Jonathan Cheung

jonathan.cheung.j@gmail.com | 647-836-2928 | github.com/jonnych6 | linkedin.com/in/jonathan-cheung6/

WORK EXPERIENCE

Arctic Wolf **April 2023 – December 2023**
Endpoint Security Developer, Intern *Remote – Waterloo, ON,CAN*

- Designed endpoint detection rules using MITRE ATT&CK, Cyber Kill Chain, and TTPs, applying both stateful and stateless Sigma rules for enhanced threat detection.
- Conducted comprehensive log analysis with Kibana and KQL, identifying IOCs, viruses, and other advanced threats across diverse environments.
- Developed and optimized Python scripts for automation, utilizing Git for version control to support collaborative development.
- Conducted Breach Failure to Detect (BFD) analysis to examine true positives, improving and refining detection rules to enhance detection capabilities.
- Created SysmonSimulator, a PowerShell tool based on Atomic Red Team scripts, to simulate Sysmon events for detection validation.
- Researched emerging threats like Living off the Land attacks and Active Directory exploitation, translating findings to improve MDR capabilities.

EDUCATION

Sheridan College **August 2024**
Honours Bachelor of Information Sciences (Cyber Security) *Oakville, ON*

- **GPA**: 3.76/4.0
- Member of ISSessions, a cybersecurity club focused on CTF challenges and industry talks, enhancing my cybersecurity skills and knowledge.

Western University **April 2020**
Bachelor of Science, Biology & Psychology *London, ON*

PROJECTS

File Integrity Monitor – PowerShell

- Developed a PowerShell script to monitor file changes (modification, deletion, creation) in target directories.
- Utilized SHA-512 hashing to track file integrity and detect unauthorized changes.
- Enhanced reporting capabilities to generate detailed logs and notifications for any detected file changes, facilitating prompt incident response.

Windows Reverse Shell - Python

- Built a reverse shell for Windows enabling remote command execution.
- Extracted system information (OS version, IP address, boot time) to gather insights into target environment.

Active Directory Lab Setup for Kerberoasting Exploration

- Created an Active Directory lab environment for Kerberoasting simulations.
- Cracked service account hashes using Empire and Kali Linux, identifying weak passwords and misconfigurations.
- Configured domain controllers, user/service accounts, and group policies for realistic testing.

SKILLS & CERTIFICATIONS

- **Certifications**: Practical Help Desk (TCM Security), Security+ (in progress)
- **Programming Languages:** Python, Windows PowerShell, Bash, Java, SQL, KQL
- **Cybersecurity Tools:** Kibana, Sysmon, Wireshark, tcpdump, Splunk, Nmap
- **Technologies & Tools**: Jira/Confluence, Git, VS Code, Microsoft Suite, VMware
- **Languages**: English, Cantonese
- **Operation Systems**: Windows Microsoft, MacOS, Linux