Chris Kosmas

Information Security Professional

My objective is to contribute to the Information Security profession through mentorship, knowledge sharing and maintaining a positive attitude. I am extremely passionate about this field and look forward to overcoming the daily challenges I face. That makes the smallest successes that much more rewarding.

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

- Help manage 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
- Manage 3rd party Red and Purple teaming projects
- Conduct weekly threat hunts to find and remediate security issues
- Create, process, tune, document and hand off alert configurations in various security devices 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 - InfoSec
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

Analyst - Professional Services
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 | 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

EDUCATION

Master of Science, Information Security Engineering
SANS Technology Institute

05/2023 - Present

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

08/2012 - 05/2016

CERTIFICATES

CISSP - (ISC)² Certified Information Systems Security Professional
https://www.credly.com/earner/earned/badge/ad3e139e-bc86-4d06-8d60-45bd623b78fa

CCSP - (ISC)² Certified Cloud Security Professional
https://www.credly.com/badges/1ae8966d-c409-4c10-a541-04c98d6400a8

GIAC x 11 (GSEC, GCIH, GSTRT, GDSA, GCIA, GSLC, GCFA, GX-CS, GX-IH, GX-IA, GSP)
https://www.giac.org/certified-professional/Chris-Kosmas/221562

SANS Security Awareness Professional (SSAP)
https://www.credly.com/badges/b4c846d8-a277-4c0c-9dc9-ffd0e2b7442c