

< Teach
Me
Skills />

Event Management

Вопросы по предыдущим темам или ДЗ

Mini-quize по прошлым темам:

1. Какие сайты вы бы использовали для получения информации о CVE?
2. Что в себя включает Vulnerability management?
3. Что выполняет команда scp в linux?
4. Что такое CyberKillChain?

Mini-quize по новой теме:

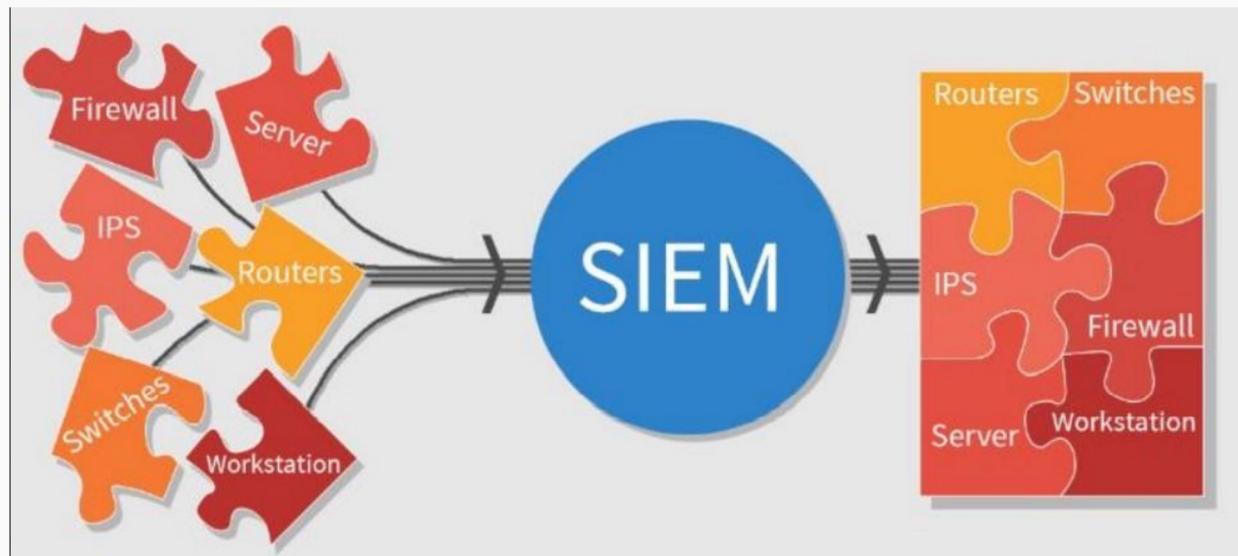
1. Какая главная метрика в SIEM?
2. Что такое нормализация данных?
3. Что такое обогащение данных?
4. Какие виды архитектур установок SIEM вы знаете?
5. Что такое Zabbix и для чего он нужен?

План занятия

1. SIEM системы
2. Источники данных
3. Методы оповещения
4. Анализ и метрики
5. Сбор syslog, auditd
6. Zabbix, Logstash, Elasticsearch

Что такое SIEM?

SIEM (Security Information & Event Management) – система сбора и анализа логов с возможностью корреляции множества разнородных событий в единый инцидент.



Рынок SIEM

splunk>



ArcSight

LogRhythm®



ELK Stack



MaxPatrol
SIEM

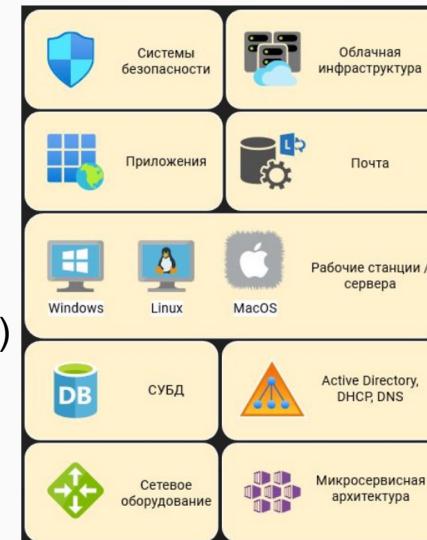
Функциональная схема SIEM: Источники данных
Источник данных для мониторинга безопасности – логи:

- Клиентские ОС
- AD\DHCP\DNS
- Антивирус
- Межсетевые экраны
- Прокси
- IPS\IDS
- VPN
- Mail
- Web-сервера
- Applications
- СКУД
- Программы по предотвращению утечки информации (DLP)
- Сетевые устройства
- Инвентаризационные выгрузки
- Отчёты об уязвимостях

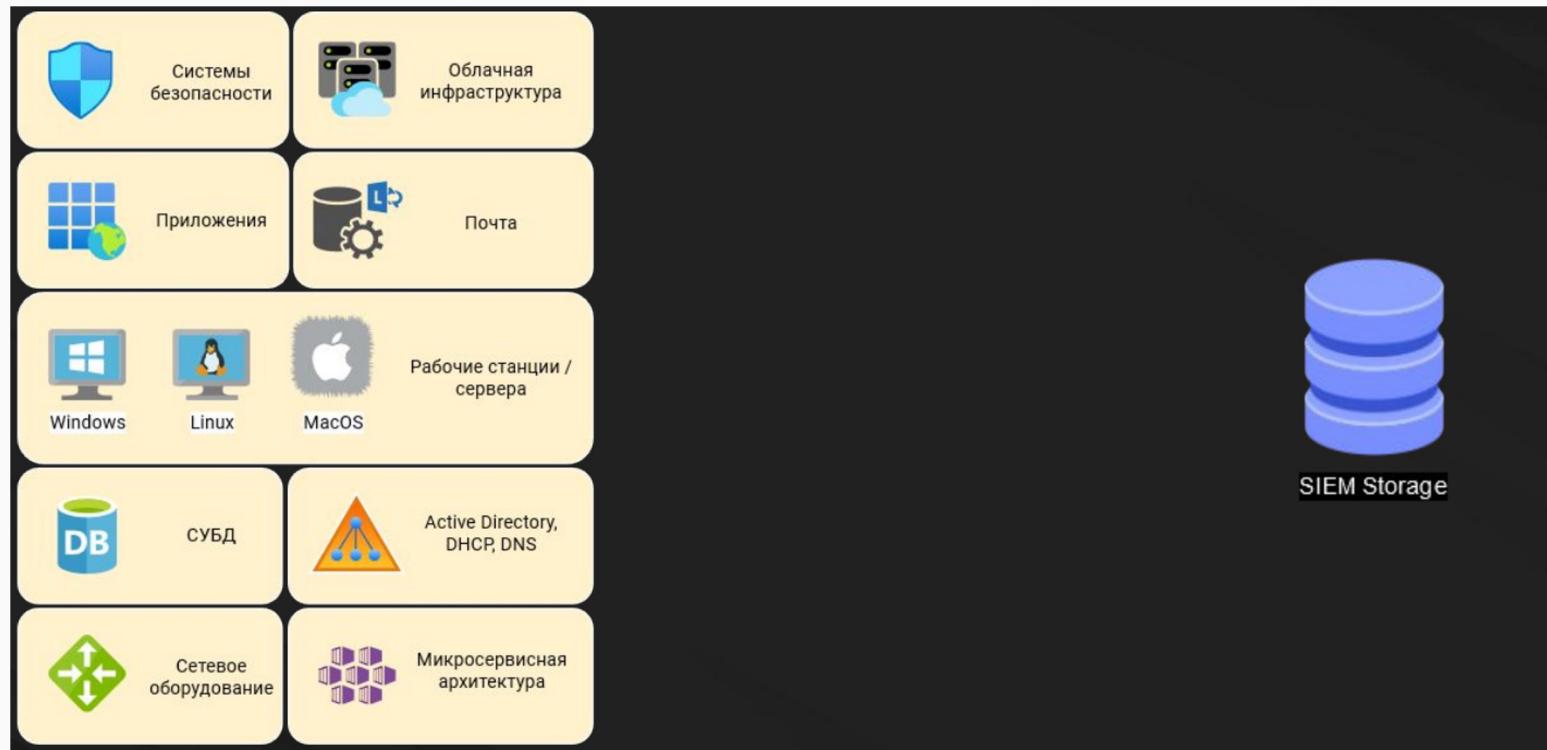
И так далее....

Источники данных

Информация собирается из многих источников и анализируется по заранее установленным критериям.

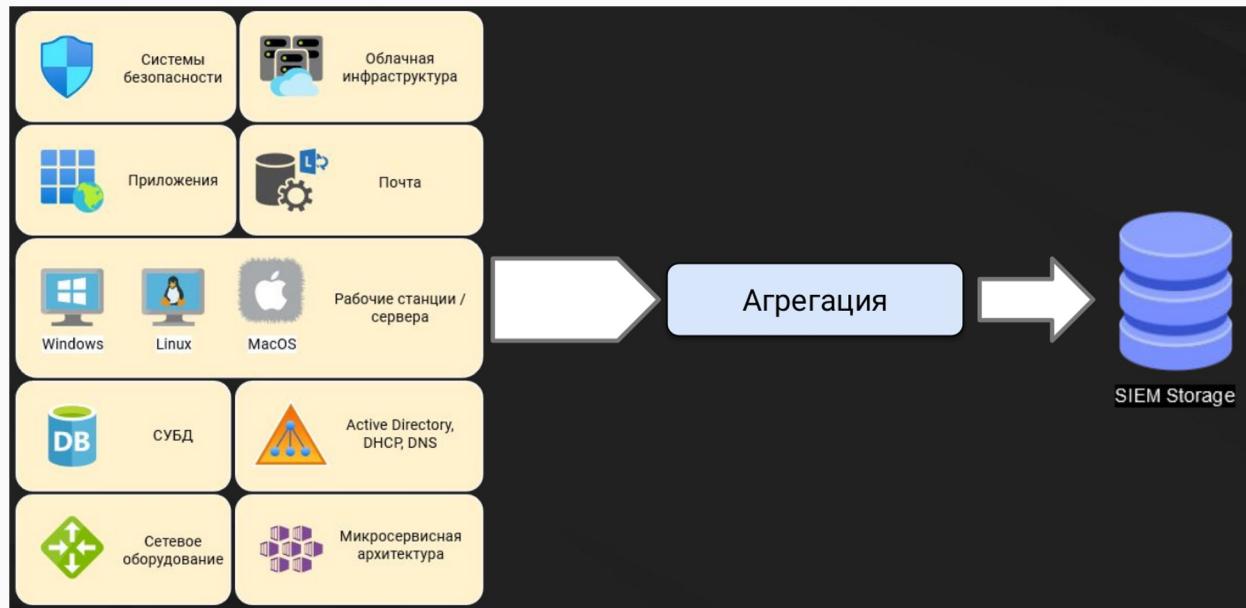


Функциональная схема SIEM: Хранение данных



Функциональная схема SIEM: Агрегация

- Централизованное хранилище данных
- Логи поступают из множества разнородных источников



Функциональная схема SIEM: Механизмы загрузки логов

Для каждой SIEM-системы всё индивидуально – зависит от набора предоставляемых коннекторов.

Наиболее распространённые способы загрузки данных:

- TCP/UDP, Syslog – передача данных по сети (транспортный уровень)
- HTTP
- Файлы
- Системные журналы
- Базы данных – возможность делать выгрузки из БД
- Скрипты
- контейнеров / подов

Event Management

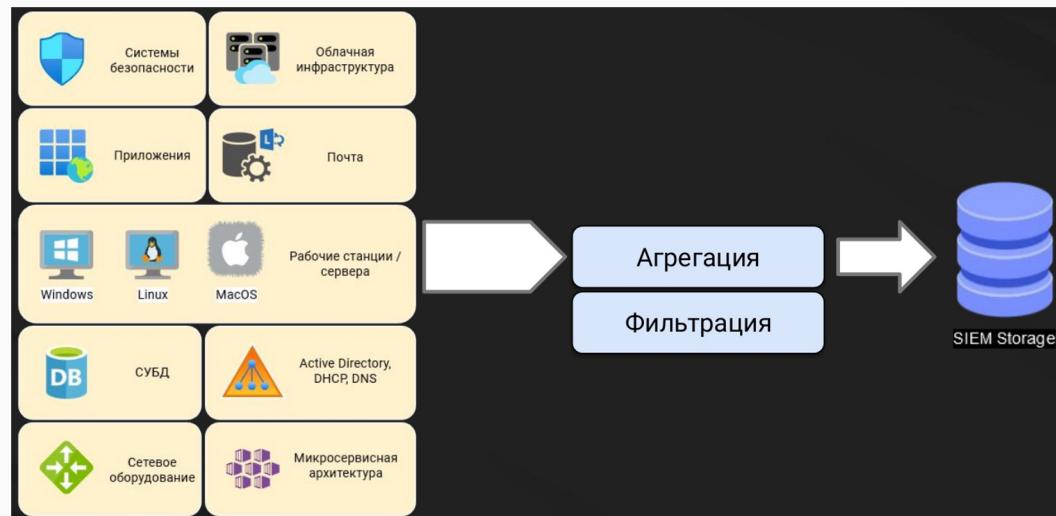
Функциональная схема SIEM: Фильтрация

Логи, которые не представляют фактической полезности с точки зрения ИБ, хранить в SIEM бессмысленно.

Пример (в редких случаях бывают полезны для ИБ):

- WARNING / ERROR / DEBUG / TRACE

Здесь нам помогает фильтрация.



Event Management

Функциональная схема SIEM: Парсинг

Разнообразие форматов данных:

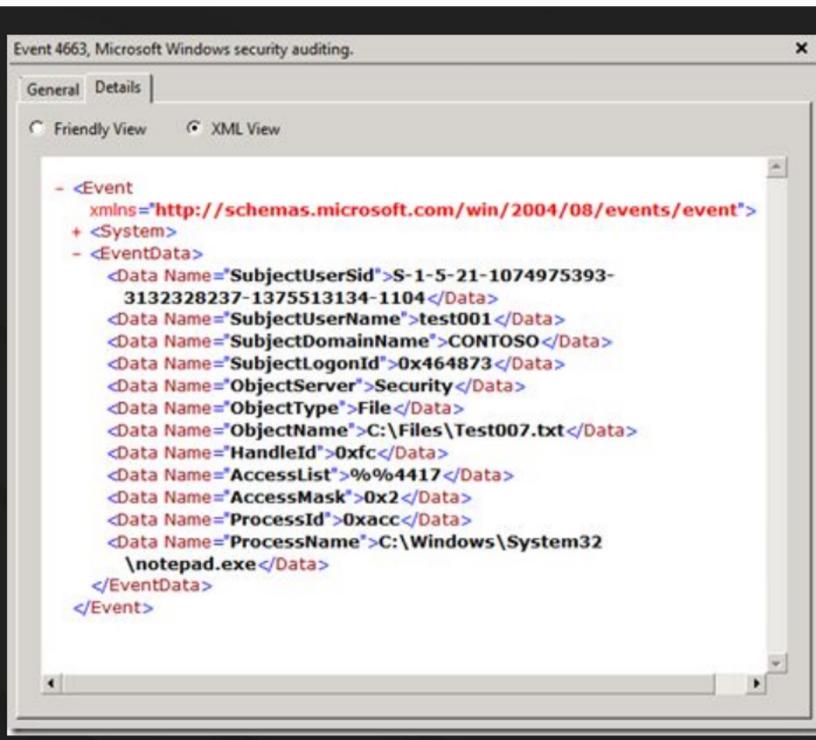
- JSON
- XML
- Syslog
- CEF
- CSV
- TSV (Tab-separated)
- Key-value
- W3C
- и так далее

Тяжелее всего парсить неструктурированные логи.

$$\begin{aligned} f(\omega) &= \int_{-\infty}^{\infty} f(x) e^{-2\pi i x \omega} dx \quad \text{with } \mathcal{F} = \frac{1}{2\pi} F \omega \\ \nabla E = 0 &\quad \nabla_x E = -\frac{1}{c} \frac{\partial H}{\partial t} \quad \nabla_t H = \frac{1}{c} \frac{\partial E}{\partial t} \\ \frac{\partial^2}{\partial t^2} \Psi &= H \Psi \\ p \left(\frac{\partial V}{\partial t} + V \cdot \nabla V \right) &= -\nabla p + \nabla \cdot T + f \\ H &= -\sum_{i=1}^n p(x_i) \log p(x_i) \\ \frac{1}{2} G^2 S^2 \frac{\partial^2 V}{\partial S^2} + r S \frac{\partial V}{\partial S} + \frac{\partial V}{\partial t} - r \cdot V &= 0 \\ \frac{\partial}{\partial t} \left[\frac{D_i}{m_i} S_i + C_i D_i + \frac{q_i H_i}{2} \left(m_i \left(1 - \frac{D_i}{P_i} \right) - 1 + 2 \frac{D_i}{P_i} \right) \right] &+ \\ TC(Q, q_i, m_i) &= \sum_{i=1}^n \left[\frac{D_i}{m_i} S_i + C_i D_i + \frac{q_i H_i}{2} \left(m_i \left(1 - \frac{D_i}{P_i} \right) - 1 + 2 \frac{D_i}{P_i} \right) \right] + \\ \frac{d \Delta p(s, \phi)}{d \phi} &= \begin{bmatrix} \beta - \delta \\ -\beta \end{bmatrix} \begin{bmatrix} \Delta p(s, \phi) \\ \Delta M(s, \phi) \end{bmatrix} \\ \int_0^{\pi/2} (\log \sin x)^2 dx &= \int_0^{\pi/2} (\log \cos x)^2 dx = \frac{\pi}{2} \left\{ \frac{\pi^2}{12} + (\ln 2)^2 \right\} \end{aligned}$$

Event Management

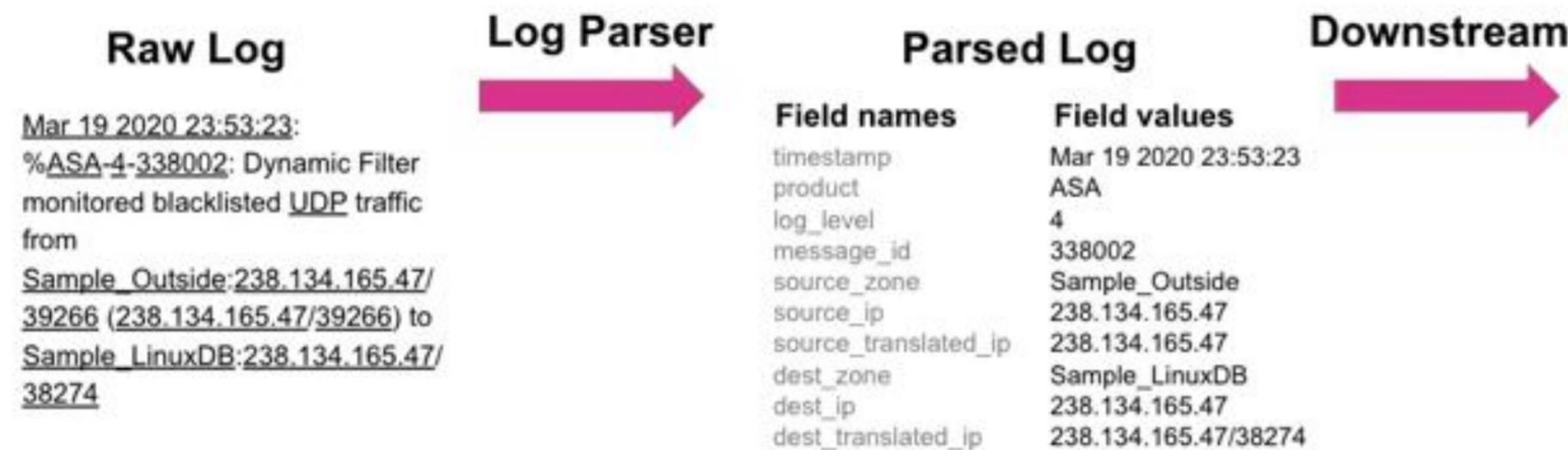
Функциональная схема SIEM: Парсинг



Feb 11 10:51:11 localhost dhclient: DHCPREQUEST on eth1 to
192.168.1.1 port 67
Feb 11 10:51:11 localhost dhclient: DHCPACK from 10.42.1.1
Feb 11 10:51:11 localhost dhclient: bound to 10.42.1.55 -- renewal in
35330 seconds.
Feb 11 14:37:22 localhost -- MARK --
Feb 11 14:44:21 localhost mysqld[7340]: 060211 14:44:21
/usr/sbin/mysqld: Normal shutdown

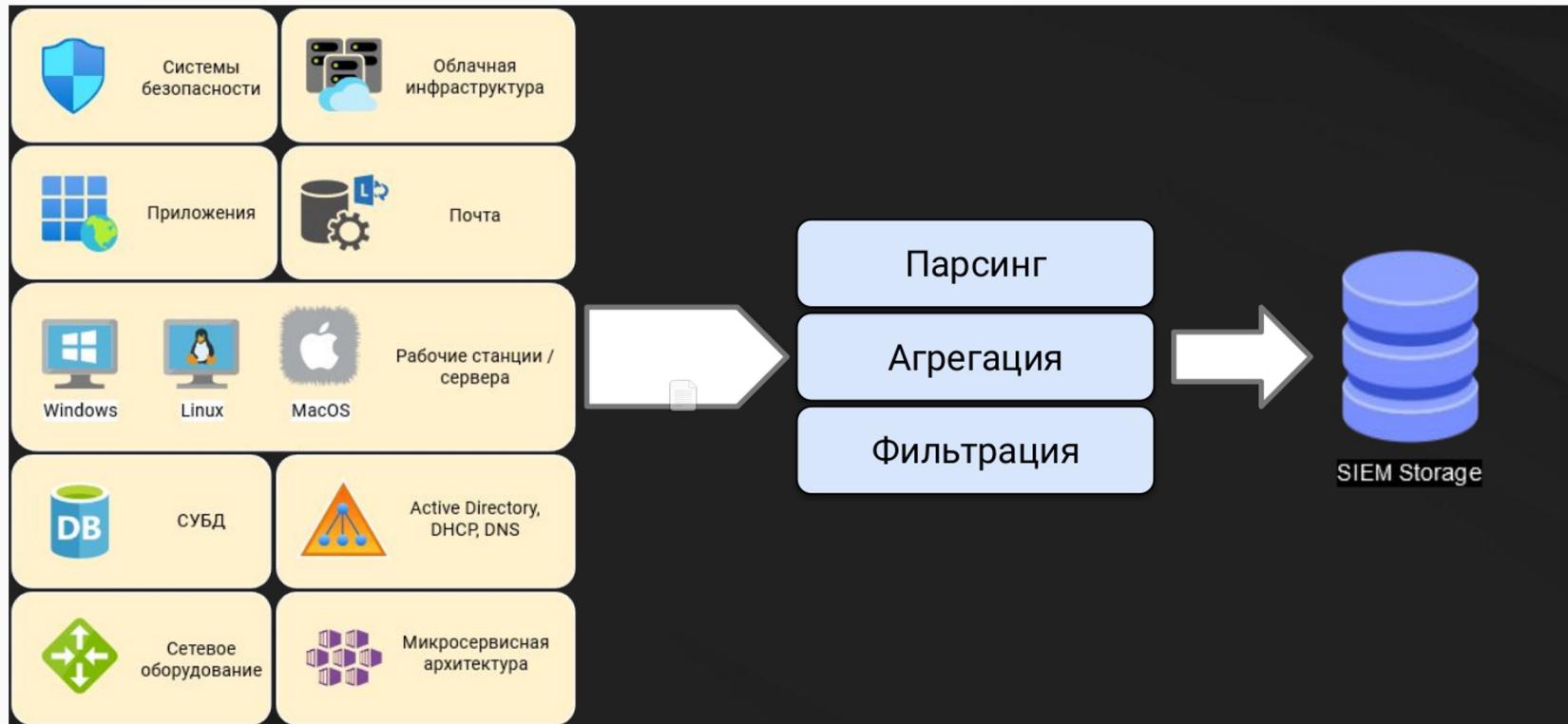
```
date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) sc-status sc-substatus sc-win32-status time-taken
2015-08-03 12:40:57 209.133.7.95 GET /course-eligibility.asp - 80 - 115.118.114.159
Mozilla/5.0+(X11;+Linux+x86_64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Ubuntu
+Chromium/37.0.2062.120+Chrome/37.0.2062.120+Safari/537.36 200 0 0 1234
2015-08-03 12:40:58 209.133.7.95 GET /css/font-awesome.min.css - 80 -
115.118.114.159 Mozilla/5.0+(X11;+Linux+x86_64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Ubuntu+Chromium/37.0.2062.120+Chrome/37.0.2062.120+Safari/537.36 200 0 0 578
```

Функциональная схема SIEM: Парсинг



Event Management

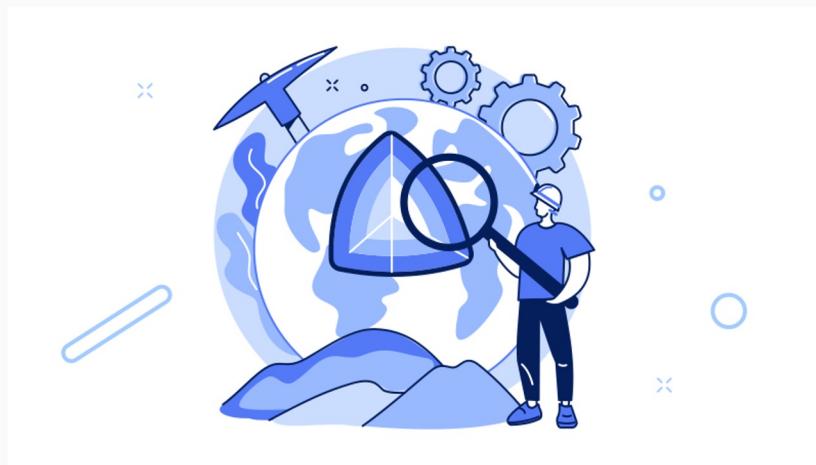
Функциональная схема SIEM: Парсинг



Функциональная схема SIEM: Обогащение

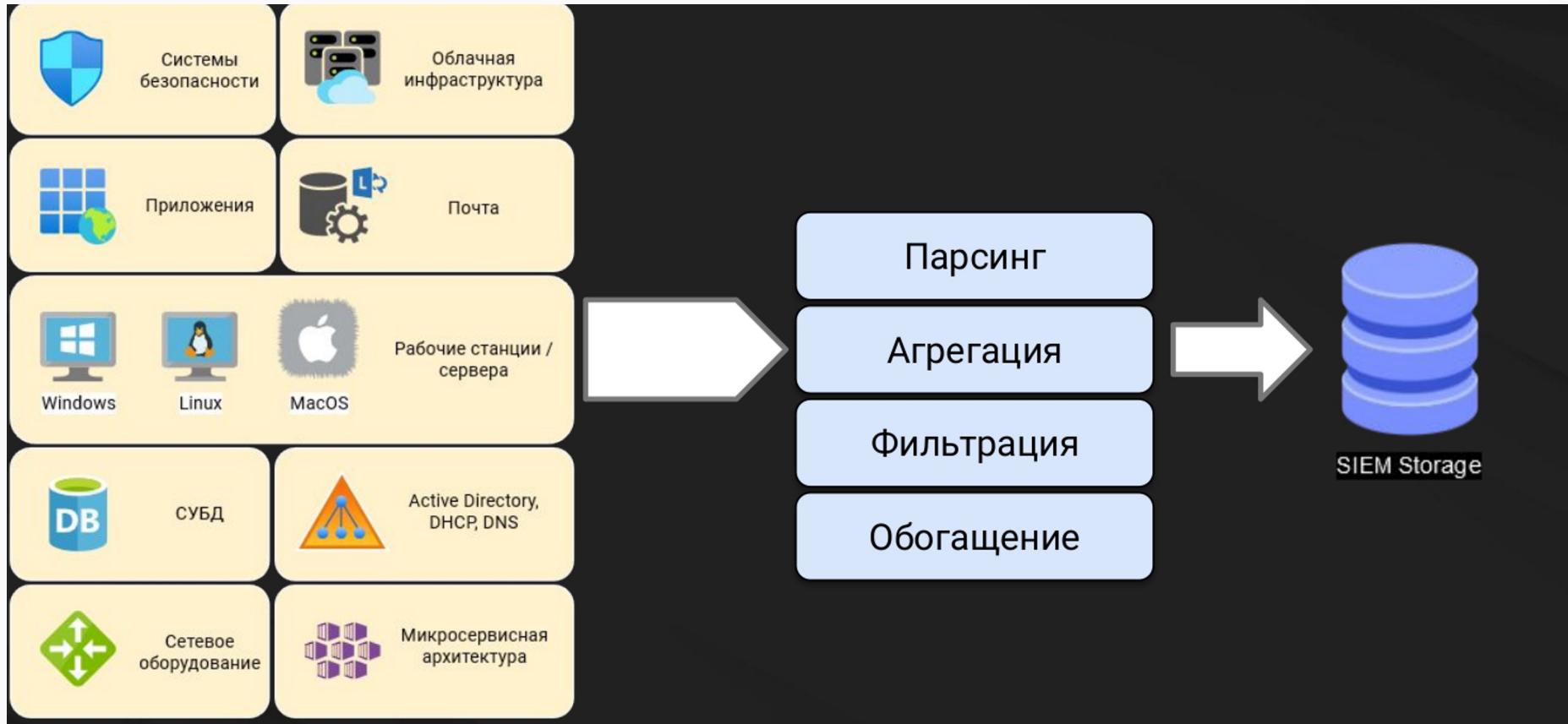
Примеры:

- IP → Геолокация (например, для регистрации попыток подключения к VPN из нестандартных мест).
- IP → Имя хоста (dns lookup)
- Имя хоста → IP (reverse dns lookup)
- IP / URL / Hostname / Hash → Репутация (например, Virustotal)
- Пользователь → Должность
- Имя виртуальной машины → Статус (Powered On/Powered Off)
- И так далее



Event Management

Функциональная схема SIEM: Обогащение



Функциональная схема SIEM: Трансформация

- Удаление / добавление определенной последовательности символов
- Маскирование чувствительных данных (паролей, токенов, ...)
- Добавление вычисляемых полей (на основе исходных полей)
- Перевод в верхний / нижний регистр, конкатенация полей, др.
- Реструктуризация лога

Event Management

Функциональная схема SIEM: Трансформация

Current Structure:

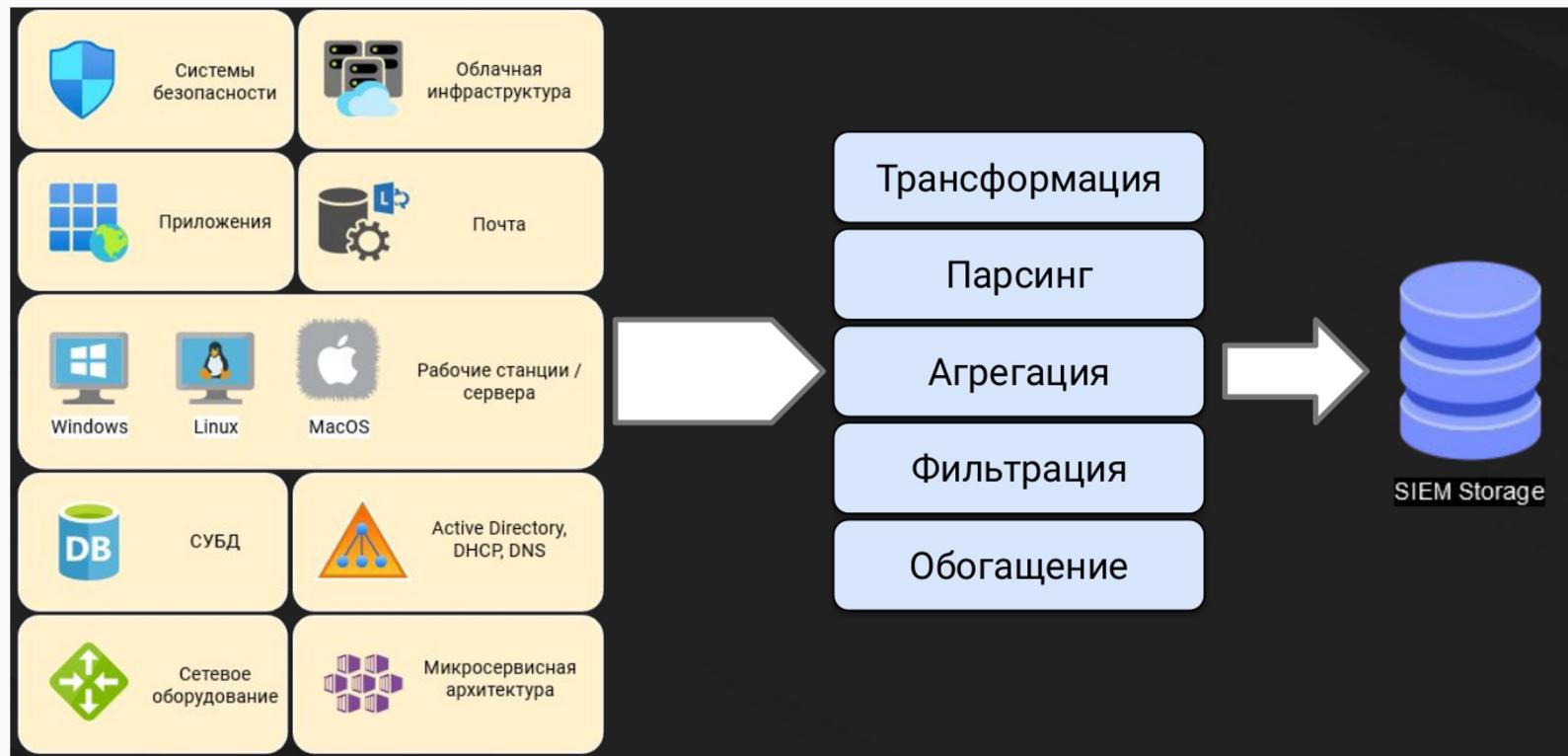
```
May 14 13:28:51 <redacted_hostname> github_audit[22200]: { "above_lock_quota":false,  
"above_warn_quota":false, "babeld":"eefbf1bc7", "babeld_proto":"http", "cloning":false, "cmdline":"/usr/bin/git  
upload-pack --strict --timeout=0 --stateless-rpc .", "committer_date":"1589477330 -0400", "features":  
"multi_ack_detailed no-done side-band-64k thin-pack include-tag ofs-delta agent=git/1.8.3.1",  
"frontend":"<redacted>", "frontend_pid":17688, "frontend_ppid":6744,  
"git_dir":"/data/user/repositories/7/nw/75/42/9d/4564/6435.git", "gitauth_version":"dcddc67b",  
"hostname":"<redacted>", "pgroup":22182, "pid":22182, "ppid":22181, "program":"upload-pack",  
"quotas_enabled":false, "real_ip":10.160.194.177, "remote_addr":127.0.0.1, "remote_port":15820,  
"repo_config":{ "ssh_enabled":true, "ldap.debug_logging_enabled":true, "auth/reactivate-  
suspended":true, "default_repository_permission":write, "allow_private_repository_forking":true },  
"repo_id":6435, "repo_name":<redacted>, "repo_public":true,  
"request_id":43358116096ea9d54f31596345a0fc38, "shallow":false, "status":create_pack_file,  
"uploaded_bytes":968 }
```

JSON Structure:

```
{"timestamp": "May 14 13:28:51", "hostname": "<redacted_hostname>", "thread": "github_audit[22200]",  
"body": { "above_lock_quota":false, "above_warn_quota":false, "babeld":eefbf1bc7, "babeld_proto":http,  
"cloning":false, "cmdline":"/usr/bin/git upload-pack --strict --timeout=0 --stateless-rpc .",  
"committer_date":1589477330 -0400, "features": "multi_ack_detailed no-done side-band-64k thin-pack include-  
tag ofs-delta agent=git/1.8.3.1", "frontend":<redacted>, "frontend_pid":17688, "frontend_ppid":6744,  
"git_dir":/data/user/repositories/7/nw/75/42/9d/4564/6435.git, "gitauth_version":dcddc67b,  
"hostname":<redacted>, "pgroup":22182, "pid":22182, "ppid":22181, "program":upload-pack,  
"quotas_enabled":false, "real_ip":10.160.194.177, "remote_addr":127.0.0.1, "remote_port":15820,  
"repo_config":{ "ssh_enabled":true, "ldap.debug_logging_enabled":true, "auth/reactivate-  
suspended":true, "default_repository_permission":write, "allow_private_repository_forking":true },  
"repo_id":6435, "repo_name":<redacted>, "repo_public":true,  
"request_id":43358116096ea9d54f31596345a0fc38, "shallow":false, "status":create_pack_file,  
"uploaded_bytes":968 }
```

Event Management

Функциональная схема SIEM: Трансформация



Функциональная схема SIEM: Поиск данных

```
SELECT [DISTINCT] {* | column_expression [[AS] column_alias],...}
FROM table_name [table_alias], ...
[ WHERE expr1 rel_operator expr2 ]
[ GROUP BY {column_expression, ...} ]
[ HAVING expr1 rel_operator expr2 ]
[ UNION [ALL] (SELECT...) ]
[ ORDER BY {sort_expression [DESC | ASC]}, ... ]
[ FOR UPDATE [OF {column_expression, ...}] ]
```

В случае с базами данных используется SQL, но SIEM – немного другой случай.

Базы данных → SQL (Structured Query Language)

IBM QRadar → AQL (Ariel Query Language)

Kibana → KQL (Kibana Query Language)

Splunk → SPL (Splunk Search Processing Language)

Azure Sentinel → KQL (Kusto Query Language)

Event Management

Функциональная схема SIEM: Поиск данных

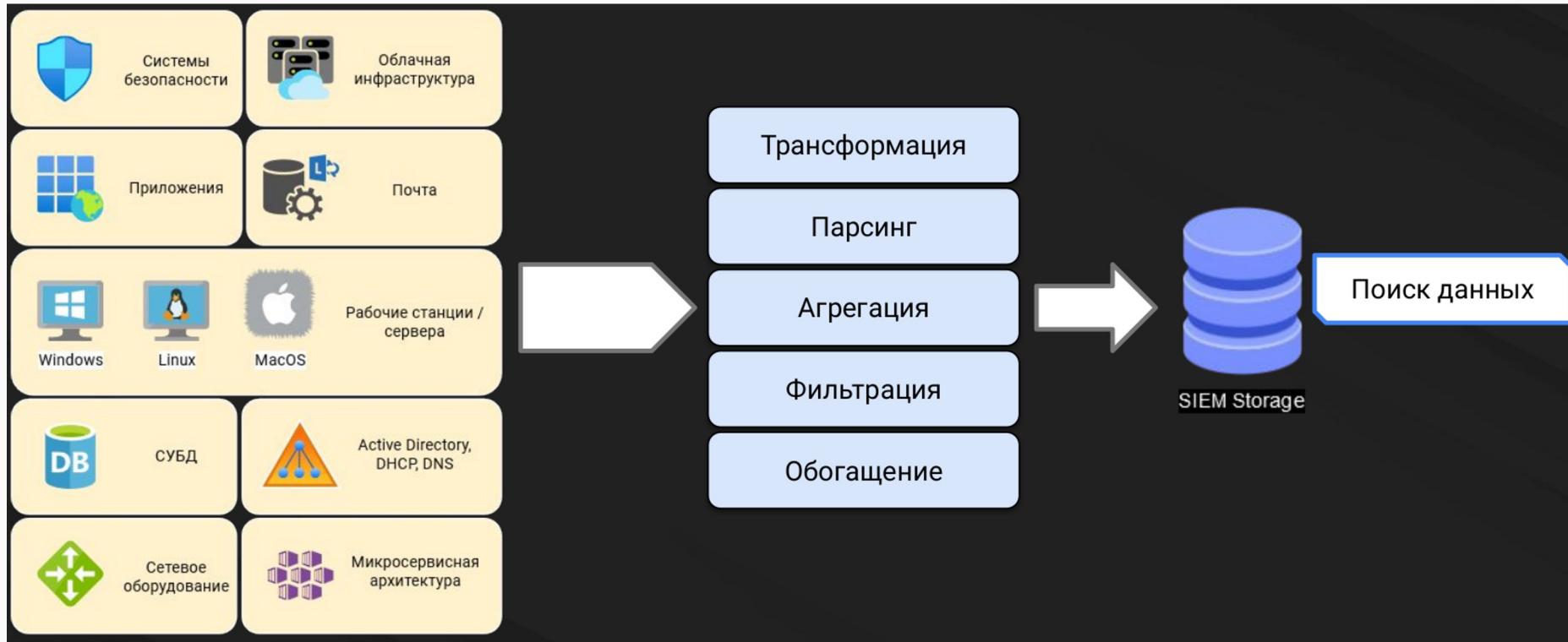
The screenshot shows the Splunk web interface with the following details:

- Header:** splunk> App: Search & Re... Messages Settings Activity Find Jason Skowronski > ?
- Toolbar:** Search Datasets Reports Alerts Dashboards Search & Reporting
- Search Bar:** New Search host="ip-172-31-3-221" Last 24 hours
- Search Results Summary:** 3,814,823 of 3,827,406 events matched No Event Sampling
- Job Controls:** Job II ■ ▶ 🔍 Fast Mode
- Event List:** Events (1,528,696) Patterns Statistics Visualization
- Timeline:** Format Timeline - Zoom Out + Zoom to Selection × Deselect 1 hour per column Feb 13, 2019 4:00 PM
- Table Headers:** List Format 20 Per Page < Prev 1 2 3 4 5 6 7 8 9 ... Next >
- Selected Fields:** host 1 source 1 sourcetype 1
- Interesting Fields:** index 1 linecount 1 splunk_server 1
- Event Data (highlighted in red box):**

i	Time	Event
>	2/13/19 10:28:17.000 PM	54.84.218.101 - - [13/Feb/2019:22:28:17 +0000] "GET /loadtest/001 HTTP/1.1" 404 178 "-" "loader.io;f0d98f1775b089b6d2e4249cb7242d47" "-" f2d8829a9ddf44612ec4ab7b04eb6f8f - - - host = ip-172-31-3-221 source = /var/log/outlogs/nginx_splunk/access.log sourcetype = access_combined_wcookie
>	2/13/19 10:28:17.000 PM	35.153.79.209 - - [13/Feb/2019:22:28:17 +0000] "GET / HTTP/1.1" 200 612 "-" "loader.io;c000c87b91b2ec488ca711d065944744" "-" ebd9d3d165fe330411879f289d460706 - - - host = ip-172-31-3-221 source = /var/log/outlogs/nginx_splunk/access.log sourcetype = access_combined_wcookie
>	2/13/19 10:28:17.000 PM	100.24.126.130 - - [13/Feb/2019:22:28:17 +0000] "GET / HTTP/1.1" 200 612 "-" "loader.io;c000c87b91b2ec488ca711d065944744" "-" ff443f9064e809c07edd536b99ce7d21 - - - host = ip-172-31-3-221 source = /var/log/outlogs/nginx_splunk/access.log sourcetype = access_combined_wcookie

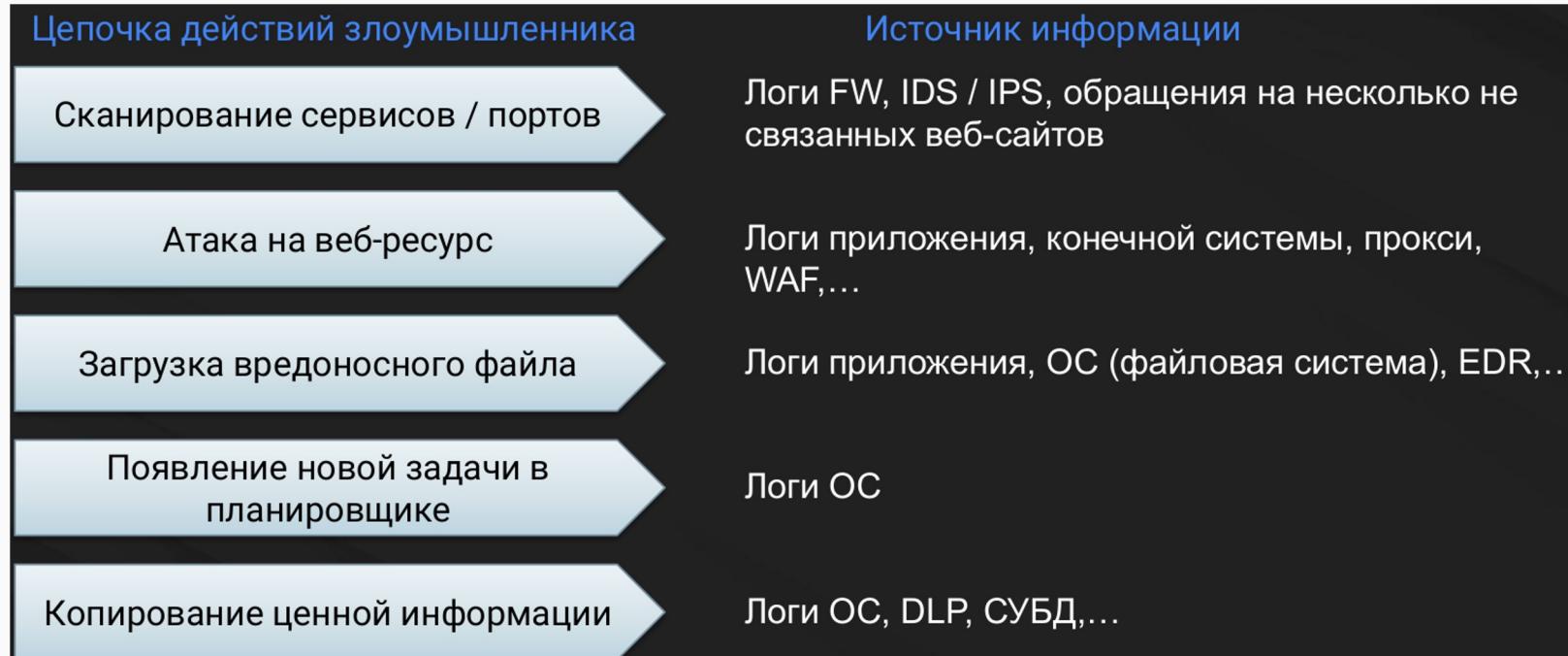
Event Management

Функциональная схема SIEM: Поиск данных



Функциональная схема SIEM: Корреляция

Корреляция — это процесс сопоставления событий с различных систем.



Функциональная схема SIEM: Обнаружение инцидентов

Специалисты ИБ пишут правила обнаружения инцидентов (алёрты), запускаемые на периодической основе.

Для компаний среднего размера количество событий может доходить до тысяч в секунду, а алертов – до нескольких сотен в день.

Источники правил:

- Встроенные в SIEM – без допиливания
- бесполезные,
- Опыт аналитиков (особенно, если в команде есть пентестер),
- Опенсорс ([SIGMA](#)),
- Данные кибер-разведки ([APT Notes](#))
- MITRE ATT&CK
- Twitter

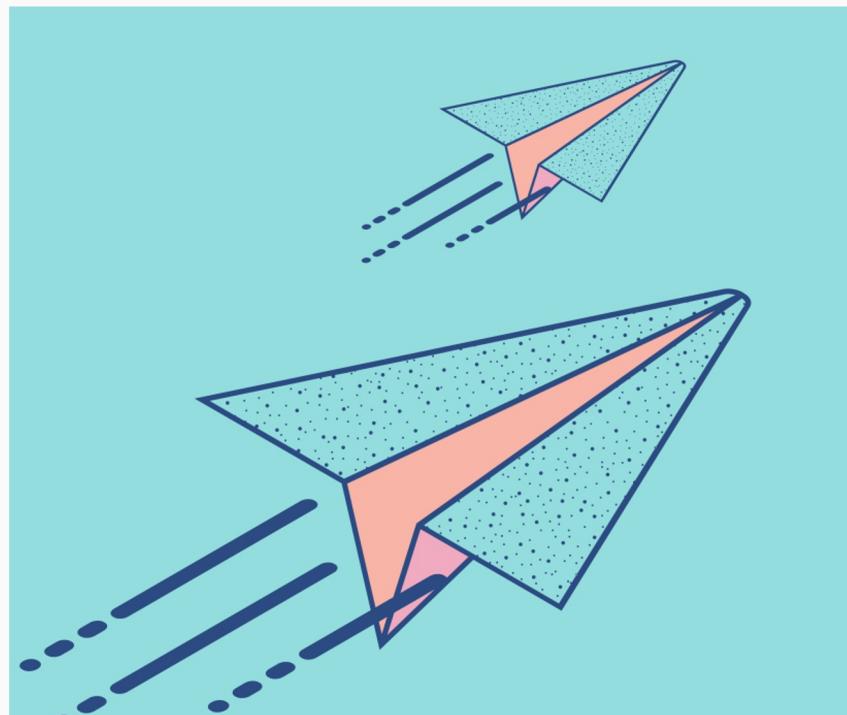
И так далее

Функциональная схема SIEM: Оповещения об инцидентах

После того как система произвела анализ схожих между собой событий, она оповещает администратора безопасности о существующих проблемах в инфраструктуре.

В зависимости от категории инцидента (критичности), к времени реагирования:

- Тикетница / IRP-система
- Почта
- Социальные сети (Telegram, Slack)



Функциональная схема SIEM: Нормализация

Ситуация: аналитик ИБ написал правило детектирования атаки перебора паролей.

Простая логика: превышение порогового значения неуспешных попыток аутентификации в единицу времени (5 / 10 / 15 минут).

Алёрт работает на основе полей

- timestamp – время регистрации события,
- user.ip – IP-адрес пользователя,
- target.ip – IP-адрес конечной системы,
- auth.type – статус аутентификации (success / failure)

В логах Windows есть поля:

- TimeCreated – время регистрации события,
- IpAddress – IP-адрес пользователя,
- WorkstationName – адрес подключения пользователя,
- EventID=4625 (auth.type=failure) – статус аутентификации.

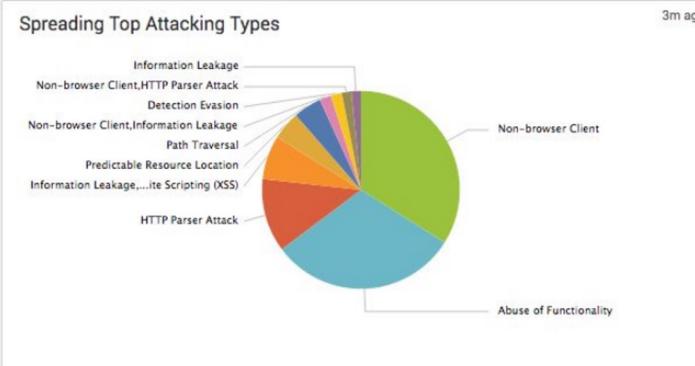
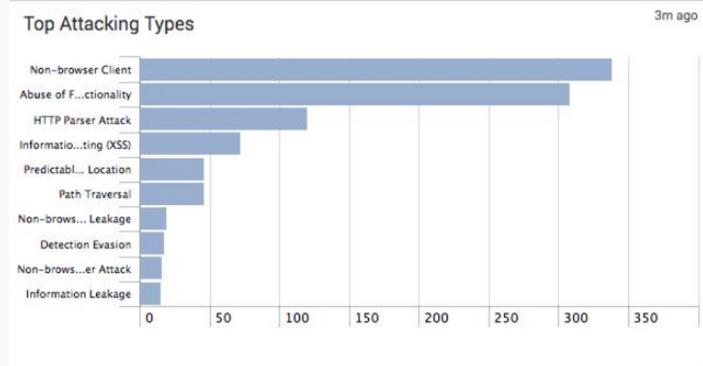
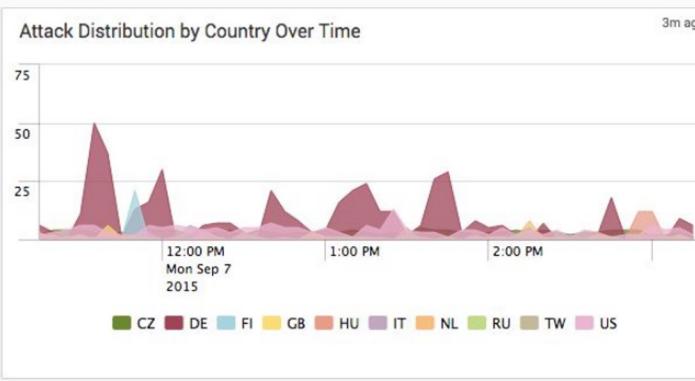
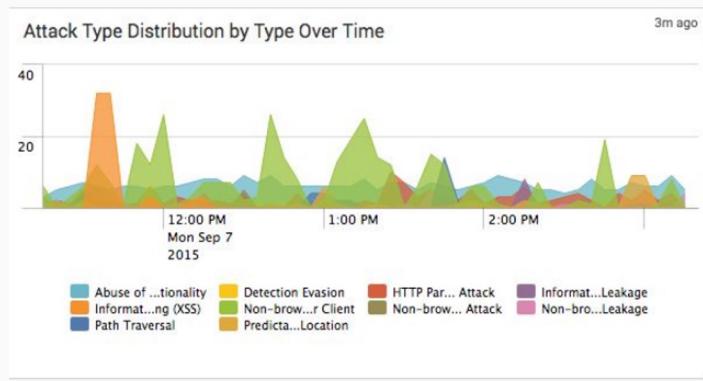
Функциональная схема SIEM: Нормализация

Вопрос: аналитик ИБ в итоге должен написать N-правил для каждой из N-систем, в каждом из правил указывая соответствующее наименование полей?

Для этого и нужна нормализация событий – приведение логов к общему формату.

Event Management

Функциональная схема SIEM: Формирование отчёtnости и визуализация

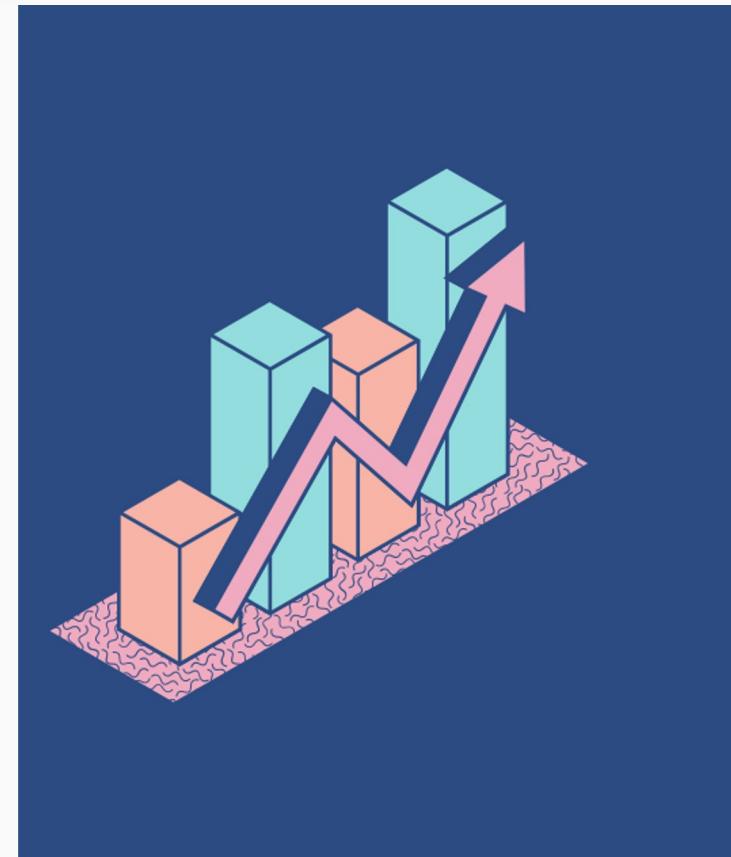


SIEM: модель чёрного ящика



Анализ и метрики

- Скорость реакции на инцидент
- Срок расследования инцидента ИБ
- Количество полученных событий за определенный период времени (EPS)



Реагирование на инциденты ИБ

splunk®
phantom



R.Vision
At the root of your security



 **MISP**
Threat Sharing



IBM Security

Event Management

Автоматизация процесса реагирования

Получение и анализ хеш-суммы, IP, URL и домена на интернет-сервисах



Сбор информации о текущих сессиях по подозрительному IP-адресу



Отправка подозрительного файла на анализ в песочницу и получение результата



Поиск индикаторов компрометации на других хостах в SIEM



Event Management

Сбор syslog, auditd ПРОЦЕСС СБОРА ЛОГОВ С ОС LINUX

syslog-ng

/etc/syslog-ng/syslog-ng.conf

```
destination d_xs-zabbix {  
file("/var/log/!remote/xs-  
zabbix.log"); };  
filter f_xs-zabbix {  
netmask("10.1.3.29/255.255.255.2  
55"); };  
log { source(net); filter(f_xs-  
zabbix); destination(d_xs-zabbix);  
};
```

rsyslog

/etc/rsyslog.d/audit.conf

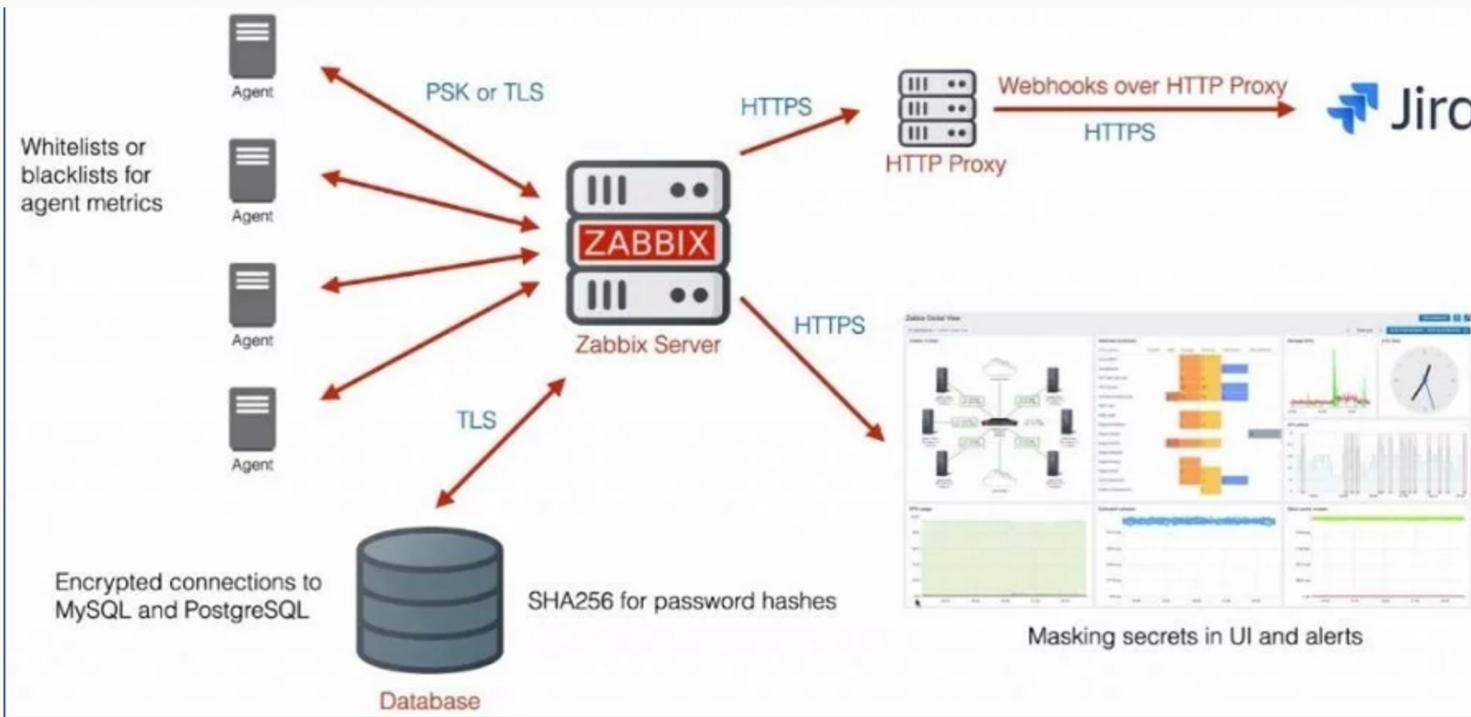
```
$ModLoad imfile  
$InputFileName  
/var/log/cups/access.log  
$InputFileTag audit_log:  
$InputFileStateFile audit_log  
$InputFileSeverity info  
$InputFileFacility local6  
$InputRunFileMonitor  
*.* @@10.1.1.6:5167
```

auditd

[описание](#)

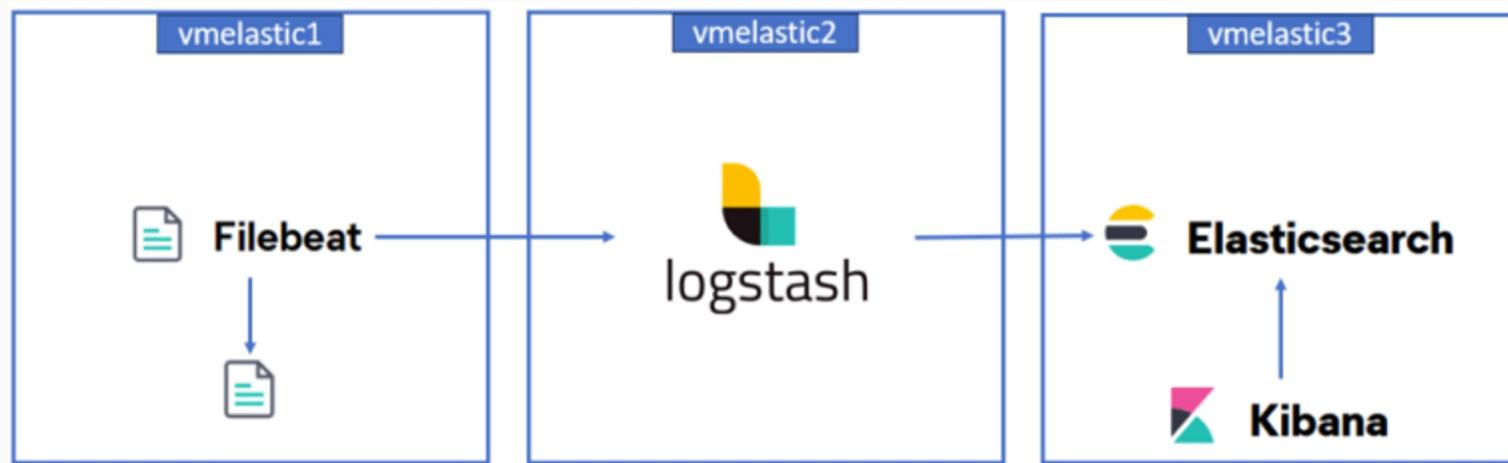
Event Management

Zabbix



Event Management

Logstash, Elasticsearch, Kibana



Спасибо за внимание!