Jordan Rivera

Senior SOC Analyst

jordan.rivera@email.com | (555) 890-1234 | linkedin.com/in/jordanrivera

SUMMARY

Experienced Senior SOC Analyst with 6+ years of expertise in threat detection, incident response, and security operations. Proven track record of identifying advanced threats and leading incident response efforts.

SKILLS

Advanced SIEM Management | Threat Hunting | Malware Analysis | Incident Response | Digital Forensics | Threat Intelligence | Security Automation | Team Leadership

PROFESSIONAL EXPERIENCE

Senior SOC Analyst - CyberDefense Solutions

Jun 2020 - Present

- Lead a team of 5 SOC analysts in 24/7 security monitoring operations
- Developed advanced detection rules that improved threat detection by 40%
- Conducted in-depth investigations of complex security incidents
- Implemented security automation that reduced false positives by 60%
- Mentored junior analysts and developed training materials

SOC Analyst - SecureTech Inc.

Mar 2017 - May 2020

- Monitored and analyzed security alerts from multiple sources
- Performed incident response for various security events
- Conducted regular threat hunting exercises
- Created comprehensive documentation for incident handling procedures

Security Operations Specialist - Global Security Services

Jan 2015 - Feb 2017

- Monitored network traffic and system logs for security incidents
- Assisted in vulnerability assessments and penetration testing
- Implemented security controls based on best practices
- Participated in incident response activities

EDUCATION

Master of Science in Cybersecurity

Technical University, 2013 - 2015

Bachelor of Science in Information Technology

State University, 2009 - 2013

CERTIFICATIONS

- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Forensic Analyst (GCFA)
- Certified Information Systems Security Professional (CISSP)
- Offensive Security Certified Professional (OSCP)

PROJECTS

Threat Hunting Framework

Developed comprehensive threat hunting framework adopted by multiple teams

SIEM Enhancement Project

Led project to optimize SIEM deployment, reducing alert fatigue by 50%

Security Automation Platform

Implemented SOAR platform for automated incident response workflows