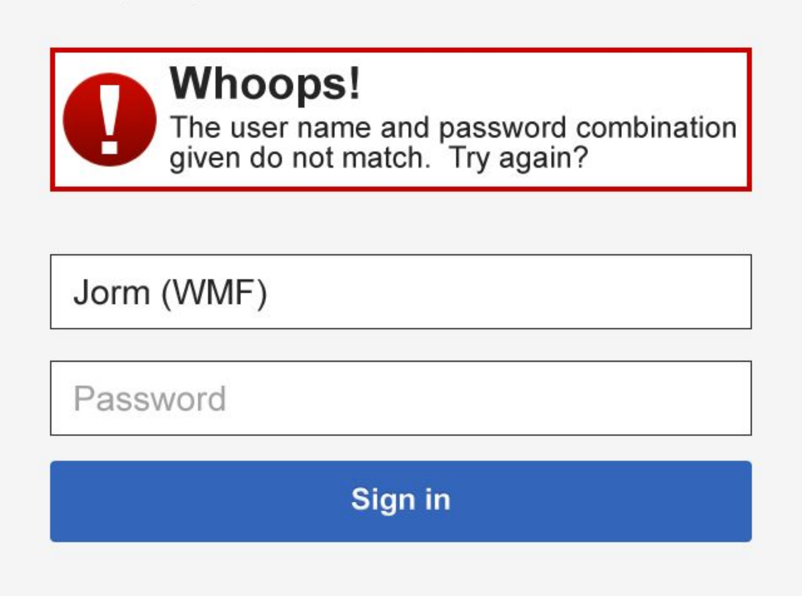
Insufficient Logging & Monitoring



Whoops!
The user name and password combination given do not match. Try again?

Jorm (WMF)

Content

- About Me
- The Impact on Your Business
- Thoughts of a Hacker
- A Lesson to Learn From
- Healthy Habits

Hello!

I am Sofia Chang,

Software Developer Intern at Teranet

Fourth-year Bcom in Business and Computer Science

The Impact on Your Business

How poor maintenance can lead to detrimental business implications

1

$4,770,000

Lost due to compromised accounts last year[1]

191+ days

Until breaches are detected[2]

100%

Of exploits could be successful[3]

[1] https://www.newswire.ca/news-releases/ibm-report-compromised-employee-accounts-led-to-most-expensive-data-breaches-over-past-year-832266970.html

[2] https://insights.securecodewarrior.com/coders-conquer-security-share-learn-series-insufficient-logging-and-monitoring/

[3] https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A10-Insufficient_Logging%252526Monitoring.html

Overview of the Vulnerability

When logs are unclear or lacking in data to show the full flow of action and monitoring is not able to notice suspicious behaviour near or in real-time.

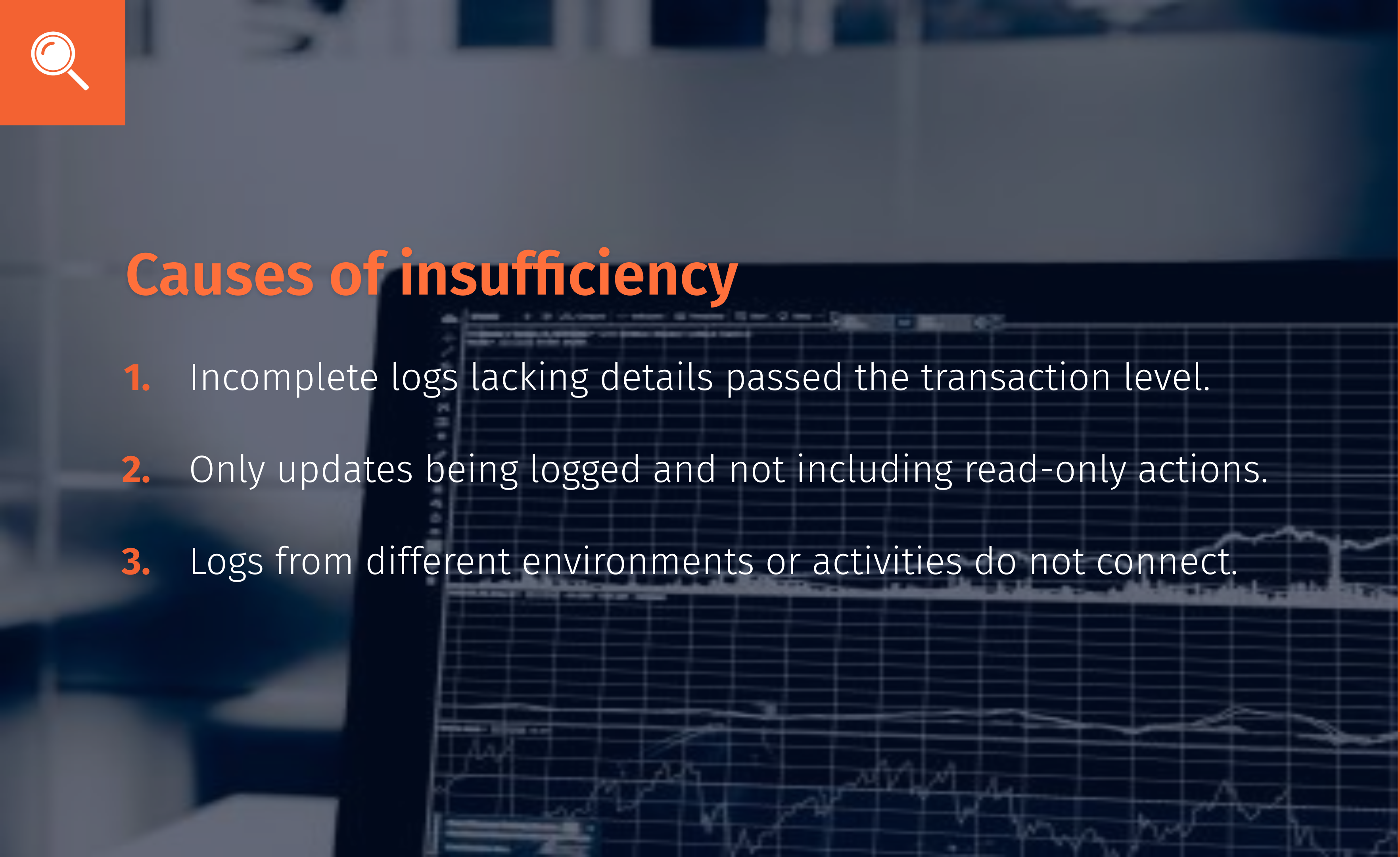
Their Role in Prevention and Recovery

Logging

- Track interactions
- Identify origin of attacks

Monitoring

- Provides information on environment
- Identity suspicious behaviour



Causes of insufficiency

1. Incomplete logs lacking details passed the transaction level.

2. Only updates being logged and not including read-only actions.

3. Logs from different environments or activities do not connect.

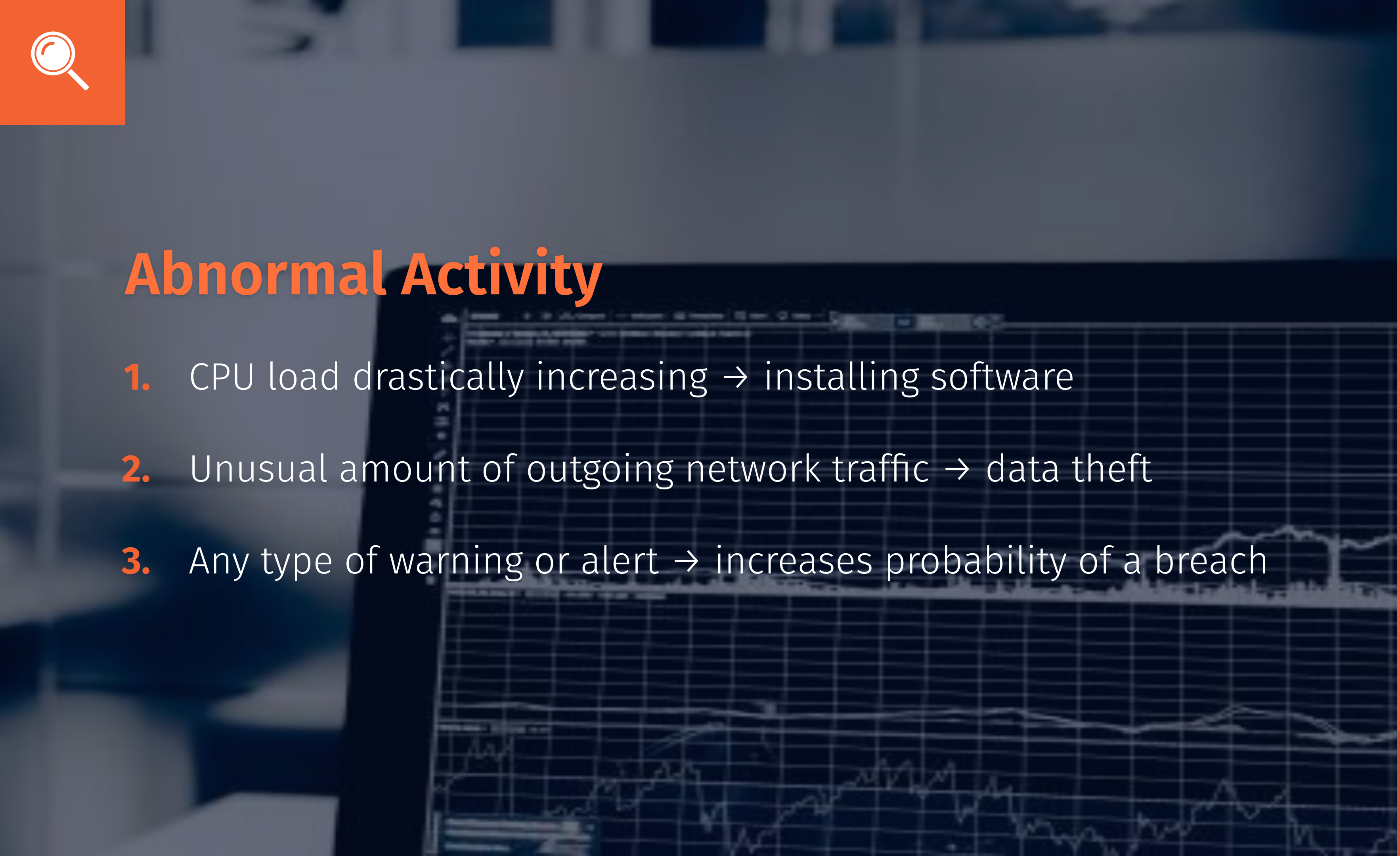
Thoughts of a Hacker

The different ways hackers can exploit your vulnerabilities

2

How to Take Advantage

- Unlogged auditable events
- Lack of warning and error messages
- Unmonitored
- Logs only stored locally
- Delayed alerts



Abnormal Activity

1. CPU load drastically increasing → installing software

2. Unusual amount of outgoing network traffic → data theft

3. Any type of warning or alert → increases probability of a breach

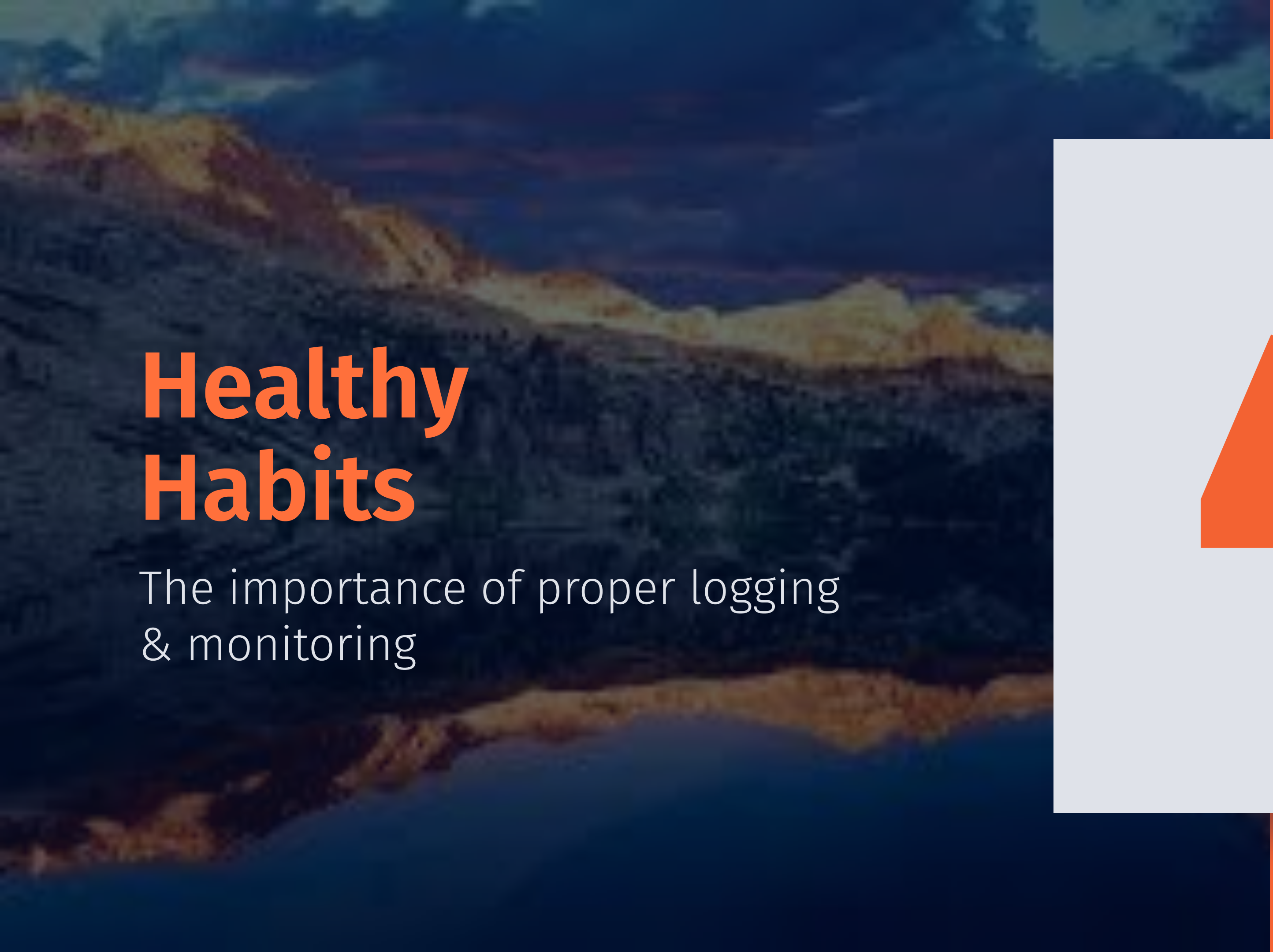
A Lesson to Learn From

Real world example of the impact to companies

3

LifeLabs

We don’t have all the information, but strong logging and monitoring plans could show us.



Healthy Habits

The importance of proper logging & monitoring

4

Creating a Plan

Develop

The overall plan for to base requirements, budget, and approach off.
The project overview.

Carry Out Requirements

Establishing aspects such as the scope, critical assets, potential attacks, mitigation strategy, technical controls, and current state.

Determine weak points

Identify which vulnerabilities are the most important for your organization to mitigate.

Creating a Plan Continued

Design

Build

Maintain

An effective design should satisfy all previous requirements and consider factors such as process, people, and IT

Utilize the tools and current services you have at your disposal with potentially adding new ones.

Keeps the plan relevant and effective. Without this all other steps are significantly less useful

Tips & Tricks

Use What You Have

A lot of your systems and applications will already produce logs for you.

Track It All

If it’s an auditable event, it is probably best to monitor it and track user access.

Clear & Concise

Have clear and concise warning and error alerts for effective tracking both in prevention and recovery.

High Value High Risk

Ensure all high-value activities are closely and easily traceable, as tampering or loss of data could be devastating.

Be Timely

The sooner you can act on attacks, the less detrimental they may be. Try to monitor in real-time when possible.

Helping Hands

Use third-party frameworks and CMS to your advantage to help you maintain your logs and monitoring

78%

Of breaches could be either prevented or mitigated with improved logging and monitoring practices.

https://www.immuniweb.com/blog/OWASP-insufficient-logging-and-monitoring.html

Thank You

Any questions?

You can find me at:

@sofia-chang

sofiamchang@gmail.com