УДК 004.056.53

АНАЛІЗ СИСТЕМ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА КІБЕРАТАКИ ДЛЯ ОПТИМІЗАЦІЇ РОБОТИ SOC

Сірівчук А. С.
кандидат технічних наук,
доцент кафедри комп'ютерних технологій та інформаційної безпеки
Михайличенко А.В.,
студентка,
Національний університет кораблебудування імені адмірала Макарова,
Миколаїв, Україна

Анотація. Забезпечення інформаційної безпеки є важливою задачею будь-якої організації. SOC займаються забезпеченням виявленню та реакції інциденти в сфері кіберзахитсу. Для забезпечення даних функцій необхідно оптимізувати процес системи моніторингу та захисту інформації в комп'ютерній системі організації. В роботі приведено короткий опис та особливості SIEM, SOAR та XDR систем та їх роль в роботі SOC.

Ключові слова: SOC, кібербезпека, система виявлення інцидентів.

Вступ. В світі, де кожна організація стикається з постійно зростаючими кіберзагрозами та широким застосуванням зловмисного програмного забезпечення, особливу увагу слід звернути на критичну інфраструктуру країни. Розуміння та своєчасна реакція на ці кіберзагрози стають вирішальними факторами для забезпечення надійного захисту інформаційних систем.

У такому контексті, роль SOC набуває особливого значення у боротьбі з кіберзлочинцями та забезпеченні кібербезпеки організації. Спеціалісти SOC відповідають за виявлення, аналіз та реагування на кіберінциденти, забезпечуючи постійний моніторинг і захист інфраструктури протягом 24 годин на добу, 7 днів на тиждень.

Правильно налаштовані та оптимізовані процеси виявлення та реагування на кібератаки, а також постійний професійний ріст операторів дозволять знизити час реагування на кіберінциденти та мінімізувати їхній вплив на інформаційні системи організації. Крім того, це забезпечить стійкість та надійність функціонування центру та допоможе забезпечити безпеку інформаційних активів організації.

Метою роботи є аналіз сучасних систем виявлення інцидентів для забезпечення оптимізації роботи SOC.

Основна частина. SOC – це одна з команд ефективного реагування на інциденти комп'ютерної безпеки [1]. Задачі розподіляються між трьома лініями ТП, відповідно до цього:

– оператор першої лінії (SOC Analyst Tier 1) – відповідає за моніторинг та контроль, швидке реагування та інвентаризацію активів комплексу;

– інженер другої лінії (SOC Analyst Tier 2) – несе відповідальність за виконання регламентних робіт з експлуатації, вносить зміни у політики доступу, створює інструкції (playbooks) щодо реагування на події (offenses) для першої лінії ТП;

– провідний інженер другої лінії (SOC Engineer) – займається діагностикою та вирішенням інцидентів, наданням консультацій, автоматизацією експлуатаційних задач.

Першочергової інструкцією у комп'ютерній безпеці виступає NIST 800-61 [1,2] (рис. 1):

В задачі SIEM входить:

–автоматичний збір та нормалізація подій ІБ;

– кореляція та пріоритизація подій ІБ;

– аналітика:

– збагачення інцидентів та дослідження загроз;

– діагностика роботи;

– виявлення аномалій;
– візуалізація даних та звітність;
– інтеграція з суміжними системами (наприклад, SOAR);
– відповідність вимогам стандартів.

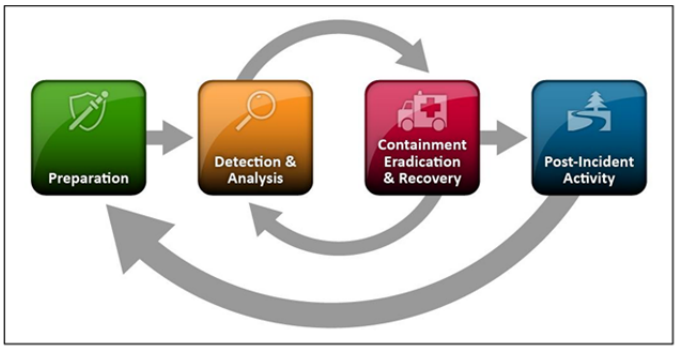

Рисунок 1. – Алгоритм обробки інцидентів згідно NIST 800-61

Оркестрація, автоматизація й реагування системи безпеки (SOAR) – це набір служб та інструментів, для автоматичного опрацювання завдань системи безпеки, що включають в себе виявлення та реагування на інциденти в в інформаційній безпеці. Оркестрація дає змогу підключатись до різних інструментів та інтеграцій, що забезпечує концентрацію інформації в одному розташуванні та можливість надання доступу до неї віддаленими шляхами, що забезпечує координацію в масштабних системах автоматизації.

Найчастіше SOAR та SIEM системи працюють спільно і дають змогу не тільки запобігати інцидентам, а й забезпечують можливість аналізу даних систем оператору кіберзахисту.

Особливості SOAR:

– додає до SIEM можливості оркестровки, автоматизації та реагування;
– не аналізує великі обсяги даних і не може самостійно захистити дані чи системи;
– потрібен досвід інтеграції, щоб переконатися, що рішення може правильно працювати з існуючою інфраструктурою безпеки організації.

Розширене виявлення та відповідь (XDR) - розроблена для забезпечення інтелектуальної, автоматизованої та інтегрованої системи безпеки. На відмінно від захисту кінцевих точок (EDR) XDR проводить аналіз також мережі, веб-трафіку та електронної пошти. На відмінно від систем SOAR та SIEM технологія XDR робить глибокий аналіз даних на всіх рівнях мережі, при цьому вона може доповнити дані для аналізу SIEM систем.

Особливостями XDR є:

– високі можливості аналізу та повна видимість IT-інфраструктури в єдиному централізованому рішенні;
– пріоритезує події безпеки;
– забезпечує швидке реагування на загрози, навіть на найприхованіші та складніші;
– використовуєтья для доповнення функцій SIEM і SOAR;
– для використання потрібні знання технологій безпеки, таких як безпека кінцевих точок, безпека мережі, безпека в хмарі тощо.

Вказані системи можуть працювати, як спільно так і в деякому відриві одна від одної. Вибір системи для захисту може обумовлюватися:

– вартістю системи захисту;
–потужністю обчислювальних машин на яких встановлена система безпеки;
автоматизація та швидкодія реакції на інцеденти;
– кваліфікація персоналу для налаштувань систем тощо.

Висновки: Розробка та оптимізація процесів виявлення та реагування на кібератаки в рамках SOC є важливим завданням. Використання інструментів, таких як SIEM, SOAR та XDR, допомагає спростити аналіз подій та дати можливість автоматичної реакції на інциденти.

Література

1. Computer Security Incident Handling Guide" by National Institute of Standards and Technology (NIST) [Електронний ресурс] – Режим доступу: https://nvlpubs.nist. gov /nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

2. "SOC Level 1: Junior Security Analyst Intro" by TryHackMe [Електронний ресурс] – Режим доступу: https://tryhackme.com/path/outline/soclevel1

ANALYSIS OF DETECTION AND RESPONSE SYSTEMS TO CYBER ATTACKS FOR OPTIMIZATION OF THE WORK OF THE SOC CENTER

Sirivchuk A.S., Ph. D., the associate Professor of the Department of Computer Technologies and Information Security

Mykhailychenko A.V., student

Admiral Makarov National Shipbuilding University, Mykolaiv, Ukraine

Abstract. Ensuring information security is an important task of any organization. SOC centers are engaged in providing detection and response to incidents in the field of cyber security. To ensure these functions, it is necessary to optimize the process of the monitoring and information protection system in the organization's computer system. The paper provides a brief description and features of SIEM, SOAR and XDR systems and their role in the work of the SOC center.

Keywords: SOC, cyber security, incident detection system.

УДК:004.4

МЕТОДИ ОЦІНКИ ТРУДОМІСТКОСТІ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ AGILE ПРОЄКТІВ

Ворона М.В.[1], Орєхов О. С.[2]

[1]PhD, викладач кафедри інформаційних управляючих систем та технологій, Національний університет кораблебудування імені адмірала Макарова,
м. Миколаїв, Україна,
mvl.vorona@gmail.com

[2]аспірант кафедри програмного забезпечення автоматизованих систем, Національний університет кораблебудування імені адмірала Макарова,
м. Миколаїв, Україна,
oleksandr.oriekhov@nuos.edu.ua

Анотація. Робота присвячена огляду методів оцінки трудомісткості розробки програмного забезпечення (ПЗ) для Agile проєктів. Обґрунтувано актуальність визначання трудомісткості розробки ПЗ на ранніх стадіях проєктування. Проведено аналіз існуючих методів оцінки трудомісткості розробки програмного забезпечення для Agile проєктів. Наведені основні сучасні тенденції розвитку оцінювання трудомісткості розробки ПЗ.

Ключові слова: оцінка трудомісткості, методологія розробки, програмне забезпечення, Agile, алгоритмічні методи, експертні судження.

Вступ.

Оцінка трудомісткості та вартості розробки ПЗ є однією із основних задач планування на ранніх етапах проєктів. Її вирішення дозволяє ІТ-компаніям коректно спланувати кількісні показники ресурсів, які необхідно виділити на розробку програмного проєкту, що в свою чергу допоможе враховувати ризики та дозволить підвищити ефективність процесу розробки. Вибір