ENERGY LOGSERVER

SIEM **FOR BEGINNERS**

ВСЕ, ЧТО ВЫ ХОТЕЛИ ЗНАТЬ ПРО УПРАВЛЕНИЕ ЛОГАМИ,
НО БОЯЛИСЬ СПРОСИТЬ

www.energylogserver.com

Эволюция технологий SIM, SEM, SIEM

ENERGY LOGSERVER

SIEM — это класс решений, который часто остается недооцененным, при этом оставаясь у всех на слуху. Задачи **SIEM** включают централизованный сбор и управление событиями безопасности из разных систем. Ему предшествовал ряд решений, которые стремились к упрощению и автоматизации контроля за инструментами безопасности.

Два распространенных типа таких систем:

- SIM (Security Information Management) — система управления логами
- SEM (Security Event Management) — система управления событиями безопасности

Хоть определения и выглядят похоже, между ними есть колоссальная разница:

1. Это скорее эволюция одной идеи по сбору событий, чем два варианта ее воплощения.
2. SIM автоматизирует сбор логов, SEM — любые события безопасности в принципе. Из-за этого отличаются источники получения информации: у SIM это программные и аппаратные решения, а у SEM — базы данных Oracle и MySQL.
3. SIM просто позволяет упростить поиск логов при помощи автоматического сбора и сортировки. У SEM есть функции контекстного анализа и корреляции собранных данных — он ищет события с общим знаменателем и может составить из них вывод об угрозе или проблеме.

SIEM (Security Information and Event Management) объединяет функции двух указанных систем, позволяя централизованно управлять информацией и событиями, которые генерируются другими решениями безопасности.

Он собирает и анализирует записи журналов, которые генерируют ваши активы. Все, что записывают ваши антивирусы, файрволлы, системы предотвращения утечек данных, защиты эндпоинтов, управления привилегированным доступом и так далее, теперь собрано в одном едином решении — в **SIEM**.

Чем обусловлено появление SIEM и потребность в решениях этого класса?

ENERGY LOGSERVER

Рост количества информации, которую должны анализировать специалисты. В эпоху диджитализации компании осознали, что типичные задачи постоянно усложняются. Для каждой из них теперь нужно понимать и связывать столько событий, что сопоставить их верно и сделать вывод на ходу буквально невозможно.

Атаки усложняются, а значит добавляется количество маркеров, которые их выдают. Современные угрозы включают в себя сразу несколько векторов — от банального фишинга до внедрения интеллектуального вредоносного ПО, а сами злоумышленники качественно маскируют свои действия и обходят системы защиты. Таким образом, ни одно отдельное решение безопасности не даст вам исчерпывающую информацию о том, что происходит что-то плохое.

При этом каждое отдельное решение имеет узкую спецификацию и предоставляет вам информацию вне контекста. Инструменты анализируют факты без привязки к ситуации, в которой они происходят. Этого становится мало, потому что ни одна атака не происходит в каких-то изолированных рамках. Атака — не событие, а их совокупность.

Сравните: сотрудник в отпуске бегло проверяет корпоративную почту — хакер крадет его данные и тоже заходит в почту. Для нас с вами это две совершенно разные ситуации, как в плане важности, так и самой сути, не говоря уже о последствиях и реакции.

А для систем контроля доступа это просто два входа в аккаунт, с разных IP- и MAC-адресов. Масштабировав ситуацию на десятки сотрудников и сотни процессов, получим безопасность, полную ненужной, а зачастую и бесполезной рутины. Чтобы проверить все подобные подозрительные случаи, вам нужно разобраться в дальнейших действиях юзера и изменениях в системе: проверить запросы на доступ к файлам, загрузку подозрительного ПО, сканирование сети и попытки повысить уровень доступа. Все это находится в разных решениях, а значит нужно проверить каждое из них.

Ваши решения не могут самостоятельно обнаружить атаку, однако предоставляют всю необходимую для этого информацию. Дело за малым – найти ее.

Расследуем инцидент вместе с SIEM

ENERGY LOGSERVER

Предлагаем разобрать на практике, какие процессы происходят внутри решения, и как они приводят к результату. Информация ниже — пошаговая демонстрация решения задачи расследования инцидента.

Мы воссоздали реальную атаку на отдельном хосте в тестовой инфраструктуре. По задумке, все началось с того, что с компьютера, который был атакован, пришло оповещение о подозрительном инциденте. Наша задача — расследовать этот инцидент как ИБ-специалист. Попробуем узнать, является ли это событие атакой. Если да — детализируем ее до мелочей, если нет — узнаем, что произошло и как избежать таких тревог.

Еще одно важное условие: будем считать, что пробелов в системе защиты нет и **SIEM** правильно интегрирована во все решения. Иными словами — решить поставленную задачу возможно, информация в системе об этом есть, нужно просто ее найти.

Принимаем условия и переходим непосредственно к **SIEM**.

Сбор логов и информации с системы

ENERGY LOGSERVER

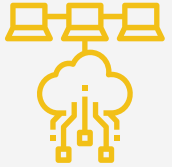
В основе любой **SIEM** находится Log Management — централизованный автоматизированный сбор записей журналов в одном месте. Мы уже выяснили, что обнаружить атаку мы сможем по совокупности событий, а значит первым этапом нам нужны данные с логов каждого решения.

Инструменты ИБ:

- файрволлы (VPN-концентраторы, веб-фильтры)
- IDS/IPS
- защита эндпоинтов (антивирусы, EDR и др.)
- DLP
- PAM, WAF, MFA

Данные об активах:

- конфигурация
- расположение
- пользователи
- порты и протоколы
- отчеты об уязвимостях
- инвентаризация ПО



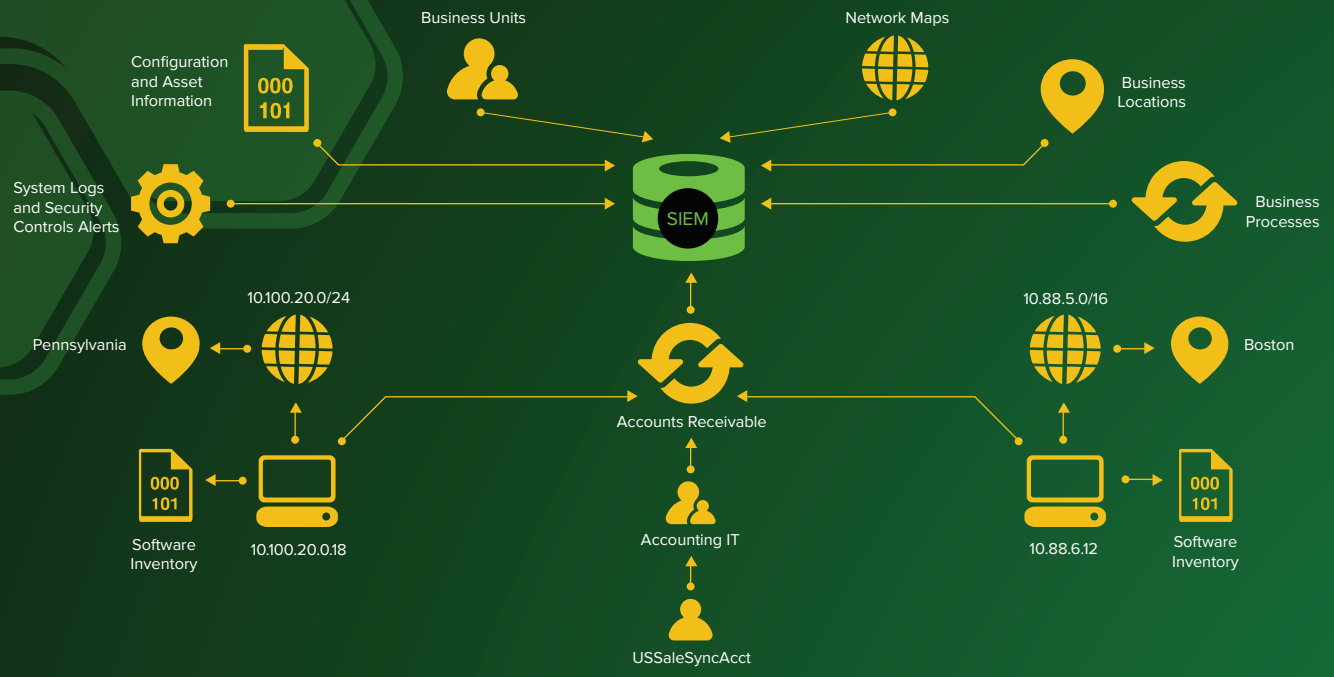
Инфраструктура:

- маршрутизаторы, коммутаторы, точки доступа
- контроллеры доменов
- серверы приложений, корпоративные порталы и сервисы
- базы данных
- журналы ОС и облачных сервисов

Как генерируются логи в вашей сети

ENERGY LOGSERVER

Каждый перечисленный выше источник создает десятки и сотни записей ежедневно, и этого не изменить. Как генерируются логи в вашей сети — показано на схеме ниже.



10.100.20.18 инициировал копирование базы данных с использованием учетных данных USSalesSyncAcct на удаленном хосте 10.88.6.12 - Status Code 0x44F8

А теперь представьте, что похожие процессы повторяются тысячи раз в день, создавая целый массив информации, в том числе — полезной. Без **SIEM** все это будет лишь мертвым грузом, в котором вручную не разобраться.

Как это работает?

При помощи лог-менеджмента мы можем достать из хранилища и просмотреть лог этого события, который сформирован на атакуемом компьютере.

Выглядит он вот так:

5ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□
b(15ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□b(1
5ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49□b(15ssh:nottyroot192.168.202.49ý¹b(15ssh:nottyroot192.168.202.49ý¹b(1¸5s
sh:nottyroot192.168.202.49ÿ¹b(1·5ssh:nottyroot192.168.202.49ÿ¹b(1½5ssh:nottyroot192.168.202.49°b(1¿5ssh:nottyroot192.168.202.49°b(1¸5ssh:nottyroot192.168.202.49°b(1·5ssh:nottyroot192.168.202.49°b(1 ¿5ssh:nottyroot192.168.202.49°b(1½5ssh:nottyroot192.168.202.49°
b(1¸5ssh:nottyroot192.168.202.49°b(1·5ssh:nottyroot192.168.202.49°b(1¿5ssh:nottyroot192.168.202.49°b(1½5ssh:nottyroot192.168.202.49 °b(1¸5ssh:nottyroot192.168.202.49°b(1·5ssh:nottyroot192.168.202.49°b(1¿5ssh:nottyroot192.168.202.49°b(1½5ssh:nottyroot192.168.202.
49°b(1¸5ssh:nottyroot192.168.202.49°b(1·5ssh:nottyroot192.168.202.49°b(1¿5ssh:nottyroot192.168.202.4°b(1½5ssh:nottyroot192.168.202.4°b(1¸5ssh:nottyroot192.168.202.4°b(1·5ssh:nottyroot192.168.202.4°b(1¿5ssh:nottyroot192.168.202.49 °b(1½5ssh:nottyroot192.168.202.49
°b(15ssh:nottyroot192.168.202.49(°b(15ssh:nottyroot192.168.202.49(°b(15ssh:nottyroot192.168.202.49*°b(15ssh:nottyroot192.168.202.49*°b(15ssh:nottyroot192.168.202.49*°b(15ssh:nottyroot192.168.202.49*°b(15ssh:nottyroot192.168.202.49,°b(15ssh:nottyroot192.168.202.49
,°b(15ssh:nottyroot192.168.202.49,°b(15ssh:nottyroot192.168.202.49,°b(15ssh:nottyroot192.168.202.49.°b(15ssh:nottyroot192.168.202.49.°b(15ssh:nottyroot192.168.202.49.°b(15ssh:nottyroot192.168.202.49.°b(15ssh:nottyroot192.168.202.490°b(15ssh:nottyroot192.168.202.4
90°b(15ssh:nottyroot192.168.202.490°b(15ssh:nottyroot192.168.202.490°b(15ssh:nottyroot192.168.202.491°b(15ssh:nottyroot192.168.202.491°b(15ssh:nottyroot192.168.202.492°b(15ssh:nottyroot192.168.202.492°b(15ssh:nottyroot192.168.202.494°b(15ssh:nottyroot192.168
.202.494°b(16ssh:nottyroot192.168.202.49R°b(16ssh:nottyroot192.168.202.49R°b(16ssh:nottyroot192.168.202.49S°b(16ssh:nottyroot192.168.202.49S°b(16ssh:nottyroot192.168.202.49T°b(1 6ssh:nottyroot192.168.202.49T°b(16ssh:nottyroot192.168.202.49V°b(1 6ssh:nottyroo
t192.168.202.49V°b(16ssh:nottyroot192.168.202.49V°b(16ssh:nottyroot192.168.202.49V°b(16ssh:nottyroot192.168.202.49W°b(1 6ssh:nottyroot192.168.202.49W°b(16ssh:nottyroot192.168.202.49X°b(16ssh:nottyroot192.168.202.49X°b(1 6ssh:nottyroot192.168.202.49Y°b(1 6ss
h:nottyroot192.168.202.49Y°b(16ssh:nottyroot192.168.202.49Z°b(16ssh:nottyroot192.168.202.49Z°b(16ssh:nottyroot192.168.202.49[°b(1 6ssh:nottyroot192.168.202.49[°b(16ssh:nottyroot192.168.202.49\°b(16ssh:nottyroot192.168.202.49\°b(16ssh:nottyroot192.168.202.49\°b(1
6ssh:nottyroot192.168.202.49\°b(1>6ssh:nottyroot192.168.202.49|°b(1?6ssh:nottyroot192.168.202.49|°b(1D6ssh:nottyroot192.168.202.49}°b(1F6ssh:nottyroot192.168.202.49}°b(1>6ssh:nottyroot192.168.202.49}°b(1?6ssh:nottyroot192.168.202.49}°b(1D6ssh:nottyroot192.168.20
2.4°b(1F6ssh:nottyroot192.168.202.4°b(1>6ssh:nottyroot192.168.202.4°b(1?6ssh:nottyroot192.168.202.4°b(1D6ssh:nottyroot192.168.202.49°b(1F6ssh:nottyroot192.168.202.49°b(1>6ssh:nottyroot192.168.202.49°b?6ssh:nottyroot192.168.202.49°b(1¼Hssh:nottyroot192.168.20
2.49¿ýb(1½Hssh:nottyroot192.168.202.49¿ýb(1»Hssh:nottyroot192.168.202.49¿ýb(1¾Hssh:nottyroot192.168.202.49¿ýb(1¼Hssh:nottyroot192.168.202.49ëýb(1½Hssh:nottyroot192.168.202.49ëýb(1»Hssh:nottyroot192.168.202.49ëýb(1¾Hssh:nottyroot192.168.202.49ëýb(1 ¼Hss
h:nottyroot192.168.202.49ëýb(1½Hssh:nottyroot192.168.202.49ëýb(1»Hssh:nottyroot192.168.202.49ëýb(1¾Hssh:nottyroot192.168.202.49ëýb(1¼Hssh:nottyroot192.168.202.49ëýb(1½Hssh:nottyroot192.168.202.49ëýb(1»Hssh:nottyroot192.168.202.49ëýb(1¾Hssh:nottyroot192
.168.202.49ëýb(1¼Hssh:nottyroot192.168.202.49ëýb(1»Hssh:nottyroot192.168.202.49ëýb(1½Hssh:nottyroot192.168.202.49ëýb(1¾Hssh:nottyroot192.168.202.49ëýb(1¼Hssh:nottyroot192.168.202.49ëýb(1»Hssh:nottyroot192.168.202.49ëýb(1½Hssh:nottyroot192.168.202.49ëý
b(1¾Hssh:nottyroot192.168.202.49ëýb(1Hssh:nottyroot192.168.202.49ëýb(1Hssh:nottyroot192.168.202.49ëýb(1Hssh:nottyroot192.168.202.49ëýb(1Hssh:nottyroot192.168.202.49ëýb(1Hssh:nottyroot192.168.202.49ëýb(1Hssh:nottyroot192.168.202.49ëýb(1Hssh:nottyroot192.16

Из этого примера становится ясно, что анализировать логи своими силами бесполезно. Тем более, что в реальной компании таких логов будет в несколько десятков-сотен-тысяч раз больше, и если один в теории можно побороть, то работать так постоянно — увы.

Вывод: Log Management помогает нам найти старые записи, но этого недостаточно для получения какой-то ценной информации. Благо, с этого **SIEM** только начинается.

Готовим данные к анализу

ENERGY LOGSERVER

Все источники логов обычно записывают события по-своему. Предполагается, что эти записи будут читаться людьми, а не машиной, поэтому разный формат логов не принято считать проблемой. Но в нашем случае важно получить возможность обрабатывать записи инструментами **SIEM**, а значит решение должно сперва привести все имеющиеся логи к некому общему знаменателю.

Например, в логе

> **“User Broberts Successfully Authenticated to 10.100.52.105 from client 10.10.8.22”**

необходимо выделить общие для всех логов элементы

> **“User [USERNAME] [STATUS] Authenticated to [DESTIP] from client [SOURCEIP]”**

Этот процесс называется нормализация. Благодаря ей **SIEM** обрабатывает огромное количество записей на уровне математических моделей и методов статистики. Проще говоря, фильтрует и сортирует логи. Разница между лог-менеджментом с нормализацией и без в том, что без нормализации мы можем обрабатывать лишь логи с одного источника. Отфильтровать логи разных источников по какому-либо общему критерию у нас не выйдет.

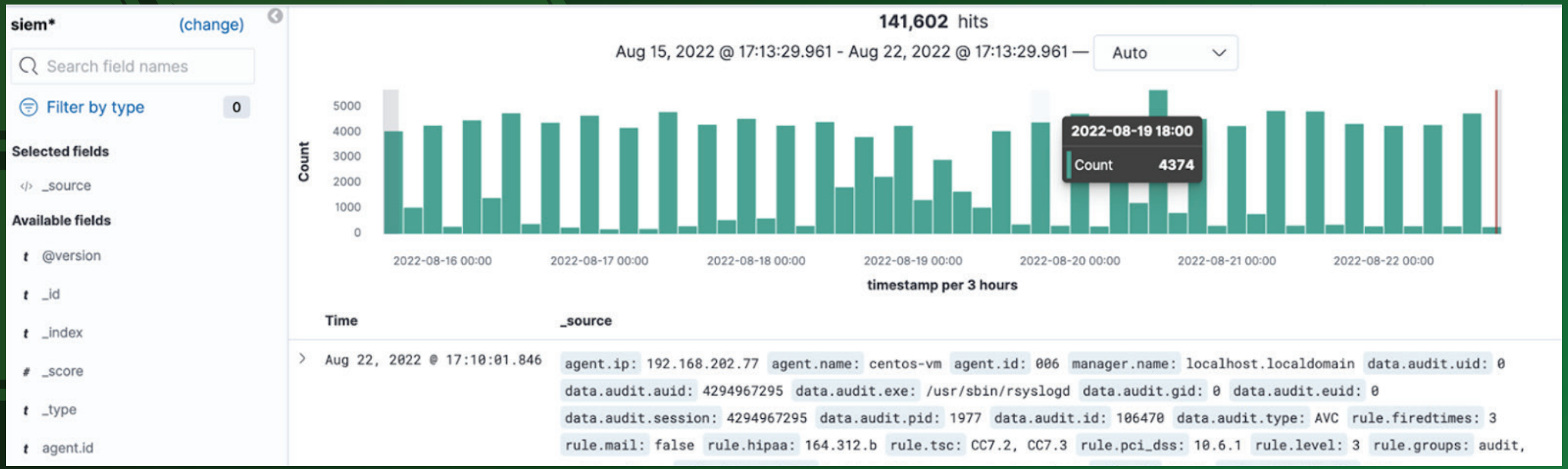
Это нам и нужно для последующих действий, ведь суть **SIEM** — дополнить информацию из одних источников данными из остальных.

Как это работает?

ENERGY LOGSERVER

Получив возможность добавить немного статистики и фильтровать данные, появляется возможность структурировать лог и что-то разглядеть.

Вот как это выглядит в консоли:



Мы видим попытки входа в учетную запись, которые не прошли из-за неправильно введенных учетных данных. **SIEM** зафиксировал время, IP-адреса и остальные характеристики запросов. Мы видим, что повторялись они много раз, видим использованные пароли, а также отмечаем разницу в миллисекунды между запросами.

Это признак машинного подбора пароля, но зачем нам делать выводы самостоятельно, если у нас есть **SIEM**? Расследуем дальше.

Суть процесса корреляции

ENERGY LOGSERVER

Корреляция позволяет найти взаимосвязь между разными событиями, связать их в одну цепочку и сравнить с состоянием нормы. В итоге мы получаем классифицированные события по принятым нами критериям (риск-менеджмент, alerts, приоритизация и т.д.). А если добавить в уравнение интеграцию с базами индикаторов компрометаций, получим возможность более эффективного обнаружения угроз при помощи **SIEM**, в том числе — атак нулевого дня.

Правила детектирования, интегрированные с системой оповещения и реагирования, позволяют настраивать сценарии реакций на события, которые не должны происходить в вашей системе. Правильно настроенная система сможет вычленять из всего многообразия логов маркерные события и уведомлять вас о потенциальной угрозе.

Если одно событие от конкретного решения может как быть совершенно безвредным, так и свидетельствовать об угрозе, то несколько таких свидетельств из разных источников уже говорят о факте атаки. Наличие информации о нормальном состоянии системы создает контекст для анализируемых событий — система не оценивает события по принципу «хорошо это или плохо?», а находит ответ на вопрос «Должно ли это происходить **в текущих условиях?»**

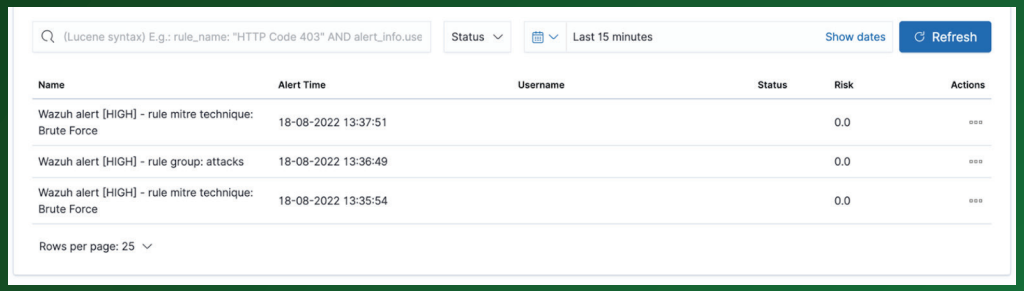
Как это работает?

ENERGY LOGSERVER

Нормализация и корреляция дают нам возможность делать что душе угодно с нашим пока еще непонятным логом. Так давайте сделаем что-то полезное!

Включаем оповещение на тип атак Brute Force

Это сразу дает нам перечень срабатываний правила (с возможностью углубиться в каждый инцидент):



— Становится проще, не так ли?

Но еще не все — мы уже нашли и выделили событие, точно видим, что у нас была атака типа Brute Force. Но нам этого мало.

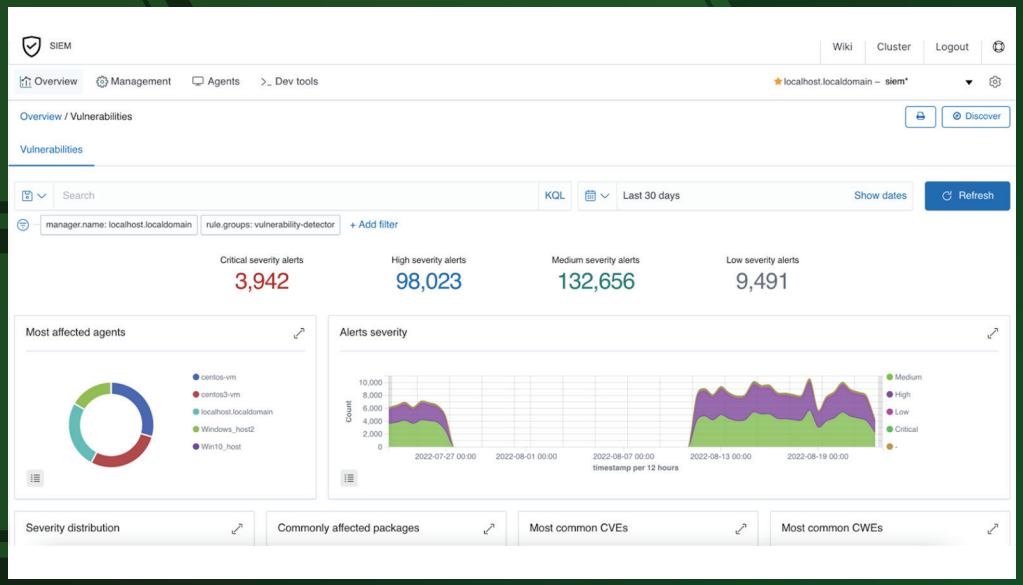
На секунду вернемся в общую картину, посмотрим, как обстоят дела в целом, и обратно нырнем в наш инцидент.

— В этот раз — поглубже.

Как это работает?

ENERGY LOGSERVER

Общий дашборд по всем событиям: достаточно беглого взгляда, чтобы оценить ситуацию и получить важные метрики. Разумеется, все это можно настраивать и кастомизировать под свои задачи.



Выделяем атаки на определенный хост:

Как это работает?

ENERGY LOGSERVER

Далее кликаем по нашему событию и изучаем детали.

Например, с какого источника на какой была воспроизведена атака...

Incident ID: -6Uer4IB9B1_si7K3kNm
Rule Name: Wazuh alert [HIGH] - rule mitre technique: Brute Force

alert_time	2022-08-18T04:03:32.019871Z
match_body.@src_ip	192.168.202.49
match_body.@timestamp	2022-08-18T04:02:33.319Z
match_body.@version	1
match_body.GeoLocation	{}
match_body._id	qaUdr4IB9B1_si7K-0Cu
match_body._index	siem-2022.08
match_body._type	_doc
match_body.agent.id	007
match_body.agent.ip	192.168.202.79

...здесь — информацию о том, что пароли были ошибочные, то есть атака не прошла...

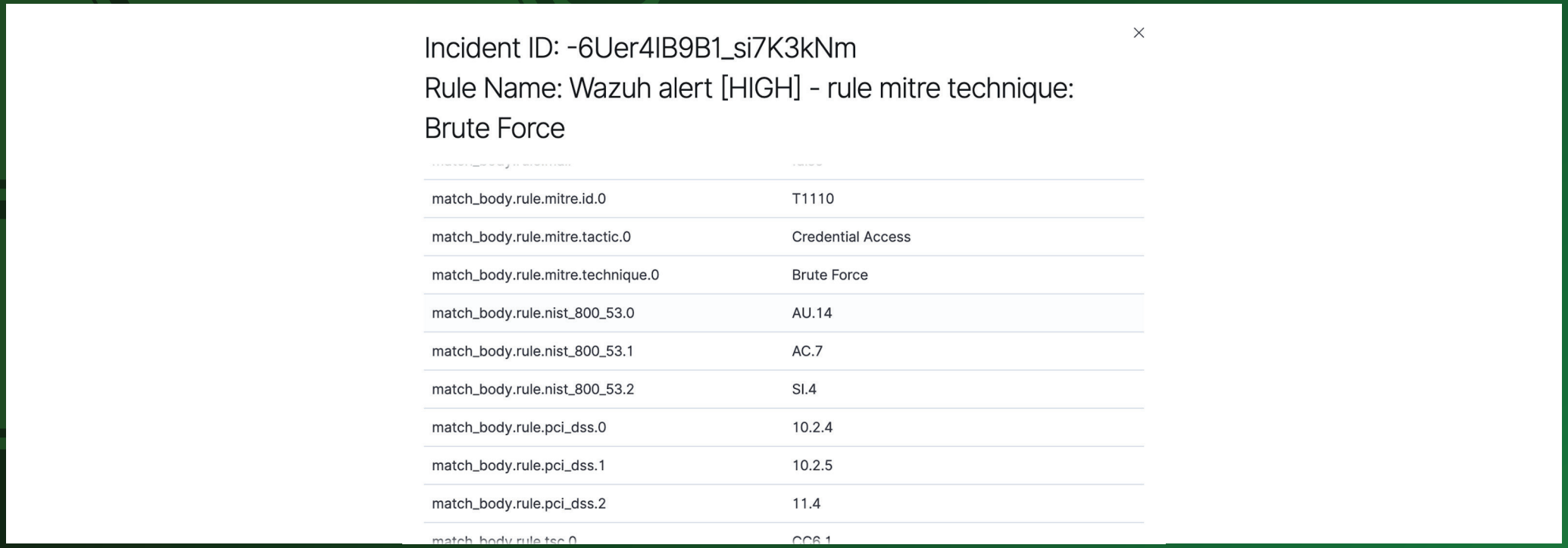
Incident ID: -6Uer4IB9B1_si7K3kNm
Rule Name: Wazuh alert [HIGH] - rule mitre technique: Brute Force

match_body.predecoder.timestamp	Aug 18 00:02:32
match_body.previous_output	Aug 18 00:02:32 centos3-vm sshd[13707]: Failed password for root from 192.168.202.49 port 37026 ssh2 Aug 18 00:02:31 centos3-vm sshd[13708]: Failed password for root from 192.168.202.49 port 37030 ssh2 Aug 18 00:02:31 centos3-vm sshd[13705]: Failed password for root from 192.168.202.49 port 37024 ssh2 Aug 18 00:02:30 centos3-vm sshd[13707]: Failed password for root from 192.168.202.49 port 37026 ssh2 Aug 18 00:02:29 centos3-vm sshd[13708]: Failed password for root from 192.168.202.49 port 37030 ssh2 Aug 18 00:02:29 centos3-vm sshd[13706]: Failed password for root from 192.168.202.49 port 37028 ssh2 Aug 18 00:02:29 centos3-vm sshd[13705]: Failed password for root from 192.168.202.49 port 37024 ssh2

Как это работает?

ENERGY LOGSERVER

...ну а тут — какой метод атаки был использован:



Incident ID: -6Uer4IB9B1_si7K3kNm
Rule Name: Wazuh alert [HIGH] - rule mitre technique: Brute Force

match_body.rule.mitre.id.0	T1110
match_body.rule.mitre.tactic.0	Credential Access
match_body.rule.mitre.technique.0	Brute Force
match_body.rule.nist_800_53.0	AU.14
match_body.rule.nist_800_53.1	AC.7
match_body.rule.nist_800_53.2	SI.4
match_body.rule.pci_dss.0	10.2.4
match_body.rule.pci_dss.1	10.2.5
match_body.rule.pci_dss.2	11.4
match_body.rule.tsc.0	CC6.1

В откровенно непонятном наборе символов, который мы получили с хоста, мы обнаружили и рассмотрели атаку до мельчайших деталей.

Теперь ответьте на вопрос — легко ли было бы достичь этого же результата без **SIEM**?

Чем это полезно?

ENERGY LOGSERVER

Представьте, что ваша компания генерирует сотни ГБ текстовых логов ежедневно. Во всем этом массиве скрывается именно та информация, которая укажет на атаку или критическую уязвимость. Но теперь вы видите сами, что обработать даже один лог — та еще задача. Даже если нанять целую армию специалистов, чьей единственной задачей будет лишь чтение логов — человеческий фактор рано или поздно вмешается в процесс.

Кстати, именно расширением отделов безопасности иногда пытаются компенсировать недостаток возможностей для анализа имеющихся событий. Больше людей сделают больше работы, это факт. Но с учетом количества подобных заданий, как в нашем примере, такое использование человеческого ресурса все равно остается неэффективным.

SIEM-система — это инструмент, который избавит специалистов от рутины и освободит время на стратегию, анализ и реагирование. **SIEM** за считанные секунды обрабатывает тысячи таких случаев, как в нашем примере. Так команда получит время и силы для оптимизации инфраструктуры, реагирования на атаки и внедрение того, что будет способствовать улучшениям. Альтернатива — разбираться днями в куче событий и ложноположительных срабатываний, что в результате приводит лишь к поддержанию текущей нормы.

В итоге **SIEM** сделает эффективнее работу всех решений, поскольку важные события, обнаруженные ими, а также другая полезная информация не пройдут мимо специалистов. В то же время сами специалисты будут продуктивнее, ведь теперь их внимания хватит на все, что действительно нуждается в их вмешательстве.

Energy Logserver — SIEM нового поколения

ENERGY LOGSERVER

SIEM от Energy Logserver удалось стереть верхний предел возможностей. Решение доступно в трех базовых конфигурациях по выбору, каждая из которых имеет определенный набор функций для решения задач разного уровня. Эту основу можно масштабировать и расширять сколь угодно без любых ограничений.

Log Management — все об управлении журналами

- Ролевая модель доступа
- Интеграция с LDAP, AD, Radius, SSO
- Масштабируемая архитектура и кластеризация
- Сотни готовых парсеров, гибкий конструктор.
- Многомерная система уведомлений и отчетности
- Многоуровневая система архивации данных
- Гибкий конструктор дашбордов и готовые шаблоны

SIEM — расширенное управление безопасностью

- Поведенческий анализ пользователей и устройств
- Динамическая интеграция с базами IoC, TTP, Threat Intellegence, MITRE ATT&CK
- GDPR, NIST, CIS, PCI DSS, HIPAA compliance
- File Integrity Monitoring (FIM)
- Сканер уязвимостей
- 1000+ правил детектирования и корреляции
- Помощь в выявлении подозрительного поведения на основе искусственного интеллекта
- Playbooks
- Мониторинг работы приложений и сервисов
- Интегрированная система управления рисками
- Система управления инцидентами

Network Probe — сетевой анализ

- Подробный анализ сетевого трафика
- Анализ Netflow (v5, v9, IPFIX, sflow. iflow. NetStrean)
- Производительность от 10 Gbps
- От 100 000 FPS
- Визуализация трафика на уровнях L2-L7
- Корреляция журналов и данных по трафику
- Проверка трафика согласно репутационным базам и IoC
- Выявление атак нулевого дня
- Анализ активности пользователей в сети

Контакты

ENERGY LOGSERVER©

Energy Logserver — это инструмент, который не вынуждает вас идти на компромиссы и уменьшать требования. Напротив, он расширяет ваши возможности и прибавляет контроля там, где, казалось бы, контроль невозможен.

Чтобы заказать демо-версию Energy Logserver, пишите на электронную почту

els@bakotech.com.

www.energylogserver.com