

## 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 (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

### 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

### Virtual Hacking Labs

- Practiced penetration testing against vulnerable virtual machines on TryHackMe and Hack the Box platforms. Created write-ups to share with colleagues and friends.

## EDUCATION

### Master of Science, Information Security Engineering

SANS Technology Institute

05/2023 - esent

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

08/2012 - 05/2016

## CERTIFICATES

CISSP - (ISC)<sup>2</sup> Certified Information Systems Security Professional

<https://www.credly.com/badges/ad3e139e-bc86-4d06-8d60-45bd623b78fa>

GIAC Security Expert (GSE)

<https://www.giac.org/certified-professional/Chris-Kosmas/221562>