Brian Kowalski

Incident Manager

brian.kowalski@email.com (410) 555-0167 Baltimore, MD linkedin.com/in/briankowalski

Summary

Incident Manager with 6 years in federal cybersecurity operations, now running incident response for a 14,000-user civilian agency network. Leads triage, containment and reporting under FISMA standards and an ITIL incident management process. Holds Security+ and GCIH, with hands-on SOC analysis and operating system hardening experience.

Experience

Incident Manager

09/2023 - Present

Chesapeake Federal Cyber Solutions Baltimore, MD

Cybersecurity contractor running the security operations center for a federal agency.

- Lead response on **40+** security incidents a quarter, from phishing to malware, meeting 1-hour federal reporting windows.
- Run major incident bridges with network, server and application teams, restoring service on 92% of P1s within 4 hours.
- Write after-action reports and update incident response playbooks for 12 attack types, including injections and cross-site scripting.
- Compile 6 FISMA incident metrics into a monthly report for the agency's security leadership.

Cybersecurity Analyst

06/2020 - 08/2023

Patapsco Defense Systems Linthicum, MD

Defense contractor with a 24/7 security operations center.

- Monitored SIEM alerts for a 9,000-endpoint defense network, triaging about 150 events a shift.
- Investigated buffer overflow and mobile code alerts, escalating 30 confirmed intrusions for incident response.
- Applied operating system hardening baselines to 400 Windows and Linux servers, lifting STIG compliance from 71% to 93%.
- Drafted computer network defense procedures adopted across 3 SOC shifts.

Education

Bachelor of Science

05/2020

University of Maryland, Baltimore County Baltimore, MD

Information Systems

Skills

- Incident Management
- Incident Response
- Cybersecurity Operations
- ITIL
- FISMA Standards
- Operating System Hardening
- Computer Network Defense
- SIEM
- System Administration
- Communication Skills

Certificates

CompTIA Security+

08/2020

CompTIA

GIAC Certified Incident Handler (GCIH)

11/2022

GIAC

ITIL 4 Foundation

04/2024

PeopleCert