Matthew Thompson

Cybersecurity Incident Manager

(312) 555-4792 matthew.thompson@example.com linkedin.com/in/matthewthompson 4567 Oak St, Chicago, IL 60614

SUMMARY

Cybersecurity professional with over 6 years of experience in forensics and incident response within dynamic security operations environments. Specializes in utilizing CrowdStrike tools, SIEM, and EDR/XDR technologies to identify, analyze, and remediate cybersecurity threats. Demonstrated ability to lead incident response initiatives, mentor junior analysts, and develop effective incident management processes. Proven track record of enhancing cybersecurity incident handling and reducing response times through continuous improvement efforts and knowledge sharing across teams. Eager to leverage skill set at SecureTech Solutions to ensure operational excellence.

EXPERIENCE

Cybersecurity Incident Manager

Cyber Defense Corp January 2021 - Present Chicago, IL

Lead and manage escalated cybersecurity incidents from detection through resolution in the Security Operations Center. Ensure business impact is minimized through effective containment and remediation efforts.

- Coordinate comprehensive technical teams during incident analysis using EDR/XDR and forensic tools.
- Document and generate detailed post-incident reports while keeping stakeholders informed of actionable insights.
- Improve playbooks and standard operating procedures based on lessons learned from previous incidents.
- Mentor junior analysts, creating a culture of shared knowledge and continuous enhancement in incident handling.

Incident Response Analyst

TechSecure Innovations June 2018 - December 2020 Chicago, IL

Supported the Security Operations Center by managing incident responses, providing vital analytical support that improved overall operational efficiency.

- Collaborated across functions to enhance detection capabilities, leading to a more efficient incident handling framework.
- Conducted thorough security assessments, contributing valuable documentation for incident management processes.
- Participated in team meetings focusing on improvements, gaining recognition as a resource for complex problem-solving.
- Regularly reviewed and improved existing processes to streamline operations further.

Intern Security Analyst

SecureNet Technologies May 2017 - August 2017 Chicago, IL

Assisted in cybersecurity monitoring and attended training programs to improve basic skills needed for future roles in information security.

- Monitored network security alerts assisting in daily reports that informed incident response activities.
- Learnt under senior staff members, absorbing real-world practice techniques in handling immediate threats.
- Participated in developing proactive measures outlined in internal policy documents aimed at preventing threat occurrences.

LEADERSHIP & AWARDS

- Awarded Employee of the Month at Cyber Defense Corp for outstanding contributions to incident resolution.
- Received excellence award from TechSecure Innovations for mentoring junior analysts effectively.

EDUCATION

Bachelor's Degree in Cybersecurity

University of Illinois at Chicago GPA: 3.8 2018 Chicago, IL

Coursework: *Network Security, Risk Management, Incident Response Planning, Digital Forensics*

CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP) 2020
- CrowdStrike Certified Falcon Administrator (CCFA) 2021

TECHNICAL SKILLS

- **Forensic Tools:** FTK Imager, EnCase, X1
- **SIEM Technologies:** Splunk, ArcSight, IBM QRadar
- **Endpoint Detection & Response:** CrowdStrike, Palo Alto Cortex, Microsoft Defender
- **Operating Systems:** Windows, Linux, macOS

- **Scripting Languages:** Python, PowerShell, Bash
- **Networking Protocols:** TCP/IP, UDP, HTTP
- **Virtualization Technologies:** VMware, Hyper-V, Virtual Box
- **Security Frameworks:** NIST, ISO 27001, COBIT
- **Incident Management Systems:** ServiceNow, JIRA, Remedy
- **Threat Intelligence Platforms:** Recorded Future, ThreatConnect, Anomali

SKILLS

- Incident Response
- Forensics
- SIEM
- EDR/XDR
- CrowdStrike
- Documentation
- Team Collaboration
- Process Improvement
- Threat Analysis
- Crisis Management
- Technical Writing
- Cybersecurity Monitoring
- Investigations

PROFESSIONAL AFFILIATIONS

- Member of ISACA (Information Systems Audit and Control Association), promoting best practices in information security.
- Participant in local cybersecurity meetups focusing on knowledge sharing and industry trends.

LANGUAGES

- English (Native)
- Spanish (Proficient)

ADDITIONAL INFORMATION

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

REFERENCES

AVAILABLE ON REQUEST