Events Management
or
How to Survive Security Incidents

Belnet Security Conference
May 2010

Agenda

- Today's Situation
- How to implement a solution
- How to handle security incidents
- Examples & tools
- Q & A

About

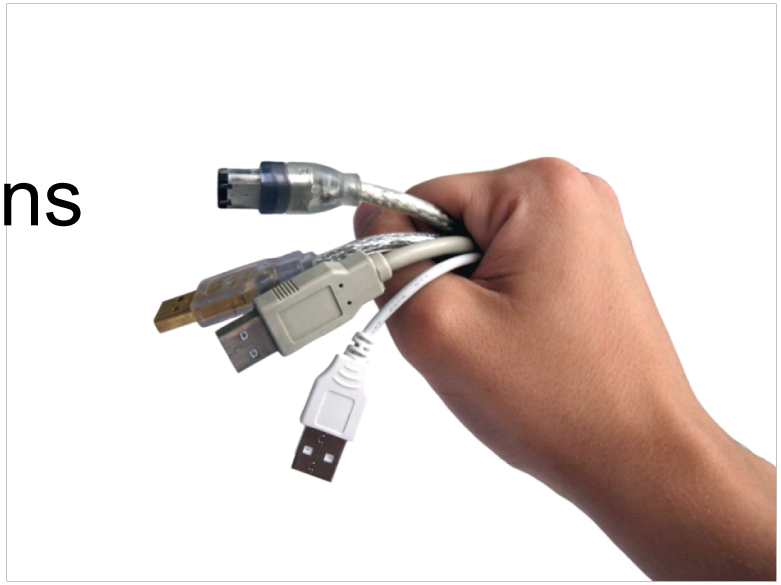
- Xavier Mertens
- Senior Security Consultant @ C-CURE
- CISSP, CISA
- Security Blogger
- BruCON Volunteer
- More info? Maltego!

Introduction

- Some scenarios
  - Present
    - Source: Real-time alerts
    - Action: Immediate investigation
  - Past (during last week or month)
    - Source: Reporting
    - Action: Adapt procedures & infrastructure
  - Investigations (smoke signal)
    - Source: Specific Request
    - Action: Forensics

Today's Issues

- Technical
  - Networks are complex
  - Based on non-heterogeneous components (firewalls, IDS, proxies, etc)
  - Millions of daily events
  - Lot of consoles/tools
  - Protocols & applications



Today's Issues (next)

- Economical
  - ”Time is Money”
    - Investigations must be performed in real-time
    - Downtime may have a huge business impact
  - Reduced staff & budgets
  - Happy Shareholders

Today's Issues (next)

- Legal
  - Compliance requirements
    - PCI-DSS, SOX, HIPAA, etc
    - Initiated by the group or business
  - Local laws
  - Due diligence & due care
    - Security policies must be enforced!

Current Situation

- Organizations are using good security perimeters based on proven solutions
- But without a clear view and control of the infrastructure
- Attacks become more and more sophisticated and frequent
- Not prepared to deal with security incidents

Requirements

To handle security incidents properly organization must rely on:

- Tools
- Procedures
  - Upstream
  - Downstream
  - Continuous (!)
- Event Management != Big Brother

Visibility

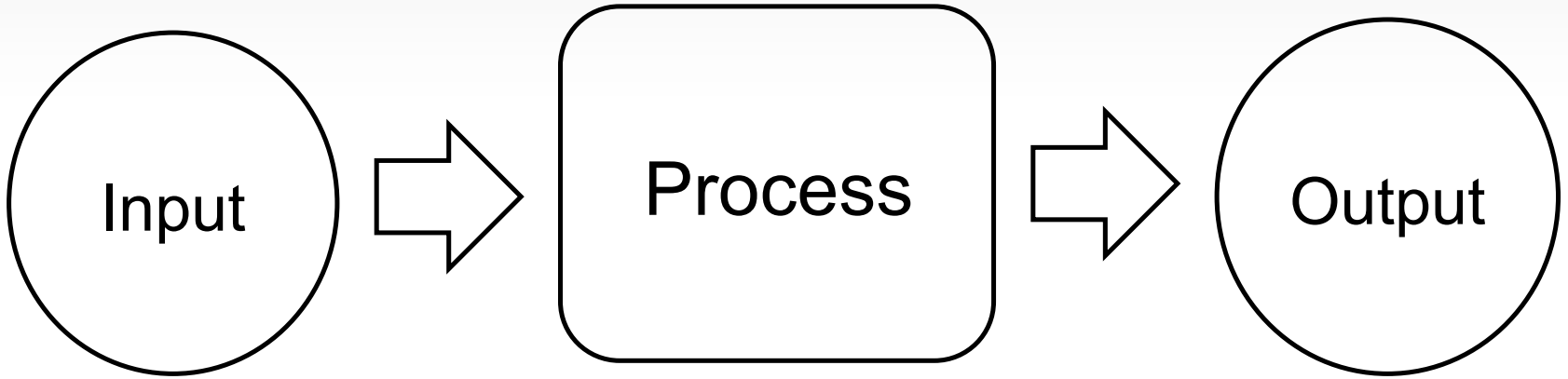
- More integration, more sources, more chances to detect a problem
- Integration of external source of information could help the detection of incidents
  - Automatic vulnerability scans
  - Import of vulnerabilities database
- Awareness

Know your Network

- Inventory
  - Devices
  - Protocols
  - Users
- Behavior
  - Bandwidth Usage
  - EPS (Events per Second)

Procedures

- Boring but required!
- Back to the Basics:



- Input → Change management
- Output → Incident management

Change Management

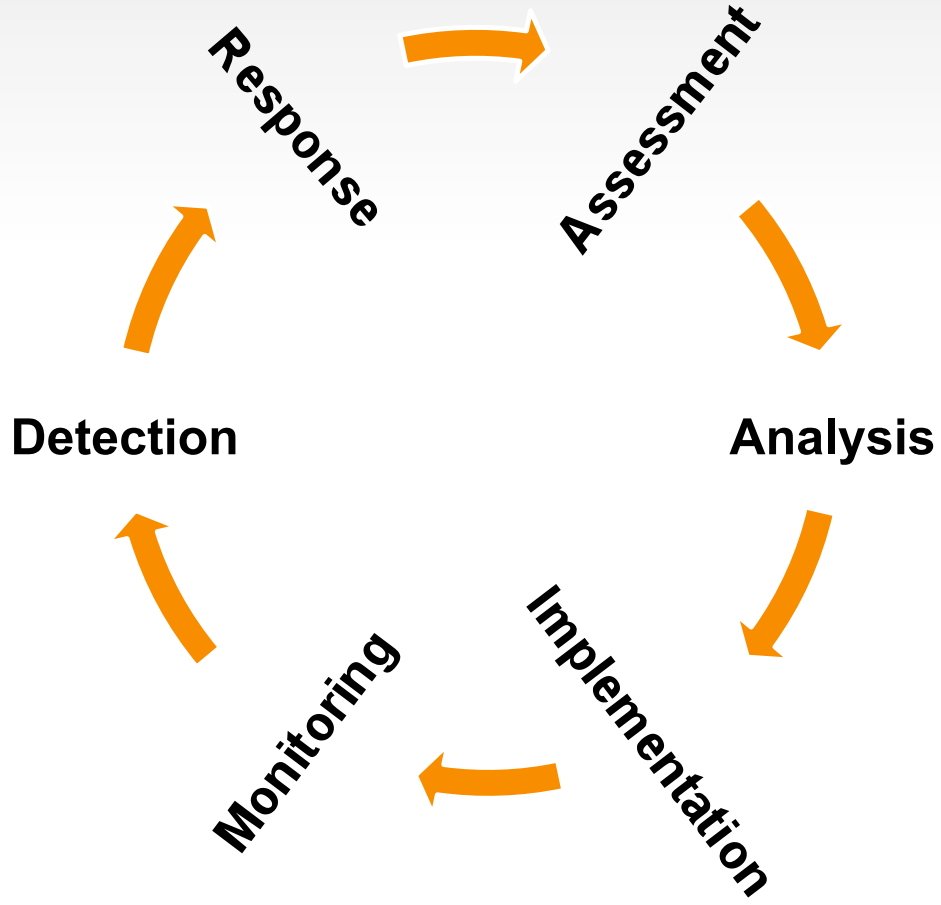
- New devices are connected
- Old devices are decommissioned
- Users provisioning
- New applications are deployed
- Security perimeter? Still valid?

Incident Management

- Business first! (MTTR)
- Avoid decisions made urgently
- Keywords
  - Understand
  - Protect
  - Recover
  - Investigate

Prevention

- Recurrent process!
- Security lifecycle
- Require time
- Informations
  - Forums
  - Blogs
  - Conferences



A Security Incident?

- Definitions
  - An event is "*an observable change to the normal behavior of a system, environment, process, workflow or person (components).*"
  - Incident is "*a series of events that adversely affects the information assets of an organization*"
- Examples? Read the press! ;-)
- You will face one!

Security Convergence

- Physical Security + Logical Security
- Example
  - Geolocalization
  - Users authentication + badge control

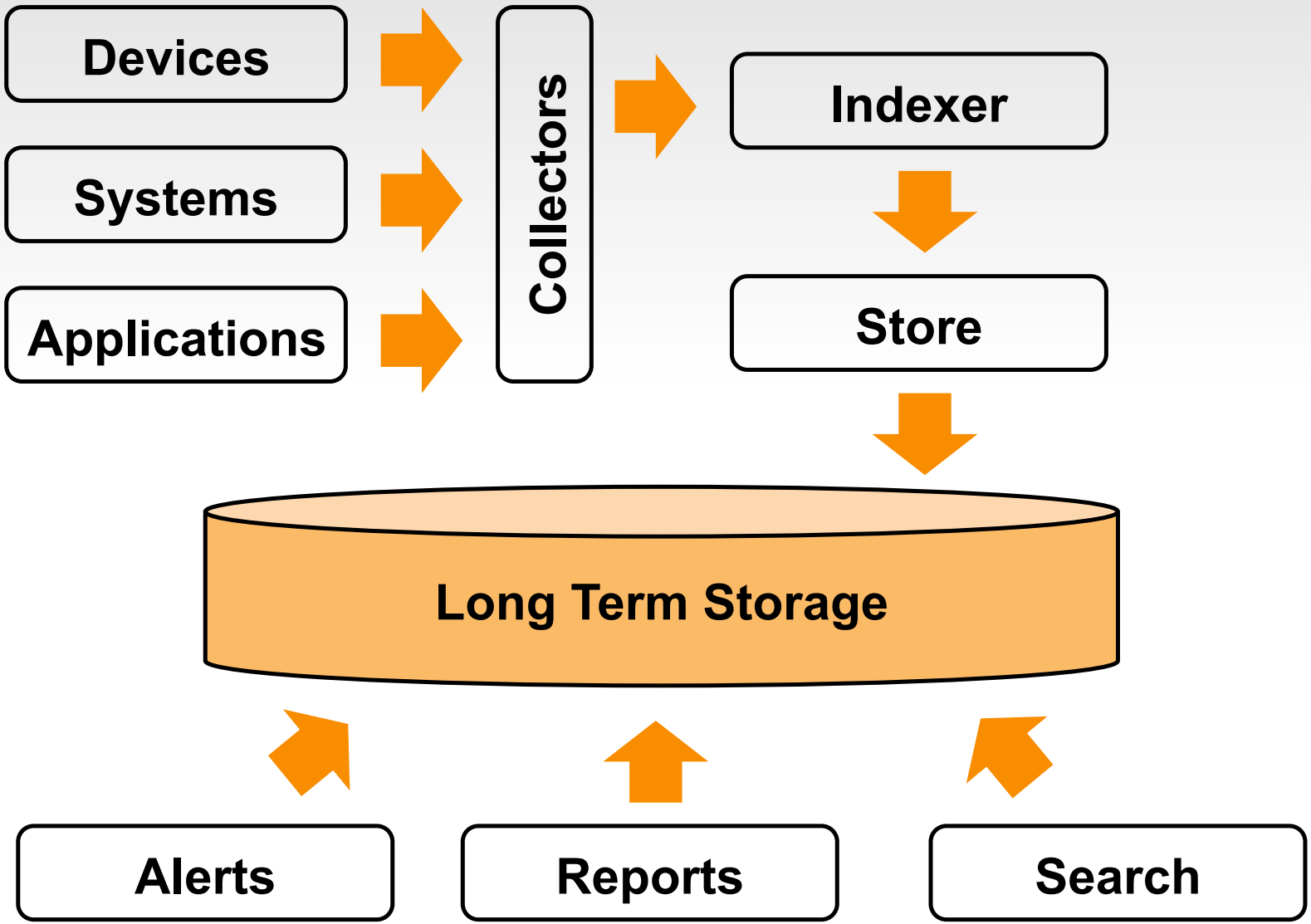
A Four-Steps Process

- Collection
- Normalization
- Index
- Storage

Three Actions

- Real-time alerts
- Reports
- ”Forensics” or ”smoke signals”

Architecture

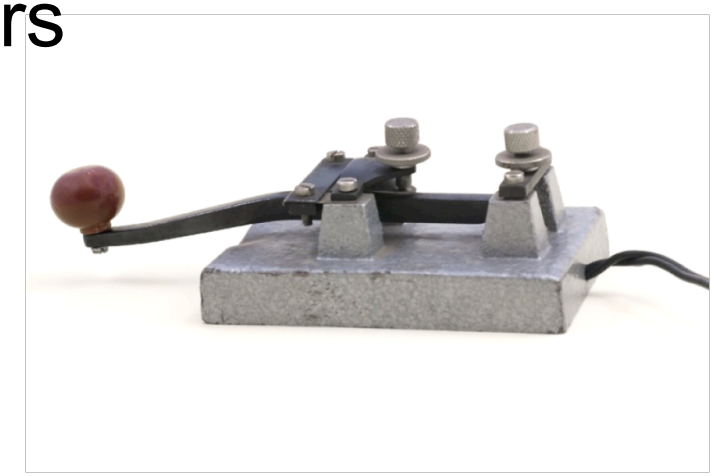


Need of a SOC?

- Yes but ...
- SOC or SPoC
- Directly depending on your organization size
- Starting with a dedicated person is enough
- Investments (time & money)
- Roles: Alerts, Reports, Investigate

Communication

- Mandatory step in the process
- Do not lie!
- Be transparant
- Online reputation
  - Must be properly managed
  - Think about shareholders
  - The press
  - Customers



Examples

- To follow...
  - Apache
  - Google
  - Splunk
- To avoid...
  - The ”Belgian Juweler”

Examples & Tools

- OSSEC
- OSSIM
- Apache mod_dlp
- Ngrep for basic DLP

Thank You!

xavier@rootshell.be

http://blog.rootshell.be

twitter.com/xme