


CCDC: Let's get down to *BUSINESS*

This is important (trust)



Weekly Schedule

Date	CPTC (10AM-12PM)	CCDC (1PM-3PM)
Jul 12	Cyber Bootcamp Kickoff!	
Jul 19	Intro to Pen Testing	Business Week 
Jul 26	Hacking Web Apps	Introduction to Networking
Aug 2	Hacking Linux	Securing Linux
Aug 9	Hacking Windows	Securing Windows
Aug 16	Consulting	Common Services
Aug 23-24	CPTC Tryouts (All day)	
Aug 30-Sep 13		CCDC Fall
Sep 20-21		CCDC Tryouts (1-5 PM)

whoami

- **Medha Swarnachandrabalaji**
@med1100
- **3rd year CS Major and Cyber Minor**
- **CCDC**
 - Alternate Member 2024-2025
 - Member 2025-2026
- **SWIFT Alumni Relations Coordinator**
- **yapper**



Table of Contents

| 01

Why Business?

| 02

Injects

| 03

Forced Vacations

| 04

Report to your boss (us)

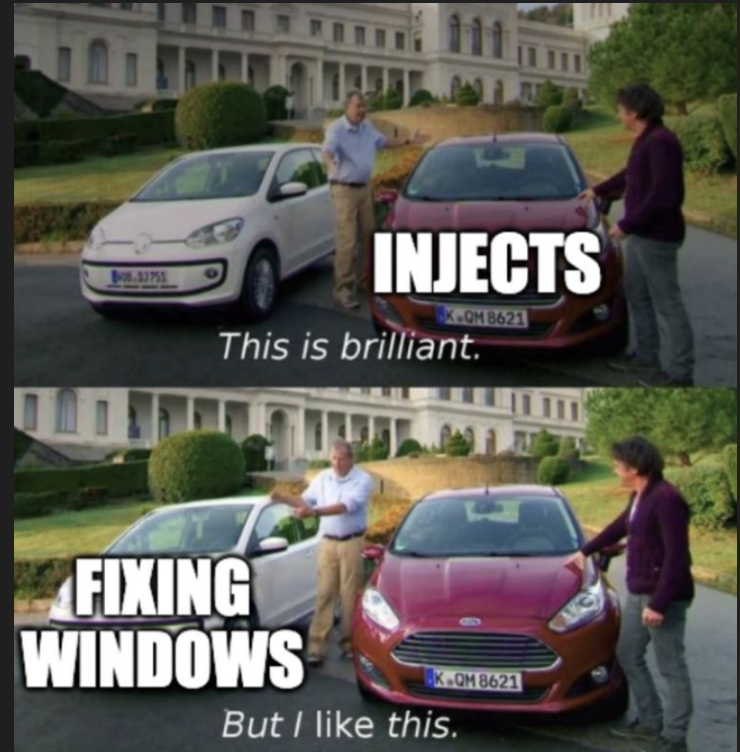
01 Business???

Da heck I thought this was a
cyber defense competition??!!!!



Whoa!

Before you roll your eyes...
Cybersecurity serves as a
function of business



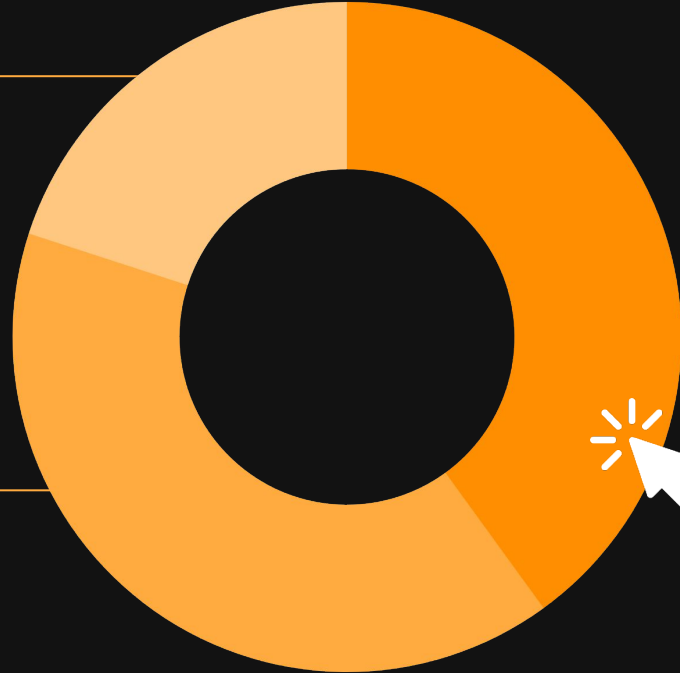
CCDC score breakdown

20%

Orange team

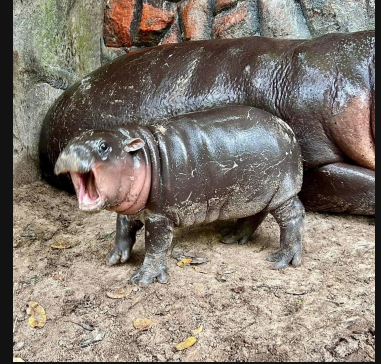
40%

Services



40%

Business injects



Fundamental principles of cybersecurity



Integrity

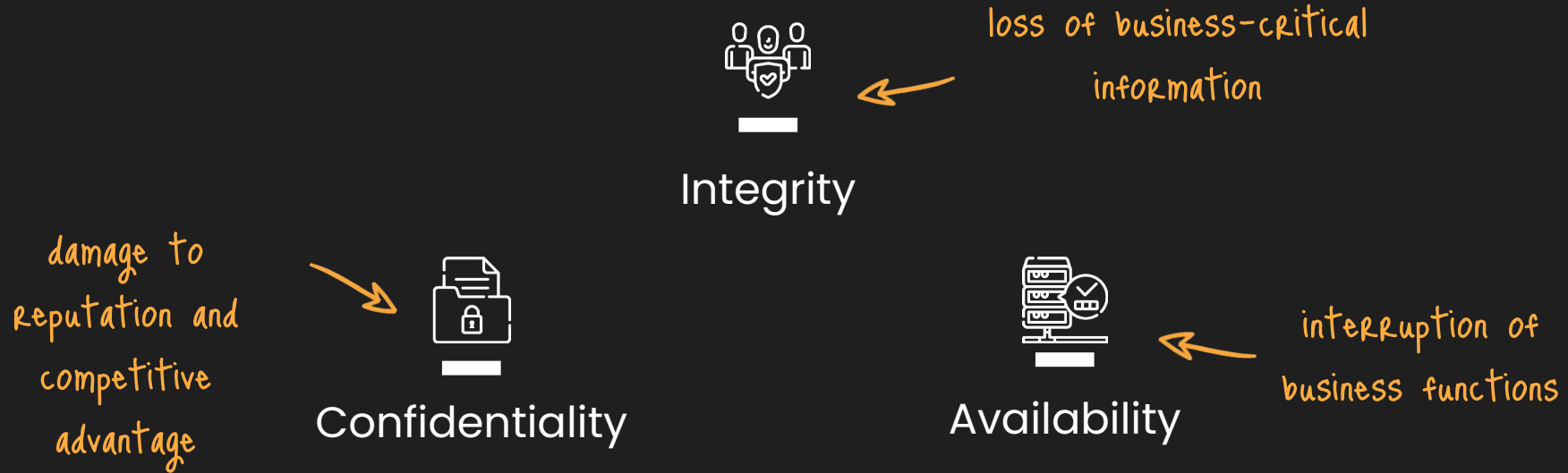


Confidentiality



Availability

Fundamental principles of cybersecurity *(in the context of a business)*



Fundamental principles of cybersecurity (in the context of a business)

**The risk of an interruption
to business is why we are
hired...**

damage to
reputation and
competitive
advantage



Confidentiality

integrity



Availability

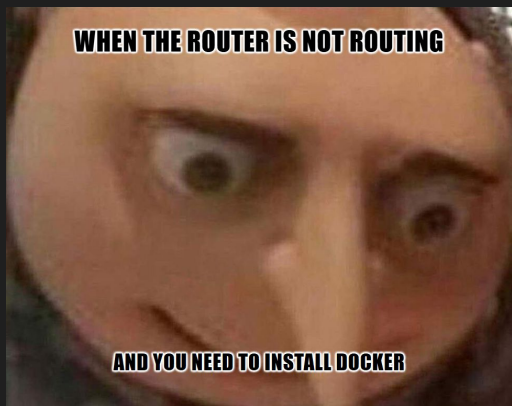
interruption of
business functions

As a result...

**we also have an obligation
to support the business**



It's more
challenging
than you
think...



Technical tasks

Why do we need three firewalls VPNs??

Broad understanding

What even is logging and where are the trees???

Who is Ms. Configuration???

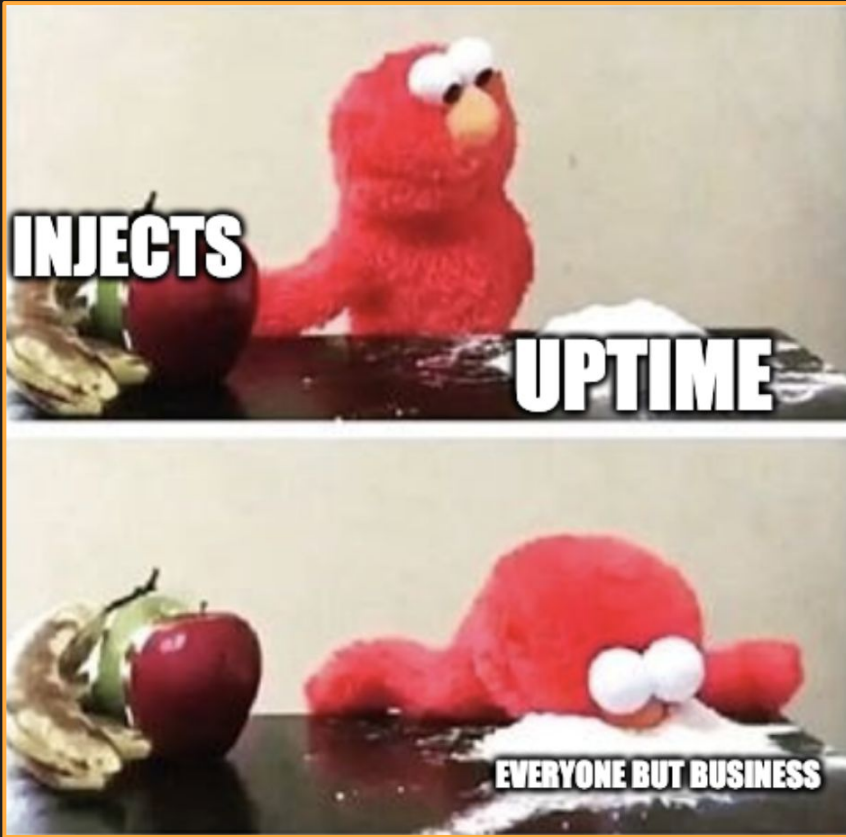
What is a kernel and where is the corn???

02

Injects

No doctors were involved in the making of these slides





Da heck is an inject?

- Tasks from business execs
- Complete within some short timeframe
- Write-ups, infographics, *presentations*
- Examples
 - Conduct a security assessment
 - Recommend a cloud solution
 - Write a Disaster Recovery Policy
 - Set up and configure a company VPN
 - Create an infographic to promote security awareness

Secret sauce to good injects



be thorough



use clear
and concise
language



provide
supporting
evidence



Being thorough



Swiss Bank XChange

Hello Team!

I hope that as you were taking inventory of our assets, that you were making notes of what software were being removed and what ports were closed.

If you have not done so already, I would like your team to perform an audit of any unnecessary software and services that are running on our systems. If you have already done this, good!
Please double check again!

The report your team shall provide as part of this audit will be a list of unnecessary software and services that were found as well as what ports were closed. These should be broken down by the hosts that they were discovered to be running on. No doubt that you will find plenty. This is to aid in our investigation of a prior team who was running these systems.

- Sebastian Herzig Gartmann



Being thorough



Swiss Bank XChange

Hello Team!

I hope that as you were taking inventory of our assets, that you were making notes of what software were being removed and what ports were closed.

If you have not done so already, I would like your team to perform an audit of any unnecessary software and services that are running on our systems. If you have already done this, good! Please double check again!

The report your team shall provide as part of this audit will be a list of unnecessary software and services that were found as well as what ports were closed. These should be broken down by the hosts that they were discovered to be running on. No doubt that you will find plenty. This is to aid in our investigation of a prior team who was running these systems.

- Sebastian Herzig Gartmann

Requirements:

1. Perform an **audit of unnecessary software and services**
 - a. Including **everything** removed prior to this inject
2. List the software and services removed
 - a. Make note of **ports that were closed**
3. **Organize findings by host**

Tips:

- **ALWAYS** take notes on what you are doing
- Anticipate inject prompts



Using professional language



Address the recipient



**Take into account who
your audience is**



**Write with intention, get to
the point**



**DON'T use colloquial
language**



DON'T neglect formatting



**DON'T guess about
information – always
check with the team**



Provide supporting evidence

**YOU ARE TRYING TO
CONVINCE YOUR “BOSS”
THAT **YOUR SOLUTION IS
THE BEST SOLUTION****





Provide supporting evidence

- Give **background** about the issue.
 - Would there be fines if we fail to fix it? Potential loss?
- **WHY** did you choose that solution?
 - What other solutions were there?
- **HOW MUCH** does your solution cost?
 - How does that compare to other solutions?
- **WHO** is going to implement your solution?
 - Who is going to maintain it?

!!! Provide supporting evidence – MUST DOs

SHOW YOUR WORK!!

- Screenshots
- Logs
- Examples of config
- Scripts that were run

NEATLY

- Categorize your evidence
 - Host
 - OS



Takeaways from experience



organization
is key



everyone has
to contribute



READ THE
PROMPT!

03

~~Forced vacations!~~ Presentations

Ayo? :0



Hold up...

VACATION?????

Hold up

**NEVERMIND IT'S
ONLY 15 MINUTES
NOW**

???

1 HOUR (OR SO)

TO CREATE YOUR SLIDES

1 OBJECTIVE

TO PRESENT YOUR BEST PROPOSAL

1 BIG ~~WASTE~~ GOOD USE OF TIME

It helps you adapt quickly and build confidence in your
presentation skills



How to impress the judges :D (slides edition)



Organized

Declutter your slides!! No long sentences!



Graphics

Use graphs, icons, screenshots...



Sources

USE STATISTICS
AND CITE
SOURCES!

How to impress the judges :D (presentation edition)



Loud

Speak with confidence and rizz them up



Fidgeting

Don't make the judges want to chuck their pens at you



Eye contact

Use open body language and maintain eye contact with the judges

04

Report to your boss!

Congrats! You're hired :D

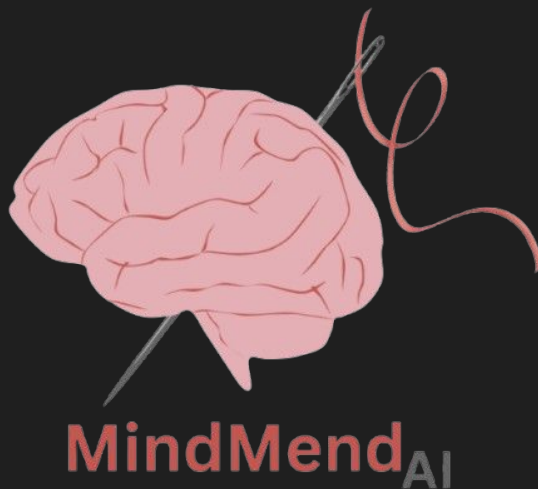




Background

The Company

- Name: MindMend
- About: MindMend is an AI therapy startup
- Athena: MindMend's AI assistant
 - Hotline for those who are seeking help with their mental health
 - Made up of database and web interface
 - Has a backup database



It's 4:30 AM, and you got an alert...

Scenario

- You are a part of the insanely talented AI security team
- Athena's database was poorly secured and a threat actor gained access to it
- They changed the database contents, poisoning Athena
- Athena is now saying not-so-kind things that could lead to negative outcomes

Objective

- 1 page report
- 30 minutes
- Technical report on what caused this for **your manager** who is rushing into the office



8:30am... your CEO is awake and angry

Scenario

- CEO wakes to "ATHENA DOWN!" and stoppage of business
- "Why should you keep your jobs if you can't prevent this?!"

Objectives

- 1 page report to **The CEO**
- 30 minutes
- Explain and justify why the team should **not** be replaced



Submit: <https://jessh.zip/week2-inject2>

Manager

- Technical rundown
- Immediately actionable steps
- Suggestions for alternative solutions
- Technical sources
- Actionable takeaways from the incident

Submit: <https://jessh.zip/week2-inject1>

C-Suite

- Estimated time to get systems back online
- Explain why this task is difficult in layman's terms
- Justify why having the same security team is worth it
- Explain the team's reputation and why you were hired at all

Submit: <https://jessh.zip/week2-inject2>

Homework!

Due July 26th @ 5 AM PST
<https://jessh.zip/2025ccdchw-2>

Live Demo

- For HW