Lista przydatnych linków o których była mowa podczas webinaru:

- Manager haseł - https://bitwarden.com/
- Serwer do automatycznej inwentaryzacji środowiska IT - https://ocsinventory-ng.org
- System do zarzadzania zgłoszeniami - https://glpi-project.org/pl/
- System do wykrywania nowych hostów w sieci - https://opmantek.com/network-discovery-inventory-software/
- System do monitorowania infrastruktury IT - https://www.zabbix.com/
- Antywirus z centralna administracja - https://www.bitdefender.com/business/smb-products/business-security.html
- Oprogramowania do wirtualizacji serwerów - https://www.proxmox.com/en/proxmox-ve
- Oprogramowanie Router które posiada IDS/IPS systemy do wykrywania i przeciwdziałania zagrożeniom z Internetu - https://www.pfsense.org/
- Zarządzenie centralnie tożsamością w Windows 10/11 Pro - https://azure.microsoft.com/pl-pl/services/active-directory/
- Centralne zarzadzanie logami systemowymi oraz wykonywanie alertów na ich podstawie - https://www.graylog.org/
- Skaner podatności aplikacji oraz systemów - https://www.openvas.org/
- MFA fizyczny klucz do autoryzacji - https://www.yubico.com/
- Aplikacja do szyfrowaniania nośników danych np. Pendrive - https://www.veracrypt.fr
- Strona zawierająca wykryte podatności w systemach IT - www.cvedetails.com
- Tęczowe tablice – https://project-rainbowcrack.com/table.htm
- Polska rzadowa strona zajmujaca się cyberbezpieczeństwem - https://cert.pl/
- OwnCloud – swój serwer plików https://owncloud.com/

Mapy Online zagrożeń IT

- https://livethreatmap.radware.com/
- https://talosintelligence.com/fullpage_maps/pulse
- https://threatmap.bitdefender.com/
- https://threatmap.checkpoint.com/
- https://cybermap.kaspersky.com/