John Doe

john.doe@example.com linkedin.com/in/johndoe +1-234-567-8901 New York, NY

Professional Summary

Cybersecurity professional with 5+ years of experience in threat detection, incident response, and security automation. Skilled in endpoint protection, detection engineering, and securing cloud environments. Adept at scripting, infrastructure troubleshooting, and collaborating across teams to enhance security postures.

Work Experience

Detection Engineer — ***CyberSafe Inc.*** **Mar 2023 – Present**

- Designed and implemented Python-based integrations for threat intelligence and alert enrichment.
- Built and maintained detection-as-code pipelines using GitHub Actions and CI/CD workflows.
- Created and tested detection rules mapped to the MITRE ATT&CK framework across various platforms.
- Utilized Docker environments to simulate attacks and validate detection logic.
- Led initiatives to automate response playbooks, reducing mean time to resolution (MTTR).

Endpoint Security Analyst — ***SecureTech Solutions*** **Jan 2021 – Feb 2023**

- Conducted threat research on ransomware and created blocklists to prevent endpoint infections.
- Investigated incidents using forensic data, log analysis, and behavioral indicators.
- Managed endpoint policy configurations across Linux/macOS/Windows to maintain compliance.
- Created custom detection rules and automated remediation scripts in Python.
- Served as Linux/macOS SME and authored internal documentation for common incident scenarios.

Cloud Security Support Engineer — ***NetGuard Technologies*** **Aug 2019 – Dec 2020**

- Advised clients on secure cloud deployments and container security best practices.
- Provided technical support for endpoint protection in virtualized (VMware/AWS) environments.
- Conducted root cause analysis of technical security issues and documented resolutions.
- Worked closely with security and development teams to ensure secure platform integration.
- Used tools like Wireshark and TCPDump for incident diagnostics and network forensics.

Previous Roles

IT Support Specialist — *Innovatech Systems* May 2018 – Jul 2019
Technical Support Analyst — *GlobalHelpdesk Co.* Jan 2016 – Apr 2018

Education

B.Sc. in Cybersecurity and Digital Forensics — ***University of Techville*** 2020 – 2022

- Coursework: Network Security (A), Malware Analysis (A), Penetration Testing (B+)
- Capstone: Investigated rootkits and developed a sandboxed malware analysis tool

A.A.S. in Information Systems — ***Tech Community College*** 2016 – 2018

Certifications

- Certified Ethical Hacker (CEH) 2024
- CompTIA Security+ 2023
- AWS Certified Security – Specialty 2023

- Cisco Certified Network Associate (CCNA) 2022

Technical Skills

Detection Engineering • Threat Intelligence • Incident Response • Automation • Endpoint Security • SIEM • Python • Bash • Linux/macOS • Docker • AWS • MITRE ATT&CK • Git/GitHub • Network Forensics

Core Competencies

Security Operations • Troubleshooting • Documentation • Threat Hunting • Collaboration • Root Cause Analysis • Vulnerability Management • Cloud Security • Communication • Process Improvement

Hobbies & Interests

- **Homelabbing**: Deploying virtual labs to simulate attacks and test defenses.
- **Open-Source Contribution**: Participating in GitHub security projects and submitting PRs.
- **Tech Blogging**: Writing about cybersecurity tools and best practices.
- **Hiking and Photography**: Enjoying nature and capturing landscapes on weekends.