Whack a P0wn

Play or Be Played

James O'Gorman

Matt Churchill

Bill Dixon

CONTINUUM WORLDWIDE℠

Introduction

- Who are we?
- What are we going to cover?
  - Part 1.
  - Part 2.
  - Later this afternoon.

CONTINUUM WORLDWIDE℠

Scenario

- Lets talk about Bob.
  - Works as a sysadmin.
  - No career path with in the company to speak of.
  - Smart guy.
  - Feels like he is smarter then his boss.
  - Feels like he is not getting paid what he is worth.
  - Bored. Work is old, tired, repetitive, and uninteresting.

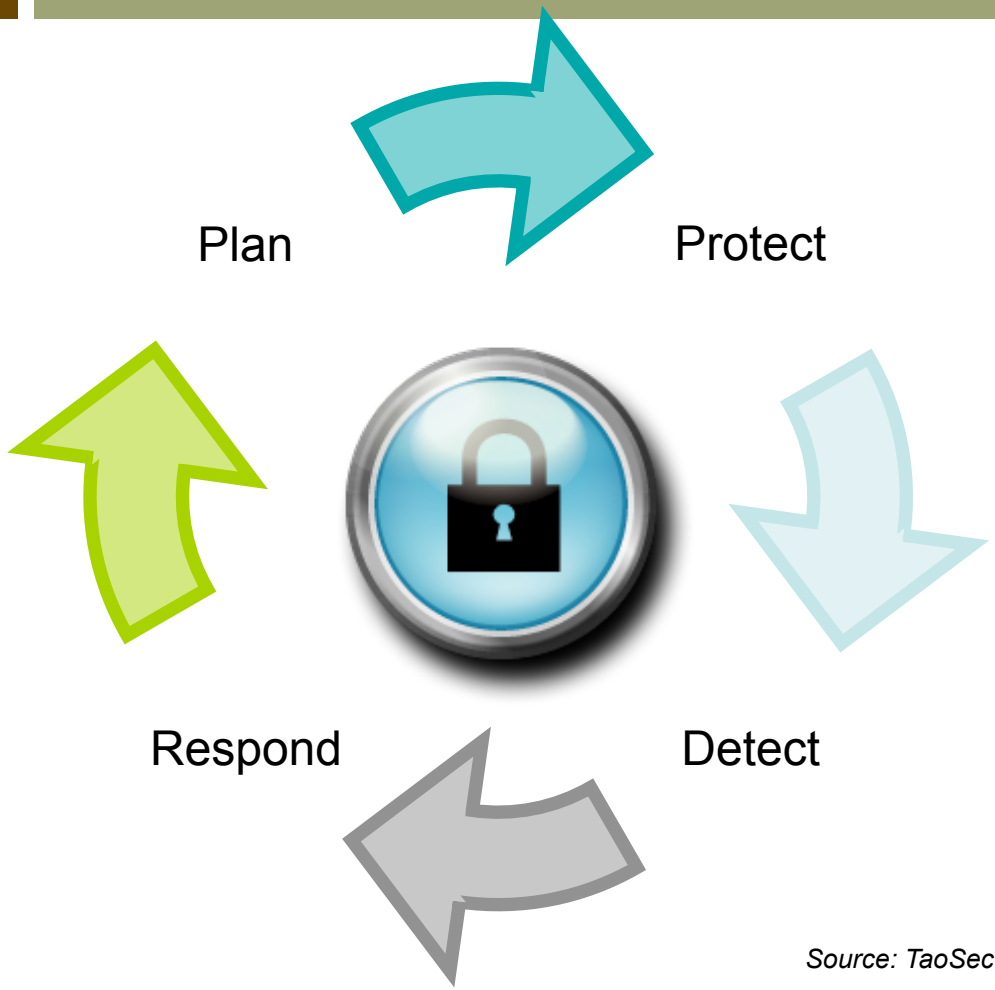
CONTINUUM WORLDWIDE℠

Scenario

- This morning Bob took action and stuck it to the man! He broke into a business partner's systems and stole some data.
- Reports start coming in, something is up!
- Investigation is kicked off....

CONTINUUM WORLDWIDE℠

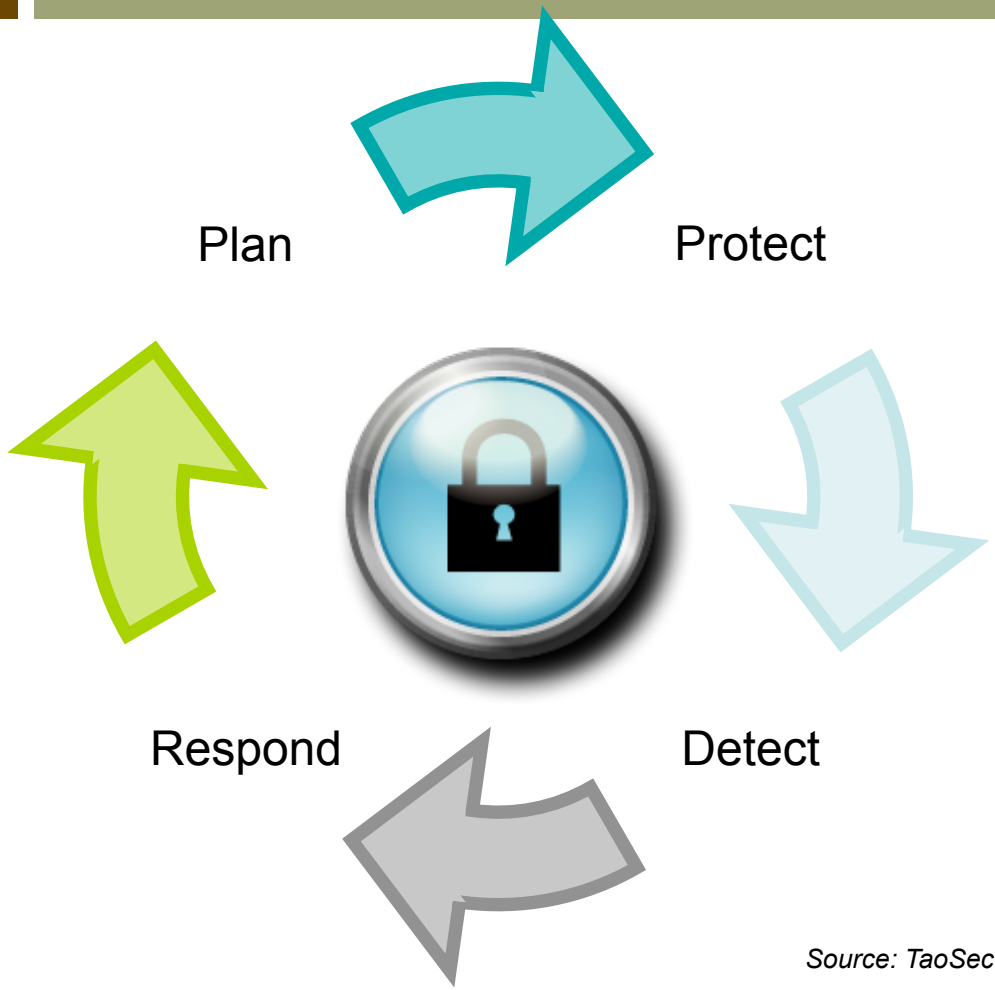
The Process of Security



Source: TaoSecurity

CONTINUUM WORLDWIDE℠

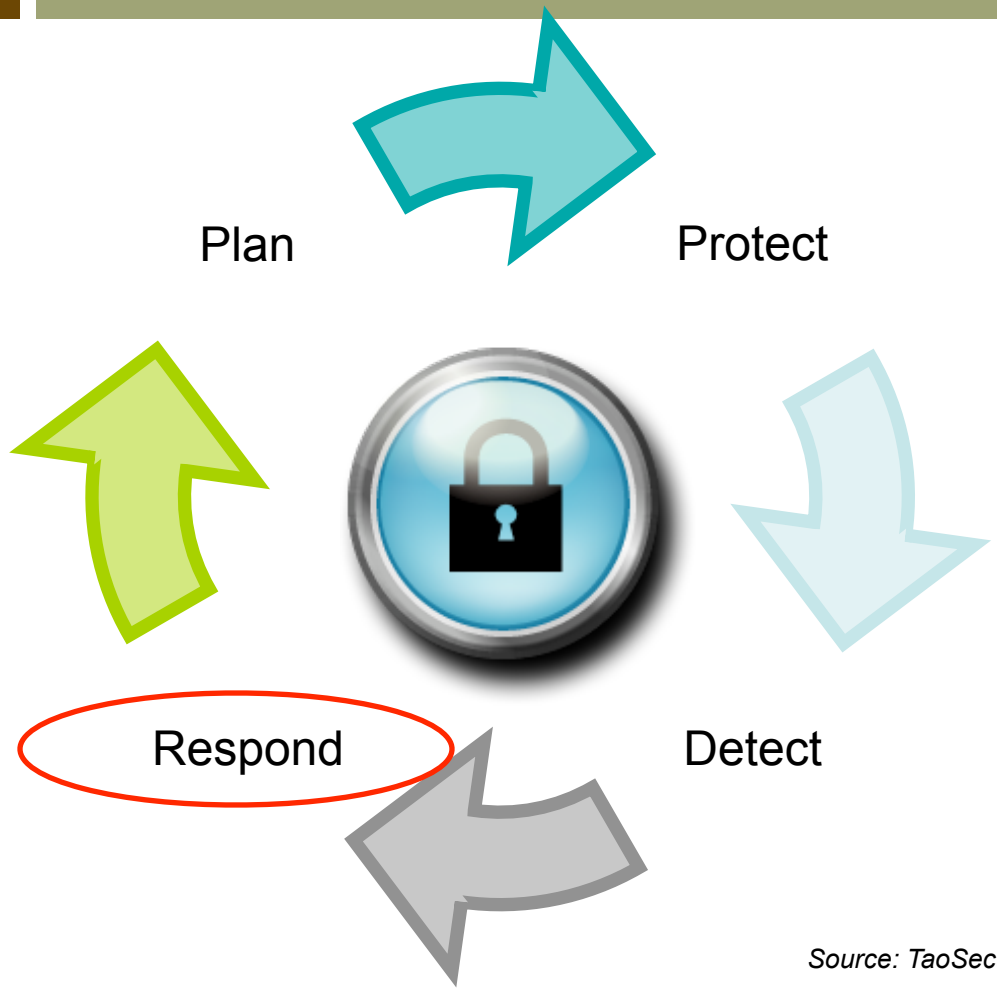
The Process of Security



Source: TaoSecurity

CONTINUUM WORLDWIDE℠

The Process of Security



Source: TaoSecurity

CONTINUUM WORLDWIDE℠

Incident Response Team Structure

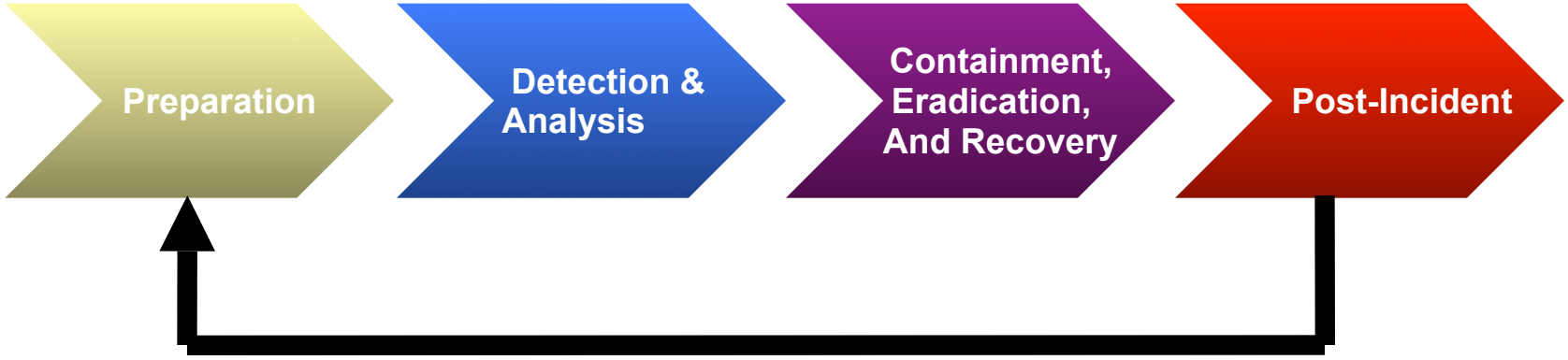
- Centralized
  - Handles all incidents in the organization
- Distributed
  - Multiple response teams
  - Central entry point
- Coordinating
  - Provides overall advice and structure

Incident Response Personnel

- 24/7 Coverage
- Staff Expertise
  - Depth and breadth of knowledge
  - Technical, physical, and administrative
  - Rotation of personnel
- Members from key areas
  - Management
  - Information Security
  - Legal
  - IT
  - HR
  - Public Relations
  - Physical Security

CONTINUUM WORLDWIDE℠

Incident Response Process



Source: http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

CONTINUUM WORLDWIDE℠

Preparation

- More than just having an incident response plan
  - Personnel
  - Policies
  - Technology
- Risk assessment and residual risk
- Defining an incident
- Plan are only as good as the quality in which they are implemented

CONTINUUM WORLDWIDE℠

Detection & Analysis

- On-going monitoring
  - Continuous assessment of:
    - Technical controls
    - Physical controls
    - Administrative controls
- Awareness

Containment, Eradication, and Recovery

- Incident Response Plans
  - Coordination
  - Point of contact
  - Communication channels
- Gathering of information
  - Preparation and Detection determine the value of the information used here

CONTINUUM WORLDWIDE℠

Post-Incident

- Conduct a lessons learned
  - Held within days of the incident
    - Review the incident process and a whole
    - Identify what worked well, what did not, and action items/ follow-ups
    - Actions taken, i.e. termination, breach notification
- Metrics
  - Incident response time
  - Impact of incident (i.e. downtime, reputation loss)

CONTINUUM WORLDWIDE℠

Network Forensics

- When is network analysis network forensics?
- Pros of network forensics over host based forensics.
- Cons of network forensics.

CONTINUUM WORLDWIDE℠

LiveCDs

- Hex - http://www.rawpacket.org/projects/hex/hex-livecd/version-103-release
- Davix - http://www.secviz.org/node/89

CONTINUUM WORLDWIDE℠

Overview

- tcpdstat (http://staff.washington.edu/dittrich/talks/core02/tools/tools.html)
  - Produces a per-protocol breakdown of traffic by bytes and packets, with average and maximum transfer rates, for a given libpcap file (e.g., from tcpdump, ethereal, snort, etc.) Useful for getting a high-level view of traffic patterns.

CONTINUUM WORLDWIDE℠

Overview

- PADS (http://passive.sourceforge.net/)
  - PADS is a signature based detection engine used to passively detect network assets. It is designed to complement IDS technology by providing context to IDS alerts.

CONTINUUM WORLDWIDE℠

Session Information

- Argus (http://qosient.com/argus/)
  - Argus is a fixed-model Real Time Flow Monitor designed to track and report on the status and performance of all network transactions seen in a data network traffic stream. Argus provides a common data format for reporting flow metrics such as connectivity, capacity, demand, loss, delay, and jitter on a per transaction basis. The record format that Argus uses is flexible and extensible, supporting generic flow identifiers and metrics, as well as application/protocol specific information.

CONTINUUM WORLDWIDE℠

Make History Repeat

- tcpreplay (http://tcpreplay.synfin.net/trac/wiki/tcpreplay)
  - Replays pcap files at arbitrary speeds onto the network.

CONTINUUM WORLDWIDE℠

Session Information

- EtherApe (http://etherape.sourceforge.net/)
  - EtherApe is a graphical network monitor for Unix modeled after etherman. Featuring link layer, ip and TCP modes, it displays network activity graphically. Hosts and links change in size with traffic. Color coded protocols display. It supports Ethernet, FDDI, Token Ring, ISDN, PPP and SLIP devices. It can filter traffic to be shown, and can read traffic from a file as well as live from the network.

CONTINUUM WORLDWIDE

Content

- dsniff suite (http://monkey.org/~dugsong/dsniff/)
  - dsniff - Decode passwords
  - mailsnarf - Decode SMTP/POP3
  - msgsnarf - Decode IMs
  - urlsnarf - Decode URLs
  - webspy - Watch web surfing

CONTINUUM WORLDWIDE

Content

- tcpflow (http://www.circlemud.org/~jelson/software/tcpflow/)
  - tcpflow is a program that captures data transmitted as part of TCP connections (flows), and stores the data in a way that is convenient for protocol analysis or debugging. A program like 'tcpdump' shows a summary of packets seen on the wire, but usually doesn't store the data that's actually being transmitted. In contrast, tcpflow reconstructs the actual data streams and stores each flow in a separate file for later analysis.

CONTINUUM WORLDWIDE℠

Content

- Wireshark (http://www.wireshark.org/)
  - Wireshark is the world's foremost network protocol analyzer, and is the standard in many industries. It is the continuation of a project that started in 1998. Hundreds of developers around the world have contributed to it, and it is still under active development.
- tshark - Command line.

CONTINUUM WORLDWIDE℠

Visualization

- Afterglow (http://afterglow.sourceforge.net/)
  - AfterGlow is a collection of scripts which facilitate the process of generating graphs.
    - tcpdump -vttttnnel -r TCPdump.tcp | tcpdump2csv.pl "sip dip dport" | afterglow.pl -c /usr/local/share/afterglow/color.properties | neato -Tgif -o test.gif

CONTINUUM WORLDWIDE℠

Visualization

- Rumint (http://www.rumint.org/)
  - rumint (room-int) is an open source network and security visualization tool

CONTINUUM WORLDWIDE℠

Visualization

- TNV (http://tnv.sourceforge.net/)
  - Depicts network traffic by visualizing packets and links between local and remote hosts.


CONTINUUM
WORLDWIDE℠