Ethan Mitchell

Cybersecurity Analyst – Tier 2

(312) 555-1234 | ethan.mitchell@example.com | linkedin.com/in/ethanmitchell | 1234 Oak Street, Hines, IL 60141

STRENGTHS

Analytical Thinking
Activity involved breaking down complex cybersecurity incidents, making problems easier to resolve consistently.

Effective Communication
Skills showcase culminated in delivering clear, actionable insights and reports that assisted multiple teams.

Mentorship
Progressed from analysis to guiding junior colleagues, converting complex concepts into digestible knowledge.

Problem-Solving
Showing proficiency in creating solutions rapidly when faced with persistent cyber challenges through collaboration.

Team Collaboration
Contributed meaningfully in cross-functional engagements, ensuring collective efforts efficiently resolved incidents.

SKILLS

Cybersecurity | Incident Response | SIEM Technologies | EDR Solutions | Security Operations Center | Problem Solving | Team Collaboration | Communication Skills | Analytical Skills | Automation Tools | Forensic Analysis | Threat Detection | Report Writing | Risk Management | Documentation

LANGUAGES

English — Native

SUMMARY

Driven cybersecurity professional with over three years of experience focused on incident response and security operations. Skilled in safeguarding digital assets and mitigating cyber threats through the use of advanced technologies, including SIEM and EDR systems. Proficient in leading investigations into incidents while collaborating closely with cross-functional teams for effective management. A strong communicator who documents response strategies clearly to foster team understanding. Enthusiastic about mentoring junior staff, contributing to a knowledgeable work environment, and continuously enhancing operational efficiency.

EXPERIENCE

Cybersecurity Analyst – Tier 2

Innovative Cyber Solutions | January 2024 - Present | Hines, IL

Overseeing incident response efforts within a dynamic Security Operations Center (SOC). Utilizing SIEM and EDR tools for real-time monitoring to swiftly address potential threats.

- Conducted real-time monitoring and triage of security alerts, guaranteeing rapid responses to potential threats.
- Led detailed investigations into cybersecurity incidents, analyzing patterns to provide impactful remediation recommendations.
- Collaborated across IT and forensic teams to optimize incident response strategies, resulting in improved documentation practices.
- Utilized SOAR platforms for automation of incident response processes, significantly increasing operational efficiency.

Cybersecurity Analyst

TechGuard Solutions | June 2021 - December 2023 | Chicago, IL

Played a key role in supporting incident response in a high-volume SOC, addressing alerts and escalations effectively.

- Engaged in managing incident response activities while maintaining situational awareness of security events.
- Developed and maintained detailed incident response documentation and playbooks to enhance team readiness.
- Participated in regular drills simulating cybersecurity scenarios to boost coordination and effectiveness.
- Contributed insights driving improvements in team training programs based on direct incident engagement experiences.

LEADERSHIP & AWARDS

- GIAC Certified Incident Handler (GCIH), 2023
- Exemplary Team Collaboration Award at Innovative Cyber Solutions, 2025

EDUCATION

Bachelor's Degree in Cybersecurity

University of Illinois | GPA: 3.8 | 2021 | Champaign, IL

Coursework: *Network Security, Incident Handling, Threat Analysis, Risk Management*

CERTIFICATIONS

- GIAC Certified Incident Handler | 2023
- EC-Council Certified Ethical Hacker | 2023

TECHNICAL SKILLS

- **SIEM Tools:** Splunk, ELK Stack, IBM QRadar
- **Incident Response Platforms:** ServiceNow, PagerDuty, Rapid7

Spanish Intermediate

MY CAREER

- Cybersecurity Analyst – Tier 2 at Innovative Cyber Solutions (2.3 Years)
- Cybersecurity Analyst at TechGuard Solutions (2.5 Years)

- **Endpoint Detection Reaction:** CrowdStrike, Carbon Black, Microsoft Defender
- **Monitoring Technologies:** Wireshark, Nessus, Snort
- **Soar platforms:** Phantom, Demisto, Runbook Automation
- **Collaboration Tools:** Slack, Microsoft Teams, Zoom
- **Documentation Software:** Confluence, SharePoint, Google Drive
- **Scripting Languages:** Python, Bash, PowerShell
- **Cloud Security Tools:** AWS Security Hub, Azure Sentinel, GCP Security Command Center
- **Network Security:** Firewalls, VPNs, IDS/IPS

PROFESSIONAL AFFILIATIONS

- Member, Cybersecurity Professionals Network
- Volunteer, Local Cyber Safety Initiatives

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST