Incident Response (IR) Lead

About Ideal Integrations

Ideal Integrations build customer loyalty by developing long-term relationships with each of out customers and enables them to realize the highest possible returns on their technology investments.

We accomplish this by offering tailored, best-in-class technology solutions developed by our certified engineers and expert technicians, and by providing premier ongoing customer support.

Incident Response Lead

The Incident Response Lead will be primarily responsible for coordinating and leading investigations and response activities after data breaches or cyberattacks and handle post-incident reviews. The Incident Response Lead will work closely with Project Management, Systems Engineering, and Cloud Services teams in recovery activities. This position will operate in a fast-paced environment and require strong communication and management skills.

Primary Accountabilities:

- Coordinate and lead investigations and response activities with IR analysts
- Work with and coordinate response activities with infrastructure team(s) involved in recovery activities
- Coordinate and lead forensics acquisition efforts
- Ensure all time spent is appropriately placed into the IR management solution on the security side
- Participate in the creation, and maintenance Incident Response Standards, Policies, Procedures, Guidelines, and Checklists
- Provide feedback to current process, procedures, and find ways to actively become better
- Hold Post-Incident reviews to ensure that we continue to improve
- Collecting all IOCs into a single location to ensure we can re-use these IOCs
- Creating scripts, tools, and/or methods to enhance current services and processes
- When not doing IR actively, or the roles above:
    - Help Threat Hunting engagements across all clients
    - Help develop new automated ways to threat hunt clients
    - Create, and provide training to Analysts, Engineers, etc. for how to improve current services
    - Threat Research that is pushed out to the team
    - Mentor SOC staff

Preferred Experience / Skills:

- A minimum 5+ years' experience in SOC / NOC / Blue Team / Red Team / Purple Team environments.
- A minimum 2+ years' experience in Incident Response Methodologies, with hands-on Incident Response experience.
- Experience in Threat Analysis
- Experience in Threat identification
- Direct system remediation
- Experience with EDR solutions
- Experience with log collection
- Experience in running high stress incident calls
- Experience in creating plans for malware eradication
- Strong communication skills
- Some heavy lifting may be required
- Some infrequent travel (up to 15%) may be required.

Certifications:

- We value and respect the We value and respect the following certifications: CFCE, CCE, GCFA, GCFE, GNFA, GREM, GASF, GCIH, EnCE, ACE but they are not required for the role.

Compensation:

- Minimum Salary: $100,000 USD - Final salary will be determined commensurately with cost of living, experience level, and/or any other legally permissible considerations.
- Commission: All employees are eligible for commissions on referred business
- Health, Dental and Vision Insurance
- Life Insurance
- Short-term and Long-term Disability Insurance
- Retirement planning options (Simple IRA)
- PTO/paid holidays
- Annual bonuses
- Remote work opportunities
- Compensation for continued education and professional development (Certs)

Classification Information:

Job Type: Full-time
Reports to: VP of Security Solutions
Date Reviewed: 11/5/2021