Susie

Junior Target
Network Analysts

.....

Key Tasks:
- Analyze network traffic
- Interpret the results
- Document and share findings

Strengths:
- International relations
- Critical thinking
- Problem analysis/framing
- Team player and good collaborator

Weaknesses:
- No knowledge of global telecommunications
- Lacks technical analysis skills
- No background in computer science or data analysis

Timeline

TASK START	PRIMING STAGE	FIRST ACTION STAGE	SECOND ACTION STAGE	THIRD ACTION STAGE

Overview

Arrives at work
Susie arrives early in anticipation of her first day on the job.

Orients self to workplace
She is given a tour of the facility and meets the people she'll be working with.

Meets one-on-one with her mentor.

Assigned to run a query on an email address that has recently been in communication with the terrorist group and they suspect belongs to a new operative.

Assigned first query
Susie is tasked with analyzing recent traffic with the email address to characterize how it is used by the Zendian group.

Directed to her workspace, gets comfortable, logs into her computer.

Selects search tool
She decides to query a MySQL database containing data that has been intercepted across Zendian communication networks.

Prepares first query
Susie refers to the documentation shared by the other analyst.

There are some examples of queries, but she has no idea if her own query will be compliant, what it will do, or if she's authorized to do it.

She drafts the syntax, using the documentation as a blueprint.

Asks another analyst to review her work.

Drafts her justification and asks another analyst to review it.

Submits her first query
With a lot of trepidation, Susie submits her first query.

She receives a lot of technical data that she doesn't know how to interpret.

Seeks help with analysis
She asks another analyst for help understanding the technical aspects of the data and where to find relevant information.

They provide her with a basic overview of the data types and their significance.

Susie begins this process but it is very time consuming.

Frames the problem area
She knows they want to look for connections between the terrorist group and the bombing event, and that the email address may belong to a new operative.

She needs to find out what the email address is being used for and see if she can use the data to make any connections to the bombing event.

She decides to start with the information she is most familiar with, and begins sorting the email data by their timestamps to create a timeline of the traffic that she can compare to the bombing event.

Notices a pattern
After some time she notices a pattern.

Looks like there was a spike in communication a few months leading up to the bombing event between the email address she has been looking at and another email address.

Further analysis
She investigate IP addresses to obtain their location data.

Unsure on how to go about this, so she asks for help.

Senior analyst helps her run query on SPFs.

Analyzes the result
The query compares IP addresses and data/timestamps to identify potential correlations between email pattern and the bombing incident.

She presents her findings to her mentor.

Reports to mentor
Susie submits her report after completing her analysis task.

Awaits feedback from mentor.

She realizes she needs to restructure her findings for archival purposes and reporting to language analysts.

Documentation
Susie opts for a manual approach to documentation.

She creating a simple table to document her actions without the use of automated tools.

Susie retraces her steps aligning them with what she did and why she did it.

Sharing report
Reviews and refines final summary of findings and analysis.

Shares her summary with the other TDNAs.

Uploads a copy of her summary and the documentation of her process in her folder on the shared drive.

Action

She checks in and goes through identification and verification processes.

Susie is working in a pod with several other analysts. They are in close proximity to each other and it's a very collaborative environment.

The Technical Director has assigned her mentor to monitor her work and the other analysts let her know that she can always come to them with questions.

She's not sure where to start so she asks someone what database they would use to search for an email address corresponding and email traffic.

The other analyst tells her "it depends," but they help her narrow down her options and share some documentation and tradecraft resources.

The data contains packets that have been intercepted as they move across networks.

In addition to other data, the packets contain emails that have been sent and received on Zendian networks.

Susie thinks she can use this database to find the email username in the metadata.

QUESTIONING AND SECOND GUESSING
- How old is the documentation and does it adhere to current compliance guidelines?
- Is she authorized to make the same query?
- Will her query be too broad; what kind of results will she get?
- Will the results include data on Oceania citizens, businesses or service providers?
- Will the query even work for the database she's searching?

Extremely **nervous** and **scared** to submit her query.

The other analyst has some suggestions on how she can narrow her search so it's not too broad and won't query information on Oceania citizens.

Another analyst reviews her justification to see if she's provided enough detail. They confirm her query and her justification.

MIME Types? MIME-Version? X-Headers? SMTP Commands? What does all this mean?

The other analyst explains how to filter, sort, and rearrange the data to look for patterns or anomalies.

Feels like learning a foreign language; she has more questions than answers.

At the same time, Susie has to keep reminding herself to document her process and write down what she's doing and why she's doing it.

This makes it difficult for her to focus on her main assignment — she feels like her attention is split between two different tasks.

Excited about the increase in communication between two identified emails, Susie decides to investigate their IP addresses to obtain their location data.

She asks a senior analyst who helps her run another query that will helps her compare the two emails data side by side.

Senior analysts guides her to run a query to compare their SPFs (sender policy framework: helps identity server email is sent from) which shows the IP address and data/timestamps to see how these correlates to the bombing.

She identifies anomalous patterns of communication that may indicate involvement or coordination related to the incident.

She presents her findings to her mentor, who assists her in mapping timestamps to location data to identify connections between bombing locations.

She believes she has made the right connections about the event that could be beneficial but is uncertain about her next steps.

She shares her rough report ands her suggested conclusion to her mentor for review and advice on the next steps.

Mentor tells her she needs to restructure her findings for archival purposes and report to language analysts.

Susie faces the challenge of having not documented her process while working, feeling overwhelmed at the prospect of retroactively tracing her steps.

She goes through all of her papers and sticky notes on her desk.

Despite feeling overwhelmed, Susie decides to adopt a manual approach to documentation.

She creates a simple table to document her actions chronologically and opts for manual documentation without any automated tools.

Susie recognizes the importance of understanding her thought process and the context behind her actions, aligning with the emphasis on knowing why she took certain steps.

Susie navigates the challenge, acknowledging the difficulty highlighted by the need to track how to answer the question or meet the objective of her analysis.

Susie remains committed to ensuring the accuracy and completeness of her report, despite the challenges she faces in the documentation process.

She reviews and updates her analysis, including her work process to make it more comprehensive.

She feels very exhausted, however, this information is important to the bombing event and she feels pressure to submit her analysis before she leaves that day.

Susie attaches her summary of analysis and findings to an email and sends it to her mentor, cc'ing the Technical Director and other senior TDNAs.

Data

THE EMAIL ADDRESS
zp43@zenmail.com

PACKETS
Pieces of data and metadata sent and received across networks.

HER FIRST QUERY
```
sprintf(command, "SELECT emailID FROM emailAddress WHERE fromAddress = 'zp43@zenmail.com';",
input[loop]);
if (mysql_query(conn, command)) {
  fprintf(stderr, "zp43@zenmail.com\n", mysql_error(conn));
```

JUSTIFICATION
Looking for connections between the email address and a Zendian terrorist group. Suspected to belong to a new operative and want to characterize how it's being used. Suspected relation to the bombing event.

TECHNICAL DATA FIELDS
- From
- To
- Subject
- Date
- Message-ID
- MIME-Version
- Body
- Attachments
- MIME-Types
- Routing Information
- X-Headers
- SMTP Commands
- Security Features
- Return-Path
- Received Headers

RESULT DATA SET
[LINK]

THE OTHER EMAIL ADDRESS
znazari@zendia.gov

RELATIONSHIP QUERY
```
($ curl emailrep.io/zp43@zenmail.com
{
  "emails": "zp43@zenmail.com",
  "znazari@zendia.org"
  "conversations": "high",
}
```

RESULT DATA SET
[LINK]

DOCUMENTATION
[LINK]

Resources

2 monitors and a laptop
Network backup storage

Handwritten notes
Bookmarks from training

MySQL Database:
Relational database management system

Documentation. Contains process notes and queries used for similar tasks. Not always detailed or well organized, often a simple, digitized document or a spreadsheet with tables and different fields.

Excel table, word processing application, notebook paper.

2 monitors and a laptop
Network backup storage
MySQL Database

2 monitors and a laptop
Network backup storage
MySQL Database

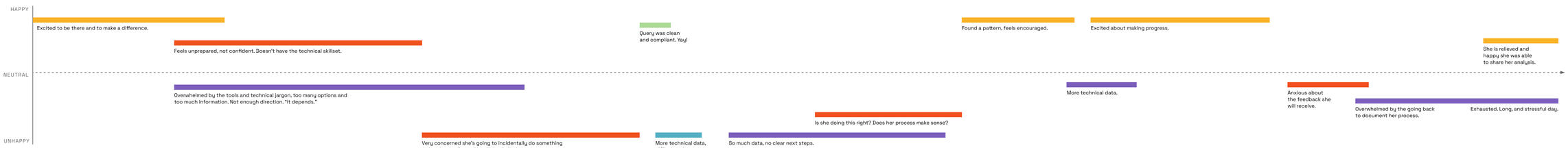
.xls data set

Handwritten notes, sticky notes, browser history, .xls data set, MySQL Database

2 monitors and a laptop
Network backup storage

Help and insights from other analysts | Help and insights from other analysts | Help and insights from other analysts | Help and insights from other analysts

Emotion



- EXCITED
- RELIEVED
- DISCOURAGED
- ANXIOUS
- OVERWHELMED

Pains and Gains

- ✕ Pain Point
- ♥ Gain Point

- ✕ No background in network analysis.
- ✕ No scripting knowledge or skills.
- ✕ No clear direction or starting point.
- ✕ Informal help network, constantly has to ask another analyst for assistance or advice.
- ♥ Collaborative work environment, likes being part of a team.
- ♥ Mission-driven; work feels impactful.

- ✕ SUPER SCARY.
- ✕ SO MUCH UNCERTAINTY. A lot of second guessing.
- ✕ No clear way to know if she is in compliance.
- ✕ Flying blind — so many questions and not a lot of straight answers.
- ✕ Extremely time consuming.
- ✕ Doesn't want to ask another analyst for help EVERY. TIME.
- ✕ There is rarely a definitive answer. Very stressful.
- ♥ Everyone watches out for each other.

- ✕ Can't enter flow state.
- ✕ Increased cognitive load.
- ♥ Effective communicator.
- ♥ Critical thinker. Good at framing the problem to identify pathways. Pattern finding.

- ✕ Information overload.
- ✕ Unsure about how to present findings.
- ✕ Anxiety about quality of analysis.
- ♥ Good at navigating a problem, identifying next steps.

- ✕ Unclear documentation and reporting process
- ✕ Challenge tracking work flow and process
- ✕ Anxiety about quality of documentation.
- ✕ Extremely time consuming and Stressful.
- ✕ Inefficient documentation process
- ♥ Gap analysis, attention to detail, clear overview of documentation process.

- ✕ Unclear documentation format
- ✕ Pressure to deliver
- ♥ Resilience skills, report drafting