

*SOC Analyst &  
Cybersecurity  
Engineer*

 +48 539 623 147

🌐 <https://chinkhuselts.github.io>

in <https://www.linkedin.com/in/chinkhusel-tsolmonbaatar-905880271/>

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.

Sep 2024 – **Engineer, Cybersecurity, Vizja University, Warsaw, Poland**  
 Expected Sep 2026 ○ Relevant Coursework: Cisco Network Architecture, Operating Systems Security  
 ○ Thesis: AI-Driven Threat Detection for Ransomware

```
graph TD; SOC[Security Operations Center (SOC)] --> SIEM[SIEM & Monitoring]; SOC --> VM[Vulnerability Management]; SOC --> NS[Network Security]; SOC --> TS[Technical Stack]; SOC --> L[Languages]; SIEM --> Splunk[Splunk (Search & Reporting)]; SIEM --> ELK[ELK Stack (Elasticsearch, Logstash, Kibana)]; SIEM --> Prometheus[Prometheus]; VM --> Tenable[Tenable (Nessus)]; VM --> RA[Risk Analysis]; VM --> PM[Patch Management]; VM --> AR[Automated Reporting (Python)]; NS --> Snort[Snort (NIDS)]; TS --> PA[Packet Analysis]; TS --> FC[Firewall Configuration]; TS --> CN[Cisco Networking (Switching/Routing)]; L --> Python[Python (Pandas for Automation)]; L --> Bash[Bash Scripting]; L --> Linux[Linux Hardening]; L --> Windows[Windows Event Logs]; L --> English[English (C1 - Advanced)]; L --> Polish[Polish (A1)]; L --> Mongolian[Mongolian (Native)];
```

The diagram illustrates the components of a Security Operations Center (SOC). It is structured as a tree with 'Security Operations Center (SOC)' at the top. Below it are five main categories: 'SIEM & Monitoring', 'Vulnerability Management', 'Network Security', 'Technical Stack', and 'Languages'. Each category has a list of associated tools or tasks: 'SIEM & Monitoring' includes Splunk, ELK Stack, and Prometheus; 'Vulnerability Management' includes Tenable, Risk Analysis, Patch Management, and Automated Reporting; 'Network Security' includes Snort; 'Technical Stack' includes Packet Analysis, Firewall Configuration, and Cisco Networking; 'Languages' includes Python, Bash Scripting, Linux Hardening, Windows Event Logs, and three levels of language proficiency (English, Polish, Mongolian).

- Security Operations Center (SOC)
  - 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)
  - Technical Stack
    - Packet Analysis
    - Firewall Configuration
    - Cisco Networking (Switching/Routing)
  - Languages
    - Python (Pandas for Automation)
    - Bash Scripting
    - Linux Hardening
    - Windows Event Logs
    - English (C1 - Advanced)
    - Polish (A1)
    - Mongolian (Native)

 $1/2$

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

- Oct 2025
- **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 – **Centralized Security Platform Implementation (ELK & Snort)**

- Dec 2024
- **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 – **WannaCry Malware Analysis**

- Dec 2024
- 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)