**Lucrare de laborator 4**

# Tema: Microsoft Sentinel (1)

**Scopul lucrării**: studierea serviciului cloud Microsoft (Azure) Sentinel ce oferă un suport pentru analiza amenințărilor și monitorizarea securității într-o întreprindere.

1. **Microsoft (Azure) Sentinel**

Microsoft Sentinel, oferă o soluție unică pentru detectarea proactivă a atacurilor, amenințărilor și luarea deciziilor de răspuns la amenințări.

Se recomandă să accesați următorul link:

[Browse all - Training | Microsoft Learn](https://learn.microsoft.com/en-us/training/browse/?terms=sentinel)

Accesați - learn.microsoft.com , unde sunt setate filtre -Sentinel, Subjects-security, Levels -Beginner

Sunt disponibile 10 module.

Creați-vă un cont pentru studiere.

Studiați următoarele 3 module:

1. [Introduction to Microsoft Sentinel](https://learn.microsoft.com/en-us/training/modules/intro-to-azure-sentinel/)
2. [Describe security capabilities of Microsoft Sentinel](https://learn.microsoft.com/en-us/training/modules/describe-security-capabilities-of-azure-sentinel/)
3. [Query, visualize, and monitor data in Microsoft Sentinel](https://learn.microsoft.com/en-us/training/modules/query-data-sentinel/)
4. **Microsoft (Azure) Sentinel. Serviciile**

Microsoft Sentinel este un serviciu scalabil, de tip cloud, care oferă:

* Managementul evenimentelor și informațiilor de securitate (SIEM- Security information and event management)
* Orchestrare, automatizare și răspuns la incidentele de securitate (SOAR- Security orchestration, automation, and response)

Managementul evenimentelor și informațiilor de Securitate (SIEM), este o soluție care ajută organizațiile să detecteze, să analizeze și să răspundă la amenințările de securitate înainte ca acestea să le perturbeze activitatea.

SIEM, combină atât gestionarea informațiilor de securitate (SIM), cât și gestionarea evenimentelor de securitate (SEM) într-un singur sistem de gestionare a securității. Tehnologia SIEM colectează date din jurnalul de evenimente dintr-o serie de surse, identifică activitatea care se abate de la normă cu ajutorul analizei în timp real și ia măsurilecorespunzătoare.

Succint, Microsoft Sentinel (figura1), oferă organizațiilor vizibilitate asupra activității din rețea, astfel încât să poată răspunde rapid la potențiale atacuri cibernetice și să îndeplinească cerințele de conformitate.

SOAR sunt concepute pentru orchestrarea sistemelor de securitate, adică coordonarea și controlul acestora. În special, vă permit să colectați date despre evenimentele de securitate din diverse surse, să le procesați și să automatizați scenarii tipice pentru a răspunde la incidentele de securitate.

SOAR integrează evenimentele de securitate într-un singur sistem, eliminând gestionarea fiecăruia dintre ele separat și ajută la analiza incidentelor complexe.

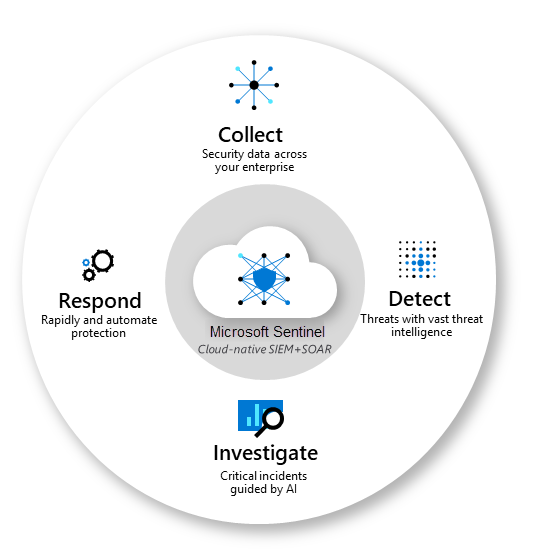


Figura 1- Serviciile Microsoft Sentinel

1. **Conținutul raportului**

# Raportul va conține descrierea succintă a sarcinilor studiate, concluzii. Perfectați și prezentați profesorului raportul și primiți întrebări sau sarcină pentru susținere.