УДК 004

SECURITY INSIGHTS

В. А. Безлюдний[1], А. М. Родіонов[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

У роботі проведений огляд технології Security Insights. Дана технологія спрямована на збір та агрегацію логів, візуалізацію та інтерпретацію. Використовуючи вбудовані або сторонні додатки, рішення безпеки та технології, як наприклад `IDS/IPS` та `SIEM`-системи.

Ключові слова: Security Insights, Хмарні сервіси, data visualization

Вступ

Все більше користувачів використовують хмарні сервіси, завдяки розвитку їх поширеності. Сучасна проблема безпеки в тому, що інфраструктура гібридної хмари є складною і межі такої системи не є очевидними, що є суттєвою завадою до імплементації старіших технологій, як `IDS/IPS`.

Саме тому потрібен прозорий метод моніторингу та контролю даних, який б надавав точну інформацію щодо можливих вразливостей чи підозрілу активність. Щоб одна або невелика група людей могла б виявити і зупинити можливу атаку в реальному часі.

1. Складові технології Security Insight

Загалом Security Insight це сучасні `SIEM` платформи з можливістю аналітики.

Для захисту системи збирається велика кількість даних, логів з різних джерел. Тобто відбувається *агрегація* (накопичення) даних з різних програм, рішень безпеки та аналітичних інструментів.

При агрегації великого об'єму даних виникає наступна проблема. Навіть якщо у користувача є можливість, і він зчитує всі попередження можливої атаки, чи будь-якої іншої загорзи даним (наприклад витік даних), користувачі просто не взмозі побачити та індентифікувати проблему, завдяки обширній кількості даних. Для оператора навіть важлива інформація буде прихована за шумом.

Ідентифікація та локалізація окремої атаки чи вразливості та відповідна реакція, при великому об'ємі даних, є складною задачею, неможливою якщо враховувати реальний час.

Тому агреговані дані повинні бути *інтерпретовані*, а саме потрібне проведення аналітики для пошуку загроз та атак.

2. Порівняння з IPS/IDS та SIEM

Security Insights має кілька суттєвих розбіжностей з альтернативами. Було розглянуто вже існуючі та ширико використовувані технології, як `IDS/IPS` та `SIEM`. Детальніше розглянемо наступні технології для їх порівняння з Security Insights. Кожна з цих технологій певним чином імплементована чи доповнена в Security Insight.

`IDS (Intrusion Detection Systems)` аналізують та моніторять мережний трафік, на ознаку відомих кіберзагроз, що намагаються проникнути або викрасти дані з захищеної мережі. Виконується це порівнянням спостережуваної мережної активності за вже відомими в базі даних ознаками.

`IPS (Intrusion Prevention Systems)` локалізовані в тій частині мережі, що й файрвол. Що між зовнішьою та внутрішньою мережою. `IPS` мають інструменти для активного блокування відомих шкідливих пакетів.

`IDS/IPS` спираються в своїй роботі на базу даних, що повідомляє їх про вже відомі загрози. Різниця в тому, що `IDS` моніторить трафік, але не може приймати будь-яких дій, єдине передати інформацію про загрозу відповідним системам, або повідомити адміністратора. Це вже залежить від `IDS` та її налаштувань.

`IPS` натомість має інструменти для контролю трафіку. Але `IDS` як і `IPS` мають спільну слабкість. Їх ефективність залежить від обширності бази даних та регулярного її доповнення, що може зайняти від кількох днів до тижнів, або навіть місяців. В той час як система залишається вразливою.

IDS можна поділити на два типи : За методом підпису (`Signature-based`) та поведінкові або аномальні `IDS` (`Behavior-based`). Хоча дана класифікація існує для `IDS`, `IPS` також можна поділити за наступними критеріями, детальні розбіжності в даному випадку не є суттєвими.

`SIEM` (Security Information and Event Management) – це програмне рішення що об'єднує та аналізує активність із багатьох різних ресурсів у всій IT-інфраструктурі.

Security Insight, беручи за основу `SIEM` технологію має схожу структуру.

SIEM платформи повинні підтримувати інтегрування будь-яких інструментів безпеки, як фаєрволи, identity providers, endpoint protection та інші. Для агрегації, аналізу прозорої інформації про систему.

Все більше організацій використовують модель віддаленого керування, що стає все доступнішою завдяки хмарній інфраструктурі. Тому сучасні SIEM повинні бути взмозі централізувати хмарні дані та швидко знайти на упередити потенційну атаку.

SIEM збирає дані безпеки з мережевих пристроїв, серверів, контролерів доменів тощо. SIEM зберігає, нормалізує, агрегує та застосовує аналітику до цих даних, щоб виявляти тенденції, загрози та дозволяє організаціям дослідити будь-які сповіщення безпеки.

SIEM надає дві основні можливості команді реагування на інцидент:

- Звітування та розслідування інцидентів безпеки.
- Сповіщення базовані на аналітиці, яка відповідає певному рулсету, що вказує на проблему безпеки.

За своєю суттю SIEM є системою агрегування даних, пошуку та звітності. SIEM збирає величезні обсяги даних із усього мережевого середовища, консолідує та робить ці дані доступними для розуміння операторів. Дані, систематизовані та класифіковані, дозволяють досліджувати порушення безпеки даних із необхідною детальністю.

3. Принципи аналітики даних

Агреговані дані потребують аналітики. Більшість сучасних SIEM, включаючи Security Insight аналітика агрегованих даних забезпечується моделями машинного навчання.

Як вже було згадано старе покоління SIEM використовувало ручний пошук загроз, що втрачає ефективність зі зростанням складності атаки та загалом витрачає час операторів рутинною роботою та інші малоефективні насьогодні методи.

Тому проводиться тренування моделей машинного навчання. Їх існує кілька типів, контрольоване (supervised) при тренуванні відомі правильні «відповіді» (структури даних), так тренують схожість поведінки при стандарній та шкідливій поведінці.

Та неконтрольоване (unsupervised) навчання, пошук та реакція на аномальну поведінку.

Security Insight та сучасні SIEM активно використовують AI та машинне навчання.

До сучасних методів аналітики даних можна навести:

- Використання методу UEBA (User and Entity Behavior Analytics), доступ до інформації про користувачів та структур, відбувається моніторинг хто користується системою та як. В залежності від рівня допуску користувача та ширини його доступу до інформації зростає ризик.
- Пріоритизація та рейтинг загроз – користувачам, додаткам тощо надається деякий індекс оцінки ризику, вищий ступінь ризику потребує більш негайної реакції.
- Автоматичне реагування на ризики та атаки, що не зустрічались раніше.
- Доступ в реальному часі до даних, що можна вважати застарими (4-5 років) і що б не використовувались звичайними SIEM.
- Пошук зв'язків серед тисяч подій, дата сетів та інших неструктурованих даних за великий проміжок часу.

Але навіть «застарілі» методи захисту, як завчасне прописання правил, кореляція та збір статистик та певним чином ручний пошук загроз все ще активно використовуються. Хоч і були достатньо доповненими для підтримки їх актуальності.

4. Вже існуючі реалізації технології Security Insight

Варто згадати вже створені імплементації, кожен варіант має свій підхід та акцент на конкретну складову технології (легкість інтеграції зовнішніх рішень, прозорість, потужніші вбудовані інстументи або підвищена інтуїтивність). Хмарний сервіс що використовує система може суттєво впливати на можливості певних реалізацій.

Але всеж в основі лежить сучасна SIEM-система з можливостями аналітики.

- IBM Cloud™ Security Advisor
- Citrix
- RelativityOne
- Confluera: Real-Time Security Insights
- CA Mainframe Security Insights Platform
- R-Vision Incident Response Platform

Висновки

Отже дослідження технології Security Insight дозволяє дослідити проблеми безпеки що виникають при використанні хмарних сервісів та при імплементації SIEM-подібних систем.

Підсумовуючи Security Insight – це агрегація даних про систему, взаємодію між її компонентами, (моніторинг) і також інтерпретація цих даних, те як вони пов'язані.

Здійснюється дана технологія за підтримки сучасних SIEM платформ, що дозволяють збирати дані з рішень безпеки наданих сторонніми розробниками та інтегруванні технологій як IDS/IPS. Використовуючи різні функції, алгоритми й принципи роботи з даними.

Перелік використаних джерел

1. IBM Cloud™ Security Advisor — Access mode: https://cloud.ibm.com/docs/security-advisor?topic=security-advisor-about.
2. Confluera: Real-Time Security Insights — Access mode: https://medium.com/confluera-engineering/real-time-security-insights-apache-pinot-at-confluera-a6e5f401ff02.
3. Relevance of new SIEM approaches — Access mode: https://www.sumologic.com/blog/siem-security-analytics/.