

# **Preventive Digital Forensics:** Creating Preventive Digital Forensics Systems to Proactively Resolve Computer Security Incidents in Organizations

JESUS RAMIREZ PICHARDO

(PMP, GCFA, GCFE, OPST, OPSA, ISO27001 Lead Auditor)

Co-author: JESUS VAZQUEZ GOMEZ, PhD

# Outline

- Objective
- Context
- Problem Statement
- The Preventive Digital Forensics Methodology
- Case Study
- Conclusions

# Objective

- Explain this work that complements the traditional Computer Forensics in the evidence acquisition phase.
- The following are crucial for the correct application of this work:
  - The maturity level of Information Security, Digital Forensics and Incident Response process.
  - The level of knowledge and control that the organization has on their critical IT services.

- What is Computer Forensics?
  - Computer Forensics is the application of scientific and specialized analytical techniques to identify, preserve, analyze and present data that are valid in a legal proceeding.
  - When we speak of an unauthorized access to a system, Computer Forensics aims to determine who was the aggressor, where the attack came from, how it was managed to violate the system and what were his subsequent actions.

- Goals of Computer Forensics
  - While it is very important to find the attacker, another important goal is to strengthen the security of the systems and networks involved applying lessons learned during the investigation.
  - Computer Forensics is *post mortem*, ergo it is reactive.
  - A new complementary approach: We can supplement the traditional Computer Forensics, to be prepared to provide digital evidence related to critical incidents most likely to occur (Preventive Digital Forensics).

# Context

- There is not a single Computer Forensics Methodology, but they all share the following fundamental processes:
  1. Incident Response AND Evidence Acquisition
  2. Research and Analysis
  3. Report results
- This work focuses on the point No. 1.

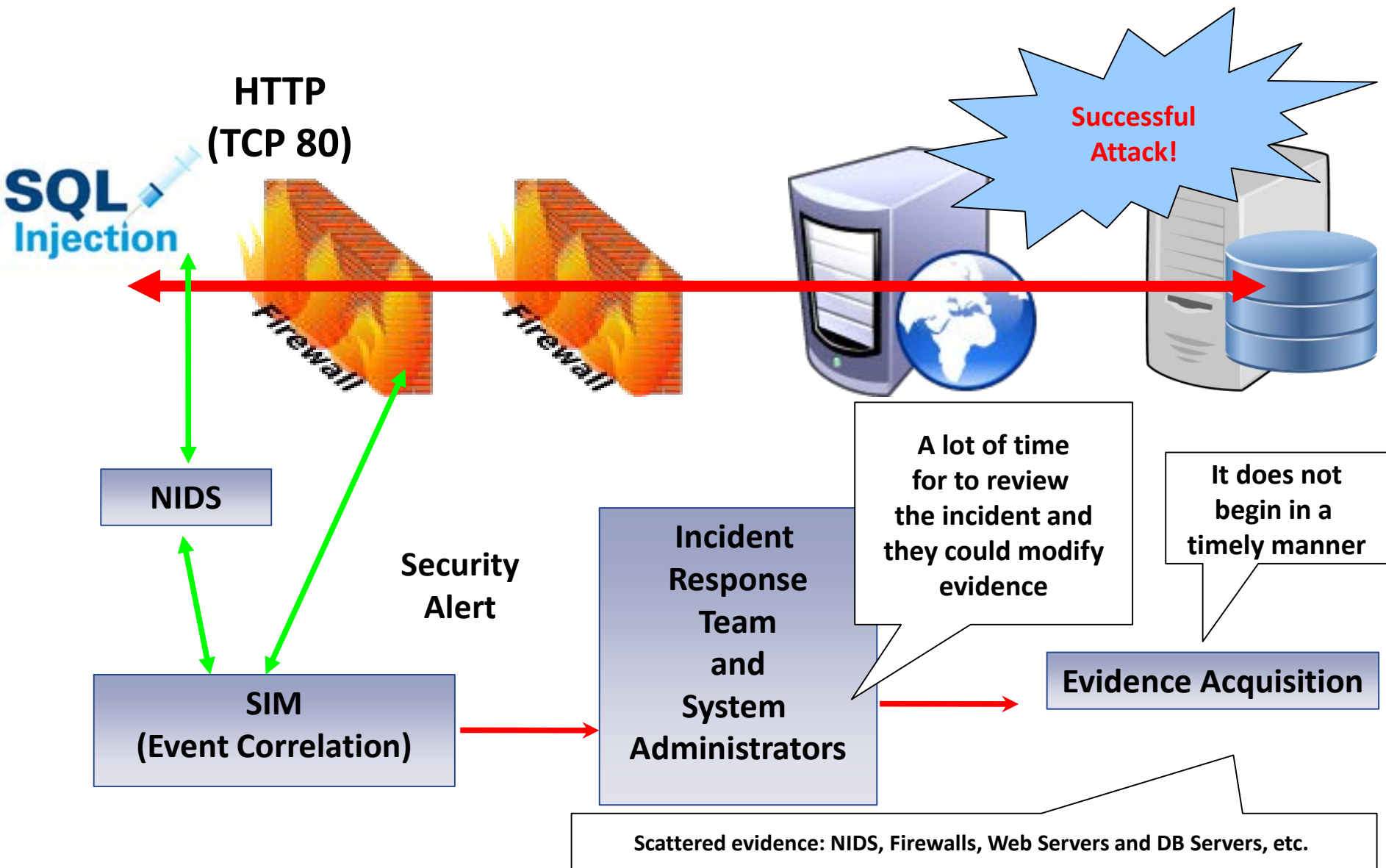
# Problem Statement

- Incident Response is the process of detecting and analyzing incidents and limiting the incident's effect.
- Then, the incident handlers will take actions to ensure that the progress of the incident is halted and that the affected systems and networks return to normal operation as soon as possible.

# Problem Statement

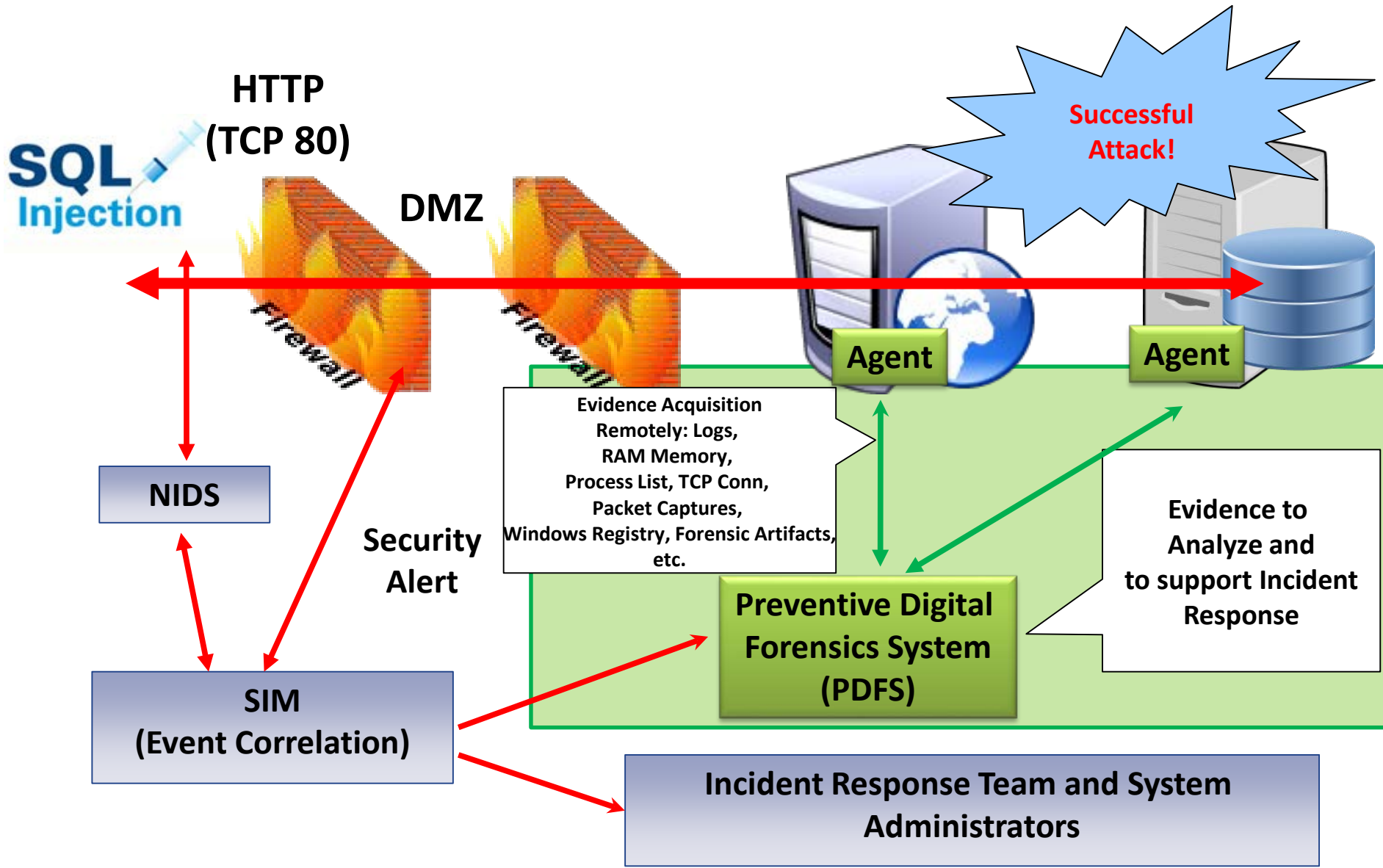
- The actions to solve the incident could modify or destroy the evidence. When it is obtained, it could have been too late.
- On the other hand, it is difficult to obtain required information very quickly (high dispersion of data across affected systems and networks).





# Proposal

- Evidence Acquisition should be done:
  - simultaneously with Incident Response,
  - in all affected systems and networks at the same time and in a timely manner,
  - without any modification of evidence.
- According to the above, I propose a “Preventive Digital Forensics System”: **If it is known which are the critical organizational systems and their information security risks** then, configure these systems in such a manner that they facilitate computer forensics.



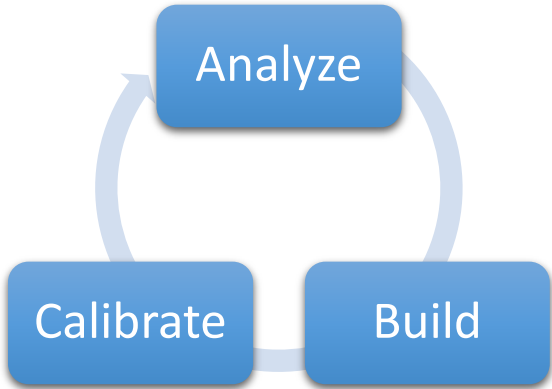
# The Preventive Digital Forensics Methodology

- It is based on experimentation, iterations and learning.
- It allows to design, to develop and to evaluate a set of digital forensic capabilities (PDFS) that will be implemented in organization's critical IT services such that they will facilitate digital forensic tasks, in order to discover and evaluate indicators of malicious behavior,
- and they will allow to give an effective response to computer security incidents in the shortest possible time and cost.

# The Preventive Digital Forensics Methodology

- A PDFS generally is a system whose elements are Agents that are implanted in technological components of the critical IT service.
- The Agents are responsible for collecting and sending the pre-incident evidence to one or more Remote Forensic Repositories which preserve and initialize the chain of custody.
- Additionally, PDFS can be incorporated into best practices related to Incident Response and traditional Computer Forensics.

**Preventive Digital Forensics**



In this context, PDFS generates specific pre-incident evidence that serve as input to traditional Digital Forensics.

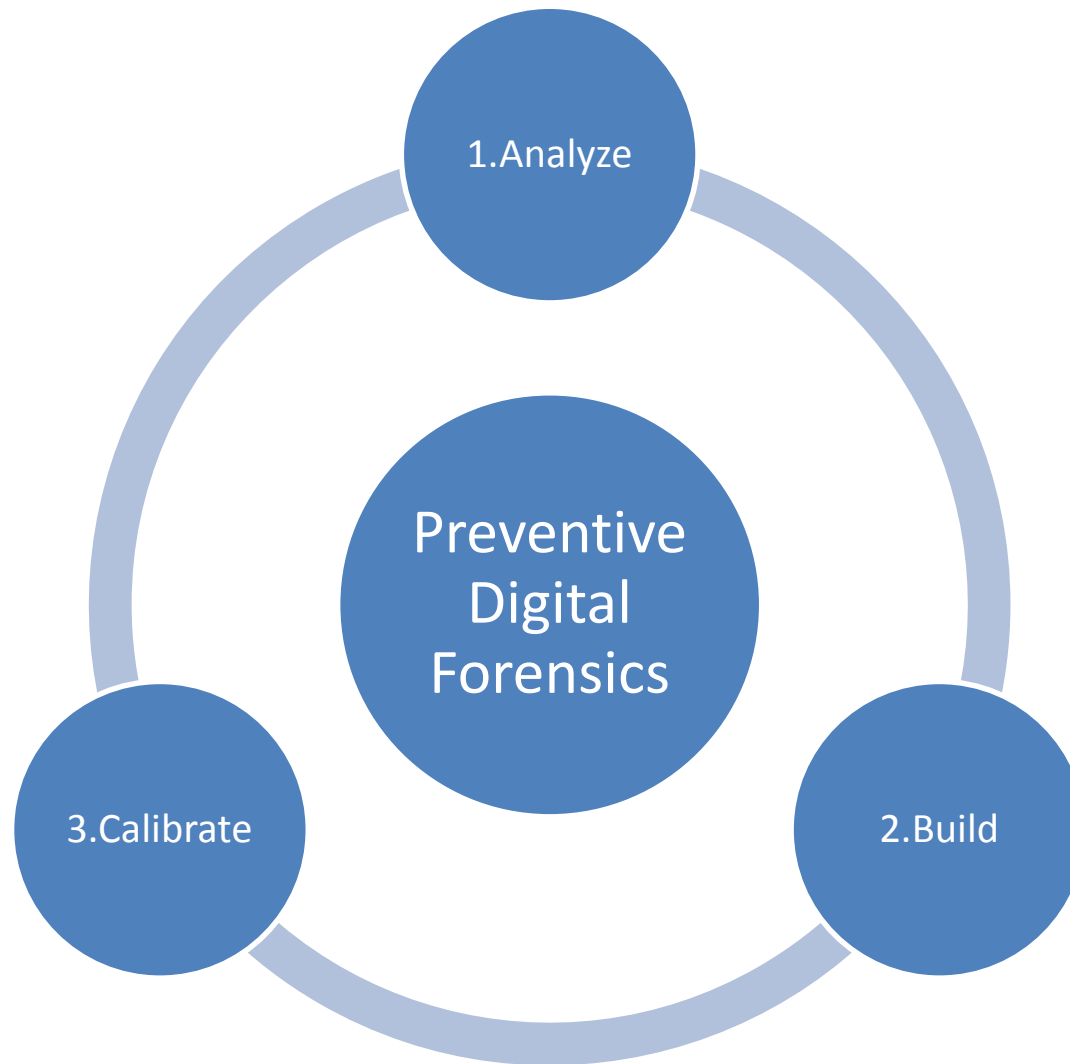


**Traditional Digital Forensics (NIST 800-86)**

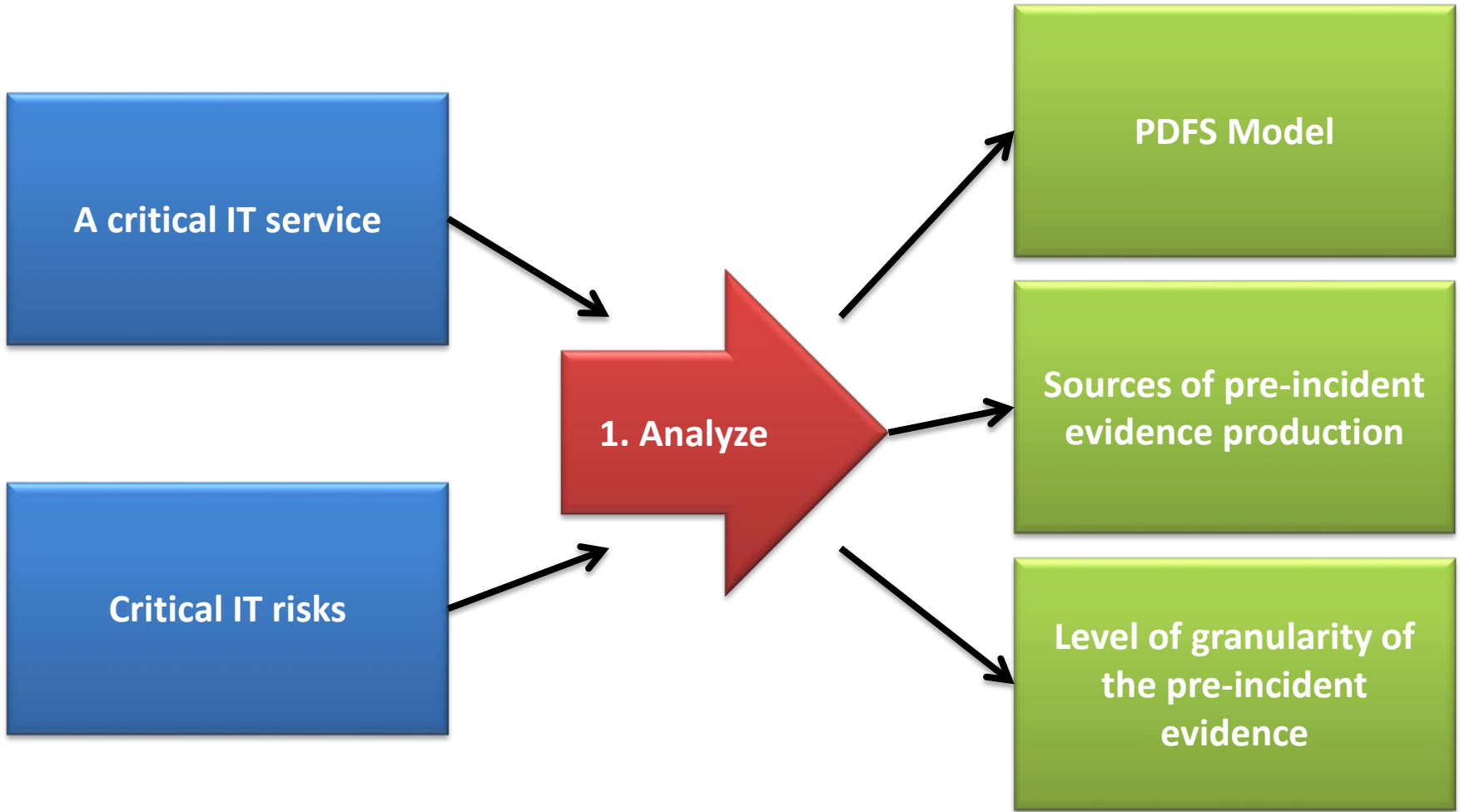


**Incident Response (NIST 800-61)**

# Preventive Digital Forensics Phases

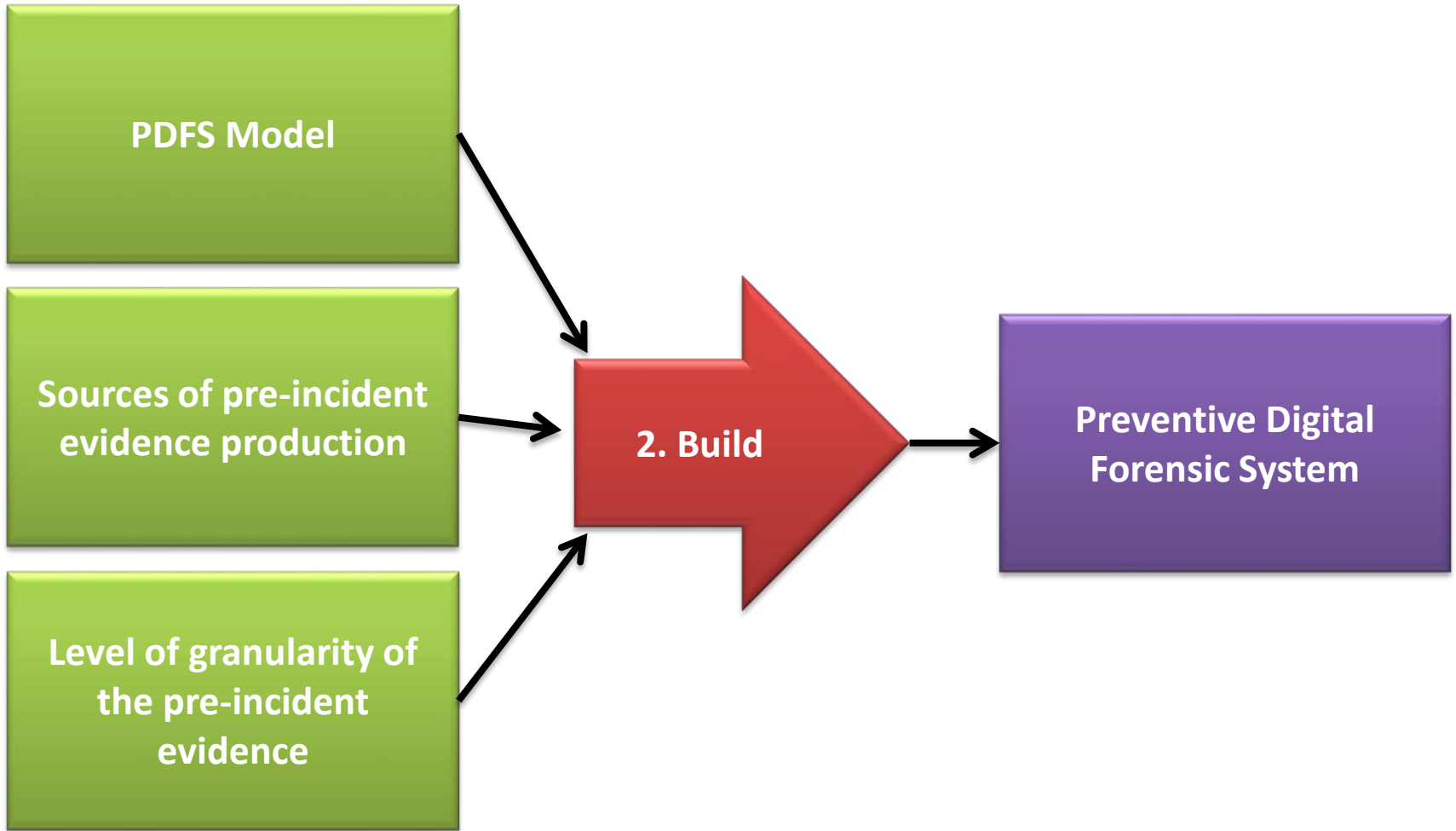


# Preventive Digital Forensics methodology (1/3)

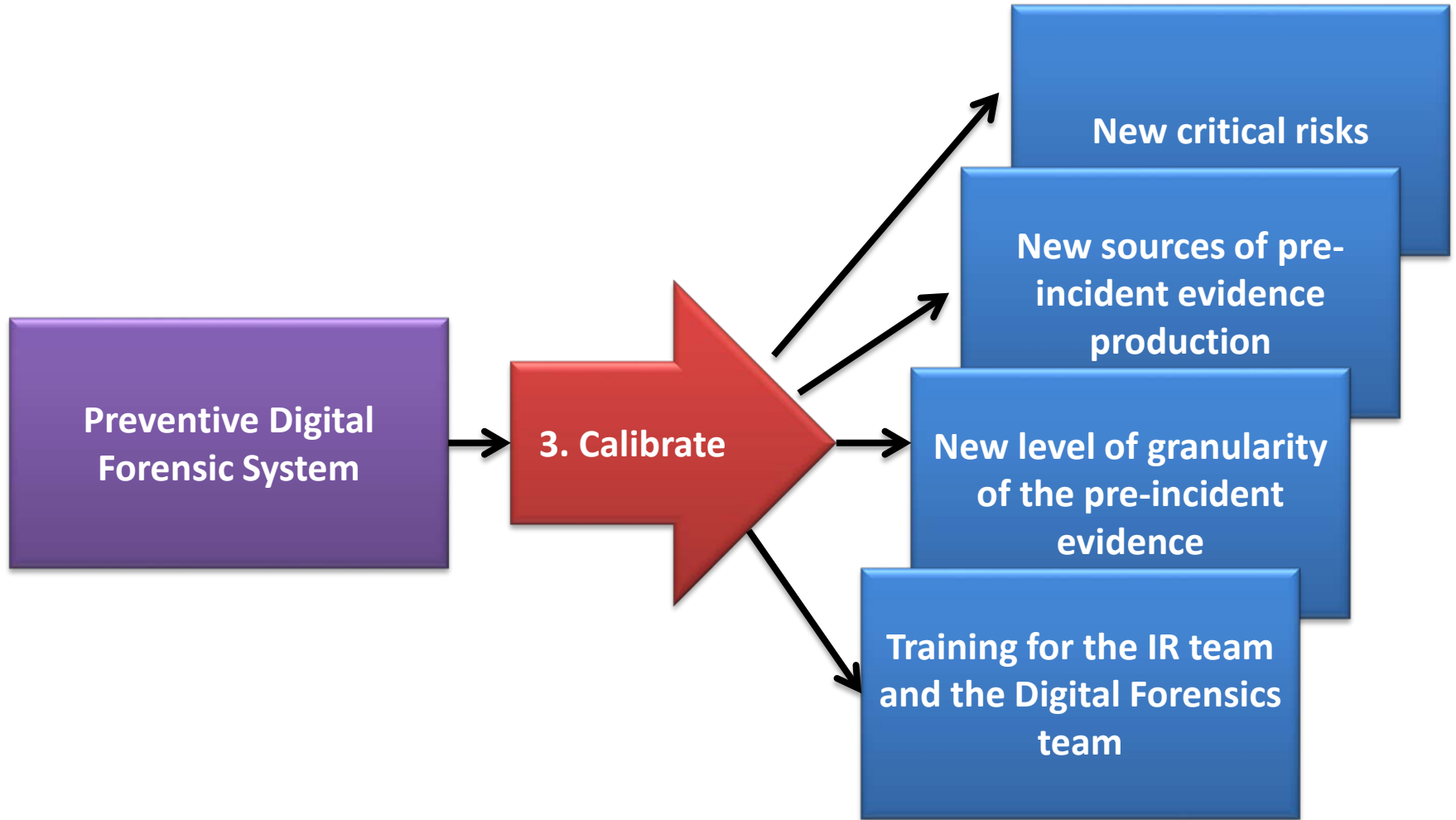




# Preventive Digital Forensics methodology (2/3)



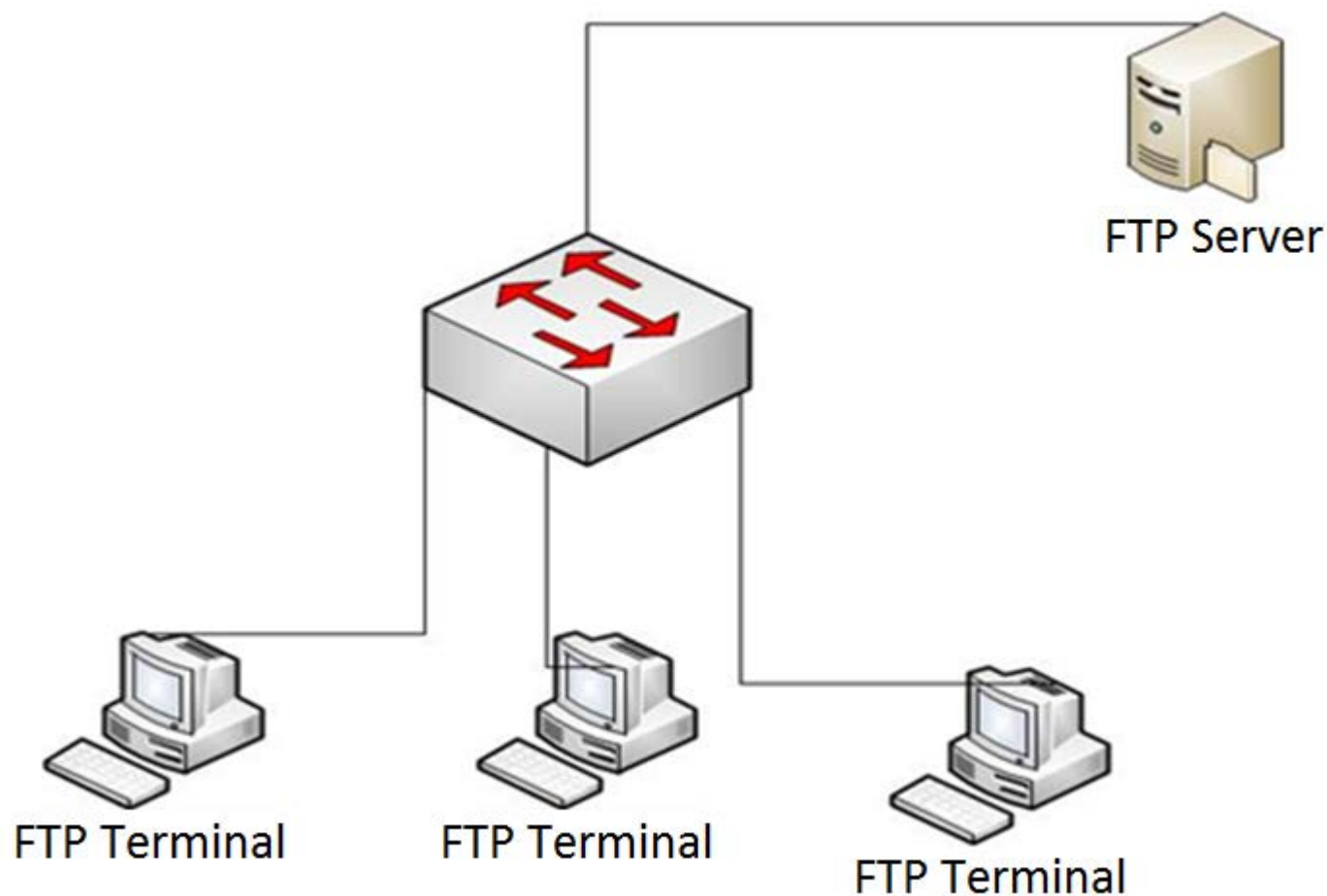
# Preventive Digital Forensics methodology (3/3)



# Case Study

- A company that we will name “Company X” is dedicated to designing advertising campaigns; has a critical IT service for collaboration and file sharing implemented on an FTP server that stores the final designs of the advertising campaigns for clients of the firm in question.
- If critical IT service is successfully attacked, Senior Management will want to have detailed and timely incident information to make the right decisions.

# 1. Analyze (Key input): Critical IT Service

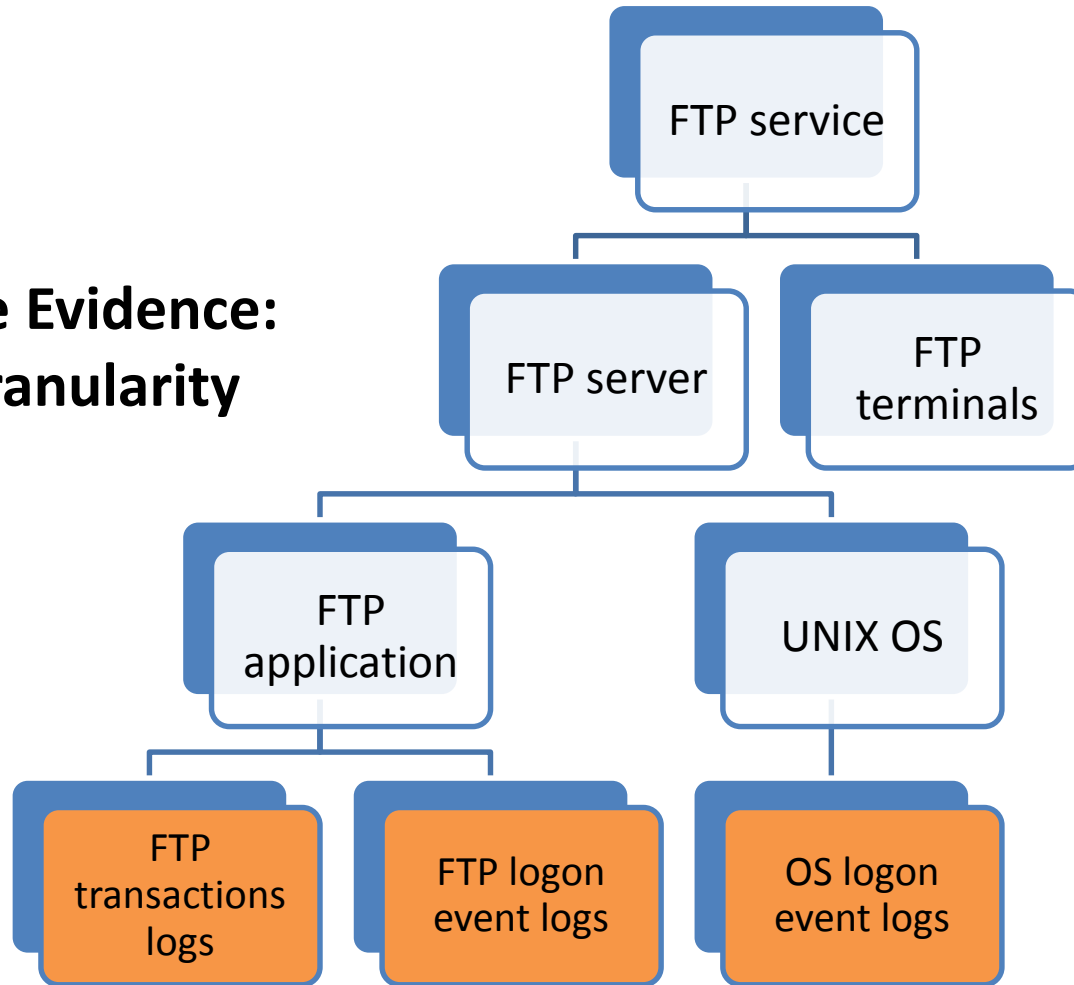


## 1. Analyze (key input): Critical IT risks

Threat	Risk estimated
Information leakage	High
Information theft	High
Intrusion on FTP server and FTP terminals	High

# 1. Analyze (key activity): Decomposition

## Pre-incident Evidence: Levels of Granularity



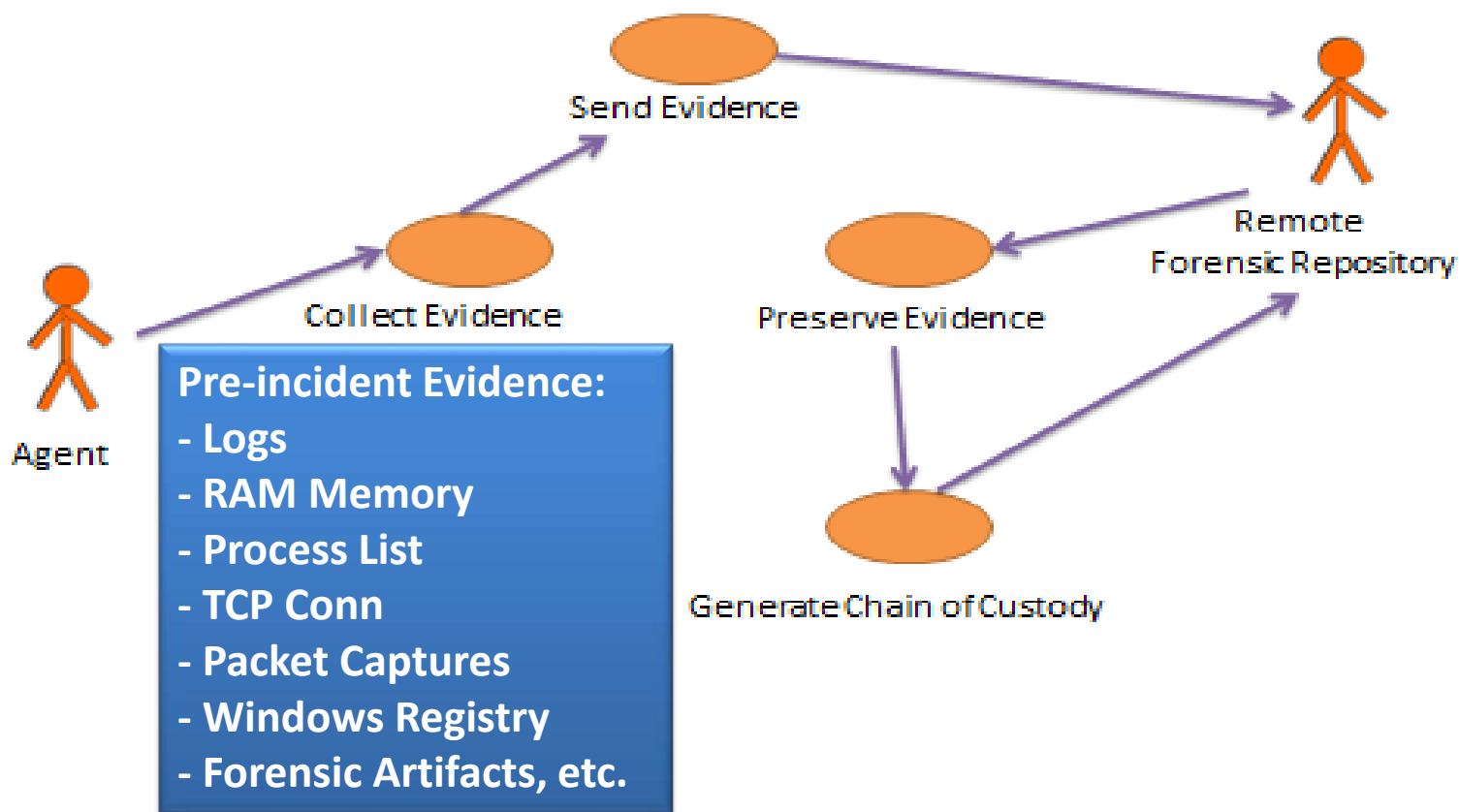
Source of pre-incident evidence production

(key output): Sources of pre-incident evidence production and their level of granularity

Critical IT Risks

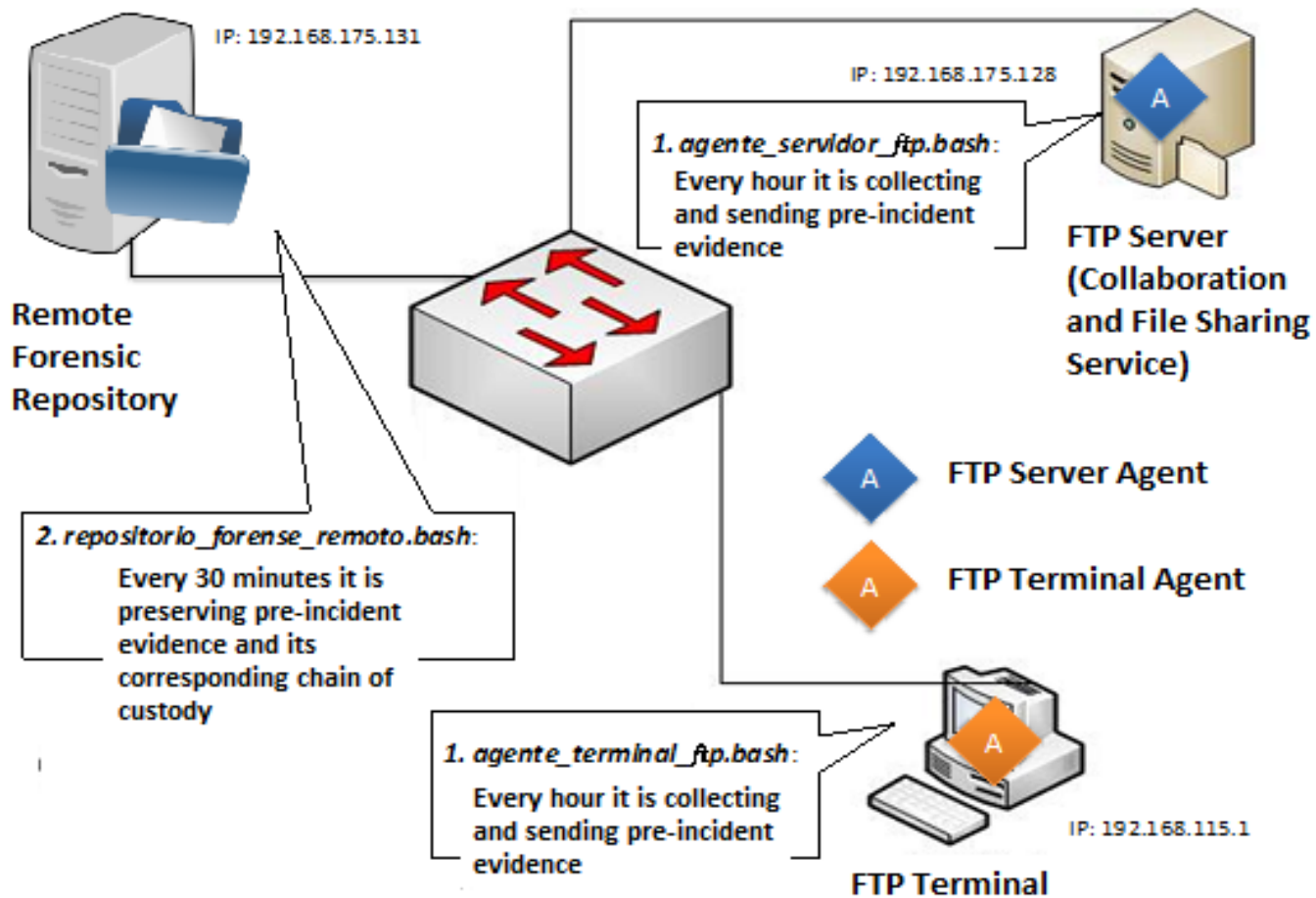
	Information leakage	Information theft	Intrusion on FTP server or FTP terminals
RAM memory (FTP server)	Process list and TCP connections		
RAM memory (FTP terminals)	Process list and TCP connections		
Syslog logs (FTP server)	OS logon events		
FTP logs	FTP transactions y FTP logon events	FTP logon events	
Syslog logs (FTP terminals)	Not required		OS logon events and program execution list

# 1. Analyze (key output): PDFS model





## 2. Build (Key output): The Preventive Digital Forensic System (PDFS)



## 2. Build (Key output): The Preventive Digital Forensic System (PDFS)

- How can I build PDFS?
  - Open Source Solutions (log management tools, packet capture tools, computer forensics tools, etc.) + SW Development “in house” (C, C++, Java, Perl, Python, BASH, etc.)
  - Commercial Solutions (EnCase, AccessData, etc).

# 3. Calibrate: through PenTest

The PDFS is collecting pre-incident evidence constantly

## EVIDENCE

Case No. \_\_\_\_\_ Inventory # \_\_\_\_\_  
Type of offense \_\_\_\_\_  
Description of evidence \_\_\_\_\_  
Suspect \_\_\_\_\_  
Status \_\_\_\_\_



Unfortunately the attack has been consummated.  
But we have evidence in the PDFS before and during the incident  
to answer the questions that support its solution.

```
Fri Jan 24 01:32:34 2014 0 192.168.115.1 272  
/home/colaboracion/archivo_confidencial_1.txt b _ o r user1 ftp 0 * c  
Fri Jan 24 01:32:34 2014 0 192.168.115.1 220  
/home/colaboracion/archivo_confidencial_2.txt b _ o r user1 ftp 0 * c  
Fri Jan 24 01:32:34 2014 0 192.168.115.1 3486  
/home/colaboracion/archivo_confidencial_3.txt b _ o r user1 ftp 0 * c  
Fri Jan 24 01:32:34 2014 0 192.168.115.1 675  
/home/colaboracion/archivo_confidencial_4.txt b _ o r user1 ftp 0 * c  
Fri Jan 24 01:32:34 2014 0 192.168.115.1 272  
/home/colaboracion/archivo_confidencial_5.txt b _ o r user1 ftp 0 * c  
Fri Jan 24 01:32:34 2014 0 192.168.115.1 220  
/home/colaboracion/archivo_confidencial_6.txt b _ o r user1 ftp 0 * c  
Fri Jan 24 01:32:34 2014 0 192.168.115.1 3486  
/home/colaboracion/archivo_confidencial_7.txt b _ o r user1 ftp 0 * c  
Fri Jan 24 01:32:34 2014 0 192.168.115.1 675  
/home/colaboracion/archivo_confidencial_8.txt b _ o r user1 ftp 0 * c  
Fri Jan 24 01:32:34 2014 0 192.168.115.1 29  
/home/user1/Documents/archivo_confidencial_9.txt b _ o r user1 ftp 0 * c  
Fri Jan 24 01:32:34 2014 0 192.168.115.1 29  
/home/user1/Documents/archivo_confidencial_10.txt b _ o r user1 ftp 0 * c  
Fri Jan 24 01:32:34 2014 0 192.168.115.1 29  
/home/user1/Documents/archivo_confidencial_11.txt b _ o r user1 ftp 0 * c
```

CE S  
ION  
AM PM  
AM PM  
AM PM  
01-255-6408

terminal  
ET  
leakage...

# Conclusions

- “... *If ignorant both of your enemy and yourself, you are certain in every battle to be in peril.*” – Sun Tzu, The Art of War.
- If it is known which are the critical organizational systems and their information security risks then, configure these systems in such a manner that they facilitate computer forensics, in order to:
  - discover and evaluate indicators of malicious behavior,
  - and to give an effective response to computer security incidents.
- The pre-incident evidence is a reliable source to detect and to mitigate threats.

# Refs

- *Forensia Digital Preventiva: Cómo crear sistemas forenses digitales preventivos para resolver proactivamente incidentes de seguridad informática en las organizaciones.* José de Jesús Ramírez Pichardo, José de Jesús Vázquez Gómez
  - [http://hammurabi.itam.mx/F/?request=forensia+digital+preventiva&func=find-b&find\\_code=WRD](http://hammurabi.itam.mx/F/?request=forensia+digital+preventiva&func=find-b&find_code=WRD)
- *A Ten Step Process for Forensic Readiness.* Robert Rowlingson
  - <http://www.digital4nzics.com/Student%20Library/A%20Ten%20Step%20Process%20for%20Forensic%20Readiness.pdf>
- *Proactive Forensics in a Reactive Environment.* Tom Prunier
  - <http://www.kshimss.org/smart05-bin/public/downloadlibrary?&itemid=87152247643274466235>

# Thanks!

## Questions & Answers

jesus.ramirez.pichardo@gmail.com

Twitter: @jesusrpichardo