NETWORK SECURITY

Ch. 12: Incident Response

PTIIK
PROGRAM TEKNOLOGI INFORMASI DAN ILMU KOMPUTER

Question

- Who is responsible for security attack (network, website, etc..) ?

Cyber Security Survey 2011

- According to survey, more attacks are committed by outsiders but attacks by insiders are viewed to be the most costly to organizations
- Result:
  - Insider Attacks Are More Damaging
  - Unknown Supplier Processes and Foreign Entity Threats Drive Concerns
  - Skilled Cyber Professionals and Technological Capabilities Greatest Defense
  - Etc, (http://www.cert.org/archive/pdf/CyberSecuritySurvey2011.pdf)

Mitigating insider attack

- An insider is anyone who has or had authorized access to an organization's network, system, or data.
- Some ways (Common Sense Guide to Mitigating Insider Threats-http://www.sei.cmu.edu/reports/12tr012.pdf) :
  - Consider threats from insiders and business partners in enterprise-wide risk assessments
  - Clearly document and consistently enforce policies and controls.
  - Incorporate insider threat awareness into periodic security training for all employees.
  - Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.

Mitigating insider attack

- Anticipate and manage negative issues in the work environment.
- Know your assets.
- Implement strict password and account management policies and practices
- Enforce separation of duties and least privilege.
- Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities
- Institute stringent access controls and monitoring policies on privileged users
- Close the doors to unauthorized data exfiltration.
- Etc.

4 Sectors

- System administrators
- Developers
- Managers
- Researcher
  - We can declare secure if all sectors working together and called CERT.

System Administrator

- Vulnerability Analysis
- Vulnerability discovery
  - to help engineers understand how vulnerabilities are created and found
- Vulnerability remediation
  - The unfortunate reality is that many software products are being shipped with vulnerabilities that attackers may be able to exploit
  - Remediation process
    - Collection * coordination
    - analysis * diclosure

Vulnerability Notes

17 May 2013	VU#774103	Linux kernel perf_swevent_enabled array out-of-bound access pri...	CVE-2013-2094
15 May 2013	VU#701572	Mutiny Appliance contains multiple directory traversal vulnerabilit...	CVE-2013-0136
14 May 2013	VU#127108	Serva32 2.1.0 TFTPD service buffer overflow vulnerability	CVE-2013-0145
14 May 2013	VU#113732	Adobe ColdFusion 9 & 10 code injection vulnerability	CVE-2013-1389
06 May 2013	VU#237655	Microsoft Internet Explorer 8 CGenericElement object use-after-f...	CVE-2013-1347
30 Apr 2013	VU#912420	IBM Notes runs arbitrary JAVA and Javascript in emails	Multiple CVEs
29 Apr 2013	VU#209131	McAfee ePolicy Orchestrator 4.6.4 and earlier pre-authenticated ...	Multiple CVEs
26 Apr 2013	VU#948155	Henry Schein Dentrix G5 uses hard-coded database credentials ...	CVE-2012-4952
25 Apr 2013	VU#521612	Citrix NetScaler and Access Gateway Enterprise Edition unautho...	CVE-2013-2767
19 Apr 2013	VU#131263	avast! Mobile Security Android application denial-of-service vuln...	CVE-2013-0122

Tools

- Automated Incident Reporting (AirCERT)
  - is a scalable distributed system for sharing security event data among administrative domains
  - The goal of AirCERT is to provide a capability to discern trends and patterns of intruder activity spanning multiple administrative domains

Patching or updating software is usually an effective way to remove vulnerabilities

Developers

- Secure coding
  - Easily avoided software defects are a primary cause of commonly exploited software vulnerabilities.
  - Secure Coding in C and C++, 2nd Edition

Manager

- Resilliance management
- Cert resilience management
- Critical Infrastructure Protection
- Resilience Measurement and Analysis
  - are being implemented
  - are being improved
  - are meeting performance objectives

Researcher

- Researchers are looking toward a next generation approach to security engineering
  - Report
  - Cyber security enginering
  - Declare awareness

blications

13

- Watching Domains That Change DNS Servers Frequently (blog entry)
- Network Analysis with SiLK
  (a FloCon 2013 presentation by Ron Bandes)
- Situational Awareness Metrics from Flow and Other Data Source
  (a FloCon 2013 presentation by Soumyo D. Moitra)
- Introduction to Anomaly Detection
  (a FloCon 2013 presentation by Char Sample and George Jones)
- Behavioral Whitelists of High-Volume Web Traffic to Specific Domains
  (a FloCon 2013 poster by George Jones and Tim Shimeall)
- Network Flow 2012: Year in Review
  (a FloCon 2013 presentation by George Warnagiris)

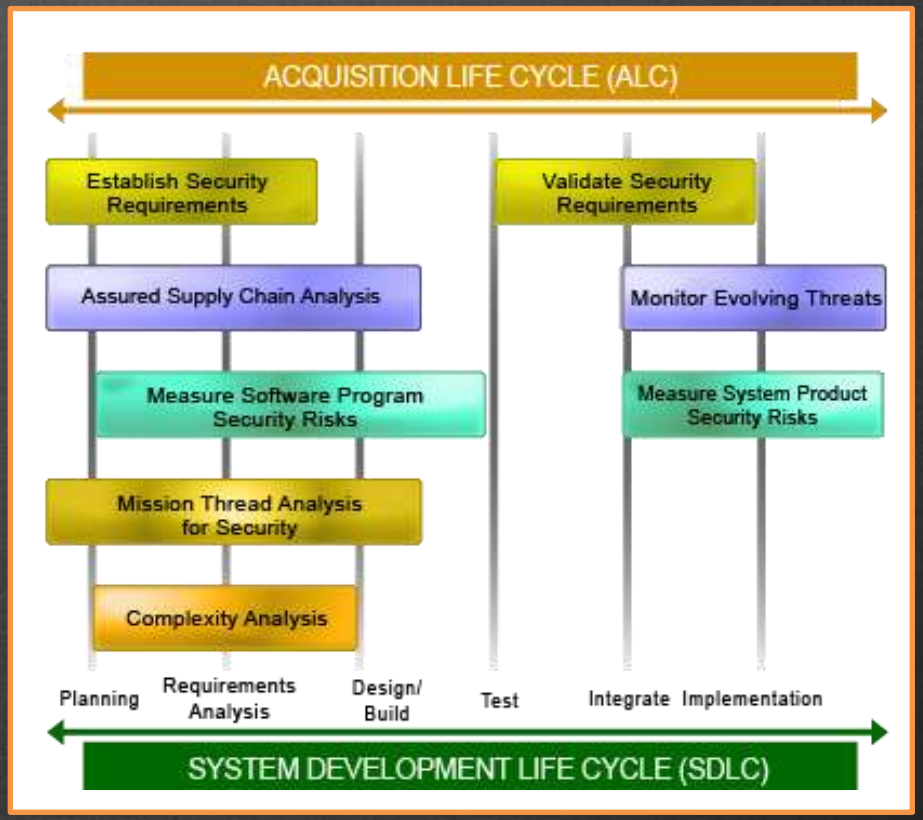
12

- Network Profiling Using Flow
  (an SEI technical report by Austin Whisnant and Sid Faber)

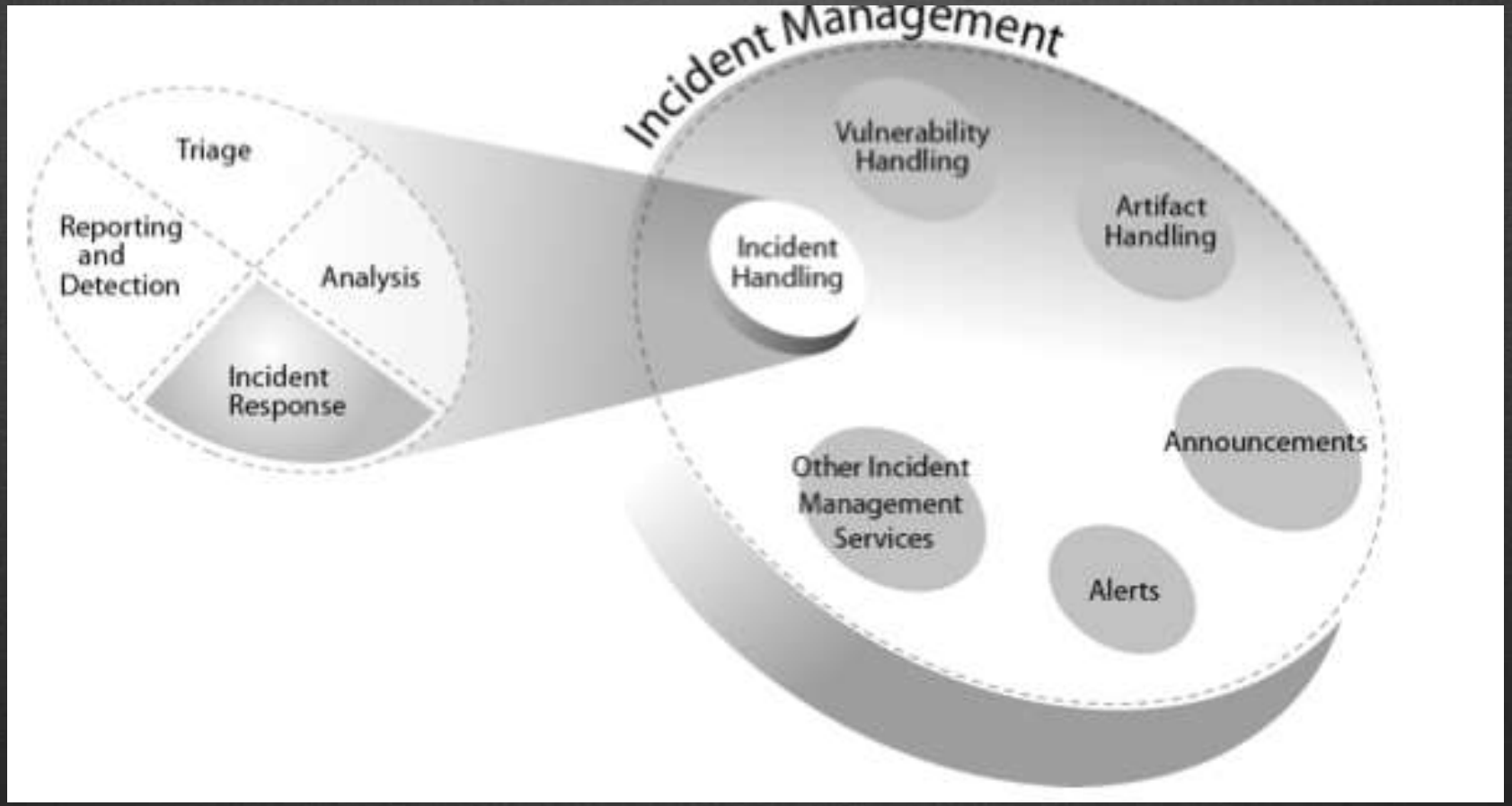
Cyber security engineering

Concern

- The cyber security engineering team addresses security and survivability throughout the development and acquisition life cycles, especially in the early stage



The Relationships



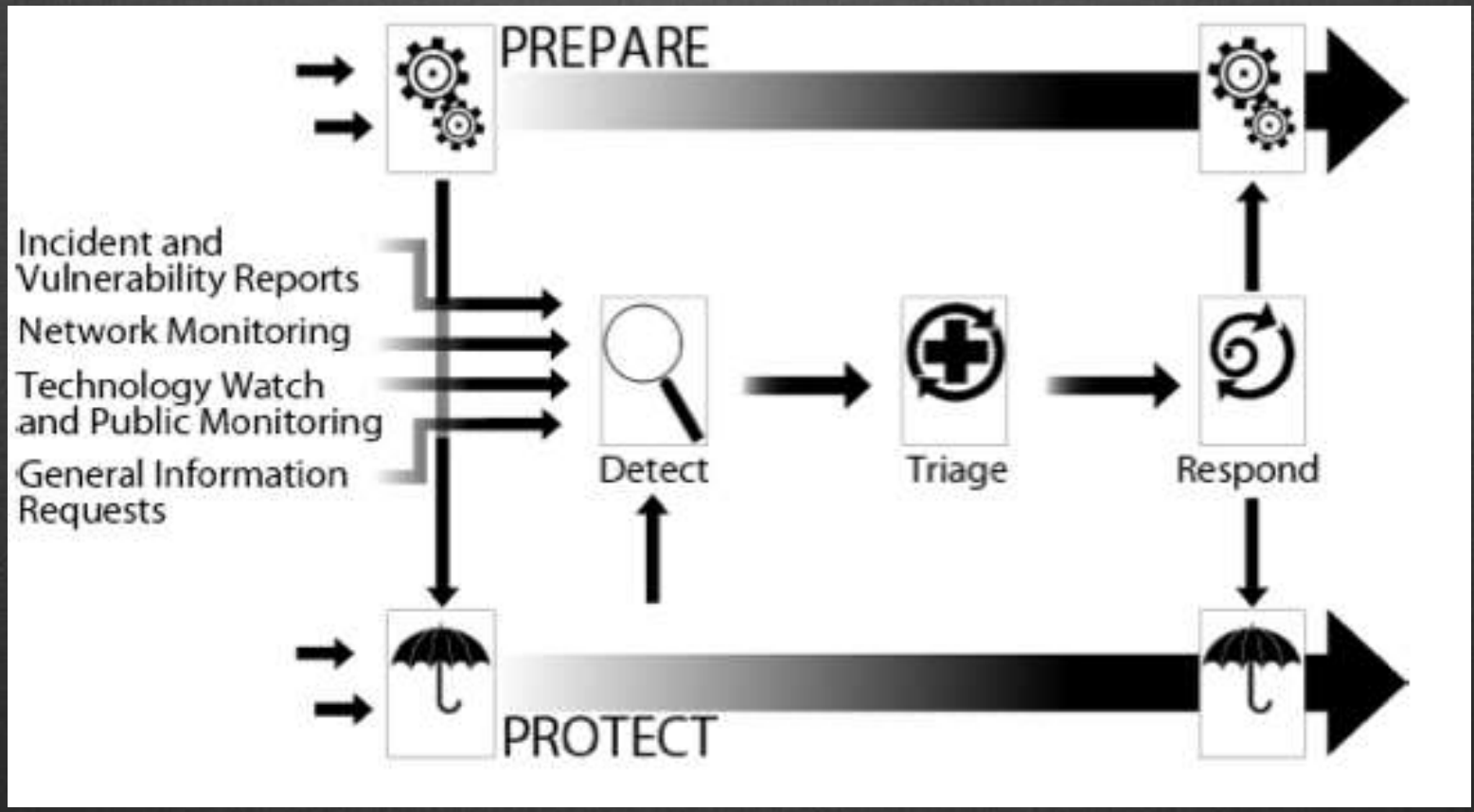
Incident Management Concepts and Processes

- prevent incidents and attacks from happening in the first place by securing and hardening their infrastructure
- training and educating staff and users on security issues and response strategies
- actively monitoring and testing their infrastructure for weaknesses and vulnerabilities
- sharing data where and when appropriate with other teams

Overview of Incident Management Processes

- plan and implement a computer security incident management capability
- secure and harden the enterprise infrastructure to help prevent incidents from occurring or to mitigate an ongoing incident
- detect, triage,15 and respond to incidents and events when they occur

Incident Management Model



Prepare/Sustain/Improve (Prepare),

- plan and implement an initial incident management or CSIRT capability
- sustain that capability
- improve an existing capability through lessons learned and evaluation and assessment activities
- perform a postmortem review of incident management actions when necessary
- pass off infrastructure process improvements from the postmortem to the Protect process

Protect Infrastructure (Protect)

- implement changes to the computing infrastructure to stop or mitigate an ongoing incident or to stop or mitigate the potential exploitation of a vulnerability in the hard- ware or software infrastructure
- implement infrastructure protection improvements resulting from postmortem re- views or other process improvement mechanisms
- evaluate the computing infrastructure by performing such tasks as proactive scanning and network monitoring, and by performing security and risk evaluations
- pass off to the Detect process any information about ongoing incidents, discovered vulnerabilities, or other security-related events that were uncovered during the evaluation

Detect Events (Detect)

- notice events and report those events16
- receive the reports of events
- proactively monitor indicators such as network monitoring, IDS, or technology watch
- functions
- analyze the indicators being monitored (to determine any notable activity that might suggest malicious behavior or identify risk and threats to the enterprise infrastructure)
- forward any suspicious or notable event information to the Triage process
- reassign events to areas outside of the incident management process if applicable
- close any events that are not forwarded to the triage process

Triage Events (Triage)

- categorize and correlate events
- prioritize events
- assign events for handling or response
- pass on relevant data and information to the Respond process
- reassign events to areas outside of the incident management process if applicable
- close any events that are not forwarded to the Respond process or reassigned to other areas

Responds

- analyze the event
- plan a response strategy
- coordinate and provide technical, management, and legal response, which can in-
- volve actions to contain, resolve, or mitigate incidents and actions to repair and re-
- cover affected systems
- communicate with external parties

An Incident Management Body of Knowledge

- Goal:
  - Allow the incident management profession to define itself.
  - Enable incident management to be standardized at all levels, including vocabulary, competencies, and process models.
  - Facilitate the creation of collective, expandable repositories for knowledge about incident management.
  - Provide guidance for developing curricula, training requirements, job competency descriptions, and certification programs for incident management.
  - Enable benchmarking, gap analysis, and process improvement of incident management within organizations.