Recognizing a Company’s Needs

May 6th, 2021

Evan Strickland
Cisco - Technical Leader
HELP ME HELP YOU
What does a Company Need
In a actual position

• Looking at the JD
• Interpreting the JD
• Researching the Company
Looking at the Job Description and exploring

- Not all Job Descriptions are well written
- Treat the job description like a strange new world
- Understand what you desire instead of what is offered
Looking at the Job Description

Just because a Recruiter messed up the post does not mean it is a bad opportunity; but it is worth being cautious.

Career Opportunity!!!

We are working with a large, growing, employee-owned Idquomanaged service provider who is looking to add a junior Security Analyst. If you are looking to grow your career in skills and title, this is a role you seriously want to consider. You will gather client requirements, make recommendations, and install the solution. If you have security scanning experience, that is a plus! This position is salaried plus quarterly bonus AND will pay for certifications and classes that will further your knowledge and skills in your role. Ideally located in Fargo.

Volt is an equal opportunity employer.

<table>
<thead>
<tr>
<th>Seniority Level</th>
<th>Employment Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate</td>
<td>Full-time</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Industry</th>
<th>Job Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Technology &amp; Services, Computer Software, Financial Services</td>
<td>Information Technology</td>
</tr>
</tbody>
</table>
Looking at the Job Description

Junior Security Analyst – JSA01

Stern Security
Raleigh, NC (+1 other)

Apply on Raleigh ISSA

💬 Over 1 month ago  🗓 Full-time  🗳 No degree mentioned

Job Summary

Ready to solidify your role in the security field? This job is for you! The Junior Security Analyst will gain knowledge in a variety of cybersecurity areas and will be expected to eventually grow into additional positions within the company. Some of the main responsibilities will include analyzing vendor security reports, running vulnerability scans, and reviewing threat intelligence.

Job Responsibilities
• Vendor Security Report Reviews
• Vulnerability Scans (Web and Network)
• Other duties as assigned

Job Skills & Qualifications

Required

1. A Security Certification

Great to have

1. IT Background
Looking at the Job Description
well written

Security Analyst
Microsoft • Redmond, WA
Posted 1 week ago • 194 views

Qualifications

Required
- 2+ years’ experience as a data scientist, software engineer, or security researcher
- BS Degree in Computer Science, Electrical & Computer Engineering or Mathematics or equivalent experience

Preferred Qualifications
- Previous experience in any of the following: identity systems, security, threat intelligence, fraud, abuse
- Outstanding math and statistics skills with demonstrated applied machine learning and/or analytics experience
- An ability to drive good decisions through data with great attention to detail and excellent logical problem-solving skills
- Proven experience with rapid prototyping, evaluation, and iterative improvement
- Proficiency with one of more of Python, SQL, Java, C#, C++
- Proficiency in interacting with big data infrastructure and resultant pipelines to perform NRT/batch analytics (e.g. Kafka, Spark, Azure Cosmos DB, HDInsight, Hadoop)
- Graduate degree in computer science, machine learning, statistics, or quantitative domain
- Strong communication skills with a demonstrated bias towards collaboration and team work
Looking at the Job Description

- Support North America in the collection, screening, analysis and dissemination of intelligence related to anti-illicit trade-counterfeit products.
- Facilitate review of online offers of purported client’s products to identify unregistered, misbranded, illegal and/or counterfeit items.
- Utilize open source intelligence (OSINT) tactics and techniques to discover and analyze key data on infringers.
- Set up new websites utilizing internal “crawling” technology to monitor client’s products in the marketplace.

Qualifications

- Bachelor's Degree or equivalent experience as a marketing analyst, brand protection analyst, crime analyst, data analyst or similar intelligence based position.
- MS Office tools (Word, Excel, PowerPoint, Teams, Outlook, etc.)
- Fast learner, team player and able to work under tight schedule and pressure
- Expected to work 30-40 hours per week.

Seniority Level
Associate

Employment Type
Full-time

Industry
Information Technology & Services, Computer Software, Financial Services

Job Functions
Information Technology
Looking at the Job Description
Strange New World

• Understand what is the most important skills and duties for the job

"LADDIE, YOU'RE TALKING TO THE ONLY REDSHIRT WHO ISN'T DEAD."
Looking at the Job Description

strange new world

• This JD wants a pen tester (but calls it an engineer)
Looking at the Job Description
strange new world

<table>
<thead>
<tr>
<th>Operations</th>
<th>Recipe</th>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>binary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>To Binary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>From Binary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BSON deserialise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BSON serialise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CBOR Decode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CBOR Encode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>From BCD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>From MessagePack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>To BCD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>To MessagePack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>YARA Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Favourites</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data format</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption / Encoding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public Key</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arithmetic / Logic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This should be absolutely no problem to decode
Looking at the Job Description

strange new world
Looking at the Job Description
What is Desired?

Minimum qualifications:
- Experience analyzing malicious traffic and building detections.
- Experience in applications security, network security, systems security or malware analysis.
- Experience in a threat intelligence, reverse engineering or related role.

Preferred qualifications:
- Experience analyzing and synthesizing threat intelligence in a high-speed environment.
- Knowledge of the current threat landscape, including common attack types and malware capabilities.
- Proficiency in using reverse engineering tools such as IDA Pro, Windbg, or Ollydbg.

Responsibilities
- Own the analysis efforts of one or more threat actors. Serve as a subject matter expert on how those actors might affect Google Cloud or customers in a specific sector (such as banking and finance).
- Write code (can be in Python, C++, Go) to help automate analyst workflows.
- Reverse engineer and document malware on various platforms. Develop signatures (Yara and custom signature types) and signals (GoogleSQL) to detect malware.
- Write reports about attacker activity, trends, and tactics, techniques and procedures (TTPs). Action requests to support Google Cloud customers incidents and brief on relevant intel as needed in conjunction with main partner teams (Threat Analysis Group, Chronicle, Trust & Safety, etc).
- Triage initial signals, cluster related samples and indicators, and provide a roadmap for addressing larger clusters of previously unknown activity.
Interpreting the Job Description
strange new world

• Understand the audience
  (Hiring Manager/Recruiter)
• Understand the culture
Interpreting the Job Description

Understand Audience

It might be worth replying in binary or base64

This individual is a mid-senior level resource that will be working on a wide variety of cyber security tasks to help organizations reduce risk and mitigate cyber attacks. Your hard work will have direct positive impact on organizations. You will work on penetration testing, vulnerability scanning, vulnerability management, security strategy, and more. This is a unique position that will work with many customers on numerous technologies in addition to contributing to an innovative and internally developed security application for customers. This individual will work on a team with other security professionals and developers.

Job Responsibilities

1. Security Testing, Mitigation, and Management
2. Other duties as assigned

Job Skills & Qualifications

Required
- 2+ years of total cyber security experience
- Penetration Testing experience
- Vulnerability management
- Solid documentation skills
- A cyber security certification
- SIEM Knowledge
- Firewall configuration knowledge
- 01010100 01101000 01101001 01110011 00100000 01110010 01101000 01101000 01101001 01101000 01101000 01110111 01101111 01101000 01101000 01101001 01101001 01100000 01100010 01100011
- 10100000 01101000 01101001 01110011 00100000 01110010 01101000 01101000 01101001 01101000 01101000 01101001 01101001 01101001 01101001 01101001
- 01001001 01101000 01101001 01110011 00100000 01110010 01101000 01101000 01101001 01101000 01101000 01101001 01101001 01101001 01101001 01101001
- 01001001 01101000 01101001 01110011 00100000 01110010 01101000 01101000 01101001 01101000 01101000 01101001 01101001 01101001 01101001
- VGhpcyBzaG9ibGkgYmUgU2tcGxldGhlGwUtZ2FsdGVyIDdhbmcuc2FxdWxsIDBCb3VzaG1vdGVyID0gQ2Fsb2c=

Great to have
- IT Background
- Security Framework experience (ex. MITRE ATT&CK, NIST, PCI, FFIEC CAT)
- Development/Scripting experience
- Forensic & Incident investigation knowledge
- Cloud security experience
Interpreting the Job Description

Understand Culture

• This company appears to be reacting heavily to a specific behaviors

What You’ll Do

• Monitor and react to security events
• Define and implement security policies, procedures, and technologies
• Track general developments in computer security, and plan the firm’s response
• Provide security expertise and advice to other teams within the company
• Define best practices cybersecurity training for employees
• Collaborate with other operations, development, and trading teams to solve business challenges
• Work at a technology-driven company where you can make an immediate impact

What You’ll Need

• Bachelor’s Degree
• Broad understanding of and deep interest in computer security
• Maintain good cybersecurity practices in your own personal life
• Good communication skills, and the ability to explain security best practices to a non-technical audience
• General understanding of computers, networks, operating systems, applications, and the web
• An engineering mindset when approaching new problems
• Willingness and aptitude for learning new skills and adapting to new technologies
• Proficiency with programming or scripting a plus
• Knowledge of finance or trading is not required
• Legal authorization to work in the U.S. is required; we will not sponsor individuals for employment authorization for this job opening
Researching a Company

• Look for clues related to the Job
• Understand the company overall
• Assess the culture

Remember, the company doesn’t know you either, so part of the Job Description is exploratory
I am Sudheer from Honeywell Staffing, I am reaching out for a Full-time open position of Lead Cloud Automation Engineer - Cyber Security that we have open with Honeywell at Atlanta, GA.

Job Title: Lead Cloud Automation Engineer - Cyber Security
Location: Atlanta, GA
Fulltime


Job Description:
- Bachelor of Science degree
- 5 years experience in a security field
- 5 years of scripting experience with Python, PowerShell, Terraform, Ansible in a cloud environment
Honeywell Suffers Cyber-Attack

By Linn Foster Freedman on March 25, 2021

Aerospace and energy equipment manufacturer Honeywell has reportedly been hit with a cyber-attack in the form of a malware intrusion that disrupted some of its information technology systems. Honeywell issued a statement on March 23, 2021, stating that it “took steps to address the incident, including partnering with Microsoft to assess and remediate the situation.”

Honeywell confirmed that it has returned to service and that it has not identified “any evidence that the attacker exfiltrated data from our primary systems that store customer information. If we discover that any customer information was exfiltrated, we will contact those customers directly.”

Manufacturing companies have been hit hard recently with cyber-attacks, which is a wake-up call to evaluate cyber-hygiene and data theft prevention protocols.
Researhing a Company
Understand the Company Overall
Researching a Company
Assess the Culture

• Understand how employees and consumers view a company
where
do we go
from
here?
Raleigh ISSA Chapter Career Services

The Raleigh ISSA Chapter Career Services is here to support Chapter Members in the search for their next career move. Learn interview techniques, job search methods, professional networking, and how to build your resume to land that next security role.

The Raleigh ISSA Chapter also lists local jobs for entry level, mid-career, senior professionals, and security leaders. If you have a job you would like the chapter to post, please send the information to media@raleighissa.org.

Current Open Positions

Junior Security Analyst - JSA01
Stern Security
Raleigh, NC
Posted 1 month ago
Tom Purdy – tepurdy@att.net
Chris Uhlig – Chris.Uhlig@disys.com
Elizabeth Cole-Walker – eacolewa@ncsu.edu
Evan Strickland – tacituacitum@gmail.com
Jon Lee – me@jonlee.us

+++++++  CAREER SERVICE RESOURCES  ++++++++  

Chapter Website -> Jobs Board ->
https://raleigh.issa.org/career-services/
Chapter LinkedIn
https://www.linkedin.com/company/issa-raleigh-chapter
Chapter Facebook
https://www.facebook.com/groups/raleighissa/
Chapter Twitter
https://twitter.com/RaleighISSA
Thank you