



Splunk Engineer


Whizdom Recruitment • Canberra City ACT 2601

 *Not provided*

 Work type
Full time

 Contract type
Contract


Job details

 Date posted
20 May 2022

 Expired On
19 Jul 2022

 Category
Information Technology

 Occupation
Software Engineering

 Base pay
Not provided

 Contract type
Contract

 Work type
Full time

 Job mode
Standard business hours

Work Authorisation
 **AUSTRALIAN CITIZEN /
PERMANENT RESIDENT**

Skills

SCRIPTING

CONTINUOUS IMPROVEMENT

GATHER REQUIREMENTS

LARGE-SCALE

NETWORK MONITORING

OPERATIONS

PRODUCT MANAGEMENT

SCHEDULE+

STRUCTURED SOFTWARE

Full job description

Overview

Our client is currently seeking a Splunk Engineer for development of a new Splunk environment as part of a large-scale build project. The Splunk Engineer will work closely with the infrastructure and application teams to gather requirements and develop the Splunk solution. The ideal candidate will be mission focused and have the ability to work as part of a multi-disciplinary team working closely with the client on a rewarding development project.

You will have a background in delivering complex solutions to achieve a successful outcome. A minimum of 3 years' experience working as a Splunk Engineer is preferred.

- Deploy a new Splunk instance and configure it for log ingestion.
- Mapping data to Splunk Common Information Model.
- Onboarding log sources.

- Develop Splunk alerts, dashboards and reports.
- Assist and provide expertise on best practices in integrating Splunk to monitor a hybrid cloud environment.
- Participate in workshops to capture requirements and design the Splunk solution.
- Act as the Splunk liaison for Splunk technical questions, issues or escalations. This will include working with Splunk Support, Product Management (i.e. roadmaps), or others as needed.
- Participates in the E2E design, development, integration and testing of platforms and services.
- Conduct backlog refinement and task estimation.

Essential Experience

- Experience deploying Splunk in greenfield environments.
- Proficient in developing in Splunk Processing Language.
- Experience with scripting languages to automate tasks and manipulate data.
- Experience with integrating solutions in a multi-vendor environment, including SaaS products.
- Knowledge of enterprise logging, with a focus on security event logging.
- Experience with enterprise-scale operations and maintenance environments.
- Experience with Python.
- Ability to solve complex technical problems.
- NV1 with the ability to pass additional security assessments.

Desirable Experience

- Splunk Certified Architect.
- Experience in Government Secure Environments.
- Experience working in software development and/or with DevOps teams.
- CI/CD and DevSecOps experience.
- Working in Agile teams.
- Designing or working with network monitoring platforms.
- Designing or working with security monitoring platforms.
- Experience with infrastructure as code development.
- Experience with Automation technologies (Ansible, SaltStack and/or Terraform).
- Network, host, and application-based security knowledge.

Desirable Qualities

- Able to build strong rapport with team members and genuinely care about their success.
- Working to a project schedule and achieve successful client-focused outcomes.
- Understanding of E8 and conforming with ISM requirements.
- Security-first mindset.

- Positive attitude towards change, continuous improvement and incrementally helping others.
- Able to work under broad direction.
- Desire to continue your own learning journey.

Location and Contract Term

This role is based in Canberra with an estimated start date as soon as possible for 12 months with extensions possible.

Security Requirements

Applicants must be Australian Citizens who hold current NV1 security clearance or higher.

How to Apply

Please upload your resume to apply. Applications close Thursday 2 June at 5pm. We will be in touch with instructions for suitably skilled candidates. Call Connie Bellam on 0480 002 453 for any further information.