Australia Jobs Expertini®

Principal Security Researcher - Threat Hunting

Apply Now

Company: Microsoft

Location: Australia

Category: computer-and-mathematical

Overview

The mission of Microsoft Security Response Center (MSRC) is to enable Microsoft to build the most trusted devices and services, while keeping our company safe and our data protected. As part of the Microsoft Security organization, and a steward of Microsoft and our customer’s data, a core function of MSRC is ensuring the security of every aspect of the business. MSRC is responsible for company-wide information security and compliance, with a strategic focus on information protection, assessment, awareness, governance, and enterprise business continuity. As customer zero, we deploy and secure these services inside Microsoft and then share best practices with enterprise customers at scale across the globe. We have exciting opportunities for you to innovate, influence, transform, inspire and grow within our organization and we encourage you to apply to learn more!

Do you want to join the Microsoft GHOST team as a Principal Security Researcher?

Do you have an interest in helping Microsoft’s clients defend themselves against targeted exploitation? Are you interested in being intimately involved in the latest, cutting edge developments in the security industry and having a direct impact on the security of all Microsoft customers? Do you want to be on the front lines of helping our customers go toe-to-toe against advanced adversaries? Are you interested in a fast-paced job full of new opportunities? If so, you might be a candidate for the Global Hunting, Oversight, and Strategic Triage team (GHOST).

We are looking for an experienced Principal Security Researcher with required analytical background to join our team to perform threat hunts, assist with investigations, develop threat intelligence, and to cultivate investigation best practices into Microsoft tooling and products. Researchers will support a global team to identify and catalog new attacker Tools, Techniques and Procedures (TTPs), victims, and deliver customer notifications to protect worldwide enterprise customers and empower customers to protect themselves via constantly improving Microsoft products.

We are looking to fill multiple roles across levels.

Our culture is centered on embracing a growth mindset, a theme of inspiring excellence, and encouraging teams and leaders to bring their best each day. In doing so, we create life-changing innovations that impact billions of lives around the world.

Microsoft's mission is to empower every person and every organization on the planet to achieve more.

Qualifications

Required Qualifications:

7+ years experience in large-scale computing, modeling, cybersecurity, and/or anomaly detection

OR Experience with threat hunting/ digital forensics/reverse engineering/incident response etc.OR Master's Degree in Statistics, Mathematics, Computer Science or related field

Other Requirements:

Ability to meet Microsoft, customer and/or government security screening requirements are required for this role. These requirements include but are not limited to the following specialized security screenings: Microsoft Cloud Background Check: This position will be required to pass the Microsoft Cloud background check upon hire/transfer and every two years thereafter.

Preferred Qualifications:

Investigation/Cybersecurity/Digital Forensics/DFIR (Digital Forensic Incident Response) certifications (e.g. Certified Information Systems Security Professional (CISSP), SysAdmin, Audit, Network and Security (SANS), Global Information Assurance Certification (GIAC) etc.)

Technical certifications based on domain (e.g., Azure, SharePoint)

Experience with Active Directory and/or cloud identity

Experience with sophisticated threat actor evidence including familiarity with typical Indicators of Compromise (IOCs), Indicators of Activity (IOAs) and Tools, Techniques and Procedures (TTPs)

Use of forensic analysis tools such as X-Ways Forensics®, WinHex®, Encase®, FTK®, etc.
Microsoft Azure and/or Office365 platform knowledge and experience

Experience with various forensic log artifacts found in Security Informationa and Event Management (SIEM) logs, web server logs, Antivirus (AV) logs, protection logs such as Host-based Intrusion Detection Systerm (HIDS) and Network Intrusion Detection System (NIDS) logs

Familiarity with Microsoft Defender 365 security stack (for Endpoints, Identity, Cloud, etc), especially with Advanced Hunting query writing

Understanding of Windows and Azure internals and where trace evidence can be found

Knowledge of third-party cybersecurity solutions, especially Extended Detection and Response (EDR) and Security Information and Event Management (SIEM) solutions

Experience working with consulting companies is a plus

Linux and/or macOS forensic analysis and threat hunting skills

#GHOST #DSR #MSFTSecurity

Responsibilities

This role is part of a collaborative team, assisting our customers with:
Leading analysis of attacker activity in on-premises and cloud environments

Identifying potential threats, allowing for proactive defence before an actual incident

Notifying customers regarding imminent attacker activity

Providing recommendations to improve customers’ cybersecurity posture going forward and performing threat intelligence knowledge transfer to prepare customers to defend against today’s threat landscape

Building proof-of-concept and prototype threat hunting tools, automations, and new capabilities

Driving product and tooling improvements by conveying learnings from threat hunting and incident response at scale to engineering partner teams

Identifying, prioritizing, and targeting complex security issues that cause negative impact to customers. Creating and driving adoption of relevant mitigations and provide proactive guidance

Collaborating with others to synthesize research findings into recommendations for mitigating security issues and sharing them across teams. Driving change within the team based on the research findings.

If you are looking for a role that will allow you to use your knowledge and experience to strengthen the security posture of customers, you will have a bright future within our Microsoft's Global Hunting Oversight and Strategic Triage team.
Benefits/perks listed below may vary depending on the nature of your employment with Microsoft and the country where you work.Industry leading healthcareEducational resourcesDiscounts on products and servicesSavings and investmentsMaternity and paternity leaveGenerous time awayGiving programsOpportunities to network and connect

Apply Now

Cross References and Citations:

1. Principal Security Researcher - Threat Hunting BollywoodjobsJobs Australia Bollywoodjobs↗

2. Principal Security Researcher - Threat Hunting Teacherjobsnearme Jobs Australia Teacherjobsnearme ↗

3. Principal Security Researcher - Threat Hunting ProtectiveservicejobsJobs Australia Protectiveservicejobs↗

4. Principal Security Researcher - Threat Hunting Johannesburgjobs Jobs Australia Johannesburgjobs↗

5. Principal Security Researcher - Threat Hunting FlightattendantjobsJobs Australia Flightattendantjobs↗

6. Principal Security Researcher - Threat Hunting Jobspro Jobs Australia Jobspro↗

7. Principal Security Researcher - Threat Hunting Losangelesjobs Jobs Australia Losangelesjobs ↗

8. Principal Security Researcher - Threat Hunting GuatemalajobsJobs Australia Guatemalajobs↗

9. Principal Security Researcher - Threat Hunting Zoologyjobs Jobs Australia Zoologyjobs↗

10. Principal Security Researcher - Threat Hunting LebanonjobsJobs Australia Lebanonjobs↗

11. Principal Security Researcher - Threat Hunting Searchcanadajobs Jobs Australia Searchcanadajobs ↗

12. Principal Security Researcher - Threat Hunting Perhourjobs Jobs Australia Perhourjobs↗

13. Principal Security Researcher - Threat Hunting Baghdadjobs Jobs Australia Baghdadjobs ↗

14. Principal Security Researcher - Threat Hunting Canadajobsearch Jobs Australia Canadajobsearch ↗

15. Principal Security Researcher - Threat Hunting PsychiatristjobsnearmeJobs Australia Psychiatristjobsnearme↗

16. Principal Security Researcher - Threat Hunting Studyjobs Jobs Australia Studyjobs ↗

17. Principal Security Researcher - Threat Hunting TransportationjobsJobs Australia Transportationjobs↗

18. Principal Security Researcher - Threat Hunting MontrealjobsJobs Australia Montrealjobs↗

19. Principal security researcher - threat hunting Jobs Australia ↗

20. AMP Version of Principal security researcher - threat hunting ↗

21. Principal security researcher - threat hunting Australia Jobs ↗

22. Principal security researcher - threat hunting Jobs Australia ↗

23. Principal security researcher - threat hunting Job Search ↗

24. Principal security researcher - threat hunting Search ↗

25. Principal security researcher - threat hunting Find Jobs ↗