Incident Response Consultant

Employment Type
Full-time

Hiring organization
Mandiant (Google Cloud)

Job Location
Reston, VA, USA
Remote work possible

Base Salary
$ 115,000 - $ 170,000

Description

?? Why This Job Matters

Breaches aren't "if," they're "when." That's where you come in. As an **Incident Response Consultant at Mandiant (Google Cloud)**, you'll be the digital firefighter — diving headfirst into breaches, hunting adversaries, and helping Fortune 500s and governments recover fast. If solving puzzles under pressure is your happy place, this is your chance to work with the team that literally *defines* modern incident response.

?? At a Glance

Detail
Info

Estimated Salary Range
$115,000 – $170,000/year (varies by location & experience)

Location
Remote (U.S.) with travel depending on client needs

What You'll Tackle
Breach investigations, digital forensics, malware analysis, threat hunting

Tech You'll Use
EDR tools (CrowdStrike, SentinelOne, etc.), SIEM, forensic toolkits, scripting (Python, PowerShell)

Certs That Help
GCFA, GNFA, GREM, OSCP, CISSP

??? What You'll Do

- Investigate active breaches: uncover attacker footprints and kill their access.
- Perform disk, memory, and log forensics to piece together the attack story.
- Threat hunt across enterprise environments to find stealthy intrusions.
- Develop remediation strategies that clients can actually execute.
- Work shoulder-to-shoulder with client execs to brief them in plain English (not jargon).
- Contribute to playbooks, tooling, and best practices for future IR work.

?? What You Bring

- 3–5+ years of hands-on **incident response, digital forensics, or threat hunting**.
- Solid understanding of attacker tactics (MITRE ATT&CK is basically your second language).
- Comfort with scripting/automation for forensic data crunching.
- Strong written + verbal communication skills (you'll brief CISOs and CEOs).
- Bonus: cloud IR experience (AWS, GCP, Azure), reverse engineering skills.

?? Why Join Mandiant (Google Cloud)?

- You're learning from the best — Mandiant is *the* name in incident response.
- Diverse clients: from Silicon Valley startups to global enterprises.
- Cutting-edge investigations — you'll see novel attacker TTPs first.
- Career growth: move into threat intel, advisory, or leadership roles.
- Culture of sharing, research, and constant leveling up.

? Ready to Jump Into the Fire?

- Update your resume with your best IR war stories.
- Be ready to talk about a breach you've worked and how you cracked it.
- Apply through Mandiant (Google Cloud) careers or via DamnJobs — either way, don't wait.
- Also explore related gigs like **Threat Intelligence Analyst** or **Digital Forensics Specialist**.