KSHITIJ TRIPATHI

kt145@hotmail.com · LinkedIn · Github · Certified PNPT · Certified PWPA

.

A cybersecurity engineer with innate curiosity and a keen attention to detail. Looking to create solutions by combining my cyber security knowledge and development skills. Skilled in threat analysis, code review, penetration testing, incident response and programming.

EXPERIENCE

07/2024 – PRESENT
CONCIERGE SECURITY ENGINEER 2, ARCTIC WOLF

- Advised clients on strengthening security operations and aligning strategies with business objectives.
- Provided actionable recommendations through executive briefings and security reports.
- Guided clients through the deployment and optimization of MDR solutions for seamless integration.
- Developed automation tools to assist Concierge engineers in their roles.
- Collaborated with engineers to optimize existing workflows and create new ones.

11/2023 – 07/2024
SECURITY ENGINEER 2, ARCTIC WOLF

- Proficiently analyzed and prioritized security events from diverse sources, optimizing response times.
- Led end-to-end security incident management, collaborating with internal and external teams, and expertly handled complex investigations.
- Adeptly prioritized tasks, balancing explicit and implied priorities, while conducting thorough quality assessments for operational improvement.
- Actively mentored team members, promoting knowledge sharing, and demonstrated commitment to continuous learning and skill development within my security expertise.
- Developed internal tooling to support SOC engineers in their workflows & communications.

06/2023 – 11/2023
SECURITY ENGINEER 1, ARCTIC WOLF

- Developed and implemented tools and scripts for workflow optimization, streamlined communication, and enhanced accountability. Gathered feedback and iteratively improved the tools based on team input.
- Automated tasks reduced administrative work by 40%, improved collaboration, and accelerated decision-making. Achieved measurable time and cost savings for the organization.
- Identified and mitigated data breaches, risks, and vulnerabilities. Provided tailored guidance and support to customers.

- Assisted senior investigators in conducting deep compromise investigations. Prepared detailed reports and responses for customers, addressing the nature of the incidents and recommending mitigation strategies.

01/2023 – 06/2023
SECURITY ANALYST, ARCTIC WOLF

- Monitored and analyzed network traffic, system logs, and security events to identify potential security incidents.
- Investigated and triaged security alerts using industry-standard tools and methodologies.
- Successfully mitigated and resolved 95% of security incidents within established SLA timeframes, minimizing the impact on business operations.

02/2022 – 01/2023
SECURITY ANALYST - INTERN, ARCTIC WOLF

- Used my time as an intern to learn all the tools and aspects of the Security Analyst role.
- Worked on hard Tier 1 tickets to under gain knowledge and experience to excel in the full-time role.
- Worked on various projects, collaborating with different departments and creating long-term solutions to pain points in Tier 1 processes.

EDUCATION

05/2022 – 12/2022
PROJECT MANAGEMENT, GEORGIAN COLLEGE

05/2021 – 12/2021
COMPUTER APPLICATION SECURITY, CONESTOGA COLLEGE

08/2016 – 09/2020
BACHELOR OF TECHNOLOGY - COMPUTER SCIENCE, GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY

SKILLS

- Python
- Bash
- Javascript
- Automation
- Scripting
- Incident Response
- Penetration Testing
- Linux
- Web Development
- Threat Intel
- Malware Analysis

PROJECTS

ACENKA

- Acenka is a vulnerability scanner for websites using CMS services.
- Built to test common CMS services for vulnerabilities.
- Technologies Used - Python, JavaScript, Flask, Linux tools.

RCOIN
- Implemented a blockchain based hotel booking application.
- This project was made as a submission to Rajasthan Hackathon 2018.
- Technologies used - Solidity, HTML/CSS, JavaScript, jQuery.

ACHIEVEMENTS

- Ranked Hacker in HackTheBox; Top 13% in TryHackMe
- 2nd Runner Up @ HackNSIT
- 2nd Runner Up @ EncryptCTF
- Rank 225 @ MITRE CTF
- Certified PNPT
- Certified PWPA

INTERESTS

- Gaming
- Programming
- Reading
- Chess
- Martial Arts
- Football
- CTF events
- Pentesting