Chinkhusel Tsolmonbaatar

SOC Analyst & Cybersecurity Engineer

Sulejówek, Poland
+48 539 623 147
husele1000@gmail.com
https://chinkhuselts.github.io
https://www.linkedin.com/in/chinkhusel-tsolmonbaatar-905880271/

Professional Summary

Proactive SOC Analyst and Cybersecurity Engineering student with over 1 year of combined practical experience in security monitoring, SIEM implementation, and incident response. I specialize in analyzing network traffic and automating vulnerability assessments to protect information assets. Fluent in English (C1) and skilled in Splunk, ELK Stack, and Snort, I am eager to join ISS to help secure global workplace environments through rigorous threat detection and efficient incident escalation.

Education

Sep 2024 – Expected Sep 2026

Engineer, Cybersecurity, *Vizja University*, Warsaw, Poland

- Relevant Coursework: Cisco Network Architecture, Operating Systems Security
- Thesis: AI-Driven Threat Detection for Ransomware

Skills

SIEM & Monitoring

- Splunk (Search & Reporting)
- ELK Stack (Elasticsearch, Logstash, Kibana)
- Prometheus

Vulnerability Management

- Tenable (Nessus)
- Risk Analysis
- Patch Management
- Automated Reporting (Python)

Network Security

- Snort (NIDS)
- Packet Analysis
- Firewall Configuration
- Cisco Networking (Switching/Routing)

Technical Stack

- Python (Pandas for Automation)
- Bash Scripting
- Linux Hardening
- Windows Event Logs

Languages

- English (C1 - Advanced)
- Polish (A1)
- Mongolian (Native)

Work Experience

Aug 2025 – Oct 2025 **SOC & Security Engineer Intern**, *Khan Bank*, Ulaanbaatar, Mongolia

- **Security Monitoring & Incident Response**: Acted as the first line of defense, monitoring thousands of daily security events in Splunk. Analyzed Windows logs, Linux Syslogs, and proxy data to detect suspicious activities like DDoS attempts, ensuring timely escalation to the CSIRT team.
- **Vulnerability Assessment Automation**: Developed a Python script (using Pandas) to automate Tenable/Nessus report processing, reducing processing time by 30% and allowing the team to focus on remediation rather than data entry.
- **Threat Intelligence & Research**: Conducted research on Akamai API security and traffic flows (North-South/East-West) to identify potential loopholes. Built a custom "ThreatMap" tool to visualize global attack vectors, helping non-technical stakeholders understand the severity of incoming threats.
- **System Hardening**: Collaborated with IT teams to harden Linux servers by securing kernel parameters and configuring firewalls, directly improving the organization's security posture.

Key Projects

Jan 2024 – Dec 2024 **Centralized Security Platform Implementation (ELK & Snort)**

- **SIEM Deployment**: Designed and built a fully functional SIEM solution using the Elastic Stack to simulate a corporate monitoring environment.
- **Network Intrusion Detection**: Integrated Snort 3 as a NIDS, configuring it to inspect network packets and forward alerts to Elasticsearch via Filebeat.
- **Dashboarding**: Created custom Kibana dashboards mapped to the MITRE ATT&CK framework to visualize attacks in real-time, gaining deep familiarity with log parsing and event correlation.

Jan 2024 – Dec 2024 **WannaCry Malware Analysis**

- Performed dynamic analysis of live ransomware in a secure CAPEv2 sandbox. Reverse-engineered the attack behavior to understand how the malware propagates, documenting indicators of compromise (IOCs) for future detection.

Certifications

- **Cisco Netacad Networking Basics Badge** – Cisco (Jan 2025)
- **Cybersecurity Engineer** – TryHackMe (Nov 2025)
- **Chess Champion** – Mongolian Community in Poland (Strategy & Logic)