MORE THAN TV

Job Description			
Job title:	Junior Cloud Security Engineer	Reporting to:	Head of Security Operations
Division:	Group Tech	Department:	Cyber Security
Status: *(Staff/ FT contract/ Freelance/ Placement)*	FT	Based at:	GIR
Hours:	37.5	Probationary period:	3 months
Suitable for P/T or Jobshare?	No	Reports to: Direct Reports:	Head of Security Operations
Team structure: *(or diagram to show how this job fits with other roles)*	This role will report to the Head of Security Operations This role will be working very closely with our Platform, On-Demand and Content Delivery Engineering teams, and will drive security capability innovation that will expand into the rest of ITV. It's a new role and you will have the freedom to influence many key technical security decisions and really make a difference to our 'More than TV' digital strategy.		
Main purpose of role:	At ITV, we want to be the digitally led company that brings brilliant content to global audiences wherever, whenever and however they choose. In order to achieve our ambition we need to think outside of the box to offer a highly agile, reliable, and scalable platform for our product engineering teams that delivers security by design without compromise. If this is something that excites you read on... This is a hands-on role, developing and maintaining the right security tools to provide high levels of security assurance across ITV Cloud Platforms. You will work with developers across ITV to ensure that security is built in from the start and integrated into our CI/CD pipelines without restricting agility or innovation. You will champion security throughout the engineering teams so that security tooling is simple, scalable and highlighly effective for engineers and developers to use. The role will also align closely with, and leverage the experience of the wider cyber security team particularly when investigating incidents.		

	This is an ideal role for someone looking for the space to develop their DevSecOps skills and wanting the challenge to help define ITV’s cloud security engineering and cyber security capabilities.
Qualifications / Professional certificate	We recognise that real world security experience is worth more than bits of paper, but if you do hold any of the qualifications below or anything else that is relevant, we will of course like to understand where and you have applied your knowledge. ● Technical related Bachelor's Degree (Computer Science or Engineering) ● AWS Certified SysOps Administrator ● AWS Certified DevOps Engineer ● AWS Certified Security - Specialty ● Google Cloud Security Engineer ● Certified Kubernetes Administrator ● Certificate of Cloud Security Knowledge (Cloud Security Alliance) ● Certified Information Systems Security Professional (ISC)^2 ● SANS Security certifications ● Certified Cloud Security Professional (ISC)^2
Key responsibilities (not all of them just the important stuff!)	Help define and embed technical security principles and standards though code Help develop, maintain and automate security tools Proactively identify vulnerabilities, provide solutions and drive remediation (ideally through automation runbooks) Continuously look for ways to improve the security capability Help in the response to security incidents across our cloud platforms Work with our Managed Security Solutions Partner (MSSP) to develop innovative ways to monitor and respond to threats across multiple Cloud platforms Support the Cyber team with automating existing enterprise wide security tools and contribute to developing innovative integrations with existing tools to orchestrate and automate security processes.
Key criteria that we will shortlist & assess candidates against: i.e. skills/knowledge/experience	1. Willingness to learn and a passion for cyber security 2. Some hands on experience in at least one of the following; Azure, GCP or AWS in a professional capacity or personal projects 3. Use of automation to solve complex problems at scale 4. Think outside the box to help embed security with agility and scalability in mind 5. Ability to solve complex technical challenges in a collaborative way 6. Willingness to learn about addressing security in VMs, containers and serverless 7. Some experience with security dashboards is a plus 8. Understand the concepts of deploying Policy as Code and container scanning, 9. Understand the concepts of hardening environments and K8s
Characteristics	- Be inquisitive, empathetic but also be able to help with technical direction - Self starter with a passion for security

	- Critical thinking with a deeply analytical mind - Seek out challenges and be solution orientated - A clear communicator able to articulate technical security risk to technical and non-technical audiences both in verbal and written form - Highly collaborative and able to influence within engineering teams
Unusual challenges or circumstances: *(e.g. travel, hours of work, short notice cover)*	The role can be based in London, Manchester or Leeds, but you will be expected to travel periodically to our Hub sites
Technical Keywords to use for search	The tools listed below are examples or tooling at ITV or tooling that we are looking to invest in. Candidates are not expected to have used all of the listed tools but are expected to have had solid hands on experience with equivalents that achieve the same outcomes. Candidates should be comfortable adapting their knowledge quickly to new tooling. Cloud providers: **Amazon Web Services (AWS)** (Preferred), **Google Cloud Platform** (GCP) (Preferred), Microsoft Azure (nice to have) Infrastructure as code tools: **Terraform** (Preferred), Google Deployment Manager, AWS Cloud Formation Infrastructure: EC2, **EKS, Kubernetes (Preferred)**, Load balancing, Serverless technologies (Lambda) Configuration Management tools: Puppet, Ansible, Chef Systems Management tools: ELK stack (centralised logging), TIG stack (centralised monitoring), sensu (alerting), CloudWatch, CloudTrail, Investigator Comfortable with programming languages & scripting: Scala, ruby, NodeJS, Java SDLC tools: Checkmarx, Snyk, Vericode, OWASP ZAP, LGTM, GITScanner, SourceClear, Sonarqube Other tools: **GitHub (preferred)**, gitlab, jira, trello, CIS benchmark, AWS well architected tool