

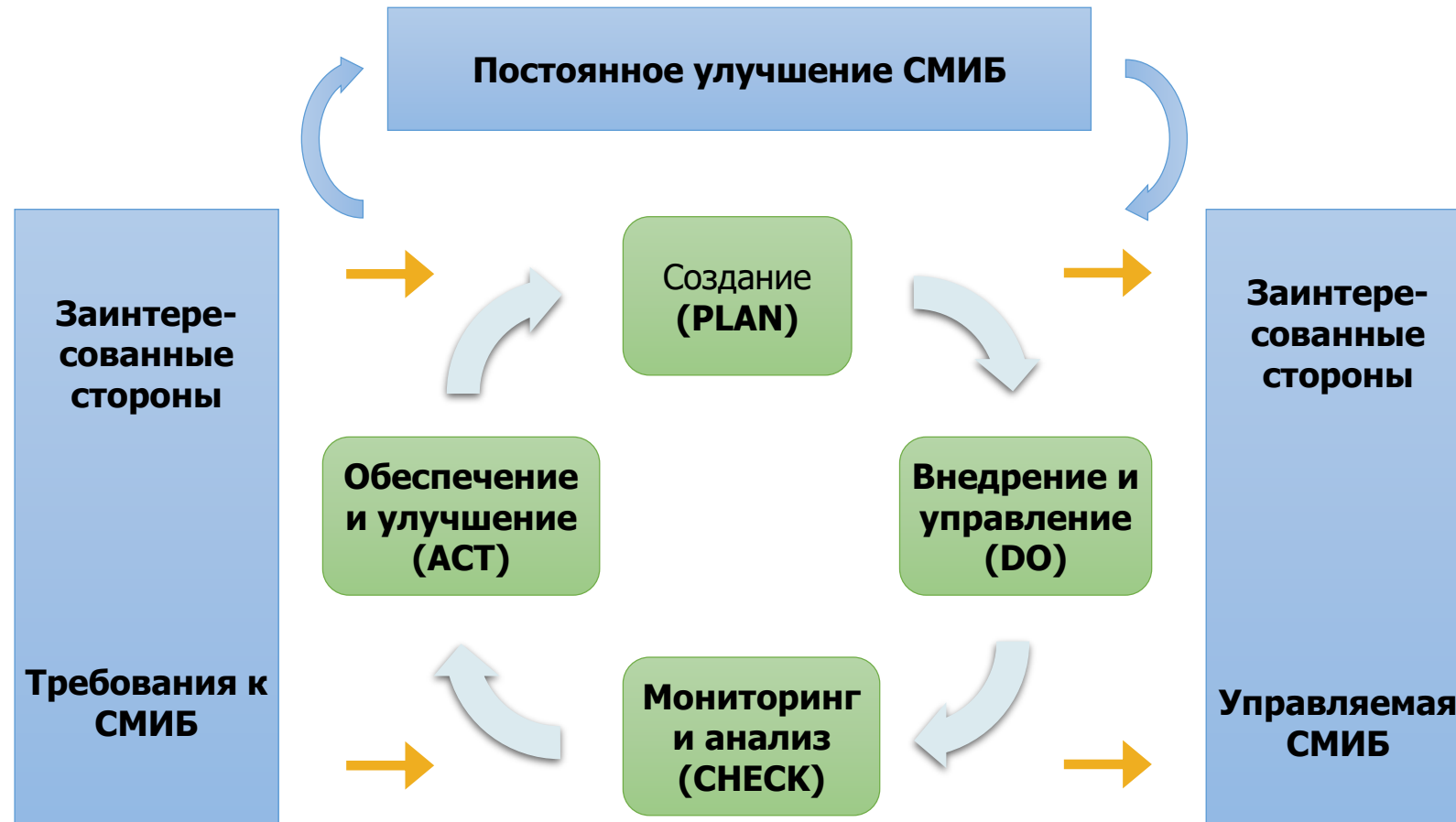
МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ В РАМКАХ СМИБ. ПРИМЕНЕНИЕ SIEM-СИСТЕМЫ «КОМРАД»

Александр Дорофеев, CISSP, CISA, CISM
Директор по развитию

СОДЕРЖАНИЕ

1. Краткое введение в СМИБ и ISO 27001
2. Управление инцидентами и сбор событий по ISO 27001
3. Зачем нужна SIEM?
4. SIEM-система «КОМРАД»
5. Правила корреляции для SIEM
6. Практика применения в ESOC

PDCA И СМИБ



СТРУКТУРА ISO 27001

- 0 Введение
- 1 Область применения
- 2 Нормативные ссылки
- 3 Термины и определения

PLAN

- 4 Контекст организации
- 5 Лидерство
- 6 Планирование
- 7 Поддержка

DO

- 8 Операционная деятельность

CHECK

- 9 Оценка производительности

ACT

- 10 Улучшение

СТРУКТУРА ISO 27001 ПОДРОБНЕЕ

PLAN

4 Контекст организации

- Понятие контекста.
- Ожидания заинтересованных сторон.
- Область распространения СМИБ.

5 Лидерство

- Приверженность руководства.
- Политика ИБ.
- Роли, ответственность и полномочия.

6 Планирование

- Оценка риска и возможностей.
- Цели ИБ.

7 Поддержка

- Ресурсы.
- Компетенция.
- Осведомленность.
- Коммуникации.
- Документируемая информация.

DO

8 Операционная деятельность

- Планирование и контроль операций.
- Оценка рисков.
- Обработка рисков.

CHECK

9 Производительность и оценка

- Мониторинг, измерение, анализ и оценка.
- Внутренний аудит.
- Анализ со стороны руководства.

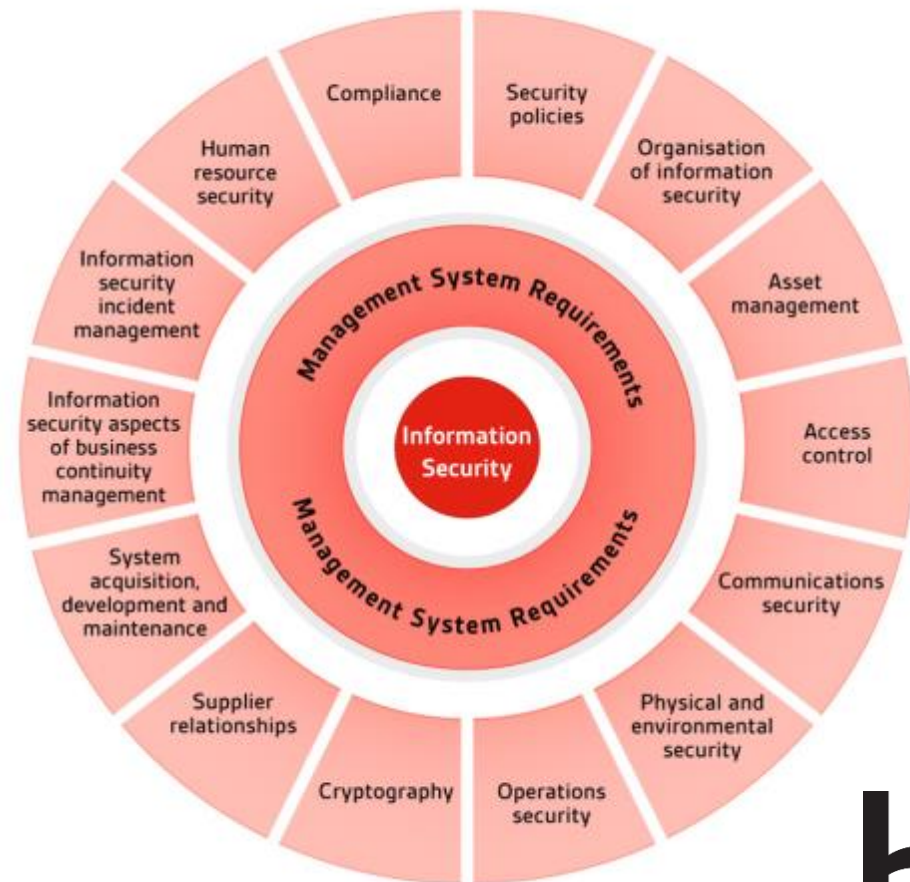
ACT

10 Улучшения

- Несоответствия и корректирующие действия.
- Постоянное улучшение.

ПРИЛОЖЕНИЕ А

- 14 доменов
- 114 средств управления



УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ПО ISO 27001

A.16.1 Management of information security incidents and improvements

- A.16.1.1 Responsibilities and procedures
- A.16.1.2 Reporting information security events
- A.16.1.3 Reporting information security weakness
- A.16.1.4 Assessment of and decision on information security events
- A.16.1.5 Response to information security incidents
- A.16.1.6 Learning from information security incidents
- A.16.1.7 Collection of evidence

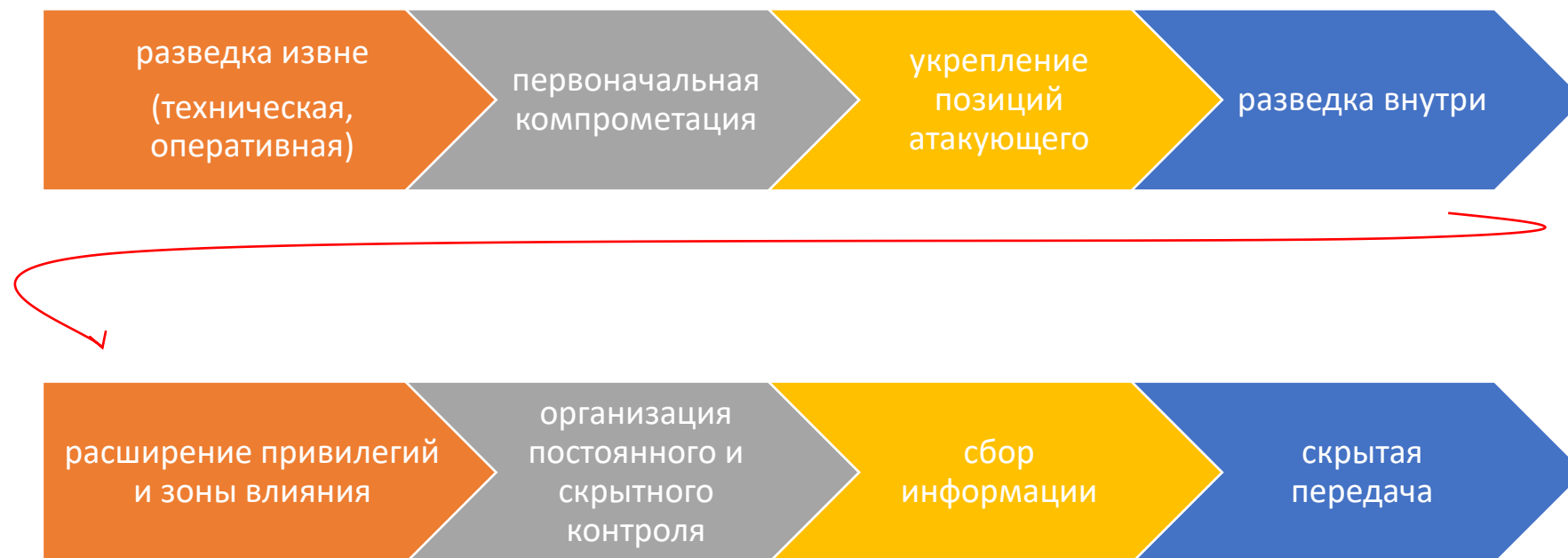
МОНИТОРИНГ СОБЫТИЙ ПО ISO 27001

A.12.4 Logging and monitoring

- A.12.4.1 Event logging
- A.12.4.2 Protection of log information
- A.12.4.3 Administrator and operator logs

Реализация требований мер ISO 27001 с помощью SIEM-системы «КОМРАД»

СОВРЕМЕННАЯ АТАКА = СПЕЦОПЕРАЦИЯ



**Как своевременно
реагировать
на таргетированные атаки?**

НЕОБХОДИМО ОТСЛЕЖИВАТЬ МАССУ ПРИЗНАКОВ НАРУШЕНИЯ ИБ



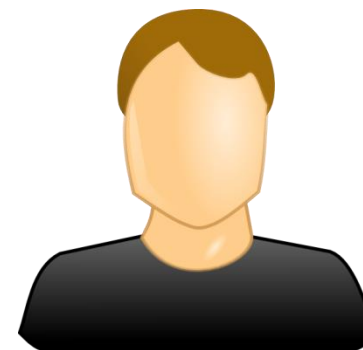
Аутентификация: как успешная,
так и неуспешная



Срабатывания
антивирусного ПО



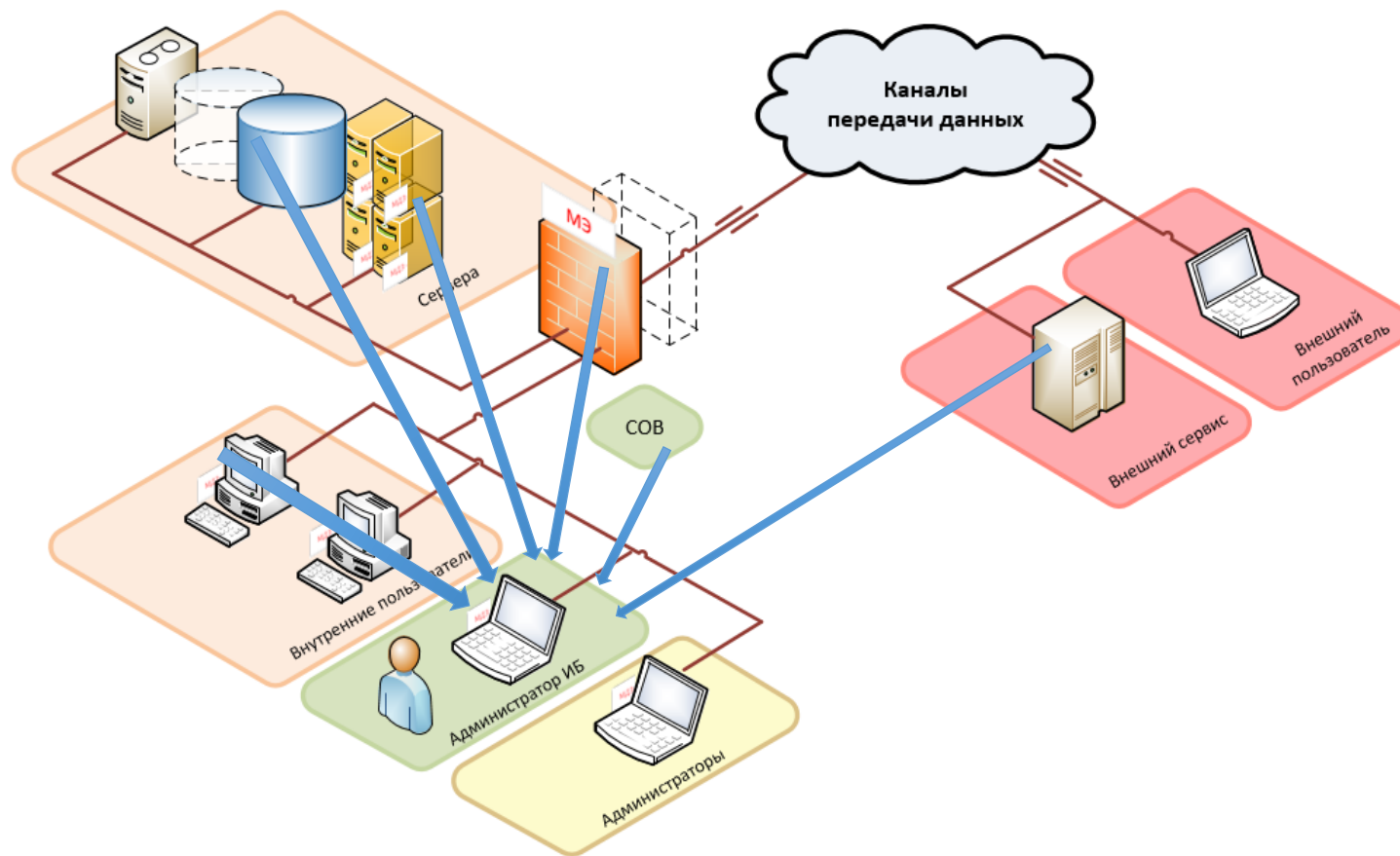
Подозрительные
запросы к СУБД



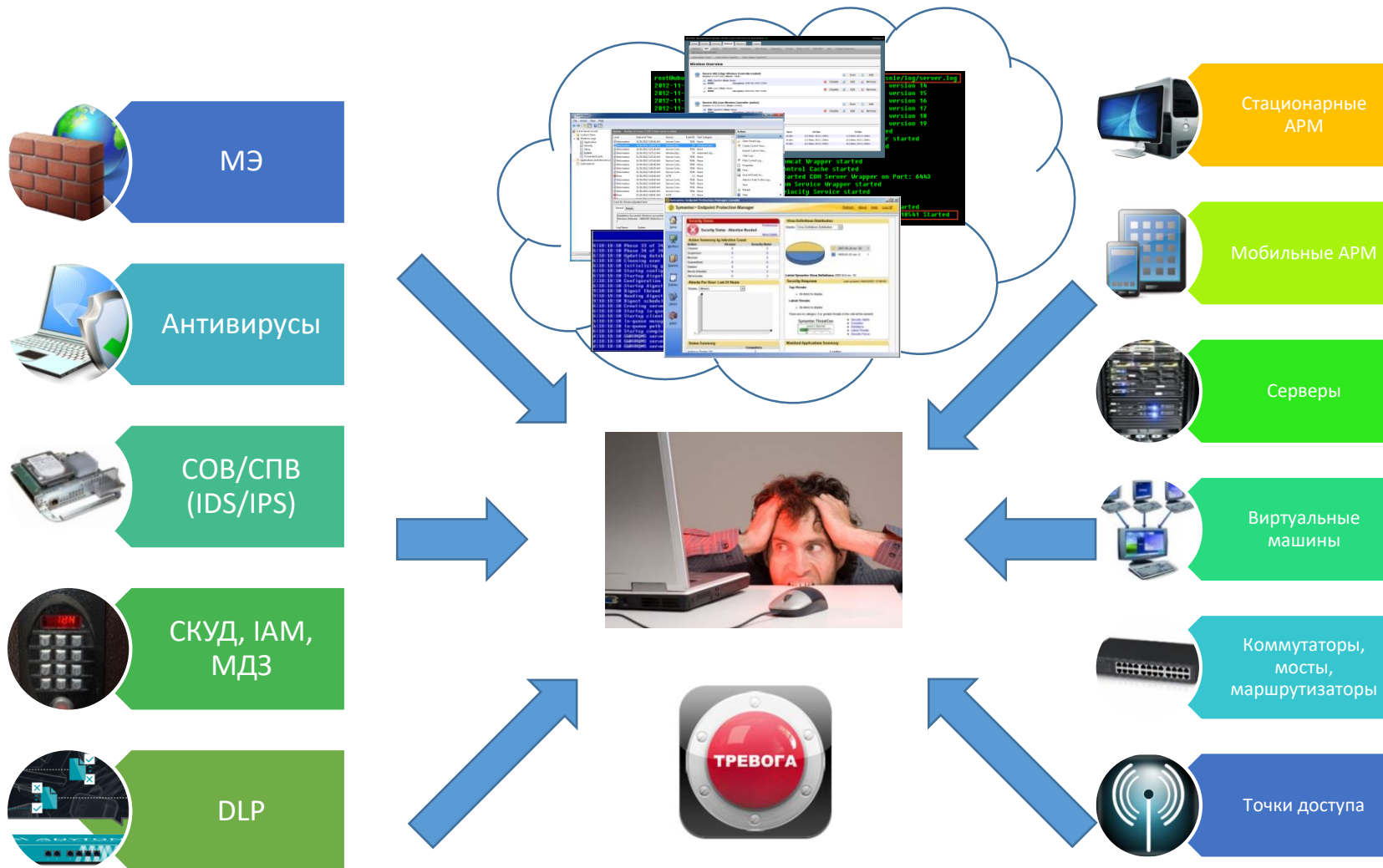
Нетипичное
поведение
пользователя в ОС

И Т.Д. И Т.П.

ДЛЯ ЭТОГО НАДО ОСУЩЕСТВЛЯТЬ МОНИТОРИНГ ВСЕЙ ИНФРАСТРУКТУРЫ



РУЧНОЙ СБОР МОЖЕТ БЫТЬ ПРОБЛЕМАТИЧНЫМ



КОМРАД

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



Сертификаты:

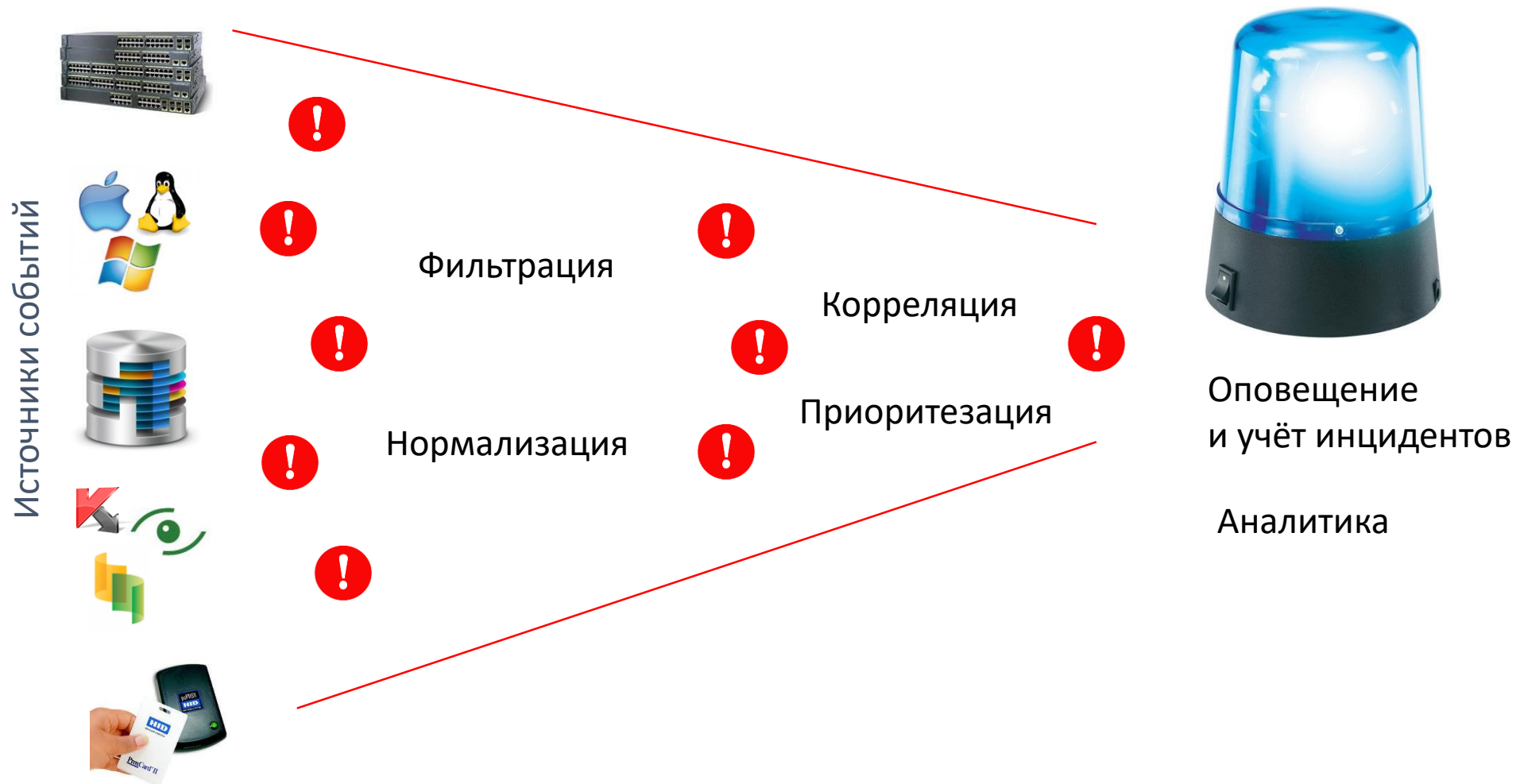


ФСТЭК России №3498

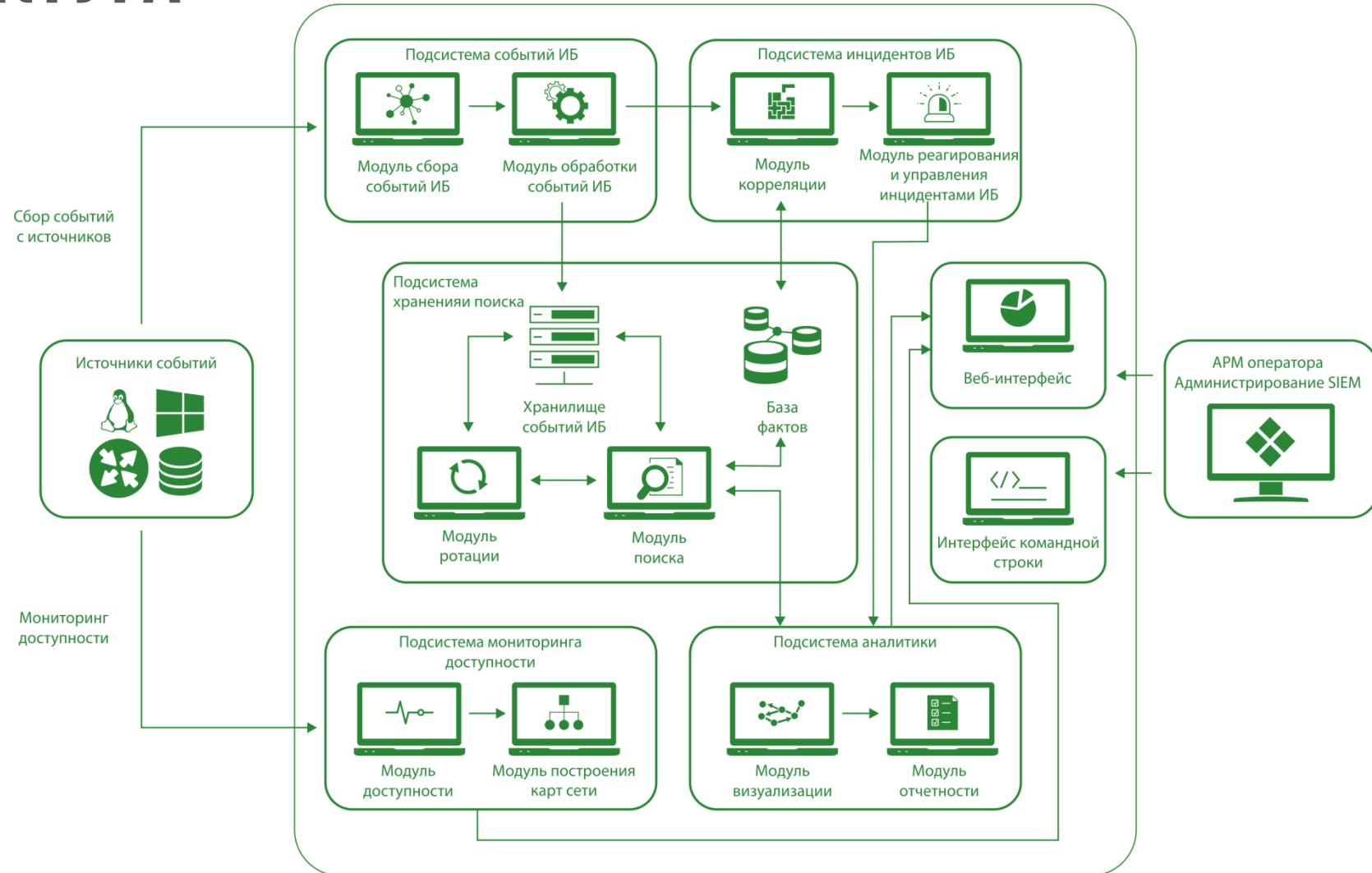


Минобороны России №2315

ПРИНЦИП РАБОТЫ SIEM-СИСТЕМЫ



АРХИТЕКТУРА



КОМРАД: ОТЛИЧИТЕЛЬНЫЕ ВОЗМОЖНОСТИ



производительность:
до 20 000 EPS



универсальный
адаптер для любого
источника событий



широкий спектр
поддерживаемых
отечественных СЗИ



удобный
пользовательский
интерфейс



визуальный анализ
данных



оповещение об инциденте
любым способом: email, SMS...

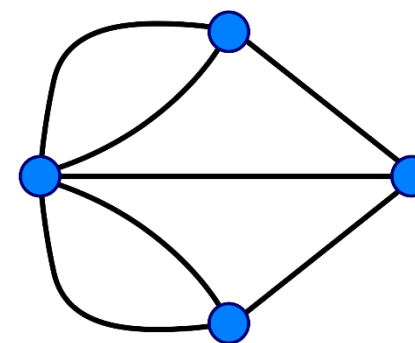
ПОДДЕРЖКА ОТЕЧЕСТВЕННЫХ СЗИ

- МЭ и СОВ «Рубикон»/«Рубикон-К»
- Сканер-ВС
- Astra Linux
- Kaspersky Security Center
- Форпост
- SecretNet 3.5-3.7 (сервер управления)
- БлокХост-Сеть
- vGate R2
- ViPNet Coordinator HW2000
- VIPNet IDS
- АССОИ «Матрица»
- ...



МЕТОДЫ КОРРЕЛЯЦИИ, ИСПОЛЬЗУЕМЫЕ В SIEM КОМРАД

- **Основанный на правилах (rule based)** — взаимосвязи между событиями определяются аналитиками в заранее заданных специфических правилах.
- **Основанный на графах (graph based)** — поиск зависимостей между системными компонентами в представлении в виде графа.



СОЗДАНИЕ НОВОГО ПРАВИЛА КОРРЕЛЯЦИИ

The screenshot shows the 'КОМРАД' (SIEM) interface. The top bar includes the logo, the name 'КОМРАД', the subtitle 'Конструктор директив', the user 'admin', and the ID '13399'. The left sidebar shows a tree view of rule categories: 'Предустановленные' (KAV, Dallas Lock, Континент) and 'Неустановлено антивиру', 'Неполная комплектация', 'Базы устарели', 'Сторонний источник баз', 'Сбой обновления', 'Остановка задачи', 'Срабатывание самозащиты', 'Срабатывание защиты', 'Ошибка активации', 'Режим ограниченной функции', 'Нарушение целостности', 'Удаление файла', 'Отключение аудита', 'Сброс мандатных уровней', 'Нарушение КС на нескольких объектах', 'Недоступность криптошифрования'.

The main area displays the configuration for 'Правило #0'. The rule is set to trigger every 1 second for 1 second. The conditions are:

- HTTP метод: равно POST
- HTTP запрос: равно /wp-login.php
- HTTP код возврата: равно 503
- Данные: содержит s3r

ПОЛЯ ДЛЯ ФОРМИРОВАНИЯ ПРАВИЛ (1)

ID плагина	АССОИ событие	CEF версия продукта	WMI категория
SID плагина	Имя шлюза	CEF ID события	WMI код события
Протокол	Тип шлюза	CEF описание	WMI причина ошибки
IP источника	Описание команды	CEF сообщение	Домашняя директория
IP назначения	Имя запроса	WMI имя компьютера	Команда
Порт источника	Имя сетевого интерфейса	WMI журнал	Действие
Порт назначения	Роль пользователя	WMI сообщение	Терминал
Имя источника	Название фильтра	WMI тип (строка)	Интерпретатор
Имя назначения	Направление трафика	WMI категория (строка)	ID пользователя
MAC источника	Адрес шлюза	WMI имя источника	ID группы
MAC назначения	CEF значимость	WMI тип события	Имя группы
Имя файла	CEF вендор	WMI номер записи	Сообщение
Имя пользователя	CEF продукт	WMI идентификатор	Категория события

ПОЛЯ ДЛЯ ФОРМИРОВАНИЯ ПРАВИЛ (2)

Сервис
Уровень тревоги
ID правила
Файл журнала
Класс COB
Группа COB
Номер CVE
Адрес ссылки
Имя тэга
Тип атаки
Имя узла
SSID шлюза
WMI идентификатор
безопасности

Событие
KAV сообщение
Результат операции
Имя шлюза
ID группы правил
Длина пакета
Приоритет правила
Классификация
Приоритет
Причина
Время отклика
Статус запроса
Код иерархии

Тип MIME
Байт передано
Комментарий
Правило
Имя компьютера
Имя сервера
Параметр
Неверный пароль
ID сигнатуры
Версия IP
Доступ
Отправлено
Получено

Информация
Длина
Объект доступа
Права
Принтер
Документ
Количество копий
Количество страниц
Порт
Тип атаки

ПРАВИЛА КОРРЕЛЯЦИИ SIEM КОМРАД «ИЗ КОРОБКИ» (1)

- 1) Xmlrpc, обнаружение PingBack-атаки.
- 2) Обнаружение межсайтового скриптинга.
- 3) Обнаружение мутированных входных данных.
- 4) Обнаружение Sql-выражений из пользовательского ввода.
- 5) Обнаружение неавторизованного Remote Code Execution-Wordpress.
- 6) Обнаружение уязвимости Local file include.
- 7) Обнаружение неавторизованного Remote Code Execution-Ping.
- 8) Обнаружение сканера уязвимостей Openvas.
- 9) Обнаружение сканера уязвимостей w3af.
- 10) Обнаружение сканера уязвимостей Acunetix.
- 11) Обнаружение исходящей активности Tor-нодов.
- 12) Обнаружение входящей активности Tor-нодов.
- 13) Обнаружение неавторизованного Content Injection-Wordpress.
- 14) Обнаружение исходящей активности на файлобменник.



ПРАВИЛА КОРРЕЛЯЦИИ SIEM КОМРАД «ИЗ КОРОБКИ» (2)

- 15) Обнаружение исходящей активности к C&C серверам.
- 16) Обнаружение исходящей активности к IRC каналам.
- 17) Обнаружение использования анонимайзеров.
- 18) Обнаружение входящей активности Mirai botnet.
- 19) Обнаружение брутфорс атаки на wordpress.
- 20) Обнаружение входящей активности crawler-ботов.
- 21) Контроль учетных записей-эскалация привилегий, создание/удаление, смена пароля.
- 22) Обнаружение брутфорс атаки на Rdp.
- 23) Обнаружения уязвимости Rdp-MaxChannelids.
- 24) Обнаружение исходящей активности к соц.сетям(vk, twitter, facebook).
- 25) Обнаружение исходящей активности Skype.
- 26) Обнаружение входящей активности Tcp-Break, таких клиентов telnet, nc
- 27) Обнаружение исходящей активности Remote Access.
- 28) Обнаружение нового пользователя в OpenVpn.
- 29) Обнаружение несоответствия сертификата в OpenVpn.
- 30) Обнаружение параллельного соединения с двух разных IP OpenVpn.
- 31) Контроль криптошлюза и обновления ключей Континента.
- 32) Нарушение целостности, удаление, отключение, контроль мандатных уровней DallasLock.
- 33) Полный контроль над KAV.



НАСТРОЙКА ПРАВИЛ КОРРЕЛЯЦИИ

Включаем сбор всего, что можем собрать с помощью SIEM-системы, и начинаем отфильтровывать лишнее.

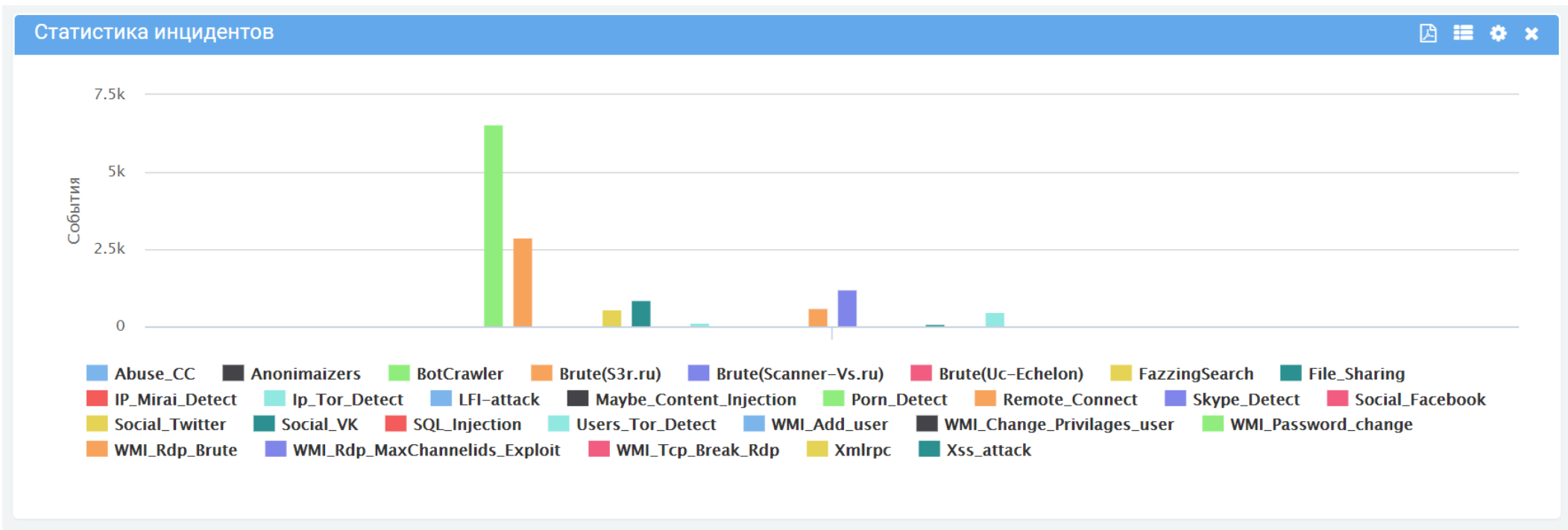


rule of thumb

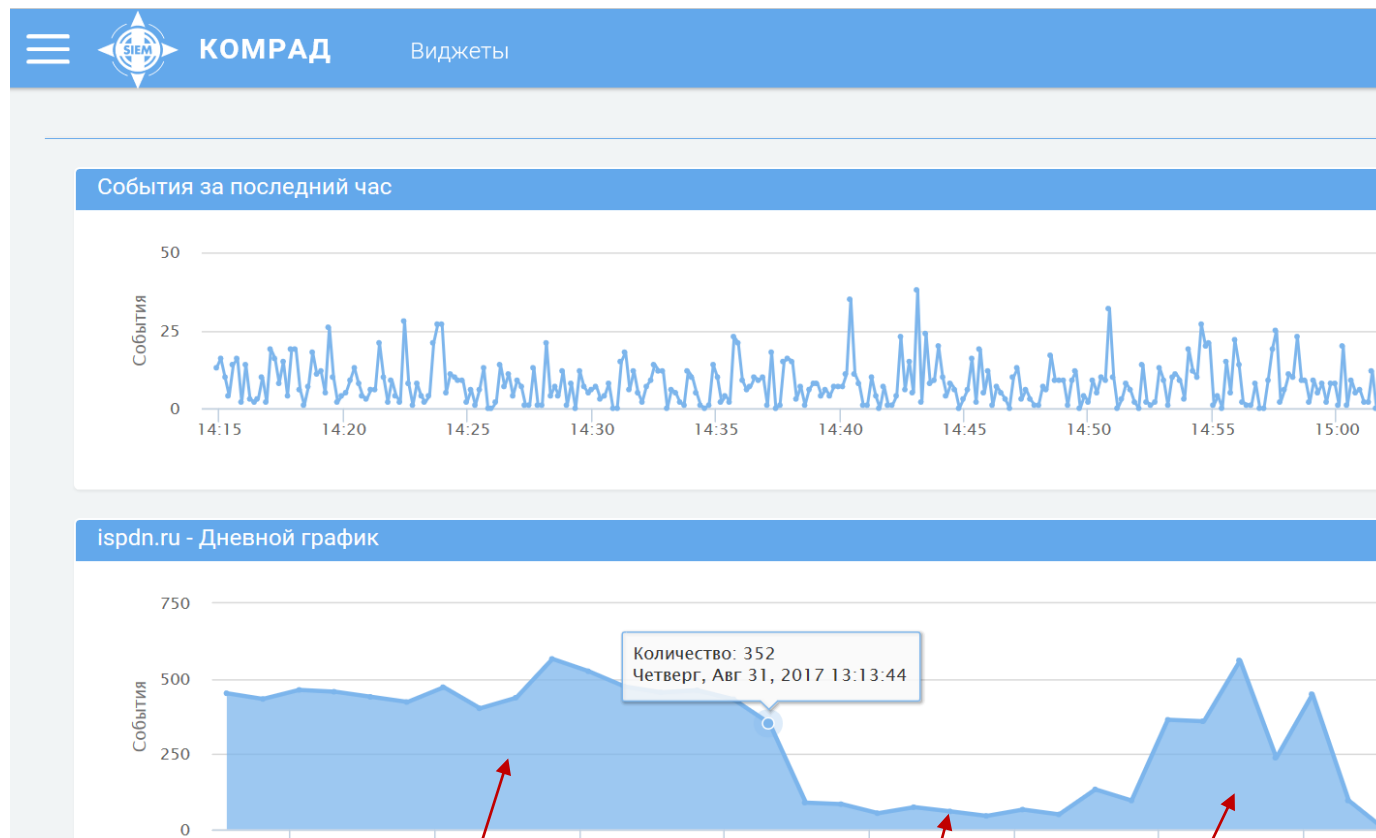
ПРАКТИКА ПРИМЕНЕНИЯ СИМ-КОМРАД В ESOC



ВСЕ ИНЦИДЕНТЫ



АТАКИ БОТОВ НА ISPDN.RU

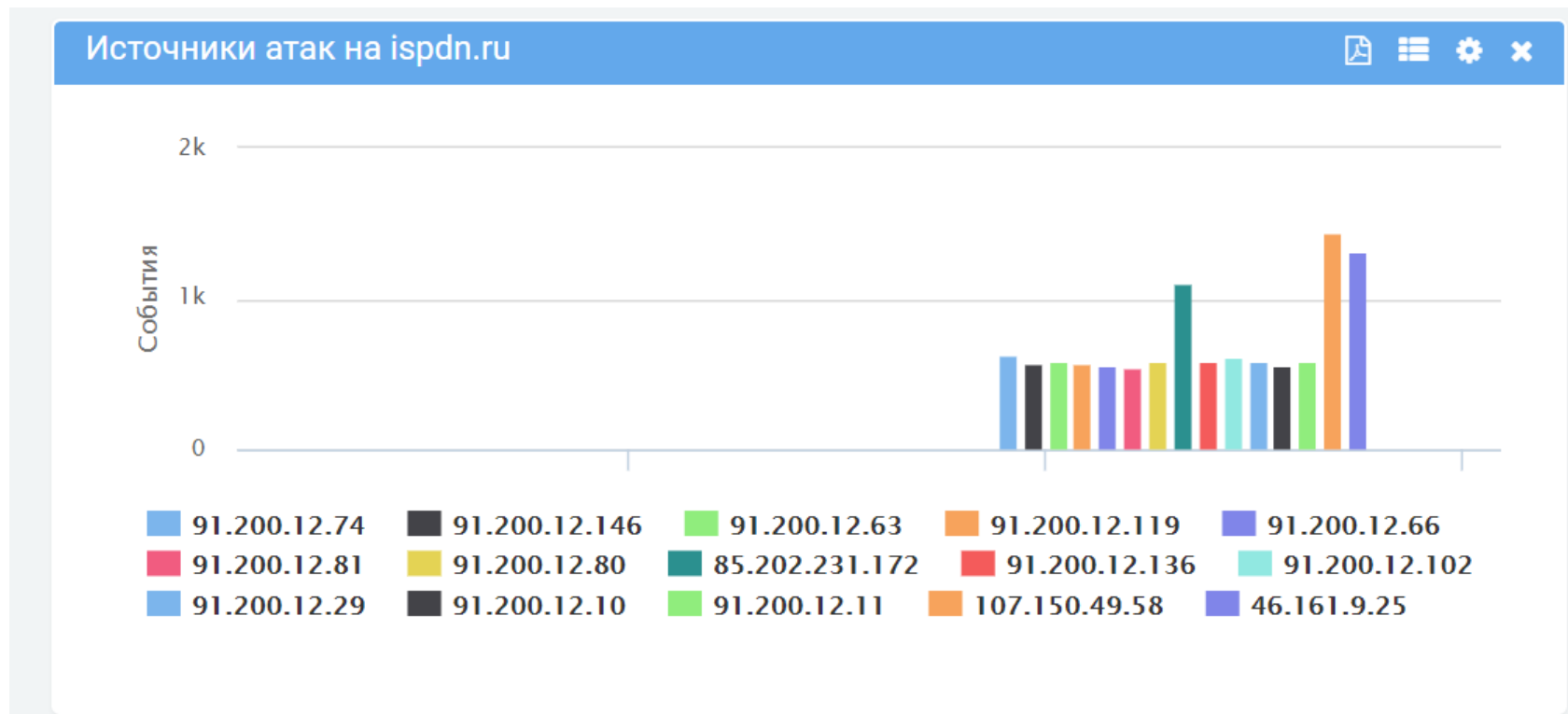


Атака

Блокировка ботов

Прорвался с нового адреса

ИСТОЧНИКИ АТАК: СОТНИ ЗАПРОСОВ В ДЕНЬ



ГОСТИ ИЗ УКРАИНЫ

СИЕМ КОМРАД Поиск по событиям admin 1339

- Причина
- Squid proxy
- Время отклика
- Статус запроса
- Код иерархии
- Тип MIME
- Байт передано
- Даллас Лок
- Комментарий
- Правило
- Имя компьютера
- Имя сервера
- Параметр
- Неверный пароль
- ID сигнатуры
- Версия IP
- Доступ
- Отправлено
- Получено
- Информация
- Длина
- Объект доступа

Данные	IP источника	источника
ispdn.ru 91.200.12.81 -- [31/Aug/2017:11:12:27 +0300] "POST /forum/forum4/topic3188/ HTTP/1.0" 302 19615 "http://ispdn.ru/forum/forum4/topic3188/" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.81 Safari/537.36"	91.200.12.81	Ukraine
ispdn.ru 91.200.12.29 -- [31/Aug/2017:11:12:17 +0300] "POST /forum/forum4/topic3188/ HTTP/1.0" 302 18757 "http://ispdn.ru/forum/forum4/topic3188/" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36"	91.200.12.29	Ukraine
ispdn.ru 91.200.12.137 -- [31/Aug/2017:11:12:07 +0300] "POST /forum/forum4/topic3188/ HTTP/1.0" 302 18839 "http://ispdn.ru/forum/forum4/topic3188/" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36"	91.200.12.137	Ukraine
ispdn.ru 91.200.12.137 -- [31/Aug/2017:11:12:04 +0300] "POST /forum/forum4/topic3188/ HTTP/1.0" 200 97114 "http://ispdn.ru/forum/forum4/topic3188/" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36"	91.200.12.137	Ukraine
ispdn.ru 91.200.12.137 -- [31/Aug/2017:11:12:03 +0300] "POST /forum/forum4/topic3188/ HTTP/1.0" 200 97114 "http://ispdn.ru/forum/forum4/topic3188/" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36"	91.200.12.137	Ukraine
ispdn.ru 91.200.12.133 -- [31/Aug/2017:11:11:55 +0300] "POST /forum/forum4/topic3188/ HTTP/1.0" 302 18839 "http://ispdn.ru/forum/forum4/topic3188/" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.81 Safari/537.36"	91.200.12.133	Ukraine
ispdn.ru 91.200.12.6 -- [31/Aug/2017:11:11:52 +0300] "POST /forum/forum4/topic3188/ HTTP/1.0" 302 18615 "http://ispdn.ru/forum/forum4/topic3188/" "Mozilla/5.0 (Windows NT 6.1; WOW64)"	91.200.12.6	Ukraine

НАШ ОТВЕТ БОТАМ: БЛОКИРОВКА ГОСТЕЙ

```
GNU nano 2.2.6 File: ispdn.ru/public_html/.htaccess

Options -Indexes
ErrorDocument 404 /404.php

#php_flag session.use_trans_sid off
php_value display_errors 0
#php_value allow_url_fopen 0

php_value max_execution_time 150
php_value memory_limit 256M
php_value upload_max_filesize 700M
php_value post_max_size 700M
php_value magic_quotes_gpc off

<IfModule mod_rewrite.c>
# Options +FollowSymLinks
RewriteEngine On
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-l
RewriteCond %{REQUEST_FILENAME} !-d
RewriteCond %{REQUEST_FILENAME} !/bitrix/urlrewrite.php$
RewriteRule ^(.*)$ /bitrix/urlrewrite.php [L]
</IfModule>
AddDefaultCharset utf-8
AddType 'text/html; charset=utf-8' .html .htm .shtml

# блокируем доступ ботам - делал Крайников
Order Deny,Allow
Deny from 91.200.0.0/16
Deny from 46.161.9.25
|
```


ВЫЯВЛЕНИЕ ПЕРЕБОРА ПАРОЛЕЙ

Скриншот интерфейса КОМРАД (Конструктор директив) для настройки правила обнаружения перебора паролей. В левой панели отображены предустановленные правила, включая KAV и Dallas Lock. В правой панели настроено правило #0 с условиями:

- HTTP метод: равно POST
- HTTP запрос: равно /wp-login.php
- HTTP код возврата: равно 503
- Данные: содержит s3r

Обращение к странице авторизации

ВЫЯВЛЕННЫЙ ПОПЫТКИ ПОДБОРА ПАРОЛЕЙ К S3R.RU

The screenshot shows the KOMRAD SIEM interface. The browser address bar displays `https://192.168.5.234/index#/correl/alerts/all`. The page title is "Инциденты" (Incidents). The user is logged in as "admin" with ID "13395".

On the left, a sidebar lists various incident categories with their counts:

- Anonimaizers: 17
- Social_VK: 68
- SQL_Injection: 16
- Users_Tor_Detect: 466
- BotCrawler: 6572
- Social_Twitter: 35
- Remote_Connect: 620
- Brute(S3r.ru): 2902
- Xss_attack: 3
- Brute(Scanner-Vs.ru): 3
- IP_Mirai_Detect: 1
- Ip_Tor_Detect: 130
- WMI_Tcp_Break_Rdp: 1
- Maybe_Content_Injection: 9
- WMI_Add_user: 1

The main area displays a table of detected incidents. The table has the following columns: "№", "Имя директивы" (Rule Name), "Дата фиксации" (Fixation Date), "События" (Events), "Длительность" (Duration), "Риск" (Risk), and "Статус" (Status). The incidents listed are all of the "Brute(S3r.ru)" type, occurring on 01/09/2017 at 06:06:40 or 06:06:39. Each incident has a count of 1 event, a duration of approximately 13 seconds, and a risk level of 0. The status column shows a yellow warning icon for the first three incidents and a red warning icon for the remaining seven.

№	Имя директивы	Дата фиксации	События	Длительность	Риск	Статус
16858	Brute(S3r.ru)	01/09/2017 06:06:40	1	00:06:13	0	⚠
16857	Brute(S3r.ru)	01/09/2017 06:06:40	1	00:06:13	0	⚠
16856	Brute(S3r.ru)	01/09/2017 06:06:40	1	00:06:13	0	⚠
16855	Brute(S3r.ru)	01/09/2017 06:06:40	1	00:06:13	0	!
16854	Brute(S3r.ru)	01/09/2017 06:06:40	1	00:06:13	0	!
16853	Brute(S3r.ru)	01/09/2017 06:06:40	1	00:06:13	0	!
16852	Brute(S3r.ru)	01/09/2017 06:06:40	1	00:06:13	0	!
16851	Brute(S3r.ru)	01/09/2017 06:06:39	1	00:06:12	0	!
16850	Brute(S3r.ru)	01/09/2017 06:06:39	1	00:06:12	0	!
16849	Brute(S3r.ru)	01/09/2017 06:06:39	1	00:06:12	0	!
16848	Brute(S3r.ru)	01/09/2017 06:06:39	1	00:06:12	0	!
16847	Brute(S3r.ru)	01/09/2017 06:06:39	1	00:06:12	0	!

ВЫЯВЛЕНИЕ ПОПЫТКИ АТАКИ ОТ ЧЕРВЯ «MIRAI»

COMRAD Конструктор директив admin 13399

Перечень директив:

- Предустановленные
 - KAV
 - Не установлено антивиру
 - Неполная комплектация
 - Базы устарели
 - Сторонний источник баз
 - Сбой обновления
 - Остановка задачи
 - Срабатывание самозащи
 - Срабатывание защиты
 - Ошибка активации
 - Режим ограниченной фу
 - Dallas Lock
 - Нарушение целостности
 - Нарушение целостности
 - Удаление файла
 - Отключение аудита
 - Сбой мандата и ур

Конструктор Реакция

Экспорт... Импорт... Сохранить директиву Приостановить

Правило #0 1 Секунд 1

И ИЛИ + Добавить + Добавить группу

IP источника из указанных Удалить

IP MIRAI

База IP-адресов, скомпрометированных MIRAI

ЧЕРВЬ ПОПЫТАЛСЯ К НАМ ЗАЙТИ...

🕒 14221

Имя директивы IP_Mirai_Detect

Риск риск 1

Статус Просмотрен

Группа default

Дата фиксации 31/08/2017 15:04:43

Дата начала 31/08/2017 15:04:37

Количество событий 1

Длительность 00:06

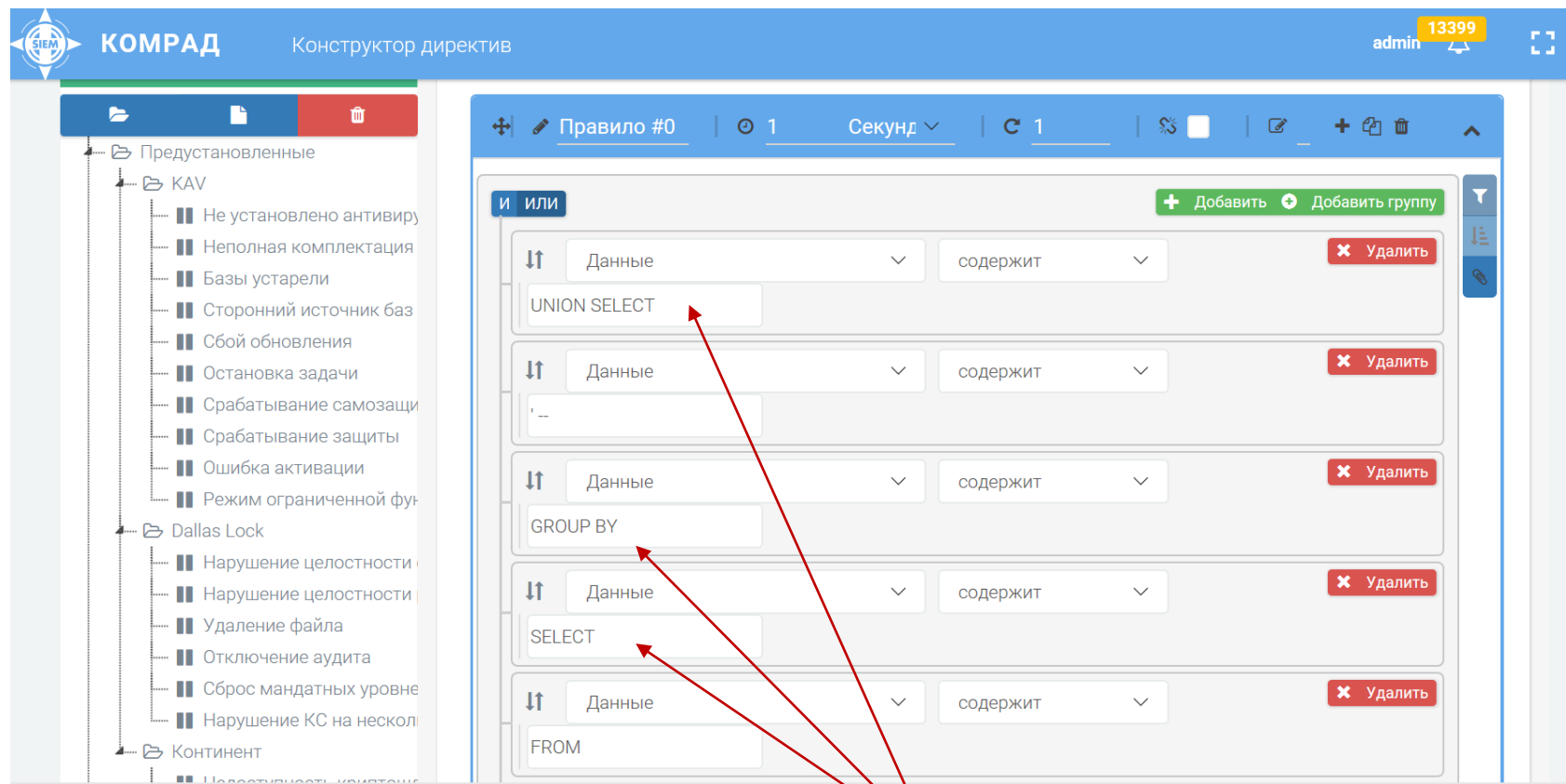
Количество событий

История изменений

Правило: Правило #0

Дата фиксации	ID плагина	SID плагина	Данные
31/08/2017 15:04:37	12506	1	ispdn.ru 158.85.81.120 -- [31/Aug/2017:15:03:41 +0300] "GET / HTTP/1.0" 200 20526 "-" "

ВЫЯВЛЕНИЕ ПОПЫТОК SQL-ИНЪЕКЦИЙ



SQL-запросы в HTTP-трафике

ПОПЫТКА SQL-ИНЪЕКЦИИ

СИЭМ КОМРАД
admin 13394
↕

5100

Имя директивы	SQL_Injection	Дата фиксации	29/08/2017 02:19:16
Риск	риск 1	Дата начала	29/08/2017 02:19:05
Статус	Просмотрен	Количество событий	1
Группа	default	Длительность	00:11

Правило: Правило #0
 Дата фиксации: 2017-08-29 02:19:05

↑
↓

02:19:05.000

Количество событий
История изменений

Правило: Правило #0

Дата фиксации	ID плагина	SID плагина	Данные
29/08/2017 02:19:05	12506	1	npo-echelon.ru 91.208.99.2 -- [29/Aug/2017:02:18:19 +0300] "GET /news/index.php?about%2Fnews%2Findex_php=&PAGEN_1=20%27%20or%20(1,2)=(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%20-%20%27x%27=%27x HTTP/1.0" 200 27589 "-" Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; elertz 2.4.179[128]; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648)*

РАЗВЕДКА И АВТОРИЗАЦИЯ

И ИЛИ + Добавить + Добавить группу

↕ ID плагина равно ✕ Удалить
1010

↕ Данные содержит ✕ Удалить
scan

И + Добавить

↕ IP источника равно ✕ Удалить
IP источника Правило #0

↕ Тип сообщения равно ✕ Удалить
sshd SSHd: Login sucessful, Acc

КОНТРОЛЬ МАНИПУЛЯЦИЙ С УЧЕТНЫМИ ЗАПИСЯМИ WINDOWS

WMI_Change_Privilages_user
WMI_Add_user
WMI_Password_change
WMI_Tcp_Break_Rdp
WMI_Rdp_Brute
WMI_Rdp_MaxCt
WMI_Remove_Us

Конструктор Реакция

Экспорт... Импорт... Сохранить директиву Приостановить

Правило #0 | 1 Секунд | 1

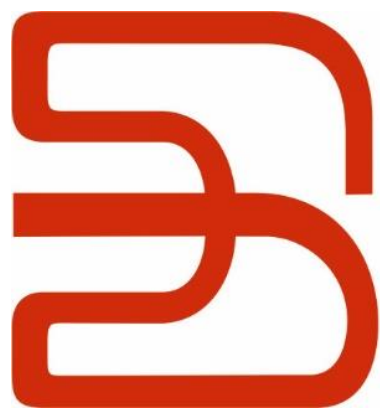
и или + Добавить + Добавить группу

WMI журнал равно X Удалить
Security

WMI код события равно X Удалить
4720

Коды специфических событий

СПАСИБО ЗА ВНИМАНИЕ!



Эшелон

комплексная безопасность