ENERGY LOGSERVER

Інформація про рішення

Як Energy Logserver відповідає вимогам PCI DSS

Стандарт PCI DSS — це протокол безпеки для зменшення шахрайства з платіжними картками. Він передбачає посилені заходи безпеки для таких організацій як банки, страхові компанії та постачальники платіжних послуг. Цей стандарт дає підприємствам орієнтир для впровадження практик захисту даних клієнтів та допомагає керувати обробкою можливих порушень безпеки.

Ми підготували буклет, щоб розповісти вам більше про стандарт PCI DSS та показати, як Energy Logserver допомагає фінансовим, страховим і державним установам та іншим організаціям виконувати вимоги захисту.

PCI DSS 3.2.1 та PCI DSS v4.0

З точки зору SIEM, PCI DSS v4.0 має кілька покращень. Ви можете ознайомитись із загальним переліком основних відмінностей в останньому розділі.
Зараз же ми хочемо зосередитись на одній з найбільш очікуваних і суттєвих змін у 4-й версії. Ми маємо на увазі вимогу **використовувати засоби автоматизованого аналізу журналів** для контролю PCI DSS 10.4.1.

Вона передбачає:

Щоденну перевірку журналів (7 днів на тиждень, 365 днів на рік, включно зі святами). Перевірка мінімізує вплив потенційного порушення та економить час спеціалістів.
Інструменти збору журналів, аналізу та сповіщень, централізовані системи керування логами, аналізатори журналів подій, рішення для керування інформацією про безпеку та подіями (SIEM). Ці автоматизовані інструменти можуть задовольнити вищезгадану вимогу.

Версія 3 дозволяла переглядати журнали вручну. Однак обробити величезну кількість логів, які генерує навіть крихітне середовище, — рутинне та непрактичне завдання для спеціаліста. Тому не дивно, що автоматизація увійшла в список сучасних вимог.

Наявність стандарту PCI DSS 4.0 стане обов'язковою після 31 березня 2025 року, а термін дії поточної версії 3.2.1 закінчується 1 квітня 2024 року. Організації можуть повторно сертифікуватися за версією 3.2.1, якщо зроблять це до закінчення терміну її дії.
У версії 3.2.1 перераховано 12 зобов'язань для осіб, які працюють із платіжними картками. Для багатьох компаній (особливо малого бізнесу) рішення, що дозволяють виконати ці зобов'язання, є надто складними чи дорогими. Головна мета — гарантувати безпеку клієнтів. Однак, звіт Verizon за 2018 рік показав, що лише 46,4% європейських організацій повністю відповідають стандартам PCI DSS.

Правильний вибір інструменту SIEM для PCI DSS: чому це важливо?

Завдання класичного SIEM полягають в інтеграції з системами, зборі та збереженні журналів даних, аналізі трафіку, нормалізації журналів і кореляції даних. Однак функції SIEM також можуть допомогти з іншими моментами, що виходять за межі його сфери відповідальності. Наприклад, він надає автоматичні звіти, щоб показати, де не встановлено рішення безпеки, а також допомагає з аудитом PCI. Отже, звіти SIEM автоматизують аудит, скорочують час його проведення та підвищують загальну ефективність.

Щоб задовольнити актуальні вимоги та майбутні зміни, компанія повинна звернути увагу на таке:

Ведення журналу:

SIEM Energy Logserver може збирати та зберігати журнали з усіх ваших систем і пристроїв, включно з тими, які зберігають або обробляють дані власників карток. Це допоможе вам виконати вимогу PCI DSS 10.6 щодо перегляду журналів і подій безпеки для всіх компонентів системи для виявлення аномалій або підозрілої активності.

Моніторинг:

SIEM Energy Logserver може моніторити ваші журнали на наявність підозрілої активності, як-от несанкціонований доступ до даних власника картки або спроби змінити конфігурацію системи. Тому ви можете виконати вимогу PCI DSS 10.1 щодо впровадження автоматизованих журналів аудиту для всіх компонентів системи, щоб виявити несанкціонований доступ до даних власника картки.

Сканування вразливостей:

SIEM Energy Logserver може сканувати ваші системи та пристрої на відомі вразливості. Він спрямований на виконання вимоги PCI DSS 11.2 щодо регулярного сканування систем і мереж.

Реагування на інцидент:

SIEM Energy Logserver може допомогти вам реагувати на інциденти безпеки, надаючи необхідну інформацію — наприклад, про джерело атаки та системи, які постраждали. Це допоможе вам виконати вимогу PCI DSS 12.8 щодо наявності плану реагування на інциденти безпеки.

Підвищте свою відповідність та уніфікуйте захист

Досягнення відповідності вимогам PCI — це не проста формальність. Щоб дотримуватись стандартів відповідності PCI, вам знадобляться відповідні інструменти.
Energy Logserver розширює межі SIEM. Рішення збирає журнали без EPS і обмежень на зберігання та інтегрує їх з усіма необхідними рішеннями, щоб ви не втратили жодного байта важливих даних. Окрім цього, рішення об’єднує численні функціональні можливості в комплексну систему, зосереджуючись на стабільній продуктивності та зменшуючи час, необхідний для перевірки відповідності PCI.
Energy Logserver SIEM розроблений для легкого розгортання з попередньо налаштованими параметрами, які спрощують запуск. Отже, ви можете миттєво розпочати моніторинг своїх систем і захистити дані платіжної картки.

Зокрема, Energy Logserver SIEM дозволяє:

Підтримувати безпеку мережі та системи

Ви можете відстежувати та аналізувати мережевий трафік, виявляти аномальні спроби входу та ідентифікувати хакерські атаки. Тому ви швидко виявлятимете загрози та реагуватимете на них, у такий спосіб сприяючи безпеці мережі та системи.

Дотримуватися політик та процедур безпеки

З SIEM від Energy Logserver ви зможете відстежувати та аналізувати журнали системи та додатків і перевіряти, чи виконуються політики та процедури безпеки. Це може допомогти вам вчасно виявити інцидент та зреагувати на нього.

Захистити дані платіжної картки

Energy Logserver SIEM дозволяє відстежувати журнали системи та програм для виявлення спроб доступу до даних платіжних карток. Це дозволяє виявляти та блокувати несанкціоновані спроби доступу до даних платіжної картки.

Регулярно перевіряти та тестувати системи

Ви зможете відстежувати системні події в режимі реального часу та створювати звіти, забезпечуючи регулярний моніторинг і тестування систем.

Підтримувати фізичну безпеку

Моніторинг подій, пов’язаних із доступом до фізичних системних ресурсів, таких як сервери та центри обробки даних, дозволяє виявляти та реагувати на несанкціонований доступ до фізичних системних ресурсів.

Отже, Energy Logserver SIEM допомагає вам відповідати вимогам PCI-DSS, консолідує ваш захист, економить ваш час і гроші, а також оптимізує керування вашою системою безпеки.

Як Energy Logserver допомагає вам відповідати вимогам PCI

Основні 10 відмінностей між PCI DSS 3.2.1 і PCI DSS 4 з точки зору SIEM:

	Покращення в PCI DSS v4.0	Функції Energy Logserver
1	**Уточнення термінів.** PCI DSS v4.0 роз'яснює значення кількох термінів, зокрема даних облікового запису, конфіденційних даних автентифікації (SAD), даних власника картки та PAN. Це важливо для SIEM, оскільки вони повинні мати можливість правильно ідентифікувати та класифікувати дані, щоб створювати ефективні сповіщення.	▶ Попередньо визначені класифікації для різних типів даних ▶ Різні інструменти для ідентифікації та класифікації даних ▶ Інтеграція з LDAP, AD, RADIUS тощо ▶ Потужні та гнучкі модулі сповіщень
2	**Розширені вимоги до логування.** PCI DSS v4.0 розширює вимоги до логування для організацій, які обробляють, зберігають або передають дані власників карток. Це передбачає вимоги до більш детального протоколювання доступу, змін і подій. Отже, SIEM краще виявлятимуть і розслідуватимуть інциденти безпеки.	▶ Можливість збирати та зберігати детальні журнали доступу, змін і подій ▶ Працює як без агентів, так і на основі агентів ▶ Сотні підготовлених аналізаторів, включно з конструктором для налаштування та створення нових ▶ Безпечне та необмежене зберігання, керування архівами
3	**Підвищена увага до управління ідентифікацією та доступом (IAM).** PCI DSS v4.0 робить більший акцент на IAM, вимагаючи від організацій запровадити ефективніші засоби контролю для керування доступом користувачів до даних власників карток. Це передбачає вимоги до багатофакторної автентифікації, найменших привілеїв і керування паролями. Цей захід допоможе знизити ризик несанкціонованого доступу до даних власників карток.	▶ Може допомогти організаціям запровадити більш ефективний контроль IAM, надаючи можливість керувати доступом користувачів до даних власників карток, застосовувати багатофакторну автентифікацію та відстежувати використання паролів ▶ Може відстежувати та контролювати рішення IAM і MFA для оптимізації їхньої кращої інтеграції
4	**Нові вимоги до хмарних обчислень.** PCI DSS v4.0 містить нові вимоги до організацій, які використовують сервіси хмарних обчислень. Ці вимоги охоплюють такі сфери, як безпека даних, контроль доступу та реагування на інциденти. Це допоможе забезпечити захист даних власника картки під час їх зберігання або обробки в хмарі.	▶ Можливість моніторингу та аудиту хмарних програм і даних ▶ Можливість збирати, зберігати та аналізувати дані з хмарних платформ і програм ▶ Глибока інтеграція з Amazon AWS, MS Azure, Google Workspace тощо
5	**Збільшення уваги до навчання з питань безпеки.** PCI DSS v4.0 приділяє більшу увагу навчанню з питань безпеки, вимагаючи від організацій проводити регулярні семінари для всіх співробітників, які працюють з даними власників карток. Цей тренінг має охоплювати такі теми, як фішинг, соціальна інженерія та захист паролів. У результаті компанії можуть зменшити ризик людської помилки, яка є основною причиною витоку даних.	▶ Може надати глибоку аналітичну інформацію про користувачів та інциденти, щоб підготувати більш релевантні тренінги ▶ Може створювати автоматизовані кейси для перевірки отриманих знань на практиці ▶ Може надати детальний аналіз інциденту для покращення взаємодії з користувачем

6	**Нові вимоги до управління вразливостями.** PCI DSS v4.0 вимагає від організацій регулярно сканувати свої системи та мережі на відомі вразливості. Це допоможе виявити та усунути недоліки безпеки до того, як зловмисники скористаються ними.	▶ Глибока інтеграція з найпоширенішими сканерами вразливостей ▶ Може збирати та довгостроково зберігати дані зі сканерів уразливостей ▶ Можна використовувати інтегрований агент для сканування вразливостей у системах Linux і Windows
7	**Підвищена увага до оцінки ризиків.** PCI DSS v4.0 приділяє більшу увагу оцінці ризиків, вимагаючи від організацій регулярно моніторити ризики для даних власників карток. Ця оцінка використовується, щоб інформувати засоби контролю безпеки організації та переконатися, що організація вживає належних заходів для захисту даних власників карток.	▶ Інтегрований модуль управління ризиками
8	**Нові вимоги до реагування на інциденти.** PCI DSS v4.0 вимагає від організацій мати план реагування на інциденти безпеки. Цей план повинен містити кроки для виявлення, локалізації та відновлення після інцидентів, що допоможе мінімізувати негативний вплив.	▶ Розслідування інцидентів і можливості реагування ▶ Широкий спектр можливостей реагування на інциденти ▶ Потужний модуль сповіщення ▶ Можливість взаємодії зі сторонніми рішеннями за допомогою API або сценаріїв, щоб забезпечити більше опцій відповіді
9	**Підвищена увага до постійного моніторингу.** PCI DSS v4.0 приділяє більшу увагу постійному моніторингу, вимагаючи від організацій регулярної перевірки своїх систем і мереж на наявність ознак атак.	▶ Можливість збирати й аналізувати журнали, контролювати мережевий трафік і виявляти аномалії ▶ Моніторинг усіх видів активів (апаратне забезпечення, мережа, кінцеві точки, бази даних, програмне забезпечення, програми, користувачі тощо) ▶ Необмежені можливості створення будь-якої візуалізації ▶ Сотні попередньо визначених інформаційних панелей ▶ Можливість аналізувати історичні дані відповідно до нових елементів керування та правил
10	**Нові вимоги до звітності.** PCI DSS v4.0 містить нові вимоги до звітності, вимагаючи від організацій повідомляти про певні інциденти безпеки в PCI SSC. Ця звітність допоможе PCI SSC відстежувати ефективність PCI DSS і виявляти нові загрози.	▶ Створення різних типів звітів про інциденти безпеки, вразливості та оцінку ризиків ▶ Автоматизовані звіти ▶ Інтеграція з системами BI, Helpdesk/ServiceDesk ▶ Можливість відстежувати ефективність засобів контролю безпеки організації та виявляти нові загрози ▶ Детальні та інтегровані звіти про відповідність (включно з NIST/NIST2, GDPR, PCI DSS, ISO 2700X тощо)

Попередня версія стандарту

Пункти: 1.1, 1.2, 1.3 **Загальна тема:** Встановлення та підтримка конфігурації брандмауера для захисту даних власника картки **Загальні характеристики:** › Аналіз мережевого протоколу NetFlow › Моніторинг доступності системи › SIEM	**Деталі:** » Аналізуючи журнали NetFlow і брандмауера, можна скласти повну картину того, як власники карток отримують доступ до даних і ресурсів. » Завдяки точному автоматичному обліку активів у поєднанні з відповідними подіями безпеки, можливе проактивне реагування на інциденти.
Пункти: 2.1, 2.2, 2.3, 2.4 **Загальна тема:** Паролі та налаштування безпеки не використовуються за замовчуванням **Загальні характеристики:** › Виявлення мережевого вторгнення (IDS) › Оцінка вразливості › Виявлення вторгнень на хост (HIDS)	**Деталі:** » Система оснащена функцією автоматичної оцінки вразливості, яка може виявити використання слабких паролів і паролів за замовчуванням. » Крім того, вбудовані функції виявлення вторгнень і моніторингу цілісності файлів сповіщатимуть користувачів про будь-які неавторизовані зміни файлів паролів або інших важливих системних файлів.
Пункти: 3.6.7 **Загальна тема:** Захист збережених даних власника картки **Загальні характеристики:** › Керування журналами › Вторгнення з виявленням хостів (HIDS) › Контроль цілісності файлів › Аналіз NetFlow › SIEM	**Деталі:** » Можна переглядати та аналізувати журнали попереджень для високопріоритетних систем, які зберігають дані власників карток. » Система містить вбудовані функції виявлення вторгнень у хост, моніторинг цілісності файлів і попередження про зміну криптографічного ключа. » Завдяки аналізу NetFlow і кореляції подій система постійно відстежує мережевий трафік і надсилає сповіщення про будь-який незашифрований трафік напрямком до або від ресурсів, пов'язаних із власниками карток.

Пункти:
4.1

Загальна тема:
Шифрування даних про власника картки через відкриті публічні мережі

Загальні характеристики:
› Аналіз NetFlow
› Поведінковий моніторинг
› SIEM

Деталі:

» За допомогою уніфікованого аналізу NetFlow і кореляції подій система може відстежувати мережевий трафік і повідомляти про будь-який незашифрований вхідний або вихідний трафік з ресурсів, які пов'язані з власниками карток.

Пункти:
5.1, 5.2, 5.3

Загальна тема:
Захист всіх систем від шкідливих програм і регулярне оновлення антивірусів

Загальні характеристики:
› Виявлення вторгнень на хост (HIDS)
› Виявлення мережевого вторгнення (IDS)
› Керування журналами

Деталі:

» Система містить вбудовану функцію виявлення вторгнень на хост, яка пропонує додатковий рівень захисту від загроз нульового дня.

» Керування журналами дозволяє збирати дані з антивірусного програмного забезпечення, покращуючи здатність системи виявляти потенційні загрози.

» Вбудована функція виявлення мережевих вторгнень сповіщає користувачів про будь-яке шкідливе програмне забезпечення, наявне в їхньому середовищі.

Пункти:
6.1, 6.2, 6.3, 6.4, 6.5, 6.6

Загальна тема:
Розробка та підтримка захищених систем і додатків

Загальні характеристики:
› Сканер уразливостей
› Виявлення мережевого вторгнення (IDS)
› SIEM

Деталі:

» Система забезпечує інтегровану та централізовану інвентаризацію активів, оцінку вразливості, виявлення загроз і можливість кореляції подій, що пропонує комплексне уявлення про стан безпеки вашої організації та конфігурацію критичних систем.

» Вбудований сканер уразливостей передбачено для перевірки найвідоміших загроз, на кшталт впровадження SQL.

Пункти:
7.1, 7.2

Загальна тема:
Обмеження доступу до даних про власників карток

Загальні характеристики:
› SIEM

Details:

» Функція автоматичної кореляції подій системи може ідентифікувати випадки неавторизованого доступу до систем, які містять дані власників карток.

Пункти: 8.1, 8.2, 8.4, 8.5, 8.6 **Загальна тема:** Визначення та автентифікація доступу до компонентів системи **Загальні характеристики:** › Керування журналами	**Деталі:** » Система містить вбудоване керування журналами, яке фіксує всі дії, пов'язані зі створенням облікового запису користувача. Вона може виявляти незашифровані паролі в критично важливих системах. » Крім того, система може збирати та співвідносити інформацію про успішні та невдалі спроби автентифікації на критично важливих пристроях.
Пункти: 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7 **Загальна тема:** Відстежуйте та контролюйте доступ до всіх мережевих ресурсів і даних власників карток **Загальні характеристики:** › Виявлення вторгнень на хост (HIDS) › Виявлення мережевого вторгнення (IDS) › Моніторинг поведінки › Керування журналами › SIEM	**Деталі:** » Система має вбудовані функції виявлення загроз, моніторингу поведінки та попередження про події (наприклад, про втручання), які можуть допомогти знайти додаткові порушення безпеки, включно із несанкціонованим доступом до даних власника картки. » Вбудована функція керування журналами дозволяє користувачам збирати та порівнювати дані про успішні та невдалі спроби автентифікації на критично важливих пристроях. » Централізований контроль доступу системи на основі ролей до журналів аудиту та подій зберігає «ланцюжок постачання» для розслідувань.
Пункти: 11.1, 11.2, 11.3, 11.4, 11.5 **Загальна тема:** Регулярні перевірки безпеки та процесів **Загальні характеристики:** › Оцінка вразливості › Вторгнення з виявленням хостів (HIDS) › Контроль цілісності файлів › SIEM	**Деталі:** » Вбудована функція оцінки вразливості системи оптимізує процес сканування та виправлення, забезпечуючи єдиний інтерфейс. » Завдяки вбудованій функції виявлення вторгнень користувачі можуть ідентифікувати підключення USB-пристроїв, включно з картами WLAN. » Можливості уніфікованої оцінки вразливості системи, виявлення загроз і кореляції подій забезпечують повну видимість у мережі. » Система також містить вбудований механізм моніторингу цілісності файлів, який попереджає користувачів про будь-які несанкціоновані зміни, внесені до системних файлів, файлів конфігурації або їх вмісту.

Підсумок

Energy Logserver SIEM — це інструмент, який може допомогти вашому бізнесу відповідати вимогам PCI DSS завдяки підтримці безпеки мережі та системи, захисту даних платіжних карток, підтримці фізичної безпеки, політики та процедури безпеки, а також регулярному моніторингу і тестуванню систем. Рішення надає попередньо визначені оцінки, які можуть допомогти вам швидко та легко проаналізувати дані. Ці оцінки можна налаштувати відповідно до ваших потреб.

Log Management — все про управління журналами

- Рольова модель доступу
- Багатовимірна система сповіщень і звітності
- Інтеграція з LDAP, AD, Radius, SSO
- Багаторівнева система архівації даних
- Масштабована архітектура та кластеризація
- Гнучкий конструктор дашбордів та готові шаблони
- Сотні готових парсерів, гнучкий конструктор

SIEM — розширене управління безпекою

- Поведінковий аналіз користувачів і пристроїв
- Динамічна інтеграція з базами IoC, TTP, Threat Intellegence, MITRE ATT&CK
- GDPR, NIST, CIS, PCI DSS, HIPAA compliance
- File Integrity Monitoring (FIM)
- Сканер вразливостей
- 1000+ правил детектування та кореляцій
- Допомога у виявленні підозрілої поведінки на базі штучного інтелекту
- Playbooks
- Моніторинг роботи додатків та сервісів
- Інтегрована система керування ризиками
- Система керування інцидентами

Network Probe — мережевий аналіз

- Детальний аналіз мережевого трафіку
- Аналіз Netflow (v5, v9, IPFIX, sflow. iflow. NetStrean)
- Продуктивність від 10 Gbps
- Від 100 000 FPS
- Візуалізація трафіку на рівнях L2-L7
- Кореляція журналів та даних з трафіку
- Перевірка трафіку згідно з репутаційними базами та IoC
- Виявлення атак нульового дня
- Аналіз активності користувачів у мережі
- Моніторинг SRT, RTT, Delay, Jitter, аномалій мережі

ENERGY LOGSERVER

Якщо ви хочете дізнатися більше про Energy Logserver SIEM, зв’яжіться з нами:

bako tech®

BAKOTECH® — міжнародна компанія, яка посідає передові позиції у сфері фокусної Value Added IT-дистрибуції та постачає рішення провідних світових IT-виробників. Позиціонуючи себе як True Value-Added IT-дистриб'ю-тор, BAKOTECH надає професійну перед- та постпродажну, маркетингову, технічну підтримку для партнерів та кінцевих замовників.
Географічно компанія працює у 26 країнах на ринках Центральної та Східної Європи, Балкан, Балтії, Кавказу, Центральної Азії, з офісами в Празі, Кракові, Ризі, Києві, Баку та Нурсултані.
Група компаній BAKOTECH є офіційним дистриб'ютором рішень Energy Logserver в Україні, країнах Балтії, Східної Європи та Центральної Азії.

els@bakotech.com