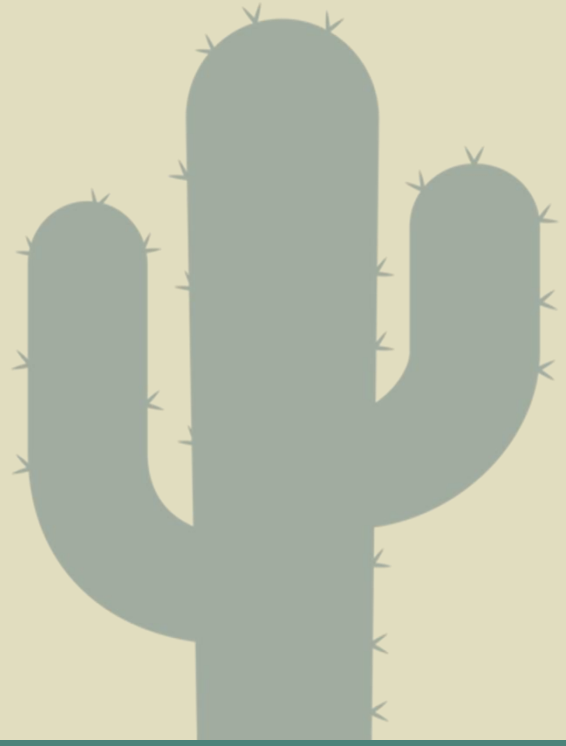
# What I Learned After My First Year as a Security Analyst

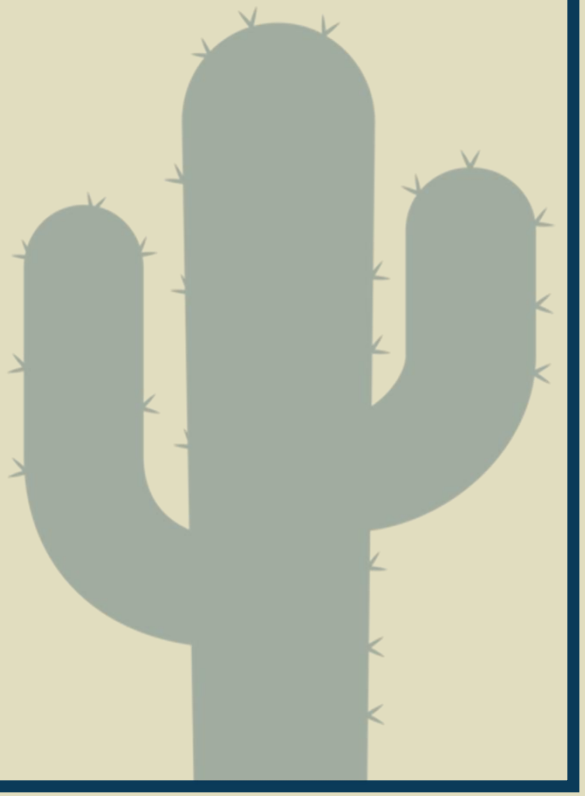


How to survive and thrive in a Security Operations Center (SOC)

# Shall we play a name?

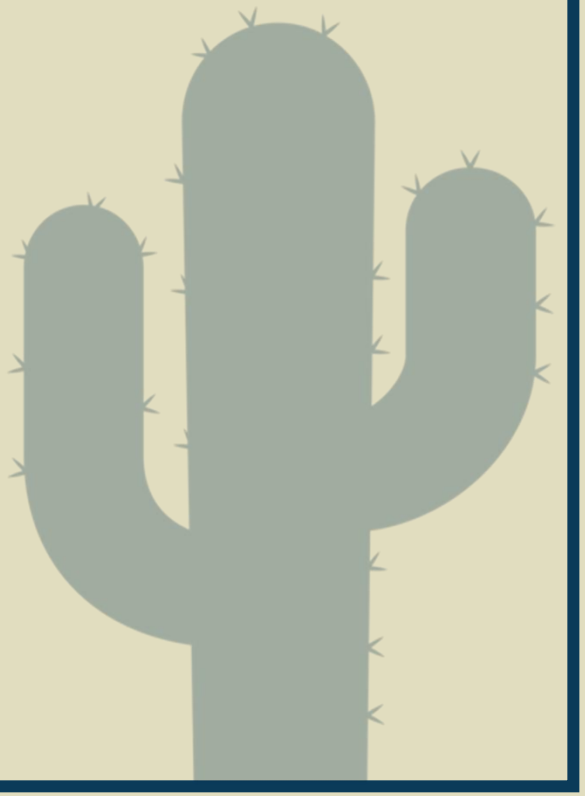
- I’m woland (Erin)
- Former "telco enthusiast"
- Investigative journalist, bartender, SOC grunt, starting in offsec
- @wolandsec

# EVERY SOC IS DIFFERENT



# What do analysts actually do?

1. You take evidence (usually logs/alarms)
2. You investigate and process these artifacts
3. Determine if there's a threat

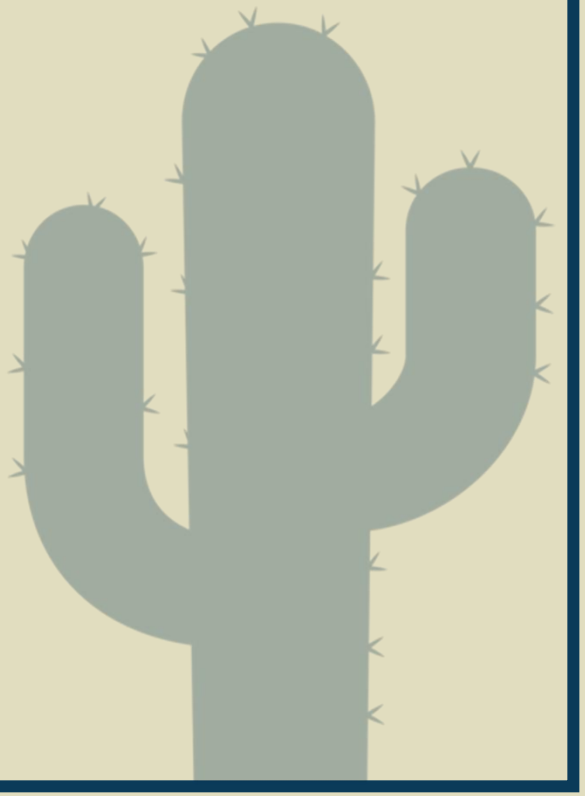


# Vital Skills

- Network and security fundamentals
- Details matter (they really, really do)
- Solid communication
- Curious, investigative mindset

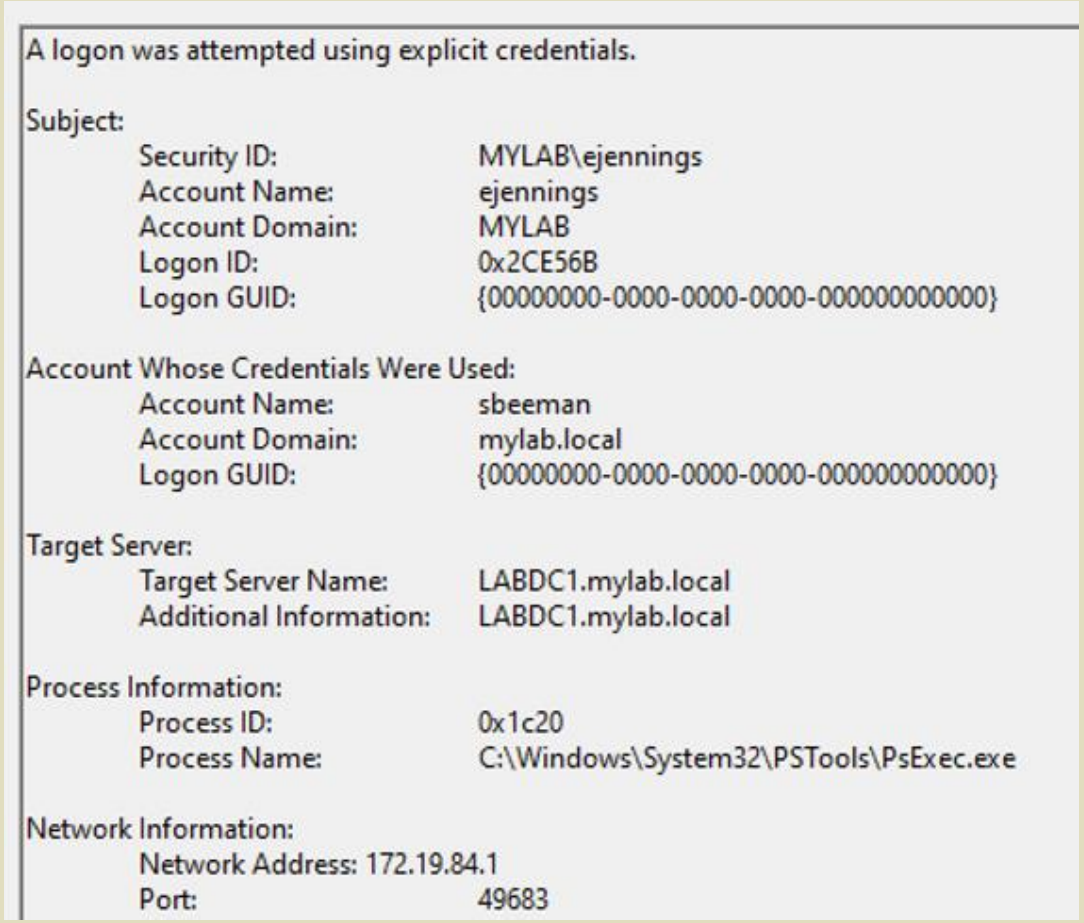
# Don’t be overwhelmed

- You’re going to be exposed to different tools, policies, and procedures (SIEMs, and SOARs, and triage, oh my!)
- It’s a marathon, not a sprint
- Most people have imposter syndrome; It’s normal and OK



# Learn to read raw log data

- Log parsing is imperfect
- Go to the source
- Gain a better understanding of your systems and how they work!



# Do you even threat intel?

- The glue that holds everything together
- What is an IOC, how do attackers operate?
- Highly volatile, tactics change quickly
- Essential to analyst operations

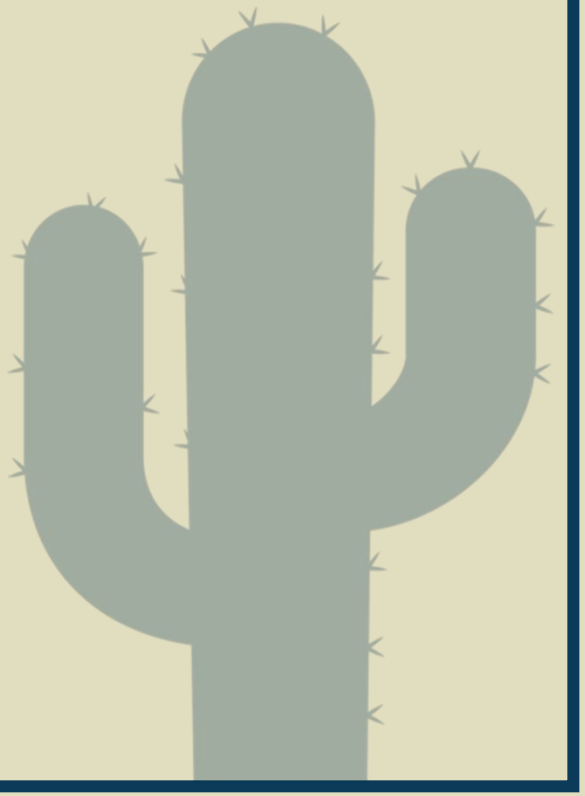
urlscan.io
A sandbox for the web

Pulsedive

VIRUSTOTAL

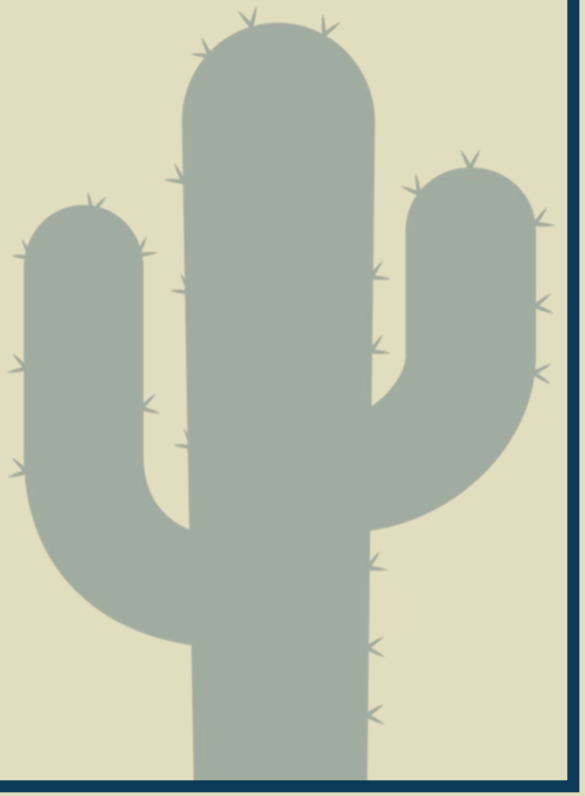
# Getting it wrong

- You’re going to get something wrong. It’s inevitable.
- There's a difference between mistakes and negligence
- Learn from it



# Getting it right

- So you’ve found true positive!
- There is no guarantee the issue will be fixed or even acknowledged
- Analysts don't get to choose the response (usually)



# Log visibility

- You’re not always going to be able to find the answer and that’s OK
- Some logs aren’t even turned on!
- SIEMs and other ops things break

# Surviving night shift

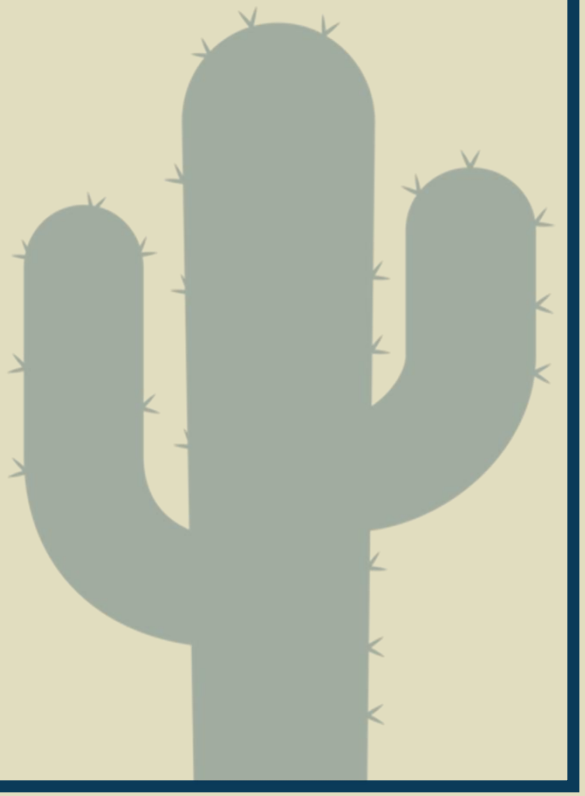
- It’s rough. Some people handle it better than others
- Keep the same sleep schedule
- Sleep aides (non habit forming), blackout curtains, and a quiet room

Before:

After:

# Every SOC has a weakness

- Only as strong as the alarm rules enabled and the analysts' understanding of them
- It's one tool out of many for defensive operations
- Preparation and communication are key

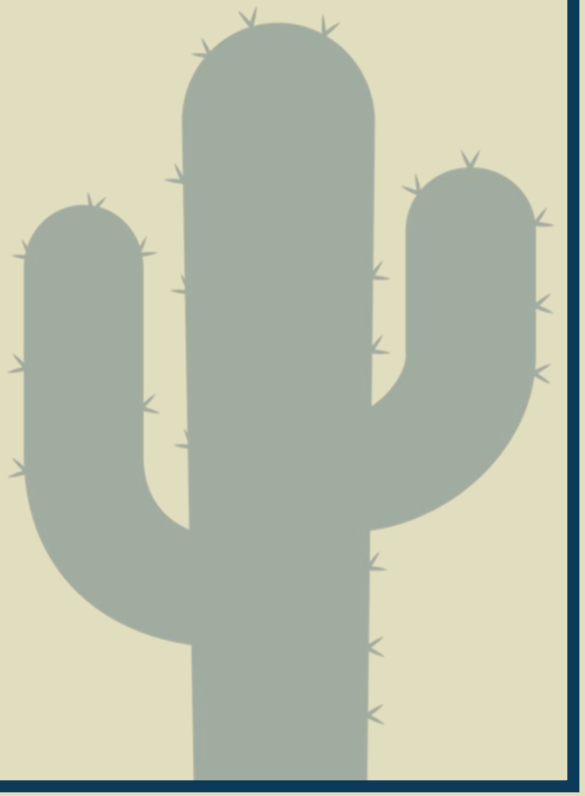


# Know when to run

- You are more than a warm body clicking buttons
- Are you learning new things?
- Is this an environment where you can grow?

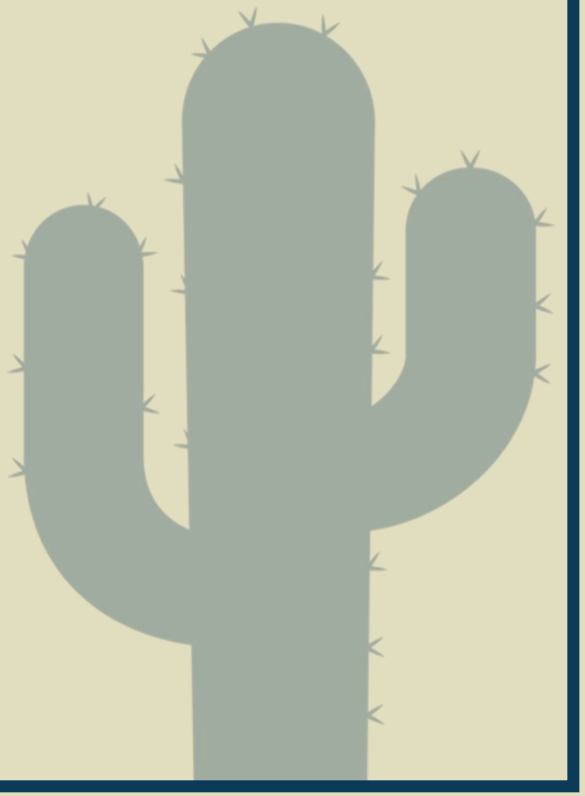
# Resources

- Start your own SOC!
- Graylog and Kibana for log management, free or trial versions of SIEMs like Splunk Free, Qradar community edition
- Splunk Boss of the SOC datasets for log data
- OpenSOC – a free SOC/threat hunting simulation CTF at defcon



# In summary…

- You’ve come a long way and we need you!
- Find out where you want to go from here
- If you genuinely care and want to learn you’re going to do fine



# Thank you