# Build your own SOC

Kitisak Jirawannakool

Information Security Specialist

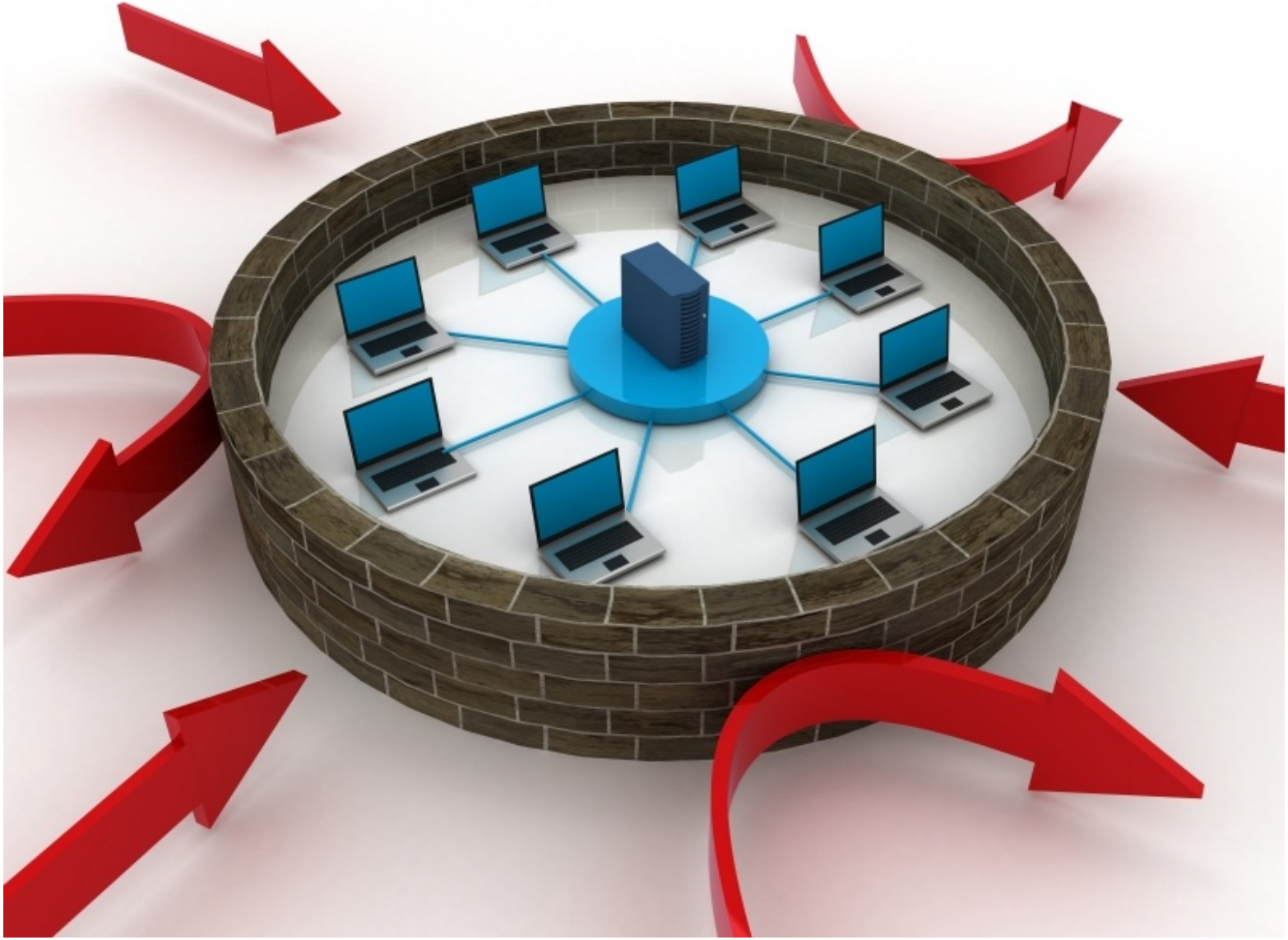
E-Government Agency (Public Organization)

kitisak.jirawannakool@ega.or.th

# Agenda

- Overview
- What is SOC?
- SOC ’s components
- Incident Response Plan

# Overview - Typical IT Security



# But.....


More Security Doesn't Make You More Secure
Better Management Does.

# Controls will be bypassed

# Traditional Incident Response

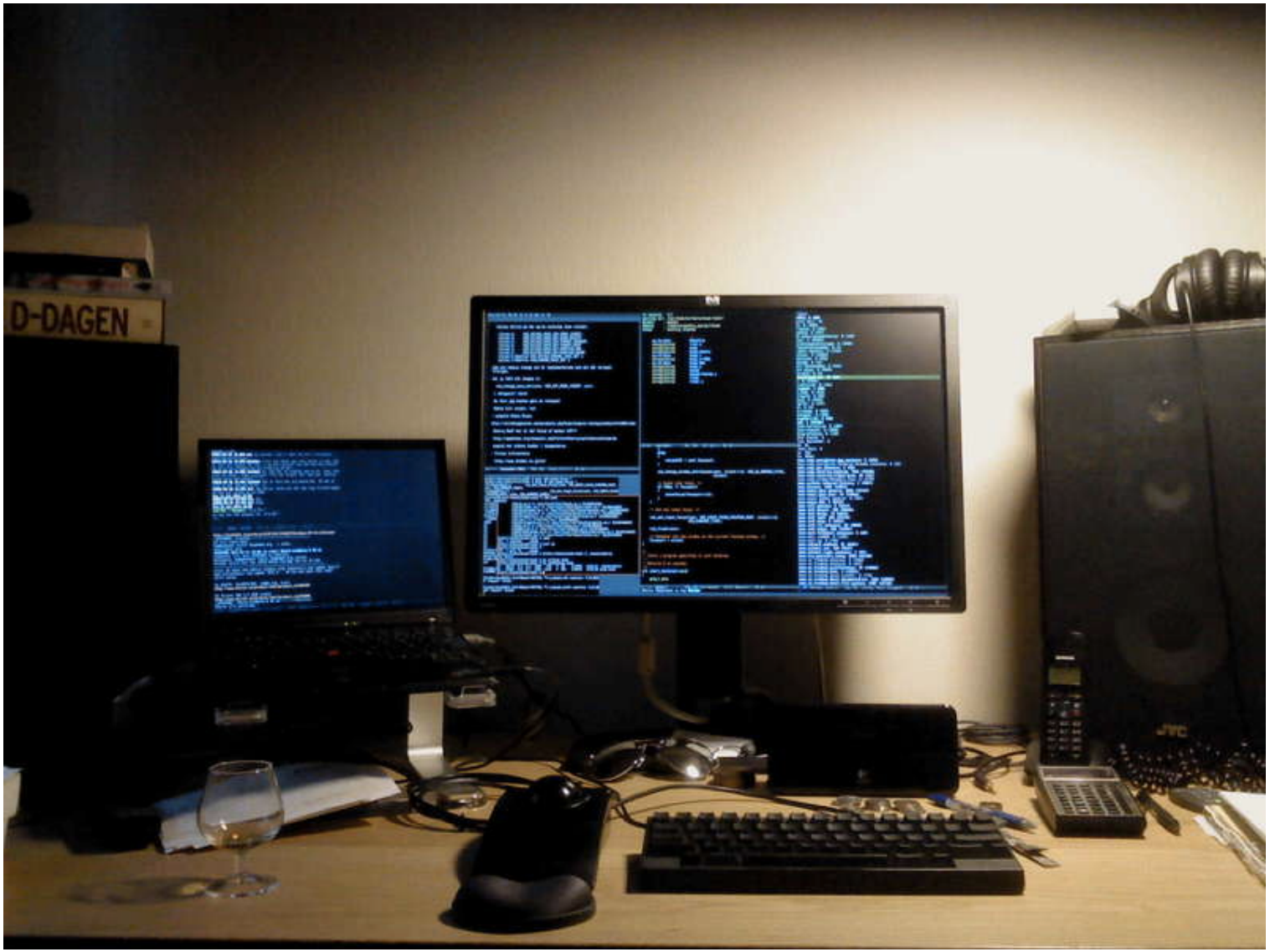
- Adhoc & Unplanned
- Deal with it as it happens
- Prolonged Recovery Times
- Damage to Company
- Lack of Metrics
- Legal Issues
- Bad Guys/Gals Getting Away

# You In Line of Fire

# What is SOC in your mind?


https://networkboxusa.files.wordpress.com/2013/09/network_box_security_operations_centre_1.jpg

# But .....




http://hack.org/mc/images/desk-20110721.jpg

# What is SOC?

- Stand for "Security Operations Center"
- PPT involved in providing situational awareness through the …
  - Detection of IT threats
  - Containment of IT threats
  - Remediation of IT threats
- Also monitors applications to identify a possible cyber-attack or intrusion (event) and determine

# Why do we need SOC?

- Central location to collect information on threats
  - External Threats
  - Internal Threats
  - User activity
  - Loss of systems and personal or sensitive data
  - Provide evidence in investigations
- Keep your organization running
  - Health of your network and systems

# Isn't a Firewall, IDS or AV enough?

- Firewall is active and known by attackers
  - Protects your systems, not your users
- Anti-Virus
  - Lag time to catch new threats
  - Matches files, but not traffic patterns
- IDS alerts on events, but doesn't provide context
  - System logs
  - Proxy logs
  - DNS logs
  - Information from other people

# Main functions

- Real-time monitoring / management
  - Aggregate logs
  - Aggregate more than logs
  - Coordinate response and remediation
  - "Google Earth" view from a security perspective
- Reporting / Custom views
  - Security Professionals
  - Executives
  - Auditors
  - Consistent
- After-Action Analysis
  - Forensics
  - Investigation
  - Automate Remediation

# Components of SOC

- People
  - SOC Staffs
  - Users
  - Managements
- Process
  - Incidents response process
  - Media handling process
- Technology
  - SIEM
  - IR System

# SOC Staffs (Ideal)

- Analysts
  - Level 1 : Security Operators
  - Level 2 : Security Analysts
  - Level 3 : Security Incident Manager
- SOC Operations Manager
- SOC Support Team
  - Supports
  - Helpdesks
  - Vendors

# SOC Operational Model

L3 : Security Incident Manager

SOC Management Team

Central Systems (SIEM, Incident DB, and KM)

L2 : Security Analysts

L1 : Security Operators

SOC Support Team (Support, Helpdesk, Vendor, and etc.)

# Analysts (the meat of the operation)

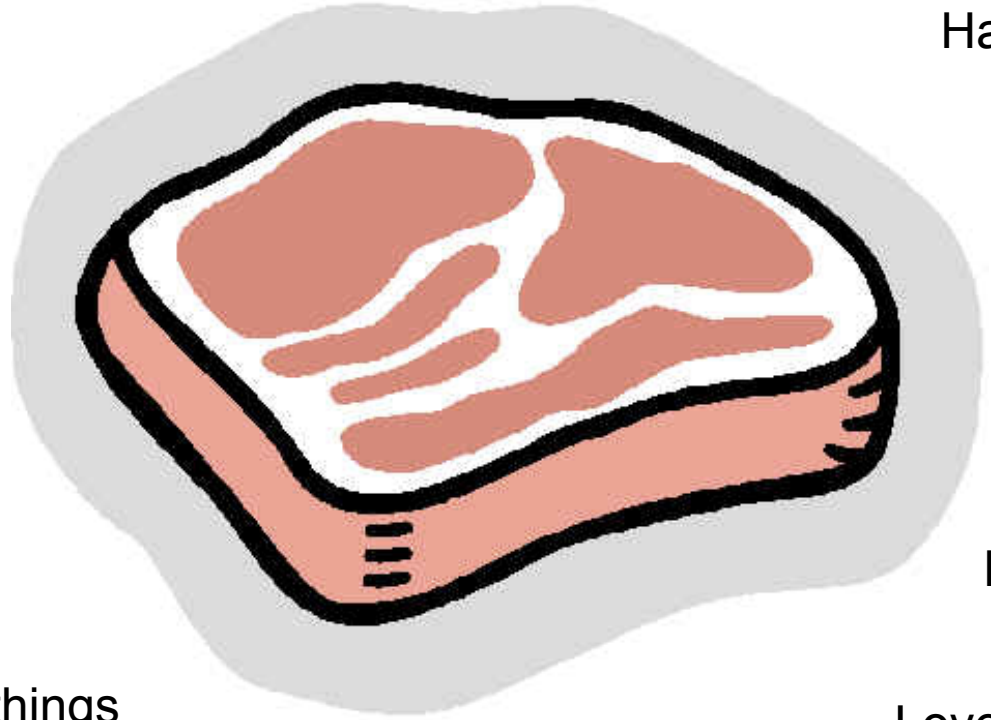
- You need highly skilled people who:

Are good at deductive reasoning and critical thinking

Know networking

Have a passion for this

Understand attacks



Don’t blink

Understand Malware

Are creative thinkers

Are open to new ideas

Don’t ever call in sick

Are comfortable with things like source code, hex, etc…

Love to keep learning

Don’t need sleep

# Other Experts

- System/Network Administrators
  - Keep the whole thing working
  - Tune IDS rules
- Forensics Experts
  - For more in-depth analysis
- Incident Response
  - To mitigate incidents after they happen
- External entities
  - Government, law enforcement, etc…

# Users (the other white meat)

- Report things
  - Phishing emails
  - Stolen property
  - Loss of data
- Do things
  - Download malware
  - Engage in inappropriate activities
- The most widely deployed IDS you have
  - If "tuned" properly…

# Management

- To interface with other entities
- Keep all the pieces from falling apart
- Make it rain (decide who gets the money)
- I guess someone has to make decisions...

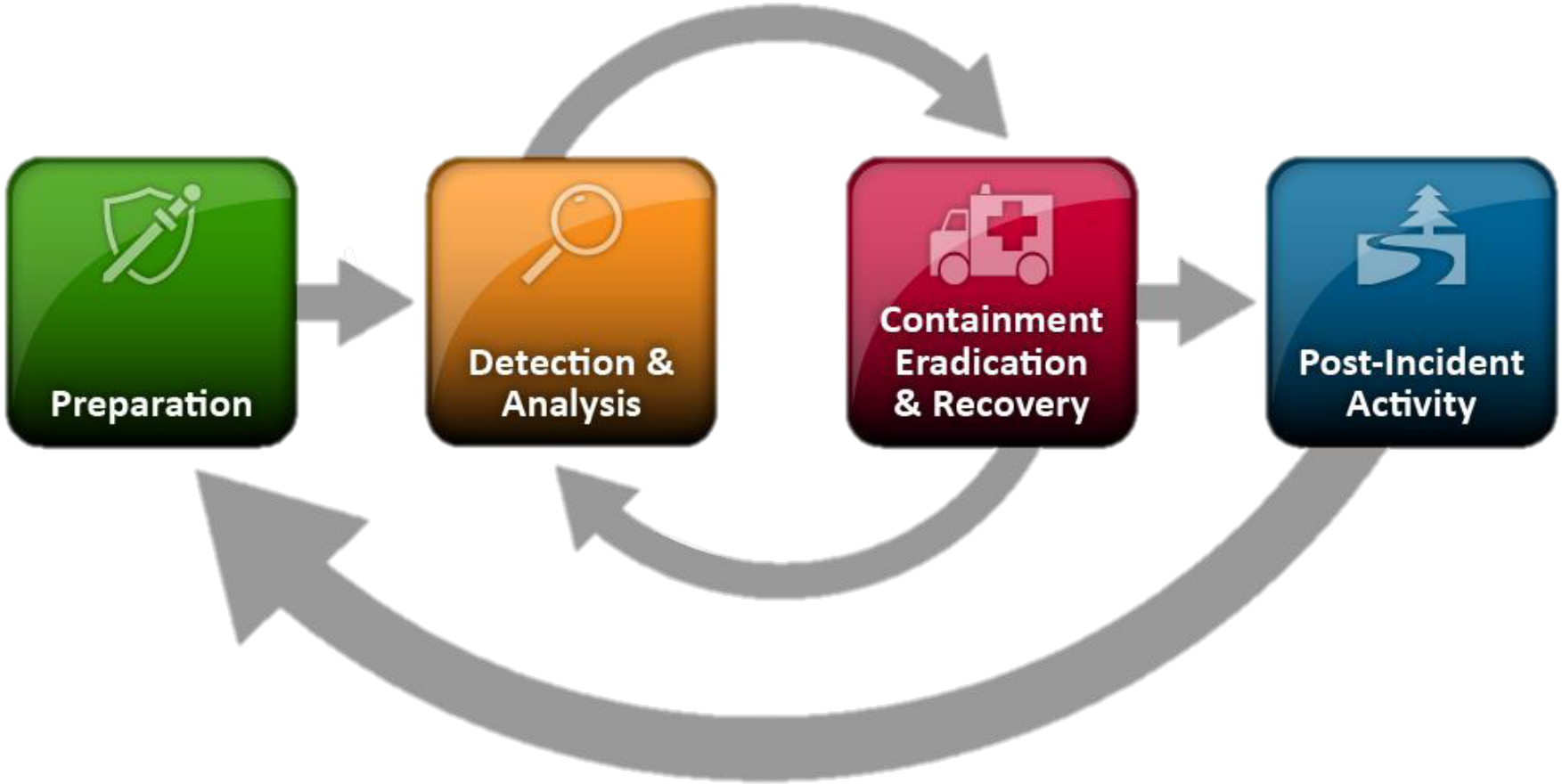
# Need to concern about SOC Staffs

- Shifting
- Training
- Boring job
- Turn over


http://www.pcghr.net/images/aboutUsimage.jpg

# Processes

- Incident Response plan



# IR Plan - Preparation

- Build the secured infrastructure
- Security policy
- Setup the monitoring system
- Prepare IR Team and process

# IR Plan - Detect & Analysis

- Setup the monitoring system
- Read logs
- Maybe someone reports
- Analysis when something's happened

# IR Plan - Response, Eradication and Recovery

- Find the attackers and how
- Remove or correct the system
- Operate the system again

# IR Plan - Post incident activities

- Study from the attacks
- Prepare the protections
- Keep record

# GovMon's IR Process (Example)

Monitoring System

SoC Staffs

EGA Contact Center

# Where the incidents come from?

- GovMon (SoC team)
- Log
- Monitoring tools
- Vendors
- CERTs or CSIRTs team

# IR Process (SoC Team)

Monitoring System

2. Found Incident

Incident

1. Keep Monitoring


3. Investigating

SoC Staffs

4. Alert to customers via EGA Contact Center and keep monitoring again

EGA Contact Center

# Incident categories

- Scan
- DoS
- Brute Force
- Malicious Code
- Exploit
- Traffic Anomaly
- Log Not Received
- System Service Down
- Log Format Error

# IR Process

EGA Helpdesk

1. Helpdesk notify User via E-mail and Phone

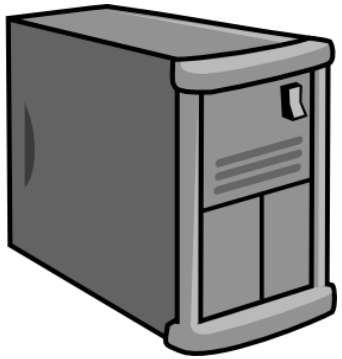
User

3. User reply to Helpdesk
- receive already
- fix already
- accept the risk
- require EGA's help

2. Check the system deeply

4. Helpdesk inform to SoC

SoC Staffs



Servers and Network

# What will we do, when incident is occurred?

- Close your eyes and ...
  - Just ignore?
  - Let it be?
  - Pray?
  - Laugh at yourself?
  - Blame others?

- Or take some actions?

# If you found attack by yourself, ....

User

1. Someone report or you found by yourself

2. Solve the problems

Incident

3. Inform to Helpdesk to keep recording or ask for help from EGA

EGA Helpdesk

4. Helpdesk will forward your requests to SoC

SoC Staffs

# Technology (SIEM)

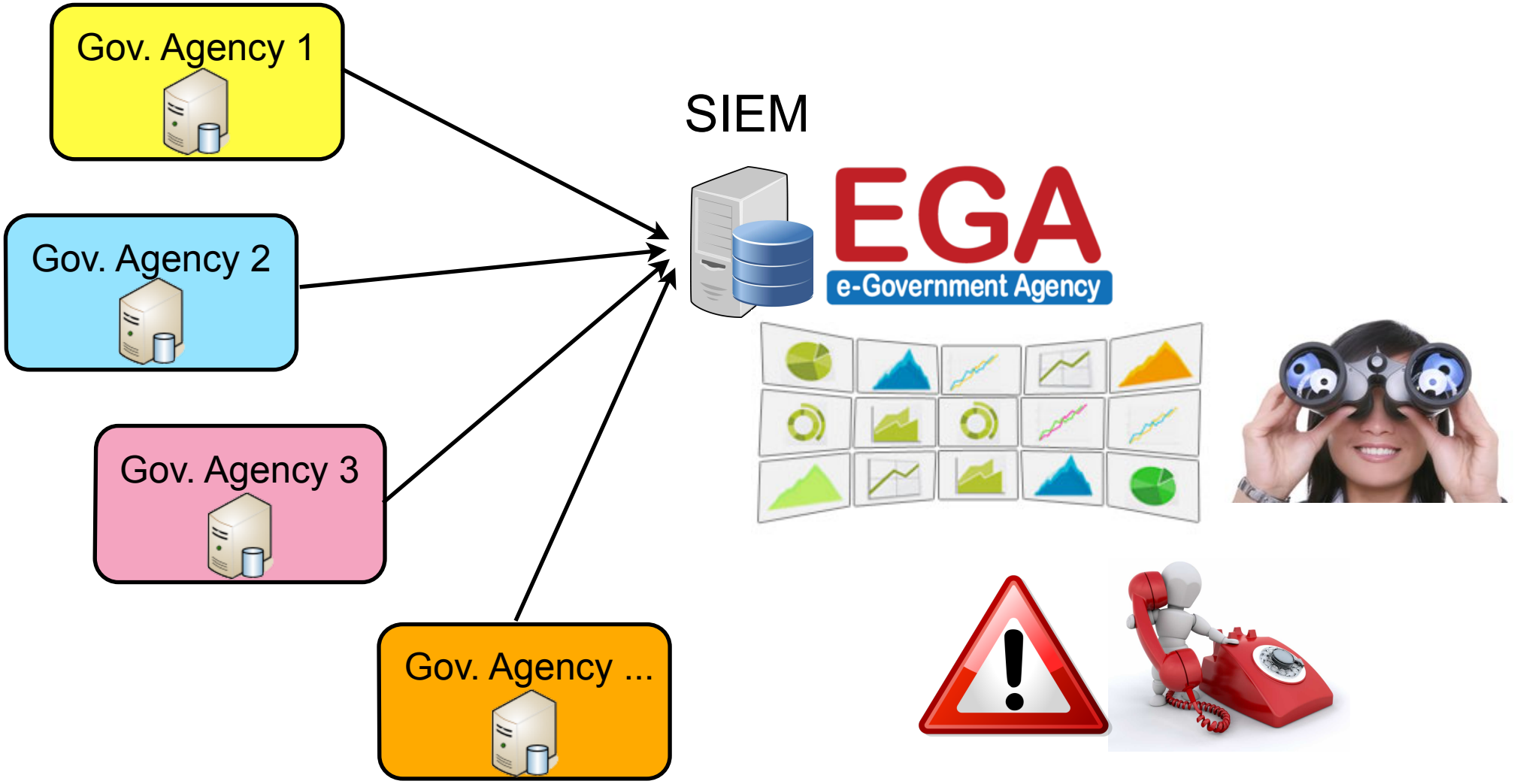
- SIEM = SIM + SEM
- Provides real-time analysis of security alerts generated by network hardware and applications
  - Data aggregation
  - Correlation
  - Alerting
  - Dashboards
  - Compliance
  - Retention
  - Forensic analysis

# SIEM and LM

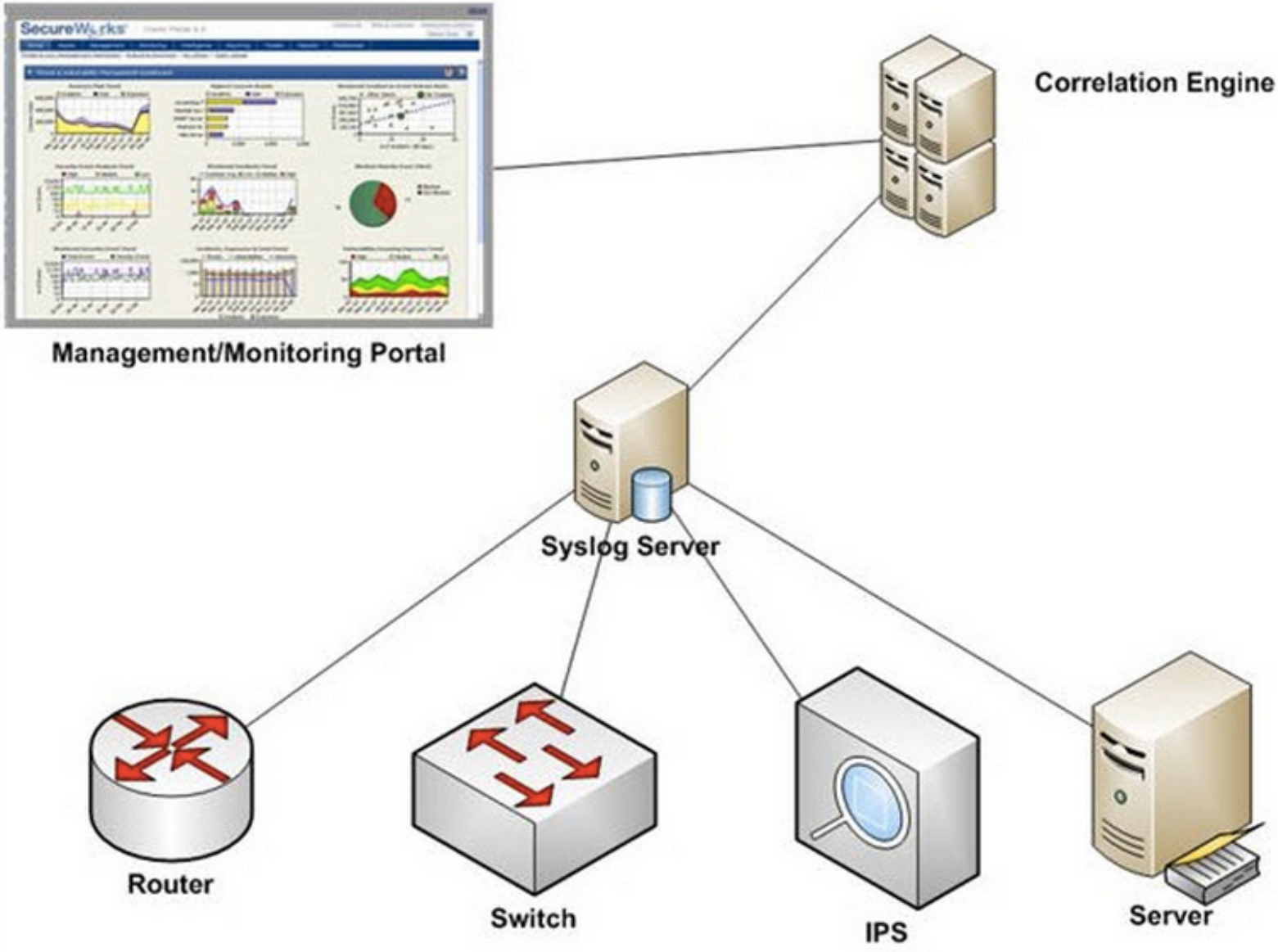
- SIEM
- Security Information and Event Management
- Focus on Security use of logs and other data

- LM
- Log Management
- Focus on all users for Logs

# SIEM (big picture)



# More details



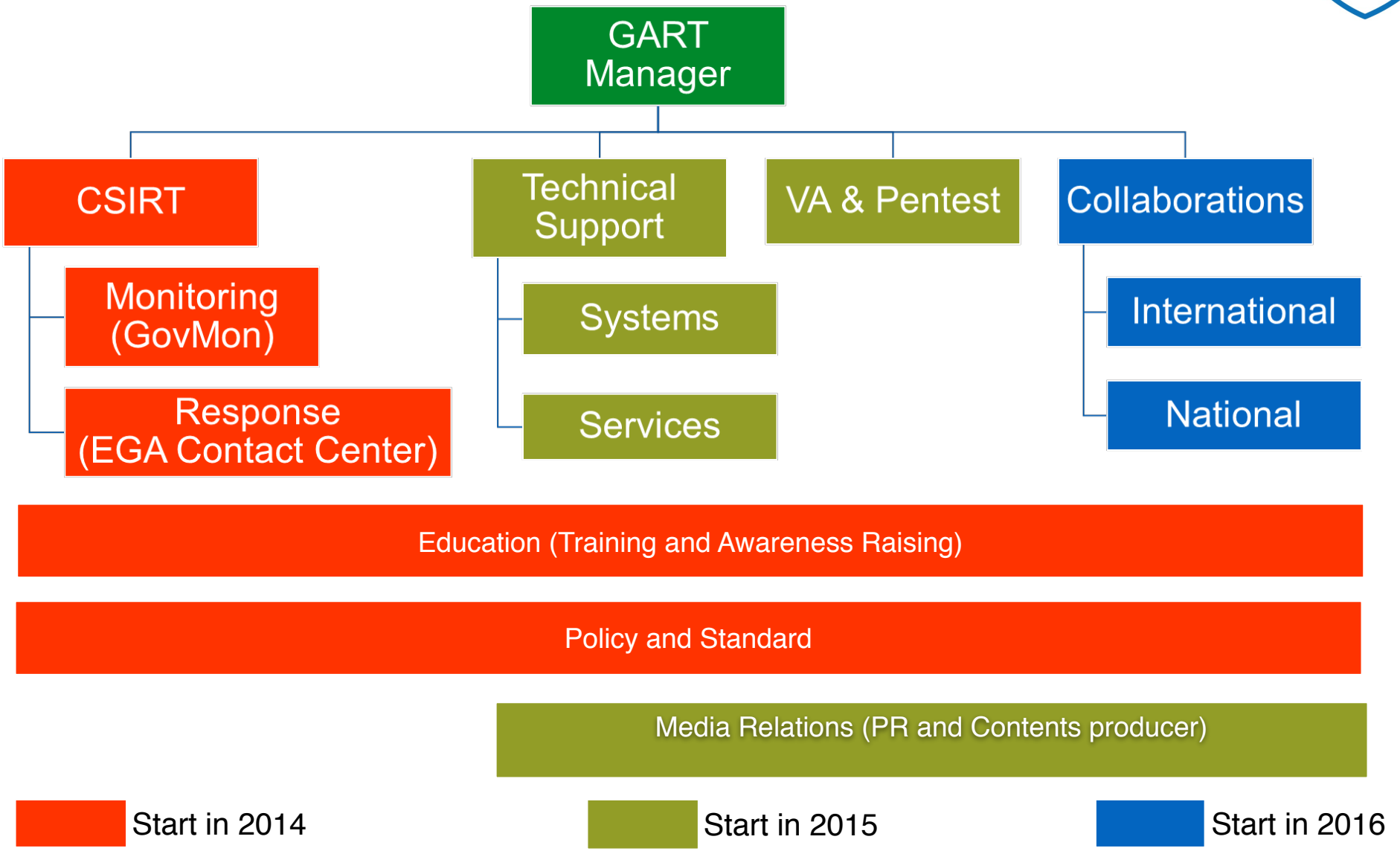
# Technology (IR System)

- Incident Management System
  - RTIR
  - OTRS
- Communication chanels
  - E-mail
  - Phone

# Mitigation/Incident Response

- User education
- User access controls
  - Stop giving users administrative access
- Proxy servers and firewalls
  - Deny access to known bad sites
  - Deny certain kinds of downloads
  - Block posting to known bad IP's

# GART's Roadmap



# References


- https://www.cert.org/incident-management/csirt-development/index.cfm
- https://en.wikipedia.org/wiki/Siem
- https://www.defcon.org/images/defcon-18/dc-18-presentations/Pyorre/DEFCON-18-Pyorre-Building-Security-Operations-Center.pdf
- http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf
- https://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528
- http://baudlabs.com/top-free-and-open-source-log-management-software/

# Conclusion

- SOC doesn't depend on only Technology but also People and Process are really important
- Lacking of experts is one of the biggest problems
- Collaboration is the key factor
- **Looking for new collaborations**


Source : http://www.openpages.com/blog/index.php/2010-grc-wish-list-collaborate

# Thank You

Contact me

kitisak.jirawannakool@ega.or.th

http://www.ega.or.th