NEXT GENERATION SECURITY OPERATION CENTER FRAMEWORK

INVENTOR: Ts. Dr. Mohamad Fadli Bin Zolkipli, Alan Yau Ti Dun
FACULTY: FACULTY OF COUMPUTER SYSTEMS & SOFTWARE ENGINEERING
UNIVERSITI MALAYSIA PAHANG, 26600 PEKAN, PAHANG, MALAYSIA
EMAIL: fadli@ump.edu.my
CO-INVENTORS: Azizah Binti Abdul Aziz, Tan Fui Bee

ITEX'18 29TH INTERNATIONAL INVENTION, INNOVATION & TECHNOLOGY EXHIBITION, MALAYSIA

www.ump.edu.my

1. INTRODUCTION

Security Operation Centers (SOC) are a **necessary monitoring security solution for organization who want to have visibility on cybersecurity assets.**

2. PROBLEM STATEMENT

Although there is existing framework that focusing on the technology aspect of SOC, there is **limited view on the elements that form the SOC** in term of people, process and technology. Organization often **failed to abstract ROI from the investment they invested on setting up SOC**.

3. GOAL

To implement a framework for Next Generation Security Operation Center (NGSOC)

4. OBJECTIVES

1. **To investigate the important of people, process and technology in security operation center.**
2. **To design an event correlation process based on pattern identification of security threads.**
3. **To integrate people, process and technology which will determine the effectiveness of the NGSOC**

5. INTELLECTUAL PROPERTY

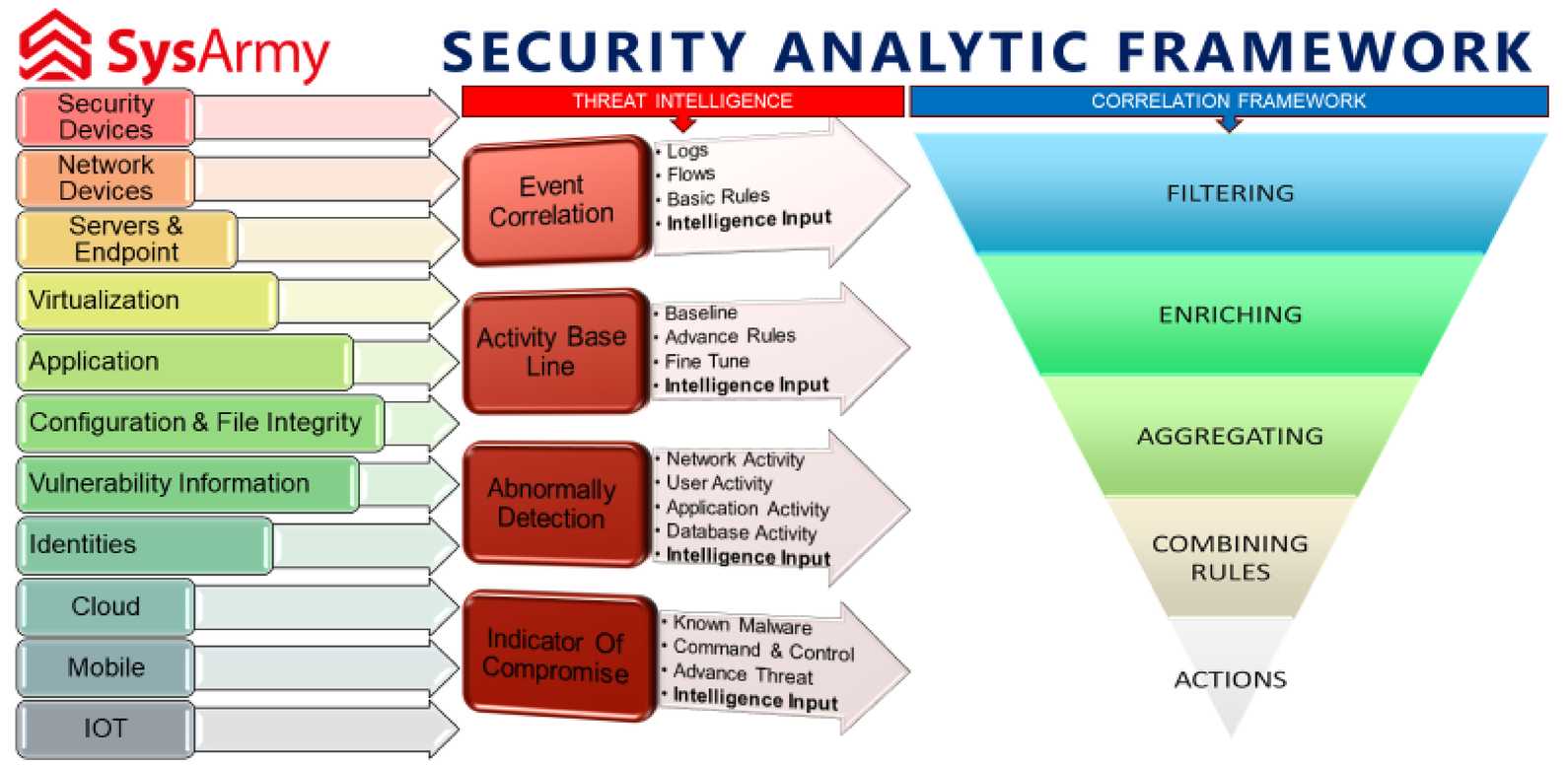
MyIPO **LY2018001778**

6. FRAMEWORK

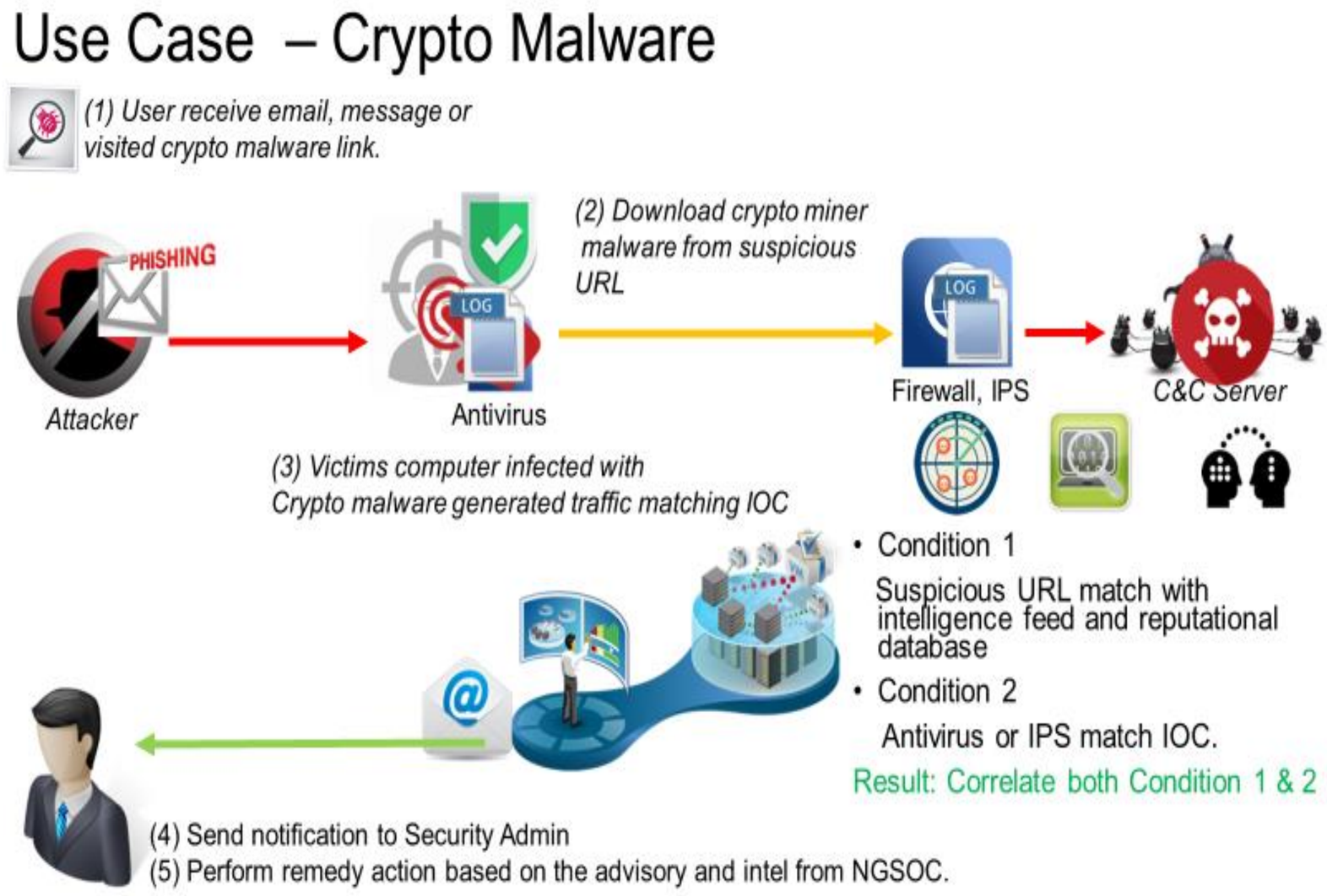
The building block of security operation center is people, process and technology. These building block can be further broken down to 6 domain as describe in table below.

Domain	Subdomain
A - Stakeholder	Stakeholder Needs
	Service Management
	NGSOC Management
	Stakeholder Reporting
B - Governance	Facilities Management
	People Management
	Operational management
	Certification
C - Security	Policy, Procedure and Process
	Physical Security
	Technical Security
	Data Security
	People Security
D - Technical	Architecture
	Technology Selection
	Tool Selection
	Operations
E - Functionality	Identify
	Protect
	Detect
	Response
	Forensics
F - Intelligence	Threat Intelligence
	Campaign Awareness

7.SECURITY ANALYTIC FLOW



8. CASE STUDY – ACTIVE MONITORING



9. BENEFITS

- Provide **comprehensive framework** for organization who need to build their own SOC or to engage 3rd party to provide SOC as a service
- Improvement of **cybersecurity threat detection**
- Advantage **to strategize defends against cyber attack**

10. PUBLICATIONS

1. Methods for Preventing Distributed Denial of Service Attacks in Cloud Computing - **Advanced Science Letters 23 (6), 5282-5285, 2017.**
2. Why Cloud Monitoring Service? An Intensive Review for the Importance Cloud Monitoring Tools - **IEEE Xplore, 2016.**
3. Active Monitoring for Hermes Ransomware v2.1 using Complex Correlation Rules In Next Generation Security Operation Center (NGSOC) – **UMP NCORN**

11. COMMERCIALIZATION

Commercial solution provided by NGSOC in the form of services is currently subscribed by more than 40 organizations at the moment including MNC, GLC and Telco.

Next Generation Security Operation Center

- **Cybersecurity Monitoring Services 24 x 7**
- **External Web Application Penetration Test As A Services**
- **External Penetration Test As A Services**
- **Forensic**

NGSOC had been commercialized at more than 40 organizations at the moment including MNC, GLC and Telco.

12. COLLABORATIONS

MSC Status Grant

An agency under MOSTI

Industrial Research Grant UIC170802

13. CONCLUSIONS

NGSOC will create significant impact on organization security posture :

- **It is significant to protect organization network including government and private sector which contain critical data and sensitive information against cyber threat**
- **Organization will be able to identify, protect, detect and response against cyber attack**

14. ACHIEVEMENTS

Malaysian Cyber Security Award 2016 – Cyber Security Innovation of The Year
Citrex 2018 - Gold Medal