Модуль 4. Основи хакінгу та розслідування інцидентів в ISC/SCADA системах

Лекція 3: **Виявлення вторгнень та ситуаційна обізнаність в ICS/SCADA.**

Мета лекції

Сформувати практичне розуміння виявлення вторгнень і підтримання ситуаційної обізнаності в ICS/SCADA для своєчасного виявлення, аналізу та стримування загроз

Основні завдання

- Пояснити роль IDS у OT середовищі та відмінності NIDS і HIDS, місця їх розгортання, сильні й слабкі сторони
- Навчити будувати базовий рівень нормальної роботи і виявляти відхилення в мережевому трафіку, на хостах і у фізичному процесі
- Показати застосування спеціалізованих OT-засобів і пасток deception, підтримку промислових протоколів, інтеграцію з SIEM
- Розкрити можливості SIEM для агрегації журналів, кореляції подій і оперативного реагування з урахуванням OT-контексту
- Сформувати підхід до безперервного моніторингу NetFlow, логів і телеметрії процесу, налаштування правил і зменшення хибних спрацювань
- Підкреслити важливість підготовки персоналу, спільної роботи IT і OT, актуальних процедур і якісної документації

3.1. Системи виявлення вторгнень (IDS/NIDS/HIDS) та їх застосування в мережах ICS

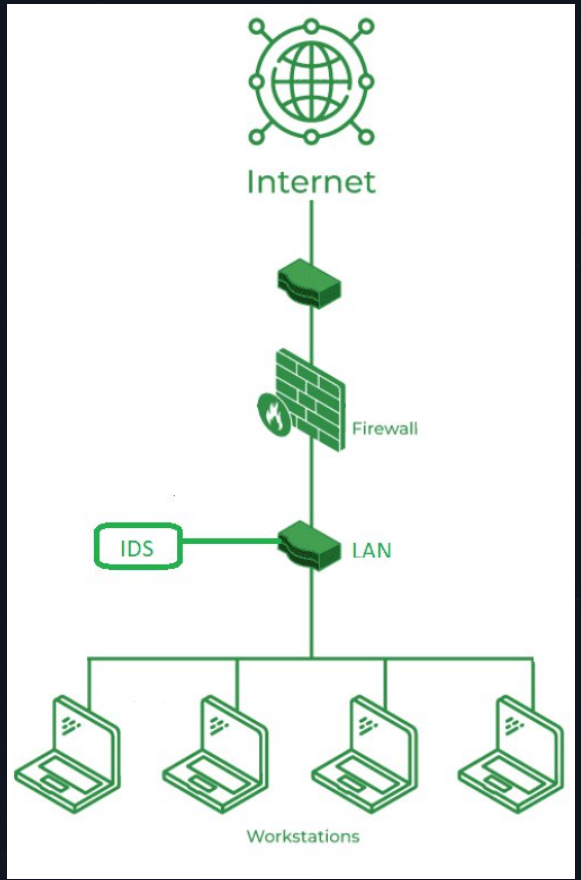
3.1.1. Системи виявлення вторгнень: Основи захисту

Що таке IDS?

Системи виявлення вторгнень (Intrusion Detection Systems, IDS) є важливим інструментом для виявлення шкідливої активності в мережах ICS. Коли вторгнення вже відбулося, першим і необхідним кроком для його нейтралізації та усунення є саме виявлення його існування.

Визначення вторгнення

Під "вторгненням" розуміється широкий спектр процесів та ефектів, пов'язаних з присутністю та діями шкідливого програмного забезпечення в ICS. Це включає несанкціонований доступ, зміни конфігурації та шкідливі дії.



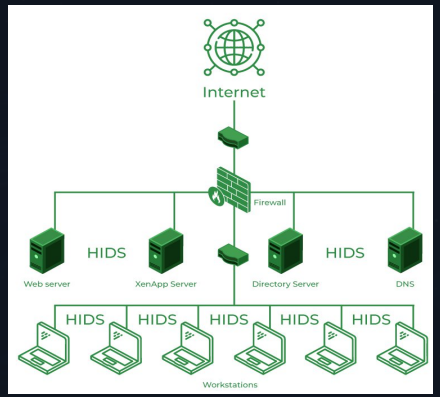
3.1.2. Типи систем виявлення вторгнень

HIDS - Хостові системи

Хостові системи виявлення вторгнень (Host-Based Intrusion Detection Systems, HIDS) - це програмне забезпечення, яке моніторить одну або кілька характеристик системи:

- Записи в журналах додатків
- Зміни конфігурації системи
- Доступ до чутливих даних на системі

У випадку спроби порушення безпеки користувачем, HIDS реагує тривогою або контрзаходом.

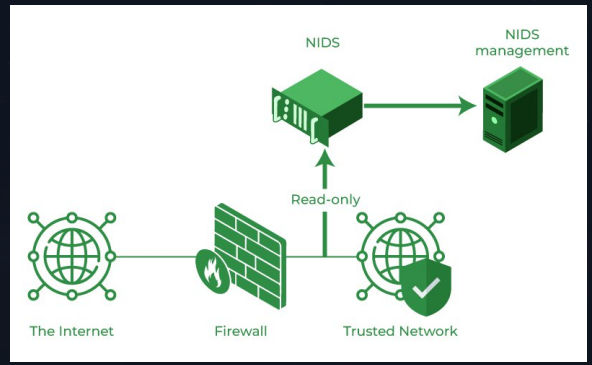


NIDS - Мережеві системи

Мережеві системи виявлення вторгнень (Network-Based Intrusion Detection Systems, NIDS) контролюють мережевий трафік для виявлення підозрілої активності:

- Сигнатурні системи виявлення
- Аномальні системи виявлення
- Гібридні системи виявлення

NIDS є невід'ємною частиною ефективного розгортання IDS в промислових мережах.



3.1.3. Snort: Потужний інструмент NIDS

Snort є популярною системою виявлення вторгнень в мережу (NIDS) з відкритим вихідним кодом, яка також може функціонувати як система запобігання вторгненням в мережу (NIPS). Snort має модульну архітектуру та гнучку мову правил, що дозволяє описувати трафік для збору.

- **Сигнатурне виявлення**

  Забезпечує виявлення відомого шкідливого програмного забезпечення, зловмисного трафіку та віддалених експлойтів на основі заздалегідь визначених сигнатур.

- **Виявлення аномалій**

  Здатна виявляти аномальний трафік, наприклад, невідомі IP-адреси або несподіване використання портів/протоколів в промислових мережах.

- **Промислові протоколи**

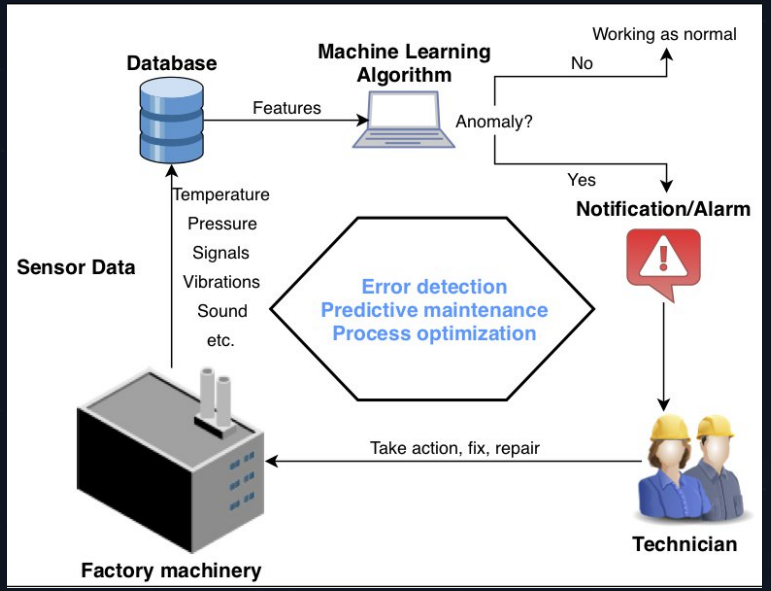
  Міністерство внутрішньої безпеки США (DHS) фінансувало розробку наборів правил Snort для кількох промислових протоколів (Modbus/IP, IEC-60870-5-104, DNP3).

3.1.4. Виявлення аномалій у фізичному процесі

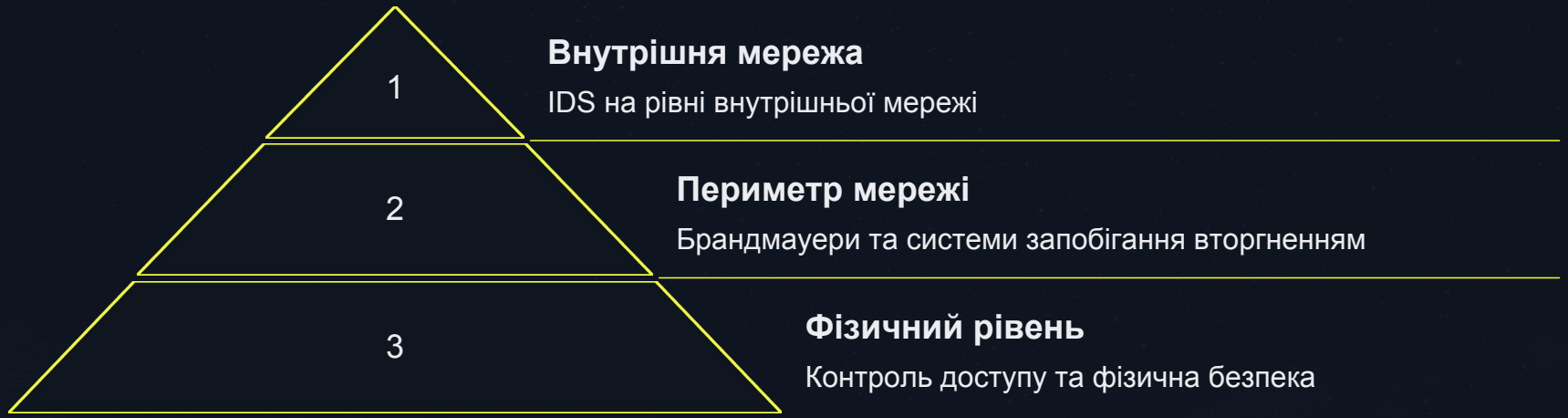
Оскільки безпека ICS, зрештою, полягає в захисті змінних процесу, а не лише мережевого трафіку, набули інтересу процесно-орієнтовані проекти для моніторингу та виявлення вторгнень. Моніторинг фізичного середовища в зоні польових пристроїв може надати дуже цінну інформацію не лише про сам фізичний процес (контроль), а й про статус виконання контролерів та цифрових пристроїв.

> Оскільки польові контролери безпосередньо впливають на фізичний процес, можна опосередковано оцінити цілісність польових пристроїв, моніторячи сам процес.

Ця концепція може бути розширена до моніторингу фізичних процесів, що відбуваються всередині самих контролерів, і таким чином безпосередньо оцінювати статус їх виконання. Приклад такої системи IDS для ПЛК був реалізований: IDS визначає базовий рівень нормальної роботи, а потім виявляє шкідливу модифікацію, подібну до Stuxnet, у логіці ПЛК.



3.1.5. Захист в глибину: Багаторівнева стратегія



IDS є одним із шарів концепції "Захисту в глибину" (Defense-in-Depth) - багаторівневої стратегії безпеки. Вона розташовується на "Рівні внутрішньої мережі" (Internal Network Layer) та використовується для виявлення вторгнень будь-якого користувача (авторизованого чи несанкціонованого).

3.1.6. Спеціалізовані системи виявлення кіберзагроз

Спеціалізовані системи виявлення/запобігання кіберзагроз для мереж АСУ ТП є важливим інструментом, оскільки цільова атака може пройти міжмережеві екрани та досягти критичного об'єкта в нижніх сегментах промислової мережі.

Виявлення вразливостей

Ці системи можуть виявляти потенційні вразливості, такі як застаріле програмне забезпечення та активи без паролів, що створюють ризики для промислової мережі.

Загрози нульового дня

Виявлення загроз нульового дня (zero-day threats) за фактом несанкціонованого оновлення прикладної програми або мережевого пристрою.

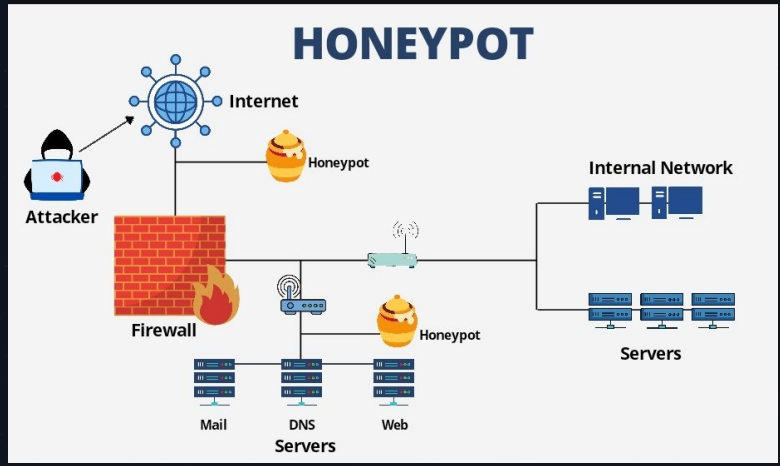
3.1.7. Медові пастки: Платформи обману

Distributed Deception Platform (DDP)

Платформи Distributed Deception Platform (DDP) дозволяють розгортати мережу підроблених, але надзвичайно привабливих для зловмисників пристроїв-приманок, які майже не відрізняються від реальних.

Ці пастки фактично є датчиками проникнення, що дозволяють виявляти зловмисне проникнення з високою ймовірністю (99%) через використання неправдивої інформації, розміщеної на них:

- Паролі
- Мережеве оточення
- Закладки
- Файли користувачів
- Конфігурації систем



99% ймовірність виявлення зловмисного проникнення завдяки використанню неправдивої інформації на пристроях-приманках.

3.1.8. Рекомендації щодо впровадження IDS

01

Комбіноване розгортання

Впроваджуйте як NIDS, так і HIDS для комплексного моніторингу мережевого трафіку та активності на хостах.

02

Спеціалізація на OT-протоколах

Використовуйте IDS, які підтримують та розуміють специфічні промислові протоколи (Modbus, DNP3, S7 тощо).

03

Базовий рівень та аномалії

Налаштовуйте IDS на визначення "базового рівня" нормальної роботи системи та виявляйте відхилення.

04

Фізичний моніторинг

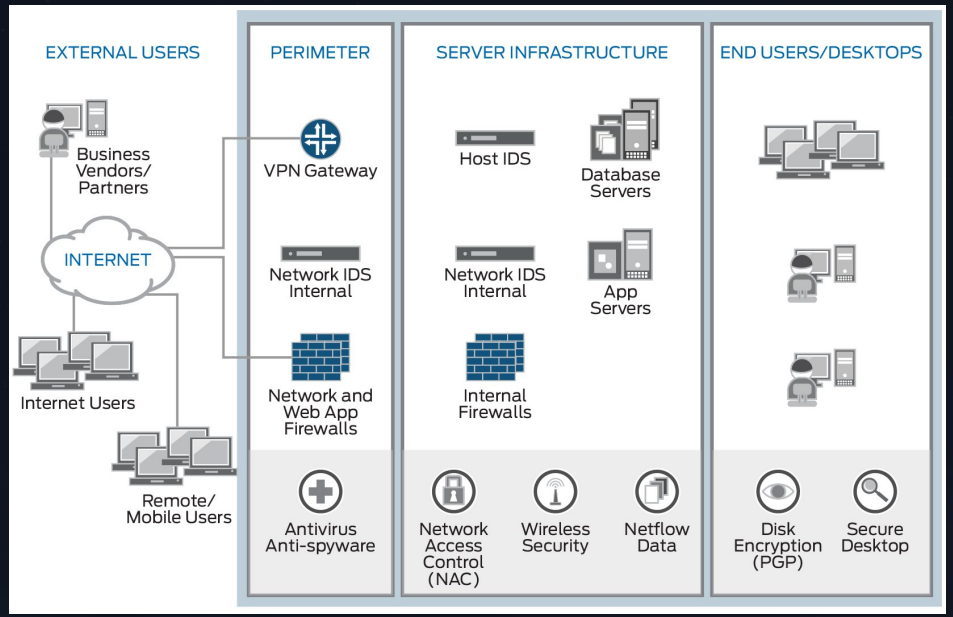
Розгляньте можливість моніторингу фізичних змін у процесі як додатковий рівень виявлення вторгнень.

05

Медові пастки

Впровадження DDP може бути ефективним способом виявлення цільових атак без ризику для реальних систем.

3.2. Системи управління інформаційною безпекою та подіями безпеки (SIEM)

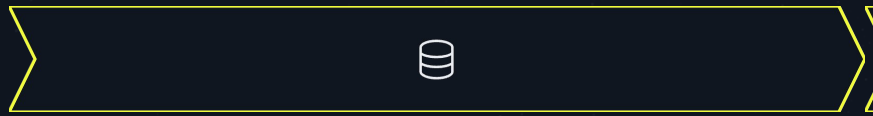


3.2.1. SIEM: Центральна система управління безпекою

Системи управління інформаційною безпекою та подіями безпеки (Security Information and Event Management, SIEM) є програмними продуктами, які відіграють центральну роль у постійному моніторингу безпеки ICS. Вони агрегують та аналізують журнали безпеки з різних джерел для виявлення інцидентів та підтримки ситуаційної обізнаності.

> SIEM-системи збирають дані журналів та події безпеки з різноманітних джерел, таких як IDS, брандмауери, операційні системи, антивірусні програми, мережеві пристрої та додатки, що були впроваджені для захисту ICS.

3.2.2. Функціональність SIEM систем



Агрегація даних

Збір журналів та подій безпеки з різноманітних джерел: IDS, брандмауери, ОС, антивіруси, мережеві пристрої

Кореляція подій

Аналіз та кореляція даних для виявлення закономірностей або послідовностей подій, які можуть вказувати на атаку

Виявлення інцидентів

Ідентифікація шкідливої активності, яка може бути непомітною при моніторингу окремих джерел

Реагування

Повідомлення про несприятливі події повинні оцінюватися персоналом за допомогою процесу оброблення інцидентів

3.2.3. SIEM у життєвому циклі кібербезпеки

Фаза планування

Визначення вимог до SIEM та планування архітектури системи моніторингу

1

Фаза обслуговування

Активне використання під час фази технічного обслуговування для постійного моніторингу безпеки

3

2

Фаза впровадження

SIEM-системи впроваджуються на цій фазі життєвого циклу кібербезпеки ICS

3.2.4. Виклики SIEM в OT-середовищі

Затримки даних

Впровадження та ефективне використання SIEM в OT-середовищі може стикатися з затримками в обробці даних через специфіку промислових мереж.

Втрата ситуаційної обізнаності

Потенційна втрата ситуаційної обізнаності через складність інтеграції різнорідних систем та протоколів.

Застаріле обладнання

Використання застарілого обладнання в промислових мережах може ускладнювати збір та аналіз журналів.

Складність моніторингу

Моніторинг кібербезпеки вимагає від персоналу глибоких знань застосунків, розуміння хибних спрацювань та вміння точно конфігурувати засоби моніторингу.

3.2.5. Рекомендації щодо впровадження SIEM

Комплексна інтеграція

Інтегруйте всі можливі джерела журналів та подій (IDS, брандмауери, контролери, сервери, робочі станції) до SIEM для отримання повного уявлення про активність у мережі.

Адаптація правил кореляції

Налаштуйте правила кореляції в SIEM для виявлення атак, специфічних для ICS/OT, враховуючи особливості промислових протоколів та поведінки технологічного процесу.

Навчання персоналу

Забезпечте глибоке навчання персоналу, який працює з SIEM, щоб вони розуміли його функціональність, вміли інтерпретувати сповіщення та ефективно реагувати на інциденти.

Постійний моніторинг

SIEM має бути частиною стратегії безперервного моніторингу, що дозволяє виявляти загрози в реальному часі та підтримувати актуальну ситуаційну обізнаність.

3.3. Концепції ситуаційної обізнаності для кібербезпеки ICS

3.3.1. Ситуаційна обізнаність: Основа кібербезпеки

Ситуаційна обізнаність (Situational Awareness) у контексті кібербезпеки ICS передбачає постійне розуміння стану мережевого середовища та дій потенційних атакерів. Це життєво важливо для забезпечення безпечної, надійної та захищеної роботи виробничих процесів.

> Ефективна ситуаційна обізнаність вимагає збору та аналізу інформації з різних джерел та рівнів ICS/OT архітектури для отримання комплексного розуміння поточного стану системи.

3.3.2. Багаторівневе розуміння ситуаційної обізнаності

Моніторинг мережі

Виявлення аномалій у мережевому трафіку, нових підключень, несподіваного використання портів/протоколів

HMI інтерфейс

Людино-машинний інтерфейс надає візуальне представлення процесу, але може бути скомпрометований атаками типу Stuxnet

Моніторинг хостів

Відстеження змін конфігурації, записів у журналах додатків та доступу до чутливих даних

Фізичний процес

Моніторинг фізичного середовища для оцінки цілісності польових пристроїв та виявлення шкідливих модифікацій

3.3.3. Аналіз даних та кореляція в ситуаційній обізнаності

Технології аналізу

Ефективна ситуаційна обізнаність базується на аналізі великих даних та машинному навчанні для виявлення та пом'якшення загроз у режимі реального часу.

Це включає використання:

- Історичних даних з фізичних систем
- Контекстних даних з численних та різноманітних датчиків
- Аналізу поведінки людини для виявлення аномалій

Мета - отримання більш високого рівня колективного бачення мережі для кращої кореляції подій та аналізу рішень.

3.3.4. Людський фактор у ситуаційній обізнаності

Моніторинг кібербезпеки не є тривіальним завданням і вимагає глибоких знань персоналу. Співробітники, які відповідають за моніторинг, повинні мати розуміння застосунків, які вони використовують, вміти розрізняти хибні спрацювання та точно конфігурувати системи безпеки для оптимізації їх точності.

Культура кібер-обізнаності

Культура кібер-обізнаності, де оператори розуміють взаємозв'язок між кібер- та фізичними системами, є критично важливою для ефективного моніторингу.

Професійні навички

Персонал повинен володіти навичками аналізу журналів, розуміння мережевих протоколів та здатністю швидко реагувати на інциденти безпеки.

3.3.5. Рекомендації щодо ситуаційної обізнаності

Інтегрований моніторинг

Створіть інтегровану систему моніторингу, яка збирає та аналізує дані з усіх рівнів ICS/OT, включаючи мережевий трафік, хостові журнали та дані фізичного процесу.

Навчання персоналу

Впроваджуйте постійне навчання персоналу, щоб підвищити їхню обізнаність про кіберзагрози та розвинути навички прийняття рішень у кризових ситуаціях.

Технології та аналітика

Використовуйте передові технології, такі як SIEM, NetFlow, та, де це можливо, машинне навчання для автоматизації виявлення аномалій та кореляції подій.

Базовий рівень

Визначте та постійно оновлюйте базовий рівень нормальної роботи системи, щоб ефективно виявляти відхилення та аномалії.

3.4. Аналіз журналів та моніторинг

3.4.1. Аналіз журналів: Основа моніторингу

Ефективний аналіз журналів та постійний моніторинг є ключовими для виявлення інцидентів та підтримки ситуаційної обізнаності в ICS/SCADA системах. Це є невід'ємною частиною фази технічного обслуговування життєвого циклу кібербезпеки.

Постійний моніторинг безпеки
Діяльність зосереджена на відстеженні технологій, впроваджених для виявлення шкідливої активності. Включає моніторинг IDS, SIEM-систем, антивірусних програм та інших систем захисту.

Моніторинг активів
Постійне відстеження пристроїв, підключених до системи, щоб переконатися, що вони використовують останні версії програмного забезпечення. Нові пристрої повинні бути ретельно досліджені.

3.4.2. Джерела даних для аналізу журналів

Журнали додатків та систем

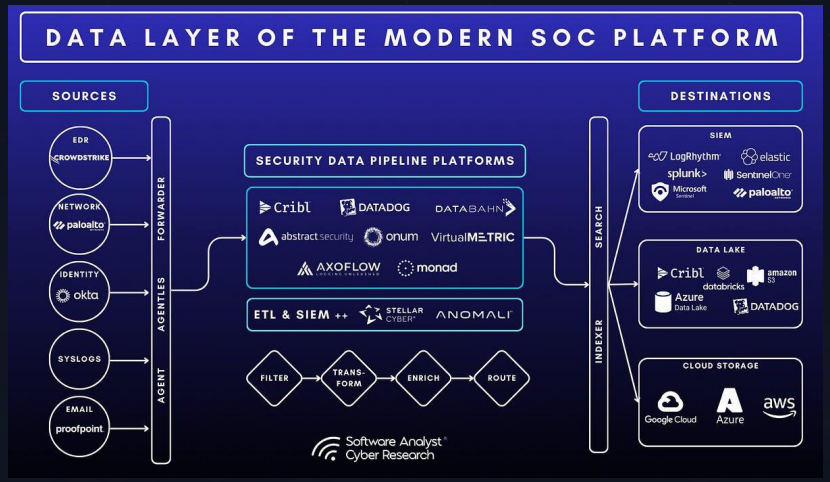
HIDS моніторить записи в журналах додатків та зміни конфігурації системи. Ці дані надають інформацію про активність на рівні хоста та можливі порушення безпеки.

Мережевий трафік

NIDS аналізує мережевий трафік. Інструменти, такі як Snort, можуть виявляти сигнатури відомого шкідливого ПЗ та аномалії, пересилаючи Syslog-повідомлення до SIEM.

NetFlow

Технологія забезпечує масштабований та доступний спосіб моніторингу мережі, збираючи та аналізуючи метадані про мережевий трафік для виявлення аномалій та інцидентів.



3.4.3. Якість аналізу та судово-медичний аналіз

Вимоги до якості

Моніторинг кібербезпеки вимагає від персоналу глибоких знань застосунків, що використовуються для моніторингу, та розуміння хибних спрацювань систем захисту.

Персонал також повинен бути здатний конфігурувати засоби та системи, що використовуються для моніторингу безпеки, для оптимізації їх точності.

Судово-медичний аналіз

Візуалізація текстових зв'язків з журналів корисна для створення методологій класифікації в судово-медичному аналізі, що допомагає в розслідуванні інцидентів.

> **Важливо:** Ефективний аналіз журналів потребує не лише технічних інструментів, а й кваліфікованого персоналу з глибоким розумінням систем та процесів.

3.4.4. Рекомендації щодо аналізу журналів

01

Розробка політик та процедур

Створіть чіткі політики та процедури для збору, зберігання та аналізу журналів з усіх критичних компонентів ICS/OT.

02

Автоматизація збору та аналізу

Використовуйте SIEM-системи та інші автоматизовані інструменти для агрегації, кореляції та аналізу журналів, щоб прискорити виявлення інцидентів.

03

Налаштування та оптимізація

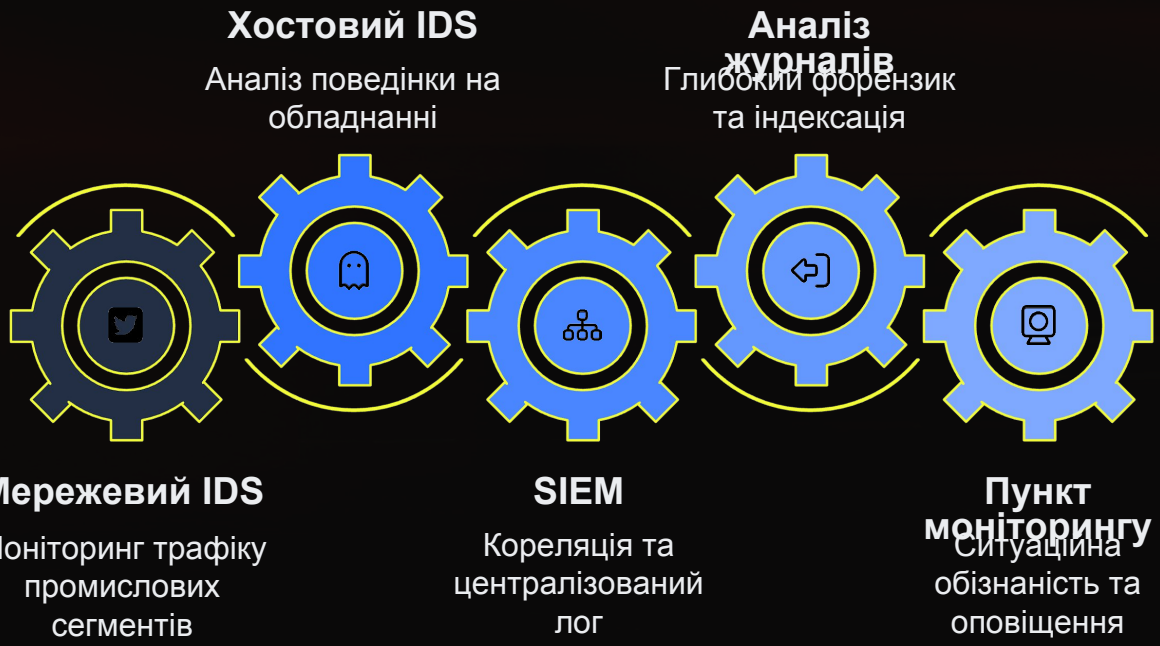
Регулярно переглядайте та оптимізуйте конфігурації систем моніторингу для зменшення хибних спрацювань та підвищення точності виявлення.

04

Командна співпраця

Забезпечте тісну співпгасю між IT- та OT-персоналом, а також експертами з кібербезпеки для комплексного розуміння даних моніторингу.

3.4.5. Інтеграція всіх компонентів виявлення



Ефективна система виявлення вторгнень та підтримки ситуаційної обізнаності в ICS/SCADA вимагає інтеграції всіх компонентів: від хостових та мережевих систем виявлення вторгнень до SIEM-систем та аналізу журналів. Тільки комплексний підхід може забезпечити належний рівень захисту критичної інфраструктури.

3.5. Висновки: Комплексний підхід до кібербезпеки ICS

Багаторівневий захист

Впровадження IDS, SIEM та систем моніторингу створює багаторівневу систему захисту, яка здатна виявляти та реагувати на різноманітні кіберзагрози в промислових мережах.

Постійна обізнаність

Ситуаційна обізнаність є основою для ефективного управління кібербезпекою, забезпечуючи розуміння поточного стану системи та дозволяючи приймати своєчасні рішення.

Людський фактор

Успіх системи виявлення вторгнень залежить не лише від технологій, а й від кваліфікованого персоналу, який розуміє специфіку промислових систем та вміє ефективно реагувати на загрози.

Кібербезпека ICS/SCADA - це не одноразове впровадження технологій, а постійний процес моніторингу, аналізу та вдосконалення, який вимагає інтеграції технічних рішень з організаційними заходами та навчанням персоналу.

Список використаних джерел

1. Radvanovsky, R., & Brodsky, J. (2016). Handbook of SCADA/Control Systems Security (2nd ed.). CRC Press.

2. Colbert, E. J. M., & Kott, A. (Eds.). (2016). Cyber-Security of SCADA and Other Industrial Control Systems. Springer.

3. Shaw, W. T. (2020). Cybersecurity for SCADA Systems (2nd ed.). PennWell Books.

4. Brooks, C. J., & Craig Jr., P. A. (2022). Practical Industrial Cybersecurity: ICS, Industry 4.0, and IIoT. Wiley.

5. Kouremetis, M. (2014). Defending a SCADA System with the Snort IDS [Presentation]. ECSSE Department.

6. National Telecom Regulatory Authority (NTRA). (2022). IoT Cyber Security Framework. EG-CERT.

7. Emerson. (2021). Industrial Security in SCADA Systems: IEC 62443-3-3 Certification. Emerson Automation Solutions.

8. Krotofil, M. (2023). Industrial Control Systems: Engineering Foundations and Cyber-Physical Attack Lifecycle. Technical White Paper.

9. UtilSec, LLC. (2024). Getting Started in ICS/OT Cyber Security: Lab Manual. UtilSec.

Дякую за увагу!