Ministerul Educației, Culturii și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

**RAPORT**

Lucrarea de laborator nr.5

*Metode și mijloace tehnice de protecție a informației*

A efectuat:

st. gr. SI-211 Chirița Stanislav

A verificat:

asist., univ. Colesnic Victor

Chisinau 2024

**LUCRAREA DE LABORATOR NR.5**

**Tema:** **Microsoft Sentinel (2)**

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

Microsoft Sentinel reprezintă o soluție avansată și integrată pentru gestionarea securității informatice, dezvoltată de Microsoft pentru a facilita monitorizarea, detectarea și reacția rapidă la amenințările cibernetice. Aceasta folosește inteligența artificială și automatizarea pentru a identifica și contracara atacuri complexe, oferind organizațiilor instrumente puternice pentru a proteja datele și infrastructurile lor IT.

O componentă esențială în ecosistemul Microsoft Sentinel este modulul de gestionare a incidentelor de securitate, cunoscut sub numele de *Security Incident Management*. Acest modul permite echipelor de securitate să investigheze incidentele, să analizeze cauzele și să răspundă eficient la amenințări, permițând o intervenție rapidă și bine fundamentată. Astfel, Microsoft Sentinel devine un instrument esențial în cadrul strategiilor de apărare cibernetică, asigurând o protecție proactivă și reacții adecvate în fața amenințărilor cibernetice emergente.

Modulul *Security Incident Management* sprijină, în mod specific, urmărirea completă a ciclului de viață al unui incident de securitate, de la detectare și analiză, până la remediere și învățare post-incident. Această funcționalitate contribuie la îmbunătățirea continuă a sistemului de apărare și a capacităților organizaționale de a răspunde la amenințări, făcând Microsoft Sentinel o soluție robustă și indispensabilă pentru organizațiile care doresc o securitate cibernetică de ultimă generație.

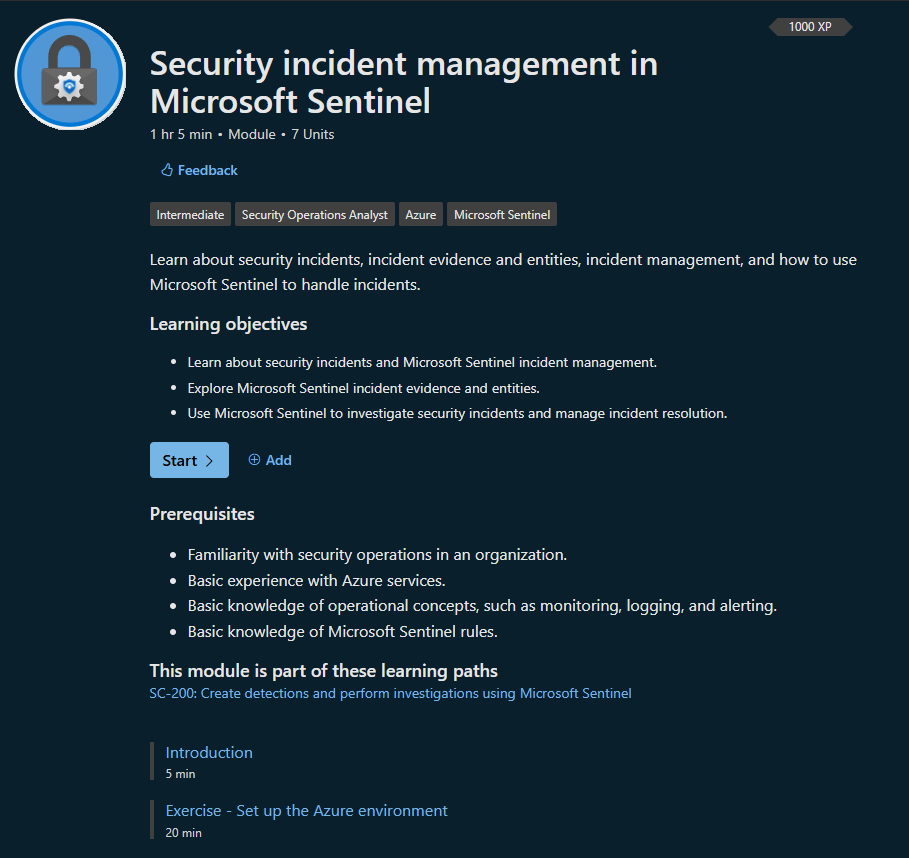
Se recomandă de accesat următorul link pentru studiere:

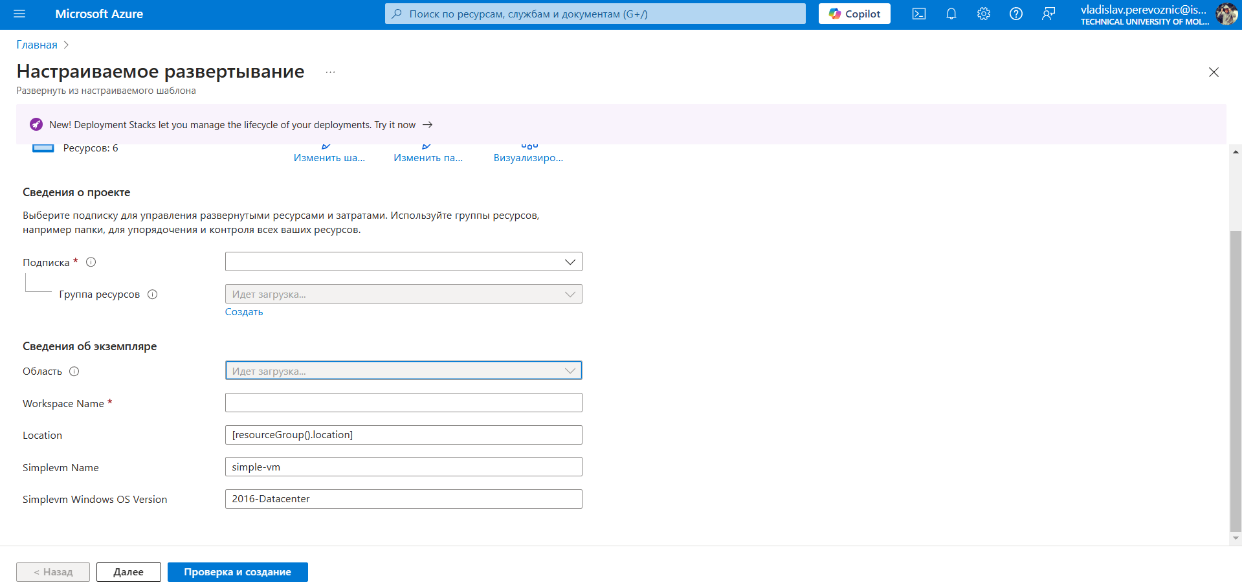
[Browse all - Training | Microsoft Learn](https://learn.microsoft.com/en-us/training/browse/?terms=sentinel)

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

Studiați modulul:

[**Security incident management in Microsoft Sentinel**](https://learn.microsoft.com/en-us/training/modules/incident-management-sentinel/)

  
 **Figura 1 – Security incident management in Microsoft Sentinel**

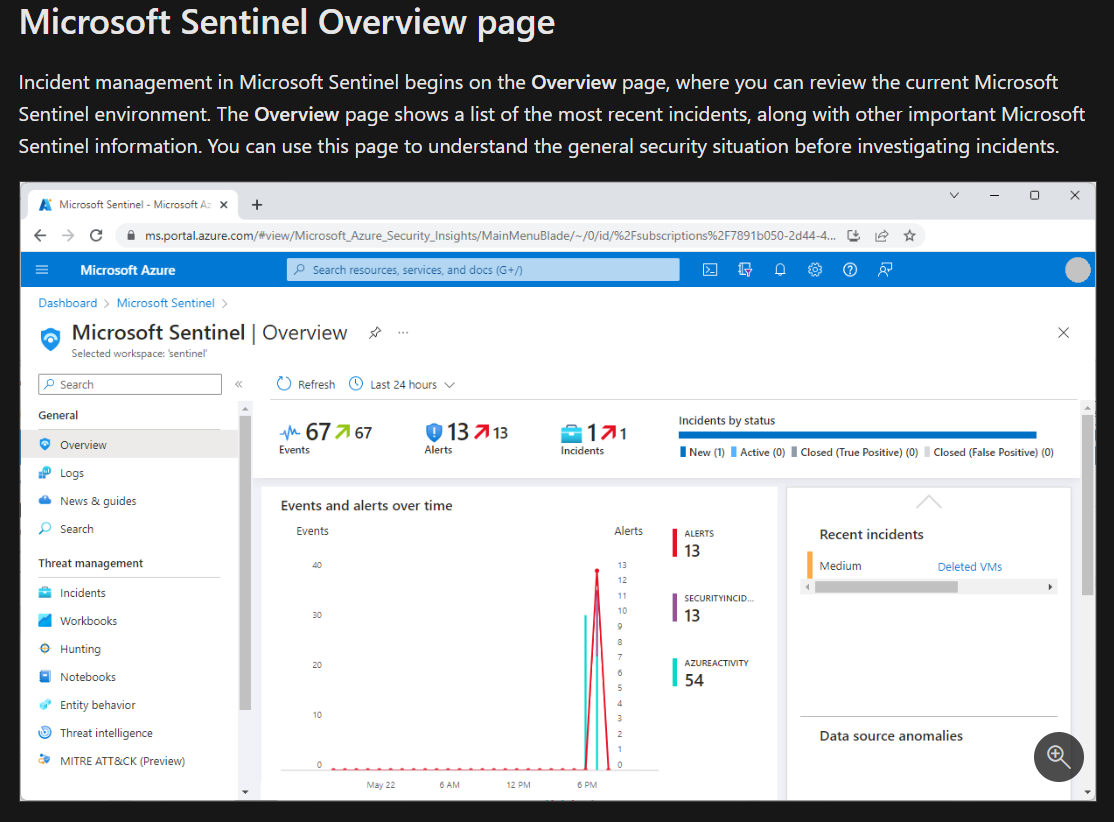
  
**Figura 2 - Secțiunea de configurare *Custom Deployment* (Implementare personalizată)**

Implementarea șablonul Azure Resource Manager  
Completare câmpurilor pentru a implementa o mașină virtuală simplă pe platforma Azure:

1. **Подписка (Subscription)**:
   * **Exemplu**: „Visual Studio Enterprise Subscription”
   * **Explicație**: Alegeți un abonament activ pe care îl aveți în Azure, în funcție de contul dvs. În acest caz, „Visual Studio Enterprise Subscription” este un abonament frecvent întâlnit la dezvoltatorii care utilizează Azure pentru proiecte de testare și dezvoltare.
2. **Группа ресурсов (Resource Group)**:
   * **Exemplu**: „MyResourceGroupVM”
   * **Explicație**: Dacă nu aveți deja o grupă de resurse, creați una nouă cu numele „MyResourceGroupVM”. Acesta va fi grupul unde vor fi stocate și gestionate toate resursele asociate mașinii virtuale și workspace-ului.
3. **Область (Region)**:
   * **Exemplu**: „West Europe”
   * **Explicație**: Alegeți o regiune apropiată sau cea recomandată pentru cerințele dvs. „West Europe” este adesea utilizată pentru implementări în Europa, având centre de date în Amsterdam și alte locații din vestul Europei.
4. **Workspace Name**:
   * **Exemplu**: „MyLogWorkspace”
   * **Explicație**: Introduceți un nume unic pentru workspace-ul Azure Monitor Logs, care va stoca toate datele de monitorizare și jurnalele generate de mașina virtuală. De exemplu, „MyLogWorkspace”.
5. **Location**:
   * **Exemplu**: [resourceGroup().location]
   * **Explicație**: Acest câmp este precompletat automat și va folosi locația grupului de resurse selectat anterior, în acest caz „West Europe”. Nu trebuie să faceți modificări aici.
6. **SimpleVM Name**:
   * **Exemplu**: „SimpleVM-Test”
   * **Explicație**: Alegeți un nume pentru mașina virtuală. În exemplul nostru, „SimpleVM-Test” este un nume potrivit pentru un VM utilizat în scopuri de testare.
7. **SimpleVM Windows OS Version**:
   * **Exemplu**: „Windows Server 2019 Datacenter”
   * **Explicație**: Alegeți versiunea sistemului de operare Windows. În loc de 2016, puteți opta pentru „Windows Server 2019 Datacenter” pentru o versiune mai nouă și mai performantă.

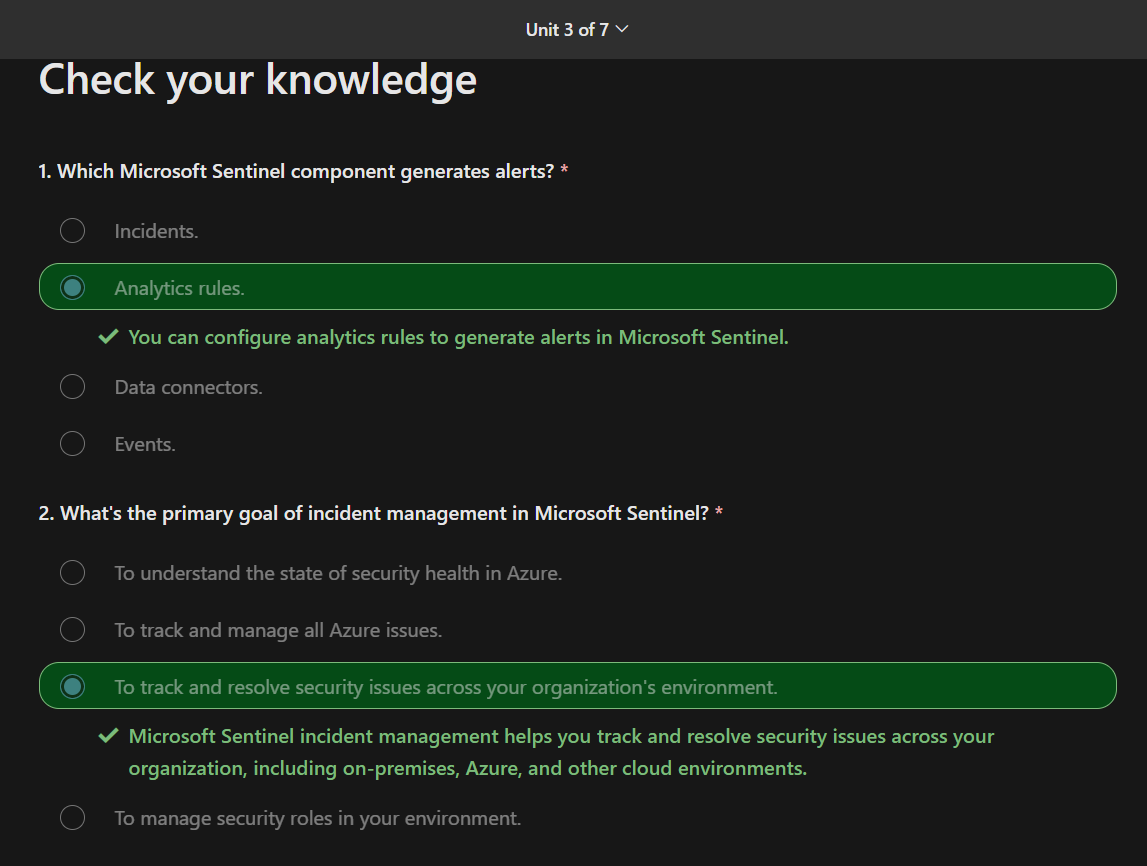
După completarea acestor câmpuri:

* Accesarea „Проверка и создание” (Verificare și creare) pentru a trece printr-o verificare a setărilor și începerea implementării mașinii virtuale.

  
**Figura 3 - Microsoft Sentinel Overview page**

Amenințările legate de tehnologie la adresa unei organizații se numesc incidente. Managementul incidentelor este procesul complet de investigare a incidentelor, de la crearea incidentelor până la investigarea și rezolvarea aprofundată. Microsoft Sentinel poate ajuta echipa IT să organizeze, să investigheze și să urmărească incidentele de la creare până la rezolvare.

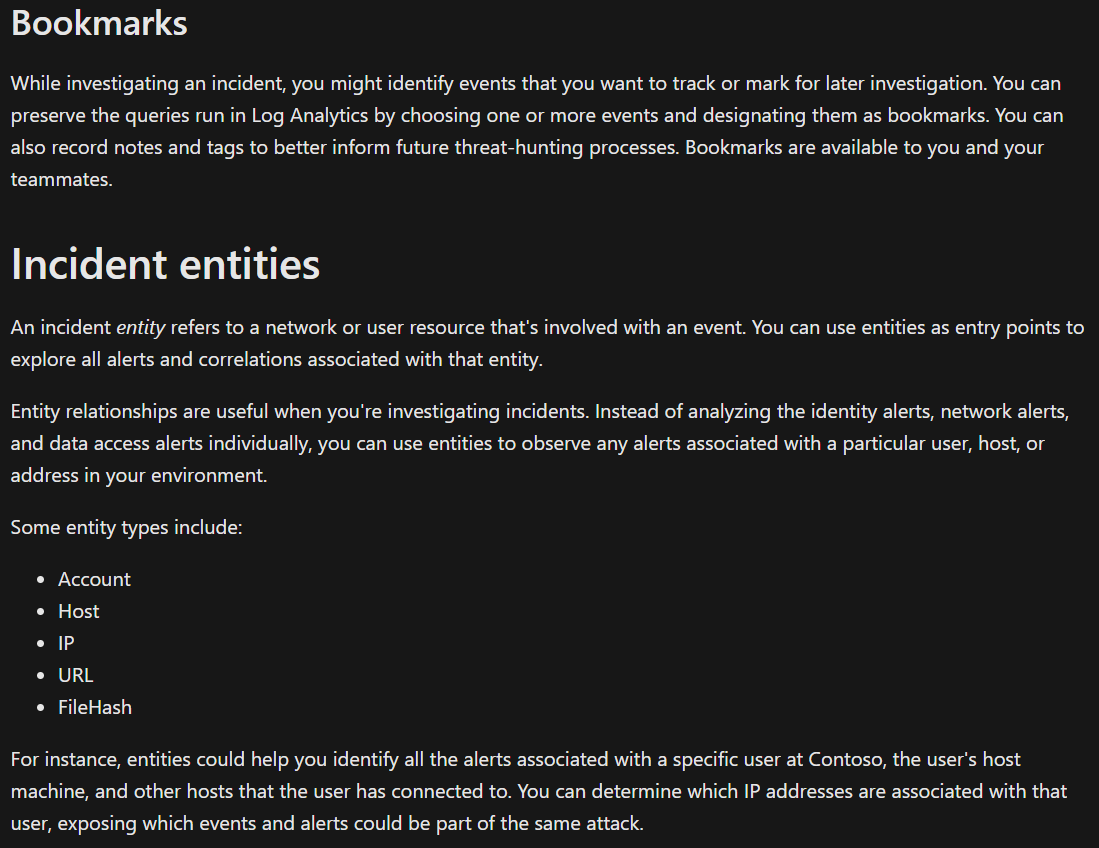
Utilizarea Microsoft Sentinel pentru a revizui informații detaliate despre incident, a atribui un proprietar de incident, a seta și a menține severitatea incidentului și pentru a gestiona starea incidentului. Microsoft Sentinel oferă un mediu complet de gestionare a incidentelor pentru a gestiona acești pași.

  
**Figura 4 – Verificarea cunoștințelor**

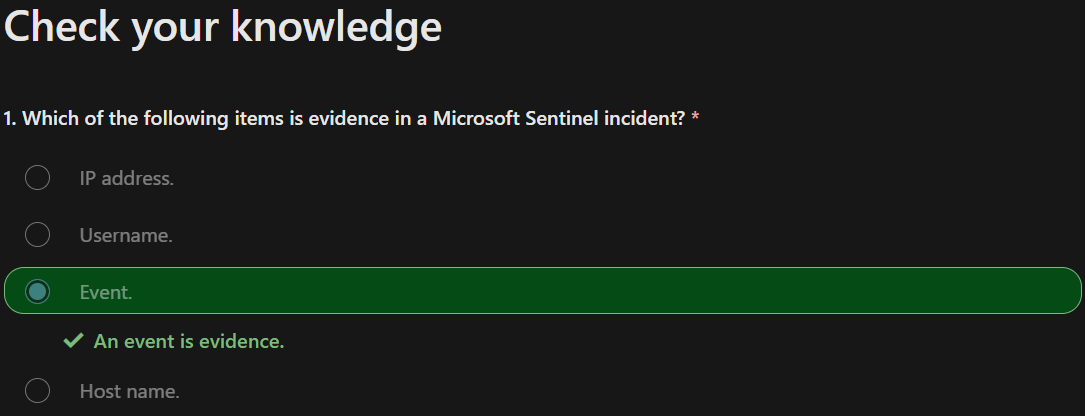
Majoritatea incidentelor sunt generate din cauza unei alerte de reguli de analiză. Exemple de alerte includ:

* Detectarea fișierelor suspecte.
* Detectarea activităților suspecte ale utilizatorilor.
* Tentativa de ridicare a privilegiului.

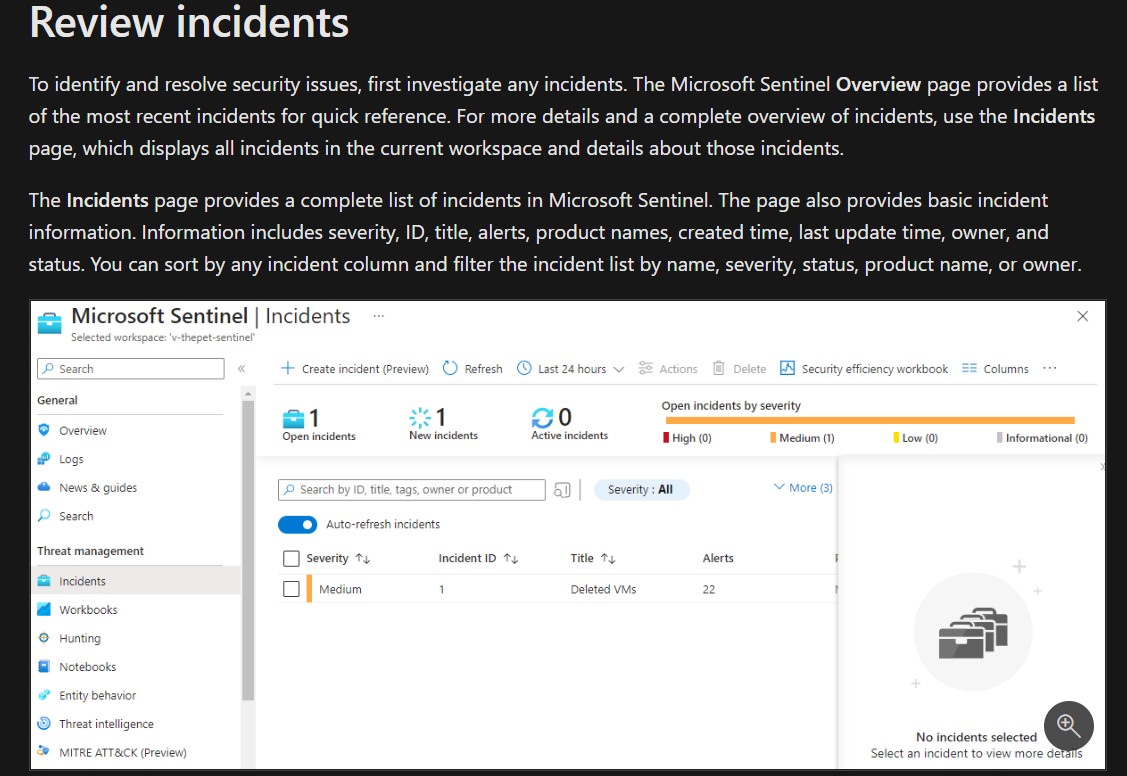
Regulile de analiză generează alerte bazate fie pe interogări Kusto Query Language (KQL), fie pe conexiunea directă la soluții de securitate Microsoft, cum ar fi Microsoft Defender pentru Cloud sau Microsoft Defender XDR. Dacă activați gruparea alertelor, Microsoft Sentinel include orice dovadă de alertă asociată incidentului.

  
**Figura 5 – Entităție incidente**

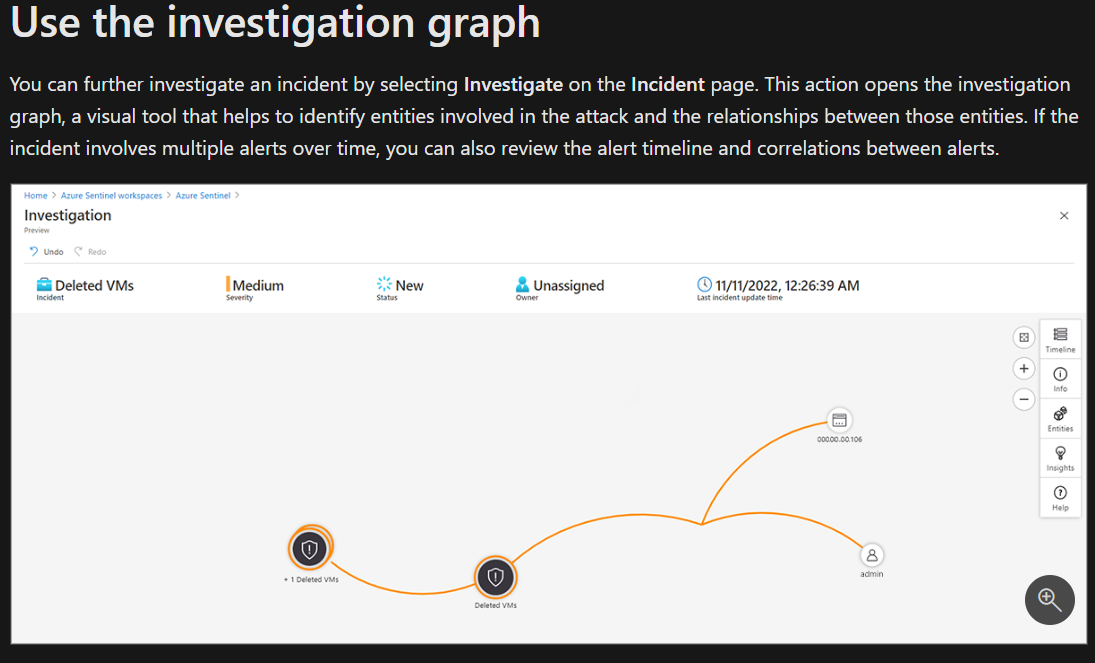
O entitate incidentă se referă la o rețea sau o resursă de utilizator care este implicată într-un eveniment. Puteți utiliza entitățile ca puncte de intrare pentru a explora toate alertele și corelațiile asociate cu acea entitate.

  
**Figura 6 – Verificarea cunoștințelor**

În Microsoft Sentinel, un eveniment este considerat o dovadă într-un incident. Un incident în Sentinel este o colecție de alerte și evenimente conexe care reprezintă o potențială amenințare sau încălcare a securității.

  
**Figura 7 – Review incidents**

Pagina Incidente oferă o listă completă de incidente în Microsoft Sentinel. Pagina oferă, de asemenea, informații de bază despre incident. Informațiile includ gravitatea, ID-ul, titlul, alertele, numele produselor, ora creată, ora ultimei actualizări, proprietarul și starea.

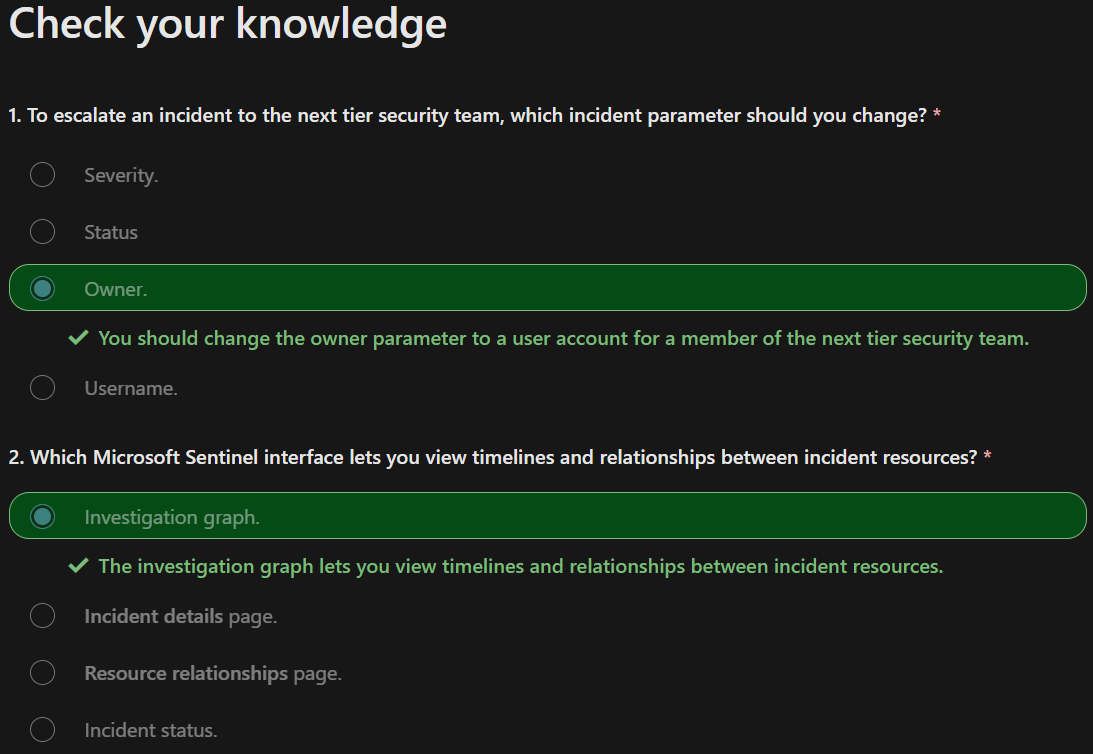
  
**Figura 8 – Investigation graph**

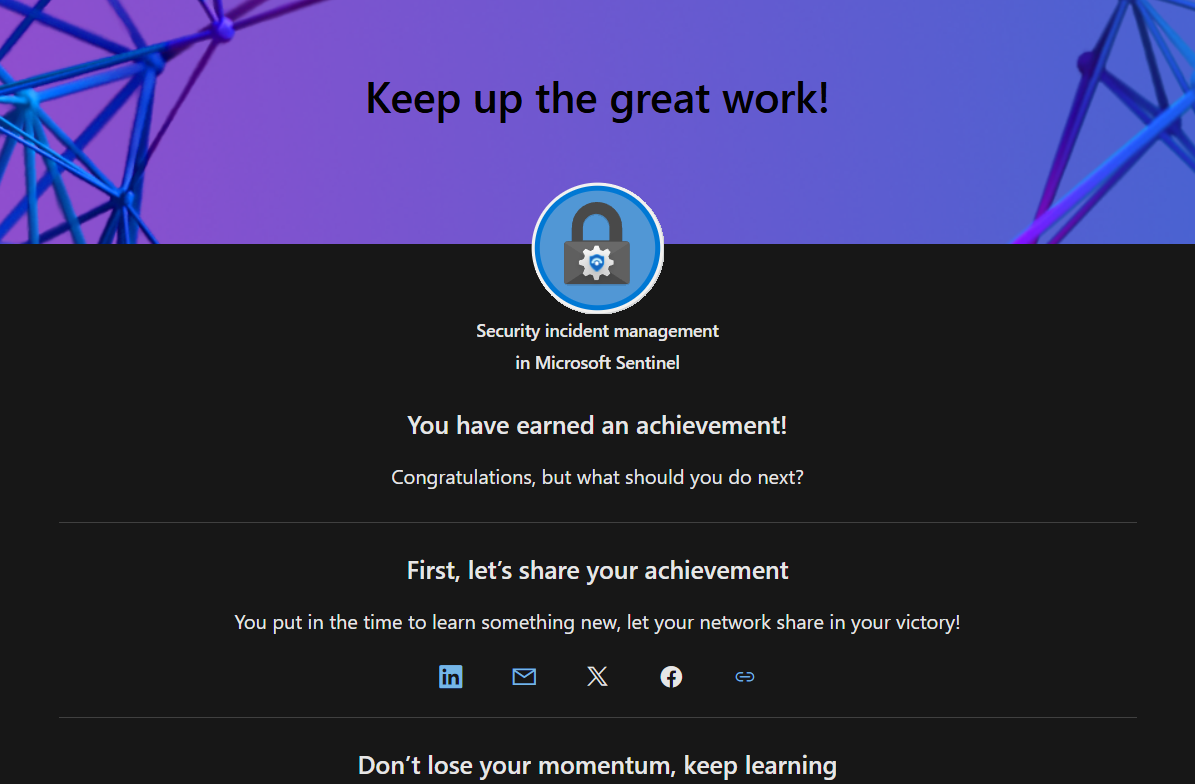
**Graficul:**

1. **Entitățile implicate**:
   * **Deleted VMs**: Reprezintă una sau mai multe mașini virtuale care au fost șterse și care au fost identificate ca făcând parte din incident. Acest lucru sugerează că acțiuni de tip „Delete” au fost efectuate asupra acestor resurse.
   * **IP Address** (0000.00.106): O adresă IP este prezentă și este conectată la activitățile suspecte. Adresele IP sunt frecvent asociate cu punctele de acces sau cu sursele traficului, ceea ce poate indica un atacator sau o sursă de atac.
   * **Username (admin)**: Apare un utilizator (admin) care are legătură cu activitățile neautorizate asupra resurselor afectate, ceea ce sugerează o posibilă compromitere a contului.
2. **Legături între entități**:
   * Liniile care leagă entitățile arată relațiile dintre ele. De exemplu, o linie între o mașină virtuală ștersă și un cont de utilizator admin poate indica faptul că acest utilizator a efectuat acțiunea de ștergere sau că este asociat cu activitatea care a dus la incident.
3. **Detalii despre incident**:

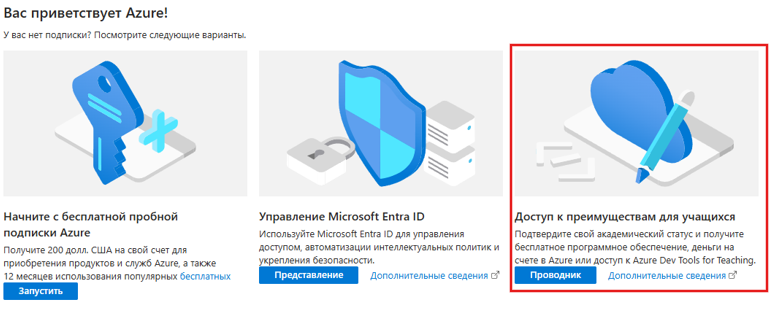
În partea de sus, sunt detalii despre incident:

* + - **Severity (Medium)**: Nivelul de gravitate al incidentului este „Medium”, indicând o amenințare cu impact moderat.
    - **Status (New)**: Incidentul este în stare „New”, ceea ce sugerează că nu a fost încă investigat sau remediat.
    - **Owner (Unassigned)**: Incidentul nu a fost atribuit unui responsabil, ceea ce înseamnă că este încă în așteptarea analizei.

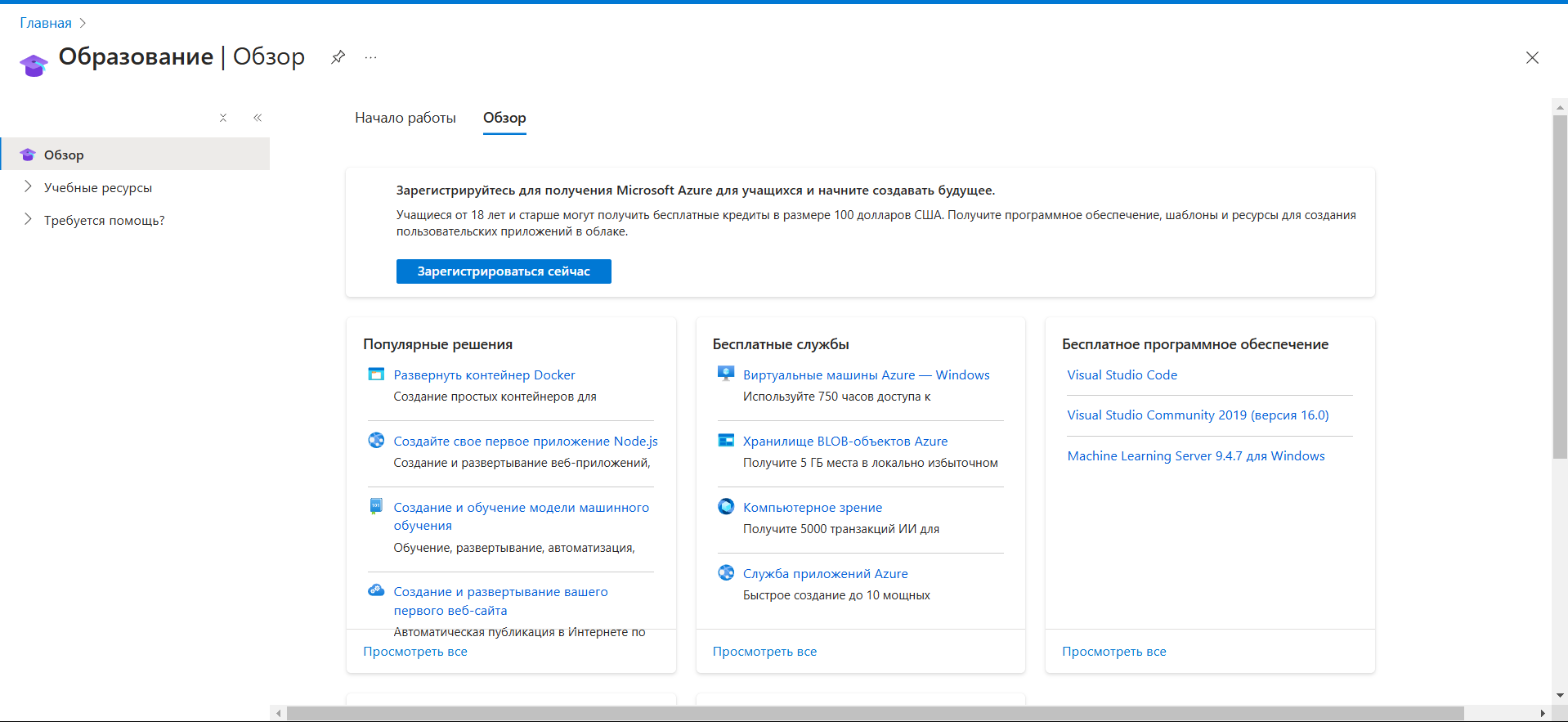


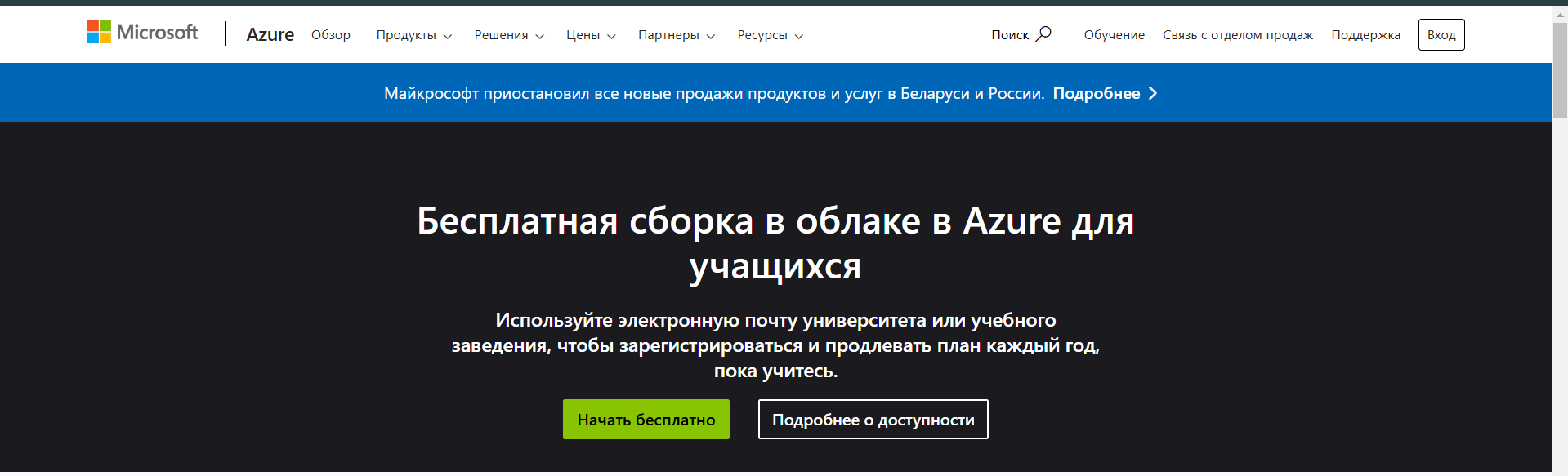
  
**Figura 10 – Realizarea cu succes**

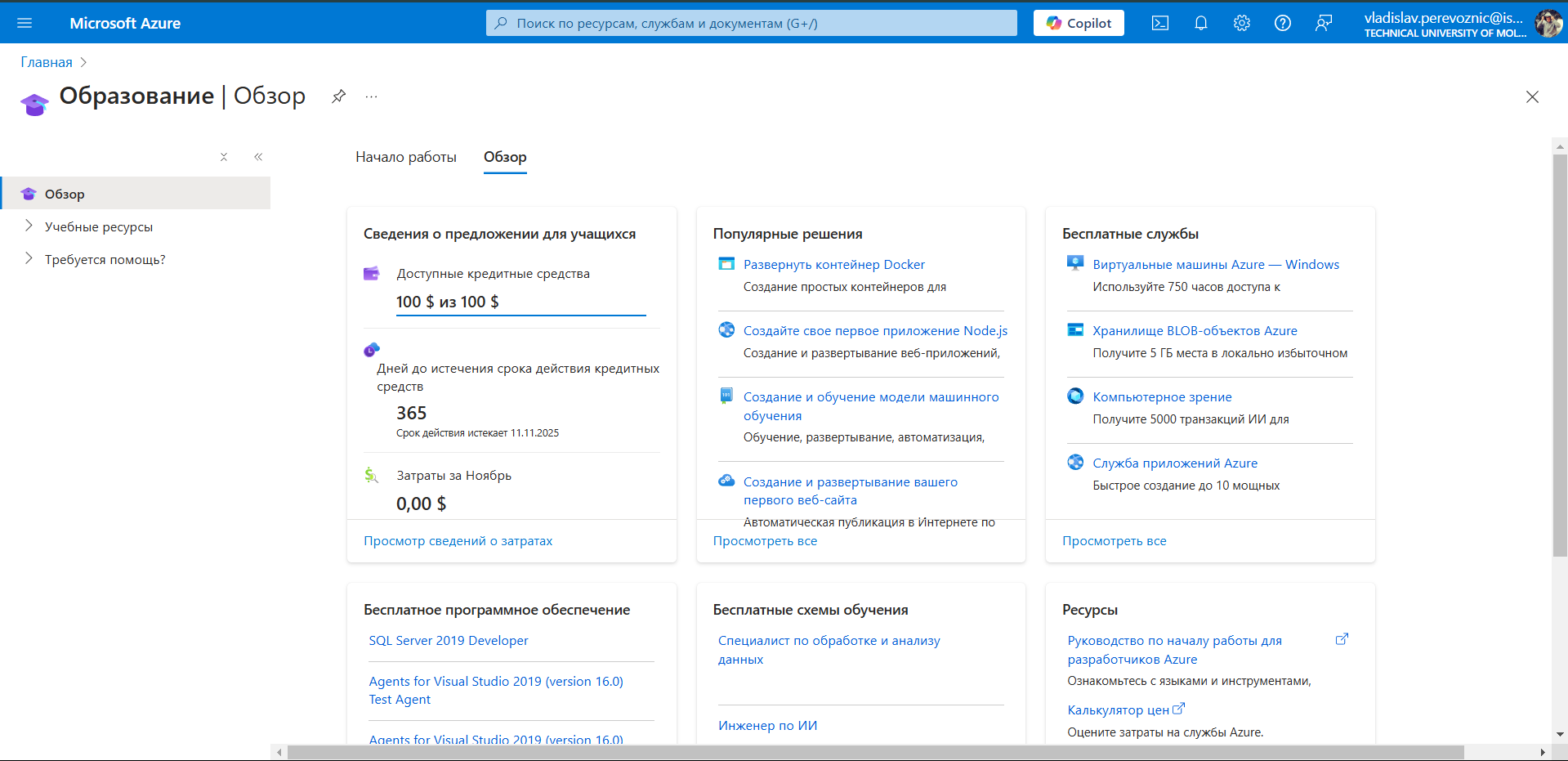
**Logarea GravytiZone Azure:**

****

**Figura 11 – Alegerea logarea pentru membru**

**  
Figura 11 – Începerea logării**

**  
Figura 11.1 – Începerea logării**

**  
Figura 13 – Realizarea logării cu succes**

**Concluzie :**

Security Incident Management în Microsoft Sentinel oferă o platformă eficientă și integrată pentru detectarea, investigarea și rezolvarea incidentelor de securitate. Prin funcții avansate, cum ar fi graficele de investigație și gestionarea proprietarilor de incidente, Microsoft Sentinel permite echipelor de securitate să urmărească în detaliu relațiile dintre resurse, să identifice rapid originea atacurilor și să vizualizeze progresul incidentelor în timp real.

Escaladarea incidentelor către niveluri superioare de echipe de securitate este facilitată prin actualizarea parametrului **Owner**, asigurând că incidentele critice sunt abordate rapid și eficient. În plus, graficele de investigație vizuale permit analizarea cronologiei evenimentelor și corelarea dintre alerte, oferind contextul necesar pentru a răspunde prompt și eficient la amenințări.

În concluzie, modulul de **Security Incident Management** din Microsoft Sentinel este esențial pentru o strategie de securitate proactivă, oferind echipelor de securitate capacitățile necesare pentru a identifica, urmări și rezolva incidentele de securitate într-un mod organizat și eficient, reducând astfel riscul general și impactul incidentelor asupra organizației.