1. Основні напрями підвищення безпеки систем та мереж на базі Windows

SIEM, SOAR, EDR, XDR

SIEM = Security Information and Event Management

Централізоване збирання та аналіз даних про події з різних джерел (сервери, мережні пристрої, програми тощо) для моніторингу, виявлення інцидентів (зокрема в реальному часі). Приклади: Splunk, IBM QRadar, LogRhythm, Exabeam, NetWitness, Microsoft Azure Sentinel та ін.

SOAR = Security Orchestration, Automation, and Response

Оркестрування, автоматизація, реагування на інциденти.

Приклади: IBM Security QRadar SOAR, Splunk SOAR, Swimlane, Cyberbit SOC 3D, CyberSponse та ін.

Гарна практика — поєднання SIEM і SOAR (видимість даних + автоматизація дій)

EDR = Endpoint Detection and Response

Захист кінцевих вузлів (зокрема робочих станцій, серверів, мобільних пристроїв). Виконує функції осучасненого антивірусного ПЗ. Працює на самих кінцевих пристроях (аналізує поведінку програм, виявляє загрози, реагує на них — ізоляція, видалення тощо). + Має можливість інтеграції в безпекову інфраструктуру (SIEM).

Приклади: SentinelOne, Microsoft Defender for Endpoint, Xcitium EDR, CrowdStrike Falcon та ін.

XDR = Extended Detection and Response

Просунутий варіант EDR (аналізує кінцеві вузли + мережний трафік, хмарні середовища, ...). Відрізняється від SIEM джерелами даних, основним фокусом уваги, підходом до виявлення загроз та реагуванням на них).

Приклади: ESET PROTECT Enterprise, Cynet Security, Microsoft Defender XDR, Cisco XDR та ін.

1. Основні напрями підвищення безпеки систем та мереж на базі Windows

SIEM vs XDR

Ключові відмінності	SIEM	XDR
Джерела даних	Журнали фаєрволів, серверів, застосунків, мережних пристроїв	Як у SIEM + кінцеві вузли, мережний трафік, хмарні середовища, хмарні застосунки, поведінка користувача
Фокус уваги	Мережа і сервери	Кінцеві вузли (не лише сервери), мережа
Підхід до виявлення загроз	Виявлення спирається *передусім* на правила та аналіз підписів (відомі патерни)	Виявлення спирається *передусім* на просунутіші аналітичні методи, машинне навчання (відомі та невідомі патерни)
Реакція на загрози	Попередження (alerts), звіти + елементи автоматизації	Попередження, звіти + автоматизація (напр., ізоляція скомпрометованих вузлів, блокування підозрілого трафіку)

Але: не забуваймо про взаємопроникнення технологій (з таблиці це теж видно).

1. Основні напрями підвищення безпеки систем та мереж на базі Windows

Корисні посилання

- Що таке SIEM і які функції виконує. Погляд Logsign. URL: https://logsign.bakotech.com/ua/what-does-a-siem-solution-do
- The Essential Guide to SIEM. Exabeam. URL: https://www.exclusive-networks.com/ie/wp-content/uploads/sites/19/2021/07/The-Essential-Guide-to-SIEM.pdf
- What is SIEM. IBM. URL: https://www.ibm.com/think/topics/siem
- Best SIEM Solutions. Top 10 SIEM systems and How to Choose. Exabeam. URL: https://www.exabeam.com/explainers/siem-tools/siem-solutions/