siem

SIEM-системы функционируют за счет сбора данных из различных источников, включая ПК, сетевые устройства, серверы и многое другое. Затем эти данные стандартизируются и консолидируются для упрощения анализа.

На платформах SIEM работают эксперты по безопасности, которые тщательно изучают данные с целью выявления потенциальных угроз. Эта процедура позволяет компаниям выявлять нарушения безопасности и проверять оповещения, предлагая важную информацию о состоянии безопасности организации.

Оповещения уведомляют персонал служб безопасности / мониторинга о том, что они должны изучить (возможное) событие безопасности или инцидент. Эти уведомления обычно лаконичны и информируют персонал о конкретной атаке, нацеленной на информационные системы организации. Оповещения могут передаваться по нескольким каналам, таким как электронная почта, всплывающие сообщения на консоли, текстовые сообщения или телефонные звонки на смартфоны.

SIEM-системы генерируют огромное количество оповещений из-за значительного объема событий, генерируемых для каждой отслеживаемой платформы. Нет ничего необычного в том, что ежечасный журнал событий варьируется от сотен до тысяч. В результате точная настройка SIEM для обнаружения событий высокого риска и оповещения о них имеет решающее значение.

Способность точно определять события высокого риска - это то, что отличает SIEM от других инструментов сетевого мониторинга и обнаружения, таких как системы предотвращения вторжений (IPS) или Системы обнаружения вторжений (IDS). SIEM не заменяет возможности ведения журнала этих устройств; скорее, он работает совместно с ними, обрабатывая и объединяя данные их журнала для распознавания событий, которые потенциально могут привести к эксплуатации системы. Интегрируя данные из многочисленных источников, решения SIEM обеспечивают целостную
стратегию обнаружения угроз и управления ими.

Бизнес-Требования SIEM и примеры использования

Агрегирование и нормализация журналов

Важность видимости угроз благодаря консолидации журналов, предлагаемой SIEM-системами, невозможно переоценить. В ее отсутствие кибербезопасность организации имеет такую же ценность, как простое пресс-папье. Консолидация журналов влечет за собой сбор терабайт информации о безопасности из важных брандмауэров, конфиденциальных баз данных и важных приложений. Этот процесс позволяет команде SOC изучать данные и распознавать подключения, что значительно улучшает видимость угроз.

Используя консолидацию журналов SIEM, команда SOC может выявлять и тщательно анализировать инциденты и события безопасности во всей ИТ-инфраструктуре организации. Благодаря централизации и сопоставлению информации из различных источников SIEM обеспечивает целостную стратегию обнаружения и обработки угроз. Такой подход позволяет организациям распознавать закономерности, тенденции и нарушения, которые могут указывать на потенциальные угрозы безопасности. Следовательно, команды SOC могут быстро и эффективно реагировать на инциденты безопасности, уменьшая последствия для организации.

Оповещение об Угрозе

Очень важно иметь SIEM-решение, которое может идентифицировать команды ИТ-безопасности и уведомлять их о возможных угрозах в огромном объеме собранных данных о событиях безопасности. Эта функция имеет решающее значение, поскольку позволяет команде ИТ-безопасности проводить более быстрые и целенаправленные расследования и своевременно и эффективно реагировать на потенциальные инциденты безопасности.

Расширенная аналитика и анализ угроз используются SIEM solutions для распознавания потенциальных угроз и генерации оповещений в режиме реального времени. При обнаружении угрозы система направляет оповещения в службу ИТ-безопасности, предоставляя им необходимую информацию для эффективного расследования и снижения риска. Благодаря оперативному

оповещению групп ИТ-безопасности решения SIEM помогают свести к минимуму
потенциальное воздействие инцидентов безопасности и защитить жизненно важные активы организации.

Контекстуализация и реакция

Важно понимать, что простого создания оповещений недостаточно. Если решение SIEM отправляет оповещения о каждом возможном событии безопасности, команда ИТ-безопасности вскоре будет перегружена огромным количеством предупреждений, и ложноположительные срабатывания могут стать частой проблемой, особенно в старых решениях. В результате контекстуализация угроз имеет решающее значение для сортировки предупреждений, определения участников, вовлеченных в событие безопасности, затронутых частей сети и сроков.

Контекстуализация позволяет группам ИТ-безопасности выявлять подлинные потенциальные угрозы и действовать быстро. Автоматизированные процессы настройки могут фильтровать некоторые контекстуализированные угрозы, уменьшая количество оповещений, получаемых командой.

Идеальное решение SIEM должно позволять предприятию напрямую управлять угрозами, часто путем остановки операций на время проведения расследований. Такой подход помогает свести к минимуму потенциальное воздействие инцидентов безопасности и защитить критически важные активы организации. Решения SIEM обеспечивают контекстную и автоматизированную фильтрацию угроз, позволяя группам ИТ-безопасности сосредоточиться на реальных угрозах, снижая утомляемость при оповещении и повышая эффективность реагирования на инциденты.

Соответствие требованиям

Решения SIEM играют важную роль в обеспечении соответствия требованиям, помогая организациям выполнять нормативные требования посредством комплексного подхода к обнаружению угроз и управлению ими.

Такие нормативные акты, как PCI DSS, HIPAA и GDPR, обязывают организации внедрять надежные меры безопасности, включая мониторинг и анализ сетевого трафика в режиме реального времени. Решения SIEM могут

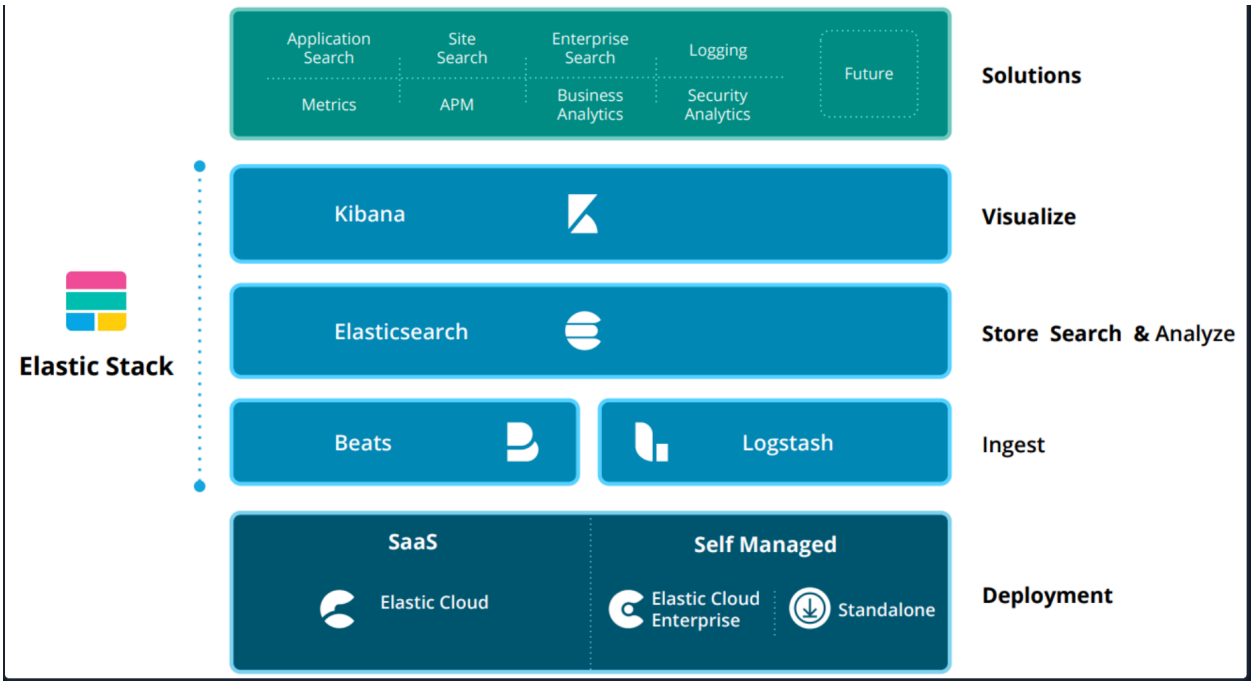
помочь организациям выполнить эти требования, позволяя командам SOC оперативно обнаруживать инциденты безопасности и реагировать на них.

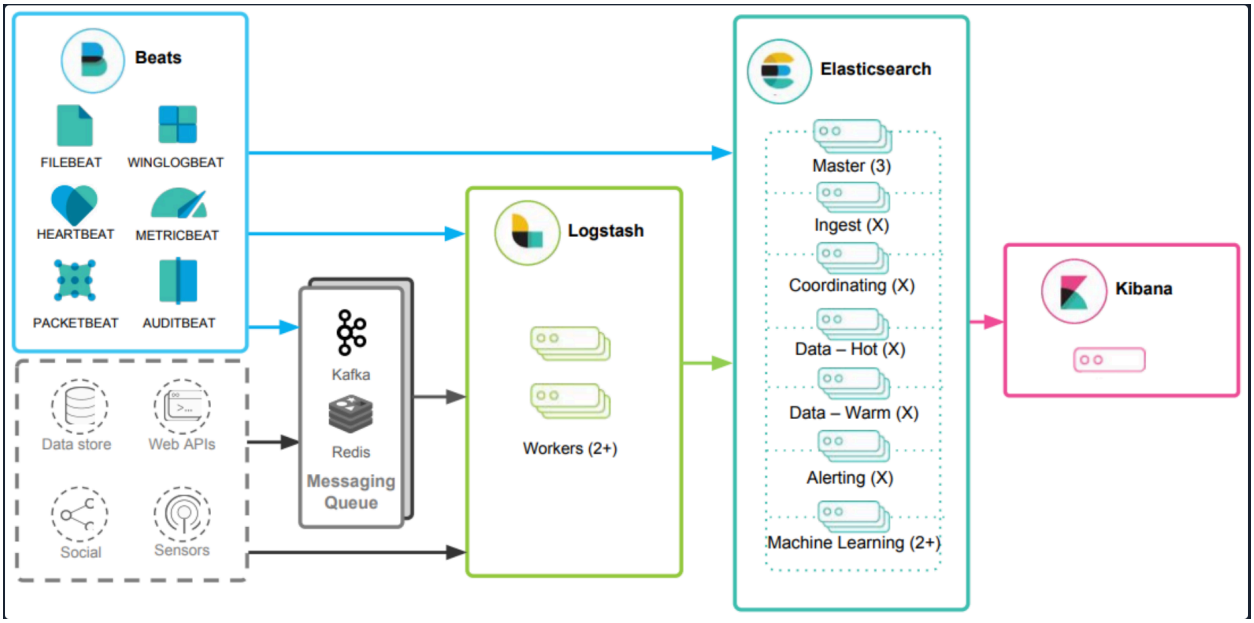
Решения SIEM также предоставляют возможности автоматизированной отчетности и аудита, которые необходимы для обеспечения соответствия требованиям. Эти функции позволяют организациям быстро и точно составлять отчеты о соответствии требованиям, гарантируя, что они соответствуют нормативным требованиям, и могут продемонстрировать соответствие аудиторам и регулирующим органам.

Потоки данных Внутри SIEM

Давайте теперь вкратце рассмотрим, как данные перемещаются внутри SIEM, пока они не будут готовы для анализа.

1. Решения SIEM принимают журналы из различных источников данных. Каждый инструмент SIEM обладает уникальными возможностями для сбора журналов
   из разных источников. Этот процесс известен как прием данных или сбор данных.
2. Собранные данные обрабатываются и нормализуются для понимания механизмом корреляции SIEM. Необработанные данные должны быть записаны
   или прочитаны в формате, который может быть понятен SIEM, и преобразованы в общий формат из различных типов наборов данных. Этот процесс называется нормализацией данных и агрегированием данных.
3. Наконец, самая важная часть SIEM, где команды SOC используют нормализованные данные, собранные SIEM, для создания различных правил обнаружения, информационных панелей, визуализаций, оповещений и инцидентов. Это позволяет команде SOC выявлять потенциальные риски безопасности и быстро реагировать на инциденты безопасности.





Elasticsearch это распределенная поисковая система на основе JSON, разработанная с использованием RESTful API. Являясь основным компонентом Elastic stack, она обрабатывает индексацию, хранение и запросы. Elasticsearch позволяет пользователям выполнять

сложные запросы и выполнять аналитические операции с записями файла журнала, обрабатываемыми Logstash.

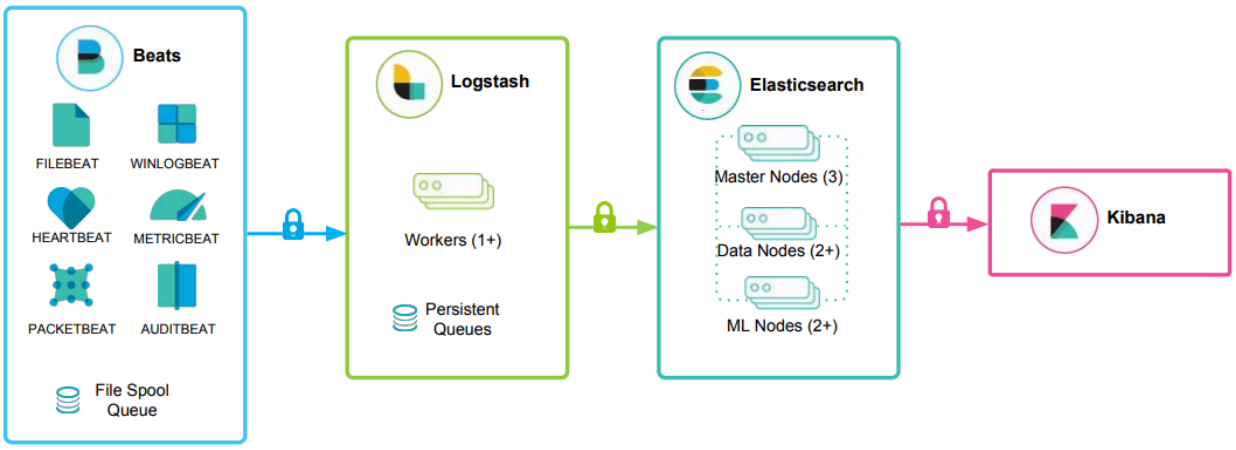
`Logstash` отвечает за сбор, преобразование и транспортировку записей файла журнала. Его сила заключается в способности консолидировать данные из различных источников и нормализовать их. Logstash работает в трех основных областях.:

1. `Process input`: Logstash принимает записи файла журнала из удаленных местоположений, преобразуя их в формат, понятный машинам.
   Он может получать записи с помощью различных методов ввода , таких как чтение из плоского файла, сокета TCP или непосредственно из сообщений системного журнала. После обработки входных данных Logstash переходит к следующей функции.
2. `Transform and enrich log records`: Logstash предлагает множество способов изменять формат записи журнала и даже содержимое. В частности, плагины фильтрации могут выполнять промежуточную обработку события, часто на основе предопределенного условия. Как только запись журнала преобразуется, Logstash обрабатывает ее дальше.
3. `Send log records to Elasticsearch`: Logstash использует плагины вывода для передачи записей журнала в Elasticsearch.

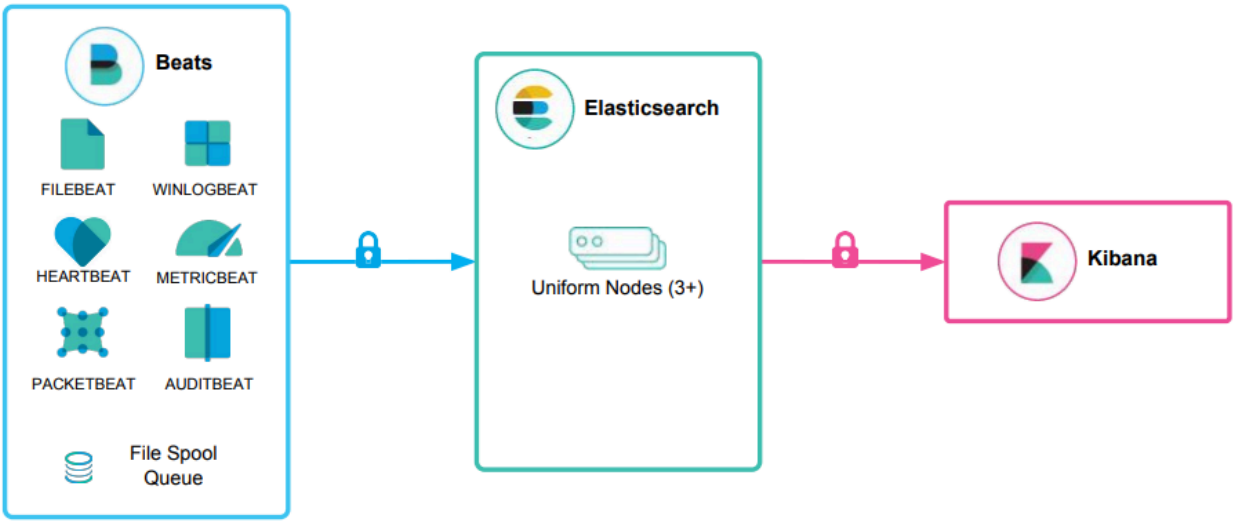
`Kibana` служит инструментом визуализации документов Elasticsearch. Пользователи могут просматривать данные, хранящиеся в Elasticsearch, и выполнять запросы через Kibana. Кроме того, Kibana упрощает понимание результатов запроса с помощью таблиц, диаграмм и пользовательских панелей мониторинга.

Примечание: `Beats` является дополнительным компонентом Elastic stack. Эти легкие универсальные средства передачи данных предназначены для установки на удаленных компьютерах для прямой пересылки журналов и метрик либо в Logstash, либо в Elasticsearch. Beats упрощают процесс сбора данных из различных источников и гарантируют, что Elastic Stack получает необходимую информацию для анализа и визуализации.

`Beats` → `Logstash` → `Elasticsearch` → `Kibana`



Beats → Elasticsearch → Kibana



Эластичный стек Как решение SIEM

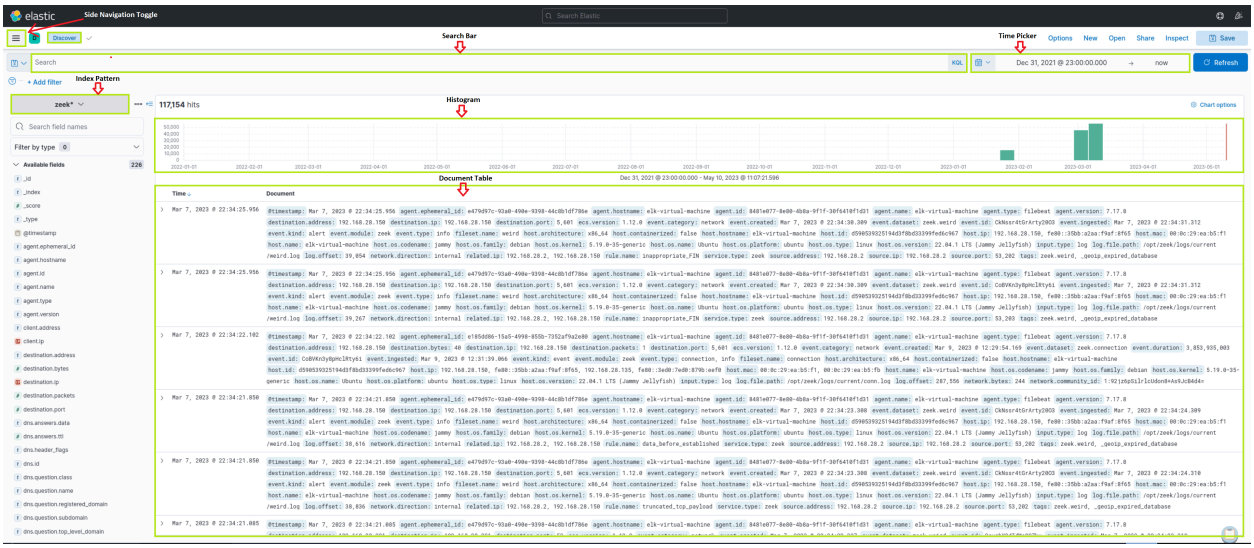
Elastic stack может использоваться в качестве решения для управления информацией о безопасности и событиями (SIEM) для сбора, хранения, анализа и визуализации данных, связанных с безопасностью, из различных источников.

Чтобы реализовать Elastic stack в качестве SIEM-решения, данные, связанные с безопасностью, из различных источников, таких как брандмауэры, идентификаторы / IP-адреса и конечные точки, должны быть загружены в Elastic stack с использованием Logstash. Elasticsearch должен быть настроен для хранения и индексирования данных безопасности, а

Kibana следует использовать для создания пользовательских панелей мониторинга и визуализаций, позволяющих получить представление о событиях, связанных с безопасностью.

Для обнаружения инцидентов, связанных с безопасностью, Elasticsearch можно использовать для выполнения поиска и корреляции собранных данных безопасности.

Как аналитики Центра управления безопасностью (SOC), мы, вероятно, будем широко использовать Kibana в качестве основного интерфейса при работе со стеком Elastic. Поэтому важно хорошо освоить его функциональные возможности.



Kibana Query Language (KQL) - мощный и удобный в использовании язык запросов, разработанный специально для поиска и анализа данных в Kibana. Это упрощает процесс извлечения информации из ваших индексированных данных Elasticsearch, предлагая более интуитивно понятный подход, чем DSL запросов Elasticsearch. Давайте рассмотрим технические аспекты и ключевые компоненты языка KQL.

- `Basic Structure`: Запросы KQL состоят из `field:value` пары, где поле представляет атрибут данных, а значение - данные, которые вы ищете. Например:

Знакомство с Эластичным стеком

```
event.code:4625
```

Уточняя запрос дополнительными условиями, такими как IP-адрес источника, имя пользователя или временной диапазон, аналитики SOC могут получить более конкретную информацию и эффективно расследовать потенциальные инциденты безопасности.

- `Free Text Search`: KQL поддерживает бесплатный текстовый поиск, позволяющий выполнять поиск определенного термина по нескольким
  полям без указания имени поля. Например:

Знакомство с Эластичным стеком

```
"svc-sql1"
```

Этот запрос возвращает записи, содержащие строку "svc-sql1" в любом индексированном поле.

- `Logical Operators`: KQL поддерживает логические операторы AND, ИЛИ, А НЕ для построения более сложных запросов. Круглые скобки можно использовать для группировки выражений и управления порядком вычисления. Например:

Знакомство с Эластичным стеком

```
event.code:4625 AND winlog.event_data.SubStatus:0xC0000072
```

Запрос KQL `event.code:4625 AND winlog.event_data.SubStatus:0xC0000072` фильтрует данные в Kibana, чтобы показывать события с кодом события Windows 4625 (неудачные попытки входа в систему) и значением подстатуса 0xC0000072.

В Windows значение подстатуса указывает причину сбоя входа в систему. Значение подстатуса 0xC0000072 указывает на то, что учетная запись в данный момент отключена.

Используя этот запрос, аналитики SOC могут идентифицировать неудачные попытки входа в систему с отключенными учетными записями. Такое поведение требует дальнейшего изучения, поскольку учетные данные отключенной учетной записи могли быть каким-то образом идентифицированы злоумышленником.

- `Comparison Operators`: KQL поддерживает различные операторы сравнения, такие как `:`, `:>`, `:>=`, `:<`, `:<=`, и `:!`. Эти операторы позволяют определить точные условия для сопоставления значений полей. Например:

Знакомство с Эластичным стеком

```
event.code:4625 AND winlog.event_data.SubStatus:0xC0000072 AND @timesta
mp >= "2023-03-03T00:00:00.000Z" AND @timestamp <= "2023-03-06T23:5
9:59.999Z"
```

Используя этот запрос, аналитики SOC могут идентифицировать неудачные попытки входа в систему с отключенными учетными записями, которые имели место в период с 3 по 6 марта 2023 года

- `Wildcards and Regular Expressions`: KQL поддерживает подстановочные знаки и регулярные выражения для поиска шаблонов в значениях полей. Например:

Знакомство с Эластичным стеком

```
event.code:4625 AND user.name: admin*
```

Запрос Kibana KQL `event.code:4625 AND user.name: admin*` фильтрует данные в Kibana, чтобы показывать события с кодом события Windows 4625 (неудачные попытки входа в систему) и где имя пользователя начинается с "admin", например "administrator", "administrator123" и т.д.

Этот запрос (если он расширен) может быть полезен для выявления потенциально вредоносных попыток входа в систему, нацеленных на учетные записи администраторов.

Как Идентифицировать Доступные Данные

"Как я могу определить доступные поля и значения?" - спросите вы.
Давайте посмотрим, как мы могли бы определить доступные поля и значения, которые мы использовали в этом разделе.

Пример : Определить неудачные попытки входа в систему с отключенными учетными записями, которые имели место в период с

3 марта 2023 года по 6 марта 2023 года
KQL:

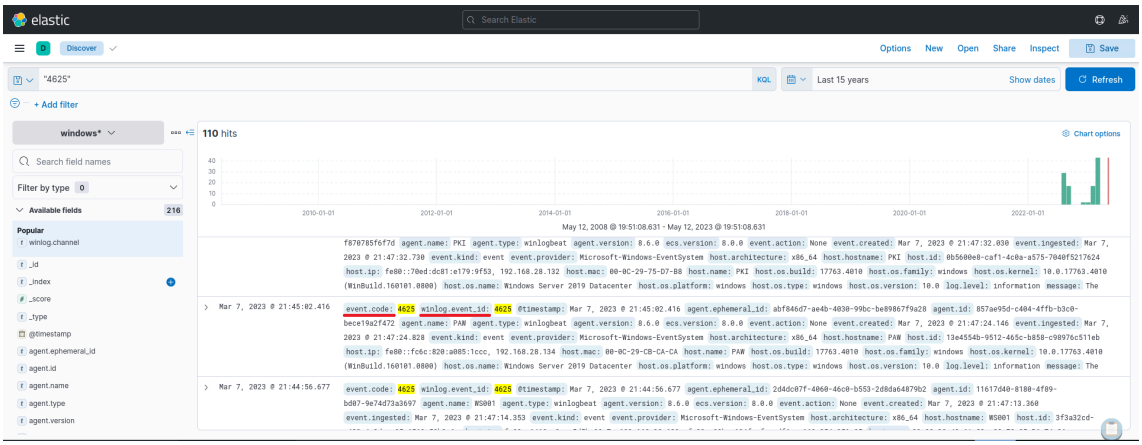
Знакомство с Эластичным стеком

```
event.code:4625 AND winlog.event_data.SubStatus:0xC0000072 AND @timesta
mp >= "2023-03-03T00:00:00.000Z" AND @timestamp <= "2023-03-06T23:5
9:59.999Z"
```

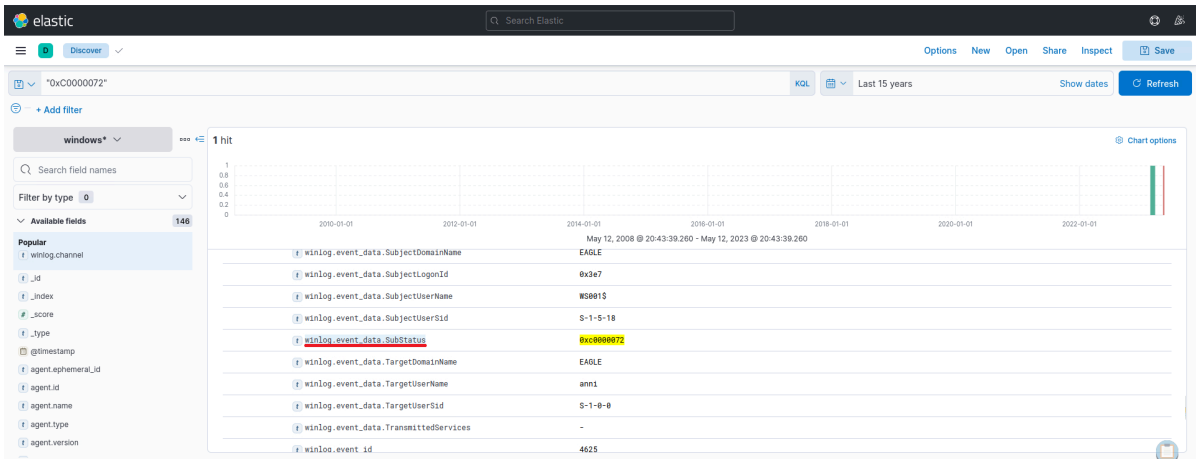
Подход 1 к идентификации данных и полей: используйте бесплатный текстовый поиск KQL

Используя функцию Discover ,
мы можем без особых усилий исследовать и просеивать доступные данные, а также получить представление об архитектуре доступных полей, прежде чем приступать к построению запросов KQL.

- Используя поисковую систему для журналов событий Windows, связанных с неудачными попытками входа в систему, мы наткнемся на такие ресурсы, как
  https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4625
- Используя бесплатный текстовый поиск KQL, мы можем выполнить поиск `"4625"`. В возвращенных записях мы замечаем `event.code:4625`, `winlog.event_id:4625`, и `@timestamp`
  - `event.code` связан с Эластичной общей схемой (ECS)
  - `winlog.event_id` связано с Winlogbeat
  - Если организация, в которой мы работаем, использует Elastic stack во всех офисах и отделах безопасности, предпочтительно использовать поля
    ECS в наших запросах по причинам, которые мы рассмотрим в конце этого
    раздела.
  - `@timestamp` обычно содержит время, извлеченное из исходного события, и оно отличается от `event.created`



- Когда дело доходит до отключенных учетных записей, вышеупомянутый ресурс сообщает нам, что значение подстатуса 0xC0000072 в журнале событий Windows 4625 указывает на то, что учетная запись в данный момент отключена. Опять же, используя бесплатный текстовый поиск KQL, мы можем выполнить поиск `"0xC0000072"`. Расширяя возвращаемую запись, мы замечаем `winlog.event_data.SubStatus` это связано с Winlogbeat



Подход 2 к идентификации данных и полей: использование документации Elastic

Было бы неплохо сначала ознакомиться со всеобъемлющей документацией Elastic, прежде чем углубляться в функцию "Обнаружение". Документация предоставляет обширную информацию о различных типах полей, с которыми мы
можем столкнуться. Вот несколько хороших ресурсов, с которых можно начать::

- Эластичная общая схема (ECS)
- Поля событий эластичной общей схемы (ECS)
- Поля Winlogbeat
- Поля ECS Winlogbeat
- Поля модуля безопасности Winlogbeat
- Поля Filebeat
- Поля ECS Filebeat ECS

Эластичная общая схема (ECS)

Общая схема Elastic (ECS) - это общий и расширяемый словарь для событий и журналов в стеке Elastic, который обеспечивает согласованность форматов полей в различных источниках данных. Когда дело доходит до поиска на языке запросов Kibana (KQL) в стеке Elastic, использование полей ECS дает несколько ключевых преимуществ:

- `Unified Data View`: ECS применяет структурированный и согласованный подход к данным, позволяющий создавать унифицированные представления в нескольких источниках данных. Например, данные, поступающие из журналов Windows, сетевого трафика, событий конечной точки или облачных источников данных, можно искать и сопоставлять, используя одни и те же имена полей.
- `Improved Search Efficiency`: Благодаря стандартизации имен полей для разных типов данных ECS упрощает процесс написания запросов в KQL. Это означает, что аналитики могут эффективно создавать запросы без необходимости запоминать конкретные имена полей для каждого источника данных.
- `Enhanced Correlation`: ECS позволяет упростить корреляцию событий из разных источников, что играет ключевую роль в расследованиях кибербезопасности. Например, вы можете сопоставить IP-адрес, задействованный в инциденте безопасности, с журналами сетевого трафика,

журналами брандмауэра и данными конечной точки, чтобы получить более полное представление об инциденте.

- `Better Visualizations`: Согласованные соглашения об именовании полей повышают эффективность визуализаций в Kibana. Поскольку все источники данных придерживаются одной и той же схемы, создание информационных панелей и визуализаций становится проще и интуитивно понятнее. Это может помочь в выявлении тенденций, выявлении аномалий и визуализации инцидентов безопасности.
- `Interoperability with Elastic Solutions`: Использование полей ECS обеспечивает полную совместимость с передовыми функциями и решениями Elastic Stack, такими как Elastic Security, Elastic Observability и Elastic Machine Learning. Это позволяет осуществлять расширенный поиск угроз, обнаружение аномалий и мониторинг производительности.
- `Future-proofing`: Поскольку ECS является основополагающей схемой в стеке Elastic, внедрение ECS обеспечивает будущую совместимость с усовершенствованиями и новыми функциями, которые внедряются в экосистему Elastic.

Роли в SOC

Команда SOC состоит из различных ролей, ответственных за непрерывный операционный аспект информационной безопасности предприятия. Эти роли могут включать:

- `SOC Director`: Отвечает за общее управление и стратегическое планирование SOC, включая составление бюджета, укомплектование персоналом и приведение в соответствие с целями организации в области безопасности.
- `SOC Manager`: Контролирует повседневные операции, управляет командой, координирует усилия по реагированию на инциденты и

обеспечивает бесперебойное сотрудничество с другими подразделениями.

- `Tier 1 Analyst`: Отслеживает оповещения и события системы безопасности, сортирует потенциальные инциденты и переводит их на более высокие уровни для дальнейшего расследования.
- `Tier 2 Analyst` Выполняет углубленный анализ эскалации инцидентов, выявляет закономерности и тенденции, а также разрабатывает стратегии смягчения последствий для устранения угроз безопасности.
- `Tier 3 Analyst`: Предоставляет передовой опыт в обработке сложных инцидентов безопасности, проводит мероприятия по поиску угроз и сотрудничает с другими командами для улучшения состояния безопасности организации.
- `Detection Engineer`: Инженер по обнаружению отвечает за разработку, внедрение и поддержание правил обнаружения и сигнатур для инструментов мониторинга безопасности, таких как SIEM, IDS / IPS и EDR-решения. Они тесно сотрудничают с аналитиками по безопасности, чтобы выявить пробелы в охвате обнаружения и постоянно улучшать способность
организации обнаруживать угрозы и реагировать на них.
- `Incident Responder`: Берет на себя ответственность за активные инциденты безопасности, проводит углубленную цифровую криминалистику, меры по локализации и исправлению, а также сотрудничает с другими командами для восстановления затронутых систем и предотвращения подобных инцидентов в будущем.
- `Threat Intelligence Analyst`: Собирает, анализирует и распространяет аналитические данные об угрозах, чтобы помочь членам команды SOC лучше понимать ландшафт угроз и активно защищаться от возникающих рисков.
- `Security Engineer`: Разрабатывает, развертывает и поддерживает инструменты, технологии и инфраструктуру безопасности, а также предоставляет техническую экспертизу команде SOC.
- `Compliance and Governance Specialist`: Обеспечивает соответствие методов и процессов обеспечения безопасности организации соответствующим отраслевым стандартам, нормативным актам и

передовой
практике, а также помогает с требованиями аудита и отчетности.

- `Security Awareness and Training Coordinator`:
  Разрабатывает и внедряет программы обучения и повышения осведомленности
  по вопросам безопасности для ознакомления сотрудников с передовыми практиками кибербезопасности и продвижения культуры безопасности внутри
  организации.

Важно отметить, что конкретные роли и обязанности на каждом уровне могут варьироваться в зависимости от размера организации, отрасли и конкретных требований безопасности.

В общем случае многоуровневую структуру можно описать следующим образом:

- `Tier 1 Analysts`: Также известные как "службы быстрого
  реагирования", эти аналитики отслеживают события безопасности и оповещения, выполняют первоначальную сортировку и переводят потенциальные инциденты на более высокие уровни для дальнейшего расследования. Их главная цель - быстро выявлять инциденты безопасности и расставлять приоритеты.
- `Tier 2 Analysts`: Эти аналитики более опытны и проводят
  более глубокий анализ обострившихся инцидентов. Они выявляют закономерности и тенденции, разрабатывают стратегии смягчения последствий и иногда помогают в усилиях по реагированию на инциденты. Они также могут отвечать за настройку инструментов мониторинга безопасности для уменьшения количества ложных срабатываний и улучшения
  возможностей обнаружения.
- `Tier 3 Analysts`: Аналитики уровня 3, которых часто
  считают самыми опытными и осведомленными аналитиками в команде, работают с самыми сложными и резонансными инцидентами безопасности. Они также
  могут участвовать в упреждающем поиске угроз, разрабатывать передовые

стратегии обнаружения и предотвращения и сотрудничать с другими командами для улучшения общего состояния безопасности организации.

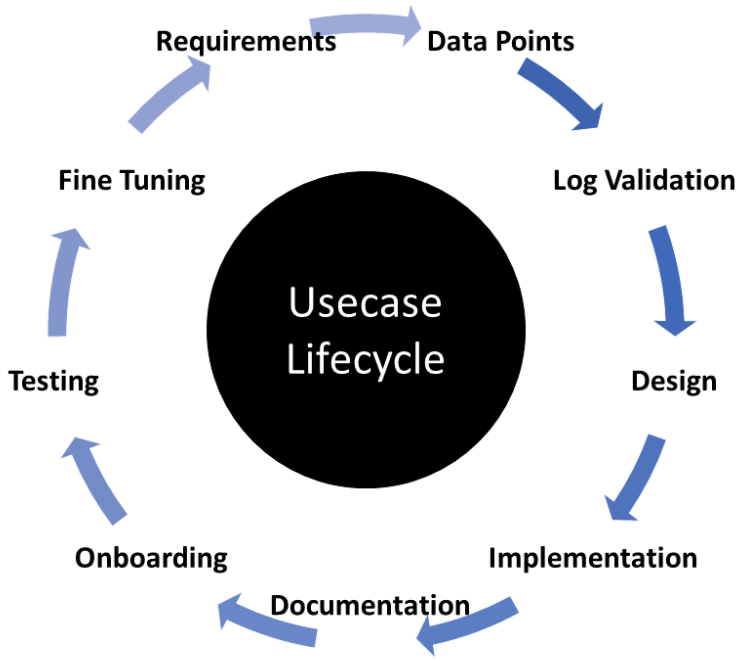
SOC 1.0 — это начальный этап, ориентированный на сетевую безопасность. Он использовал разрозненные инструменты, что приводило к несвязанным оповещениям и неэффективности. Некоторые организации до сих пор полагаются на этот устаревший подход.

Переход к **SOC 2.0** был вызван появлением сложных, многовекторных угроз. Эта версия основана на интеллектуальном анализе данных (телеметрия, информация об угрозах), что позволяет выявлять скрытые атаки. Акцент сместился на полную осведомленность о ситуации, управление уязвимостями и совместную работу.

Когнитивный SOC (следующее поколение) призван устранить недостатки SOC 2.0, такие как нехватка экспертизы и слабое взаимодействие с бизнесом. Для этого внедряются системы машинного обучения, которые помогают принимать решения и реагировать на инциденты, со временем повышая свою эффективность.

Жизненный цикл разработки вариантов использования SIEM

При разработке любых вариантов использования необходимо учитывать следующие важные этапы:



1. Requirements:
   Поймите цель или необходимость варианта использования, точно определив
   конкретный сценарий, для которого требуется оповещение. Требования могут быть предложены заказчиками, аналитиками или сотрудниками. Например,
   целью может быть разработка варианта использования обнаружения для атаки методом перебора, который запускает оповещение после 10 последовательных сбоев входа в систему в течение 4 минут.
2. Data Points:
   Определите все точки передачи данных в сети, где учетная запись пользователя может быть использована для входа в систему. Соберите информацию об источниках данных, которые генерируют журналы для попыток
   несанкционированного доступа или сбоев входа в систему. Например, данные могут поступать с компьютеров под управлением Windows, Linux, конечных
   точек, серверов или приложений. Убедитесь, что в журналах фиксируются важные сведения, такие как пользователь, временная метка, источник, место назначения и т.д.

3. `Log Validation`:
   Проверяйте журналы, убедившись, что они содержат всю важную информацию,
   такую как пользователь, временная метка, источник, место назначения, имя компьютера и название приложения. Подтвердите, что все журналы получены во время различных событий аутентификации пользователя для критических
   точек данных, включая локальную, веб-аутентификацию, аутентификацию приложений, VPN и OWA (Outlook).

4. `Design and Implementation`:
   После определения и проверки всех журналов с различными точками данных и источниками приступайте к разработке варианта использования, определяя
   условия, при которых должно срабатывать оповещение. Учитывайте три основных параметра: условие, агрегирование и приоритет. Например, в случае использования атаки методом перебора создайте оповещение о 10 сбоях входа в систему за 4 минуты, учитывая при этом агрегирование, чтобы избежать ложных срабатываний, и установив приоритет оповещения на
   основе привилегий целевого пользователя.

5. `Documentation`:
   Стандартные операционные процедуры (SOP) подробно описывают стандартные
   процессы, которым аналитики должны следовать при работе с оповещениями.
   Сюда входят условия, агрегированные данные, приоритеты и информация о других командах, которым аналитики должны сообщать о действиях. SOP также содержит матрицу эскалации.

6. `Onboarding`:
   Начните со стадии разработки, прежде чем переносить оповещение непосредственно в производственную среду. Определите и устраните все пробелы, чтобы уменьшить количество ложных срабатываний, затем переходите к производству.

7. `Periodic Update/Fine-tuning`:
   Получайте регулярную обратную связь от аналитиков и поддерживайте

актуальные правила корреляции, внося их в белый список. Постоянно уточняйте и оптимизируйте вариант использования, чтобы обеспечить его эффективность и точность.

Как создать варианты использования SIEM

- Осознайте свои потребности, риски и установите соответствующие оповещения для мониторинга всех необходимых систем.
- Определите приоритет и воздействие, затем сопоставьте оповещение с цепочкой уничтожений или структурой MITRE.
- Установите время до обнаружения (TTD) и Время до реагирования (TTR) для оповещения, чтобы оценить эффективность SIEM и производительность аналитиков.
- Создайте стандартную операционную процедуру (SOP) для управления оповещениями.
- Опишите процесс уточнения оповещений на основе мониторинга SIEM.
- Разработайте План реагирования на инциденты (IRP) для устранения действительно позитивных инцидентов.
- Установите соглашения об уровне обслуживания (SLA) и Соглашения об оперативном уровне (OLA) между командами для обработки оповещений и соблюдения IRP.
- Внедрите и поддерживайте процесс аудита для управления предупреждениями и отчетами аналитиков об инцидентах.
- Создайте документацию для проверки состояния регистрации машин или систем, основы для создания оповещений и частоты их срабатывания.
- Создайте документ базы знаний, содержащий важную информацию и обновления инструментов управления обращениями.

Что такое сортировка оповещений?

Alert triaging, выполняемый аналитиком Центра операций безопасности (SOC), представляет собой процесс оценки и приоритизации

предупреждений безопасности, генерируемых различными системами мониторинга и обнаружения, для определения их уровня угрозы и потенциального воздействия на системы и данные организации. Это включает систематический анализ и категоризацию предупреждений для эффективного распределения ресурсов и реагирования на инциденты безопасности.

`Escalation` является важным аспектом сортировки оповещений в среде SOC. Процесс эскалации обычно включает уведомление руководителей, групп реагирования на инциденты или назначенных лиц в организации, которые уполномочены принимать решения и координировать усилия по реагированию. Аналитик SOC предоставляет подробную информацию
об оповещении, включая его серьезность, потенциальное воздействие и любые соответствующие выводы, сделанные в ходе первоначального расследования. Это позволяет лицам, принимающим решения, оценить ситуацию и определить соответствующий план действий, такой как привлечение специализированных групп, инициирование более широких процедур реагирования на инциденты или привлечение внешних ресурсов, если это необходимо.

Эскалация гарантирует оперативное получение важных предупреждений и облегчает эффективную координацию между различными заинтересованными сторонами, позволяя своевременно и эффективно реагировать на потенциальные инциденты безопасности. Это помогает использовать опыт и возможности принятия решений сотрудников, ответственных за управление угрозами или инцидентами более высокого уровня внутри организации и их смягчение.

Каков идеальный процесс сортировки?

1. `Initial Alert Review`:

- Тщательно просмотрите первоначальное оповещение, включая метаданные, временную метку, IP-адрес источника, IP-адрес назначения, затронутые системы и запускающее правило / подпись.
- Проанализируйте связанные журналы (сетевой трафик, систему, приложение), чтобы понять контекст предупреждения.

1. `Alert Classification`:

- Классифицируйте предупреждение на основе серьезности, воздействия и срочности, используя предопределенную систему классификации организации.

1. `Alert Correlation`:

- Сопоставьте предупреждение со связанными предупреждениями, событиями или инцидентами, чтобы выявить закономерности, сходства или потенциальные индикаторы компрометации (IoC).
- Запросите SIEM или систему управления журналами, чтобы собрать соответствующие данные журнала.
- Используйте каналы аналитики угроз для проверки известных шаблонов атак или сигнатур вредоносных программ.

1. `Enrichment of Alert Data`:

- Соберите дополнительную информацию, чтобы обогатить данные оповещений и получить контекст:
  - Собирайте записи сетевых пакетов, дампы памяти или образцы файлов, связанные с предупреждением.
  - Используйте внешние источники информации об угрозах, инструменты с открытым исходным кодом или изолированные программы для анализа подозрительных файлов, URL-адресов или IP-адресов.
  - Проведите проверку затронутых систем на наличие аномалий (сетевые подключения, процессы, модификации файлов).

1. `Risk Assessment`:

- Оцените потенциальный риск и воздействие на критически важные активы, данные или инфраструктуру:
  - Учитывайте ценность затронутых систем, чувствительность данных, требования соответствия и последствия для регулирования.
  - Определите вероятность успешной атаки или потенциального бокового движения.

1. `Contextual Analysis`:

- Аналитик учитывает контекст, связанный с предупреждением, включая затронутые активы, их критичность и чувствительность обрабатываемых

ими
данных.

- Они оценивают существующие средства контроля безопасности, такие как брандмауэры, системы обнаружения / предотвращения вторжений и решения
для защиты конечных точек, чтобы определить, указывает ли предупреждение на потенциальный сбой управления или метод уклонения.
- Аналитик оценивает соответствующие требования к соблюдению требований, отраслевые нормативные акты и контрактные обязательства, чтобы понять последствия предупреждения для состояния организации в области соблюдения законов и нормативных актов.

1. `Incident Response Planning`:

- Инициируйте план реагирования на инцидент, если предупреждение является значительным:
  - Документируйте сведения о предупреждениях, затронутых системах, наблюдаемом поведении, потенциальных IoC и данных об обогащении.
  - Назначьте членам группы реагирования на инциденты определенные роли и обязанности.
  - Координируйте работу с другими командами (сетевые операции, системные администраторы, поставщики) по мере необходимости.

1. `Consultation with IT Operations`:

- Оцените потребность в дополнительном контексте или недостающей информации, проконсультировавшись с ИТ-подразделениями или соответствующими подразделениями:
  - Участвуйте в обсуждениях или встречах, чтобы получить информацию о затронутых системах, недавних изменениях или текущих мероприятиях по
техническому обслуживанию.
  - Сотрудничайте, чтобы разобраться в любых известных проблемах, неправильных конфигурациях или сетевых изменениях, которые потенциально
могут приводить к ложноположительным предупреждениям.

    - Получите целостное представление об окружающей среде и любых действиях, не связанных с вредоносным ПО, которые могли вызвать оповещение.
    - Задокументируйте выводы и информацию, полученные в ходе консультации.

1. `Response Execution`:

- На основе анализа предупреждений, оценки рисков и консультаций определите соответствующие ответные действия.
- Если дополнительный контекст разрешает предупреждение или идентифицирует его как событие, не связанное с вредоносным ПО, выполните необходимые действия без эскалации.
- Если предупреждение по-прежнему указывает на потенциальные проблемы с безопасностью или требует дальнейшего расследования, приступайте к действиям по реагированию на инцидент.

1. `Escalation`:

- Определите триггеры для эскалации на основе политик организации и серьезности предупреждений:
    - Триггеры могут включать в себя компрометацию критически важных систем / активов, продолжающиеся атаки, незнакомые / сложные методы,
      широкомасштабное воздействие или внутренние угрозы.
- Оцените предупреждение о срабатывании триггеров эскалации, учитывая потенциальные последствия, если они не будут усилены.
- Следуйте внутреннему процессу эскалации, уведомляя команды более высокого уровня / руководство, ответственное за реагирование на инциденты.
- Предоставьте исчерпывающую сводку предупреждений, их серьезность, потенциальное воздействие, дополнительные данные и оценку риска.
- Документируйте все сообщения, связанные с эскалацией.
- В некоторых случаях переходите к внешним организациям (правоохранительным органам, поставщикам услуг реагирования на

инциденты, сертификатам) на основе законодательных / нормативный требований.

1. `Continuous Monitoring`:

- Постоянно следите за ситуацией и ходом реагирования на инциденты.
- Поддерживайте открытую коммуникацию с расширенными командами, предоставляя обновленную информацию о разработках, выводах или изменениях в степени серьезности / воздействии.
- Тесно сотрудничайте с усиленными командами для скоординированного реагирования.

1. `De-escalation`:

- Оцените необходимость деэскалации по мере продвижения реагирования на инцидент и того, как ситуация находится под контролем.
- Деэскалация происходит, когда риск снижен, инцидент локализован и дальнейшая эскалация становится ненужной.
- Уведомите соответствующие стороны, предоставив краткое описание предпринятых действий, результатов и извлеченных уроков.

Регулярно пересматривайте и обновляйте процесс, приводя его в соответствие с политикой, процедурами и руководящими принципами организации. Адаптируйте процесс к возникающим угрозам и меняющимся потребностям.

Skill Assessment

1. Navigate to http://[Target IP]:5601, click on the side navigation toggle, and click on "Dashboard". Review the "Failed logon attempts [All users]" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst”

   Consult with IT Operations

2. Navigate to http://[Target IP]:5601, click on the side navigation toggle, and click on "Dashboard". Review the "Failed logon attempts [Disabled user]" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

   Escalate to a Tier 2/3 analyst

3. Navigate to http://[Target IP]:5601, click on the side navigation toggle, and click on "Dashboard". Review the "Failed logon attempts [Admin users only]" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

   Nothing suspicious

4. Navigate to http://[Target IP]:5601, click on the side navigation toggle, and click on "Dashboard". Review the "RDP logon for service account" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

   Escalate to a Tier 2/3 analyst

5. Navigate to http://[Target IP]:5601, click on the side navigation toggle, and click on "Dashboard". Review the "User added or removed from a local group" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

   Consult with IT Operations

6. Navigate to http://[Target IP]:5601, click on the side navigation toggle, and click on "Dashboard". Review the "Admin logon not from PAW" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

Consult with IT Operations

7. Navigate to http://[Target IP]:5601, click on the side navigation toggle, and click on "Dashboard". Review the "SSH Logins" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

   Escalate to a Tier 2/3 analyst