

Chris Kosmas

Information Security Professional

I have over 10 years of experience in various technical information security roles. I love solving difficult problems, sharing what I know, and learning something new every day.

chris@ckosmas.com

847-372-4600

Greater Chicago Area

ckosmas.com

WORK EXPERIENCE

HUNT Analyst

Kirkland & Ellis

01/2022 - Present

Chicago, Illinois

Achievements/Tasks

- Incident Response and Threat Intelligence - manage technical aspects of security incidents and conduct intelligence gathering analysis of adversary tactics and strategies
- Investigations - conduct investigations on highly sensitive matters, insider threats, HR related events and other non-traditional security incidents
- Security Assessments - lead Red and Purple team projects
- Threat Hunting - conduct weekly threat hunts to identify and remediate issues traditional security tools won't find
- Detection Engineering - create, process, tune, document and hand off alert configurations in various security tools to operations team to action
- Technical risk assessments - performed technical risk assessments for IT projects, technologies, web applications and third-party vendors
- Vulnerability management - identified vulnerabilities and worked with various teams to remediate

Consulting Engineer

CDW

09/2019 - 01/2022

Remote

Achievements/Tasks

- Penetration Testing - conducted network, wireless, social engineering, web app, and cloud penetration tests

Cyber Threat Engineer

Trustwave

04/2019 - 09/2019

Chicago, Illinois

Achievements/Tasks

- Security Operations - 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

- Engineering - 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.

Virtual Hacking Labs

- Practiced penetration testing against vulnerable virtual environments on [TryHackMe](#).

Security Blog

- Maintained an information security blog about interesting topics on my [website](#).

Azure Sandbox

- Built out an Azure Sandbox environment to test various cloud configurations and implementation best practices.

Active Directory Home Lab

- Created and maintained a small Active Directory environment in my home lab comprised of one domain controller, one server and two workstations.

EDUCATION AND CERTIFICATIONS

SANS Technology Institute - Master of Science, Information Security Engineering (05/2023 - 11/2025)

University of Illinois Urbana-Champaign - Bachelor of Science, IS/IT and Marketing (08/2012 - 05/2016)

GIAC - GIAC Security Expert (GSE) (11/2024 - Present)

ISC2 - Certified Information Systems Security Professional (CISSP) (07/2020 - 10/2025)