Security Engineer

Sydney, New South Wales, Australia

Applications no longer accepted

Job number	1199129
Date posted	Jan 11, 2022
Travel	0-25 %
Profession	Engineering
Role type	Individual Contributor
Employment type	Full-Time

Azure Security Engineering

The vision of the Azure Reliability (AzRel) group is to improve reliability and resilience of Azure services to deliver world class customer experience. We achieve best in class standards by driving operational excellence towards identifying risks, opportunities and thematic issues and ensuring reliability for our customers.AzRel is a vibrant & exciting place to work, but we also understand that people have commitments outside of work. Work-life balance, and flexible work arrangements are all part of the core ethos in Microsoft, and we in AzRel strive to provide a working environment that is inclusive for all. In support our continued and exciting growth we are looking for diverse, experienced Security Incident Engineers to join our evolving Security response capability.As an Azure Security Engineer, you will partner with Azure service teams and key stakeholders to drive security remediation programs, address vulnerabilities, and apply the learnings. Your scope may also include the management of complex, multi-team projects.The successful candidate will have proven experience in responding, resolving, and recovering from cyber security incidents and reporting complex information in briefing to senior stakeholders. You will be experienced in leading and presenting all elements of the Security Response lifecycle including identification, containment, and eradication. You will possess broad technical skills such that you are able to play a key part in understanding the details of the incident to make accurate, informed decisions at both the strategic and technical team lead levels.We are looking for an experienced security engineer to work in a highly collaborative, dynamic environment as part of the team responsible for security incident response at Microsoft. As a member of the incident response team, you will lead detailed investigations and analysis of security-related findings, alerts, and events across the Microsoft Network. You will manage escalations and incidents in close coordination with teams across the Microsoft Cyber Defense Operations Center, security product groups and services. You will have the opportunity to participate in security testing and simulated response.

Responsibilities

- Coordinate appropriate response activities across teams or directly with stakeholders to rapidly remediate potential threats
- Develop playbooks to improve processes and information sharing across teams
- Initiative and project-related support to provide Security Operations and Incident Response perspective and subject matter expertise
- Some after-hours responsibilities and escalations

Qualifications

You will have the following background:

- 2 years of experience in security support operations/engineering, and/or incident response
- Demonstrated experience in computer security related disciplines, including but not limited to the following subject areas: software vulnerabilities and exploitation, host forensics, malware analysis, network traffic analysis, Insider Threat and web-focused security topics. Demonstrated enthusiasm for learning new things and ability to pick up new ideas quickly.
- Knowledge of Microsoft Azure, AWS, GCP or similar cloud computing platforms
- Demonstrated knowledge of common/emerging attacks techniques.
- Knowledge and understanding of co-ordinating cross-organisational responses to security incidents.
- The ability to communicate confidently and clearly on conference calls, in meetings and via email, at all levels of the organization is essential.
- Crisis management skills: able to set priorities, pursue multiple threads at the same time, accurately reflect current state and drive towards desired state.
- Knowledge and understanding of information risk concepts and principles, as a means of relating business needs to security controls.
- Confident in collaborating, building trust and respect with people outside of the immediate team
- Must be able to participate in a multi-location on-call rotation
- Demonstrates maturity and leadership qualities when dealing with conflicting views and difficult conversations
- Candidates must pass the Microsoft Cloud background check upon hire/transfer and every two years thereafter

Preferred, not required:

- Experience in analysing a wide variety of network and host security logs to detect and proactively identify security issues
- Understanding of common threat analysis model's such as the Diamond Model, Cyber Kill Chain, and MITRE ATT&CK
- Software Engineering/Development/Technical Program Management experience
- Solid understanding of system internals on MacOS, Windows, and/or Linux
- Experience automating and/or scripting with Python, PowerShell, C#, or javascript
- Experience working within a diverse organization to gain support for your ideas; Seeks to leverage work of others to increase effectiveness
- Experience building, delivering and supporting extensible, high scale service platforms
- PMP, ITIL, Six Sigma with demonstrated application towards service improvement
- Familiarity/experience with SRE concepts
- Strong reporting and analytics experience

Microsoft is an equal opportunity employer. All qualified applicants will receive consideration for employment without regard to age, ancestry, color, family or medical care leave, gender identity or expression, genetic information, marital status, medical condition, national origin, physical or mental disability, political affiliation, protected veteran status, race, religion, sex (including pregnancy), sexual orientation, or any other characteristic protected by applicable laws, regulations and ordinances. If you need assistance and/or a reasonable accommodation due to a disability during the application or the recruiting process, please send a request via the Accommodation request form.

Life at Microsoft

Culture

We're working together to build strong communities inside and outside the workplace.

Benefits

Microsoft sees the whole person and looks to support your well-being on every level.

Diversity and inclusion

We value individuality. The experiences that have shaped your world view can help us shape ours.