

Morgan Taylor

Senior Security Analyst

morgan.taylor@email.com | (555) 789-0123 | linkedin.com/in/morgantaylor

SUMMARY

Experienced Senior Security Analyst with 7+ years of expertise in threat detection, incident response, and security operations. Proven track record of identifying advanced threats and leading incident response efforts to protect organizational assets.

SKILLS

Advanced SIEM Management | Threat Hunting | Malware Analysis | Incident Response | Digital Forensics | Threat Intelligence | Security Automation | Team Leadership | Risk Assessment | Compliance (NIST, ISO, GDPR)

PROFESSIONAL EXPERIENCE

Senior Security Analyst - CyberDefense Solutions

Jun 2020 - Present

- Lead a team of 6 security analysts in 24/7 SOC operations
- Developed advanced detection rules that improved threat detection by 45%
- Led incident response for major security incidents, including ransomware attacks
- Implemented security automation that reduced false positives by 60%
- Conducted threat hunting exercises that identified previously undetected threats

Security Analyst - SecureTech Inc.

Mar 2017 - May 2020

- Monitored and analyzed security alerts from multiple sources
- Performed incident response for various security events
- Conducted regular vulnerability assessments and penetration testing
- Created comprehensive documentation for incident handling procedures

Network Security Specialist - Global Security Services

Jan 2015 - Feb 2017

- Monitored network traffic and system logs for security incidents
- Implemented security controls based on best practices
- Assisted in security architecture design
- 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

Specialization in Network Security

CERTIFICATIONS

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

PROJECTS

Threat Hunting Framework

Developed comprehensive threat hunting framework adopted by multiple teams

Security Automation Platform

Implemented SOAR platform for automated incident response workflows

Advanced Persistent Threat Detection

Created detection methodology for identifying sophisticated APT activities