James Michael Rylander

California USA
jamesmrylander@gmail.com
https://github.com/jamesryla

CYBERSECURITY PROJECTS

Splunk with Sysmon & IIS logs to track Conti ransomware

Conducted a comprehensive tabletop exercise simulating a Conti ransomware attack, documenting critical insights and leveraging Splunk to trace the APT's movements.

Splunk with Sysmon logs to track Blacksun ransomware

Simulated an APT attack by the Blacksun group, leveraging Splunk to monitor and analyze threat activities, while documenting key findings and refining SIEM usage for improved threat detection.

EXPERIENCE

Self Employed Remote — *Private Tutor*

2017 - PRESENT

Private tutor multiple students in daily high school education, prepare students for TOEFL and IELTS English examinations and university, maintain communication with schools to ensure student's attendance & grades & work with parents to reach educational goals for their children.

Guitar Center San Marcos, CA — *Operations Lead*

2015 - 2018

Inventory, shipping & receiving, cash handling, inventory systems management, team management, scheduling, logistics.

Field Report Collective Portland, OR — *Project Manager/Business Development Manager*

2013 - 2015

Sales, photo & video content creation, project management (basecamp, asana), proposal & contract writing, project scheduling, social media management (in house & clients).

Asian Art Museum San Francisco, CA — *Store Associate (temporary position)*

2012 - 2012

Sales, inventory, visual merchandising, membership management.

Museum of Photographic Arts, San Diego, CA — *Store Coordinator, Exhibit Preparator + Product Photographer*

2009 - 2011

Maintain store inventory, produce P.O.'s & receiving vouchers, maintain positive relationship with vendors, produce change orders, create new displays, maintain store website, write product descriptions for webstore, run & maintain physical gallery, membership sales, installation staff for new exhibits, art handling.

EDUCATION

Academy of Art University — San Francisco, CA

2011 - 2012

CERTIFICATIONS

Security+ Certification
CompTIA - February 2024

Digital Forensics Basics
Texas A&M - Engineering Extension Service - January 2023

TryHackMe Enthusiast
Top 700 users, over 400 rooms completed.

SKILLS

Blue Team Focused:
Experienced in utilizing SIEM systems for real-time threat detection and response. Proficient in implementing and aligning security strategies with industry-standard defense frameworks. Adept at leveraging threat intelligence to proactively identify and mitigate potential risks.

Detail-Oriented:
Excellent communication skills, both verbal and written. Strong ability to prioritize tasks, manage time effectively and organize responsibilities efficiently.