AT&T Cybersecurity

КРАТКИЙ ОБЗОР РЕШЕНИЯ

Соответствие AlienVault USM требованиям PCI DSS

Компании, работающие по стандарту PCI DSS, должны соответствовать широкому спектру технических и эксплуатационных требований. Соответствие данным стандартам необходимо не просто ради избежания штрафов и санкций, а для обеспечения безопасности клиентов. К сожалению, многие организации изо всех сил стараются не выполнять эти требования. В отчете PCI Compliance Verizon 2018 установлено, что только 46,4% компаний в Европе полностью соотвествуют стандарту PCI DSS.

PCI DSS 3.2.1

PCI DSS 3.2.1 содержит 12 требований, которые должны соблюдаться всеми организациями, работающими с платежными картами, включая продавцов, процессинговые центры, финансовые учреждение и поставщиков услуг. Большинство компаний стремятся соответствовать этим требованиям используя несколько отдельных продуктов. Результат такого подхода проявляется в итоговой высокой стоимости и сложности интеграции разных продуктов технологий. Этот вариант особенно проблематичен для небольших организаций, у которых меньше ресурсов для приобретения, конфигурации и управления отдельными решениями.

Единый подход с AlienVault

Альтернатива автономным технологиям – это решение, которое объединяет несколько инструментов в комплексную платформу, управляемую единой консолью. Платформа AT&T Cybersecurity AlienVault Unified Security Management™ (USM) предоставляет пять основных технологий обеспечения безопасности, каждая из которых позволяет ускорить проверку на соответствие PCI DSS 3.2.1. AlienVault USM имеет 3 варианта установки – физическое, виртуальное и облачное устройство:

Обнаружение активов – объединяет три основных механизма, чтобы обеспечить вам полную видимость устройств, находящихся в вашей сети.

- Активное сетевое сканирование
- Пассивный мониторинг сети
- Инвентаризация активов

[1] **Verizon 2018 PCI Compliance Report**

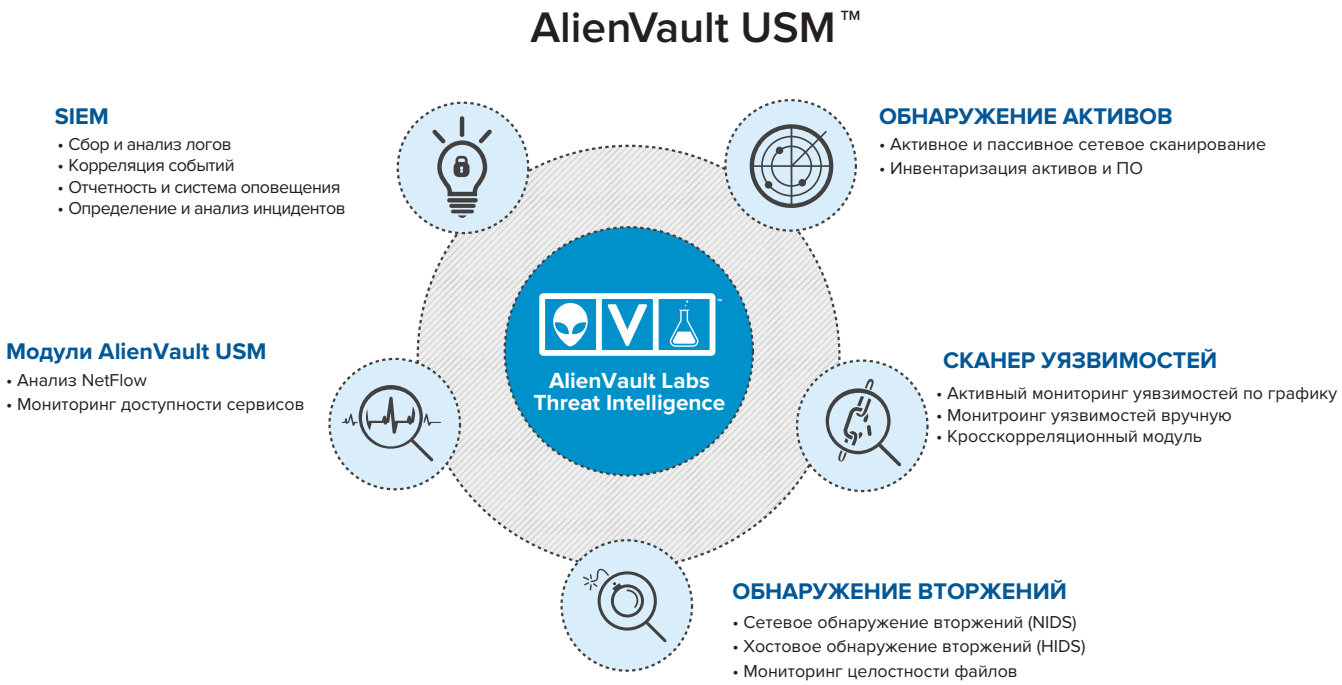


Рисунок 1 - Модули AlienVault USM

Обнаружение активов – это первый важнейший шаг для того, чтобы защитить вашу инфраструктуру. AlienVault USM обеспечивает полную видимость устройств, которые находятся и появляются в вашей сети.

Оценка уязвимости – идентифицирует активы с непропатченным ПО, небезопасными конфигурациями и другими уязвимостями:

- Ручное проведение анализа на уязвимости
- Мониторинг уязвимостей в режиме реального времени

Интегрированный сканер уязвимостей показывает слабые места в вашей инфраструктуре. Благодаря этому вы можете определить необходимость установки патча или внесение соответствующих изменений на конкретном активе. Непрерывная корреляция обнаруженных уязвимостей с нашей базой данных дает своевременную информацию о безопасности вашей инфраструктуры.

Обнаружение вторжений – предоставляет возможность идентификации угроз в сетевом трафике и на конечных точках, используя встроенные технологии мониторинга безопасности от лаборатории AlienLabs:

- Сетевая IDS (NIDS)
- Хостовая IDS (HIDS)
- Мониторинг целостности файлов (FIM)

Встроенный мониторинг целостности файлов , доступный при использовании HIDS, установленных на конечных точках, предупреждает вас о несанкционированной модификации системных файлов, конфигурационных файлов или их содержания. Мониторинг сетевой активности , используя хостовую (HIDS) и сетевую (NIDS) системы обнаружения вторжений, позволяет определить, кто пытался получить доступ к системам, файлам и их содержимому

Поведенческий мониторинг – позволяет выявлять аномалии в NetFlow, а также дает возможность обнаружения проблем в работоспособности вашей инфраструктуры:

- Обслуживание и мониторинг инфраструктуры
- Анализ NetFlow
- Анализ сетевых протоколов / захват пакетов

Интегрированный поведенческий мониторинг собирает данные, чтобы помочь вам понять нормальное состояние системы и сетевой активности. Это упрощает процесс реагирования на инциденты при обнаружении подозрительного поведения или потенциального инцидента. Полный захват пакетов позволяет провести комплексный анализ сетевого трафика по протоколам, обеспечивая полное ретроспективное воспроизведение событий, которые произошли во время потенциального инцидента.

SIEM – определение и устранение угроз, а также надежная архивация информации о всех произошедших событиях в вашей инфраструктуре:

- Сбор логов
- Нормализация логов
- Корреляция событий
- Реагирование на угрозы

Вы можете автоматически коррелировать данные логов со встроенными и созданными правилами безопасности для выявления нарушений.

OTX – открытая система обмена данными об угроз ах

OTX – это открытое сообщество для обмена данными о новых угрозах, которое обеспечивает совместную защиту и исследование угроз. Оно интегрируется с AlienVault USM и OSSIM, а также имеет возможность экспорта IoC практически на любой продукт безопасности. OTX обеспечивает открытый доступ для всех, что позволяет вам сотрудничать с сообществом профессионалов в области информационной безопасности.

Этот доступ дает возможность проводить совместные исследования, позволяя всем в сообществе OTX активно делиться последними данными, тенденциями и методами распространения угроз. Он также ускоряет распространение свежей информации об угрозах и автоматизирует процесс обновления инфраструктуры безопасности. OTX позволяет всем в сообществе активно сотрудничать, укрепляя свою собственную защиту и помогая другим делать то же самое.

Платформа USM интегрирует пульсы (объединенные в группы IoC) из OTX, которые предоставляют пользователям краткую информацию о конкретных угрозах, информацию о том, какое ПО может быть атаковано, а также связанные индикаторы компрометации (IoCs) , которые могут быть использованы для обнаружения угроз.

Преимущества системы AlienVault OTX:

- Забирает у атакующей стороны преимущество и передает его защищающейся
- Открыта для всех, кто подписался, а не только для пользователей AlienVault
- Дает подписчикам пользу от индикаторов, которыми поделились другие участники
- Предоставляет совместное использование данных об угрозах, ускоряет их распространение среди всех участников в автоматическом режиме
- Дает полную видимость тенденций угроз благодаря данным, собранным из 140 стран по всему миру.

Современная защита от AlienVault Labs

Исследовательская группа AlienVault Labs тратит огромное количество времени на обработку информации о различных типах атак, последних угрозах, уязвимостях и эксплойтах.

Интегрированная в USM система обнаружения угроз от AlienVault Labs позволяет IT-командам не тратить собственное время на проведение исследований по возникающим инцидентам. Команда AlienVault Labs регулярно предоставляет информацию об угрозах как скоординированный набор обновлений для платформы USM, которая ускоряет и упрощает обнаружение и устранение угроз:

Чтобы ваша защита была актуальной, AlienVault Labs регулярно отправляют восемь типов обновлений:

- Сигнатуры NIDS
- Сигнатуры HIDS
- Базу данных обнаружения и инвентаризации активов
- Базу данных уязвимостей
- Правила корреляции событий
- Шаблоны и модули для отчетов
- Шаблоны реагирования на инциденты / руководство «как поступать» для каждого аварийного сигнала
- Плагины для подключения источников данных

Увеличьте свое соответствие стандартам и объедините свою защиту

В AT&T Cybersecurity мы понимаем, что соответствие PCI – это серьезный процесс, а не просто процедура для галочки. Для достижения соответствия PCI требуется правильный набор инструментов. Объединяя функции в комплексную систему, AlienVault USM предлагает решение, ориентированное на постоянную работу и существенно сокращающее время проверки на соответствия требованиям PCI.

Мы также понимаем, что простота и эффективность идут рука об руку. Вот почему мы создали все эти основные функции обеспечения безопасности в интегрированной платформе, объединив вашу защиту, экономя ваше время и деньги, делая управление вашей системой безопасности более простым.

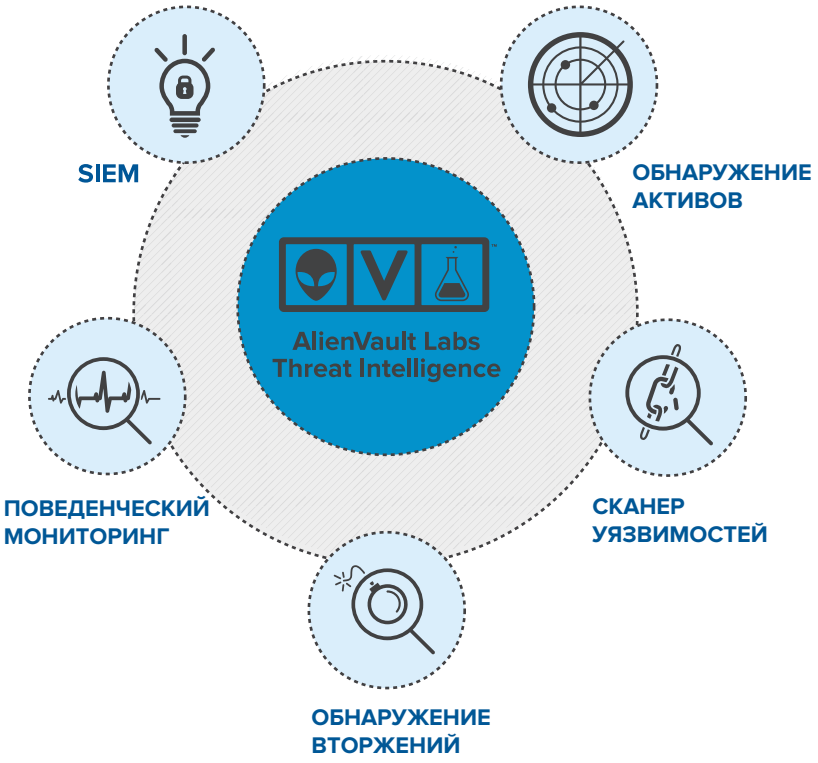
Для получения дополнительной информации о том, как начать сотрудничать с нами, чтобы мы могли помочь вам удовлетворить ваши требования по соответствию PCI, свяжитесь с нами по телефону +380 44 273-3333 или отправьте письмо по адресу **alienvault@bakotech.com**

Как AlienVault USM помогает вам соблюдать требования PCI DSS 3.1

ТРЕБОВАНИЯ PCI DSS		СООТВЕТСТВУЮЩИЕ ВОЗМОЖНОСТИ AV	ПРЕИМУЩЕСТВА УНИФИЦИРОВАННОГО УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ
1.1, 1.2, 1.3	Установка и поддержка конфигурации файервола для защиты данных держателей карт	› Анализ NetFlow › Мониторинг доступности системы › SIEM › Обнаружение Активов	› Анализ NetFlow и логов файервола обеспечивает полную видимость доступа к данным и ресурсам, связанным с держателями карт. › Встроенное обнаружение активов позволяет динамически производить инвентаризацию активов. Ресурсы, связанные с владельцами карт, можно идентифицировать и контролировать на предмет аномальной активности. › Точная и автоматическая инвентаризация активов в сочетании с соответствующими событиями безопасности ускоряет реагирование на инциденты и анализ угроз.
2.1, 2.2, 2.3, 2.4	Не используются пароли и настройки безопасности по умолчанию	› Обнаружение сетевых вторжений (IDS) › Оценка уязвимости › Обнаружение хостовых вторжений (HIDS)	› Встроенная автоматическая оценка уязвимостей определяет использование слабых и дефолтных паролей. › Встроенное обнаружение вторжений на хостах и мониторинг целостности файлов будут сигнализировать о том, когда были изменены файлы с паролями и другие критические системные файлы.
3.6.7	Защита сохраненных данных держателя карты	› Управление логами › Обнаружение хостовых вторжений (HIDS) › Контроль целостности файлов › Анализ NetFlow › SIEM	› Просмотр и анализ логов с предупреждениями для систем с высоким приоритетом (содержащие данные держателей карт). › Встроенное обнаружение вторжений на хостах, мониторинг целостности файлов и сигнализация об изменениях криптографических ключей. › Анализ NetFlow и корреляция событий отслеживает трафик и выдает предупреждения о незашифрованном трафике в / из ресурсов, связанных с владельцами карт.
4.1	Шифрование передачи данных держателей карт через открытые, общедоступные сети	› Анализ NetFlow › Поведенческий мониторинг › SIEM	› Унифицированный анализ NetFlow и корреляция событий отслеживает трафик и выдает предупреждения о незашифрованном входящем и исходящем трафике из ресурсов, связанных с владельцами карт.

	ТРЕБОВАНИЯ PCI DSS	СООТВЕТСТВУЮЩИЕ ВОЗМОЖНОСТИ AV	ПРЕИМУЩЕСТВА УНИФИЦИРОВАННОГО УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ
5.1, 5.2, 5.3	Защитита всех систем от вредоносных программ и регулярное обновление антивирусных программ	› Обнаружение хостовых вторжений (HIDS) › Обнаружение сетевых вторжений (IDS) › Управление логами	› Встроенное обнаружение хостовых вторжений обеспечивает дополнительный уровень защиты от угроз нулевого дня. › Управление логами обеспечивает сбор данных от антивирусного ПО. › Встроенное обнаружение сетевых вторжений предупреждает о вредоносных программах в вашей среде.
6.1, 6.2, 6.3, 6.4, 6.5, 6.6	Разработка и поддержка безопасных систем и приложений	› Обнаружение активов › Сканер уязвимостей › Обнаружение сетевых вторжений (IDS) › SIEM	› Встроенная и консолидированная инвентаризация активов, оценка уязвимости, обнаружение угроз и корреляция событий дают комплексное представление о безопасности организации и критической конфигурации систем. › Встроенный сканер уязвимостей проверяет на наличие наиболее известных угроз (например, SQL-инъекций)
7.1, 7.2	Ограничение доступа к данным о держателях карт	› SIEM	› Автоматические идентификаторы корреляции событий при неавторизованном доступе к системам с данными держателей карт.
8.1, 8.2, 8.4, 8.5, 8.6	Определение и аутентификация доступа к системным компонентам	› Управление логами	› Встроенное управление логами фиксирует все действия по созданию учетной записи пользователя и умеет определять незашифрованные пароли в критических системах. Также доступен сбор и корреляция успешных и неуспешных попыток аутентификации на критических устройствах.
10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7	Отслеживание и контроль доступа ко всем сетевым ресурсам и данным держателя карты	› Обнаружение хостовых вторжений (HIDS) › Обнаружение сетевых вторжений (IDS) › Поведенческий мониторинг › Управление логами › SIEM	› Встроенные функции обнаружения угроз, поведенческого мониторинга и сигналов о событиях (например, о несанкционированном доступе), за которыми следуют дополнительные нарушения правил безопасности, такие как получение доступа к данным держателей карт. › Встроенное управление логами позволяет собирать и сопоставлять успешные и неуспешные попытки аутентификации на критических устройствах. › Централизованный контроль доступа на основе ролей для аудиторских логов и логов событий сохраняет «цепочку поставок» для проведения расследований.
11.1, 11.2, 11.3, 11.4, 11.5	Регулярная проверка системы безопасности и процессов	› Оценка уязвимости › Обнаружение хостовых вторжений (HIDS) › Контроль целостности файлов › SIEM	› Встроенная оценка уязвимости упрощает процесс сканирования и исправления – благодаря наличию единого интерфейса. › Встроенное обнаружение хостовых вторжений идентифицирует подключение USB-устройств, включая карты WLAN. › Унифицированная оценка уязвимости, обнаружение угроз и корреляция событий обеспечивают полную видимость вашей сети. › Встроенный механизм контроля целостности файлов, сигнализирующий о несанкционированном изменении системных файлов, файлов конфигурации или их содержимого.

AlienVault USM™



БАКОТЕК® – международная группа компаний, которая занимает лидирующие позиции в сфере фокусной Value Added IT-дистрибуции и поставляет решения ведущих мировых IT-производителей. Позиционируя себя как True Value Added IT-дистрибьютор, БАКОТЕК предоставляет профессиональную до- и пост-продажную, маркетинговую, техническую поддержку для партнеров и конечных заказчиков. Территориально группа компаний работает в 26 странах на рынках Центральной и Восточной Европы, Балкан, Балтии, Кавказа, Центральной Азии с офисами в Праге, Кракове, Риге, Минске, Киеве, Баку и Нур-Султане.

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: alienvault@bakotech.com