Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

Lucrarea de laborator nr. 4

*Metode și mijloace tehnice de protecție a informației.*

A efectuat: st. gr. SI-211 Chihai Adrian

A verificat: dr. conf.univ. Colesnic Victor

Chișinău – 2024

**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.

Microsoft (Azure) Sentinel este o soluție de gestionare a securității și a evenimentelor de tip SIEM (Security Information and Event Management) bazată pe cloud, oferită de Microsoft în cadrul platformei Azure. Acesta ajută organizațiile să detecteze, să prevină și să răspundă la amenințările de securitate prin colectarea și analizarea datelor din întreaga infrastructură IT, atât on-premise cât și în cloud.

Azure Sentinel permite monitorizarea și analiza în timp real a jurnalelor de securitate, utilizând algoritmi avansați de inteligență artificială și machine learning pentru a detecta activități anormale și atacuri cibernetice. În plus, oferă o platformă centralizată pentru investigarea și remedierea incidentelor de securitate, precum și capacitatea de automatizare a răspunsului la amenințări prin intermediul fluxurilor de lucru automatizate (playbooks).

Prin utilizarea Azure Sentinel, organizațiile pot reduce volumul de alerte false, îmbunătăți vizibilitatea asupra potențialelor riscuri și spori capacitatea de răspuns la incidente de securitate.

**Introduction to Microsoft Sentinel**

Acest modul oferă o introducere generală în **Microsoft Sentinel**, explicând cum funcționează și cum poate fi utilizat pentru a îmbunătăți securitatea unei organizații. Modulele cheie abordate includ:

* **Ce este Microsoft Sentinel?**: O soluție SIEM (Security Information and Event Management) și SOAR (Security Orchestration, Automation, and Response) bazată pe cloud, care colectează date din multiple surse pentru a detecta amenințările și a oferi soluții rapide de răspuns.
* **Beneficiile Azure Sentinel**: Modularitatea, scalabilitatea și integrarea cu diverse surse de date, precum și cu alte servicii Azure, îl fac un instrument versatil pentru managementul securității.
* **Flux de lucru**: Prezintă cum Microsoft Sentinel poate colecta și centraliza loguri din diverse surse, cum ar fi infrastructura on-premise, aplicațiile cloud și soluțiile de securitate third-party, pentru a oferi o vedere unificată a stării de securitate.

Acest modul ajută utilizatorii să înțeleagă cum Sentinel le poate îmbunătăți securitatea și cum se poate implementa ușor în infrastructura existentă.

**Describe security capabilities of Microsoft Sentinel**

Acest modul se concentrează pe capacitățile de securitate oferite de **Microsoft Sentinel**. Printre punctele abordate se numără:

* **Colectarea și analiza datelor**: Sentinel poate colecta date de securitate dintr-o gamă largă de surse, precum firewall-uri, servere, dispozitive IoT, aplicații cloud și soluții de securitate externe, integrându-le într-un singur flux.
* **Detectarea amenințărilor**: Cu ajutorul inteligenței artificiale și algoritmilor de machine learning, Sentinel poate detecta comportamente anormale, incidente și atacuri cibernetice care altfel ar fi greu de observat. De asemenea, Sentinel utilizează playbooks pentru a automatiza acțiunile de răspuns.
* **Răspuns și investigare**: Sentinel nu doar detectează amenințările, ci oferă și unelte pentru investigarea incidentelor de securitate. Integrarea cu instrumente SOAR permite automatizarea acțiunilor de răspuns, reducând timpul necesar pentru remedierea problemelor.
* **Capacități de prevenție**: Prin integrarea cu Microsoft Defender și alte soluții de securitate, Sentinel poate oferi prevenție și măsuri proactive împotriva atacurilor cibernetice prin identificarea punctelor slabe din infrastructura organizației.

Acest modul ajută utilizatorii să înțeleagă cum Sentinel își folosește capabilitățile avansate pentru a îmbunătăți securitatea și a automatiza gestionarea amenințărilor.

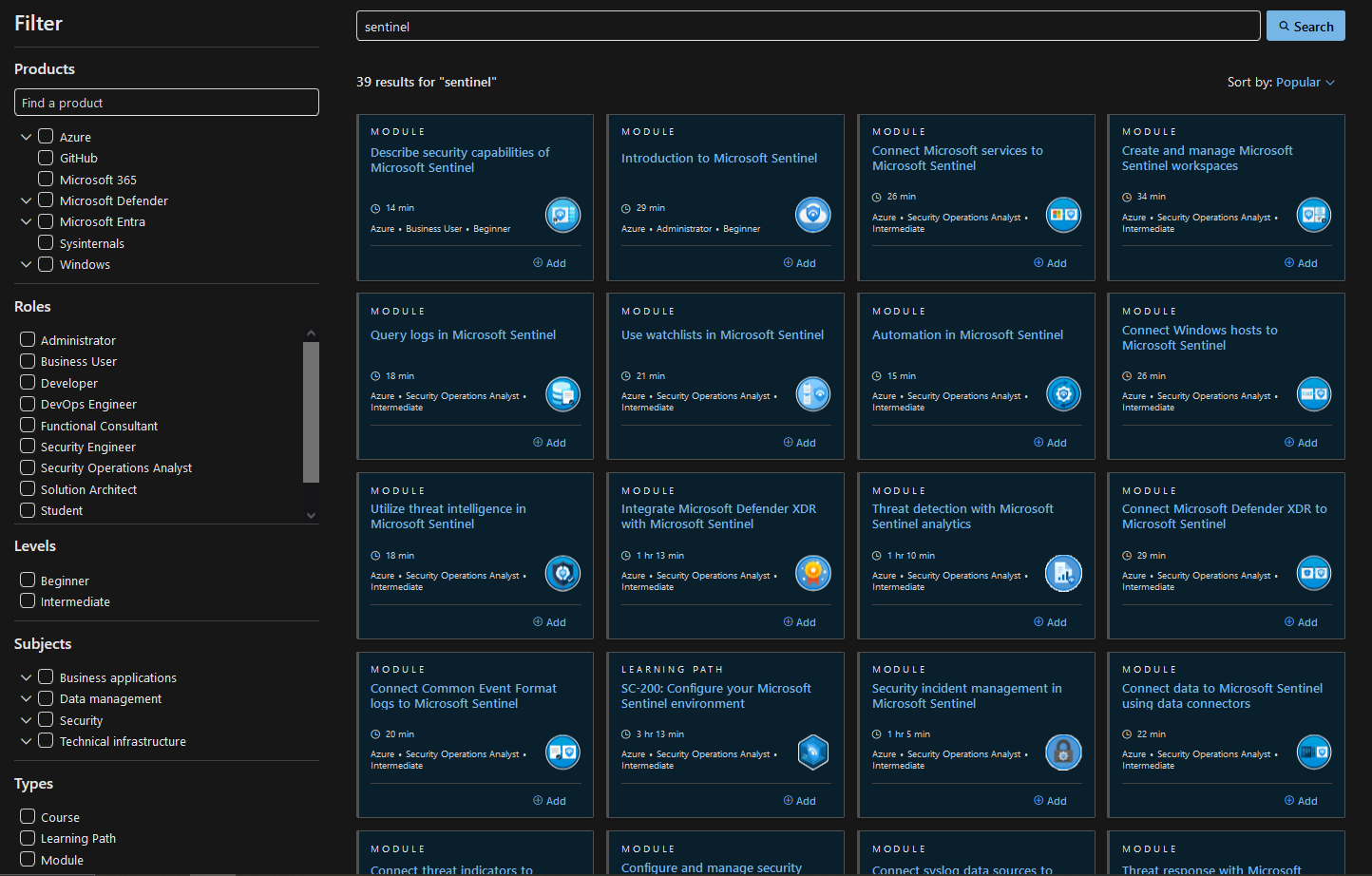


Figura 1.1 – Modulele Microsoft Sentinel

**Query, visualize, and monitor data in Microsoft Sentinel**

Acest modul se axează pe modul în care utilizatorii pot interoga, vizualiza și monitoriza datele colectate în **Microsoft Sentinel**. Printre conceptele cheie abordate sunt:

* **Interogarea datelor**: Utilizând **KQL (Kusto Query Language)**, utilizatorii pot crea interogări complexe pentru a extrage date relevante din jurnalul de securitate și din alte surse de date. KQL este un limbaj de interogare puternic, similar cu SQL, dar optimizat pentru analiza jurnalelor.
* **Vizualizarea datelor**: Microsoft Sentinel oferă tablouri de bord și vizualizări personalizabile pentru a prezenta datele într-un mod ușor de înțeles. Graficele, diagramele și alte forme de reprezentare vizuală permit o analiză rapidă a datelor și identificarea tendințelor sau anomaliilor.
* **Monitorizarea și crearea de alerte**: Sentinel permite configurarea de alerte personalizate, care notifică echipa de securitate când sunt detectate activități suspecte sau potențiale atacuri. Utilizatorii pot seta politici și reguli de alertare pe baza datelor monitorizate în timp real.
* **Workbook-uri și Dashboards**: Acestea oferă o interfață vizuală pentru analiza datelor și monitorizarea în timp real a amenințărilor, permițând echipelor de securitate să aibă o vedere clară asupra stării generale de securitate a organizației.

Изображение выглядит как текст, снимок экрана, графический дизайн, дизайн

Автоматически созданное описание

Figura 1.2 – Introduction to Microsoft Sentinel

Modulul **Introduction to Microsoft Sentinel** oferă o privire generală asupra soluției de securitate bazate pe cloud, **Microsoft Sentinel**, și explică cum aceasta poate ajuta organizațiile să își protejeze infrastructura IT. Acest modul este destinat să familiarizeze utilizatorii cu conceptele de bază și funcționalitățile platformei, fiind un punct de plecare pentru a înțelege capacitățile și beneficiile Sentinel în gestionarea securității cibernetice.

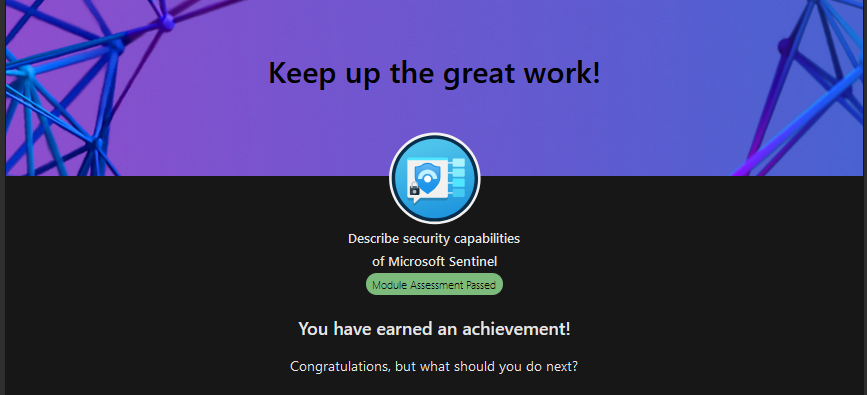


Figura 1.3 – Describe security capabilities of Microsoft Sentinel

Modulul **Describe Security Capabilities of Microsoft Sentinel** se concentrează pe funcționalitățile de securitate pe care le oferă Microsoft Sentinel. Acesta explică modul în care Sentinel colectează și analizează date din diverse surse pentru a detecta amenințări cibernetice, utilizând algoritmi de inteligență artificială și machine learning. De asemenea, modulul acoperă capacitățile Sentinel de a automatiza răspunsul la incidente, de a investiga amenințările și de a preveni atacurile prin integrarea cu alte soluții de securitate, cum ar fi Microsoft Defender.

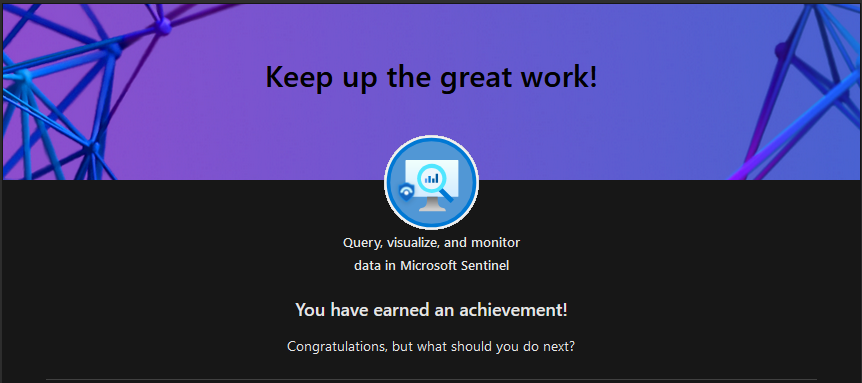


Figura 1.4 - Query and visualize data with Microsoft Sentinel

Modulul **"Query and visualize data with Microsoft Sentinel"** este despre utilizarea instrumentelor și tehnologiilor oferite de Microsoft Sentinel pentru a interoga și vizualiza datele colectate din sursele de securitate, în scopul analizei și monitorizării evenimentelor și incidentelor de securitate.

**Concluzie:** Microsoft Sentinel se dovedește a fi o soluție esențială pentru gestionarea securității și a evenimentelor într-o organizație modernă. Această platformă bazată pe cloud permite organizațiilor să detecteze, să prevină și să răspundă rapid la amenințările de securitate prin utilizarea unor tehnologii avansate de inteligență artificială și machine learning. Interogarea și vizualizarea datelor, facilitate de Kusto Query Language (KQL), oferă utilizatorilor instrumentele necesare pentru a extrage și analiza informații relevante din diverse surse. Tablourile de bord personalizabile și graficele contribuie la identificarea rapidă a tendințelor și anomaliilor, îmbunătățind astfel eficiența echipelor de securitate.

Un alt aspect important este capacitatea de automatizare a răspunsului la incidente, care permite organizațiilor să reacționeze prompt la amenințări, reducând astfel timpul necesar pentru remedierea problemelor. Flexibilitatea și scalabilitatea Microsoft Sentinel fac din această soluție un instrument adaptabil la nevoile organizațiilor, contribuind la îmbunătățirea generală a securității cibernetice. În concluzie, Microsoft Sentinel nu doar că îmbunătățește capacitatea de detecție și răspuns, dar și permite o gestionare mai eficientă a securității într-un peisaj IT tot mai complex și provocator.