Michal Markevych

Chicago, IL | 847-387-9196 | michalmarkevych@gmail.com |https://www.linkedin.com/in/mmarkevych

SUMMARY

An ambitious and dedicated individual with a strong background in cybersecurity and computer engineering. My strong analytical skills and ability to think outside the box have led me to develop innovative solutions to each project I undertake. As a passionate and resourceful person, I am ready to join a team and help them achieve limitless goals.

EDUCATION

Illinois Institute of Technology, Chicago, IL December 2023

Master of Security and Cyber Forensics

- Certification Courses taken for CompTIA Linux+, CySA+, Network+, Security+

Bachelor of Science in Computer and Cybersecurity Engineering

- Specialization in Security of IoT

PUBLICATIONS

"A Review of Enhancing Intrusion Detection Systems for Cybersecurity Using AI" June 2023

- KNOWLEDGE-BASED ORGANIZATION Conference in Sibiu, Romania
- Presented findings on AI-based IDS systems in front of a panel of colonels and security professionals
- Developed a test data flow model using the GPT-4 model to simulate operation of IDS

WORK EXPERIENCE

Cybersecurity Intern

Vomark Technologies, Wheeling, IL May 2022 - Present

- Conducted vulnerability assessments on entire organization's systems using **Splunk** and **Azure Sentinel** SIEM systems, identifying and mitigating *45 critical vulnerabilities* within a one-week timeframe.
- Worked alongside Network Engineers and Website IT teams to remediate vulnerabilities, resulting in a 39% reduction in overall security risk as measured by subsequent vulnerability assessments.
- Used **NIST CSF, NIST SP 800-53, and ISO 27001** standard to develop an information security framework and management system tailored to Vomark Technologies.
- Engaged in **Red Team exercises** using Kali Linux and Tenable Nessus providing insight on potential attack vectors and overall threat intelligence.

Medical Security Engineering Intern

Vomark Technologies, Wheeling, IL May 2020 – May 2022

- Launched the integration of *cybersecurity measures* into the repair and maintenance process for over 200 SIEMENS and PHILIPS ultrasound machines.
- Improved efficiency of exportation of ultrasounds by 8% over the course of 18 months using **Microsoft EXCEL** data analytics.
- Developed comprehensive protocol for handling software issues during system-software discrepancies leading to cut down of new engineer onboard training by 5 hours.
- *Promoted* within 12 months due to strong performance, impact on ultrasound exportation process, and contributions to cybersecurity enhancement.

Embedded Systems Engineer Intern March 2019 - March 2020

Adler Planetarium, Chicago, IL

- Completed arduino coding training and within 2 weeks integrated GPS on NiteLite (night imaging balloon satellite which analyzes light pollution over Chicago's skyline).

- Designed PCB’s for satellite’s magnetic compass leveraging Eagle with a team of engineers, bringing the prototype from stage 3 to stage 4.
- Debugged faulty arduino code for tracking in satellite prototype, allowing engineering team to develop next stage of movement sensors.

SKILLS

- **VULNERABILITY TESTING AND SECURITY TOOLS** : Nmap, Burp Suite, SIEM, Metasploit, Nslookup, whois, dig, Hydra, John-the-ripper, Dirb, Maltego, Flawfinder, FindBugs
- **ENGINEERING DEVELOPMENT AND CODING**: Java, Python, Bash/Powershell/Python Scripting, Arduino/C++
- **COMPLIANCE AND REGULATORY FRAMEWORKS:** NIST SP 800-53, SOC 2, PCI DSS 4.0, MITRE ATT&CK, Cyber Kill Chain, ISO 27001
- **LANGUAGES**: English and Polish

PROJECT EXPERIENCE

Azure SIEM system October 2023

- Successfully implemented an Azure Sentinel cloud-based Security Information and Event Management **(SIEM)** system as part of a cybersecurity project.
- Deployed a highly vulnerable virtual machine (Honeypot) on the Azure cloud platform, deliberately exposing it to the internet to attract and monitor potential cyberattacks.
- Actively monitored and logged a wide range of cyberattacks from various IP addresses using custom workbook queries.
- Leveraged Azure Sentinel and AI mapping software to transform attack data into a geographical map, allowing for the visualization of attack origins by country.

Cybersecurity Policy August 2022 - December
2022 Illinois Institute of Technology

- Led a team of 4 Masters and PhD Students to create a functioning security policy specifically targeted at Web Application Security, Acceptable Use Policy, and Role Definitions.
- Implemented an effective Information Security policy to maintain confidentiality, integrity, and availability of university resources with adaptations from NIST Cybersecurity Framework. ● Addressed vulnerabilities in the university's website, focusing on authentication, SSL certificates, web application headers, and cross-site scripting.

Hyperloop - Electrical Lead January 2019 - November 2020
Hyperloop IIT

- Calculated quantity and wiring of battery cells to power MagLev Hyperloop Pod saving $2,000. ● Lead the electronics team by coordinating weekly objectives and delegating tasks to efficiently meet showcase deadlines.

CERTIFICATIONS

- CompTIA Security+ October 2023

HONORS AND ACHIEVEMENTS

- As the **captain** of the NCAA Division III Men's Volleyball Team at IIT, led the team in kills, earning honorable mention for **All-Conference player of the year**
- Dean’s List at Illinois Tech, multiple semesters August 2022 - August 2023
  Completed thesis on *IoT Issues and the Promise of SDN Technology* August 2021 - March 2022