SHINJI NOBUHARA

IT Security Engineer / Software Engineer (Chicago, USA)
TEL: **E-mail**: shinjin2@illinois.edu

EDUCATION

Master of Science, Computer Science, University of Illinois Urbana-Champaign, Chicago, IL, USA
Bachelor of Computer Science, Oregon State University, Corvallis, OR, USA (GPA: 3.94 / 4.00)

WORK EXPERIENCE

IT Security Engineer, Omron Software, Kyoto, Japan Mar. 2021 - Jul. 2024

- Served as a core member of the **SOC and security operations team**, responsible for detecting, analyzing, and responding to security incidents across enterprise systems using **EDR and SIEM platforms**. Consistently achieved **incident triage within 30 minutes**, helping minimize operational and business impact.
- Identified inefficiencies in existing threat detection and investigation processes and **redesigned incident response workflows**, enabling faster root-cause analysis and **standardized incident reporting within 30 minutes** across teams.
- Led updates to secure development and security operations policies to align with **NIST Cybersecurity Framework (CSF) 2.0**, strengthening organizational maturity across **Identify, Protect, Detect, Respond, and Recover** functions.
- Conducted regular **application and infrastructure vulnerability assessments** using **IBM AppScan** and **Nessus Professional**, translating scan results into prioritized remediation actions based on **OWASP Top 10** and **CVSS scoring**.
- Recognized inconsistencies in threat assessment across group companies and **standardized threat evaluation criteria**, reducing risk assessment discrepancies by approximately **20%** and improving cross-organization security alignment.
- Played a key role in **onboarding and operationalizing new security tools** in a fast-paced SOC environment, enabling rapid adoption without disruption to ongoing monitoring and response activities.

Software Engineer, Staff Service Engineering, Okayama, Japan Jul. 2019 - Feb. 2021

- Developed a **home-visit nursing management system** using **VB.NET** and **Microsoft SQL Server**, supporting clinical operations and data management.
- Collaborated with a **6-member development team**, delivering features on schedule without project delays.

TECHNICAL SKILLS

Programming Languages: Python, C/C++, Java, JavaScript, PHP, VB.NET, SQL
Security & Monitoring Tools: Microsoft Defender for Endpoint, Securonix, Carbon Black, CrowdStrike, Sentinel, Splunk
Vulnerability & Penetration Testing: AppScan, Nessus, Nmap, Burp, Wireshark, Metasploit
Frameworks & Technologies: Flask, Node.js, React, Bootstrap, Laravel, ZeroMQ
Parallel / System Computing: OpenMP, CUDA, OpenCL, MPI
Databases: Microsoft SQL Server, MySQL, SQLite
Operating Systems: Windows, Linux

PROJECTS

Penetration Testing Lab (Personal Project)

- Built vulnerable and attacker virtual machines using VirtualBox and conducted end-to-end penetration tests.
- Performed reconnaissance and exploitation using **Nmap, Burp Suite, Wireshark, and Metasploit**, successfully escalating privileges and capturing root flags.

  GitHub: https://github.com/nobu1/PenetrationTestProject

SOFT SKILLS

- Quickly ramped up on new security platforms when assigned to the SOC team, independently learning and operationalizing **Microsoft Defender for Endpoint** and **Securonix** to maintain uninterrupted monitoring and response.
- Led security coordination meetings with **overseas group companies**, clearly articulating risk levels, investigation findings, and next steps in English to drive timely action.
- Communicated incident status and security risks in a **clear, concise, and actionable manner** to both technical and non-technical stakeholders, enabling faster decision-making during security events.