Christopher Gudzak

904-434-4979
ChristopherGudzak@gmail.com
https://github.com/ChristopherGudzak
https://www.linkedin.com/in/christopher-gudzak/

EDUCATION

St. Johns River State College — **AA** - Environmental science
LetsDefend — SOC Analyst Learning Path & Cyber Kill Chain
Hackthebox — SOC Analyst Prerequisites & Linux Fundamentals

CERTIFICATIONS

CompTIA Security+ (Expected 05/25)
Google Cybersecurity Professional Certification
FEMA National Incident Management System (NIMS): ICS-100
SOC Fundamentals course
HTB Academy Linux Fundamentals (Expected 03/25)

PROJECTS

Project: Apply filters to SQL queries **Source:** https://github.com/ChristopherGudzak/Apply-filters-to-SQL-queries
Platforms and Technology Used: SQL - Practical training environment labs (Google)

Project: Password Strength Analyzer **Source:** ChristopherGudzak/Password-Strength-Analyzer: Password Strength Analyzer
Platforms and Technology Used: VS Code & Python

EXPERIENCE

Company: Google Cybersecurity — December 11, 2024
Title: Cyber Security Analyst

- Competent in beginner-level Python, Linux, SQL, Security Information and Event Management (SIEM) tools, and Intrusion Detection Systems (IDS).
- Common cybersecurity risks, threats, and vulnerabilities, as well as the techniques to mitigate.
- Foundational Networking and Network Security
- Assets, Threats, and Vulnerabilities

Company: HackTheBox
Title: SOC Analyst Prerequisites

- Fundamental IT and Information Security | Networking, Linux and Windows operating systems, basic programming and scripting, Assembly.

Company: LetsDefend
Title: SOC Fundamentals

- Log management, Endpoint Detection & Response(EDR), Security Orchestration Automation & Response(SOAR)

SKILLS AND TECHNOLOGIES

- Competent in beginner-level Python, Linux, SQL, Security Information and Event Management (SIEM) tools, and Intrusion Detection Systems (IDS).
- Common cybersecurity risks, threats, and vulnerabilities, as well as the techniques to mitigate.
- Foundational Networking and Network Security
- Assets, Threats, and Vulnerabilities
- Log management, Endpoint Detection & Response(EDR), Security Orchestration Automation & Response(SOAR)
- Fundamental IT and Information Security | Networking, Linux and Windows operating systems, basic programming and scripting, Assembly.
- Fundamental SQL, Queries, Filters

Incident Response & Investigation:

- **Threat hunting** and identifying security incidents
- Analyzing and responding to security breaches
- Developing incident response procedures
- Coordinating with other teams for breach remediation

Communication Skills:

- Strong verbal and written communication for documenting incidents
- Collaboration with other teams, such as incident response, IT, and management

Threat Detection:

- Identifying and responding to security threats, such as Distributed Denial-of-Service (DDoS) attacks, phishing, and malware

Security Event Management:

- Performing log analysis and correlation to detect threats
- Responding to security alerts generated by SIEM or network security systems

Incident Management & Reporting:

- Creating incident reports and documenting findings
- Maintaining accurate logs and history for regulatory compliance (e.g., **GDPR**, **HIPAA**)

Network Security:

- Firewalls
- VPNs and secure network design
- Intrusion detection and prevention (IDS/IPS) systems
-