SOC Functional Areas

3rd Cyber Defense Community Meetup

Wahyu Nuryanto

Security Analyst

February 14th, 2018

Grha Datacomm

What is a SOC

What is a SOC

Security Operations – Protecting the **confidentiality, integrity, and availability** information systems of an organization through: **proactive design** and configuration, **ongoing monitoring** of system state, **detection** of unintended actions or undesirable state, and **minimizing damage** from unwanted affects

SOC Functional Areas

Command Center

Network Security Monitoring (NSM)

Threat Intelligence

Incident Response

Forensics

Self Assesment

Command Center

- ✓ The Command Center performs command and control of all activity related to SOC
- ✓ Single point of entry for security related requests or incidents
- ✓ Authority to direct response and notify constituents
- ✓ Identification and deconfliction of incidents

NSM

- ✓ NSM is a cornerstone capability of a SOC, NSM itself isn’t a SOC
- ✓ Network security monitoring is watching data in motion
- ✓ This multitude of data is frequently aggregated into a single resource of data called SIEM
- ✓ The main objective is fast and accurate detection of issues

Threat Intelligence

- ✓ An insecure system won’t be compromised without a threat leveraging the vulnerability
- ✓ By studying the threats to our environment, we can better prepare, detect, and respond
- ✓ The main objective is tactical and strategic advantage over adversaries
- ✓ “*Know thy self, know thy enemy. A thousand battles, a thousand victories*” Sun Tzu

Incident Response

- ✓ Incident Response is engaged after a problem detected by NSM or external notification
- ✓ Strives to minimize the damage from the incident
- ✓ Perform thorough analysis to determine extent of the incident
- ✓ Leverages lessons learned from incidents to enhance defensibility of the organization

Forensic

- ✓ In support of Incident Response, specialized capabilities to determine the extent of the incident and proactively prevent spread of adversary with detection based on forensic analysis
- ✓ The main objective is detailed data and event analysis for incident verification and impact assessment
- ✓ The data may include but not limited to: Indicator of Compromise, Application data, Operating System artifacts, Logs, etc.

Self Assessment

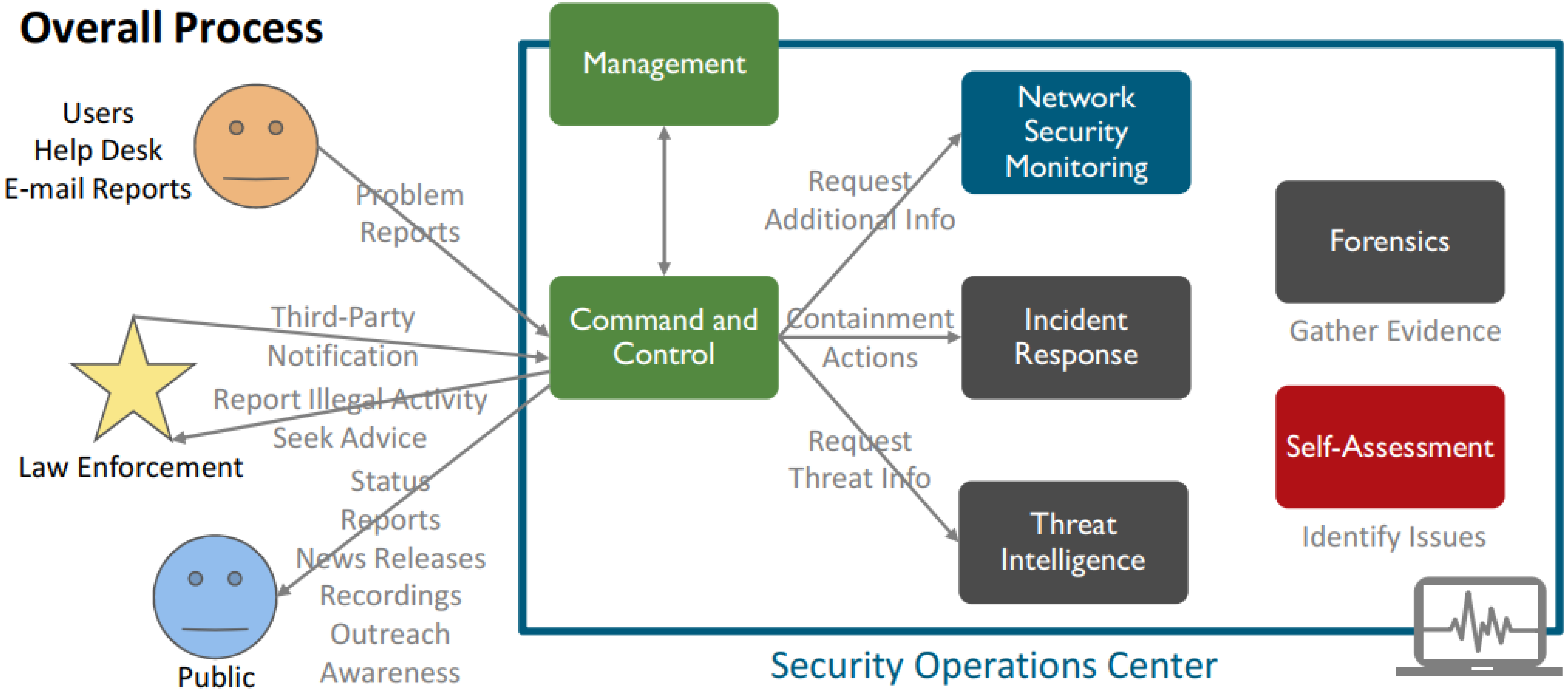
- ✓ The objective of self-assessment is to reflect on the state of the information and information systems the organization owns and is responsible for.
- ✓ Configuration Monitoring
- ✓ Vulnerability Assessment
- ✓ Penetration Testing
- ✓ Exercises

Structure of SOC

- ✓ Pool of People
  - ✓ Everyone on one team, share responsibility, rotate rolls or matrix based on skillset and capability
- ✓ Attacker Phase Mirroring
  - ✓ Organized groups as counter to attacker behaviors (usually based on kill chain)
- ✓ Functional Group
  - ✓ Organized based on functional areas explained before

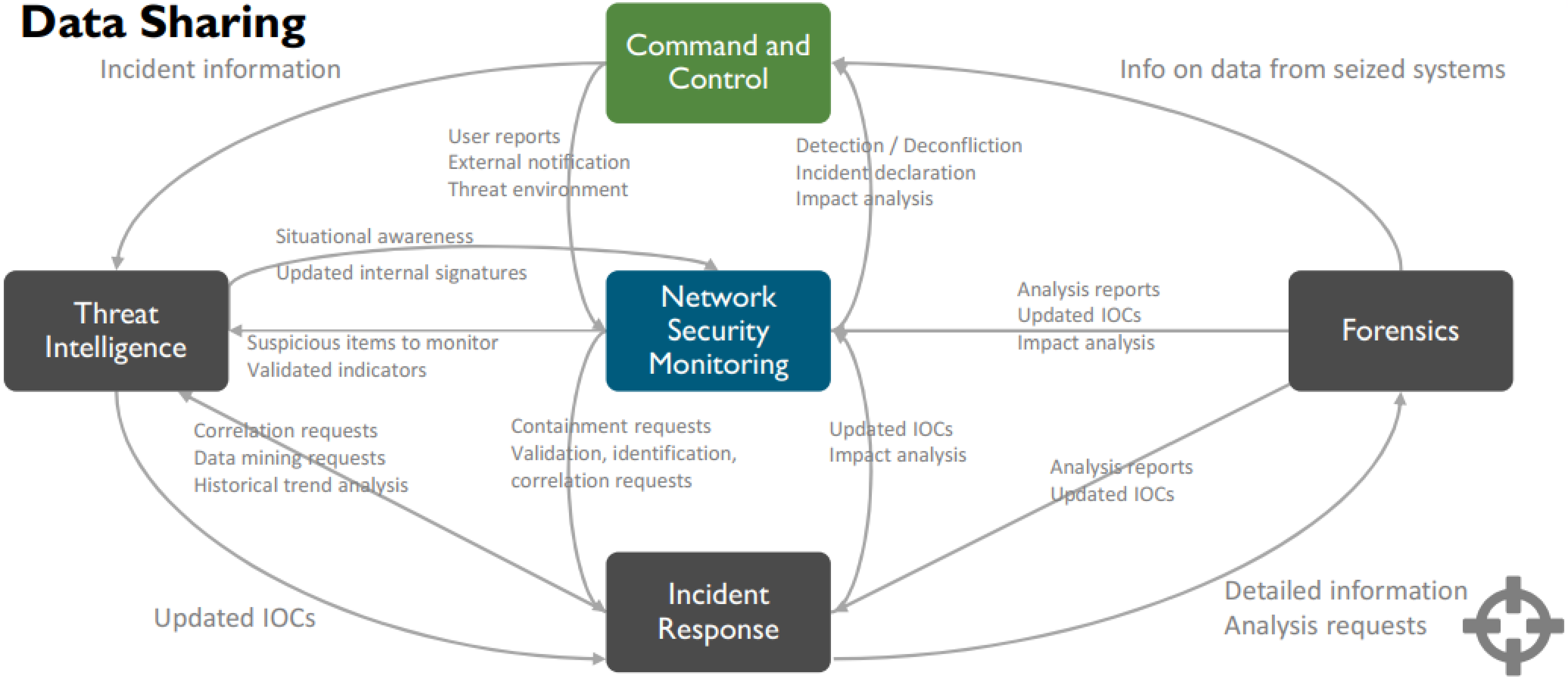
CC Process

Overall Process



NSM Process

Data Sharing



Command and Control

Network Security Monitoring

Threat Intelligence

Forensics

Incident Response

Incident information

Info on data from seized systems

User reports
External notification
Threat environment

Detection / Deconfliction
Incident declaration
Impact analysis

Situational awareness

Updated internal signatures

Suspicious items to monitor
Validated indicators

Analysis reports
Updated IOCs
Impact analysis

Correlation requests
Data mining requests
Historical trend analysis

Containment requests
Validation, identification, correlation requests

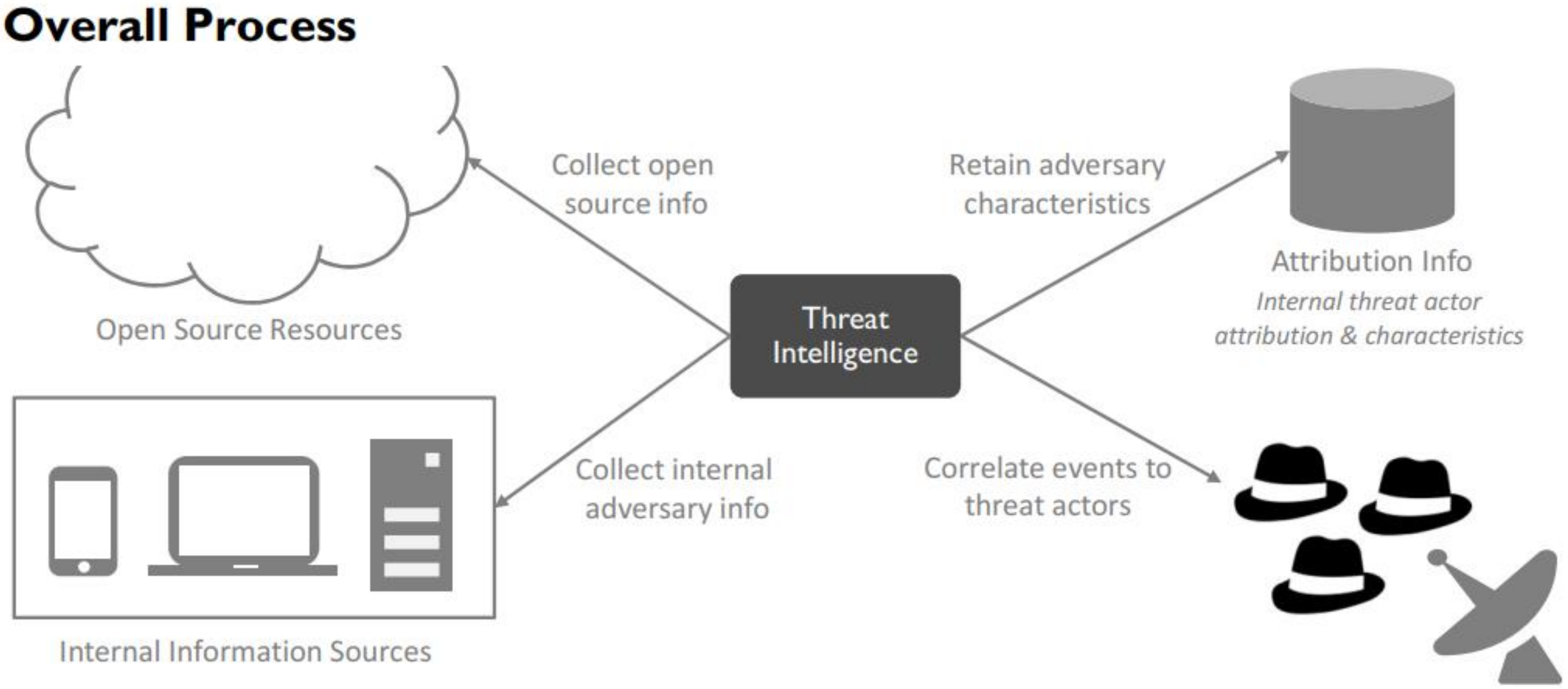
Updated IOCs
Impact analysis

Analysis reports
Updated IOCs

Updated IOCs

Detailed information
Analysis requests

TI Process



Overall Process

Open Source Resources

Collect open source info

Threat Intelligence

Retain adversary characteristics

Attribution Info

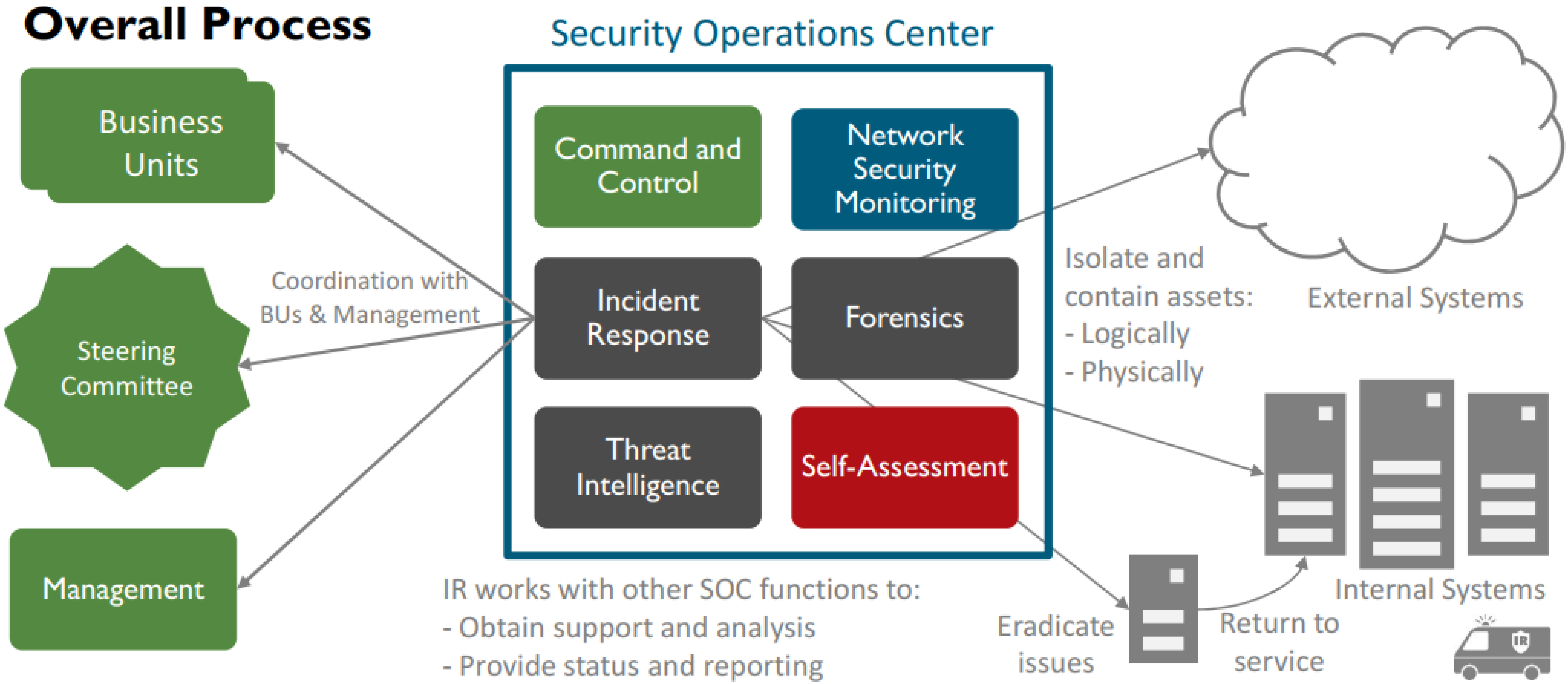
Internal threat actor attribution & characteristics

Collect internal adversary info

Internal Information Sources

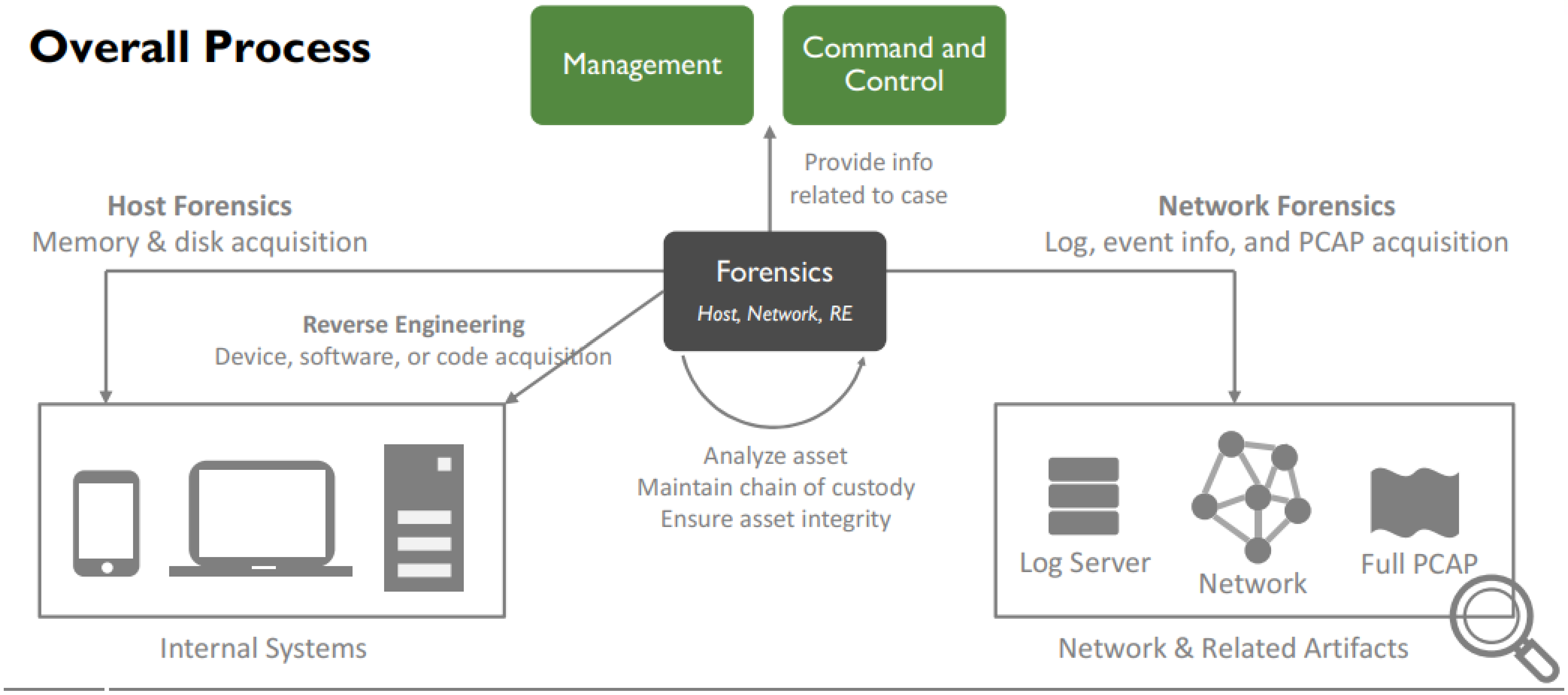
Correlate events to threat actors

IR Process

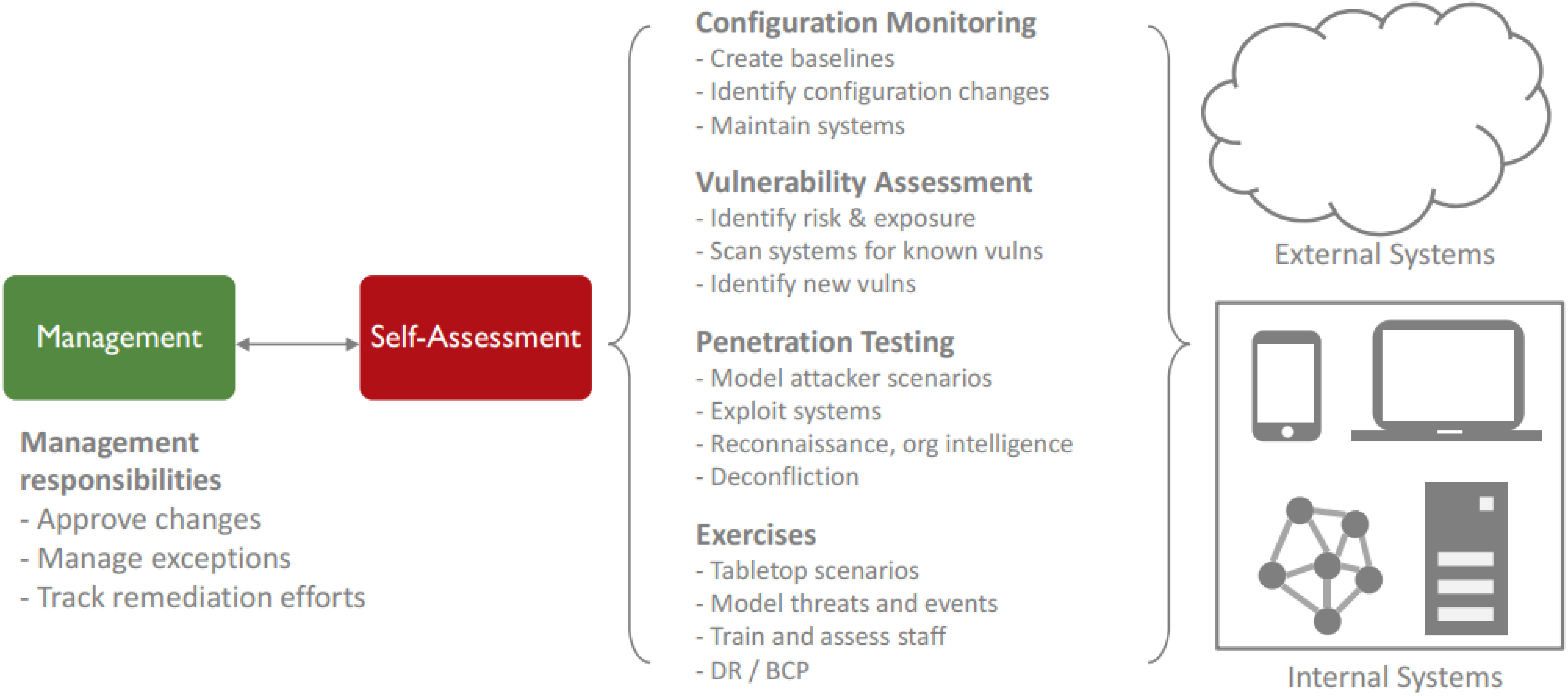

Overall Process
Business Units
Steering Committee
Management
Coordination with BUs & Management
Security Operations Center
Command and Control
Network Security Monitoring
Incident Response
Forensics
Threat Intelligence
Self-Assessment
IR works with other SOC functions to:
- Obtain support and analysis
- Provide status and reporting
Isolate and contain assets:
- Logically
- Physically
External Systems
Internal Systems
Eradicate issues
Return to service
IR

Forensic Process

Overall Process



SA Process



Management

Self-Assessment

Management responsibilities
- Approve changes
- Manage exceptions
- Track remediation efforts

Configuration Monitoring
- Create baselines
- Identify configuration changes
- Maintain systems

Vulnerability Assessment
- Identify risk & exposure
- Scan systems for known vulns
- Identify new vulns

Penetration Testing
- Model attacker scenarios
- Exploit systems
- Reconnaissance, org intelligence
- Deconfliction

Exercises
- Tabletop scenarios
- Model threats and events
- Train and assess staff
- DR / BCP

External Systems

Internal Systems

Questions

Terima Kasih