Please read this first: Texts in this format are notes and suggestions and should be removed before sending the CV!

Jane Doe

Cybersecurity Analyst

Address: 123 Your Street, Your City, ST 12345
Phone: 123.456.7890
Email: no_reply@example.com
Website(s): (LinkedIn, GitHub, blog, etc.)

Summary

SOC analyst with three years experience monitoring, detecting, investigating and resolving security incidents. Well-versed in configuring SIEM solutions and improving incident response time.

Experience

Cybersecurity analyst (Tier 2) - Company, Location

MONTH 20XX - PRESENT

- Reduced Mean Time to Detect (MTTD) by X% following the incident response plan I put in place.
- Responsible for SIEM tooling operation and administration (Splunk & Elastic).
- Proactively developed SOC tooling, techniques, and processes to improve incident response.
- Collaborated closely with the engineering team with new app developments.

Make quantifiable impact statements when discussing your experience. For example, how many endpoints were you supporting?

Junior cybersecurity analyst - Company, Location

MONTH 2021 - MONTH 2022

- Monitored security incidents in real-time using Wireshark and Splunk.
- Analyzed threats and escalated incidents to Tier 2 analysts for remediation.

- Utilized playbooks, checklists, and online resources for guidance in response to incidents.

For more experienced SOCs, you can remove any previous IT-related experience, such as desk support roles, as this is no longer relevant.

Skills & tools

- Endpoint operating systems (Microsoft, Linux, and Kali).
- Core networking principles.
- Infrastructure security devices (firewalls, proxies, IDS/IPS).
- Supporting enterprise level services.
- Anti-virus, anti-malware, ransomware, data leak protection.
- Vulnerability management, endpoint forensics, and intrusion analysis activities.
- Cloud computing platforms (AWS, Azure, GoogleCloud).
- Python, PowerShell, Bash, Java.

Tooling is important to SOC analysts, especially security information and event management (SIEM) solutions. Ensure you list all relevant tools you are confident in and be prepared to elaborate on them during an interview.

Certifications

- CompTIA N+.
- CompTIA Security+.
- ISC2 SSCP.
- Splunk Core Certified Power User.

Place skills and certifications above education, as practical proof of analyst experience holds more weight.

Education

Bachelor's degree in computer science - School Name, Location

MONTH 20XX - MONTH 20XX