

## Security Operations Center Analyst Iii - Incident Commander

[Apply Now](#)

Company: Gallagher Australia

Location: South Australia

Category: other-general

Overview Gallagher is one of Australia's and the world's largest Insurance broking and risk management companies with over 35,000 employees globally. We pride ourselves on being a socially responsible, ethical and collaborative organisation expressed through our Shared Values, The Gallagher Way. We are also proud to be on the Forbes World's Best Employers list as the only Insurance brokerage. As a SOC Analyst III – (Incident Commander), you will play a crucial role in protecting our organization's digital assets and infrastructure from cyber threats. You will be responsible for promptly detecting, analysing, and responding to security incidents to minimize their impact and prevent future occurrences. This position requires a deep understanding of security operations, incident response methodologies, and advanced threat detection techniques. You will collaborate with cross-functional teams to investigate incidents, perform root cause analysis, and develop proactive measures to enhance our overall security posture. This role reports into the APAC IT Security Manager, with a dotted line into the global Cyber Incident commander. \*This role is open to candidates based anywhere in Australia providing you hold Australian PR and Citizenship.\*

**Key Responsibilities**

- Incident Response Management: Lead and coordinate the organization's incident response activities, ensuring swift and effective incident resolution in accordance with global SOC response procedures
- Monitor security alerts and incidents to identify potential threats, vulnerabilities, and indicators of compromise.
- Perform in-depth analysis of security incidents, including the identification and containment of threats, and recommend appropriate response actions.
- Conduct detailed forensic analysis and investigations to determine the root cause and impact of security incidents.

Develop and maintain incident response playbooks, standard operating procedures, and communication protocols. Threat Detection and Analysis: Utilize security monitoring tools and technologies to identify potential security incidents and breaches. Perform proactive threat hunting activities to detect advanced threats and vulnerabilities in the environment. Conduct analysis of security events and logs to identify patterns, trends, and emerging threats. Collaborate with threat intelligence teams to incorporate external intelligence into detection and response strategies. Incident Mitigation and Recovery: Execute timely and effective containment, eradication, and recovery activities in response to security incidents. Coordinate with IT teams to isolate affected systems, patch vulnerabilities, and implement corrective actions. Assist in system and network hardening activities to improve the overall security posture of the organization. Support business continuity and disaster recovery plans to ensure resilience in the event of a security incident. Incident Reporting and Documentation: Prepare accurate and detailed incident reports, including the description of events, actions taken, and lessons learned. Maintain comprehensive documentation of incident response activities, including evidence collection and preservation. Collaborate with legal and compliance teams to ensure adherence to regulatory requirements and incident reporting obligations. Required skills and experience Bachelor's degree in Computer Science, Information Security, or a related field. Minimum of 6 years of experience in a dedicated incident response role within a Security Operations Centre (SOC) environment. Strong knowledge of incident response methodologies, tools, and industry frameworks (e.g., NIST CSF, MITRE ATT&CK). Knowledge of malware analysis techniques, digital forensics, and memory analysis. Familiarity with cloud security concepts and technologies (e.g., AWS, Azure and GCP). Excellent analytical and problem-solving skills, with the ability to think critically under pressure. Strong communication, stakeholder engagement and interpersonal skills to effectively collaborate with cross-functional teams,. Relevant certifications such as CISSP, GCIH, GCIA, or similar are highly desirable. Knowledge of security frameworks and standards such as ISO 27001, Australian Government PSPF / ISM., NIST, GDPR, PCI DSS. IT framework knowledge: COBIT, ITIL If you are motivated and have a strong desire to learn and succeed in a thriving niche market, this is the rewarding role you have been looking for. If you believe you are the right person for this role, please apply now. For further information please contact us at \*\*\*\*\*. Gallagher offers great benefits and career development opportunities including: Competitive remuneration and excellent incentive program Salary sacrificed superannuation Flexible working options Gallagher Rewards and

discounts at 350+ major retailers Employee Stock Purchase Plan to invest and share in company's growth potential Any offer of employment and subsequent continuing employment is dependent upon the completion of relevant pre-employment background checks. All applicants are required to undergo employment screening through probity checks prior to commencing. Gallagher is an Equal Employment Opportunity (EEO) employer committed to the principles of workplace diversity and inclusion. We welcome all people regardless of ethnicity, faith, sexual orientation, gender identity and lifestyle choices.

[Apply Now](#)

#### Cross References and Citations:

1. [Security Operations Center Analyst Iii - Incident Commander Personaltrainerjobs Jobs South Australia Personaltrainerjobs ↗](#)
2. [Security Operations Center Analyst Iii - Incident Commander KenyajobsJobs South AustraliaKenyajobs ↗](#)
3. [Security Operations Center Analyst Iii - Incident Commander CeojobsJobs South AustraliaCejobs ↗](#)
4. [Security Operations Center Analyst Iii - Incident Commander Viennajobs Jobs South AustraliaViennajobs ↗](#)
5. [Security Operations Center Analyst Iii - Incident Commander Philadelphiajobs Jobs South Australia Philadelphiajobs ↗](#)
6. [Security Operations Center Analyst Iii - Incident Commander Searcheruropeanjobs Jobs South Australia Searcheruropeanjobs ↗](#)
7. [Security Operations Center Analyst Iii - Incident Commander EntertainmentjobsnearmeJobs South Australia Entertainmentjobsnearme ↗](#)
8. [Security Operations Center Analyst Iii - Incident Commander BangkokjobsJobs South AustraliaBangkokjobs ↗](#)
9. [Security Operations Center Analyst Iii - Incident Commander Socialmediajobopportunities Jobs South Australia Socialmediajobopportunities ↗](#)
10. [Security Operations Center Analyst Iii - Incident Commander Russiajobs Jobs South](#)

**AustraliaRussiajobs ↗**

**11. Security Operations Center Analyst Iii - Incident CommanderSearchnzjobs Jobs South AustraliaSearchnzjobs ↗**

**12. Security Operations Center Analyst Iii - Incident CommanderKazakhstanjobs Jobs South Australia Kazakhstanjobs ↗**

**13. Security Operations Center Analyst Iii - Incident CommanderAttorneyjobsJobs South AustraliaAttorneyjobs↗**

**14. Security Operations Center Analyst Iii - Incident CommanderBankingjobsnearme Jobs South Australia Bankingjobsnearme ↗**

**15. Security Operations Center Analyst Iii - Incident CommanderLahorejobs Jobs South AustraliaLahorejobs ↗**

**16. Security Operations Center Analyst Iii - Incident CommanderEnforcementjobsJobs South Australia Enforcementjobs↗**

**17. Security Operations Center Analyst Iii - Incident CommanderSearchaustralianjobs Jobs South Australia Searchaustralianjobs↗**

**18. Security Operations Center Analyst Iii - Incident CommanderMicrobiologistjobs Jobs South Australia Microbiologistjobs ↗**

**19. Security operations center analyst iii - incident commander Jobs South australia ↗**

**20. AMP Version of Security operations center analyst iii - incident commander ↗**

**21. Security operations center analyst iii - incident commander South australia Jobs ↗**

**22. Security operations center analyst iii - incident commander JobsSouth australia ↗**

**23. Security operations center analyst iii - incident commander Job Search ↗**

**24. Security operations center analyst iii - incident commander Search ↗**

**25. Security operations center analyst iii - incident commander Find Jobs ↗**

Source<https://au.expertini.com/jobs/job/security-operations-center-analyst-iii-incident--south-australia-gallagher-australia-2708-40147/>

Generated on: 2024-05-02 by Expertini.Com