SR. STAFF SECURITY ENGINEER

Posting ID: EM183063F5  
Company: Barrick Gold  
Position Type: Full-Time  
College Major(s): Electrical/Computer Engineering (EE/CpE), Computer Science (CS)

Company Website: https://www.barrick.com/  
Work Location: Henderson, NV  
Salary: DOE  
College Level(s): Graduate Student, PhD. Student

OVERVIEW

Barrick Digital is seeking a seasoned cyber security engineer with proven understanding in enterprise security focused on building tool sets and processes to support the Information Security Program (ISP). This role will be a driving force behind the adoption of new security technologies rooted in behavioral analytics and machine learning. The successful candidate will be a subject matter expert with hands-on experience in a wide range of cloud technologies, tools and methodologies. As a Cyber Security Engineer, you will apply your experience and expertise to better the overall security posture of Barrick by working across teams, business units, and project managers to further the security strategy and address security concerns.

Roles and Responsibilities
This is a hands-on technical role that will provide the right candidate an exciting opportunity to leverage and grow technical, process and leadership skills in an exciting area of the company.

- Foster a security-centric and consultative relationship with the business, mine sites, and other IT teams.
- Recommend, implement and support solutions to improve Barrick’s security posture.
- Review, maintain and administer security policies, procedures, and other documentation.
- Provide consultation, architecture to project teams on security best practices and security design requirements.
- Design, implement, and manage security practices and solutions for servers, infrastructure, workstations, mobile devices, and industrial control systems, perimeter defense, and other common enterprise technologies.
- Manage logging and analytics, firewalls, IPS, AV, spam and URL filtering, and other security-specific tools.
- Manage security practices and protection for end-users, including email, web access, anti-virus, and other common endpoint solutions.
- Approve and administer user accounts, permissions, and access rights.
- Manage and respond to security related incidents and investigations for all Barrick sites.
- Conduct research on products, services, protocols, and standards to remain abreast of developments in the technology industry.
• Research, implement, and manage the security of cloud-based technologies.
• Conduct risk assessments, including vendor risk.
• Perform vulnerability scans and ensure appropriate remediation activities are fulfilled.
• Develop and deliver security training across the company.
• Perform other security functions or tasks as directed.
• Experience in threat modeling and risk identification.
• Experience in security vulnerability assessments and remediation techniques.

Education and Qualifications
• Bachelor’s Degree in Computer Science or in “STEM” Majors (Science, Technology, Engineering and Math)
• 8+ years’ experience in Information Technology
• 6 + years’ experience in Cyber Security engineering and support

Eligibility Requirements:
• Legal authorization to work in the U.S. is required.
• Must be willing to travel
• Must be willing to work out of an office located in Northern Virginia, DC Area

Technical Expertise:
• Minimum of 5 years of experience with detection technologies (e.g. Snort, Suricata, Bro, netsniff)
• Minimum of 4 years of experience with scripting languages (e.g. Ruby, Python, Perl, and Powershell)
• Minimum of 2 years of experience with cloud technologies (e.g. AWS, Azure, OpenStack)
• Minimum of 1 year of experience with secure development life-cycles
• Minimum of 1 year of experience with identity management and authentication
• 5-7 years of experience administering Windows and Unix-like operating systems (e.g. Linux, OSX)
• 5-7 years’ experience administering orchestration tools such as Puppet, SALTStack, Chef, or Ansible
• Experience in computer security incident response, including forensic investigations and chain of custody
• Experience with CheckPoint (R80) and Cisco ASA firewalls.
• Experience with Cisco AMP and Cisco Email Security Appliances
• Experience with multifactor authentication mechanisms
• Experience with the Cisco networking technology stack, including VPN
• Experience in Enterprise logging, log analysis and correlation engines
• Nice to have familiarity with industrial control systems Cyber Security norms and standards (IEC62443, NERC-CIP, ANSSI, ISO 27k…)
• Prior experience working within an Agile framework (Scrum/Kanban)
• One or more Security Certifications or equivalent (CISSP, etc.)
• One or more Platform Certifications or equivalent (RHCE, LFCE, etc)
• Knowledge of CI/CD and automation tools (Chef, Git, Jenkins)
• Experience in securing cloud infrastructure such as AWS, Azure and alike (i.e., inspection, logging, WAF, VM)
• Experience in deployment of cloud controls for infrastructure, platform, and applications (IaaS/SaaS/PaaS), specifically within AWS, Azure and GCP
• Familiarity with data analytics and machine learning principles and techniques
• Knowledge of SIEM API integration techniques
Business Acumen:
● Strong problem-solving abilities and capable of articulating specific technical topics or assignments
● Experience in building scalable and highly available distributed systems
● Expert in breaking down problems and estimate time for development tasks
● Evangelizes how our technology solves customer problems from a technology and business perspective

Personal Attributes:
● Able to work under minimal supervision
● Excellent communication skills and the ability to interface with senior leadership with confidence and clarity
● Must have proven verbal communications and written documentation skills
● Able to work well with global teams, including time-zone flexibility
● Skilled in providing oversight and mentoring team members. Shows ability to effectively delegate work

How to Apply
Go to: https://jobs.barrick.com/jobs/sr-staff-security-engineer-2625