Title: Cyber security laboratory

The Cybersecurity Laboratory is a modern, well-equipped environment designed for analyzing advanced simulations of cyberattacks and testing various hardware and software solutions to counter them. This laboratory enables the execution of activities such as testing digital technologies under simulated attack conditions, analyzing the effects resulting from cyber incidents, and evaluating the effectiveness of different measures for protecting computer infrastructure.

It is specifically designed for hands-on learning and understanding of the processes of identifying, analyzing, and evaluating cyber risks using professional risk assessment tools. By using the laboratory, users gain the opportunity to thoroughly explore the consequences of the most common types of cyberattacks and develop greater awareness of their severity, as well as the effective methods of protection and defense.

Infrastructure/Equipment Overview Table

	Description
Partner	Military Academy General Mihailo Apostolski – Skopje
Equipment Type	Cyber security laboratory
Target group	Startups, industrial companies, and researchers
Key Technology	IDS, IPS, SIEM
Status	Available for use
Prerequisites for use	Relevant project or need, basic technical knowledge

---

Description of infrastructure/equipment

The Cybersecurity Laboratory is equipped with specialized infrastructure that enables the execution of practical exercises, simulations, and research related to information security, incident response, and cyber-attack analysis. The following equipment and systems are part of the laboratory:

Hardware Equipment

- High-performance workstations (Intel i7, GPU, 24GB RAM) for network traffic analysis, penetration testing, and virtualization.
- Virtualization-supported servers (VMware, VirtualBox, Hyper-V) for hosting simulated networks and IDS/IPS systems.
- Storage infrastructure (NAS/SAN) for logs, backups, and simulation data.

- Network equipment: managed switches, routers, firewall devices, VLAN configurations, and Wi-Fi access points for simulating real-world network environments.
- IoT devices and embedded systems for testing cybersecurity in smart devices and industrial control systems.

Software Equipment

- SIEM platforms: Wazuh, ELK Stack for log analysis and incident detection.
- IDS/IPS systems: Snort, Suricata, Zeek for real-time network traffic analysis.
- Simulation tools: GNS3, Cisco Packet Tracer for network modeling.
- Penetration testing tools: Kali Linux, Metasploit, Burp Suite, Nmap, Wireshark.
- Vulnerability assessment tools: OpenVAS, Nikto.
- Virtualization and containerization platforms: VirtualBox, Docker, Kubernetes for dynamic testing and distributed simulations.
- Risk assessment and security management tools.

Network Configuration

- Separate physical and virtual networks for simulating DMZ, corporate LAN, internet, and attacker networks.
- Promiscuous mode and SPAN ports for analyzing network traffic without affecting production networks.
- Environment isolation via VLANs and virtual firewalls for controlled experiments.

Visual Support

- Interactive whiteboard and projectors for live demonstrations and analyses.
- Internal LMS and cloud-based remote access for remote participation and access to the lab.
- Session recording for analysis and repetition of lab exercises.