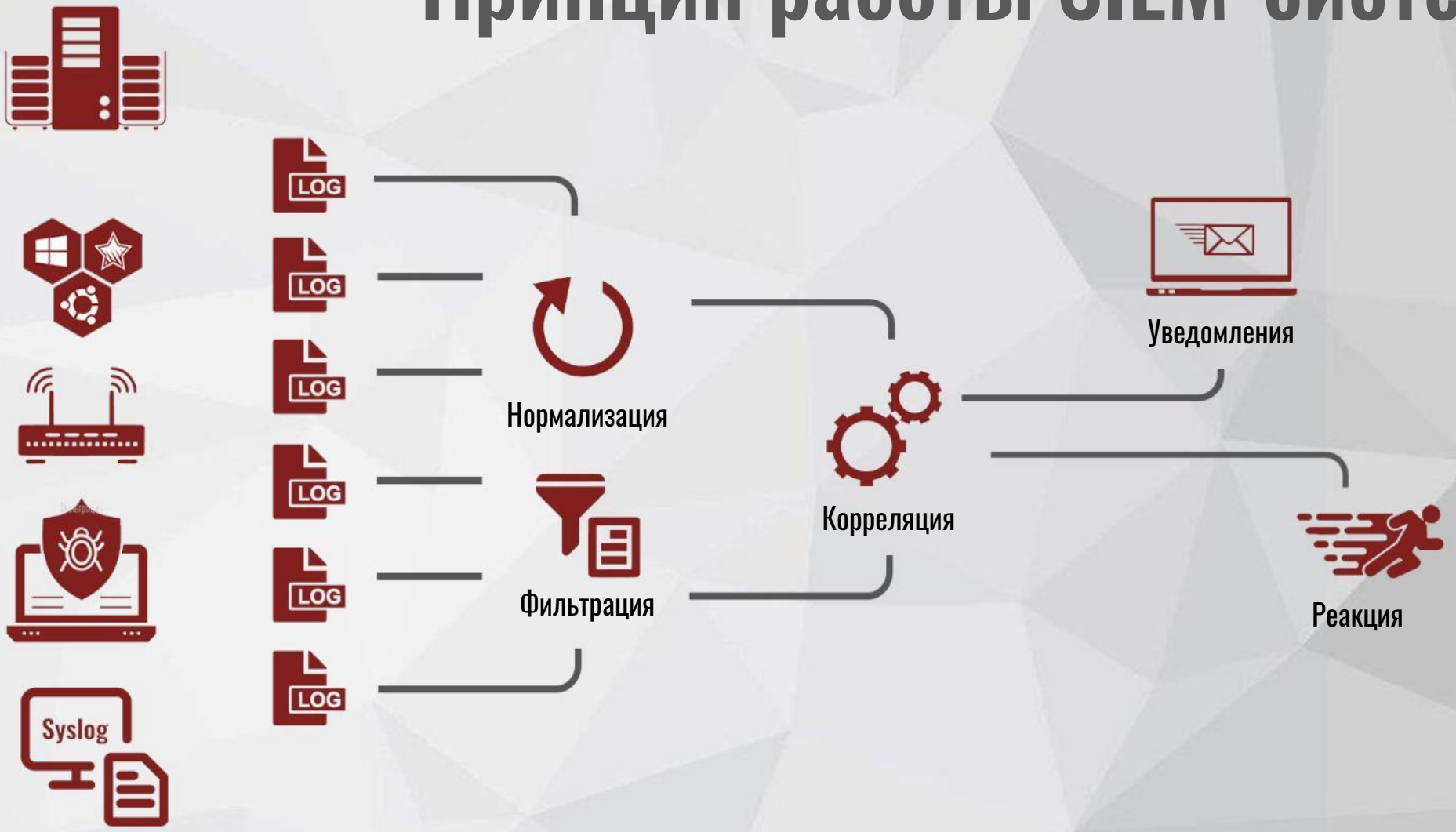
Решение: применение SIEM-системы

SIEM-система позволяет делать самое сложное - выявлять действия злоумышленников

KOMRAD Enterprise SIEM 4.3

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

Принцип работы SIEM-системы



Основной функционал SIEM-системы

- Лог-менеджмент: сбор и хранение событий
- Обработка событий: парсинг, фильтрация и корреляция событий
- Аналитика (отчеты, дашборды и т.п.)
- Управление инцидентами

Основные вопросы к SIEM-системе

Возможная производительность и требуемое аппаратное обеспечение

Поддерживаемые источники «из коробки»

Возможность подключения нестандартного источника событий

Возможности самостоятельной настройки системы

Способы оперативного оповещения об инциденте

Возможность автоматического реагирования на инциденты

ГОССОПКА

Возможность передачи инцидентов в систему ГосСОПКА

Требования к квалификации персонала для внедрения и сопровождения

Минимальные требования к аппаратному обеспечению

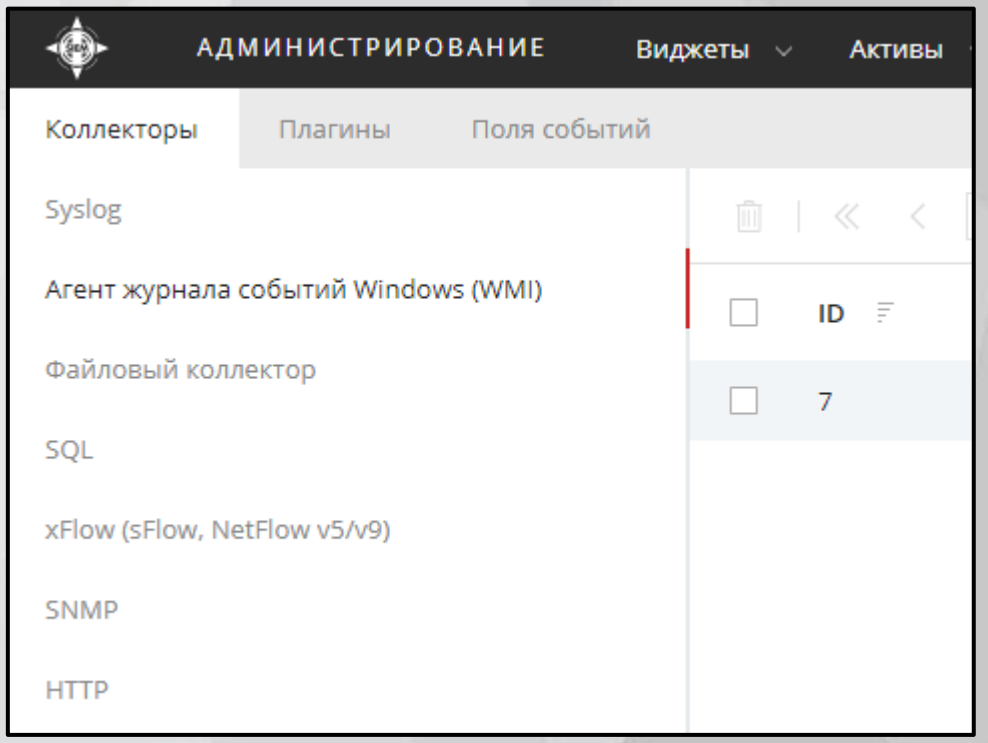
- ОЗУ: 4 GB
- CPU: 2 ядра
- SSD: 100 GB
- **500 - 5000 EPS**

- ОЗУ: 64 GB
- CPU: 4-8 ядра
- SSD: 10 Tb
- **20-25 тыс. EPS**

- ОЗУ: 128 GB
- CPU: 8-10 ядер
- SSD: 100 Tb
- **60-65 тыс. EPS**

Сбор событий

- Без агента, пассивный – syslog, xFlow, HTTP
- Без агента, активный – SNMP, SQL, файловый
- С агентом – WMI

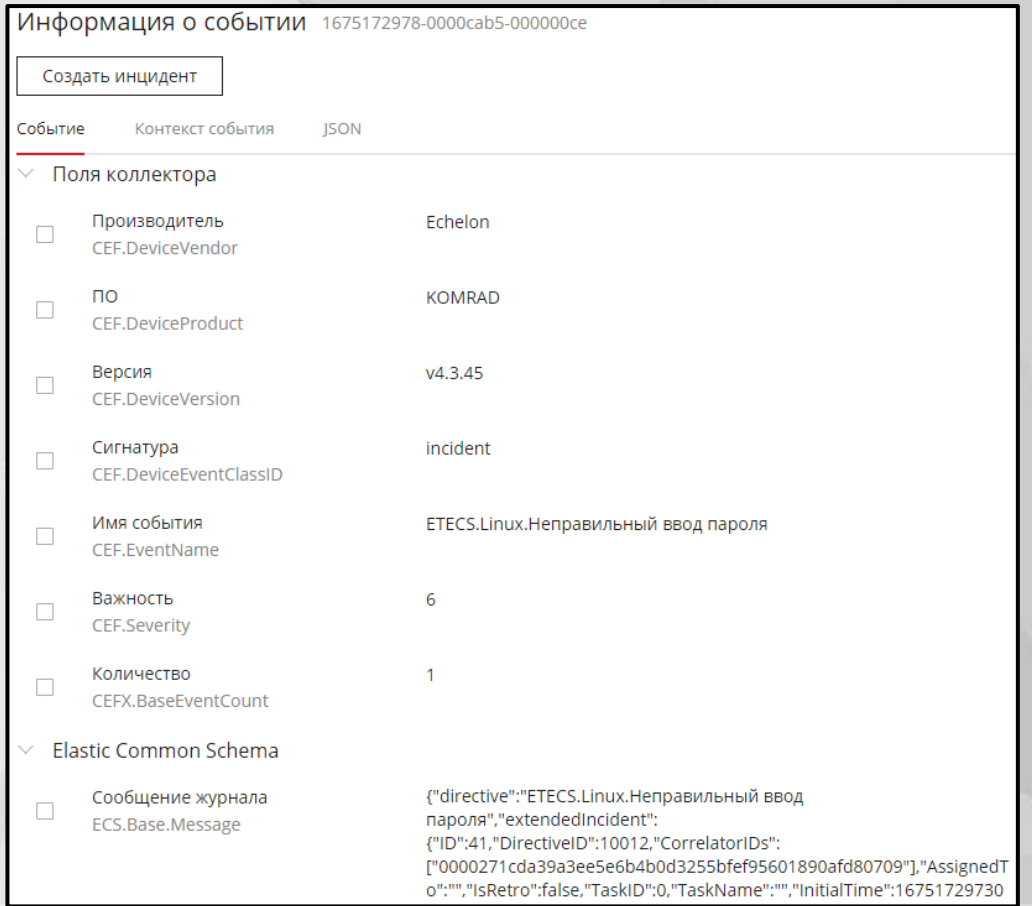


Нормализация (разбор) событий

- Сырое событие:

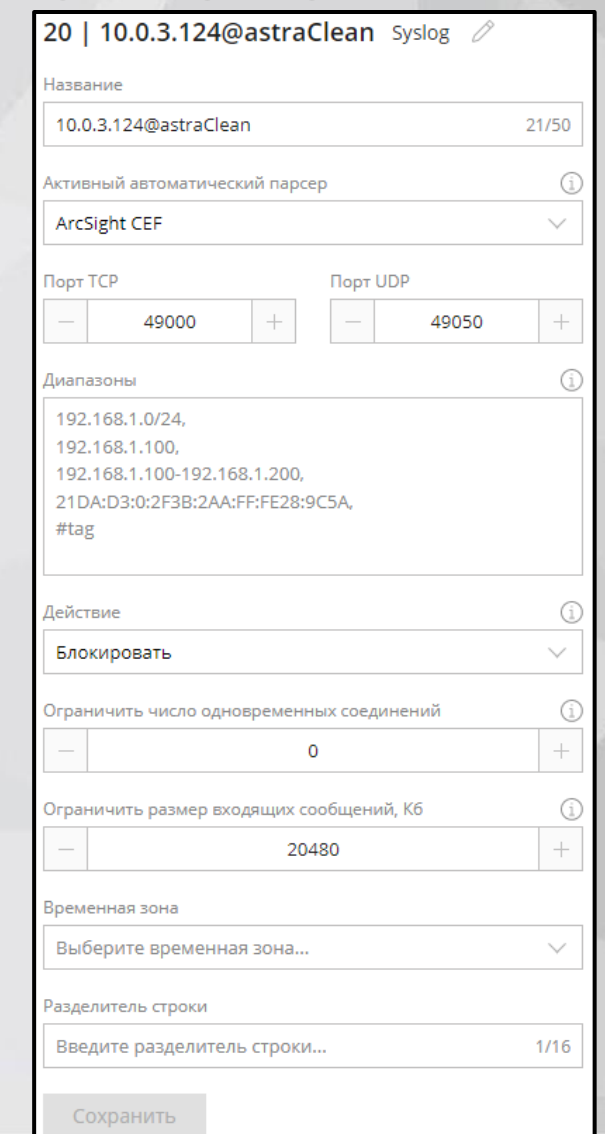
- 2023-01-31T16:49:38+03:00 komrad-node CEF:0|Echelon|KOMRAD|v4.3.45|incident|ETECS.Linux.Неправильный ввод пароля|6|type=3 start=1675172973000 rt=1675172977464 sl=715 cnt=1 ECS.Event.ID=41 ECS.Rule.ID=10012 ECS.Organization.ID=75 ECS.Related.IP=["10.0.3.38"] ECS.Error.Message=false type=2 msg={"directive":"ETECS.Linux.Неправильный ввод пароля","extendedIncident":

Разобранное событие:



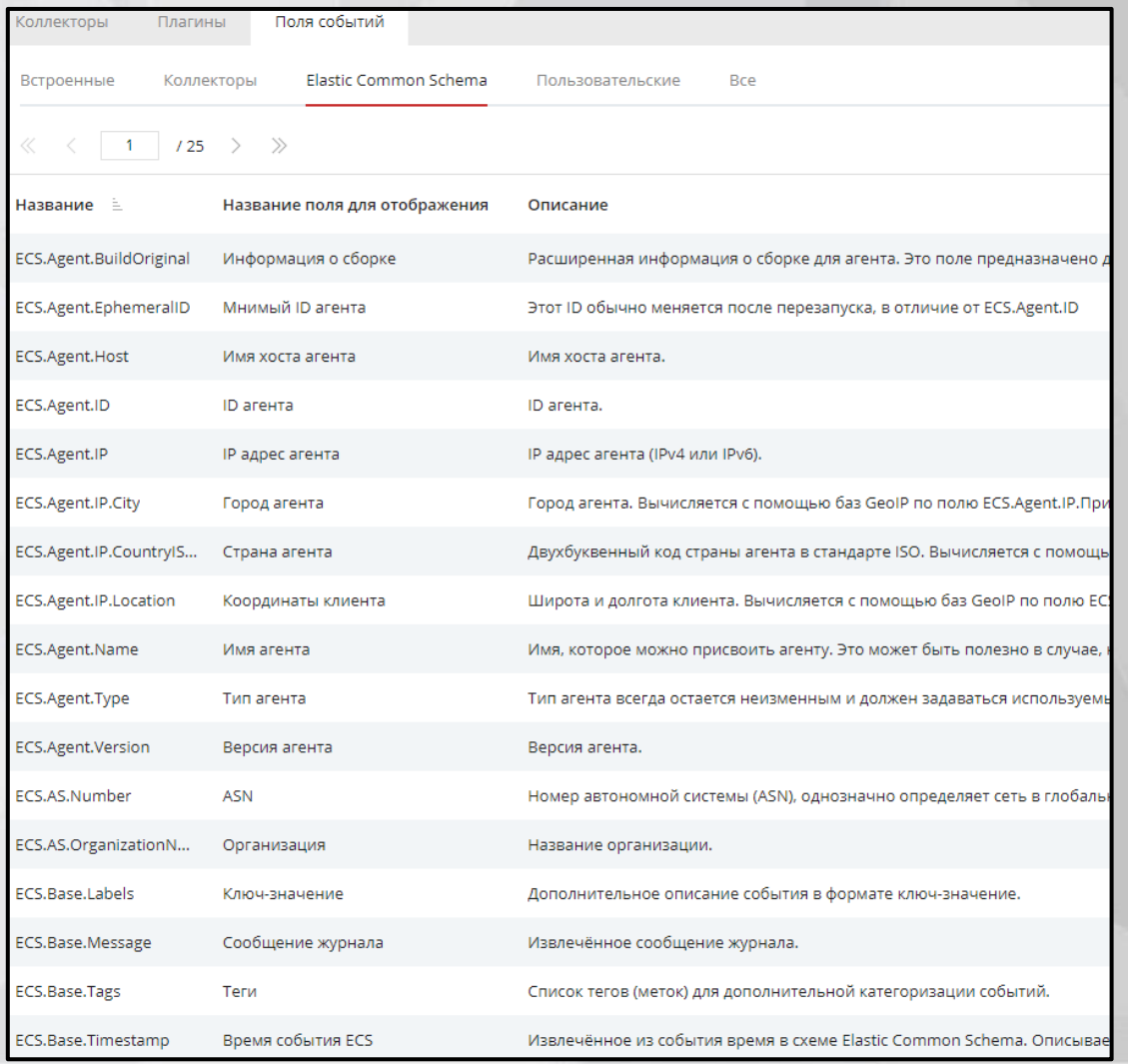
Поддерживаемые стандарты и технологии разбора событий

- 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



Elastic Common Schema

- События, получаемые от источников разбираются во внутреннюю структуру события KOMRAD Enterprise SIEM.
- Внутренняя структура использует поддерживает общепринятый стандарт Elastic Common Schema.

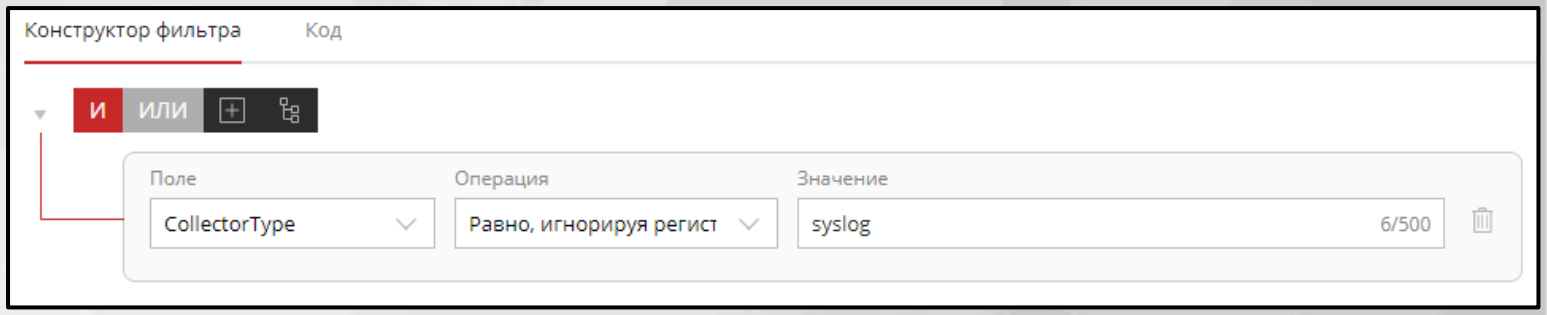

Коллекторы Плагины Поля событий

Встроенные Коллекторы Elastic Common Schema Пользовательские Все

1 / 25

Название	Название поля для отображения	Описание
ECS.Agent.BuildOriginal	Информация о сборке	Расширенная информация о сборке для агента. Это поле предназначено д
ECS.Agent.EphemeralID	Мнимый ID агента	Этот ID обычно меняется после перезапуска, в отличие от ECS.Agent.ID
ECS.Agent.Host	Имя хоста агента	Имя хоста агента.
ECS.Agent.ID	ID агента	ID агента.
ECS.Agent.IP	IP адрес агента	IP адрес агента (IPv4 или IPv6).
ECS.Agent.IP.City	Город агента	Город агента. Вычисляется с помощью баз GeoIP по полю ECS.Agent.IP.При
ECS.Agent.IP.CountryIS...	Страна агента	Двухбуквенный код страны агента в стандарте ISO. Вычисляется с помощь
ECS.Agent.IP.Location	Координаты клиента	Широта и долгота клиента. Вычисляется с помощью баз GeoIP по полю EC
ECS.Agent.Name	Имя агента	Имя, которое можно присвоить агенту. Это может быть полезно в случае,
ECS.Agent.Type	Тип агента	Тип агента всегда остается неизменным и должен задаваться используем
ECS.Agent.Version	Версия агента	Версия агента.
ECS.AS.Number	ASN	Номер автономной системы (ASN), однозначно определяет сеть в глобаль
ECS.AS.OrganizationN...	Организация	Название организации.
ECS.Base.Labels	Ключ-значение	Дополнительное описание события в формате ключ-значение.
ECS.Base.Message	Сообщение журнала	Извлечённое сообщение журнала.
ECS.Base.Tags	Теги	Список тегов (меток) для дополнительной категоризации событий.
ECS.Base.Timestamp	Время события ECS	Извлечённое из события время в схеме Elastic Common Schema. Описывае

Фильтры событий



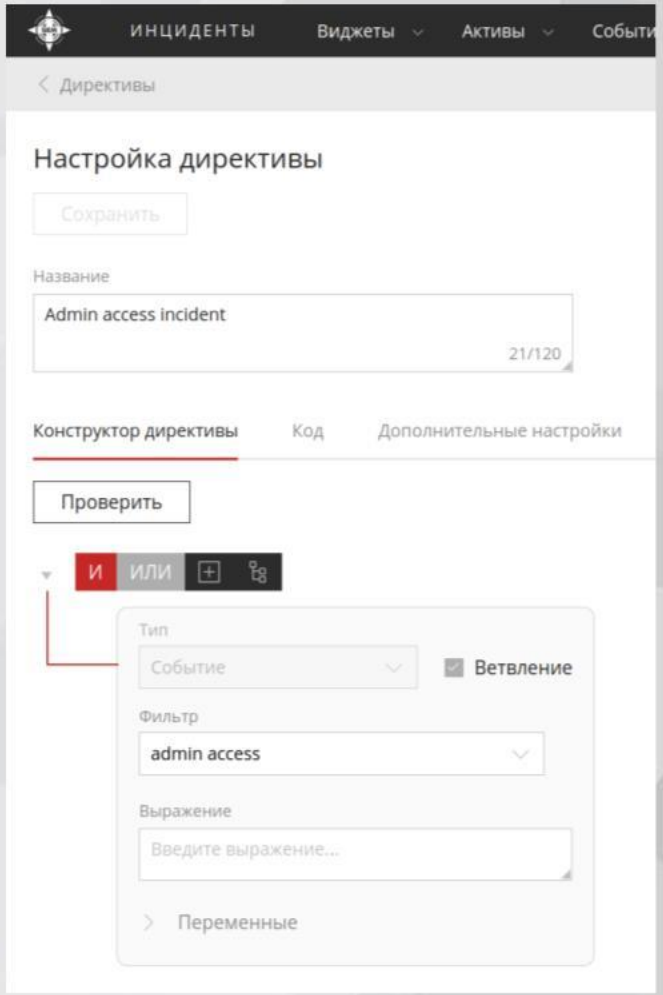
СОБЫТИЯ | Виджеты | Активы | События | Инциденты | Администрирование | Ru | admin

1 / 1967 | ETECS.Syslog.Все события | 31.01.2023, 15:04 — 31.01.2023, 17:04 | Найти

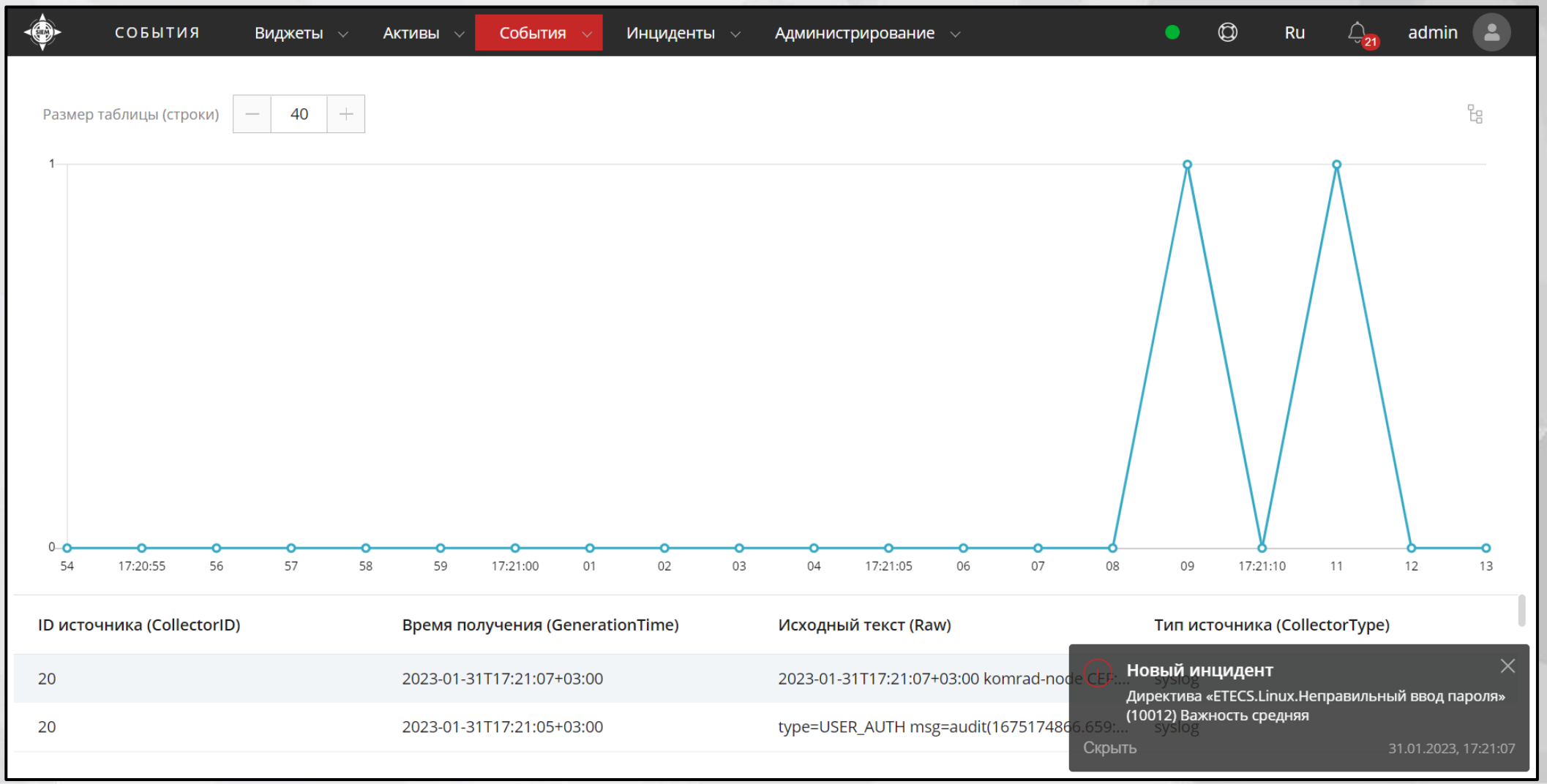
ID источника (CollectorID)	IP активов (AssetIPs)	Время получения (GenerationTime)	Исходный текст (Raw)	Порядковый номер лога (Auditd.Log.Sequence)	Тип источника (CollectorType)
10.0.3.124@astraClean 20	10.0.3.38	31.01.2023, 17:02:10	type=PROCTITLE msg=audit(1675173731.411:4...	435	syslog
10.0.3.124@astraClean 20	10.0.3.38	31.01.2023, 17:02:10	type=PATH msg=audit(1675173731.411:435): it...	435	syslog
10.0.3.124@astraClean 20	10.0.3.38	31.01.2023, 17:02:10	type=CWD msg=audit(1675173731.411:435): cw...	435	syslog
10.0.3.124@astraClean 20	10.0.3.38	31.01.2023, 17:02:10	type=SYSCALL msg=audit(1675173731.411:435)...	435	syslog
10.0.3.124@astraClean 20	10.0.3.38	31.01.2023, 17:02:10	type=AVC msg=audit(1675173731.411:435): par...	435	syslog

Директивы корреляции

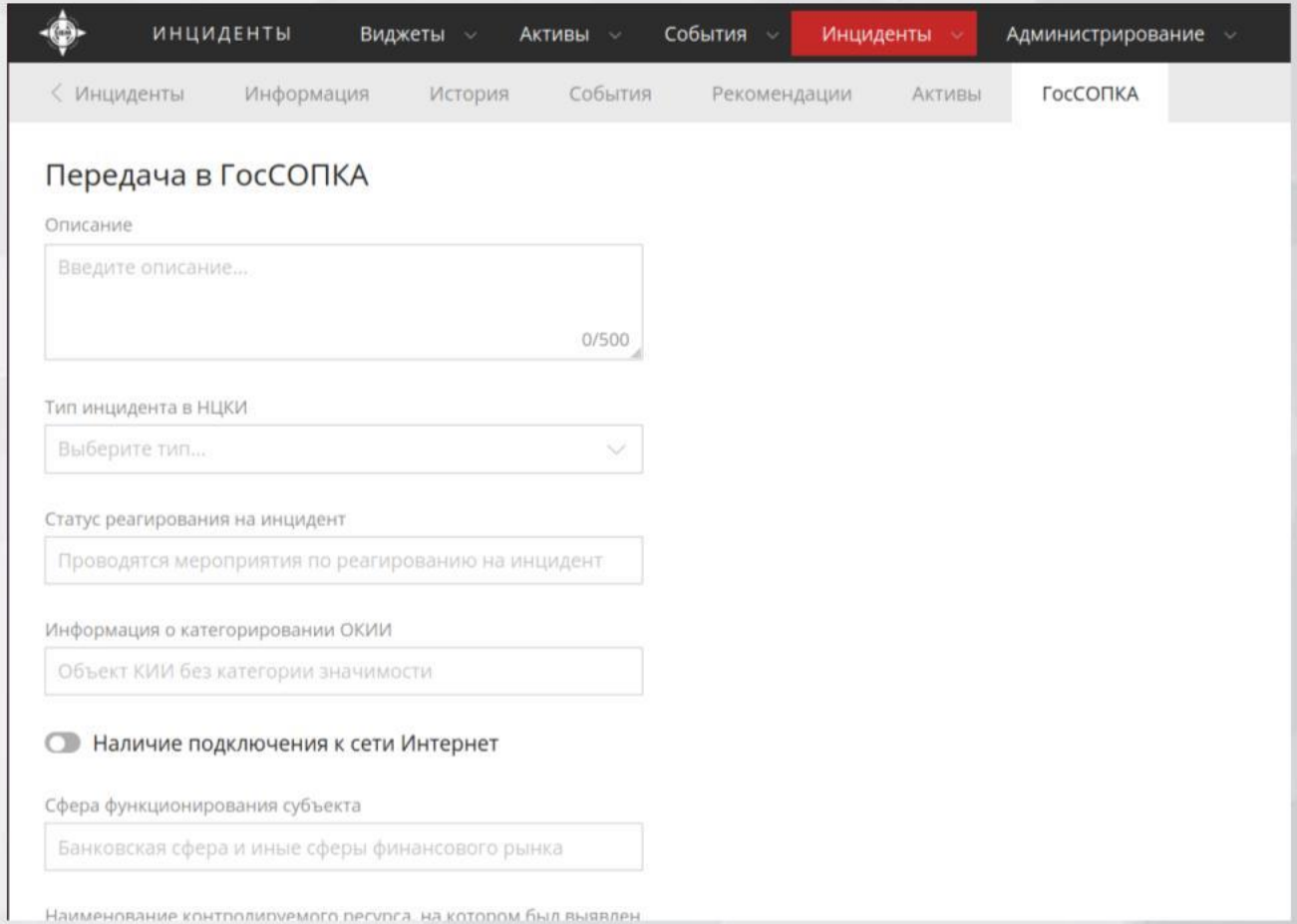
- Простой вариант: ссылка на фильтр
- Продвинутый:
  - Определение последовательности событий с временными окнами
  - Работа с переменными
  - Проверка отсутствия события



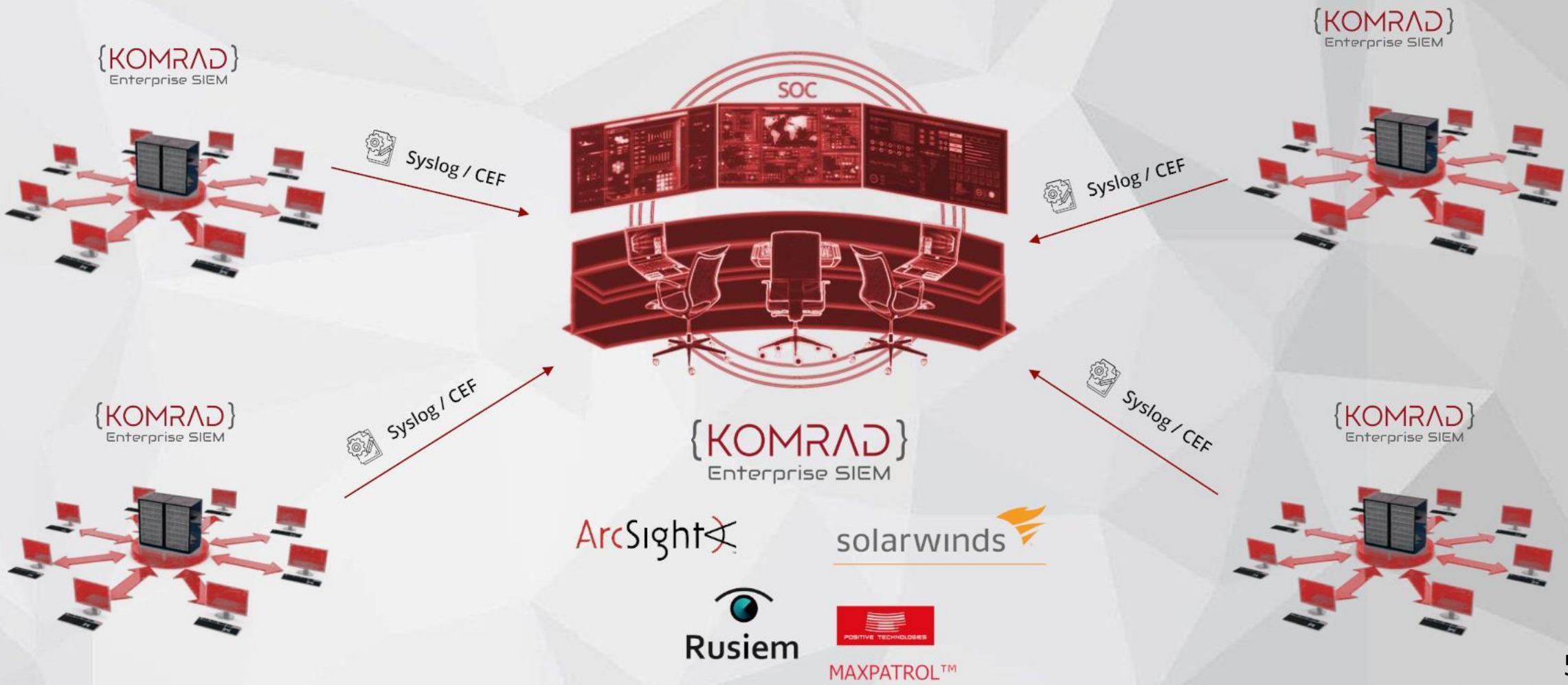
Уведомление: в интерфейсе и по SMTP



Инцидент может быть передан в ГОССОПКА автоматически или в ручном режиме



Отправка событий в другие системы



SIEM-система – ядро SOC

- Таким образом SIEM-система позволяет автоматизировать самые критичные функции, которые должен реализовать современный центр мониторинга информационной безопасности.
- SIEM-система должна быть дополнена также решениями класса СОВ, анализа защищенности и управления инцидентами.

Персонал для внедрения и сопровождения

Для внедрения и сопровождения KOMRAD Enterprise SIEM необходимы следующие специалисты:

- Системный администратор для развертывания продукта и подключения источников.
- Сетевой администратор для конфигурации сетевой инфраструктуры.
- Специалист по информационной безопасности для формирования фильтров, директив корреляции и регулярного контроля за работой системы.

План пилотного проекта

1. Заключение NDA (при необходимости).
2. Передача дистрибутива или образа виртуальной машины.
3. Организация пилотной площадки.
4. Подключение источников событий.
5. Создание фильтров и разработка директив.
6. Тестовая эксплуатация.
7. Корректировка и дополнение правил корреляции.

On-line презентация

Ознакомиться с функциональными возможностями KOMRAD Enterprise SIEM можно в online-режиме.

Для этого необходимо:

- Обратиться к интегратору, являющемуся авторизованным партнёром вендора
- Согласовать время проведения.

Оставайтесь на связи

Группа пользователей KOMRAD 4

- Ссылки на дистрибутивы и документацию
- Оперативная помощь по применению продукта
- https://t.me/komrad4

Новостной telegram-канал Echelon Eyes

- Материалы вебинара: презентации, видео
- Новости об уязвимостях, инцидентах, эксплойтах, изменениях в нормативной базе
- https://t.me/EchelonEyes

{KOMRAD}
Enterprise SIEM

СПАСИБО ЗА ВНИМАНИЕ!

Эшелон
комплексная безопасность

+7 (495) 223-23-92
E-mail: partners@npo-echelon.ru