Наслов: Лабораторија за сајбер безбедност

Лабораторијата за сајбер безбедност е современо опремена средина наменета за анализа на напредни симулации на сајбер напади и тестирање на различни хардверски и софтверски решенија за справување со нив. Во оваа лабораторија се овозможува изведување на активности како што се: тестирање на дигитални технологии во услови на симулирани напади, анализа на ефектите што произлегуваат од сајбер-инциденти, како и проценка на ефикасноста на различни мерки за заштита на компјутерската инфраструктура.

Специјално е дизајнирана за практично учење и разбирање на процесите на идентификација, анализа и евалуација на сајбер ризици, со помош на професионални алатки за проценка на ризик. Преку користење на лабораторијата, корисниците добиваат можност детално да ги истражат последиците од најчестите типови на сајбер напади и да стекнат поголема свесност за нивната сериозност, како и за ефективните методи на заштита и одбрана.

Табела за преглед на инфраструктура/опрема

	Опис
Партнер	Воена Академија „Генерал Михаило Апостолски“
Тип на опрема	Лабораторија за сајбер безбедност
Целна група	Стартапи, индустриски компании и истражувачи
Клучна технологија	Сајбер безбедност, дигитална форензика
Статус	Достапно за користење
Предуслови за користење	Релевантен проект или потреба, основни технички познавања

Опис на инфраструктурата/ опремата

Лабораторијата за сајбер безбедност располага со специјализирана инфраструктура која овозможува реализација на практични вежби, симулации и истражувања поврзани со информациска безбедност, инцидентен одговор и анализа на сајбер-напади. Следнава опрема и системи се дел од лабораторијата:

Хардверска опрема

- Високо перформантни работни станици (Intel i7, GPU 24GB RAM) за анализа на мрежен сообраќај, пенетрационо тестирање и виртуелизација.
- Сервери со поддршка за виртуелизација (VMware, VirtualBox, Hyper-V) за хостирање на симулирани мрежи и IDS/IPS системи.

- Складишна инфраструктура (NAS/SAN) за логови, backup и податоци од симулации.
- Мрежна опрема: управувани switch-ови, рутери, firewall-уреди, VLAN конфигурации и Wi-Fi access точки за симулација на реални мрежни средини.
- IoT уреди и вградени системи за тестирање на сајбер-безбедност во паметни уреди и индустриски контролни системи.

Софтверска опрема

- SIEM платформи: Wazuh, ELK Stack за анализа на логови и откривање на инциденти.
- IDS/IPS системи: Snort, Suricata, Zeek за реална анализа на мрежниот сообраќај.
- Симулациски алатки: GNS3, Cisco Packet Tracer за мрежно моделирање.
- Pentesting алатки: Kali Linux, Metasploit, Burp Suite, Nmap, Wireshark.
- Алатки за анализа на ранливости: OpenVAS, Nikto.
- Виртуелизациски и контејнерски платформи: VirtualBox, Docker, Kubernetes за динамично тестирање и дистрибуирани симулации.
- Алатки за проценка на ризик и управување со безбедност.

Мрежна конфигурација

- Одделни физички и виртуелни мрежи за симулација на DMZ, корпоративна LAN, интернет и напаѓачки мрежи.
- Promiscuous mode и SPAN порти за анализирање на мрежен сообраќај без влијание на продукциските мрежи.
- Изолација на средини преку VLAN и виртуелни фаерволи за контролирани експерименти.

Педагошка и визуелна поддршка

- Интерактивна табла и проектори за демонстрации и анализи во живо.
- Интерен LMS и cloud-based remote access за учество и пристап до лабораторијата од далечина.
- Снимање на сесии за анализа и повторување на лабораториските вежби.