James Espinosa

SECURITY ENGINEER, DETECTION & RESPONSE

Profile

Security practitioner with over 5+ years of combined security experience, including responding to data breaches on behalf of organizations ranging from startups to Fortune 500 corporations. Experience leading incident response investigations and mentoring junior consultants and security analysts.

Employment History

Security Engineer, Cloudflare, San Francisco, CA

MARCH 2019 — PRESENT

- Build and deploy tools to help increase detection signal and improve response.
- Lead program development for detection in our production environment.

Incident Response Lead, TransUnion, Chicago, IL

APRIL 2018 — NOVEMBER 2018

- Lead Tier 3 security incident response efforts and mentored Tier 2 analysts.
- Revamped response playbooks for the Security Operations Center (SOC).
- Designed workflows to help automate incident response playbooks.

Principal Consultant, The Crypsis Group, Chicago, IL

MAY 2016 — APRIL 2018

- Lead breach response investigations and coordinated with client, legal, insurer, and both technical and non-technical resources.
- Mentored junior consultants in incident response and computer forensics.

Consultant, Mandiant, A FireEye Company, Westchester, IL

JULY 2015 — APRIL 2016

- Conducted large-scale investigations and examined endpoint and network sources of evidence for the presence of attacker activity.
- Conducted enterprise-wide searches for indicators of compromise.

Security Researcher, SpiderLabs, Trustwave, Chicago, IL

OCTOBER 2012 — JULY 2015

- Analyzed malware, exploits, malicious network traffic, and network-based vulnerabilities for signature development and to support the IR team.
- Researched vulnerabilities and the mechanisms for detecting their presence on remote systems.

Education

Bachelor of Science, DePaul University, Chicago, IL

SEPTEMBER 2010 — JULY 2013

Information Assurance & Security Engineering

Certifications

GIAC Certified Forensic Analyst (GCFA)

JANUARY 2019 — JANUARY 2023

License #15054

Details

San Francisco, CA
(847) 687-4793
jamesejr@gmail.com

Links

Homepage

LinkedIn

GitHub

Skills

- Incident Response
- Computer Forensics
- Threat Detection
- Threat Hunting
- Response Automation
- Computer Programming

Languages

- English
- Spanish

Hobbies

Music production, photography, cooking, reading, hiking, and traveling.