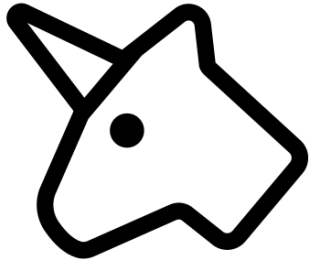


Open SysConf'19

GrayLog: от сбора логов до анализа и реакции на инциденты

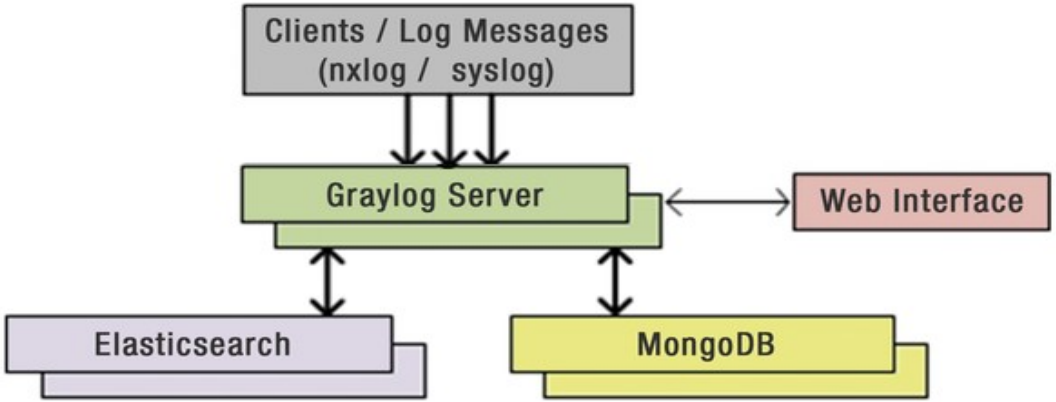
Денис Ковязин, SCM

Первые шаги

С помощью мануала GrayLog вы установили:

http://docs.graylog.org/en/3.1/pages/installation.html

И он даже может собирать логи через input syslog (udp:5139) и GELF (udp:12201):



Первые шаги

Вы сконфигурировали клиентов и они отправляют данные на ваш Graylog:

Linux:

```
cat /etc/rsyslog.conf | grep \@
authpriv.*
@10.11.12.13:5139
*.alert                         @10.11.12.13:5139
*.emerg                         @10.11.12.13:5139
*.critical                      @10.11.12.13:5139
*.error                         @10.11.12.13:5139
*.warning                       @10.11.12.13:5139
```

Cisco:

```
show run | inc logg
logging buffered informational
logging trap debugging
logging origin-id hostname
logging facility syslog
logging 10.11.12.13 transport udp port 5139
```

Windows:

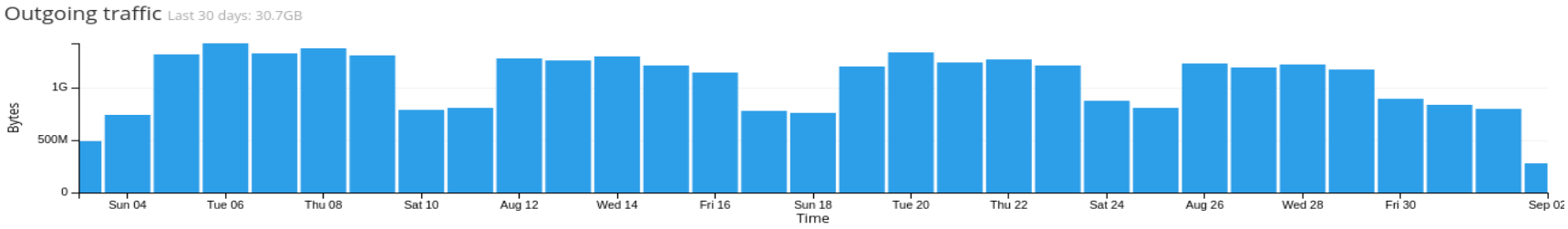
```
<Extension gelf>
Module xm_gelf
</Extension>

<Input in>
    Module      im_msvistalog
</Input>

<Output out>
Module om_udp
Host 10.11.12.13
Port 12201
OutputType GELF
</Output>

<Route 1>
    Path        in => out
</Route>
```

Первые проблемы

1) Данные приходят в Graylog, но их много и они недостаточно структурированы.

2) Необходимо регулярно анализировать собраные данные, но непонятно как

3) Нужны уведомления о наиболее критичных событиях



Что говорят стандарты (NIST)

Активность пользователей

- **Мониторинг успешных входов в систему за 30 дней**
- **Список активных пользователей (*)**
- **Появление в списке любого неожиданного аккаунта требует расследования (например, дефолтные аккаунты которые должны быть отключены)**
- **Создание, удаление, модификация пользователей**
- **Создание, удаление, модификация групп пользователей**
- **Доступ к встроенные учетным записям**
- **Попытки доступа через отключенные и неизвестные аккаунты**
- **Доступ привилегированных аккаунтов и изменения в конфиге**
- **Доступ сервисных аккаунтов (доменные учетные записи серверов БД, приложений и т.п.)**

***- Graylog не решает данную проблему**

Что говорят стандарты (NIST)

Отчеты

- **Доступ через через недоверенные сети (VPN / WLAN)**
- **Top 10 целей**
- **Top 10 атакующих**
- **Top 10 атак (сигнатур)**
- **Доступ в интернет с критичных сетевых устройств (за которыми не должны работать пользователи или по крайней мере не пользоваться доступом в интернет)**
- **Текущий список открытых инцидентов (*)**
- **Текущий список закрытых инцидентов (*)**
- **Время разрешения инцидентов (*)**

***- Graylog не решает данную проблему**

Что есть “из коробки”?

1) Сообщения от Linux / Cisco / NetApp и т.п. получаемые в syslog-input имеют только базовые поля facility и severity

2) Сообщения от Windows-систем получаемые в GELF-input, достаточно хорошо структурированы, так как в основе EventLog в Win2008 и выше используется XML

3) В Graylog экстракторы входят GROK и RegExp паттерны, позволяющие извлекатьиз поля message типовые значения типа адресов IPv4, MAC-адресов, mnemonic,local_level, local_facility

4) Можно создать дополнительно экстракторы на основе Regexp-паттерн для извлечения любой другой информации из поля message

Что нужно сделать дополнительно?

1) Разбить данные на потоки (Stream) чтобы структурировать данные получаемые от однородных ОС и прикладных систем, умеющих отсылать самостоятельно события в Syslog (например, McAfee EPO)

2) Дописать regexp экстраторы для извлечения данных в syslog сообщения для формирования уведомлений и отчетов согласно требованиям стандарта

3) По критериям NIST создать Dashboard / Search query (для отчетов)

4) По критериям NIST и собственным требованиям сформировать уведомления по тревогам (например, для отслеживания brute-force атак)

Разбиваем данные на потоки

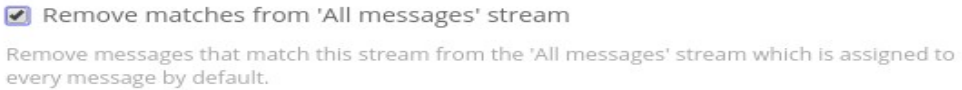
Выводить данные в отдельный поток имеет смысл в той ситуации, когда структура данных имеет различия. То есть, если у вас собираются данные с 4-х категорий устройств:

- **Устройства с Cisco IOS**
- **Windows серверы**
- **Linux-серверы**
- **SNMP модули ИБП**

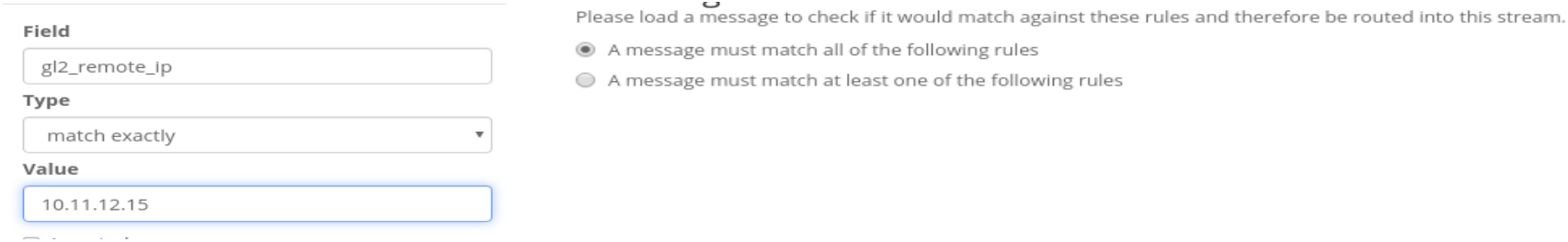
То вам желательно разбить данные на 4 потока. В качестве критерия выделения в поток, можно использовать любое поле сообщения, часто это ip адрес клиента (Field gl2_remote_ip must match exactly 10.12.13.14)

Разбиваем данные на потоки

При создании потока желательно указать, что отобранные сообщения необходимо убрать из потока “All Messages”



Создав поток, нужно выбрать критерии отбора (любое из полей сообщения) и указать оператор объединения условий (AND / OR):

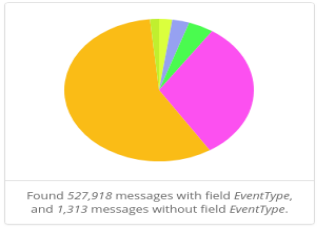


Анализируем события

Прежде чем дописывать экстракторы, нужно понять, каких данных не хватает. Для этого необходимо пройтись по потокам и выяснить, какие сообщения нас интересуют. Хорошей отправной точкой будет формирование диаграмм Quick Values по полю severity (и аналогичным) для определение наиболее важных событий:

Quick Values for *EventType*

Add to dashboard ▾ Customize ▾



Found *527,918* messages with field *EventType*, and *1,313* messages without field *EventType*.

Value	%	Count
Top 5 values		
AUDIT_SUCCESS	57.44%	303,216
INFO	31.57%	166,643
WARNING	4.29%	22,670
ERROR	2.93%	15,445
VERBOSE	2.24%	11,802
Others		
AUDIT_FAILURE	1.54%	8,140
CRITICAL	0.00%	2

Примеры запросов для быстрого поиска важных событий

Windows: EventType:(ERROR OR AUDIT_FAILURE)

Syslog: Severity<=3

Cisco IOS: local_level:<=3

Пишем экстракторы

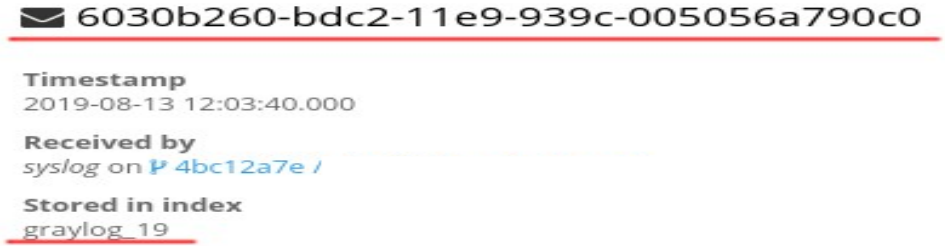
Банальная ситуация: есть интересные события, но хочется их анализровать по своим критериям. Например, какие аккаунты стучались на sshd и с каким результатом.

Текстовым поиском по слову sshd находим сообщение:

server0037 sshd[24007]: Failed password for someuseraccount from 10.11.14.15 port 37424 ssh2

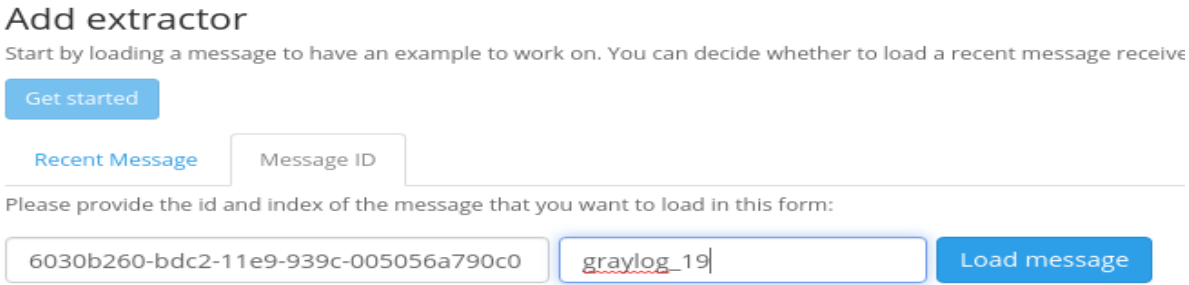
Можно, конечно, гордо нажать Save search criteria

Но с аналитикой потом будут проблемы. Поэтому мы напишем regexp экстракторы. Для начала, нужно узнать ID сообщения и имя index. Все эти параметры будут доступны при открытии сообщения



Пишем экстракторы

При создании экстратора укажем input и сообщение, на котором мы будет тестировать экстратор:



После загрузки, укажем, что будет создаваться regular expression экстрактор для поля message, кнопка Try поможет с проверкой regexp:

Примеры экстракторов

IOS destination IPv4: "[dst|to].*:([0-9]+.[0-9]+.[0-9]+.[0-9]+)/.*"

IOS config admin: "Configured\ from\ console\ by (.*?)\ on"

IOS interface: : "Ethernet(.*?)\,"

ASA destination IPv4: "\-\>\ .*\/([0-9]+.[0-9]+.[0-9]+.[0-9]+)\("

Linux auditctl rhost:"regex_value": "rhost=(.*?)\ "

Linux auditctl user: "regex_value": "\ user\=(.*)?"

Linux auditctl PAM module: "pam.*?\((.*?)\)"

Linux sshd user: "sshd.*\ password\ for\ (.*?)\ "

Linux sshd result: "sshd.*\: (.*?)\ password"

Linux block device error: "error\ on\ dev\ (.*?)\,"

Формируем отчеты и уведомления

Чтобы сформировать отчеты, необходимо определиться с кодами интересующих нас и NIST событий

Windows:
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor

Cisco ASA:

https://www.cisco.com/c/en/us/td/docs/security/asa/syslog/b_syslog/syslogs-sev-level.html

Cisco IOS:

https://www.cisco.com/en/US/docs/security/asa/asa80/system/message/logmsgs.pdf

Linux: лучше продолжать искать по severity

Формируем отчеты и уведомления

Windows (должен быть включен аудит, поле EventID)

Категория	Коды событий
Операции с аккаунтами пользователей	4720 – создание 4722 – включение 4723 – установка пароля 4725 – отключение 4726 – удаление
Операции с группами	4727,4754 – создание 4735,4737,4755 – модификация 4764 – удаление
Доступ (все виды логона)	4624 – успех 4625 – отказ
Привилегированный доступ	4672,4673,4674
Изменения объектов в AD(включая GPO)	5136 - модификация 5137 – создание 5141 - удаление

Формируем отчеты и уведомления

Cisco IOS (поле mnemonic, помимо local_level:<=2)

Категория	Коды событий
Логон	sec_login-4-login_failed
Изменения конфига	sys-5-config*
Отключение порта по port-securty	pm-4-err_disable
ACL запрет	sec-6-ipaccesslogp
WLAN достижение максимума попыток подключения к WLAN	dot11-4-maxretries
Ошибки Dynamic ARP Inspection	sw_dai-4-dhcp_snooping_deny

Формируем отчеты и уведомления

Cisco ASA (поле mnemonic, помимо local_level:<=2)

Категория	Коды событий
ACL запрет	asa-4-106023
ACL менеджмент-протокола запрет	asa-3-106100
IP Spoof / ассиметричный ответ (uRPF)	asa-2-106016
Teardrop	asa-4-400009
SLA монитор смена статуса	asa-3-622001
IPSEC проблема аутентификации peer	asa-3-713167
SSLVPN проблемы аутентификации и авторизации	/asa-3-7510[0-1][0-9]/

Формируем отчеты и уведомления

Самые простые инстументы для автоматического формирования отчетов – Saved Search и Dashboard. Запрос, который нас интересует – неуспешные попытки авторизации (EventID:4625) под встроенной учетной записью Administrator (TargetUserName:Administrator). Поисковый запрос будет иметь вид:

EventID:4625 AND TargetUserName:(administrator OR ADMINISTRATOR)

Если устроит вывод в табличном виде, достаточно нажать

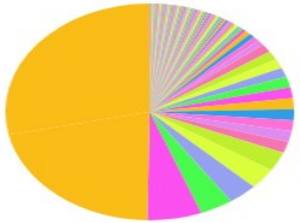
Поисковый запрос сохранится в

Формируем отчеты и уведомления

Можно пойти дальше и сделать автоматически обновляемые Dashboard. Удобно для всяких Top n*. к примеру, если нас интересует Top-100 внешних Src IP атакующих Cisco ASA за 1 месяц, то данный запрос решает эту задачу:

ASAInterface:Outside AND mnemonic:(asa-3-106100 OR asa-4-106023) AND !IPV4:10.*

- **Выберем период (relative, 30 days)**
- **В Quick Values выберем IPV4**
- **После формирования диаграммы жмем Add to Dashboard**
- **После добавления, приводим диаграмму к тому виду, который нам нужен в Dashboards (количество значений, сортировка top/bottom, тело запроса, временной период и т.п.)**



Value	%	Count
Top 100 values		
92.118.37.67	21.35%	65,898
185.254.122.18	6.08%	18,778
185.254.122.40	3.72%	11,475
185.143.221.214	3.29%	10,147
185.254.122.21	3.12%	9,621
77.247.108.187	2.92%	9,002

*** Формирование диаграммы bottom по mnemonic дает хорошую возможность определить наиболее редкие события и найти аномалии**

Формируем отчеты и уведомления

Уведомления на e-mail штатно поддерживаются Graylog, процедура настройки отправки через SMTP relay хорошо описана в документации:
https://community.graylog.org/t/how-to-send-email-alerts-using-gmail/4103

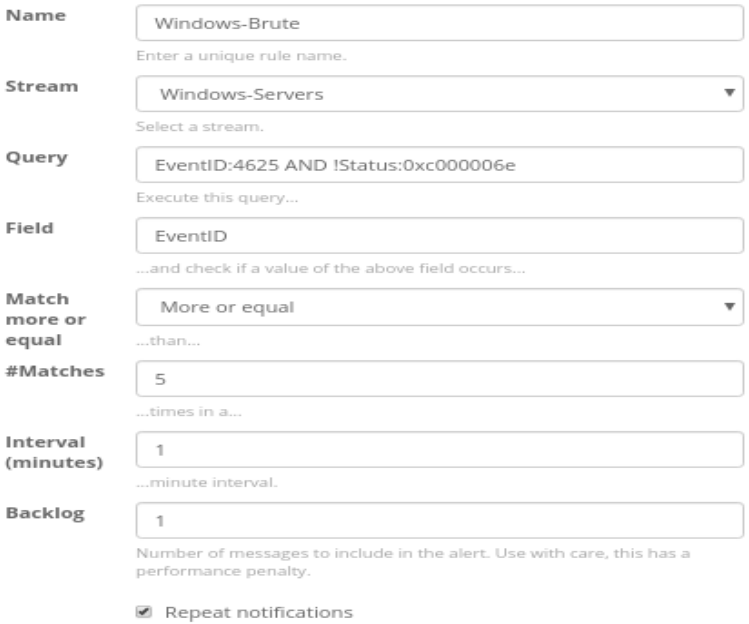
Однако часто возникает задача генерировать сообщение по более гибкому условию – например, N событий за M минут. Штатно, такого функционала нет, но он легко добавляется плагином Aggregates из Graylog Marketplace

https://marketplace.graylog.org/addons/0d01a899-138a-4f77-a9e7-04be4cc5e190

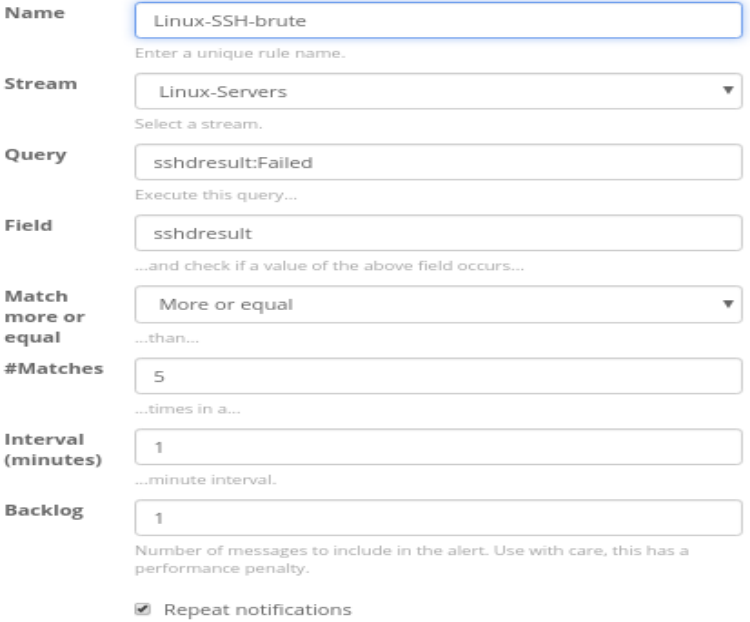
Разберем пример конфигурации правила и создания уведомления типа: пять неуспешных попыток авторизации – отправка e-mail

Формируем отчеты и уведомления

Windows



Linux



*** - не создавайте правил с Field=message. Пишите экстрактор нужного параметра**

Формируем отчеты и уведомления

Aggregates сразу создает Alert conditions, остается создать шаблоны уведомления для каждого потока

Syslog stream

body: Stream description: ${stream.description} Alert Condition Title: ${alertCondition.title} ${if stream_url}Stream URL: ${stream_url}${end} ${if backlog}Last messages accounting for this alert: ${foreach backlog message} ${message.timestamp} ${**message.message}** ${end}${else}<No backlog> ${end}

email_receivers: <empty>

sender: graylog@domain.tld

subject: Graylog alert for stream: ${stream.title}: ${check_result.resultDescription}

GELF stream

body: Stream description: ${stream.description} Alert Condition Title: ${alertCondition.title} ${if stream_url}Stream URL: ${stream_url}${end} ${if backlog}Last messages accounting for this alert:${foreach backlog message}${message.timestamp}${**message.message}${message.fields.full_message}**${end}${else}<No backlog>${end}

email_receivers: <empty>

sender: graylog@domain.tld

subject: Graylog alert for stream: ${stream.title}: ${check_result.resultDescription}

Примеры реализации требований NIST

Активность пользователей

- **Мониторинг успешных входов в систему за 30 дней=EventID:4624**
- **Появление в списке любого неожиданного аккаунта требует расследования (например, дефолтные аккаунты которые должны быть отключены)=EventID:4624 AND !TargetUserName:/ID.*/ (ID.* префикс в соответсвии с системой именования аккаунтов)**
- **Создание, удаление, модификация пользователей=EventID:/472[0-6]/**
- **Создание, удаление, модификация групп пользователей=EventID:(4727 OR 4754 OR 4735 OR 4737 OR 4755 OR 4764)**
- **Доступ к встроенным учетным записям=EventID:(4624 OR 4625) AND TargetUserName:(administrator or ADMINISTRATOR)**
- **Попытки доступа через отключенные и неизвестные аккаунты=EventID:4625 AND (locked OR disabled)**
- **Доступ привилегированных аккаунтов и изменения в конфиге =EventID:/467[2-4]**

Примеры реализации требований NIST

Отчеты

- **Доступ через через недоверенные сети:**
- **VPN=mnemonic:/asa-3-7510[0-1][0-9]/ OR mnemonic:asa-3-713167**
- **WLAN=mnemonic:dot11-4-maxretries (мониторинг отказов в подключении)**
- **Top 10 целей=ASAInterface:Outside AND mnemonic:(asa-3-106100 OR asa-4-106023) AND ASADst:(10.* OR 1.2.3.14*) [1.2.3.14* блок внешних IP]**
- **Top 10 атакующих=ASAInterface:Outside AND mnemonic:(asa-3-106100 OR asa-4-106023) AND !IPV4:10.***

*** Отчеты по атакам всегда специфичны для для систем предотвращения вторжений. Под каждую конкретную систему необходимо писать экстракторы, затем выводить данные по извлеченным полям в отчет.**

**** Доступ в недоверенные сети из критичных сетей также пишется отдельно с учетом правил сегментации сети с привязкой к диапазонам IP конкретных сегментов.**

Реакция на инциденты

Вариант 1:

Вариант 2: