NEEL KOTAK

+1(808) 753-9778 ◇ Threat Detection and Response Analyst ◇ San Antonio, TX
neelkotak13@gmail.com ◇ linkedin.com/in/neel-kotak/ ◇ github.com/neelkotak13

OBJECTIVE

Accomplished Cyber Warfare Officer with 4 years of experience in the United States Air Force and proven expertise in rogue systems investigations, advanced malicious cyber activity detection, and agile methodology-based hunts. Currently pursuing an MS in Cyber Security from Georgia Tech Institute of Technology, complementing practical experience with advanced academic knowledge. Highly skilled in memory and disk forensics, programming languages like C/C++, Java, Python, and penetration testing. More recently experienced in Defensive Cyber, I have always had a knack for offensive cyber concepts, penetration testing, and reverse engineering/malware analysis seeking out practical experience from multiple college internships.

EDUCATION

Master of Cyber Security, Georgia Institute of Technology — Expected 2024
Relevant Coursework: Advanced Malware Analysis, Network Security, Information Policy and Management, Secure Computing Systems, Applied Cryptography, Information Security Lab: System and Network Defenses

Bachelor of Computer Science, University of Hawaii at Manoa — 2015 - 2019

CERTIFICATIONS

CompTIA Security+ - May 2020
GCFA - Aug 2021
GCIH - Jan 2023
DoD 8570: IAT Level III | CSSP Analyst | Incident Responder
TS/SCI with CI Poly - Jul 2021

SKILLS

Cybersecurity	Malicious Activity Hunting with ELK, Forensic Analysis, Penetration Testing
Programming/Scripting	C/C++, Java, JavaScript, HTML/CSS, Python, Lisp, Bash, Assembly (x86)
Incident Management	SIEM Status Tracking, Investigation management via DFIR IRIS
Network Protocols	Arkime, Wireshark, Zeek, analysis of common protocols: TCP, UDP, IP DNS, etc...

EXPERIENCE

Cyber Protection Team Mission Element Lead (CPT MEL) — May 2020 - Present
U.S. Air Force — *San Antonio, TX*

- Led 10+ member teams on rogue systems investigations for proactive threat hunting on multiple networks spanning over 3000+ endpoints and petabytes of network traffic, uncovering novel APTs Tactics, Techniques, and Procedures (TTPs) which deterred, disrupted, and degraded cyber actors
- Extensive experience with memory and and disk based forensic artifacts, including use of volatility, FTK imager, and KAPE forensics for intensive analysis of disk and memory images
- Directed and analyzed countless suspicious and malicious binaries via static and behavioral analysis, enhancing total industry knowledge of sophisticated threat actors
- Wrote extensive python and powershell scripts to automate and search IOCs across large data sets for malicious activity, which amplified efficiency and number of findings across multiple missions
- Wrote multiple technical reports that focused on threat actor findings, assessed network security posture, and recommended mitigation for network referencing NIST 800-53 guidance, bolstering network defenses and reducing adversary attack surface

- Created, reviewed and validated detection rules team playbook for use in ELK stack to enhance detection of IOCs, which reduced indications of false positives

Cyber Security Analyst Dec 2019 - May 2020
American Savings Bank *Honolulu, HI*

- Monitored SIEM, Firewall logs, IDS/IPS for anomalous events and suspicious activity, leading to the detection and mitigation of 20+ potential security threats monthly
- Authored multiple incident response reports for events resulting in confirmed findings across enterprise of 50+ bank branches state-wide
- Conducted weekly vulnerability scan of all bank workstations, servers, and ATMs, contacted server managers to fix patches via nessus/tenable, resulting status tracking via monthly vulnerability reports
- Monitored email alerts for Data Loss Prevention (DLP), PII, and customer information

Engineering Researcher, Advanced Course in Engineering May 2019 - Aug 2019
Air Force Research Labs (AFRL) *Rome, NY*

- Completed rigorous research and graduate-level coursework in a wide breath of cybersecurity topics focused on Red Team Tactics.
- Introduced to Reverse Engineering concepts: Sandbox tested and emulated network services to conduct dynamic behavioral analysis and used debuggers and disassemblers such as GDB, IDA/Ghidra for static analysis.
- Tested of Network Penetration conceptions through use of open source tools Metasploit, Powershell Empire, Unicorn packer, and reverse shells.
- Firewall evasion tactics focused on network baselining, covert Command and Control (C2) channels, packet encapsulation to bypass firewall rules.

Cyber Intern, Advanced Cyber Education Jul 2018 - Aug 2018
Air Force Institute of Technology (AFIT) *Dayton, OH*

- Classroom instruction component on cyberspace operations, cyber war exercises, and cyber officer development focused on the study of cyber and its challenges
- Focused coursework on core cybersecurity concepts, followed by week-long practical capstone Cyber Network Defense Exercise testing Defense in Depth, Systems Analysis, Network Penetration, and Computer Network Defenses
- Received Distinguished Graduate award, top 10 percent performer in program