OIC-CERT
Computer Emergency Response Team

CyberSecurity MALAYSIA

UTeM
اونيۏرسيتي تيکنيکل مليسيا ملاک
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

HANDLING INSIDER THREATS

Dr. Warusia Mohamed Yassin

PhD (Security In Computing)

warusia@gmail.com

+60165358502

7th March 2019

Sources: interest, informationAge

MANY THANKS.....

OIC-CERT COMMITTEE, CYBER SECURITY MALAYSIA & UTeM

OIC-CERT
Computer Emergency Response Team

CyberSecurity
MALAYSIA

UTeM
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

AGENDA

- Insider Threats
- Insider Threats Indication
- Insider Threats Detection & Prevention
- Insider Threats Response
- Guidelines to Combat Insider Threats

INSIDER THREATS

CERT's Definition

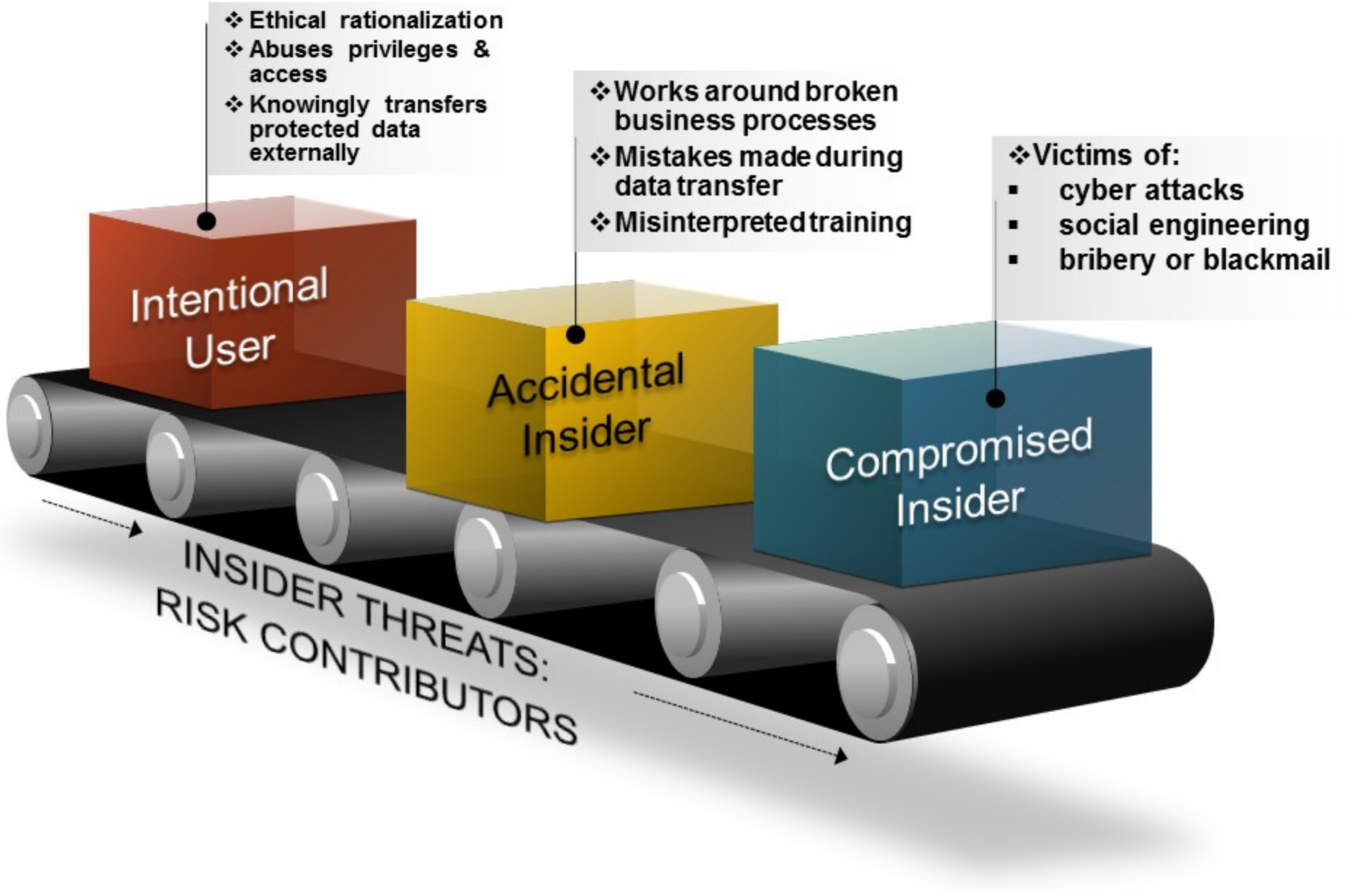
- *A person who has or had **authorized access** to an organization's network, system or data and **intentionally or accidently exceeded or misused that access** in a manner that negatively **affected the confidentiality, integrity, or availability** of the organization's information or information systems.*

Motive

- *To affect confidentiality, integrity and availability of Data, Systems and Operations*

Why Insider

- *Have privileged and legitimate access as well as know about the organization and its critical assets, i.e. current & former employee, vendors, business associates, victims…*



EXAMPLE OF INSIDER THREATS

EMPLOYEE| VENDOR| VICTIM

EMPLOYEE

1. An insider ran HR database queries in an attempt to find out how much the salary of everyone in the IT department was making, all the way up to the CTO.

2. Adam the insider gets fired and the administrator forgets to void Adam's (login) credentials. Adam goes home, logins into his work machine and takes some malicious action (introduces bugs into source, deletes files and backups, etc.…)

VENDOR

1. A broker based in the bank stock trading initiated thousands of transactions without customer permission in order to drive up his commissions.

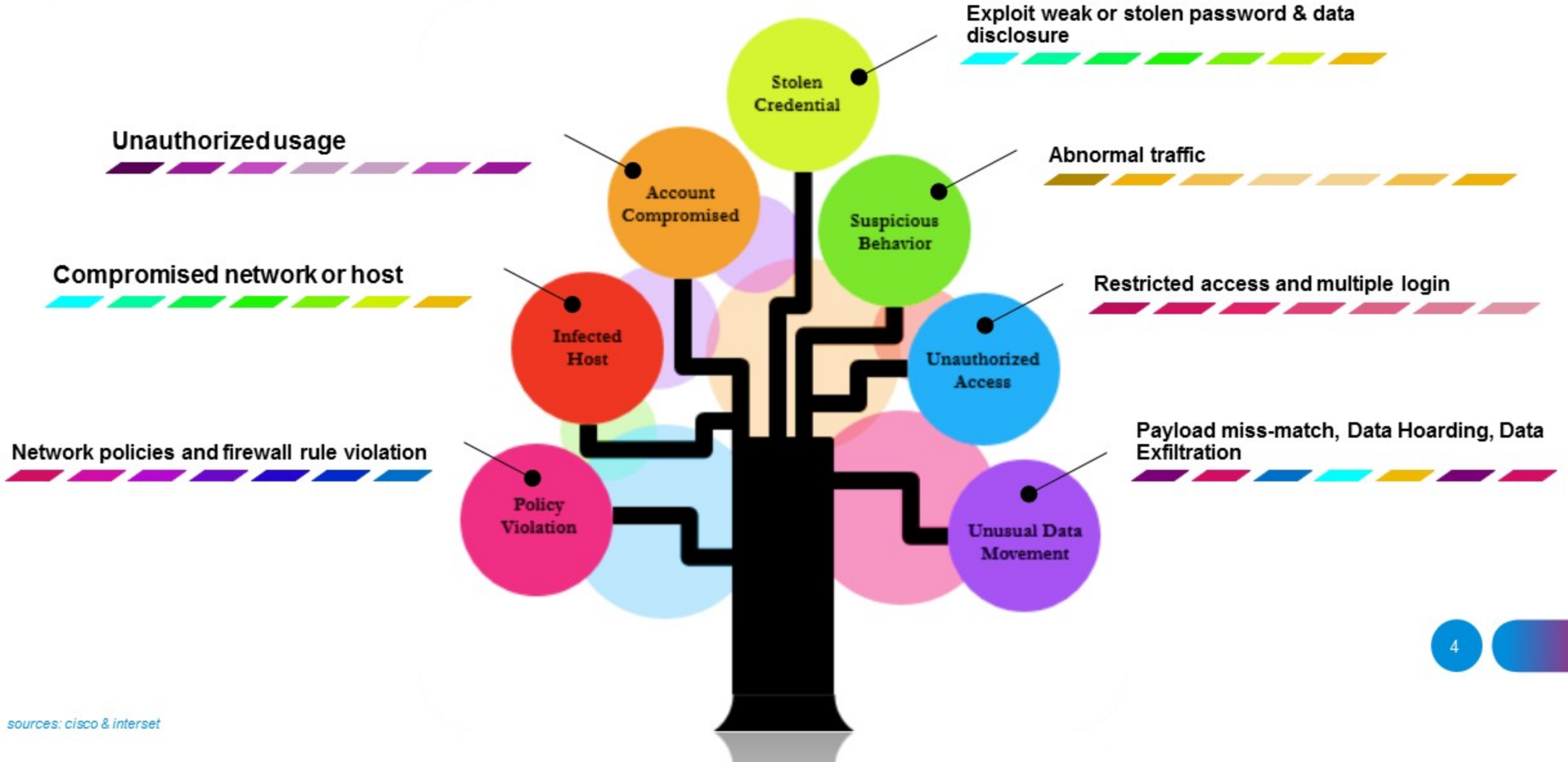
2. The system administer namely Vendor stole personal information of millions customers (credit card).

VICTIM

1. *Victim of spam email in which the attacker gain authorized access once password information leaked by privileged user.*

2. *Infected & Compromised host i.e. Botnet or C&C.*

INSIDER THREATS INDICATION



sources: cisco & interset

IMPACT OF INSIDER THREATS

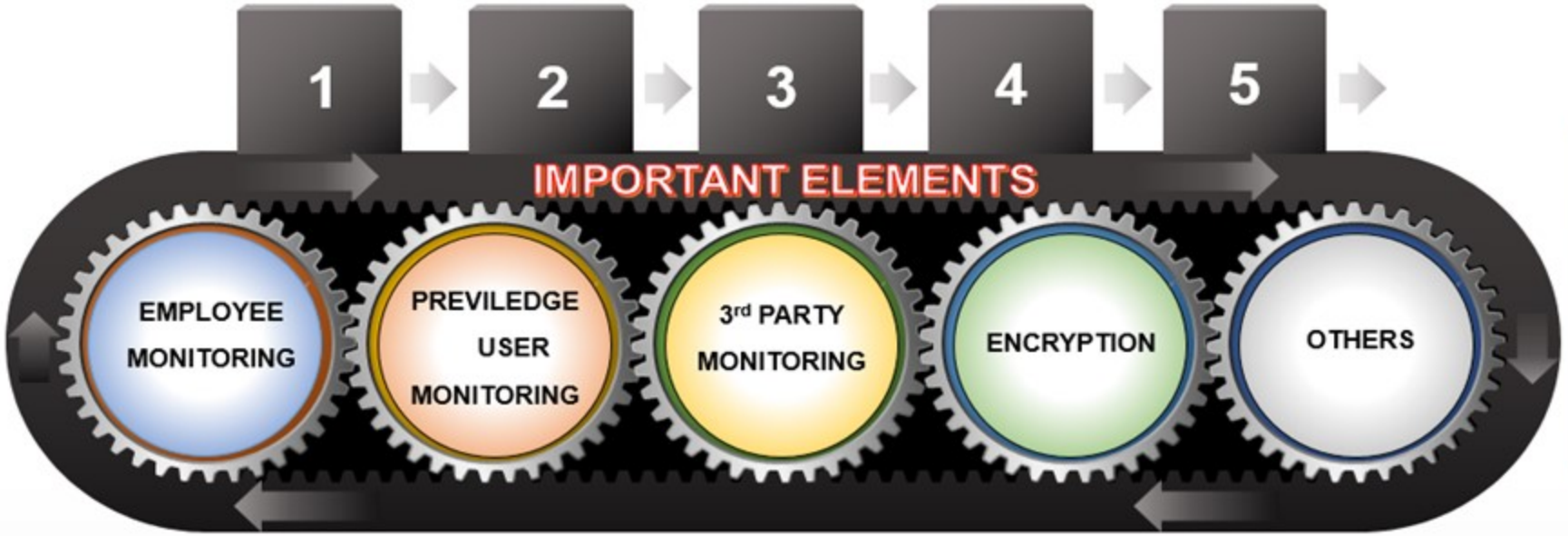
Bad reputation, data leakage, stealing valuable information, defacement…..

IMPACT EVERYONE……

Loss of confidential and controlled information……

sources: https://www.flaticon.com and CSO

INSIDER THREATS DETECTION & PREVENTION



1. Employee Monitoring

a. *Monitoring every single employee activity and. logging activities.*

b. *i.e. email logs, remote access logs, app logs, file and database access logs.*

2. Privileged User Monitoring

a. *Monitoring unauthorized changes, unnecessary access and abusing privileges.*

b. *i.e. creation of local accounts, creating backdoors and unauthorized access.*

3. 3rd Party Monitoring

a. *Abnormal remote access, Unauthorized changes, unscheduled tasks.*

b. *i.e. VPN during non-working hours passwords resets and installing backdoors.*

4. Encryption

a. *Employing effective and strong encryption.*

b. *i.e. prevent breaches of confidential data.*

5. Others

a. *Employing insider threat detection tools, training for employee, and etc.*

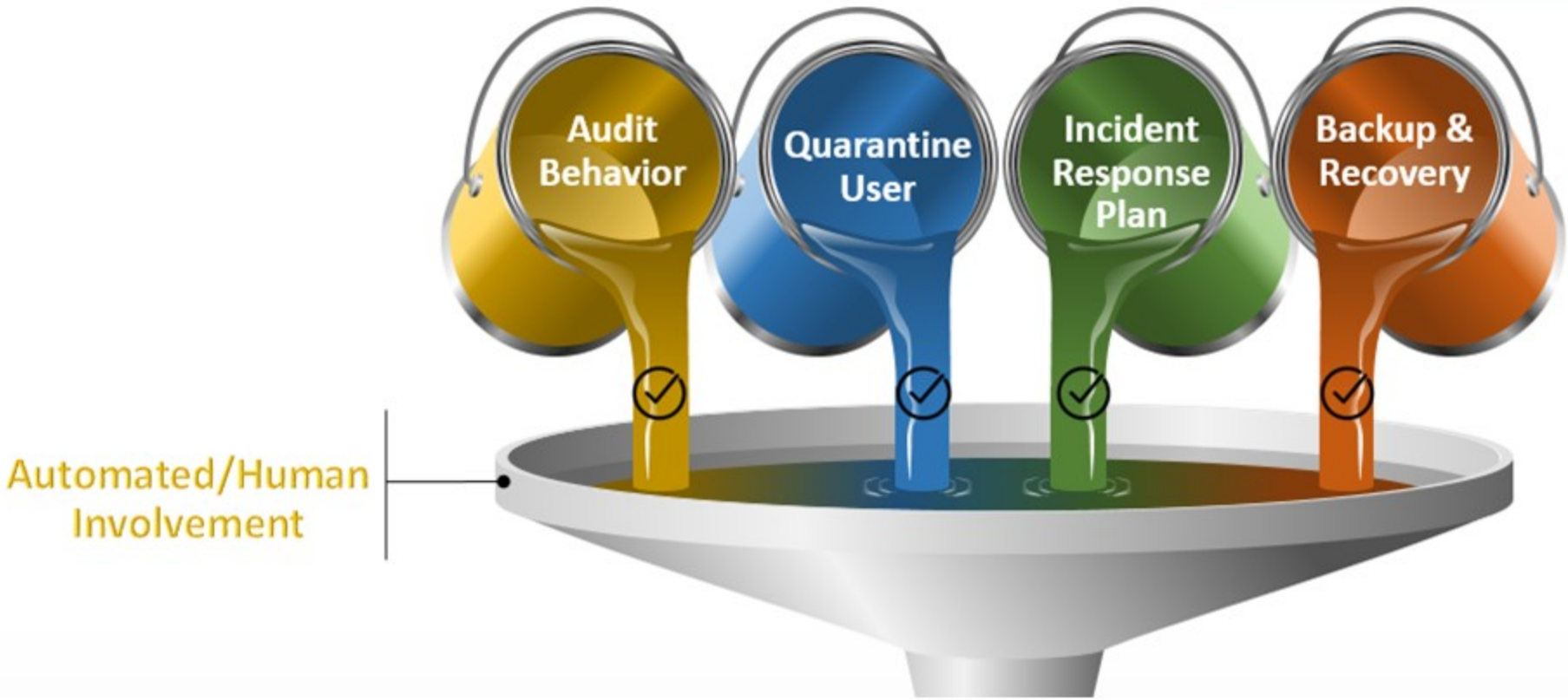
b. *i.e. remediate & mitigate insider threats as well as awareness training*

c. *Access control, split access, least privileged.*

sources: observeit

INSIDER THREATS RESPONSE

Action required responding to insider threats…



GUIDELINE TO COMBAT INSIDER THREATS

COMBAT INSIDER THREATS
TO MINIMIZE IMPACT

What if a "bad guy" is authorized to use your IT systems…?

Loss of confidential and controlled information……

sources: networkworld by linda
https://www.flaticon.com

GUIDELINE TO COMBAT INSIDER THREATS

human resources

employee verification process, examine suspicious behavior and security awareness training

least privileged

Enforce separation of duties and least privilege

password policy

Implement strict password and account management practices

GUIDELINE TO COMBAT INSIDER THREATS

logging activity

Log, monitor and audit employee online activity

defense layer

Use layered defense against attacks i.e. remote attacks

investigations

Collect and save data for use of investigations

INSIDER THREATS DETECTION APPROACH

Research opportunity ……. Detecting insider threats

CORRELATION

Log analysis, Scrutinized logs and event…

DETECTING ANOMALY

Profile-based detection, Classification (rule)…

DISCOVERING PATTERN

Behavioral analysis (suspicious user & device, machine learning)…

STATISTICAL ANALYSIS

Scoring and distance, Threshold…

INSIDER THREATS FACTORS

MACHINE

- technical impact on machine, misconfiguration

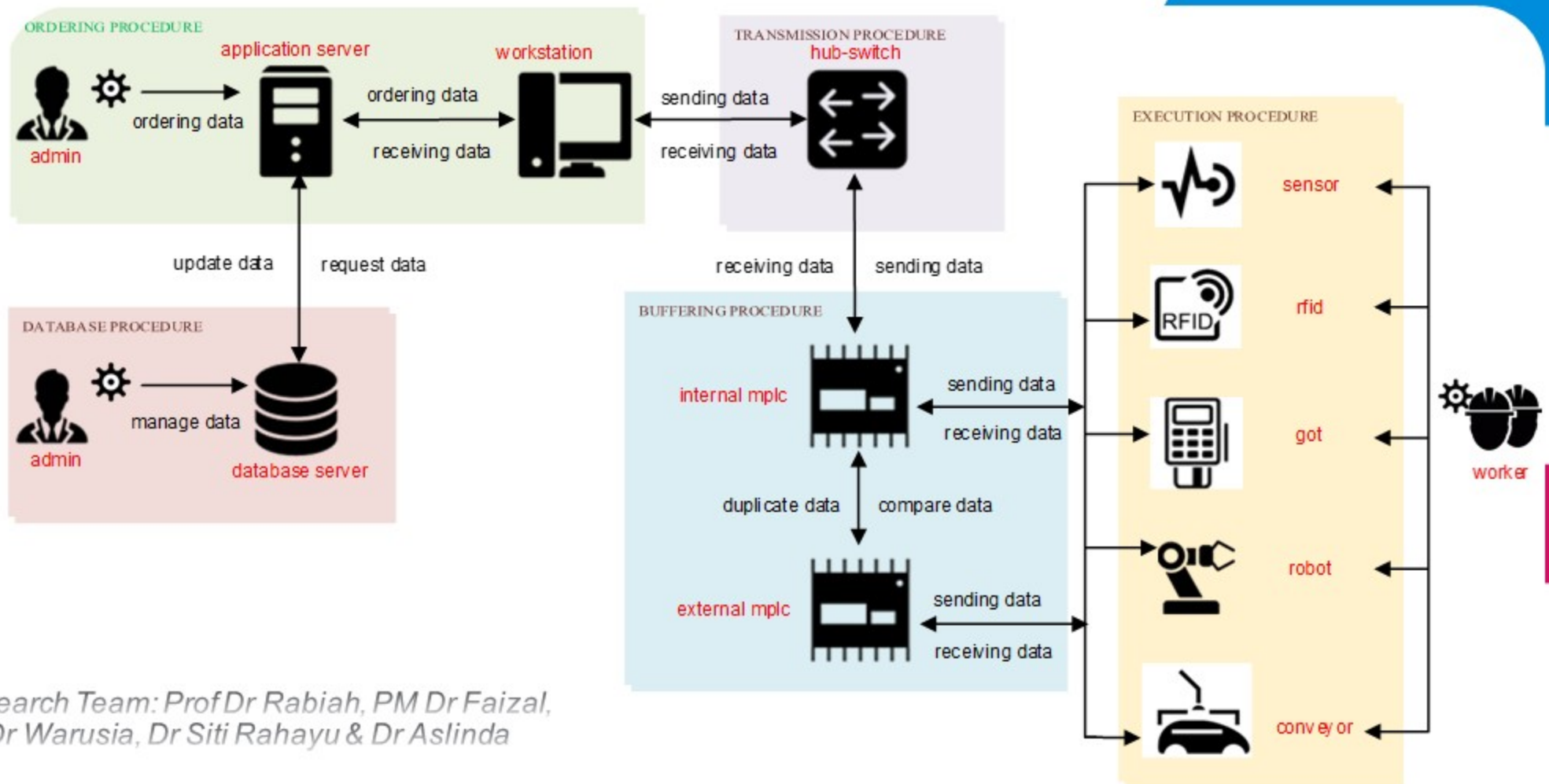
SYSTEM

- operational procedure, failure of production

HUMAN

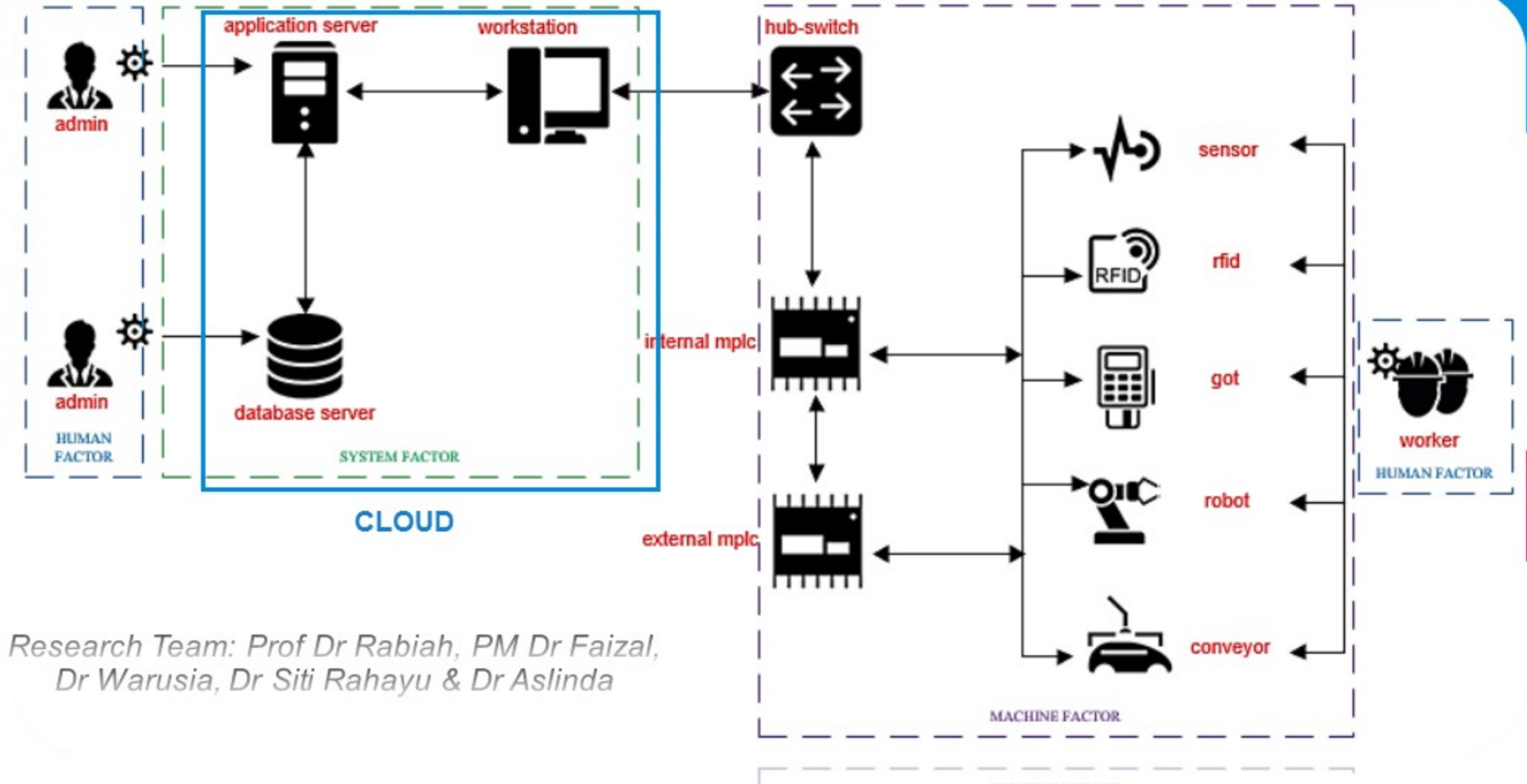
- employee behavior, unintentional threats, user personality

CURRENT RESEARCH UNDER TRGS
INSIDER THREATS DETECTION (MANUFACTURING)



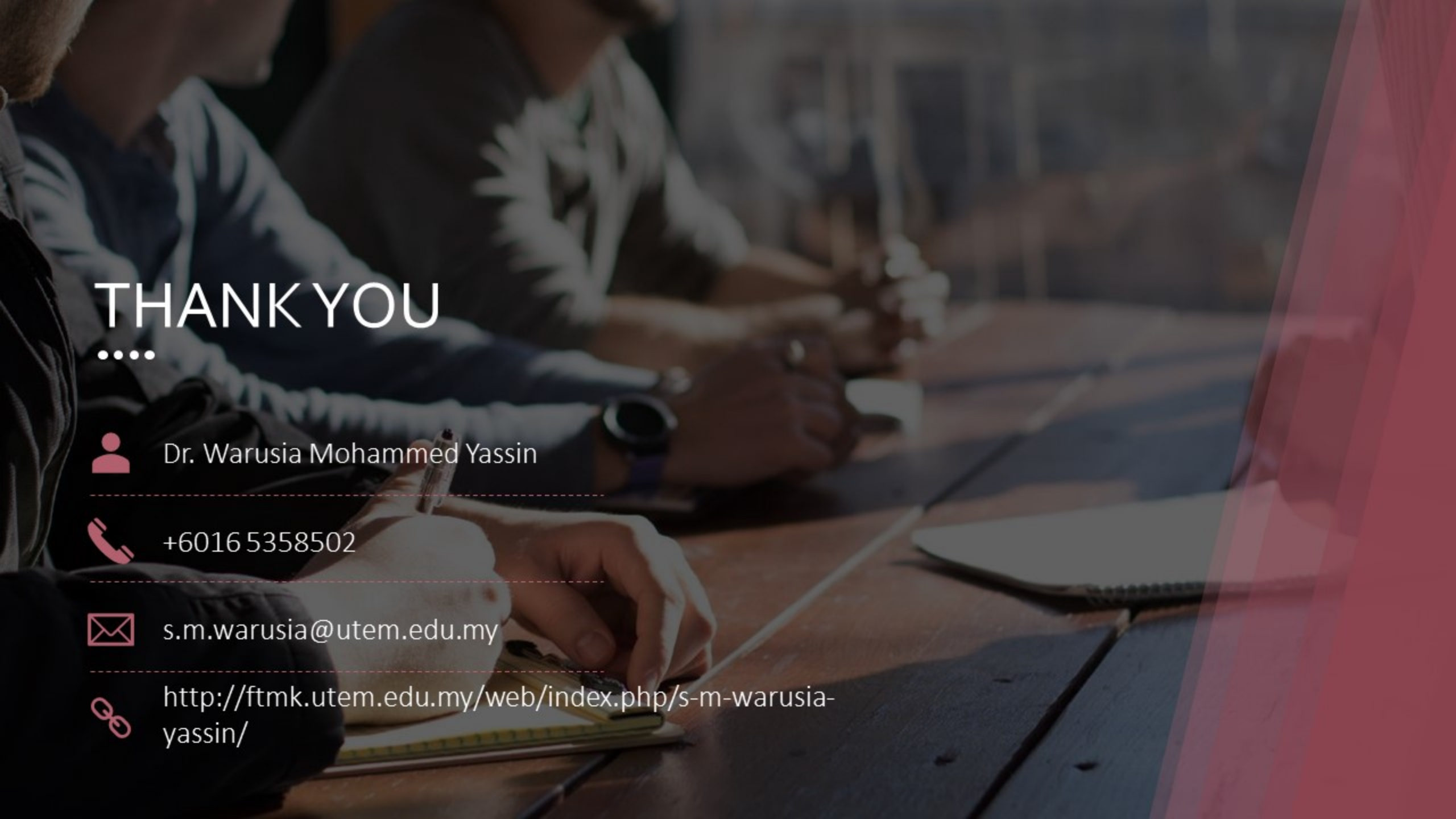
Research Team: Prof Dr Rabiah, PM Dr Faizal, Dr Warusia, Dr Siti Rahayu & Dr Aslinda

CURRENT RESEARCH UNDER TRGS
INSIDER THREATS DETECTION (MANUFACTURING)



Research Team: Prof Dr Rabiah, PM Dr Faizal, Dr Warusia, Dr Siti Rahayu & Dr Aslinda

Q & A



THANK YOU

Dr. Warusia Mohammed Yassin

+6016 5358502

s.m.warusia@utem.edu.my

http://ftmk.utem.edu.my/web/index.php/s-m-warusia-yassin/