Chris Kosmas

Information Security Professional

I have over 10 years of experience in incident response, threat detection, and security testing. I love solving difficult challenges, sharing what I know, and learning something new every day.

chris@ckosmas.com

847-372-4600

Greater Chicago Area

ckosmas.com

WORK EXPERIENCE

Incident, Response & Forensics Analyst
Kirkland & Ellis, LLP

02/2024 - Present *Chicago, Illinois*

Achievements/Tasks

- Manage technical aspects of security incidents and conduct intelligence gathering analysis of adversary tactics and strategies
- Conduct investigations on highly sensitive matters, insider threats, HR related events and other non-traditional security incidents
- Lead 3rd party Red and Purple team projects
- Conduct weekly threat hunts to find and remediate security issues traditional security tools won't catch
- Create, process, tune, document and hand off alert configurations in various security tools to operations team to action

Cyber Security Engineer
Kirkland & Ellis, LLP

01/2022 - 02/2024 *Chicago, Illinois*

Achievements/Tasks

- Performed technical risk assessments for IT projects, technologies, web applications and third-party vendors
- Identified vulnerabilities and worked with various teams to remediate

Consulting Engineer (Penetration Testing)
CDW

09/2019 - 01/2022 *Remote*

Achievements/Tasks

- Conducted external/internal network, wireless, social engineering, web app, and cloud penetration tests on customer environments in different industry verticals

Cyber Threat Engineer
Trustwave

04/2019 - 09/2019 *Chicago, Illinois*

Achievements/Tasks

- Reviewed logs from SIEM, firewall, and EDR devices daily to identify and remediate potential threats in customer environments

Security Analyst
Sirius Computer Solutions

07/2016 - 04/2019 *Skokie, Illinois*

Achievements/Tasks

- Supported multi-million dollar customer network and security infrastructure tool implementations

SKILLS

Incident Response | Penetration Testing | Forensics | Threat Hunting | Red Teaming | Purple Teaming | Detection Engineering | Malware Reverse Engineering | Exploitation | Threat Intelligence | Cloud | Networking | Operating Systems | Scripting | Active Directory | Vulnerability Management | Risk Assessments | Cybersecurity Frameworks | Security Awareness | Project Management | Technical Writing | Executive Communication | Consulting | Customer Service | Mentorship

PERSONAL PROJECTS

ChatGPT Memory Forensics Research Project

- Conducted a research project that investigates memory forensic artifacts left behind by the web-based version of ChatGPT. Link to my research paper: https://www.sans.org/white-papers/scrutinizing-web-based-llm-private-browsing-mode-analysis-memory-artifacts-privacy-implications

Virtual Hacking Labs

- Practiced penetration testing against vulnerable virtual machines on TryHackMe. Link to my profile: https://tryhackme.com/p/thrylos

Active Directory Lab

- Created mini Active Directory domain in VMware Workstation comprised of one Windows domain controller, one Windows Server, and two Windows Clients to learn administration and penetration testing.

EDUCATION

Master of Science, Information Security Engineering
SANS Technology Institute

Bachelor of Science, IS/IT and Marketing
University of Illinois at Urbana-Champaign

CERTIFICATES

GIAC Security Expert (GSE)
https://www.giac.org/certified-professional/Chris-Kosmas/221562