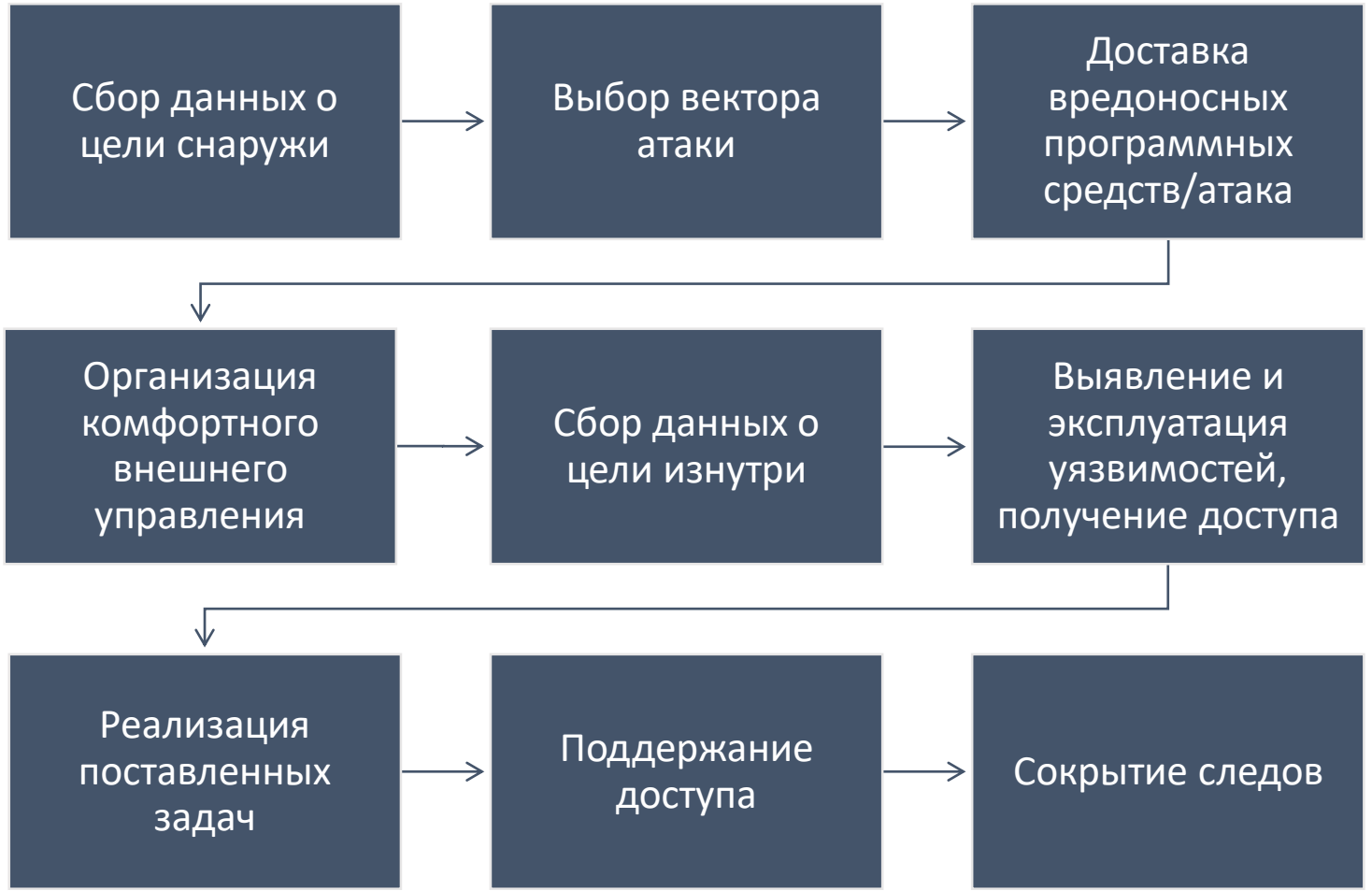
Эшелон
комплексная безопасность

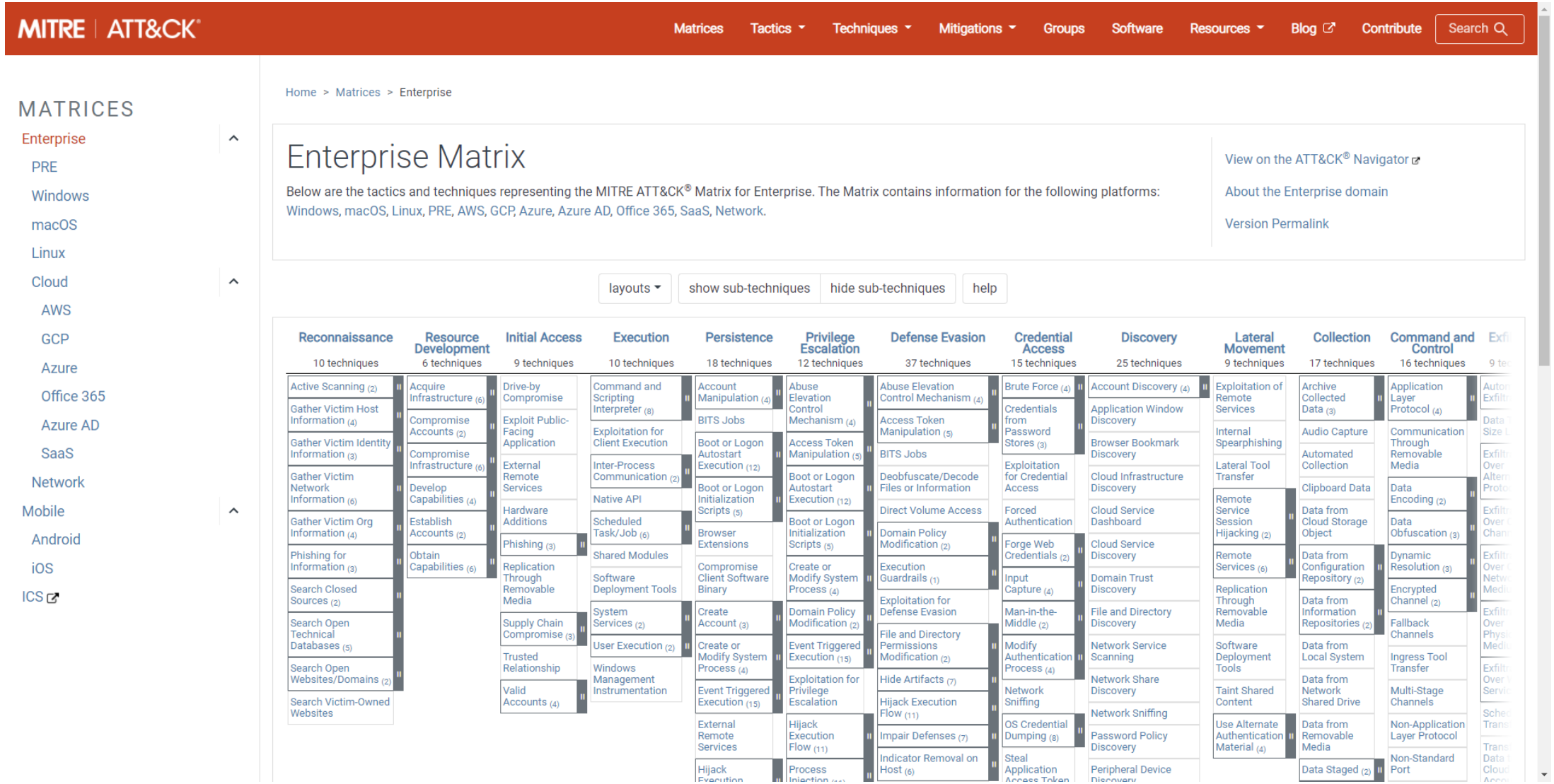
Система мониторинга событий ИБ

Дмитрий Донской
Директор по развитию

Современная таргетированная атака = спецоперация

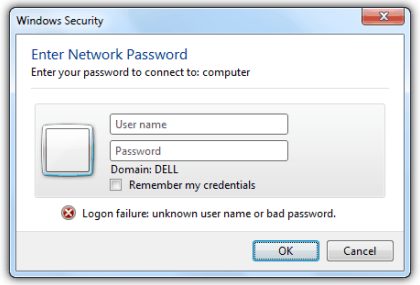


Векторы атак. 14 тактик с более чем 500 техник взлома



Как своевременно обнаруживать таргетированные атаки?

Необходимо отслеживать признаки нарушения ИБ



Авторизация: как успешная, так и неуспешная

Срабатывания антивирусного ПО, IDS\IPS, DLP, СЗИ

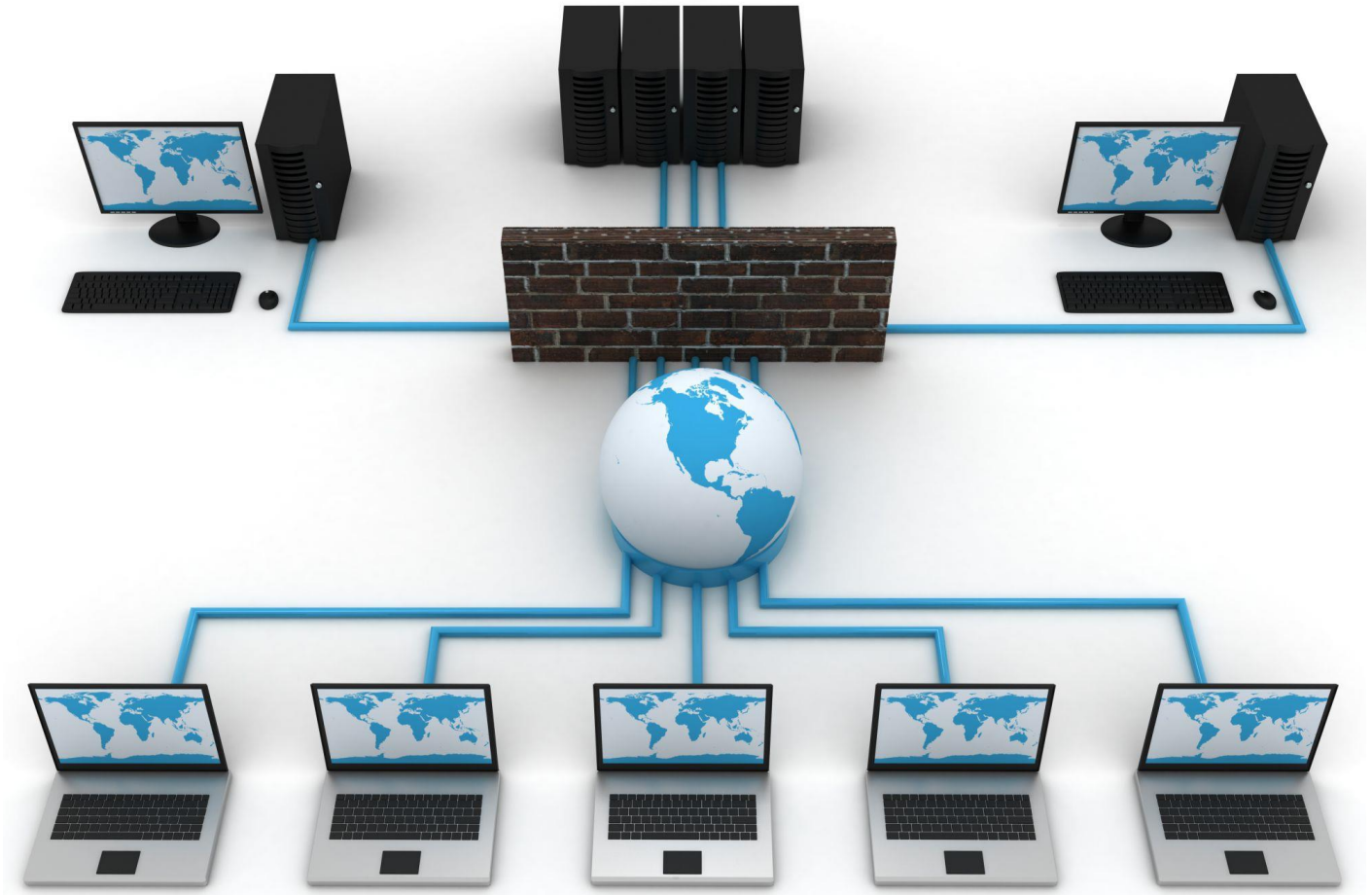
Бесконтрольный выход в Internet и соцсети

Подозрительные запросы к СУБД

Нетипичное поведение пользователя

Удаленный доступ

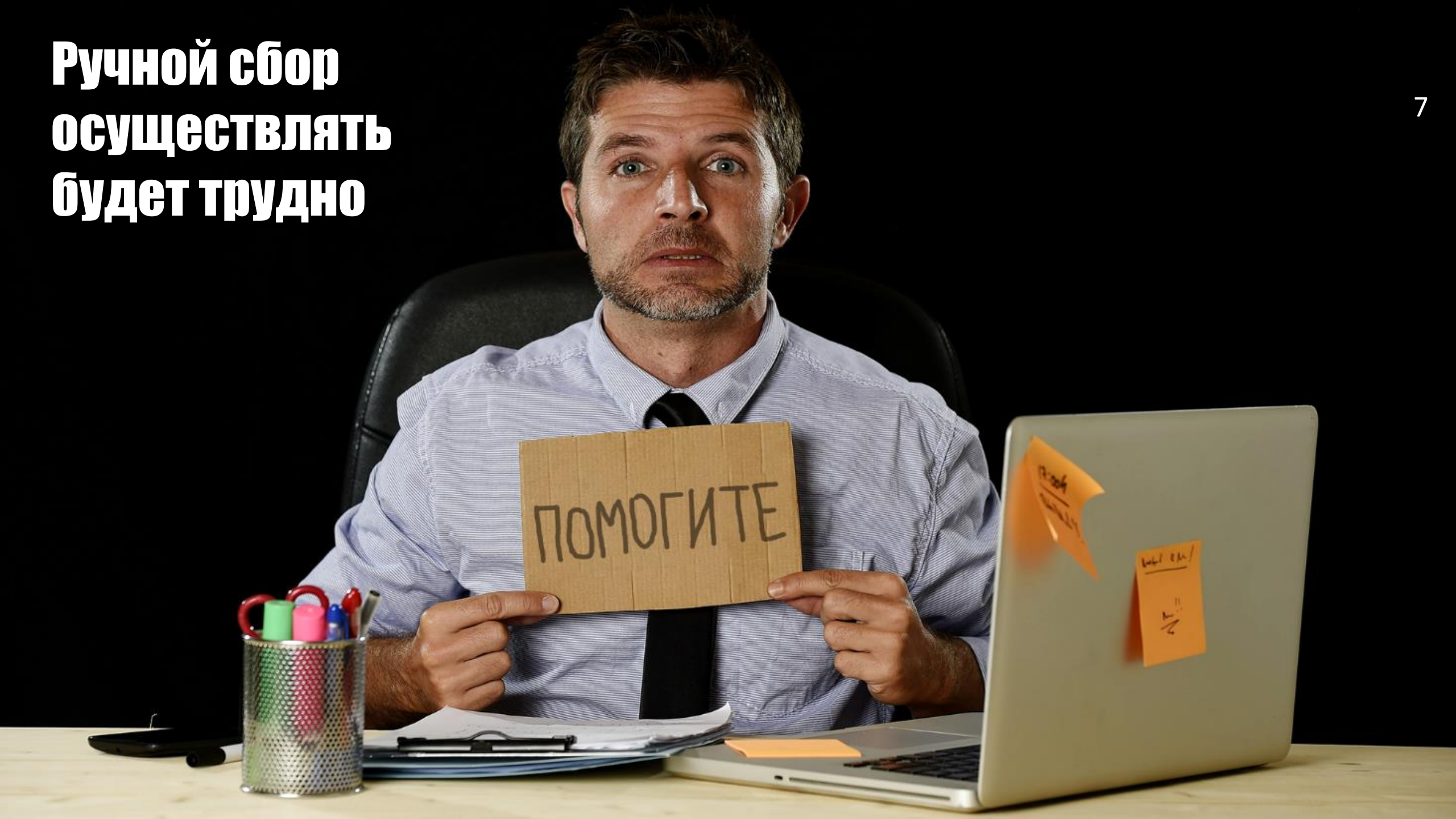
Для этого надо осуществлять мониторинг критичных сегментов инфраструктуры

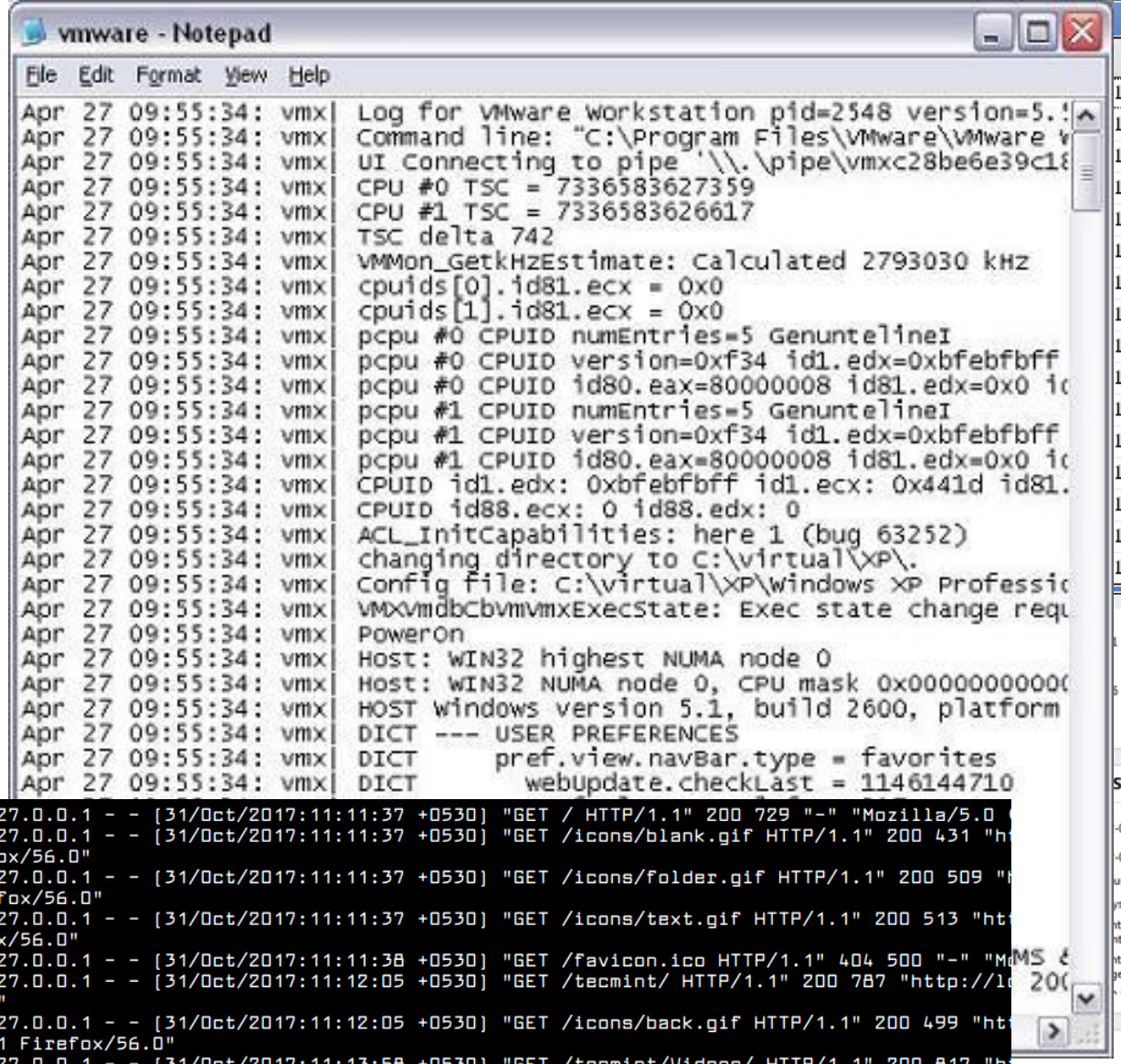


Соответствующее требование включено в:

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

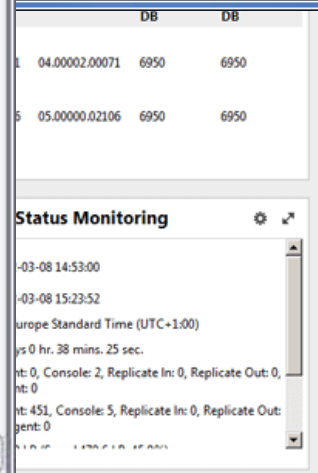
Ручной сбор осуществлять будет трудно

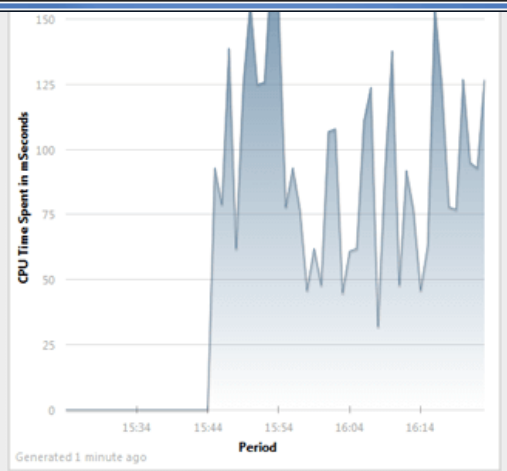


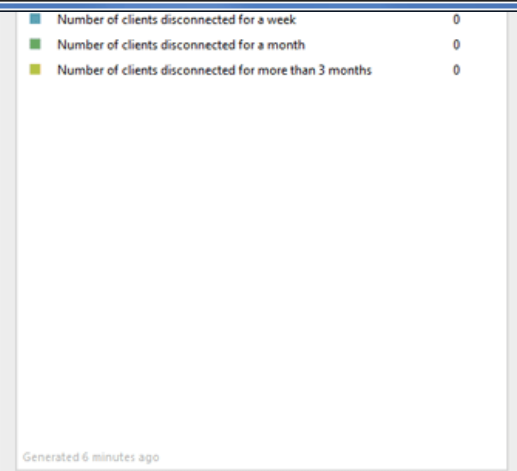


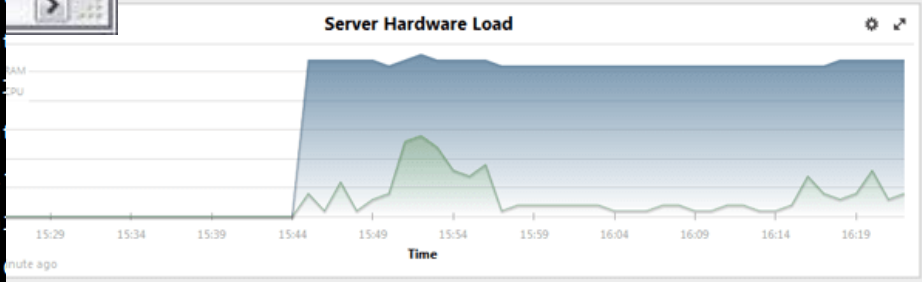

```
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET / HTTP/1.1" 200 729 "-" "Mozilla/5.0 (
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/blank.gif HTTP/1.1" 200 431 "ht
fox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/folder.gif HTTP/1.1" 200 509 "h
efox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/text.gif HTTP/1.1" 200 513 "htt
ox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:38 +0530] "GET /favicon.ico HTTP/1.1" 404 500 "-" "Mo
127.0.0.1 - - [31/Oct/2017:11:12:05 +0530] "GET /tecmint/ HTTP/1.1" 200 787 "http://lo
0"
127.0.0.1 - - [31/Oct/2017:11:12:05 +0530] "GET /icons/back.gif HTTP/1.1" 200 499 "htt
01 Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:13:58 +0530] "GET /tecmint/Videos/ HTTP/1.1" 200 817 "ht
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 "ht
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)
```

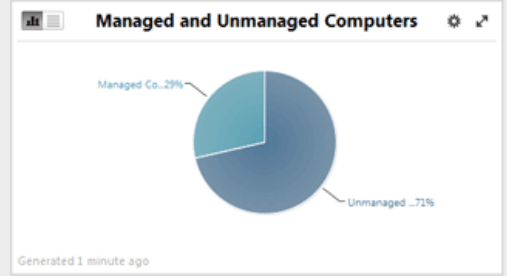
	Source	Thread...	Severity	Event Id	Text
12:09:25....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 194.28.7...
12:09:28....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 194.28.7...
12:12:40....	WinGate NAT	248	Info	2	Authorisation 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....











Решение: применение SIEM-системы

Что такое SIEM-система?

{KOMRAD}
Enterprise SIEM

SIEM-система – это единая точка входа событий с разных источников, и управление этими событиями

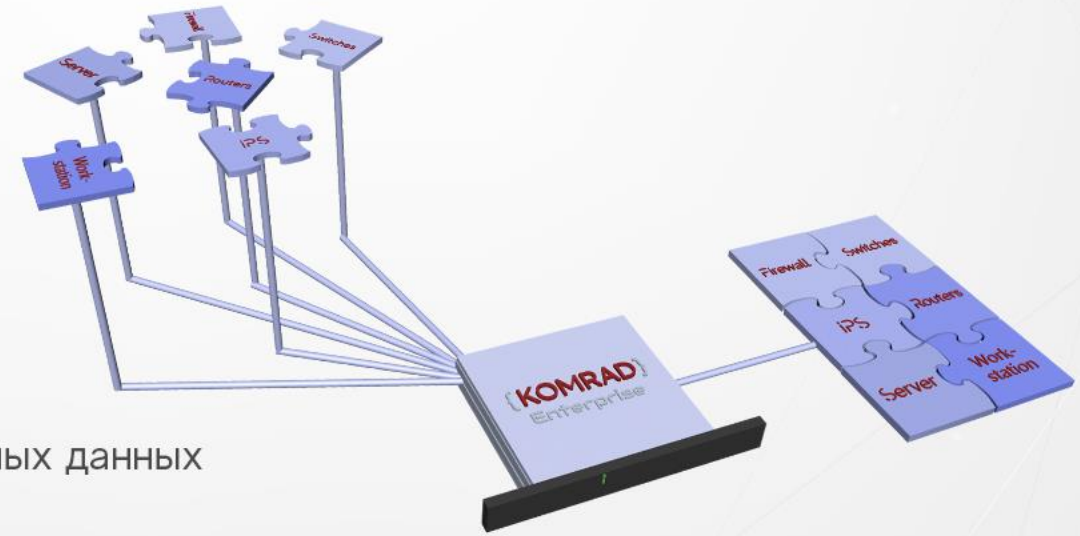
Собирает события из различных источников (Windows, Linux, IDS, DLP, СЗИ, сетевые устройства)

Анализирует поступившие события

Управляет событиями IT и ИБ

Предупреждает об угрозах и инцидентах

Хранит все события для просмотра детализированных данных



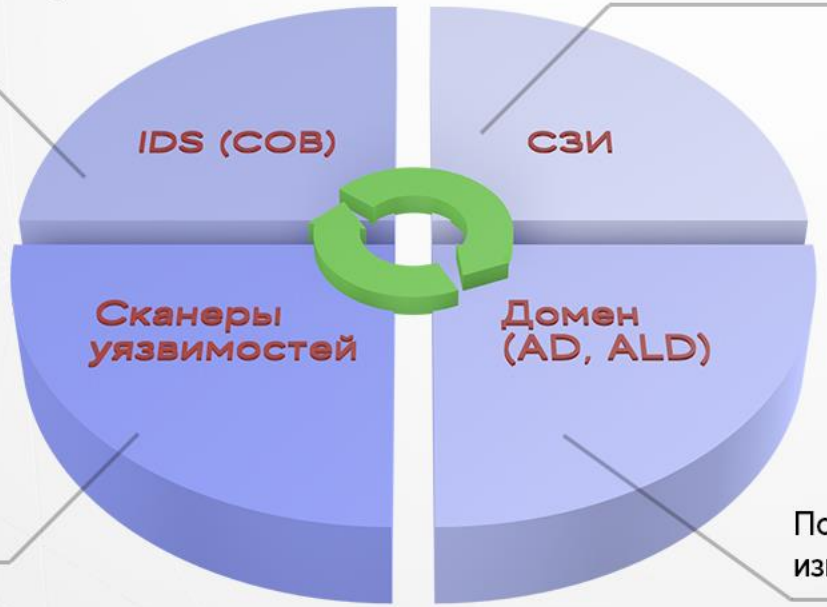
SIEM - централизованная система управления событиями ИБ

npo-echelon.ru

События бывают разными?

Распознает только сигнатуры угроз в пакетах и протоколах

Видят файлы, имена хостов, контролируемые процессы



Находят уязвимости в активах

Пользователи, активные службы, изменения конфигураций

SIEM-система КОМРАД

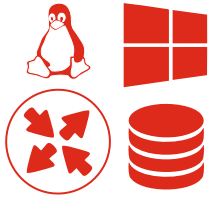
- Аналитический инструмент для ИТ и ИБ
- Единый центр входа всех событий
- Позволяет держать руку на пульсе всех событий
- КОМРАД собирает и выявляет – человек думает

KOMRAD Enterprise SIEM 4.0

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

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 и Windows

Минимальные требования к аппаратному обеспечению

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

Имеющиеся коннекторы

{KOMRAD}
Enterprise SIEM

- Astra Linux
- МЭ и СОВ «Рубикон»/«Рубикон-К»
- Сканер-ВС
- Kaspersky Security Center/
- Kaspersky Endpoint Security
- Dr.Web
- SecretNet Studio
- DallasLock
- vGate R2
- ViPNet Coordinator HW2000
- VIPNet IDS
- TLS Континент
- DeviceLock

А также:

- **Windows** (системные журналы и журналы приложений)
- **Linux** (журналы: стандартные, Auth, Dpkg, LAST,
- LASTB, WHO, Apport, Cups, Samba, Kernel,
- Qume, KVM, LibVirt, Auditd)
- **Suricata**
- **Zeek**
- **Postfix**
- **Nginx**
- **Apache HTTP-server**
- **IPtables**
- **OSquery**

npo-echelon.ru

В рамках внедрения существует возможность самостоятельно писать коннекторы.

Примеры директив

malware Заражение вредоносным программным обеспечением. Берутся из средств антивирусной защиты

malware distribution Распространение вредоносного программного обеспечения. Берутся из средств антивирусной защиты

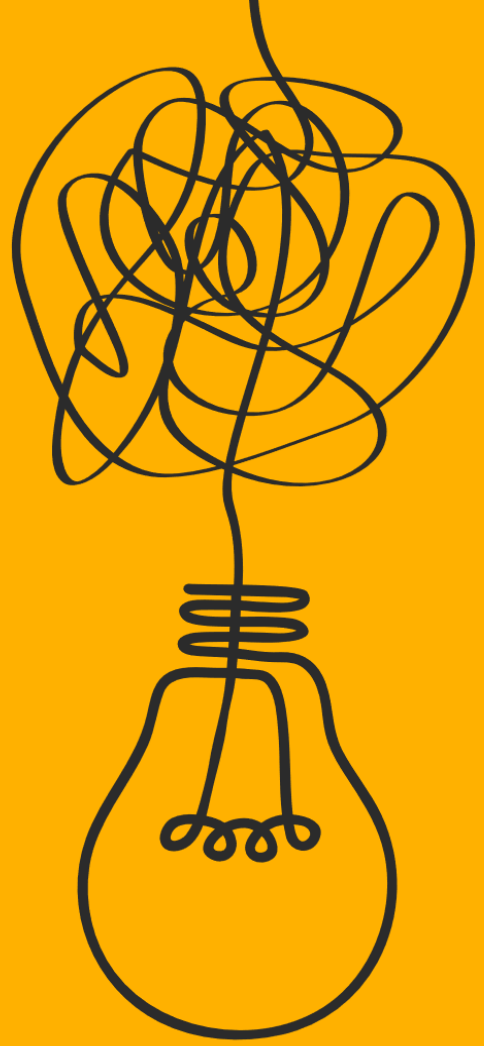
intrusion Несанкционированный доступ в систему. Берутся из журналов аутентификации

intrusion attempt Попытки несанкционированного доступа в систему или к информации. Берутся из журналов аутентификации

information gathering Сбор сведений с использование ИКТ. Мониторинг событий связанных со сканированием сети и активов

abusive content Распространение информации с неприемлемым содержимым. Данные берутся из DLP систем

vulnerability Уязвимость. Данные берутся из сканеров уязвимостей



SIEM-система может
быть простой в использовании

ПРЕИМУЩЕСТВА, КАК ЕСТЬ

- Нет ничего лишнего, за что нужно доплачивать
- Модульная система, покупаете то, что нужно
- Возможность купить минимальную конфигурацию и расширять функционал по мере потребностей

- Не требуются высокоспециализированные специалисты
- Директивы корреляции можно писать самим

- Минимальная стоимость владения после покупки
- Оперативное принятие мер на изменение требований регуляторов к реагированию на инциденты

- Онлайн и оффлайн курсы, вебинары, собственный учебный центр

Условия лицензирования

{KOMRAD}
Enterprise SIEM

В отличие от большинства других SIEM-систем, дистрибутив КОМРАД работает как на коммерческих, так и открытых ОС

- ✔ Стоимость лицензии не привязана к операционной системе
- ✔ Стоимость лицензии зависит от функционала
- ✔ Стоимость лицензии зависит от наличия сертификата соответствия ФСТЭК России

npo-echelon.ru

КОМРАД включен в реестр отечественного ПО.

Для кого мы сделали новую версию KOMRAD Enterprise SIEM?

- Средний и крупный бизнес
- Государственные структуры
- Банки и финансовые организации
- Субъекты КИИ
- Соискатели лицензии ФСТЭК России

SIEM-система должна защищать вашу инфраструктуру так же, как и антивирус!

Когда нужна SIEM-система

{KOMRAD}
Enterprise SIEM

Обеспечение безопасности бизнеса

- Вовремя пресечь сетевые атаки и попытки компрометации ИС
- Узнать о веерных вирусных заражениях
- Заблокировать попытки несанкционированного доступа
- Выявить слабые места в инфраструктуре
- Донастроить средства защиты информации

Соответствие стандартам и требованиям регуляторов

- **ФСТЭК России**
  (приказы 17,21,31,235 приказы)
- **ФинЦЕРТ**
  (382-П, СТО БР ИББС-1.3-2016,
  СТО БР БФБО-1.5-2018, ГОСТ Р 57580.1-2017)
- **ГосСОПКА**
  (приказы ФСБ 367, 368)
- **PCI DSS**
- **ISO 27001**

npo-echelon.ru

5 шагов по развёртыванию SIEM

{KOMRAD}
Enterprise SIEM

I. ПОДГОТОВИТЕЛЬНЫЙ ЭТАП
- Обследование инфраструктуры
- Формирование ТЗ и выбор функционала

II. ВНЕДРЕНИЕ/ПИЛОТ
- Установка и базовая настройка
- Настройка источников событий
- Разработка правил реагирования (корреляции)

III. ТЕСТОВАЯ ЭКСПЛУАТАЦИЯ
- Тонкая настройка системы
- Корректировка и дополнение правил корреляции

IV. ПРИЁМО-СДАТОЧНЫЕ ИСПЫТАНИЯ
- Проверка срабатывания правил корреляции на инциденты

V. ЭКСПЛУАТАЦИЯ
- Проведение внешних и внутренних пентестов
- Тонкая настройка средств защиты информации

npo-echelon.ru

КАК ПОЛУЧИТЬ DEMO-ВЕРСИЮ?

- ✓ Получите демо-версию, написав нам на адрес getkomrad@npo-echelon.ru
- ✓ Вступите в группу в Telegram: https://t.me/joinchat/DGLERFfkEY5F7SOnUmwPvg
- ✓ Есть вопросы и предложения – пишите на partners@npo-echelon.ru

Дмитрий Донской
Директор по развитию
+7 495 223-23-92 # 733
+7 909 678-60-90
+7 915 433-42-83
d.donskoy@npo-echelon.ru