Multiplicando la Inteligencia

Inteligencia de Amenazas para una mejor respuesta

Mauricio Campiglia

@MCampiglia

/in/mauriciocampiglia

mauricio@campiglia.org

¡Mucho gusto!

#whoami

- Una fork en GitLife que seguro será mucho mejor software!
    - **Padre**
- cat /dev/sec | grep * >> /dev/mind
    - **Curioso**, muy curioso, navegante compulsivo
- hexdump /tmp/life/* >> /dev/mind
    - **Nerdo** [sí, para mí “nerdo” es un cumplido…]
- Ex-multicertificado, ex-**CISA** (*ISACA*), ex-**PCI-P**, ex-**CCNP Security** (Cisco)
- Ex **IBM**, ex **CERTuy**, ex **Deloitte**, ex CTO, ex CISO, ex COO, ...
    - “*wc -l ~/.history*” da un número más grande de lo que quiero reconocer…

- Gerente de Operaciones en **SABYK**
- Docente en **Universidad ORT Uruguay**

SABYK

UNIVERSIDAD ORT
Uruguay

2

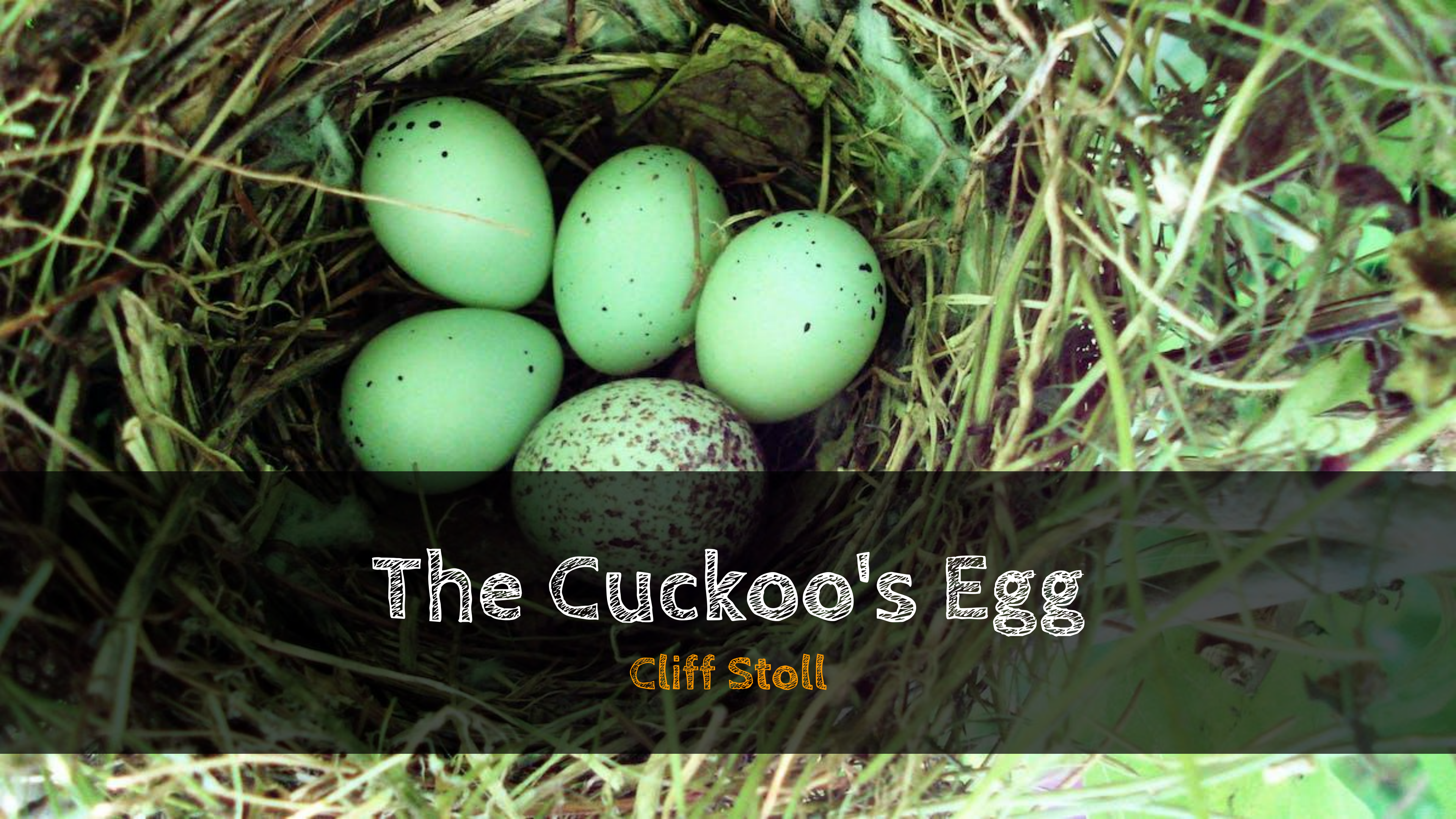
Les cuento un secreto...

Un poco de historia

Inteligencia

The fog of war

Carl von Clausewitz



The Cuckoo's Egg

Cliff Stoll

Ciberinteligencia

¿De qué hablamos?

Indicadores de Compromiso

Datos

Negative Powers
$\int x^{-3}dx = \frac{x^{-2}}{-2}+C = \boxed{-\frac{1}{2x^2}+C}$
$\int \frac{1}{x^2}dx = \int x^{-2}dx = \frac{x^{-1}}{-1}+C = \boxed{-\frac{1}{x}+C}$
$\boxed{\int x^{-1}dx = \ln|x|+C}$ (if power is -1)
$\int \frac{1}{4x}dx = \frac{1}{4}\int\frac{1}{x}dx = \frac{1}{4}\int x^{-1}dx = \boxed{\frac{1}{4}\ln|x|+C}$
Fractional
$\int x^{2/3}dx = \frac{x^{\frac{2}{3}+1}}{2/3+1}+C = \frac{x^{5/3}}{5/3}+C = \boxed{\frac{3}{5}x^{\frac{5}{3}}+C}$
$\int\sqrt{x}\,dx$ $\int\sqrt{x^3}\,dx$ $\int\sqrt[3]{x^2}\,dx$

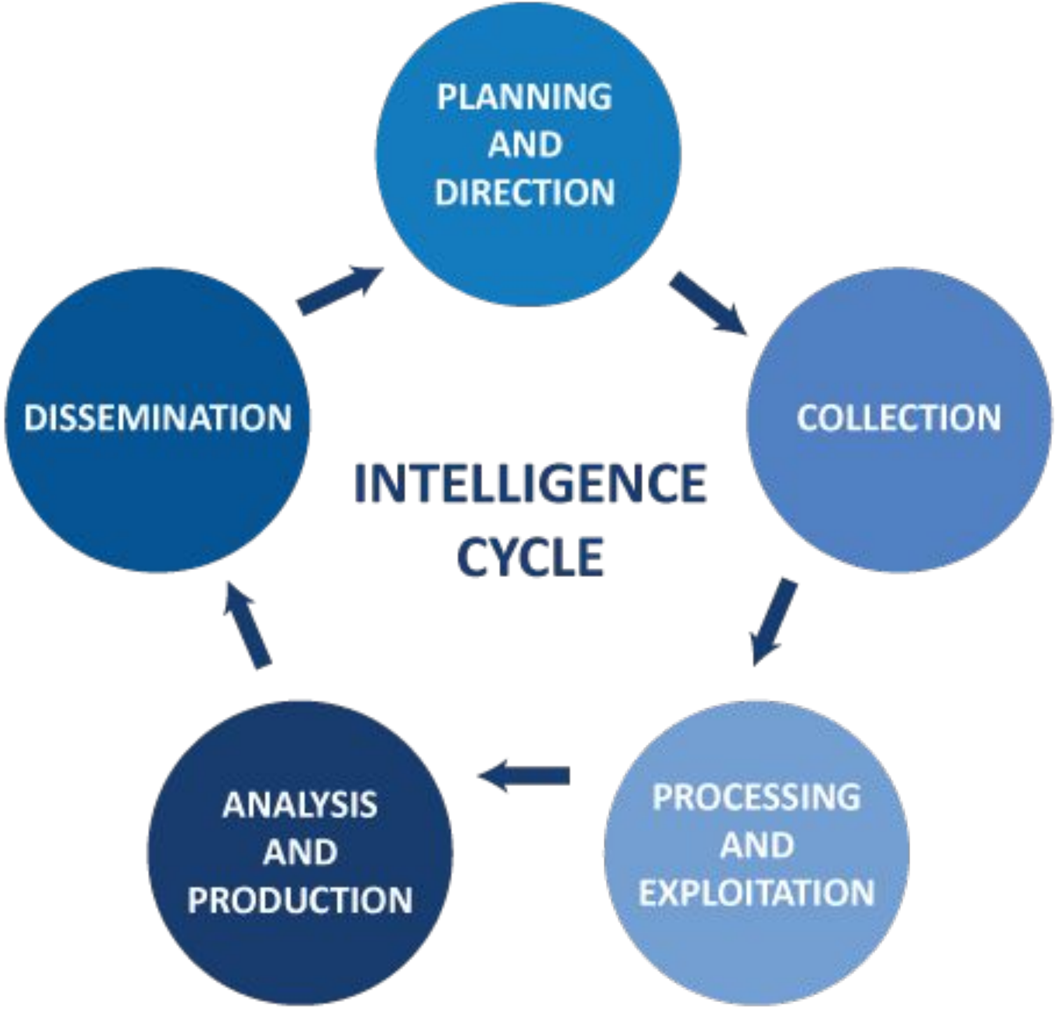
Inteligencia

Datos + Análisis (y si me permiten, contexto)

Investigación de Incidentes

Honeypots y Señuelos

Fuentes oscuras...



INTELLIGENCE CYCLE

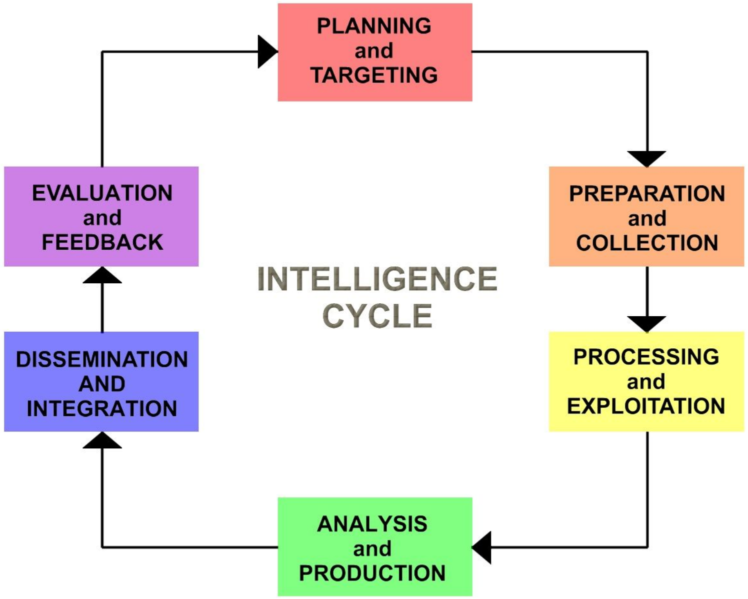
PLANNING AND DIRECTION

COLLECTION

PROCESSING AND EXPLOITATION

ANALYSIS AND PRODUCTION

DISSEMINATION



INTELLIGENCE CYCLE

PLANNING and TARGETING

PREPARATION and COLLECTION

PROCESSING and EXPLOITATION

ANALYSIS and PRODUCTION

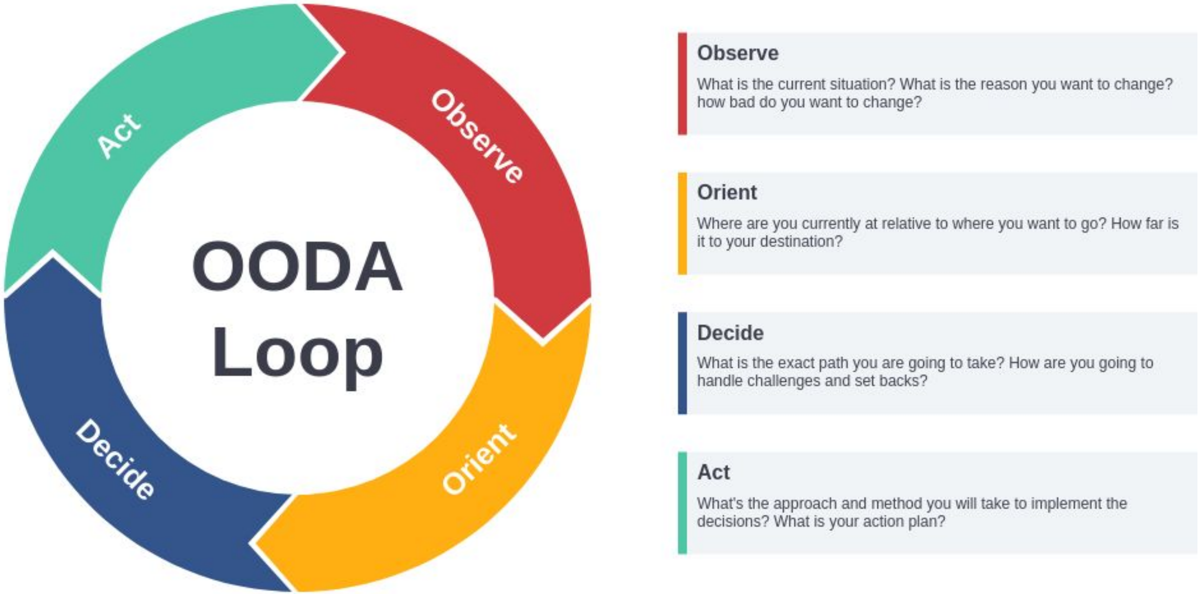
DISSEMINATION AND INTEGRATION

EVALUATION and FEEDBACK

El ciclo de Inteligencia

(¿Corregido?)

Colección y Proceso



Observe

What is the current situation? What is the reason you want to change? how bad do you want to change?

Orient

Where are you currently at relative to where you want to go? How far is it to your destination?

Decide

What is the exact path you are going to take? How are you going to handle challenges and set backs?

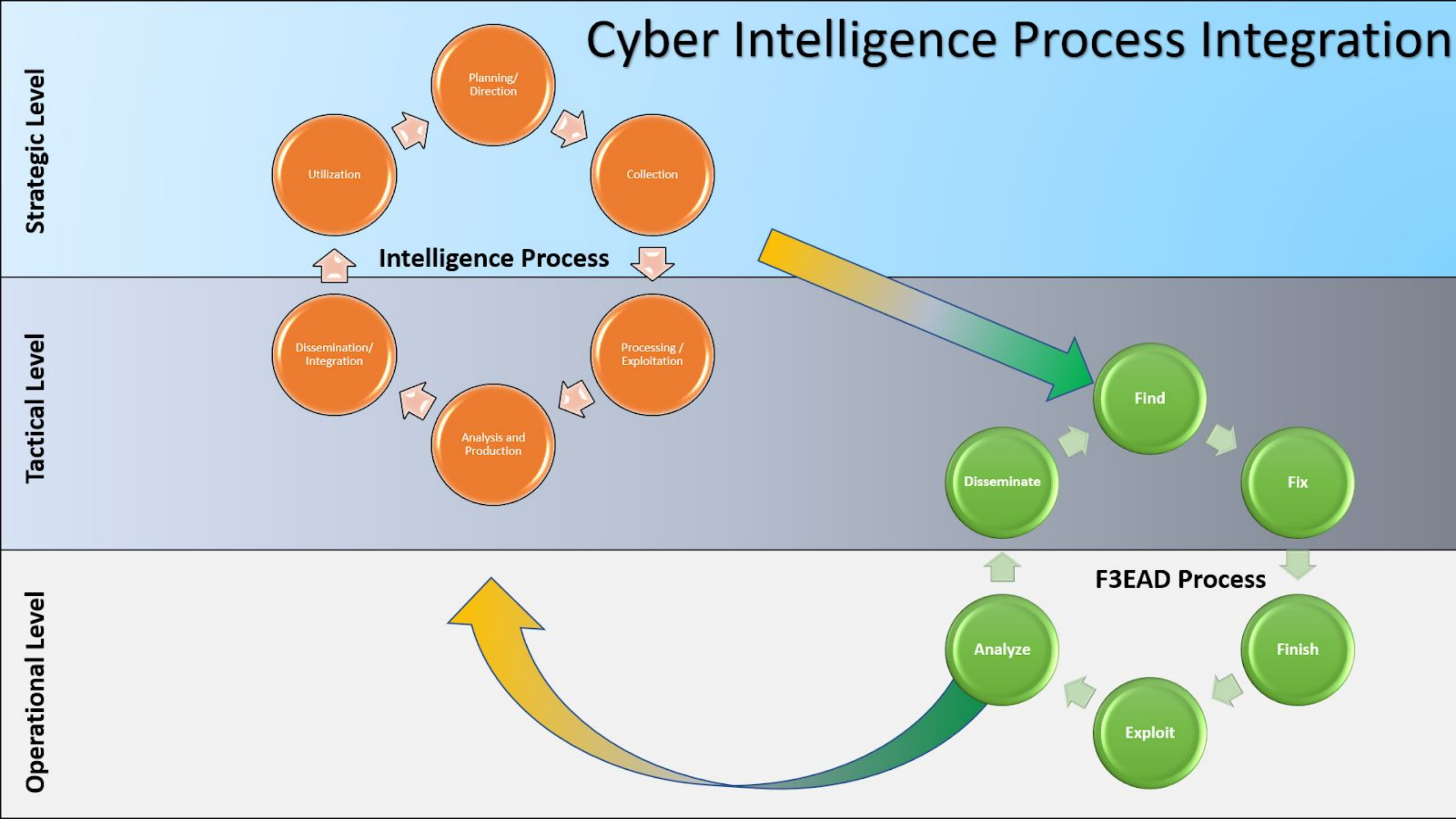
Act

What's the approach and method you will take to implement the decisions? What is your action plan?

El bucle OODA

¿Y a mí qué?

Cyber Intelligence Process Integration



Strategic Level

Tactical Level

Operational Level

Intelligence Process

Planning/ Direction

Collection

Processing / Exploitation

Analysis and Production

Dissemination/ Integration

Utilization

F3EAD Process

Find

Fix

Finish

Exploit

Analyze

Disseminate

The Cyber Kill Chain and F3EAD

Phase 1: Preparation

How do we limit the exposure of our critical information?

How can they exploit vulnerabilities to these systems ?

Phase 2: Intrusion

How do we monitor for malicious payloads and exploitation attempts?

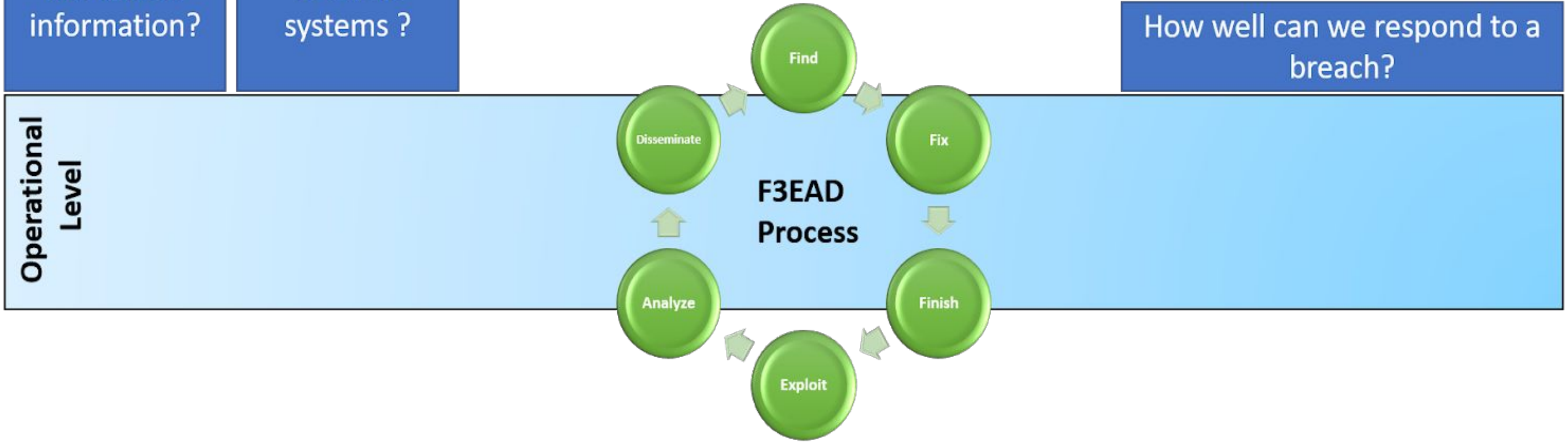
Who has the administrative privileges to install software?

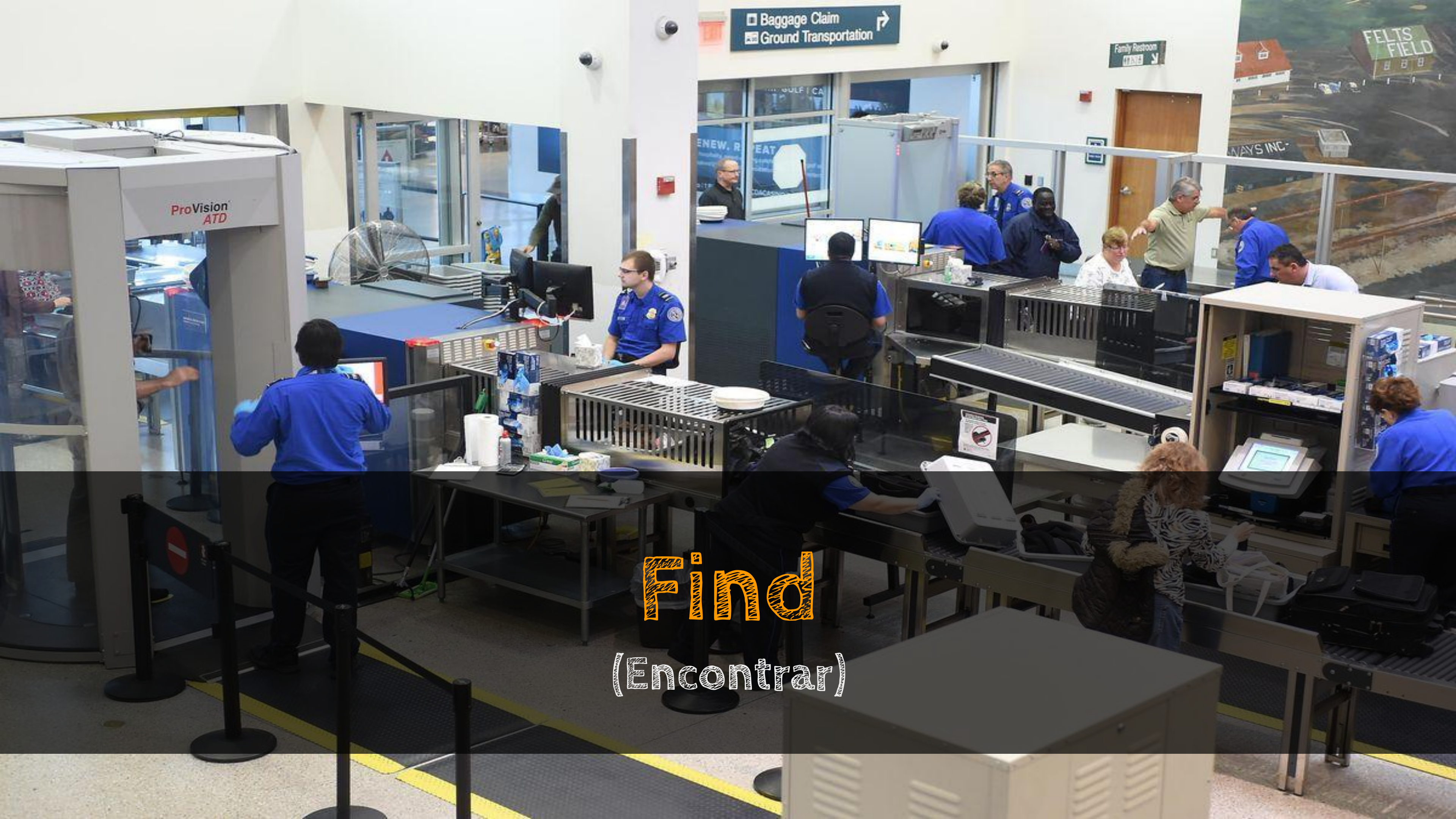
Phase 3: Breach

How do we monitor for privilege escalation?

How do we monitor for data exfiltration?

How well can we respond to a breach?



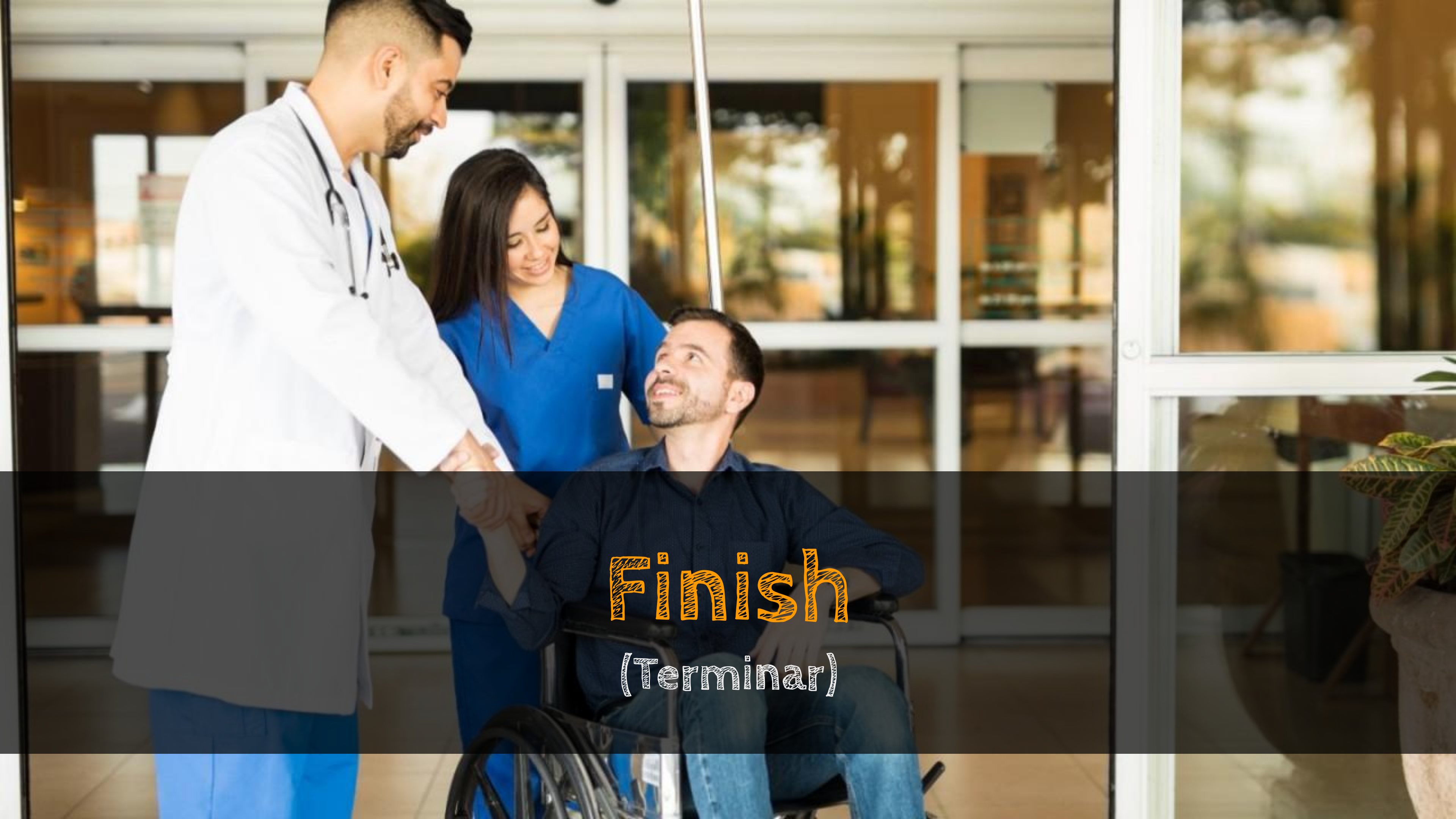


Find

(Encontrar)

Fix

(Reparar)



Finish

(Terminar)

Exploit

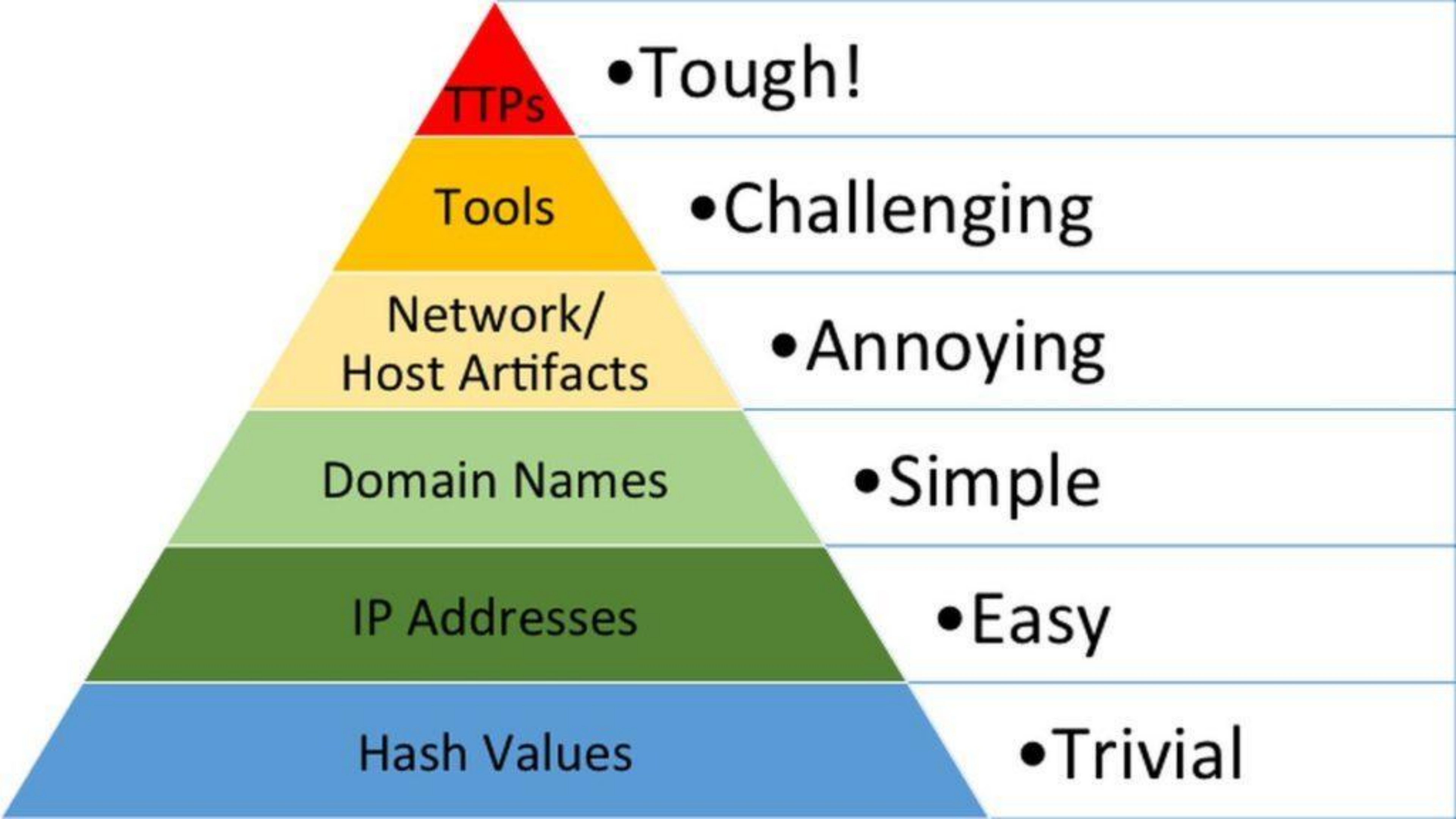
(Explotar)

Analyze

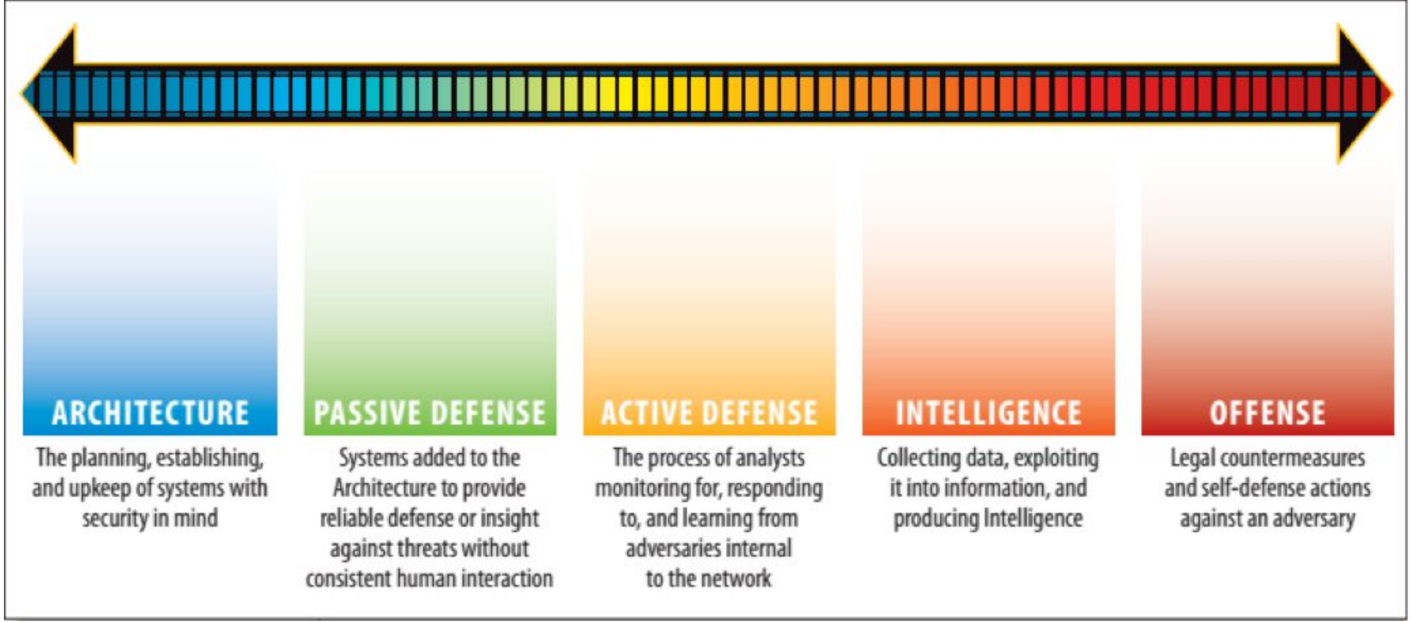
(Analizar)

Disseminate

(Diseminar)



TTPs	•Tough!
Tools	•Challenging
Network/ Host Artifacts	•Annoying
Domain Names	•Simple
IP Addresses	•Easy
Hash Values	•Trivial



ARCHITECTURE

The planning, establishing, and upkeep of systems with security in mind

PASSIVE DEFENSE

Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

ACTIVE DEFENSE

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

INTELLIGENCE

Collecting data, exploiting it into information, and producing Intelligence

OFFENSE

Legal countermeasures and self-defense actions against an adversary

Defensa Activa

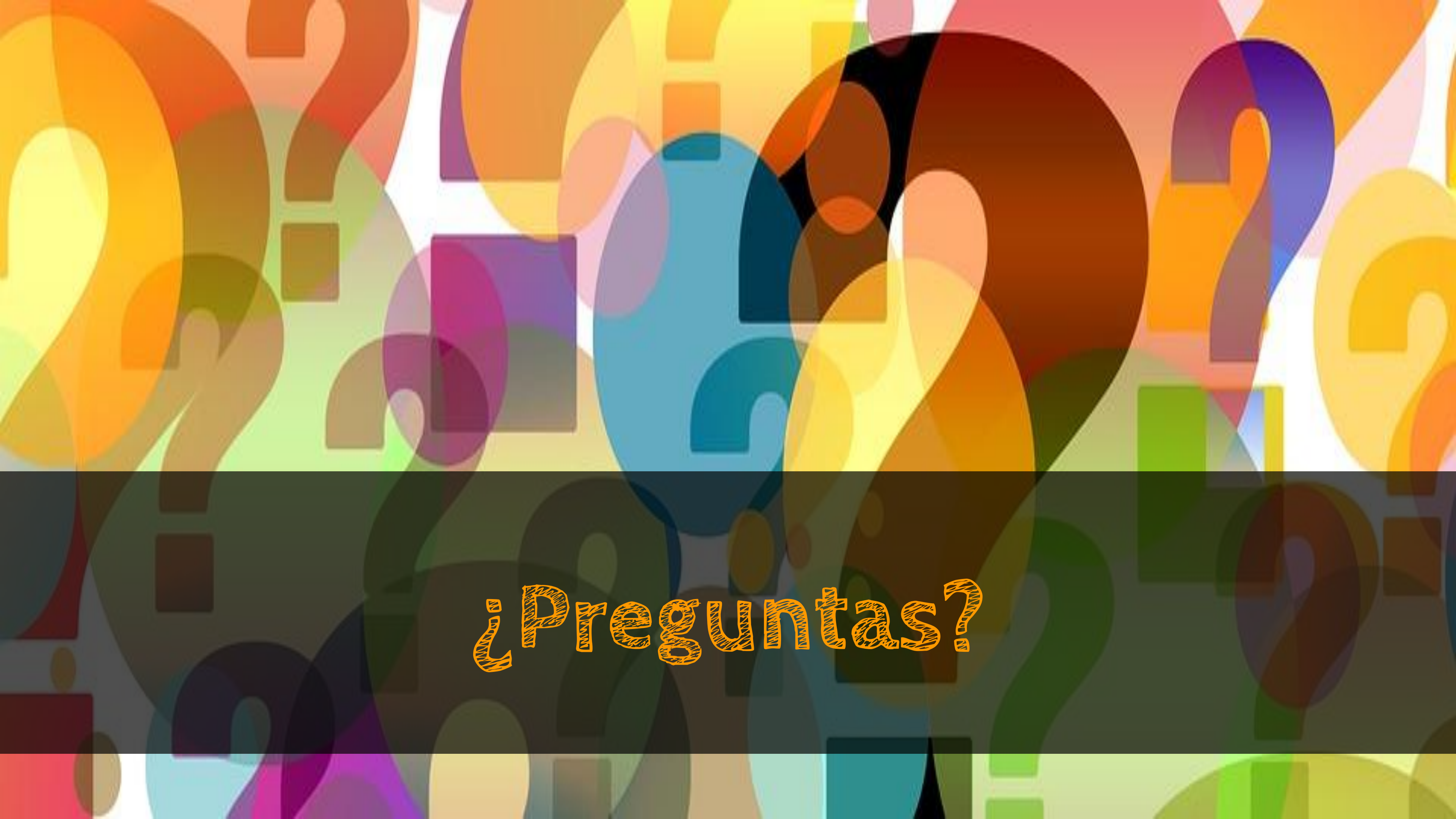
AGETIC
Digitalizando Bolivia

Martes 29 - Taller Sala Verde (P2) - 13:30

Inteligencia de amenazas mediante fuentes abiertas

Gonzalo Nina

¡No se lo pueden perder!



¿Preguntas?

Mauricio Campiglia

@MCampiglia

/in/mauriciocampiglia

mauricio@campiglia.org