Matvii Yushchenko

JOBS

1. IT Security Incident Response Manager (SuperbTech, Inc.):

https://www.ziprecruiter.com/c/SuperbTech,-Inc./Job/IT-Security-Incident-Response-Manager/-in-Santa-Ana,CA?jid=1e460bf1366c4d21&lvk=ZGAZQg-u2AZgccFtEKU-Hw.--LnD1bJQdB

2. Incident Response Manager (FireEye):

https://jobs.smartrecruiters.com/FireEyeInc1/743999687531847-incident-response-manager

3. Manager, Information Security Incident Response (Lam Research Corporation):

https://www.disabledperson.com/jobs/31513758-sr-manager-information-security-incident-response

INCIDENT RESPONSE MANAGER POSITION REQUIREMENTS

1. Job Description

The role of the Incident Response Manager is to lead and coordinate the response and recovery activities from information security incidents, and manage function-related business processes. This includes:

- ✓ collaboration with appropriate business partners to analyze and contain information security incidents;
- ✓ establish oversight of information security incidents and communicate analysis, containment, and remediation efforts to all involved partners;
- ✓ determine the root cause of incidents and work with stakeholders and responsible parties to remediate any identified control gaps or failures;
- ✓ escalate issues to management in a timely manner with appropriate information regarding risk, action times, and root cause analysis;
- ✓ maintain and utilize an incident response, recovery plans.

2. Required Education

Bachelor's or Master's degree from an accredited college in Technology related discipline (Computer Science, Engineering, Information Systems, etc.) or equivalent experience/combined education.

3. Required Skills + Working Experience

Required Skills and Experience:

- ✓ 3+ years of experience with Information Security related activities;
- ✓ experience conducting analysis/investigation and containment of potential data breeches or cyber security incidents;
- ✓ ability to lead technical bridge lines to develop quick containment solutions to cyber-security incidents;
- ✓ experience with forensic tools, EDR, MDR, CASB & SIEM/SOAR tools;
- ✓ ability to communicate effectively across all levels of a global financial institution;
- ✓ familiarity with security vulnerabilities, exploits, attacks, malware and digital forensics;
- ✓ ability to manage projects, milestones and deliverables for business-related objectives;
- ✓ experience with ServiceNow or similar security incident management/ticketing systems;
- ✓ in-depth familiarity with most operating systems, particularly UNIX and Windows;
- ✓ understanding of models/frameworks such as Kill Chain and MITRE ATT&CK;
- ✓ ability to review, edit, and manage business critical documentation, requiring strong written and verbal communication skills.

4. Personal Qualities

- ✓ ability to leverage project management skills to effectively budget, scope, and execute engagements;
- ✓ ability to manage multiple projects and manage tight deadlines;
- ✓ public speaking engagement experience;
- ✓ ability to lead a team of highly technical security professionals;
- ✓ strong project management, written, and verbal communication skills;
- ✓ ability to learn quickly.

5. Certification

One or more of the following professional certifications requited:

- ✓ Qualified Security Assessor (QSA)
- ✓ Certified Information Systems Auditor (CISA)
- ✓ Certified Information Systems Security Professionals (CISSP)
- ✓ Certified Information Security Manager (CISM)
- ✓ Certified Information Privacy Professional (CIPP)
- ✓ GIAC Certified Incident Handler (GCIH) or GIAC Network Forensic Analyst.
- ✓ GIAC Certified Forensic Analyst (GCFA)

CISSP, CISM, GCFA, GNFA, GSEC, GCIH professional certifications preferred

6. Salary

As of Nov 2, 2020, the average annual pay for an Incident Response Manager is $142,340 a year.