

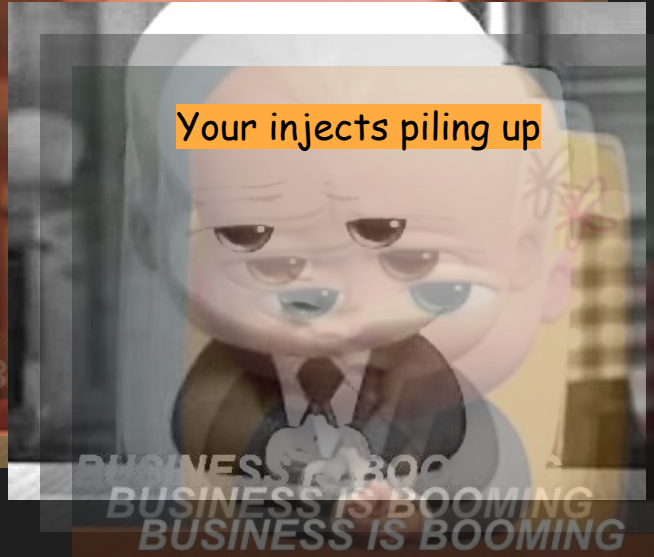
CCDC:




Let's get down to ***BUSINESS***

I promise this is important T.T

<https://jessh.zip/ccdcweek2>



Weekly Schedule

| Date | CPTC (10AM-12PM) | CCDC (1PM-4PM) |
|-------------------|------------------------------------|--|
| Jul 13 | Cyber Booteamp Kickoff! | |
| Jul 20 | Intro to Pen Testing | Business Week  |
| Jul 27 | Hacking Web Apps | Introduction to Networking |
| Aug 3 | Hacking Linux | Securing Linux |
| Aug 10 | Hacking Windows | Securing Windows |
| Aug 17 | Consulting | Common Services |
| Aug 24-25 | CPTC Tryouts (All day) | |
| Aug 31-Sep 1 | | CCDC Tryouts (1-5PM) |

whoami

- ❖ jessica leung | @jeSSH
- ❖ ex-CCDC business monkey
- ❖ SOC @ SpaceX



New Inject Came In



Its Compliance

whoami

- ❖ **evan deters | eggvan**
- ❖ **ex-CCDC captain**
- ❖ **systems engineer @ Boeing**



whoami

- ❖ **Dylan Michalak**
- ❖ **4th year CS major**
- ❖ **CCDC**
 - Windows team 2023-2024
 - Captain 2024-2025
- ❖ **Other**
 - Co-Director of SWIFT Competitions
 - Threat Research Intern @ Binary Defense
 - I like rock climbing (basic, boring) and cooking (less basic, boring)



Table of Contents

| 01 Why Business?

| 02 Injects

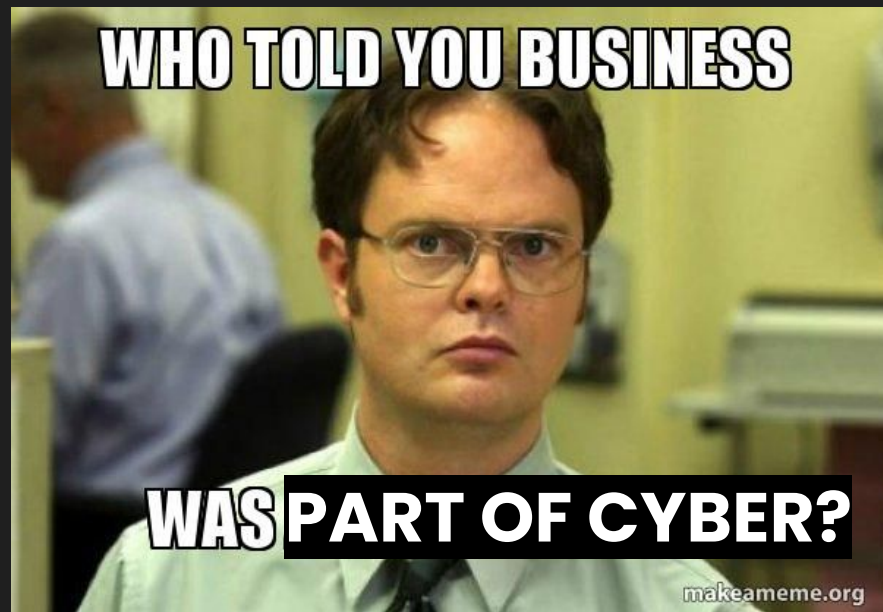
| 03 Forced Vacations

| 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%

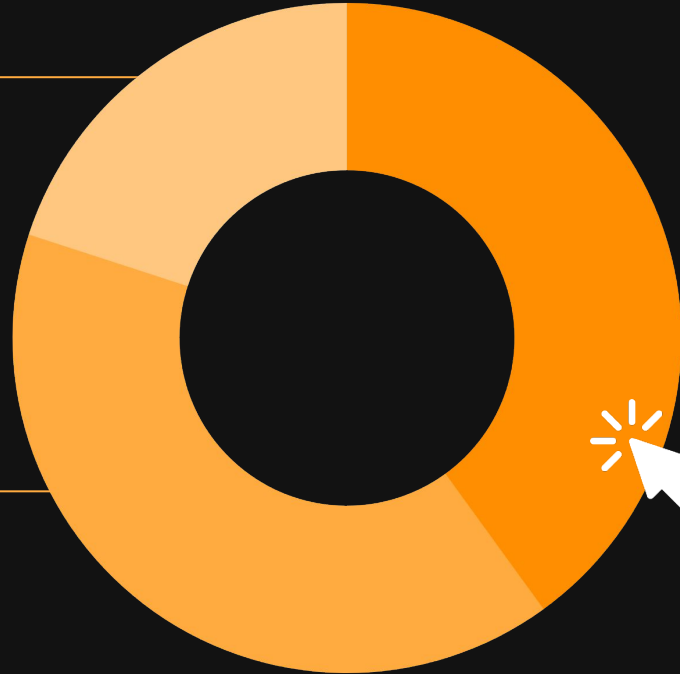
Orange team

40%

Services

40%

Business injects



Fundamental principles of cybersecurity



Integrity

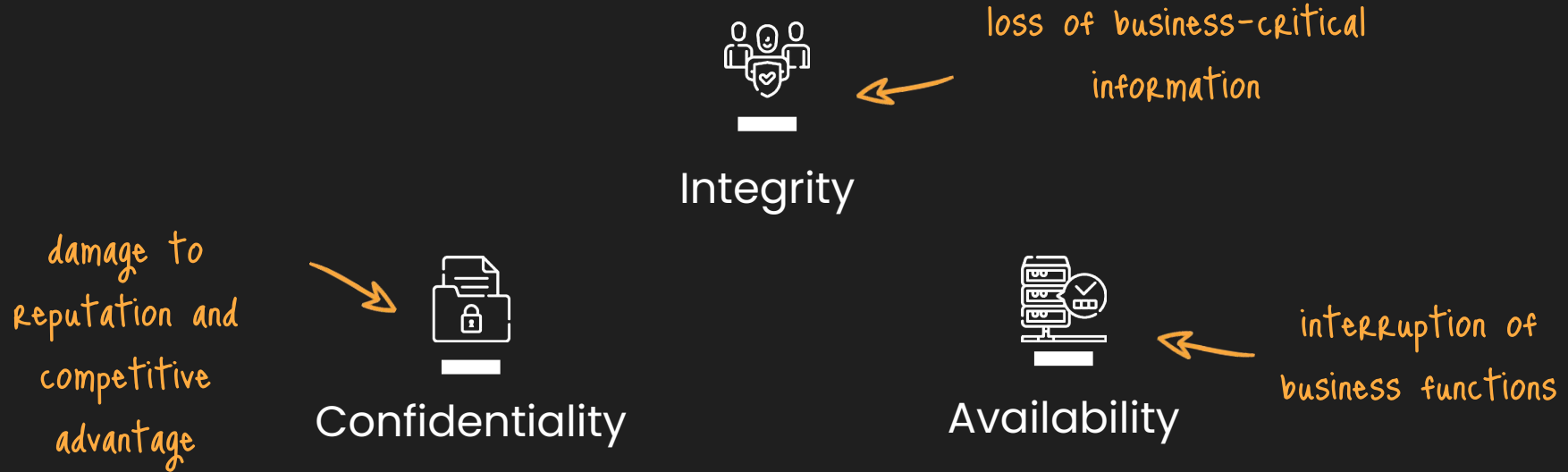


Confidentiality



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...



Infinite curveballs

They took gsuite from me

Technical tasks

Why do we need three firewalls VPNs??

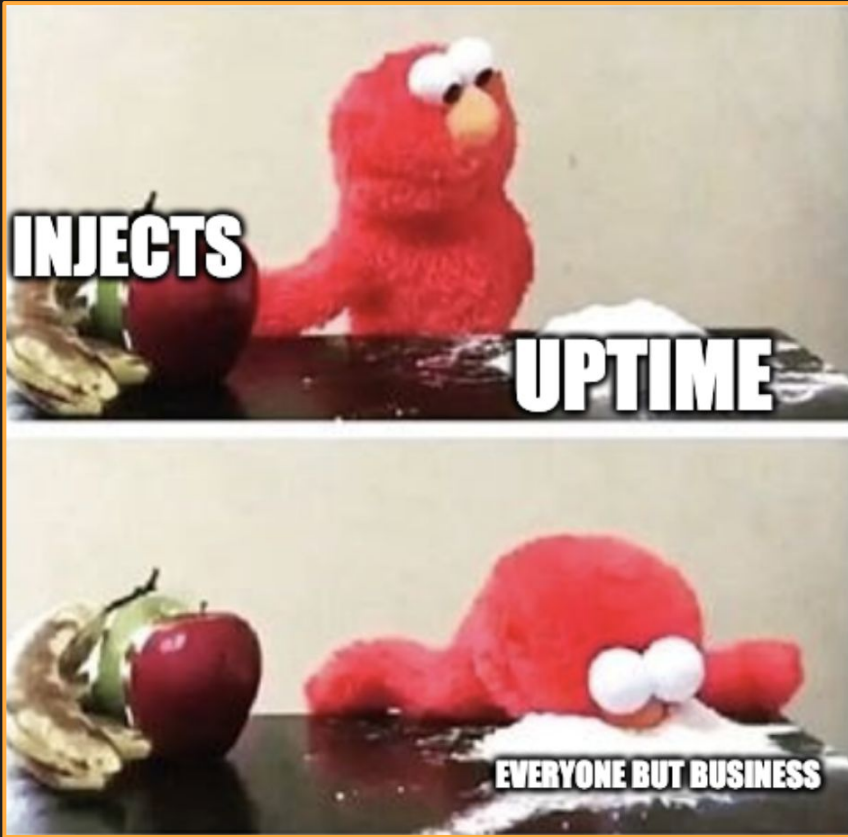
Broad understanding

What even is a cloud and why does it migrate???

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

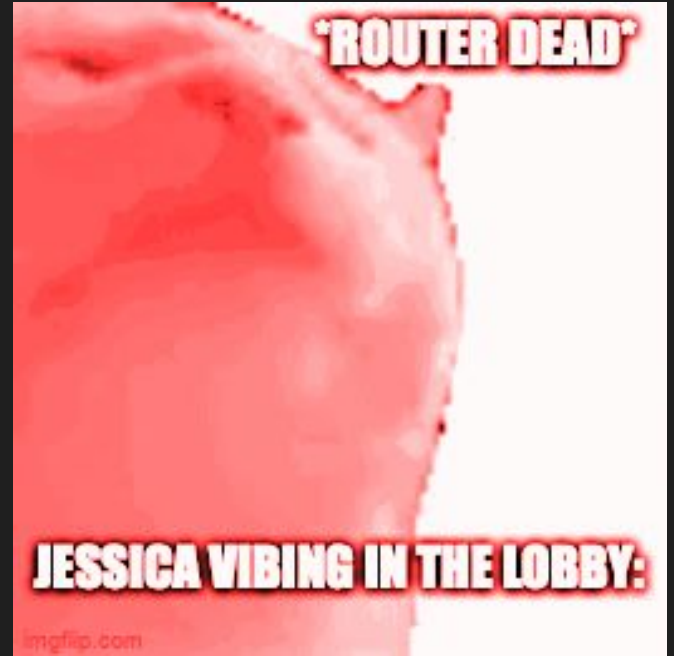


READ THE
PROMPT!

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's actually pretty valuable and has helped me a lot



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!

Yep! You're hired :0





It's 2:00am... you just got paged...

Scenario

- You work in the SOC at a bank
- Crowdstrike update went wrong
- 200 Windows machines are bricked

Objectives

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



Submit: <https://jessh.zip/week2-1>

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

Scenario

- CEO wakes to frozen transactions and stoppage of business
- "Why are we paying for a tool that destroyed our business?!"

Objectives

- 1 page report
- 30 minutes
- Explain and justify the usage of an EDR **to your C-Suite**



Submit: <https://jessh.zip/week2-2>

Manager

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

Submit: <https://jessh.zip/week2-1>

C-Suite

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

Submit: <https://jessh.zip/week2-2>

Homework!

Due July 27th @ 5 AM

<https://jessh.zip/ccdchw-2>