Безпека операційних систем і комп'ютерних мереж

Лекція 22

Системи виявлення атак Intrusion Detection Systems, Intrusion Prevention Systems

Системи виявлення атак

- *Системи виявлення атак* (*СВА)* – це програмні або програмно-апаратні системи, які автоматизують процес аналізу подій в інформаційно-комунікаційній системі з міркувань безпеки
  - англ. – *Intrusion Detection Systems (IDS)*
  - рос. – *Системы обнаружения атак*, (*СОА*)
- Крім виявлення атак (тих, що реально здійснюються, або тих, що є потенційно можливими), СВА здатні здійснювати реагування на атаки – від найпростіших звітів до активного втручання при визначенні проникнень
- У наш час СВА вважаються необхідним елементом інфраструктури безпеки
- Технологія виявлення атак базується на трьох складових:
  - ознаках, що описують порушення політики безпеки
  - джерелах, у яких шукають ознаки порушень політики безпеки
  - методах аналізу інформації, яку одержують з різни джерел

Можливості СВА (1/2)

- Можливість блокування джерела атаки, перешкоджаючи її здійсненню
  - Найбільш ефективним є блокування атак у випадках, коли у системі є вже відомі, але ще не виправлені вразливості
  - Причини такої ситуації:
    - у деяких системах не можуть бути виконані всі необхідні відновлення й модифікації;
    - адміністратори іноді не мають досить часу або ресурсів для відстеження й встановлення всіх необхідних відновлень;
    - користувачам можуть бути необхідні функціональність мережних сервісів і протоколів, які мають відомі уразливості;
    - як користувачі, так і адміністратори роблять помилки при конфігуруванні й використанні систем.
- Можливість здійснювати реакцію на атаку, якщо системою зафіксований факт атаки і її джерело
  - Це дозволяє змусити атакуючого відповідати за власну діяльність
- Можливість визначення преамбул атак, які здебільшого є зондуванням мережі або деяким іншим тестуванням для виявлення вразливостей
  - За наявності СВА сканування буде виявленим, і доступ зловмисника до системи може бути заблокованим
  - Навіть наявність простої реакції на зондування мережі означає підвищений рівень ризику для атакуючого і може змусити його відмовитись від подальших спроб проникнення в мережу

Можливості СВА (2/2)

- Виконання документування існуючих загроз для мережі й систем
  - Документована інформація про атаки може бути корисною при складанні звітів служби захисту інформації
  - Розуміння частоти й характеру атак дозволяє вжити адекватних заходів безпеки
- Забезпечення контролю якості розробки й адміністрування безпеки, особливо у великих і складних ІТС
  - Функціонування СВА протягом тривалого часу надає інформацію про типові способи використання системи
  - Це може дозволити виявити вади у здійсненні керування безпекою, і виправити процедури керування
- Одержання корисної інформації про проникнення, що мали місце, з наданням поліпшеної діагностики для виявлення й коригування факторів, що сприяли компрометації системи
  - Навіть коли СВА не має можливості блокувати атаку, вона може зібрати про неї детальну і достовірну інформацію, яка може бути покладеною в основу відповідних правових і адміністративних заходів
- СВА допомагає визначити розташування джерела атак по відношенню до локальної мережі (зовнішні або внутрішні атаки)
  - Це важливо при прийнятті рішень про розташування ресурсів у мережі

Класифікації СВА за різними характеристиками (1/3)

- *На якому етапі її здійснення фіксується атака*
  - Типовим для СВА є виявлення атак *у реальному часі*, тобто в момент їх здійснення
    - Такі СВА є класичними.
  - Існують системи, які здійснюють аналіз журналів реєстрації, і таким чином виявляють атаки, *які були здійснені раніше*.
  - Іноді до СВА відносять засоби, які здійснюють аналіз системи і попереджають про *потенційну можливість здійснення атаки*.
    - До таких засобів відносяться сканери вразливостей
- *Інформаційні джерела*
  - *СВА рівня мережі* (*network-based IDS*)
  - СВА рівня вузлів (*host-based IDS*)
    - СВА рівня ОС
    - СВА рівня СКБД
    - СВА рівня прикладних програм
- *Метод аналізу*
  - *Виявлення зловживань* (*misuse detection*)
  - *Виявлення аномалій* (*anomaly detection*)

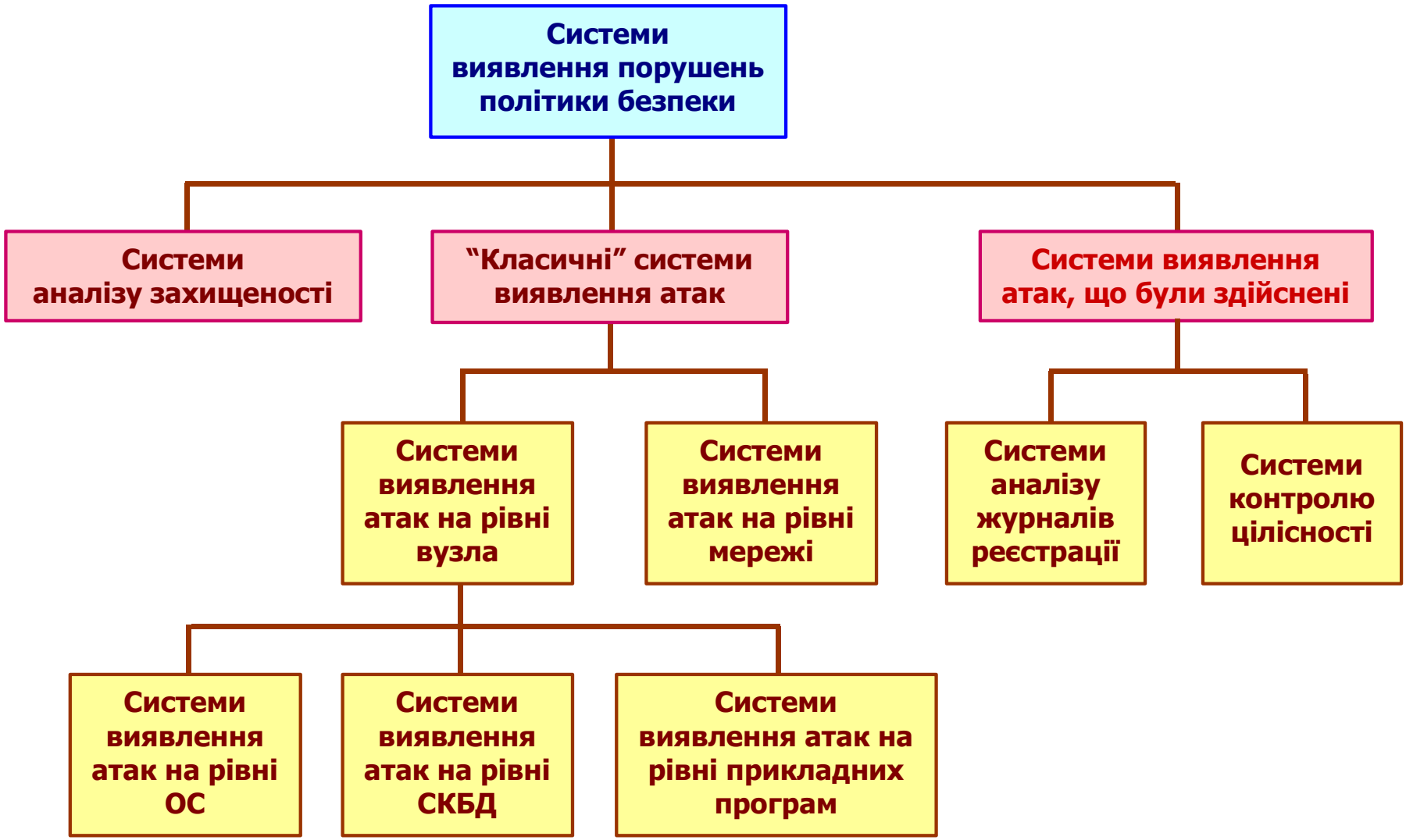
Класифікації СВА за різними характеристиками (2/3)

- *Швидкість реакції* (затримка в часі між одержанням інформації із джерела та її аналізом і реакцією на неї)
  - *СВА пакетного режиму* (*interval-based IDS*)
    - Багато ранніх СВА рівня вузлів використовували таку схему роботи, тому що вони цілком залежали від накопичення записів аудита в ОС
    - СВА пакетного режиму не виконують ніяких активних дій у відповідь на виявлені атаки
  - *СВА реального часу* (*real-time IDS*)
    - СВА реального часу обробляють безперервний потік інформації від джерел
    - Це є переважною схемою роботи СВА рівня мережі, які одержують інформацію з потоку мережного трафіку
    - Виявлення проникнення, що здійснюється СВА реального часу, приводить до результатів досить швидко, і це дозволяє СВА виконувати певні дії у відповідь в автоматичному режимі.
- *Характер відповіді* (набір дій, які система виконує після виявлення проникнень)
  - Активні заходи
    - Автоматичне втручання в деяку іншу систему (наприклад, керування комутатором або мережним екраном)
  - Пасивні заходи
    - Звіт СВА, зроблений для людей, які потім виконують деякі дії на основі даного звіту

Класифікації СВА за різними характеристиками (3/3)

- *Архітектура СВА* (визначає, які функціональні компоненти СВА наявні, і як вони взаємодіють один з одним)
  - Основні архітектурні компоненти:
    - система, на якій виконується ПЗ СВА (*host*)
    - система, за якою СВА спостерігає (*target*)
  - Раніше СВА, переважно, виконувалися на тих же системах, які вони захищали
  - З появою робочих станцій і персональних комп'ютерів у більшості архітектур СВА передбачається виконання СВА на окремій системі, тим самим розділяючи системи host і target
    - Це поліпшує безпеку функціонування СВА.
  - Сучасні СВА, як правило, складаються з таких компонентів:
    - сенсор, що відслідковує події в мережі або системі
    - аналізатор подій, виявлених сенсорами
    - компонента ухвалення рішення
- *Способи керування* (яким чином можна керувати елементами СВА, їхніми вхідними та вихідними даними)
  - *централізоване керування* (керування усім моніторингом, виявленням й звітністю здійснюється безпосередньо з єдиного "поста")
  - *частково розподілене керування* (моніторинг і визначення керуються з локального вузла, а ієрархічна звітність спрямовується в одне або більше центральних розташувань)
  - *повністю розподілене керування* (моніторинг і визначення виконуються з використанням підходу, заснованому на агентах, коли рішення про відповідь приймаються в точках аналізу)

Узагальнена класифікація СВА



СВА рівня мережі

- СВА рівня мережі визначають атаки, захоплюючи й аналізуючи мережні пакети
  - У сучасних системах часто використовується множина сенсорів, розташованих у різних точках мережі. Ці пристрої переглядають мережний трафік, виконуючи його локальний аналіз та створюючи звіти про атаки для центральної керуючої консолі.
- СВА рівня мережі є найпоширенішими
  - До них належить переважна більшість комерційних СВА
- Переваги СВА рівня мережі:
  - Декілька оптимально розташованих СВА можуть переглядати велику мережу
  - Розгортання СВА рівня мережі не впливає сильно на продуктивність мережі
    - Сенсори, як правило, є пасивними пристроями, які прослуховують мережний канал без впливу на нормальне функціонування мережі
  - СВА рівня мережі можуть бути зроблені практично невразливими до атак або навіть абсолютно невидимими для атакуючих

Недоліки СВА рівня мережі

- СВА рівня мережі, захоплюючи трафік, не гальмує роботу самої мережі, але може не встигати обробляти всі пакети у великій або зайнятій мережі
  - При підвищеному навантаженні в мережі СВА може пропустити атаку, не виявивши її
  - Деякі виробники намагаються вирішити дану проблему, повністю реалізуючи СВА апаратно
  - Необхідність швидко аналізувати пакети може призвести до того, що розробники СВА будуть обмежувати її можливості визначенням невеликої кількості атак або ж використовувати як можна менші обчислювальні ресурси, що знижує ефективність виявлення
- У сучасних мережних технологіях намагаються уникати спільного середовища передачі даних, що ускладнює підключення сенсорів СВА рівня мережі
  - Для того, щоби СВА могла переглядати мережний трафік від декількох хостів, необхідне її підключення до маршрутизатора (комутатора) та таке налаштовування мережного обладнання, при якому на порт, що пов'язаний з СВА, буде потрапляти (дублюватись) увесь трафік сегмента
    - це створює проблему через необхідність дуже великої перепускної спроможності цього порту та самої СВА.
- СВА рівня мережі не можуть аналізувати зашифровану інформацію
  - Ця проблема дуже актуальна при використанні VPN
- Більшість СВА рівня мережі не здатні зробити висновок про те, чи була атака успішною; вони можуть тільки визначити, що атака була розпочата
  - Після того як СВА виявить атаку, адміністратор повинен вручну досліджувати кожний атакований хост для визначення, чи відбулося реальне проникнення

СВА рівня вузла

- СВА рівня вузла мають справу з інформацією, зібраною усередині єдиного комп'ютера
- СВА рівня вузла звичайно використовують в якості інформаційних джерел журнали реєстрації подій, що створюються ОС та прикладними програмами
- Деякі СВА рівня вузла розроблені для підтримки централізованої інфраструктури керування й одержання звітів СВА, що може допускати єдину консоль керування для відстеження багатьох хостів
- Переваги СВА рівня вузла:
  - СВА рівня вузла, з їхньою можливістю стежити за подіями локально по відношенню до хосту, можуть визначити атаки, які не можуть виявити СВА рівня мережі.
  - На відміну від СВА рівня мережі, СВА рівня вузла можуть "бачити" наслідки початої атаки, тому що вони можуть мати безпосередній доступ до системної інформації, файлів даних і системних процесів, які є ціллю атаки
  - СВА рівня вузла здатні аналізувати діяльність із великою вірогідністю й точністю, визначаючи тільки ті процеси й користувачів, які мають відношення до конкретної атаки
  - СВА рівня вузла часто можуть функціонувати в оточенні, у якому мережний трафік зашифрований, коли джерела інформації рівня вузла створюються до того, як дані шифруються, і/або після того, як дані розшифровуються на хості призначення
  - На функціонування СВА рівня вузла не впливає топологія мережі
  - Коли СВА рівня вузла працюють із результатами аудита ОС, вони можуть надати допомогу у виявленні "троянських коней" або інших атак, які порушують цілісність ПЗ

Недоліки СВА рівня вузла

- СВА рівня вузла більш складні у керуванні, тому що інформація повинна бути сконфігурована й повинна управлятися для кожного хоста, що переглядається
- Джерела інформації (а іноді й частина засобів аналізу) для СВА рівня вузла розташовані на тому ж хості, що є метою атаки, тому, як складова частина атаки, СВА може бути атакована й відключена
- СВА рівня вузла не завжди можуть визначити сканування мережі, або інші впливи, метою яких є вся мережа, тому що СВА спостерігає тільки за мережними пакетами, одержуваними конкретним хостом
- СВА рівня вузла можуть бути блоковані деякими DoS-атаками
- Коли СВА рівня вузла використовує результати аудита ОС як джерело інформації, об’єм інформації може бути величезним, що потребує додаткових ресурсів для зберігання в системі
- СВА рівня вузла використовують обчислювальні ресурси хостів, за якими вони спостерігають, що впливає на продуктивність спостережуваної системи

СВА рівня прикладних програм

- *СВА рівня прикладних програм* (*application-based IDS*) є специфічною підмножиною СВА рівня вузла, які аналізують події, пов'язані з конкретним прикладним ПЗ
  - Найбільш типовими джерелами інформації, що використовуються такими СВА, є журнали реєстрації транзакцій прикладного ПЗ
- Здатність взаємодіяти безпосередньо з прикладною програмою, з конкретним доменом, або використовувати знання, специфічні для певної прикладної програми, дозволяє СВА рівня прикладних програм визначати підозріле поводження авторизованих користувачів, що перевищує їхні повноваження
  - Такі порушення можуть виявитися тільки при аналізі взаємодії користувача з прикладною програмою
- Переваги СВА рівня прикладних програм:
  - СВА рівня прикладних програм можуть аналізувати взаємодію між користувачем і програмою, що часто дозволяє відстежити неавторизовану діяльність конкретного користувача
  - СВА рівня прикладних програм, як правило, можуть працювати в зашифрованих оточеннях, тому що вони отримують інформацію у кінцевій точці інформаційного обміну, де інформація представлена вже в незашифрованому вигляді

Недоліки СВА рівня прикладних програм

- СВА рівня прикладних програм можуть бути більш уразливі, ніж СВА рівня ОС, до атак на записи реєстрації подій
  - журнали реєстрації прикладного ПЗ можуть бути захищені менш надійно, ніж результати аудита ОС
- СВА рівня прикладних програм часто переглядають події на користувальницькому рівні абстракції, на якому у більшості випадків неможливо визначити “троянських коней” або інші подібні атаки, пов’язані з порушенням цілісності ПЗ

- Для компенсації зазначених недоліків СВА рівня прикладних програм доцільно використовувати у комбінації з СВА рівня ОС та/або рівня мережі

Аналіз подій у СВА

- Існує два основних підходи до аналізу подій для виявлення атак:
  - *виявлення зловживань* (*misuse detection*)
    - У технології виявлення зловживань відомо, яка послідовність даних є ознакою атаки
    - Аналіз подій полягає у пошуку таких “небажаних” послідовностей даних, які називають *сигнатурами* (*signature*)
    - Технологія виявлення зловживань використовується в більшості комерційних СВА
  - *виявлення аномалій* (*anomaly detection*)
    - У технології виявлення аномалій відомо, що являє собою “нормальна” діяльність і “нормальна” мережна активність
    - Аналіз подій полягає в спробі виявити аномальне поводження користувача або аномальну мережну активність
    - Ця технологія на сьогоднішній день є предметом досліджень і використовується в обмеженій формі незначним числом СВА
- Існують сильні й слабкі сторони, пов'язані з кожним підходом. Вважається, що найбільш ефективні СВА застосовують в основному виявлення зловживань із невеликими компонентами виявлення аномалій

Виявлення зловживань (сигнатурний метод)

- Детектори зловживань контролюють діяльність системи, аналізуючи подію або множину подій на відповідність заздалегідь визначеному зразку (сигнатурі), що описує відому атаку
- Найбільш типова форма визначення зловживань, що здебільшого використовується у комерційних продуктах, визначає кожний зразок події, що відповідає атаці, як окрему сигнатуру
- Проте існують складніші підходи для виявлення зловживань, що отримали назву технологій аналізу на основі стану (*state-based*), які можуть використовувати єдину сигнатуру для визначення групи атак

Переваги й недоліки сигнатурного методу

- Переваги сигнатурного методу:
  - Детектори зловживань є дуже ефективними для визначення атак
  - Детектори зловживань не створюють величезного числа помилкових повідомлень
  - Детектори зловживань можуть швидко й надійно діагностувати використання конкретного інструментального засобу або технології атаки
    - Це може допомогти адміністраторові скорегувати заходи для забезпечення безпеки
  - Детектори зловживань дозволяють адміністраторам, незалежно від рівня їхньої кваліфікації в області безпеки, почати процедури обробки інциденту
- Недоліки сигнатурного методу:
  - Детектори зловживань можуть визначити тільки ті атаки, про які вони знають
    - Необхідно постійно обновляти їхні бази даних для одержання сигнатур нових атак
  - Більшість детекторів зловживань розроблені таким чином, що можуть використовувати тільки строго певні сигнатури, а це не допускає визначення варіантів загальних атак

Виявлення аномалій (1/2)

- Детектори аномалій визначають ненормальне (незвичайне) поводження на хості або в мережі
  - Вони припускають, що атаки відрізняються від “нормальної” (законної) діяльності і можуть бути визначені системою, що вміє відслідковувати ці відмінності.
- Детектори аномалій створюють профілі, що представляють собою нормальне поводження користувачів, хостів або мережних з’єднань
  - Ці профілі створюються, виходячи з даних історії, зібраних у період нормального функціонування.
  - Потім детектори збирають дані про події й використовують різні метрики для визначення того, що аналізована діяльність відхиляється від нормальної
- Детектори аномалій і СВА, що на них засновані, часто створюють велику кількість помилкових повідомлень, тому що зразки нормального поводження користувача або системи можуть бути дуже невизначеними.
  - Незважаючи на цей недолік, вважається, що СВА, засновані на виявленні аномалій, мають можливість визначати нові форми атак, на відміну від СВА, заснованих на сигнатурах, які цілком покладаються на відповідність зразку минулих атак.

Виявлення аномалій (2/2)

- Деякі форми визначення аномалій створюють вихідні дані, які можуть бути далі використані як джерела інформації для детекторів зловживань
  - Наприклад, детектор аномалій, заснований на визначенні граничного припустимого рівня, може створювати діаграму, що представляє собою “нормальну” кількість файлів, доступних конкретному користувачеві. Детектор зловживань може використовувати цю діаграму як частину сигнатури виявлення, що говорить: “якщо кількість файлів, доступних даному користувачеві, перевищує задану нормальну діаграму більш ніж на 10%, варто ініціювати сигнал попередження”.
- Деякі комерційні СВА включають обмежені форми виявлення аномалій
  - Мало хто покладається винятково на дану технологію.
  - Виявлення аномалій, що включено до існуючих комерційних систем, звичайно використовується для виявлення зондування мережі або сканування портів.
- Виявлення аномалій залишається предметом досліджень в області активного виявлення проникнень, і швидше за все буде відігравати зростаючу роль в СВА наступних поколінь

Метрики й технології, використовувані при виявленні аномалій (1/2)

- *Визначення припустимої межі*
  - Основні атрибути поводження користувача й системи виражаються в кількісних термінах
    - число файлів, доступних користувачеві в даний період часу
    - число невдалих спроб входу в систему
    - кількість процесорного часу, що використовується процесом тощо
  - Для кожного атрибута визначається деякий рівень, що встановлюється як припустимий
    - Граничний рівень може бути статичним або евристичним – наприклад, може визначатися не певним значенням деякої величини, а його зміною
- *Статистичні метрики*
  - Параметричні
    - передбачається, що розподіл атрибутів профілю відповідає конкретному зразку
  - Непараметричні
    - розподіл атрибутів профілю визначається у процесі “навчання”, виходячи з набору значень, які спостерігалися за певний період часу

Метрики й технології, використовувані при виявленні аномалій (2/2)

- *Метрики, засновані на правилах*
  - Такі метрики аналогічні непараметричним статистичним метрикам у тому, що дані, за якими спостерігають протягом певного часу, визначають припустимі зразки, але відрізняються від них тим, що ці зразки специфіковані як правила, а не як чисельні характеристики
- *Інші метрики*
  - Нейромережі
  - Генетичні алгоритми
  - Моделі імунних систем
- Перші дві технології найбільш розповсюджені у сучасних комерційних СВА.

Переваги й недоліки виявлення аномалій

- Переваги виявлення аномалій:
  - СВА, засновані на виявленні аномалій, фіксують несподіване поводження і, таким чином, мають можливість визначити симптоми атак без знання конкретних деталей атаки
  - Детектори аномалій можуть створювати інформацію, що надалі буде використовуватися для визначення сигнатур для детекторів зловживань
- Недоліки виявлення аномалій:
  - Виявлення аномалій звичайно створює велику кількість помилкових сигналів про атаки при непередбаченому поводженні користувачів і непередбаченій мережній активності
  - Виявлення аномалій часто вимагає деякого етапу навчання системи, під час якого визначаються характеристики нормального поводження
    - Від якості проведення цього навчання суттєво залежить подальша ефективність СВА

Можливі відповідні дії СВА

- **Активні відповіді**
  - ***Збирання додаткової інформації***
  - ***Зміна оточення***
    - вставити TCP-пакет з прапором RST у з'єднання порушника з ціллю його атаки, тим самим розриваючи з'єднання;
    - переконфігурувати маршрутизатори та мережні екрани для блокування пакетів з IP-адреси, яку визначили як джерело атаки;
    - переконфігурувати маршрутизатори та мережні екрани для блокування на стороні атакованого вузла мережних портів, протоколів або сервісів, які використовує порушник;
    - в екстремальних ситуаціях переконфігурувати маршрутизатори та мережні екрани для блокування усіх з'єднань до системи, на яку здійснюється атака.
  - ***Виконання дії проти порушника***
- **Пасивні дії**
  - ***Тривоги й оповіщення***
  - ***Використання SNMP Traps***
  - ***Можливості звітів і архівування***
  - ***Можливість зберігання інформації про збої***

Додаткові інструментальні засоби

- Існує кілька видів інструментальних засобів, які доповнюють СВА і часто позначаються розробниками як системи виявлення проникнення, тому що вони виконують аналогічні функції
  - Антивірусне програмне забезпечення
  - Засоби аналізу вразливостей
  - Засоби контролю цілісності файлів
  - Принади (*honey pots*), або *обманні системи*