THE STUDENT SOC EXPERIENCE

By: Jonathan Morales

CYSE 368

3/31/2026

FROM SHADOWING TO INDEPENDENT

Biggest difference between reflections before is being able to work on it individually

Pager Duty, Firewall Requests, Endpoint detections, and Risky Users

Gained confidence as an individual

PAGER DUTY

- NOTIFIED ON ALERT
- DETERMINE WHETHER IT'S MALICIOUS
- NOTES AND ACT
- MICROSOFT DEFENDER
- DIFFERENCE BETWEEN UNWANTED ADD AND MALICIOUS EMAIL

ENDPOINT DETECTIONS

- See detection in Crowdstrike
- Begin notes and investigation
- SHA, file path, disk operations
- Determine whether it's malicious
- Act

RISKY USER

- Qradar
- Malicious activity/ IP
- Look at typical history
- Note and act

FIREWALL REQUESTS

- Determine specifically what they are asking for
- Resolve domains and Ips if needed
- Make sure there is a legitimate need for connection
- Note objects modified and created
- Note and commit changes and push to devices

KNOWLEDGE GAINED

- Many bad actors take additional steps to hide or mask attacks
- Human error significantly results to many compromises
- Vpn's/ Proxy Servers can make data complex
- Other comprised users in networks may try to compromise yours
- While Cybersecurity knowledge is good you must understand business as well

IMPROVED SKILLS

File path recognition

Viewing and understanding data

SQL

Detection of malicious behavior vs spam/ ads

Security vs personal preferences

Networks

Firewalls

THANKYOU!

Once again, I would like to thank y'all for your time and knowledge provided throughout this internship. Which has been extremely valuable to my professional development and growth in my career.