

SNaps Security Nagios Advanced Perimetral System

Jorge Higueros

jorge.higueros@consulmatic.com

Who I am

Jorge Higueros

- 10 Years IT Experience
- Master IT security Systems
- Cobit 5 Certified
- Offensive Security Certified
- ITIL V3 Service Operation
- ISO 20000 Implementing
- PCI Auditor

Introduction

Physical security is one of the most overlooked aspects when designing a computer system. While some of the issues discussed below are expected, others, such as the detection of an internal attacker to the company that tries to physically access an operating room the same, no.

This can lead to an attacker that is easier to achieve and make a tape copy of the room, trying to access the same logical way.

The main threats are expected in physical security are:

- Natural disasters, storms accidental fires and floods.
- Threats caused by man.
- Unrest, internal and external deliberate sabotage.

Benefits

- Minimizes risk
- Removes need for multiple or remote command centers
- Integrates and analyzes information from disparate traditional physical security
- Proactively resolves security-related or emergency situations with real-time
- Presents standard operating procedures
- Provides real time compliance auditing and reporting

Agenda

- The Importance of Physical Security
- Components of Physical Security
- Why???????
- Monitoring and Physical Security Perimeter
- SNaps
- Alerts System
- Mobile APP
- Expandable Architecture
- Reports

The Importance of Physical Security

Physical security is a key for companies and institutions in general factor, as having access to the facilities, or compromising the physical integrity of the information system of boxes and vaults.

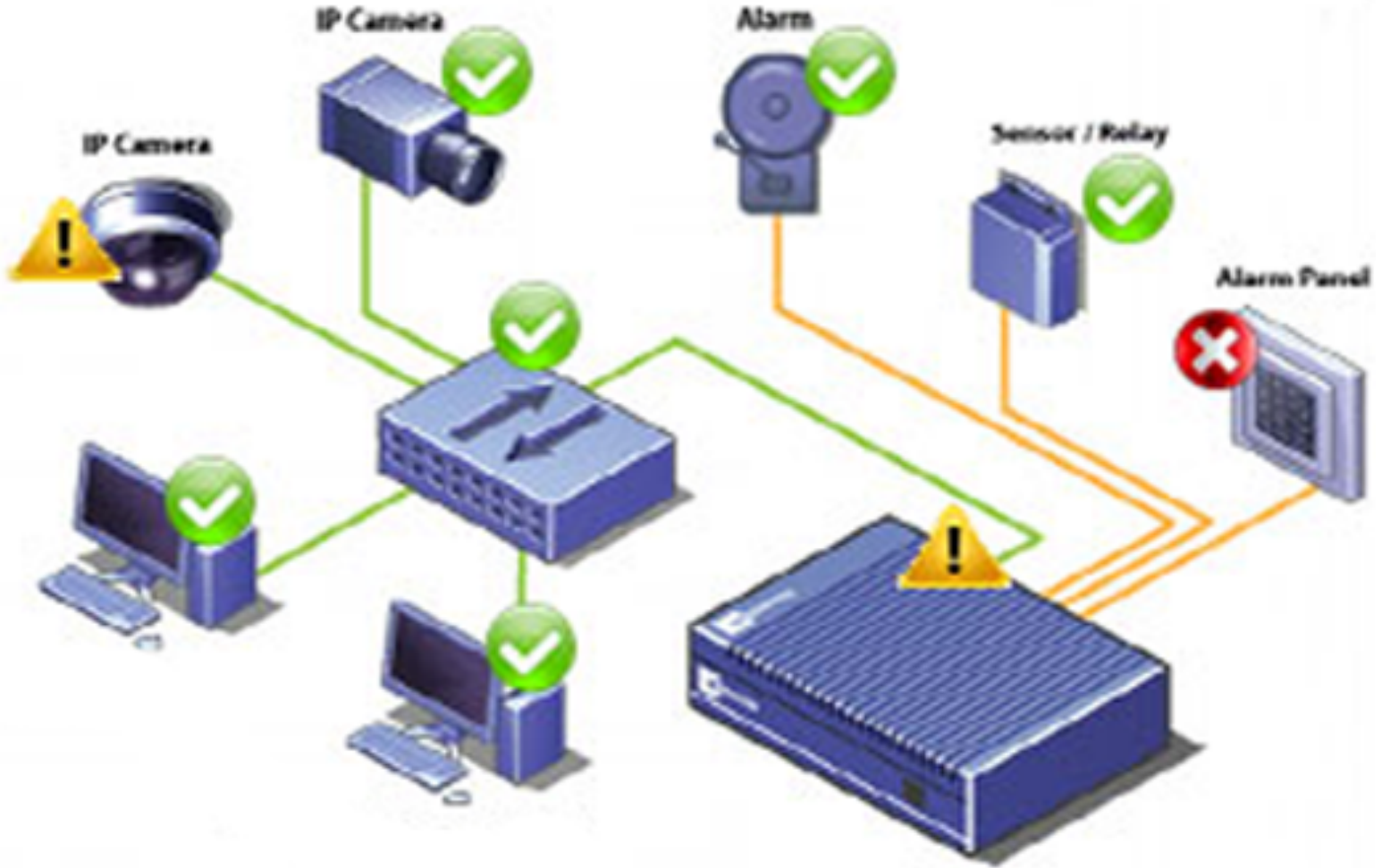


The Importance of Physical Security

Threats to physical security include:

- Interruption of services
- Theft
- Physical damage
- Unauthorized disclosure
- Loss of system integrity

Diagram



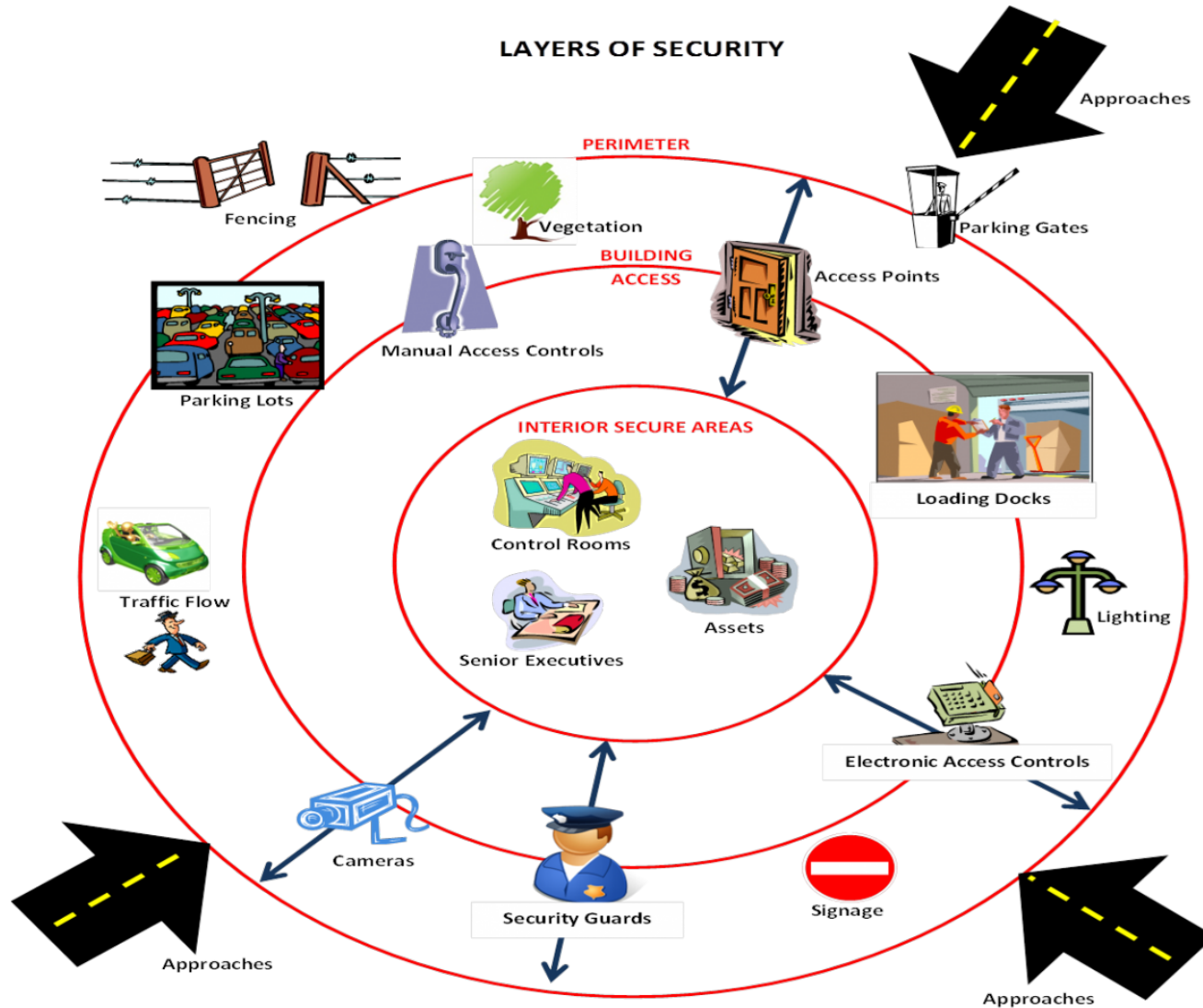
The Importance of Physical Security

Physical security, like general information security, should be based on a layered defense model.

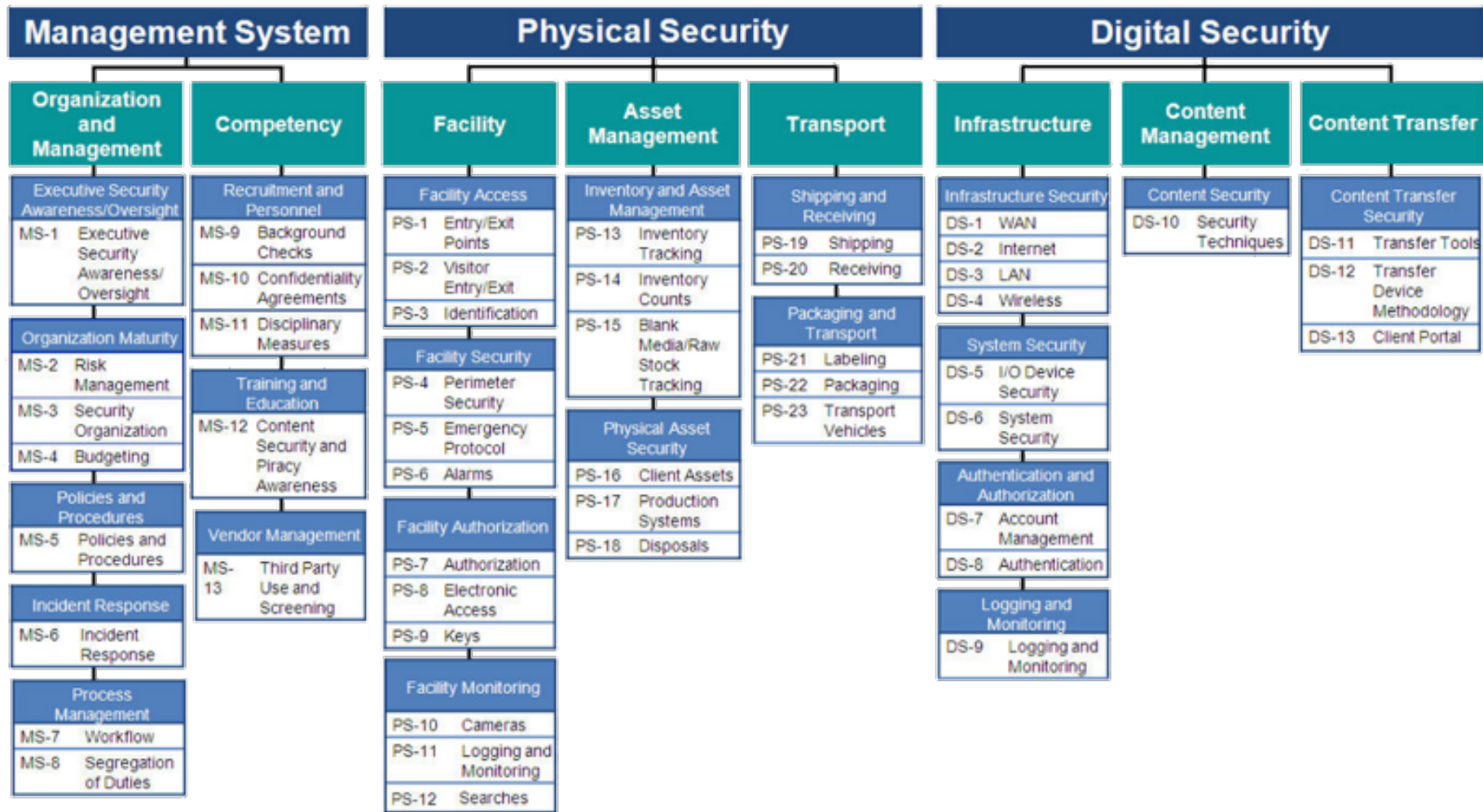
Layers are implemented at the perimeter and moving toward an asset.

Layers include: Deterrence, Delaying, Detection, Assessment, Response

Components of Physical Security



Policy Compliance Physical Security





WHY?

Monitoring and Physical Security Perimeter

The safety monitoring activities help protect a business from threats within the company as well as external threats.



Monitoring and Physical Security Perimeter

External security activities focus on the physical security of facilities or buildings, as well as measures to protect the business from intrusions, either physical or through the computer network.



SNaps

Nagios Perimeter Security Appliance System (SNAPS) is a solution to:

Monitoring:

- Banks
- Companys all types
- Houses
- Malls

SNaps

- It provides a centralized view of all security features lets us know state they are in and if something is malfunctioning, or has activated an alarm or sensor.

SNaps

Unified Security solution SNAPS provides proactive management and monitoring of the main elements of physical security:

SNaps

Alarm System

Security Camera Monitor Status

Cut Energy Sensors:

Sensors integrated environment:

Temperature

Humidity

Smoke

SNaps

Cut Fiber Sensors and Communications
Infrared barriers

Own energy system which can power up all
the components up to 2 hours



Process Monitoring With SNaps



SNaps Dashboard

Nagios XI

Logged in as: nagiosadmin

System Ok: ●●●●●

Logout

Home Views Dashboards Reports Configure Tools Help Admin

Search...

Servicegroup Summary
Servicegroup Overview
Servicegroup Grid
Nagios BPI
Metrics

Performance Graphs

Host Graphs
Graph Explorer

Maps

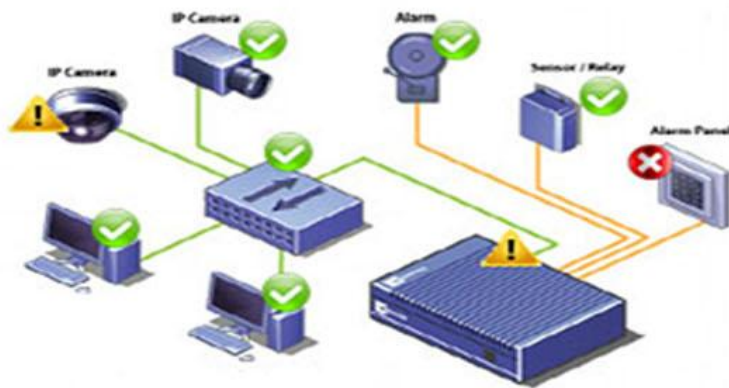
BBmap
Hypermap
Minemap
Nagvis
Network Status Map

Incident Management

Latest Alerts
Acknowledgements
Scheduled Downtime
Mass Acknowledge
Recurring Downtime
Notifications

Monitoring Process

Process Info
Performance
Event Log



Host	Service	Status	Current	Target	Time	Message
NAS	CPU	Ok	57d 7h 32m 13s	1/5	2014-10-15 23:14:03	CPU LOAD OK - Current load is 0.64
	Disk	Ok	57d 7h 36m 3s	1/5	2014-10-15 23:12:26	DISK OK - 1 disks found, no problems
	Info	Ok	57d 7h 31m 22s	1/5	2014-10-15 23:13:46	px4-3000-THYS80 (No Such Object available on this agent at this OID), Uptime: 588686585 (68 days)
	Mem	Ok	17d 22h 56m 55s	1/5	2014-10-15 23:12:22	MEMORY OK - Current memory usage is at 70%
	Ping	Ok	57d 7h 53m 28s	1/5	2014-10-15 23:10:26	OK - 172.168.1.20: rta 0.123ms, lost 0%



Nagios XI 2014R1.5 • [Check for Updates](#)

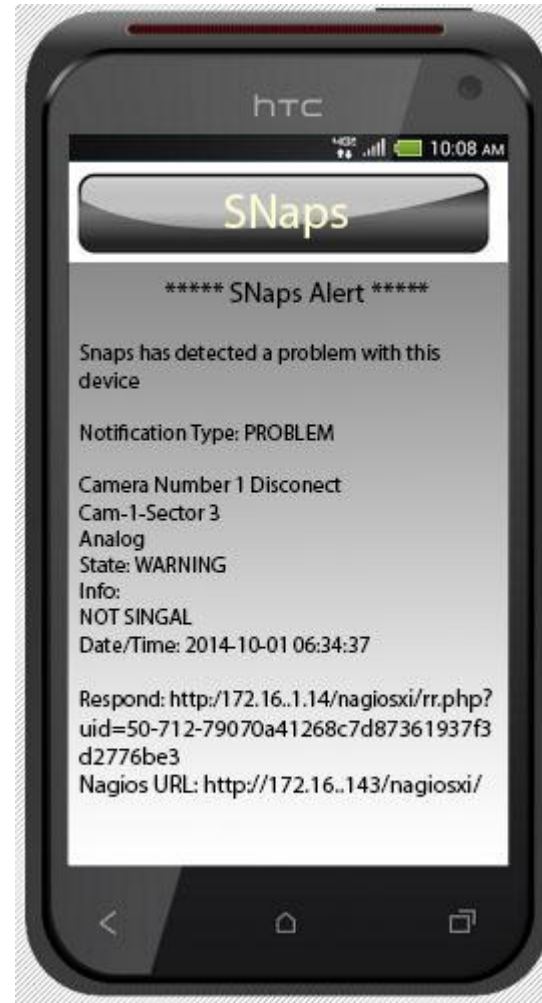
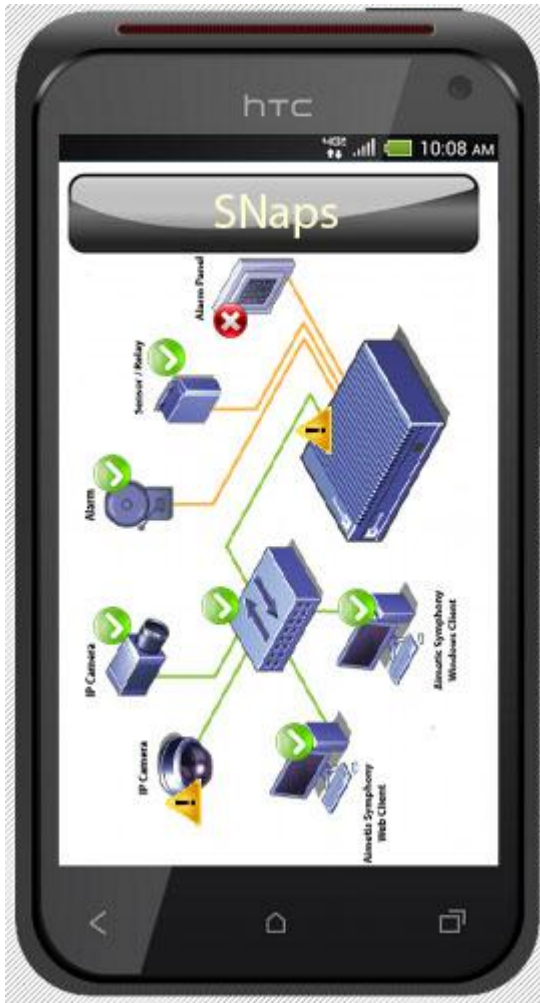
[About](#) | [Legal](#) | Copyright © 2008-2014 Nagios Enterprises, LLC

Alert System

- SNAPS: Reports in real time (email, SMS, jabber Telegram, WatsApp) problems that may arise within the perimeter security components.



Snaps Mobile



Expandable Architecture

Easy integration with internal and third-party applications, as well as replication of number of SNaps Within the SOC reporting infrastructure.

Expandable Architecture



Reports

Reports: Ensures that established SLA levels are achieved, providing historical vision of incidents, notifications, and alert response for later analysis.

No problem.
We get questions
from alien
invaders
all the
time.

