ANEXĂ LA REFERATUL DE NECESITATE
privind achiziția de licențe software pentru cercetare

I. Detectify Deep Scan, versiune Application Scanning, perioada **12 luni – 1 buc.**

Detectify este o platformă de vulnerability scanning pentru aplicații web.
Se vor scana periodic toate domeniile instituționale principale cmu-edu.eu și subdomeniile aferente platformelor educaționale și administrative, cu rulare automată lunară pentru detecția vulnerabilităților web.
Scanarea se va face pentru 5 domenii/subdomenii/aplicații web

II. SNORT Business, perioada 12 luni, 1 sensor - 1buc

Snort este un sistem Intrusion Detection and Prevention (IDS/IPS)
Senzorul va fi instalat pe Debian 13.

Traficul analizat va include fluxuri de trafic precum :

a). Trafic administrativ / instituțional

- Reprezintă comunicațiile dintre servere, echipamente și aplicații de management IT:
- Servicii de autentificare: **LDAP, RADIUS, Kerberos**
- Servicii de administrare: **SSH, RDP, WinRM**
- Management echipamente: **SNMP, HTTPS, API-uri interne**
- Backupuri și replicări: **rsync, NFS, SMB, iSCSI**
- **Scop:** monitorizarea integrității și detectarea activităților neautorizate în segmente critice (ex: VLAN Management, VLAN Servere).

b). Trafic educațional / academic

- Include fluxurile generate de utilizatorii din campus (profesori, studenți, laboratoare):
- Acces platforme educaționale: **Moodle, Teams, Zoom, Webex, elearning.umc.ro**
- Acces resurse online: **navigare HTTP/HTTPS, baze de date academice, repo-uri Git**
- Transfer fișiere între laboratoare și servere (ex: **FTP/SFTP, SMB/CIFS**)
- **Scop:** identificarea anomaliilor (exfiltrare date, scanări interne, descărcări neautorizate).

c) Trafic de rețea general / infrastructură

- Fluxuri fundamentale de funcționare a rețelei:
- **DNS, DHCP, ARP, ICMP (ping)**
- Pachete broadcast/multicast interne
- Comunicații între VLAN-uri sau între gateway și echipamente

- **Scop:** detecția tentativelor de spoofing, ARP poisoning, DHCP rogue, DoS intern.

d) Trafic web și aplicațional

- Aplicații interne (intranet, portal studenți, ERP, e-learning)
- Servicii externe (autentificare SSO, API-uri REST, site-uri educaționale)
- Protocoluri: **HTTP, HTTPS, WebSocket**
- **Scop:** identificarea atacurilor de tip **SQL Injection**, **XSS**, **Command Injection**, etc.

e) Trafic IoT și camere IP

- Comunicații generate de camerele de supraveghere, sisteme de acces, senzori, afișaje digitale
- Protocoale: **RTSP, ONVIF, HTTP, MQTT**
- **Scop:** detectarea conexiunilor externe neautorizate sau a tentativelor de compromitere a camerelor.

f) Trafic inter-VLAN / inter-site

- Trafic între campusuri (CENTRU, FAR, BN, CSN etc.)
- Tuneluri VPN / IPsec / OpenVPN între sedii
- **Scop:** monitorizarea fluxurilor pentru scurgeri de date sau conexiuni anormale între segmente.

g) Trafic suspect / potențial malițios

- Scanări de porturi, brute-force, tentative de exploit
- Conexiuni către IP-uri cunoscute ca malițioase
- Activități tip Command & Control (C2)
- **Scop:** detecția și alertarea prin SNORT (semnături IDS).

III. Maltego Professional, Subscripție Maltego Professional, perioada **12 luni – 1 buc.**

Maltego este un instrument de *OSINT* și *link analysis*.

Se vor folosi 1 licența educațională pentru cadrele didactice. Se vor analiza atât surse OSINT publice, cât și baze interne. Se solicită training introductiv pentru utilizare.

IV. ProSuite de la Provalis Research, Subscripție ProSuite Research, perioada **36 luni – 2 buc.**

ProSuite include instrumente pentru analiză calitativă și cantitativă a datelor textuale (QDA Miner, WordStat, SimStat).

Licențele vor fi instalate pe 2 stații de lucru pentru cercetare socio-economică. Este o achiziție noua. Se vor utiliza modulele QDA Miner și WordStat.

V. **Subscripție OpenNebula Elemental (Single Master Node + High Availability Extension + Pack 10 Managed Nodes),** perioada **12 luni – 1 buc.**

OpenNebula este o platformă de virtualizare și cloud orchestration.

Infrastructura va fi on-premise, rulată pe serverele proprii pentru laboratoarele virtuale educaționale.

VI. **Subscripție Jira Premium, 10 utilizatori, versiune cloud perioada 12 luni – 1 buc.**

VII. **Subscripție Nessus Professional, perioada 12 luni – 1 buc.**

Nessus este un *vulnerability scanner* pentru rețele și sisteme.

Nessus va fi utilizat pentru scanarea a 50 IP-uri interne. Se dorește integrare cu ManageEngine. Este o achiziție nouă pentru utilizare educațională.

VIII. **Subscripție BurpSuite Professional, 2 utilizatori perioada 12 luni – 2 buc.**

BurpSuite este o platformă de testare a securității aplicațiilor web.
Aplicația va fi utilizată în mediul on-premise, in primul rand pentru testarea securității platformelor interne educaționale. Se dorește training de bază pentru cadre didactice.

IX. **ManageEngine Vulnerability Manager Plus Professional Edition Subscription Model,** Annual subscription fee for 50 Workstations+ ManageEngine Vulnerability Manager Plus Professional Edition – Subscription Model – Annual subscription fee for 5 Network Device **- 2 buc.**

ManageEngine VM Plus este o platformă de management al vulnerabilităților
Se dorește acoperirea a 50 de stații de lucru, 2 servere Windows/Linux si a 5 Network Devices. Majoritatea endpointurilor rulează Windows 10/11 Education, Linux Debian. Nu există alte produse ManageEngine active. Vor accesa consola 2 administratori IT. Implementarea dorită este una de tip Standalone

Întocmit: Crăciunescu Bogdan