YURIY GOSHOVSKIY

773-680-4766 | yuriygosh@gmail.com | linkedin.com/in/yuriygosh | www.yuriy.us

Cybersecurity Professional with an A.A.S degree in Cybersecurity and practical experience from a 12-month internship at a major healthcare organization. Proficient in threat hunting, automation, security data analysis, and defensive security engineering. Currently pursuing a bachelor's degree, set to graduate in May 2025. Committed to leveraging automation to solve security scaling challenges.

Career highlights include:

- Proactive professional with 2 years of experience in security engineering, analysis, and threat hunting. Successfully developed an automated solution to track security testing, improving audit readiness.
- Standardized the process of hunting indicators of compromise (IOCs) within Cyber Threat Intelligence, significantly enhancing the organization's threat detection and response capabilities.
- Leveraged automation (PowerShell, Blob Storage, MS Graph API & PowerBi) to solve retrospective threat hunting challenges and advance security maturity of DevSecOps.

EDUCATION:

B.S. Cybersecurity | Lewis University | GPA: 3.60 — *Expected May 2025*
A.A.S Cybersecurity | College of DuPage | GPA: 3.75 — *August 2024*

CERTIFICATIONS & TRAINING:

CWNA | TestOut Security Pro

WORK EXPERIENCE:

Northwestern Medicine — **Chicago, IL**
Security Analyst Intern (Returning) — *May 2024 - Present*

- Helped migrate log sources and ingestion methods from Sentinel into Azure Data Explorer (ADX) by leveraging KQL and Microsoft docs, achieving $5,000 in quarterly savings.
- Analyzed phishing trends and designed Microsoft Exchange mail flow rules, reducing monthly reconnaissance-related emails from 300 to 150.
- Built an automated indicator of compromise (IOC) hunting process for the Cyber Threat Intelligence program using Blob Storage, Defender XDR, and the Microsoft Graph API.

Northwestern Medicine — **Chicago, IL**
Security Analyst Intern — *May 2023 - December 2023*

- Automated the provisioning of Active Directory (AD) accounts by writing PowerShell scripts, reducing monthly manual account creation from 300 minutes to 75 minutes.
- Utilized Microsoft Graph API to identify and manage 1,000 inactive service accounts, disabling or vaulting within CyberArk, effectively reducing a significant threat vector by nearly 90%.
- Identified 200+ terminated users with active AD accounts and scripted their account disabling.

PROJECTS:

Youtube Channel — **Chicago, IL**
www.youtube.com/@homelabd — *March 2023 - Present*

- Launched a security-focused YouTube channel, independently recording and editing content, reaching over 20,000 viewers across 5 videos, and built a community on Discord.

Department of Energy CyberForce Program — **Chicago, IL**
Participant — *September 2023 - October 2023*

- Led the College of DuPage cyber team in the Department of Energy's CyberForce competition, achieving 62nd out of 169 teams and ranking as the 3rd highest-scoring two-year institution.

SKILLS/TOOLS SUMMARY:

- Threat Hunting: KQL, Azure Sentinel, Microsoft Defender for Endpoint, Cisco Umbrella
- Identity Access Management: Active Directory, Azure Entra ID
- Scripting, Automation & DevSecOps: PowerShell, Bash, Microsoft Graph API
- Privacy & Risk Management: NIST, MITRE ATT&CK, HIPPA