



# Unplanned Job Searches

February 2<sup>nd</sup>, 2023

Evan Strickland  
Cisco - Technical Leader



*(chuckles)*  
*I'm in danger.*

## By the numbers

Google  
12,000

Meta:  
11,000

Microsoft:  
10,000

Salesforce:  
8,000

Amazon:  
10,000

Cisco:  
4,100

Carvana:  
4,000

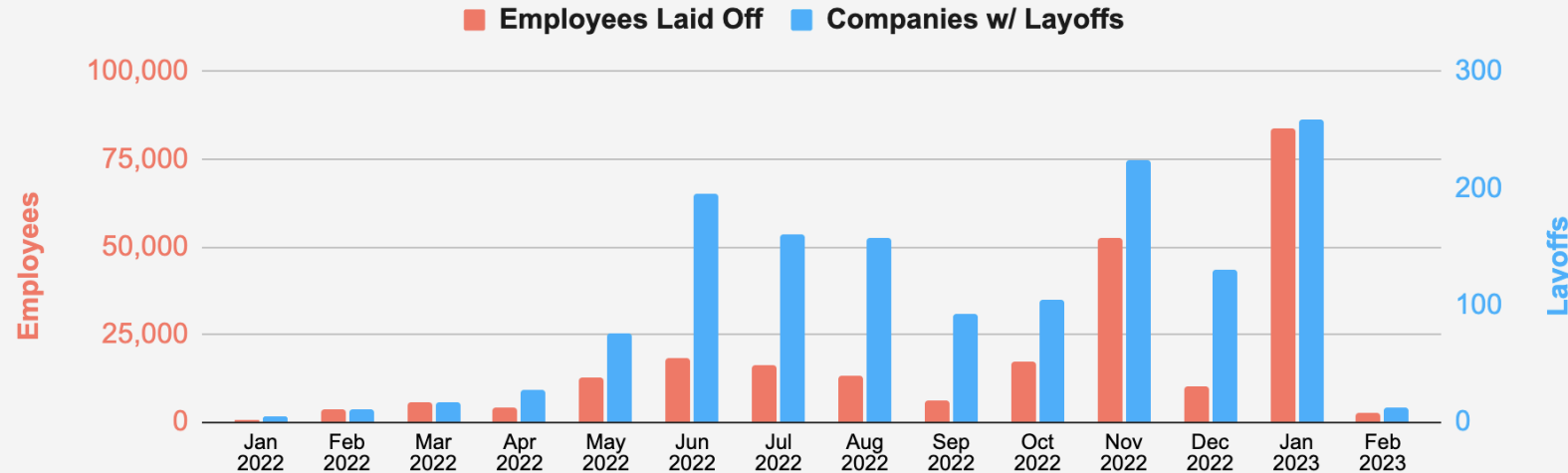
Twitter:  
3,700



# You are not alone

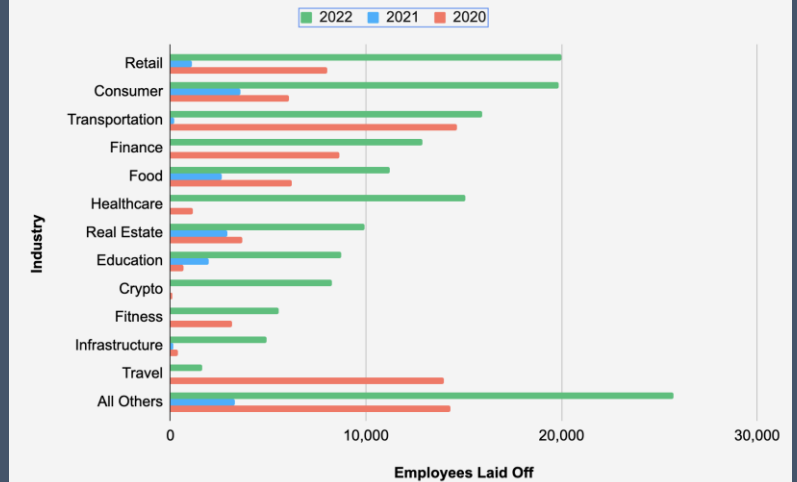
## Tech layoffs in 2022-2023

Source: <https://layoffs.fyi>



## Tech layoffs by industry since COVID-19

Source: <https://layoffs.fyi>



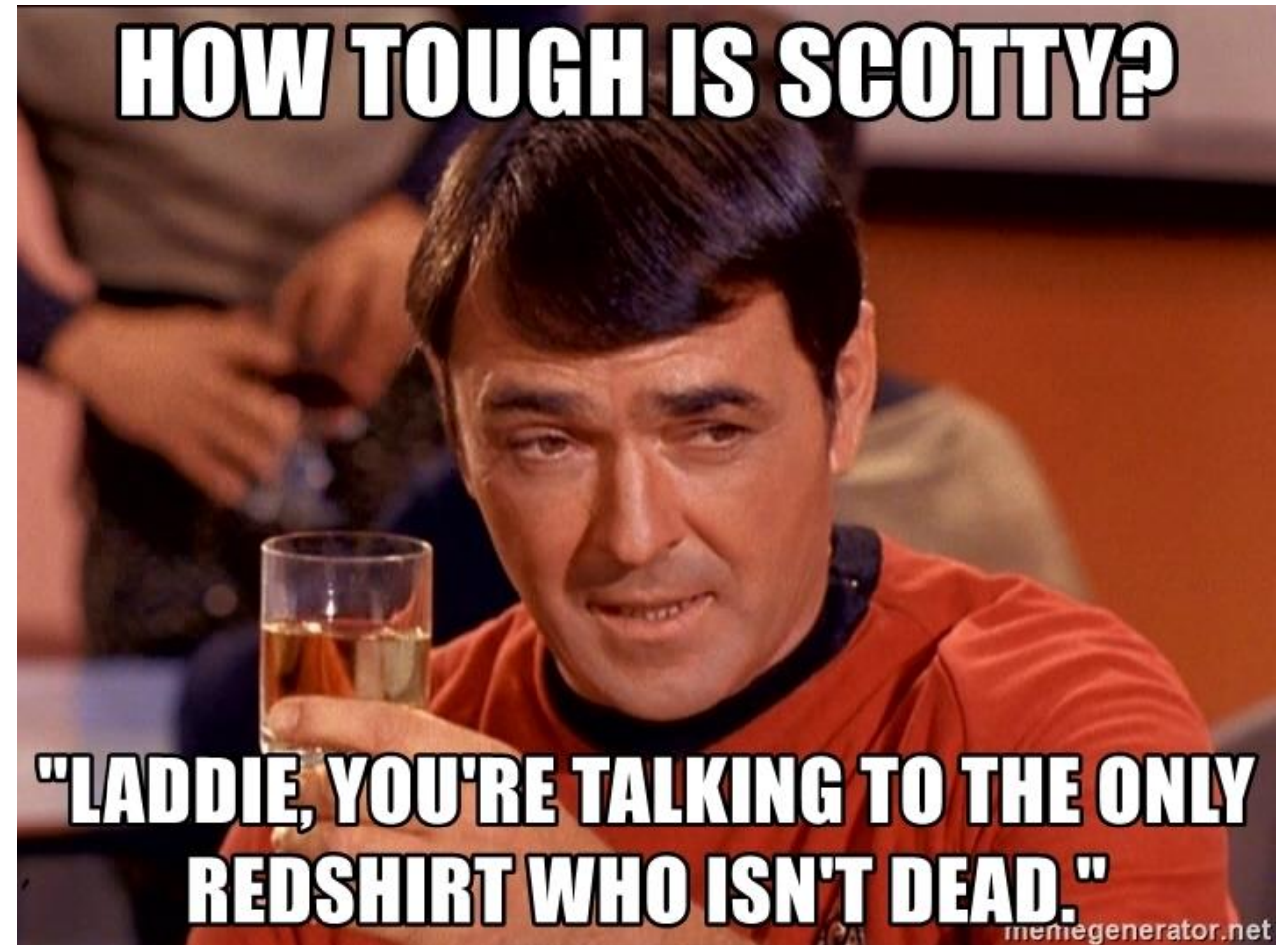
## Prepare now for Job Opportunities

- Know if the job is right in a recession
- Treat hiring like a strange new world
- Understand what is required instead of what is offered
- Don't fall for “do more with less”



## Recession Resistant Jobs (No job is Recession Proof)

- “Cost center” or a “Revenue generator”
- Difficult to Hire or replace
- High level of Competence Required



# A Down-turn but A Need

---

- Dark Reading Take-aways
- 70% surveyed believe a budget cut or freeze
- Skills Gap is huge (76% not ready for the required jobs)
- Salaries have plateaued





## Security Engineer, Cloud Threat Analysis, Cloud CISO

Google · Raleigh, NC

Posted 2 weeks ago · 45 views

# Looking at the Job Description What is Desired?

### Minimum qualifications:

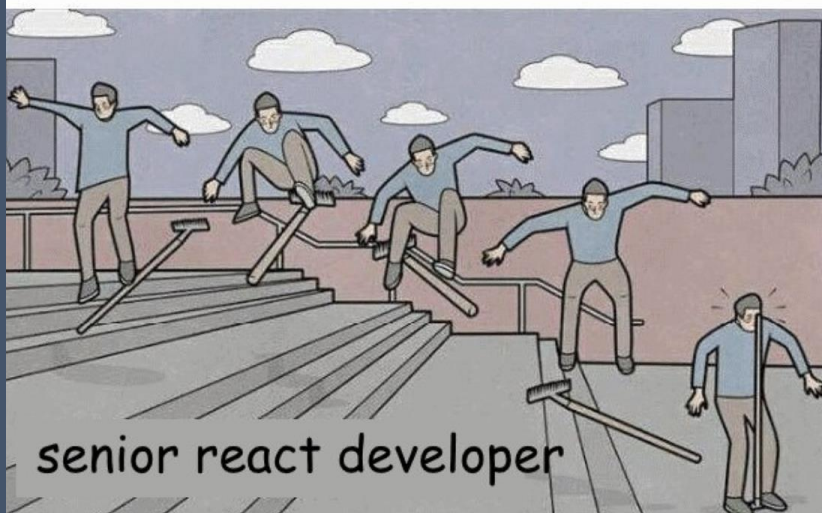
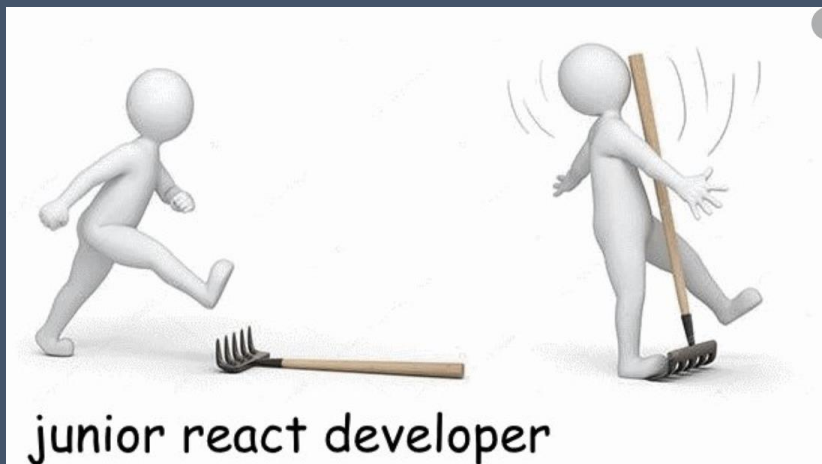
- Experience analyzing malicious traffic and building detections.
- Experience in applications security, network security, systems security or malware analysis.
- Experience in a threat intelligence, reverse engineering or related role.

### 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.



# Understand what is Required over what is Offered

## Basic Qualifications

- Minimum 12 years of experience performing any combination of Information System Security, Security Assessment & Authorization, Cybersecurity, Computer Forensics, or Insider Threat, to include:
  - Minimum 12 years of experience performing vulnerability assessment, analysis, and mitigation; analyzing security system logs, security tools, and data; network monitoring, and intrusion detection using host-based and network-based intrusion detection systems (IDS) and log management applications; testing, installing, patching, and upgrading computer hardware and operating systems (Windows, and UNIX) in an enterprise environment; identifying, collecting, processing, documenting, reporting, cyber security/incident response events; architecting, engineering, developing and implementing cyber security/incident response policies and procedures; engineering, testing, installing, patching, and upgrading various information security hardware and software applications.
  - Minimum 12 years of experience performing requirements analysis, program development activities, architecting, engineering, integrating, developing and/or deploying information technology products (hardware and software) in an enterprise environment.
  - Minimum 12 years of experience using one or more of the following security tools: SourceFire, Arcsight, Splunk, NetWitness, Guidance Software, Digital Guardian, SureView, Intelliview, Nessus, and Foundstone.
  - Minimum 12 years of penetration testing experience for networks, web applications, and enterprise systems. Experience with Federal cybersecurity standards, industry best practices and guidelines.
- Master's degree or equivalent combination of education and work experience
- Secret security clearance required
- Required Certifications:
  - Pen test + certification required
  - CEH certification required



## Chief Cyber Security Advisor

NTT DATA Services · Washington, DC (On-site) 1 week ago ·

# Don't fall for “Do more with less”

- Look at the scope
- Recognize where a company is attempting cost cutting measures

## What You'll Do

You will play a key role in the Product Security team, building a Secure SDLC based in Automation, you will conduct security design reviews, threat modeling and contribute to embedding security in engineering processes and tooling. You will engage and influence across the engineering and product teams, building strong relationships in favor of building a secure product by default. By using your experience of Application security, APIs, Microservices and AWS you will contribute to improve our defenses to ensure the product is robust and ready to face the current threat landscape. You will contribute to evolving our secure coding guidelines, and security knowledgebase.

As a SME in Application Security technologies you will continuously research to identify changes in the threat landscape, in order to adapt our Application security controls and SDLC strategy.

## What You'll Need

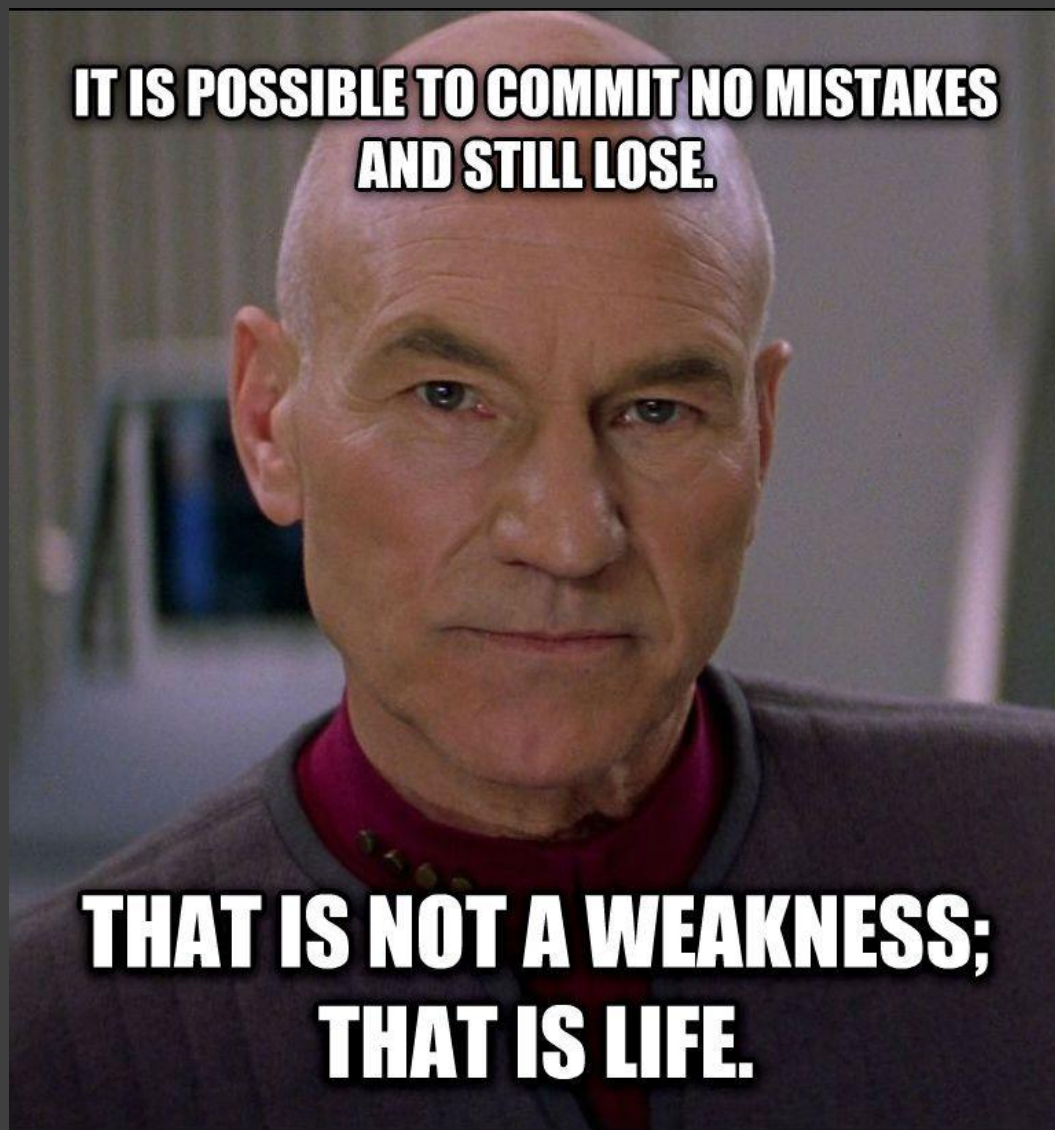
- Strong security experience in Web Application and API security
- Experience with microservice, API gateway, service mesh architecture security
- Experience in SDLC, Appsec and vulnerability management at scale
- Experience in AWS
- Experience working in a highly diverse, multicultural and distributed organization.
- Ability to gain trust and set up good relationships with different stakeholders.
- Automation and programming skills (Python, Java)

3	Miro	SF Bay Area	119	2/2/2023	7%	Other	<a href="https://miro.com/blog/">https://miro.com/blog/...</a>	Series C
---	------	-------------	-----	----------	----	-------	--	----------



# Gain Composure

- Remember your successes in your job
- Remember the people who you have helped
- Do not forget those who care about you professionally and personally
- Work on healthy habits



Instead of internalizing  
work on  
*moving forward*

- Find ways of quantifying the good, but invisible things from a job
- Work on a plan for success
- Do not give 100%

# Looking at the Job Description strange new world

## Mid-Senior Cyber Security Engineer – MSCSE01



Stern Security  
Raleigh, NC (+1 other)

- This JD wants a pen tester  
(but calls it an engineer)

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 01110011 01101000 01101111 01110101 01101100 01100100 00100000 01100010 01100101 00100000 01100001 01100010 01110011 01101111 01101100 01110101 01110100 01100101 01101100 01111001 00100000 01101110 01101111 00100000 01110000 01110010 01101111 01100010 01101100 01100101 01101101 00100000 01110100 01101111 00100000 01100100 01100101 01100011 01101111 01100100 01100101
- VGhpCyBzaG91bGQgYmUgc2ltcGxllGFzIHdlbGwulFlvdSBhcmUgb25lIHNOZXAgYXdheSBzbyBhcHBseSB0b2RheQ==

#### 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

# Looking at the Job Description strange new world

[Download CyberChef](#)

Last build: A month ago

Options About / Support

Operations

binary

To Binary

From Binary

BSON deserialise

BSON serialise

CBOR Decode

CBOR Encode

From BCD

From MessagePack

To BCD

To MessagePack

YARA Rules

Favourites

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Recipe

From Binary

Delimiter  
Space

Byte Length  
8

Input

start: 414  
end: 413  
length: -1

length: 413  
lines: 1

01010100 01101000 01101001 01110011 00100000 01110011 01101000 01101111 01110101 01101100 01100100  
00100000 01100010 01100101 00100000 01100001 01100010 01110011 01101111 01101100 01101010 01110100  
01100101 01101100 01111001 00100000 01101110 01101111 00100000 01110000 01110010 01101111 01100010  
01101100 01100101 01101101 00100000 01110100 01101111 00100000 01100100 01100101 01100011 01101111  
01100100 01100101

Output

start: 46  
end: 46  
length: 0

time: 2ms  
length: 46  
lines: 1

This should be absolutely no problem to decode

# Looking at the Job Description strange new world

[Download CyberChef](#)

Last build: A month ago

Options About

Operations

base64

To Base64

From Base64

Show Base64 offsets

Fork

From Base32

From Base58

From Base85

Parse SSH Host Key

To Base32

To Base58

To Base85

Favourites

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Recipe

From Base64

Alphabet  
A-Za-z0-9+/=

☒ Remove non-alphabet chars

Input

start: 89 end: 90 length: 92  
length: 1 lines: 1

VGhpcyBzaG91bGQgYmUgc2ltcGxlIGFzIHd1bGwuIFlvdSBhcmUgb251IHV0ZXAgYXdhcSBzbyBhcHBseSB0b2RheQ==

Output

start: 67 end: 67 length: 67  
length: 0 lines: 1

This should be simple as well. You are one step away so apply today

# Interpreting the Job Description

strange new world

- Understand the audience (Hiring Manager/Recruiter)
- Understand the culture



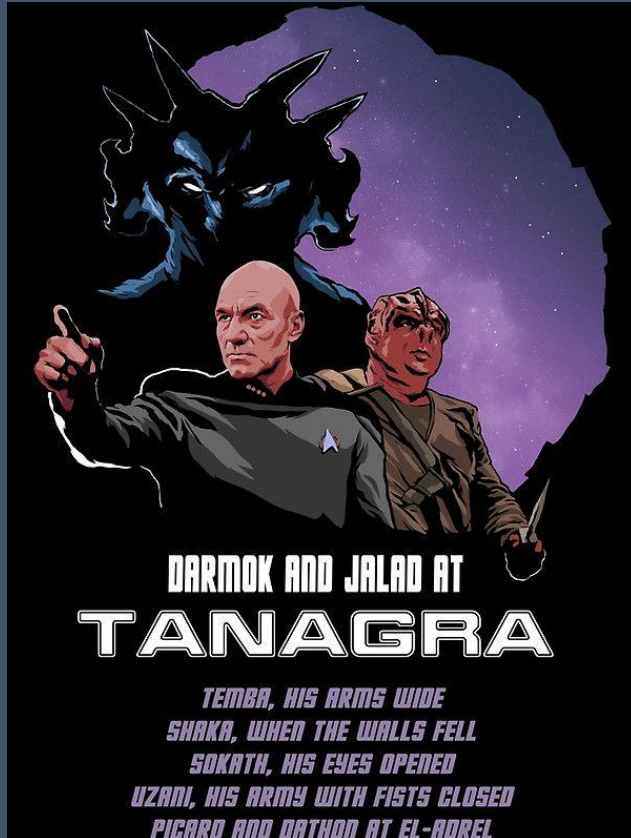
# Interpreting the Job Description

## Understand Audience

### Mid-Senior Cyber Security Engineer – MSCSE01

S Stern Security  
Raleigh, NC (+1 other)

- 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 01110011 01101000 01101111 01110101 01101100 01100100 00100000 01100010 01100101 00100000 01100001 01100010 01110011 01101111 01101100 01110101 01110100 01100101 01101100 01111001 00100000 01101110 01101111 00100000 01110000 01110010 01101111 01100010 01101100 01100101 01101101 00100000 01110100 01101111 00100000 01100100 01100101 01100011 01101111 01100100 01100101
- VGhpcyBzaG91bGQgYmUgc2ltcGxllIGFzIHdlbGwulFlvdSBhcmUgb25lIHNOZXAgYXdheSBzbyBhcHBseSB0b2RheQ==

##### Great to have

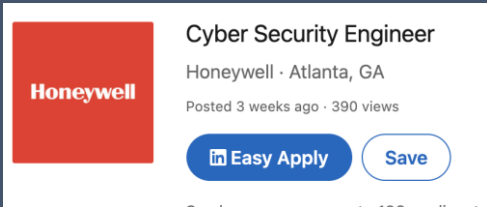
- IT Background
- Security Framework experience (ex. MITRE ATT&CK, NIST, PCI, FFIEC CAT)
- Development/Scripting experience
- Forensic & incident investigation knowledge
- Cloud security experience

# 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





# Researching a Company Looking for Clues

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

Link to Apply: [https://careers.honeywell.com/us/en/job/HRD119015/Lead-Cloud-Automation-Engineer-Cyber-Security?utm\\_source=SwatiN](https://careers.honeywell.com/us/en/job/HRD119015/Lead-Cloud-Automation-Engineer-Cyber-Security?utm_source=SwatiN)

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



Cyber Security Engineer

Honeywell · Atlanta, GA

Posted 3 weeks ago · 390 views

Easy Apply

Save

# Honeywell Suffers Cyber-Attack

By [Linn Foster Freedman](#) on March 25, 2021

POSTED IN [CYBERSECURITY](#)

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.

# Researching a Company Looking for Clues

public data breach company list

All

News

Images

Maps

Shopping

More

About 69,400,000 results (0.94 seconds)

All Data Breaches in 2019 – 2021 – An Alarming Timeline

- 533 Million Users – Facebook, April 03, 2021. ...
- 5 Billion – Keepnet Labs, June 9, 2020. ...
- 47.5 Million – Truecaller, May 27, 2020. ...
- 26.3 Million – LiveJournal, May 27, 2020. ...
- 8.3 Billion – AIS, May 25, 2020. ...
- 25 Million – Mathway, May 25, 2020. ...
- 2.3 Million – Indonesia, May 22, 2020. ...
- 9 Million – EasyJet – May 19, 2020.

[More items...](#)

<https://selfkey.org> · Blog ·

All Data Breaches in 2019 - 2021 - An Alarming Timeline ...

UpGuard Security Rating

A

874

/ 950

UpGuard's Cyber Security Ratings range from 0 to 950. The higher the score, the more likely Honeywell has good security practices.


Company info

Honeywell

→

Company	Honeywell
Employees	108,490
Location	Morris Plains, NJ, United States.
CEO	Darius Adamczyk
Last updated	May 06, 2021
Industries	Manufacturing

# Researching a Company Understand the Company Overall

 U.S. Securities and Exchange Commission

## EDGAR Search Results

SEC Home » Search the Next-Generation EDGAR System » Company Search » Current Page

**INTERNATIONAL BUSINESS MACHINES CORP CIK#: 0000051143 (see all company filings)**

SIC: 3570 - COMPUTER & OFFICE EQUIPMENT  
State location: NY | State of Inc.: NY | Fiscal Year End: 1231  
(Office of Technology)  
Get [insider transactions](#) for this issuer.

Business Address  
1 NEW ORCHARD ROAD  
ARMONK NY 10504  
9144991900

Mailing Address  
1 NEW ORCHARD RD  
ARMONK NY 10504

**Filter Results**

Filing Type:  Prior to: (YYYYMMDD)  Ownership? ☐ include ☒ exclude ☐ only Limit Results Per Page 40 Entries







Search Within Files [EDGAR](#) | Full Text Search  
Enter keywords

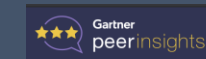
Items 1 - 40 [RSS Feed](#)

Filings	Format	Description	Filing Date	File/Film Nu
8-K	<a href="#">Documents</a> <a href="#">Interactive Data</a>	Current report, item 5.07 Acc-no: 0001104659-21-059030 (34 Act) Size: 485 KB	2021-04-30	001-02360 21878181
10-Q	<a href="#">Documents</a> <a href="#">Interactive Data</a>	Quarterly report [Sections 13 or 15(d)] Acc-no: 0001558370-21-004922 (34 Act) Size: 19 MB	2021-04-27	001-02360 21859190
8-K	<a href="#">Documents</a> <a href="#">Interactive Data</a>	Current report, items 7.01 and 9.01 Acc-no: 0001558370-21-004495 (34 Act) Size: 1 MB	2021-04-20	001-02360 21837961
8-K	<a href="#">Documents</a> <a href="#">Interactive Data</a>	Current report, items 2.02, 7.01, and 9.01 Acc-no: 0001558370-21-004470 (34 Act) Size: 4 MB	2021-04-19	001-02360 21834863

Explore  
IBM  
Security™  
solutions


Transform your security program  
with the largest enterprise security

	Security platform		Data security		Identity and access management
	Services		SIEM		SOAR

 Enter a vendor, product, or market name

Write a Review Categories Log In For Vendors

All Categories > Security Information and Event Management > IBM > QRadar SIEM

 **QRadar SIEM Reviews**  
by IBM in Security Information and Event Management  
4.4 ★★★★★ 414 Reviews

Overview Reviews Ratings Alternatives

**QRadar SIEM Ratings Overview**

4.4 ★★★★★ 414 Reviews (All Time)

Rating Distribution

5 Star	46%
4 Star	39%
3 Star	12%
2 Star	2%

Review weighting ☐ Reviewed in Last 12 Months ☒ [EMAIL PAGE](#)

73% Would Recommend

Customer Experience

Evaluation & Contracting	4.3
Integration & Deployment	4.2
Service & Support	4.1
Product Capabilities	4.4

How likely a  0 1 2 Not likely at all

UpGuard Security Rating

**B 779** / 950

# Researching a Company

## Assess the Culture

- Understand how employees and consumers view a company

union pacific sucks twitter

About 598,000 results (0.59 seconds)

<https://twitter.com/hashtag/unionpacificsucks>

**#unionpacificsucks hashtag on Twitter**

See Tweets about #unionpacificsucks on Twitter. ... Never mind, Union Pacific sucks. ... WTF Union Pacific @UnionPacific #unionpacificsucks pic.twitter.com/ ...

<https://www.indeed.com/.../EmployeeReviews>

**Working at Union Pacific: 995 Reviews about Management ...**

The work itself is not bad but the company is lacking in several areas. Pros. pizza party if nobody gets hurt.

★ ★ ★ ★ ★ Rating: 2.8 · 2,104 reviews

<https://www.indeed.com/Companies/UnionPacific>

**Working at Union Pacific: 2,088 Reviews | Indeed.com**


moral is low but nothing is done about it by management. The work itself is not bad but the company is lacking in several areas. Pros.

★ ★ ★ ★ ★ Rating: 2.8 · 2,104 reviews

**yahoo!**

Southern stands for and who we want to be moving forward."

**1. Union Pacific**



*Union Pacific*

- Glassdoor rating: 1.9**
- Industry: Rail**

Founded in 1862 by President Abraham Lincoln, Union Pacific connects two-thirds of the



Tom Purdy – [tepurdy@att.net](mailto:tepurdy@att.net)

Chris Uhlig – [Chris.Uhlig@disys.com](mailto:Chris.Uhlig@disys.com)

Elizabeth Cole-Walker – [eacolewa@ncsu.edu](mailto:eacolewa@ncsu.edu)

Evan Strickland – [tacituacitum@gmail.com](mailto:tacituacitum@gmail.com)

Jon Lee – [me@jonlee.us](mailto: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

