SIEM ДЛЯ ЧАЙНИКОВ

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

www.alienvault.com

Применяющиеся технологии
SLM/LMS, SIM, SEM, SEC, SIEM

Хотя ИТ-индустрия и сделала выбор в пользу термина «SIEM», как универсального для этого типа решений информационной безопасности, он развился из нескольких различных технологий, которые были до него.

- **LMS** (Система управления логами, англ. Log Management System) – система, которая собирает и хранит логи (операционных систем, приложений и т. д.) с нескольких хостов и систем в одном месте, обеспечивая централизованный доступ к этим данным.

- **SLM / SEM** (Система управления логами/событиями, англ. Security Log/Event Management) – SLM предназначена в первую очередь для аналитиков по безопасности, а не системных администраторов. SEM – это система определения наиболее значимых для безопасности событий.

- **SIM** (Система управления информацией, англ. Security information Management) – это система управления активами с возможностями обработки событий безопасности. С ее помощью хосты могут генерировать отчеты об уязвимостях в системе, обнаруживать вторжения, предупреждения антивируса могут быть показаны в соответствии с определенной системой.

- **SEC** (Корреляция событий безопасности, англ. Security Event Correlation) – три неудачные попытки входа в одну учетную запись из трех разных источников – это всего три строки в логах. Для аналитика это своеобразная последовательность событий, которые необходимо рассмотреть более подробно, а поиск шаблонов в логах – причина подать сигнал тревоги, когда это происходит.

- **SIEM** (Управление информацией и событиями безопасности, англ. Security information and Event Managemen) – это все вышеперечисленное. Поскольку вышеупомянутые технологии объединяются в отдельных продуктах, произошел общий термин для управления событиями и информацией, созданной с помощью элементов управления и инфраструктуры безопасности. Мы будем использовать термин SIEM для остальной части этой брошюры.

В: Что в логах?
В: **Что в логах?!!**

О: Вопросы, на которые нужно дать ответ:
О: “**Кто сегодня нас атакует?**”
О: “**Как они получили доступ к нашей корпоративной сети?**”

Многие думают, что элементы управления безопасностью дают полную информацию, необходимую для обеспечения безопасности. Но часто они содержат только то, что они обнаружили – в них нет контекста «до и после».

Этот контекст, как правило, очень важен для того, чтобы отделить “ложное положительное” (false positive) от “истинного” (true) обнаружения, реальную атаку от просто неправильно настроенной системы.

Успешные атаки на компьютерные системы редко выглядят как настоящие атаки, за исключением самых примитивных. Если бы это было не так, мы могли бы автоматизировать все средства защиты без необходимости использования человеческих сил.

Злоумышленники обычно пытаются удалить или исправить записи в логах, чтобы спрятать свои следы. Ведь это источник информации, которому можно доверять, и который имеет критически важное значение для любого исследования вмешательства в работу компьютерных систем.

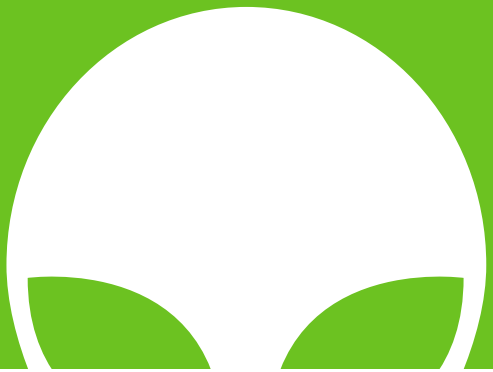
Слепые и слон

SIEM более подробно и детально видит то, что происходит в вашей сети, чем это может обеспечить любая другая система управления безопасностью или источник информации:

- ваша система обнаружения вторжений (IDS) распознает только пакеты, протоколы и IP-адреса;
- ваш Endpoint Security видит файлы, имена хостов и пользователей;
- в ваших service logs отображаются логины пользователей, активность служб и изменения конфигурации;
- ваша система управления активами видит приложения, процессы и владельцев.

Ничего из вышеперечисленного по отдельности не может сказать, что происходит у вас в системе...
Но вместе они могут!

SIEM
Единый взгляд на вашу безопасность



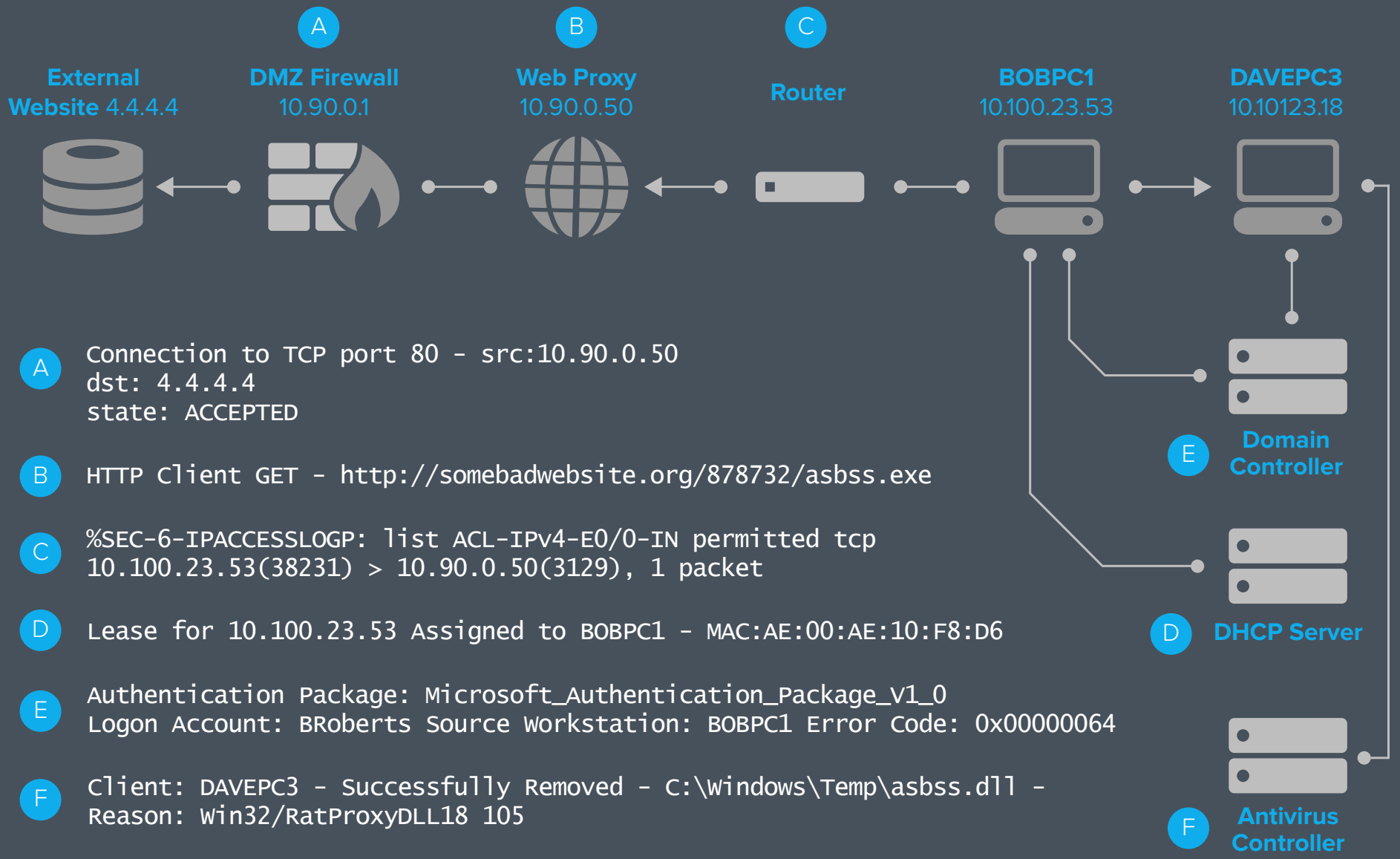
SIEM – это просто управление над имеющимися системами и контроль безопасности.

Он объединяет и унифицирует информацию, содержащуюся в ваших системах, позволяя анализировать ее и управлять при помощи единого интерфейса.

SIEM является прекрасным примером принципа «garbage in, garbage out».
SIEM полезен только тогда, когда вы отправляете ему информацию.

Чем более полная информация о вашей сети, системах и активах, которую получает SIEM, тем более эффективнее он будет помогать вам обнаруживать и анализировать угрозы.

Компьютер Боба был скомпрометирован файлом asbss.exe, который попал с вредоносного веб-сайта. Этот зловред затем использовал учетную запись Боба, чтобы попытаться заразить davEPC3, но антивирус поймал его. Однако, машина Боба "bobPC1", вероятно, все еще скомпрометирована. **Мы должны блокировать вредоносный домен и очистить рабочее пространство Боба, как можно скорее.**



Пуд логов и переполненная чаша записей об активах

- Сбор логов – это сердце и душа SIEM. Чем больше источников логов, отправляющих данные в SIEM, тем больше может быть достигнуто с помощью этой системы.
- Необработанные логи сами по себе редко содержат легкую для понимания информацию.
- Эксперты по безопасности ограничены временем и возможностями, чтобы контролировать каждую операцию в системе.
- При помощи логов специалисты видят только информацию типа «Connection from host A to host B».
- Аналитик нуждается в информации, чтобы сделать обоснованную оценку любого события, связанного с безопасностью.
- Для получения полной информации из логов необходим процесс корреляции.

Рецепт от шефа: список ингредиентов для качественного развертывания SIEM

ЛОГИ И СИГНАЛЫ ТРЕВОГИ

Контроль безопасности

- обнаружение вторжений
- защита конечных точек (антивирус и т. д.)
- предотвращение утечки данных
- VPN-концентраторы
- веб-фильтры
- межсетевые экраны

Инфраструктура

- маршрутизаторы
- коммутаторы
- контроллеры доменов
- беспроводные точки доступа
- серверы приложений
- базы данных
- корпоративне порталы и приложения

ИНФОРМАЦИЯ ОБ ИНФРАСТРУКТУРЕ

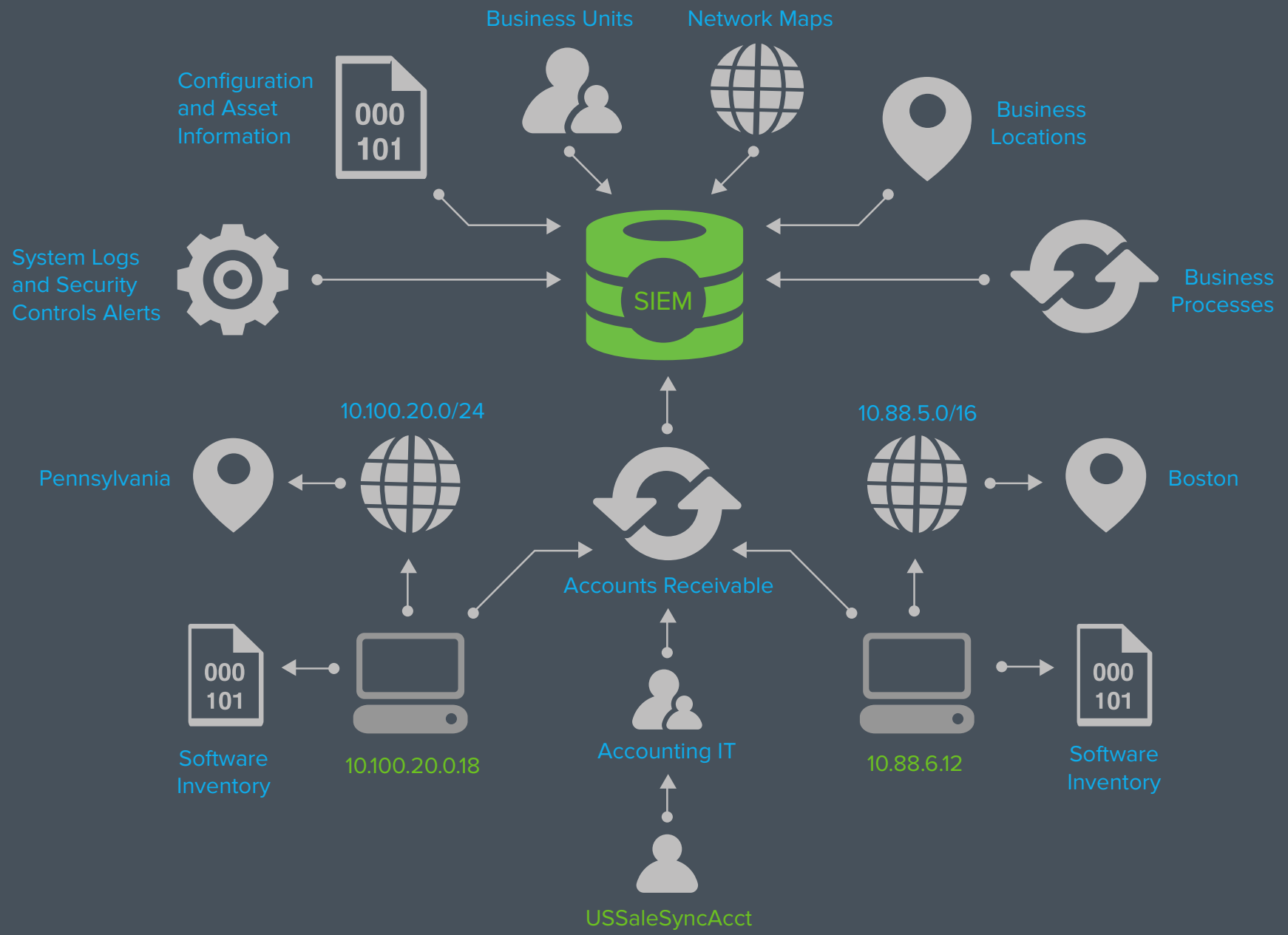
Данные об активах

- конфигурация
- местоположения
- владельцы
- сетевые карты
- отчеты об уязвимостях
- инвентаризация ПО

Бизнес-информация

- сопоставления бизнес-процессов
- точки соприкосновения
- партнерская информация

КАК ГЕНЕРИРУЮТСЯ ЛОГИ В ВАШЕЙ СЕТИ



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

Держитесь: сила корреляции

Корреляция – это процесс сопоставления событий с различных систем (хостов, сетевых устройств, элементов управления безопасностью и всего другого, что отправляет логи в SIEM).

События из разных источников могут быть объединены и сопоставлены друг с другом для обнаружения моделей поведения, невидимых для отдельных устройств.

Они также могут быть сопоставлены с уникальной для **вашего бизнеса** информацией.

Корреляция позволяет автоматизировать обнаружение событий, которые **не должны** возникать в вашей сети.

Красота **корреляции логов**

Чтобы понять разницу между обычным информированием и корреляцией логов сравните это:

```
“14:10 7/4/20110 User BRoberts Successful Auth to
10.100.52.105 from 10.10.8.22”
```

и это:

```
“Учетная запись из отдела маркетинга подключилась к
системе с офисного компьютера в тот день, когда никто
не должен находиться в офисе”
```

Медленно готовьте в течении восьми часов
Подавайте голодным аналитикам

Ваша сеть генерирует огромное количество данных. Например, компании из списка Fortune 500 могут генерировать 10 ТБ текстовых логов в месяц, и это в обычном режиме.

Вы не можете нанять большое количество людей, чтобы искать несоответствия в каждой строке этих логов. Серьезно, даже не думайте об этом. Даже если вы прочитаете каждую строку, вам будет настолько скучно, что вы никогда ничего не обнаружите, даже если это будет прямо перед вашими глазами.

Корреляция логов позволяет определять подозрительные события в ваших системах, и помогает аналитикам понять, что необходимо исследовать дополнительно.

Они смогут обнаружить кусочки информации, которые приводят к другим фрагментам информации, и так далее.

Это позволяет выполнить поиск логов и найти подозрительную активность в базе данных, это одна из функций SIEM.

Хорошо, что SIEM – это по большому счету...

...Гигантская база данных с логами

Было бы очень удобно, если бы каждая ОС и каждое приложение в мире записывали свои логи в одинаковом формате. Но это не так. Большинство логов написано, чтобы их читали люди, а не компьютеры.

По этой причине использование поиска логов из разных источников становится затруднительным.

Эти два лога говорят одно и то же для человека,
но очень отличаются с точки зрения машины:

```
“User Broberts Successfully Authenticated to
10.100.52.105 from client 10.10.8.22”

“100.100.52.105 New Client Connection 10.10.8.22
on account: Broberts: Success”
```

Нам необходимо преобразовать каждый лог в приемлемый для человека формат

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

“100.100.52.105 New Client Connection 10.10.8.22
on account: Broberts: Success”
```

Поэтому, когда вы видите SIEM, в описании которого говорится о том, сколько устройств он поддерживает – имеется ввиду с какого количества устройств он может собирать и анализировать логи.

Поиск и кросс-корреляция

Разбирая логи на составляющие, мы нормализуем их, что позволяет производить поиск в логах с нескольких устройств и коррелировать события между ними. Как только мы нормализовали логи и добавили в таблицу базы данных, мы можем выполнять поиск в стиле базы данных, например:

```
Show [All Logs] From [All Devices] from the [last two
weeks], where the [username] is [Broberts]
```

Это позволяет нам также выполнять автоматическую корреляцию, сравнивая поля между логами, периодами времени, типами устройств.

```
Если определенный актив ошибается при входе на 3 разных
сервера, использовав одинаковые логин и пароль за последние
6 секунд, подать сигнал тревоги
```

Как и в случае с любой базой данных, нормализация событий позволяет формировать итоговый отчет, основываясь на информации в логах.

```
Какие учетные записи пользователей получили доступ к
наибольшему числу отдельных хостов за последний месяц?

Какая подсеть генерирует наибольшее количество неудачных
попыток входа в день в среднем за полгода?
```

Но погодите, **есть кое-что еще!**

- Теперь вы знаете, что SIEM — это способ собирать и обрабатывать данные с систем, которые формируют вашу информационную инфраструктуру.

- SIEM может давать аналитикам доступ к информации из систем, не предоставляя им доступ к самим системам.

- Корреляция событий позволяет кодировать знания(encode security knowledge) о безопасности в автоматическом поиске событий и информации об активах. Это нужно для предупреждения о событиях, которые происходят в вашей системе, и служит отправной точкой для анализа логов.

- Чтобы оставаться в курсе сегодняшних угроз и вектора их развитий, вам необходимо больше, чем просто SIEM.
  Вам нужны соответствующие данные, унифицированный подход и интегрированная информация об угрозах, чтобы действительно получить полную картину о структуре вашей безопасности.

AlienVault® USM™

предоставляет это все вместе

SIEM и Log Management

Быстро коррелируйте и анализируйте события безопасности при помощи встроенных SIEM и Log Management

powered by

AV Labs Threat Intelligence

Определение и инвентаризация активов

Обнаруживайте все активы в вашей сети при помощи пассивного и активного сканирования

Мониторинг поведения

Анализируйте NetFlow (sFlow), следите за сервисами на ваших устройствах

Определение вторжений

Определяйте и реагируйте на угрозы быстрее со встроенной сетевой системой обнаружения вторжений (NIDS), хостовой системой обнаружения вторжений (HIDS) и мониторингом целостности файлов

Сканер уязвимостей

Находите уязвимости на ваших активах при помощи активного сетевого сканирования и беспрерывного мониторинга уязвимостей

Features:	AlienVault USM	Traditional SIEM
Management		
Log Management	✓	✓
Event Management	✓	✓
Event Correlation	✓	✓
Reporting	✓	✓
Trouble Ticketing	Built-in	$$ (3rd-party product that requires integration)
Security Monitoring Technologies		
Asset Discovery	Built-in	$$ (3rd-party product that requires integration)
Network IDS	Built-in	$$ (3rd-party product that requires integration)
Host IDS	Built-in	$$ (3rd-party product that requires integration)
Netflow	Built-in	$$ (3rd-party product that requires integration)
Full Packet Capture	Built-in	$$ (3rd-party product that requires integration)
File Integrity Monitoring	Built-in	$$ (3rd-party product that requires integration)
Vulnerability Assessment	Built-in	$$ (3rd-party product that requires integration)
Additional Capabilities:		
Continuous Threat Intelligence	Built-in	Not available
Unified Management Console for security monitoring technologies	Built-in	Not available

Следующие шаги:

- Посмотрите 3-минутный обзор
- Попробуйте попробуйте live-демо на нашем сайте
- Начните обнаруживать угрозы при помощи бесплатной 30-дневной триальной версии
- Получить от SIEM больше, благодаря нашей USM
- Присоединяйтесь к открытому сообществу обмена данными об угрозах (OTX)

BAKOTECH®

Группа компаний БАКОТЕК – официальный дистрибьютор решений AlienVault в Украине, Казахстане, странах Балтии, Восточной Европы и СНГ.

По всем вопросам, связанным с продукцией AlienVault, пожалуйста, обращайтесь:
+380 44 273-3333, **alienvault@bakotech.com**

www.alienvault.com