Vikas Singh
Chandigarh, Chandigarh - Email me on Indeed: indeed.com/r/Vikas-Singh/8644db42854c4f6a

I've 4.6 years of IT experience in Identity and Access Management with Infosys limited. It involves
troubleshooting and resolving workflow errors and provisioning user access. I perform identity
and access management activities, updating existing access and provisioning workflows, manage
operations within the IAM environment. Currently I'm working on automating the work flow of
Security Intelligence and Response Team with Phantom and Python scripting.
I'm trained in Python, Solaris administration, Java and PLSQL. I'm able to handle multiple tasks
and work as a team Member. I've excellent analytical, problem solving and programming skills.
I'm committed; goal oriented, & has zeal to learn new things & technologies.
I am graduated in Electronics and Communication Engineering in 2013 with excellent grades. I
possess good problem solving & interpersonal skills, good communication skills and team spirit.

WORK EXPERIENCE

Technology Analyst

Infosys Limited - Chandigarh, Chandigarh -

October 2013 to Present

A. Change Management:
Installing and upgrading RT and RTIR for improved request handling with MySQL database.

B. Python Automation:
Automating various use cases for the Security Intelligence and Response Team using Python
scripting and Phantom tool integrating it with various tools i.e. Splunk, Request Tracker for
Incident Response (RTIR), Remedy etc.

Below are the use cases details:

Use Cases Description
Proxy Blocks Enable the ability to block domains and URLs automatically on Bluecoat proxies
using a list maintained in SPLUNK
Palo Alto Blocks Enable the ability to block domains and URLs automatically on Palo Alto proxies
using a list maintained in SPLUNK
Threat Intel Email feed ingestion Take emails from an external distribution group and parse the
emails for IOCs
Email Eradication
When a Malicious email has been detected as being received in the Microsoft Exchange email

system perform eradication steps to remove the email from the email messaging platform

Email Quarantine Email addresses alerted as malicious need to be added to a quarantine list
Malware Response When malware is detected by alert or scanning initiate containment
procedures for the affected device in question
Unapproved Devices

https://www.indeed.com/r/Vikas-Singh/8644db42854c4f6a?isid=rex-download&ikw=download-top&co=IN

When alerts for Unapproved Devices, equipment that is not in Organization's asset inventory, is
triggered containment needs to occur for the device in question

IOC Detect and Scanning using Tanium and Fireeye HX
When Indicators of Compromise, IOC, are received from various sources, threat intel feeds,
exploded malware the network environment needs to be scanned for any of the indicators of
compromise provided.

Clear Text Passwords detected
Automatically flag users password to reset in Active Directory when an alert in SPLUNK for a clear
text password detected fires

Create ticket from Splunk or MSSP Alert
Develop a script that takes the details of an alert from an alert generated in SPLUNK and create
or append to a ticket in the ticketing system in use

Triage and Identification Execute the triage and identification steps that are performed manually
today

Information Security Analyst

Infosys Limited - Chandigarh, Chandigarh -

2013 to Present

A. Identity management

Infosys Limited -

May 2014 to December 2017

management May 2014 - Dec 2017

Following are my roles and responsibilities in the project:
A. Identity management:
Tracking and processing identity creation for all the new hires along with basic access e.g.: Email,
Active Directory accounts and including mandatory security related groups. Also, making sure

access is disabled on the user's departure date and cleaning up of all the access. Reviewing
access periodically and updating it accordingly.

B. Access management:
This involves provisioning/de-provisioning access to users across 300+ applications using various
global and in house tools like RSA security console, SAP, Identity IIQ etc. across multiple platforms
like, UNIX, Database and application front end. Making sure standard operative procedures (SOP)
are followed, validation checks are completed and appropriate approvals are gathered before
access is granted.

C. Quality Management:
Performing quality checks on random samples of requests on daily basis and sharing QAP results
with administrators.
- Monitoring and tracking the corrective actions are taken within defined timeframe.

- Doing RCA on major issues
- Developing Service Improvement Plan (SIP) and Process Improvement Plan (PIP) based on the
QAP analysis

D. Risk Management:
Identifying risk areas through daily and periodic report E.g. Segregation of duties violation (SOD)
report, Active directory infraction report etc.
- Working with various teams to mitigate the violations.
- Assisting auditors by provide details and justification on audit samples.

E. Client Coordination:
Coordinating with client daily, weekly for the operations, issues and feedback with the respective
reports prepared.

EDUCATION

Bachelor of Technology in Electronics and Communication Engineering

GLA Institute of Technology and Management - Mathura, Uttar Pradesh

September 2009 to June 2013

SKILLS

SECURITY (5 years), INFORMATION SECURITY (5 years), ACTIVE DIRECTORY (3 years), UNIX
(Less than 1 year)

ADDITIONAL INFORMATION

TECHNICAL SKILLS

- Operating Systems: Windows, Solaris
- Languages: Python, Core Java, SQL, Unix
- Software: Sailpoint IIQ, Oracle IAM, Beeline, SAP, Active Directory, Phantom, Quest change
auditor, Microsoft Office Suite
- Information Security: Concepts and best practices