CAPA

2017 AUSTRALIA PACIFIC Aviation & Corporate Travel SUMMIT

# Is your flying CyberSafe?
# Cyber Risks Of Modern Aviation

April 5th, Dubai, UAE

**Jorge Sebastiao, CISSP**
**ICT Security Expert**
**Cloud Practice Leader**

HUAWEI

# Disclaimer & Copyright

- *Please note that this presentation is for informational, knowledge sharing and educational purposes only. Any comments or statements made herein do not necessarily reflect the views of Huawei. The information is intended for the recipient's use only and should not be cited, reproduced or distributed to any third party without the prior consent of the authors. Although great care is taken to ensure accuracy of information neither the author, nor Huawei can be held responsible for any decision made on the basis of the information cited.*
- *The content of this presentation is based on information gathered in good faith from both primary and secondary sources and is believed to be correct at the time of publication. The author can however provide no guarantee regarding the accuracy of this content and therefore accepts no liability whatsoever for any actions taken that subsequently prove incorrect.*
- *The practices listed in the document are provided as is and as guidance and the author and Huawei do not claim that these comprise the only practices to be followed. The readers are urged to make informed decisions in their usage.*
- *The information presented in this presentation is not intended to be, and should not be construed as, an offer to sell any products or services or a solicitation of an offer to buy any products or services . Any such offer or sale will be made pursuant to, and the information presented at this meeting is qualified in its entirety by, authorized offering documents and related disclosure schedules or similar disclosure documentation.*
- *All logos and brand names belong to their respective owners and we do not claim any relationship or association, implied or otherwise, with them.*
- *Use of any materials by virtue of relationships and associations, if any, are mentioned explicitly.*
- *Author has taken care to attribute all sources for external materials used in this presentation, and any oversight is regretted. If you, as owner, or as viewer, find any reason to dispute the use of these materials kindly communicate the same to author.*
- *Any omissions, in terms of attribution, may be due to an error of author and not intentional.*

# Sampling of Cyber Risk

Radios


Users & Social Media


GPS

#11

---LX PNR---
PURGE PURGE CREATION ORIGINATOR
DATE FLT NO TIME DATE TELETYPE DUTY SIGN CITY
29OCT11 LX4245 1542 19SEP11 MUCRM1A LX
PNR ADDRESS: RJSMRU EDE945A9
NAMES
1HASBROUCK/EDWARDJMR

ITINERARY
AC7687 K 14OCT11 BOSYUL HK 1 1645-5 1752-5 Y-K I D
AC0832 K 14OCT11 YULBRU HK 1 1945-5 0835-6 Y-K I D
LX4245 H 29OCT11 LJUZRH HK 1 0745-6 0900-6 Y-H L 1AT$01
LX0038 H 29OCT11 ZRHSFO HK 1 1315-6 1620-6 Y-H L 1AT$01

PRN Legacy Systems

Drones

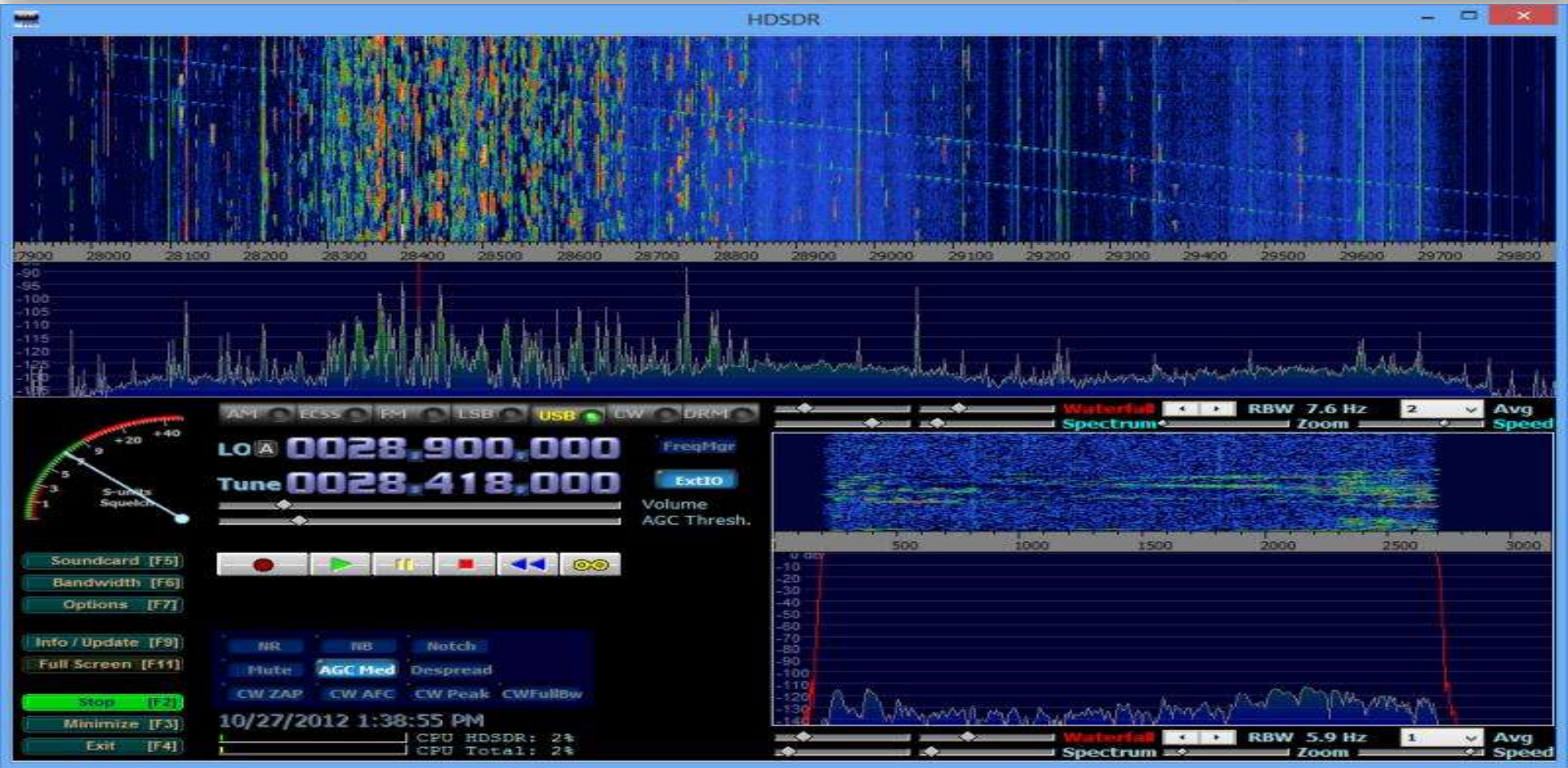
# SDR Radios


FlightAware
1090MHz Mode S Filter
SMA-F — SMA-M


RTL-SDR.COM


RTL-SDR.COM

# SDR Intercept - Disrupt



# Radios


بریکنگ نیوز : پاکستانی ہیکروں نے بھارتی ائیرلائن کا سسٹم ہیک کر
کے جہاز میں دل دل پاکستان کے گانے چلا دئے، پائلٹ پاگل ہوگئے

# Taking control Drone GPS


# Taking control ADS-B


```
*02C18C90FDBC7000000000000000;
*028102B6FB4C87000000000000000;
*028102B6FB4CA7000000000000000;
*028102B6FB4C87000000000000000;
```

| Nr. | ICAO24 | Regist. | Ident | Alt |
|---|---|---|---|---|
| 18 | A4ECA6 | USA | | 4250 |
| 17 | AC3068 | USA | N885A | 7875 |
| 16 | A3F0BC | USA | | 30000 |
| 15 | C01E10 | C-FLJZ | | 12000 |
| 14 | A284B5 | N261WN | | 35000 |
| 13 | AB7B8C | N839UA | | 950 |
| 12 | A3A086 | N33266 | | |
| 11 | ABAC48 | N951NN | | 6700 |
| 10 | AC5110 | N893GA | | 31975 |
| 9 | A708DA | N552WN | | 15875 |
| 8 | A03816 | N113HQ | | 29000 |

```
71C254 Short-air-sourv. Korea          AC:
A86E6C Short-air-sourv. USA            AC:
AC9731 Short-air-sourv. USA            AC:
71C254 Short-air-sourv. Korea          AC:
A86E6C Short-air-sourv. USA            AC:
A86E6C Short-air-sourv. USA            AC:
```

# Drones Risks

# Instagram Boarding Passes



# PNR


[redacted] 6a
*** ELECTRONIC TICKET ***
F 1.1HASBROUCK/EDWARDMR
HW1ACWW 29AUG PMIME5
1 AC 761 A SA 9SEP YULSFO HK1 0830 1130 CABY
FONE-
1.WW1-H 1 415 824-0562
2.WW1-P 1 415 824-0214
3.WW1-A 1130 TREAT AVE./**/SAN FRANCISCO CA/94110 US
4.WW1-A AIRCANADA//HASBROUCK.ORG/MEMBER EMAIL
TKT-
1.1 K29AUGWW1WW 01421380664S3
AP FAX-
1.1 SSRFQTVYYPN1 /UA00168716753
RMKS-
1.1 C/H IS EDWARD HASBROUCK/CA USER ENTERED CREDIT CARD/USD 248
.78/ALL PSGRWEB BOOKING/EMAIL TO C/H
2. MOP: CHARGE MY CREDIT CARD
3. PASSENGER REQUESTED I/R DELIVERY BY EMAIL TO AIRCANADA//HASBR
OUCK.ORG
4. TIDGERGJK1J4
5. BKIP 172.24.96.31 29AUG06 17:22
---HISTORY---
RCVD-INTERNET PNR GUEST
WW1 AC WW 17233/29AUG
WW1 GS WW IOIBMC1 17233/29AUG
NO FLOWN SEGS
Home and Mobile
Telephone Numbers
Home Address
Email Address
Frequent Flyer Number
Credit Card Number (redacted)
Timestamped IP Address

# Hack Airplanes though Entertainment system

# 0 Day Exploits - Guaranteed

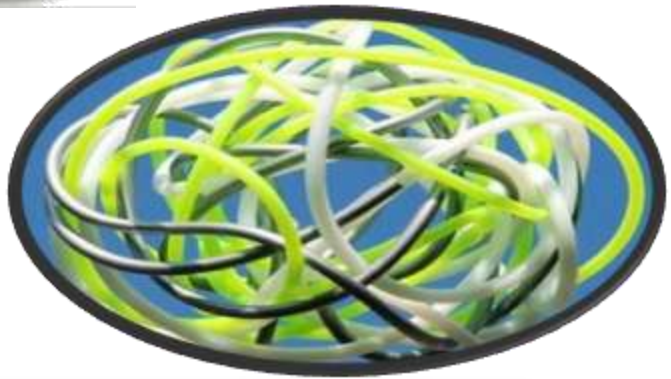
# Cyberspace Characteristics

Asymmetric

Attribution Problems


No Borders

Complex Interconnected Systems



# Our security enemy is?

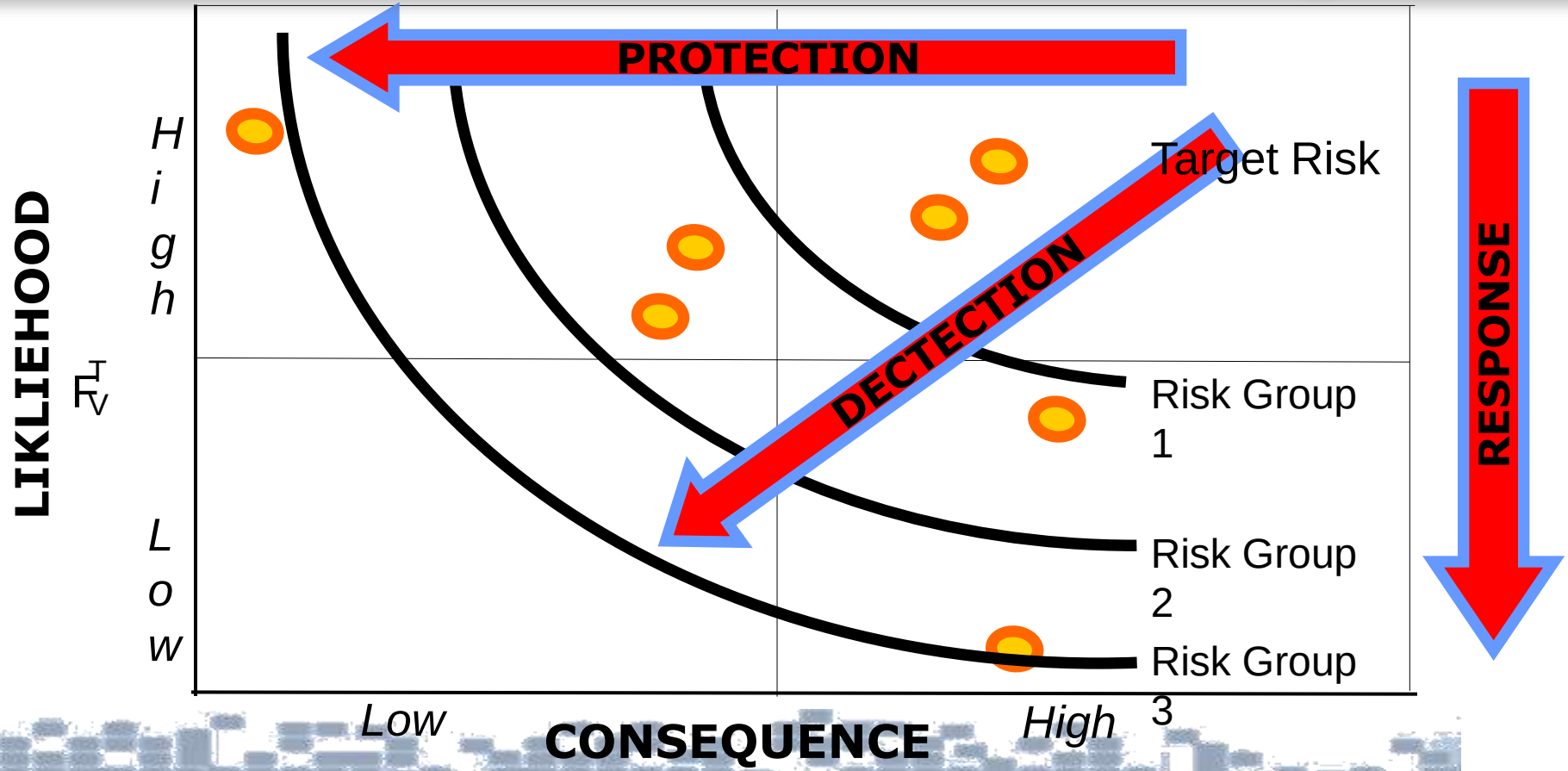
# Security Nightmare

# Outdated Assumptions?

# Effective Countermeasures

# Wrong Skills?

# Risk Reduction Strategies!



# Build Airport Cyber Security Intelligence

## Multiple Sources Intel

Internal Security Research

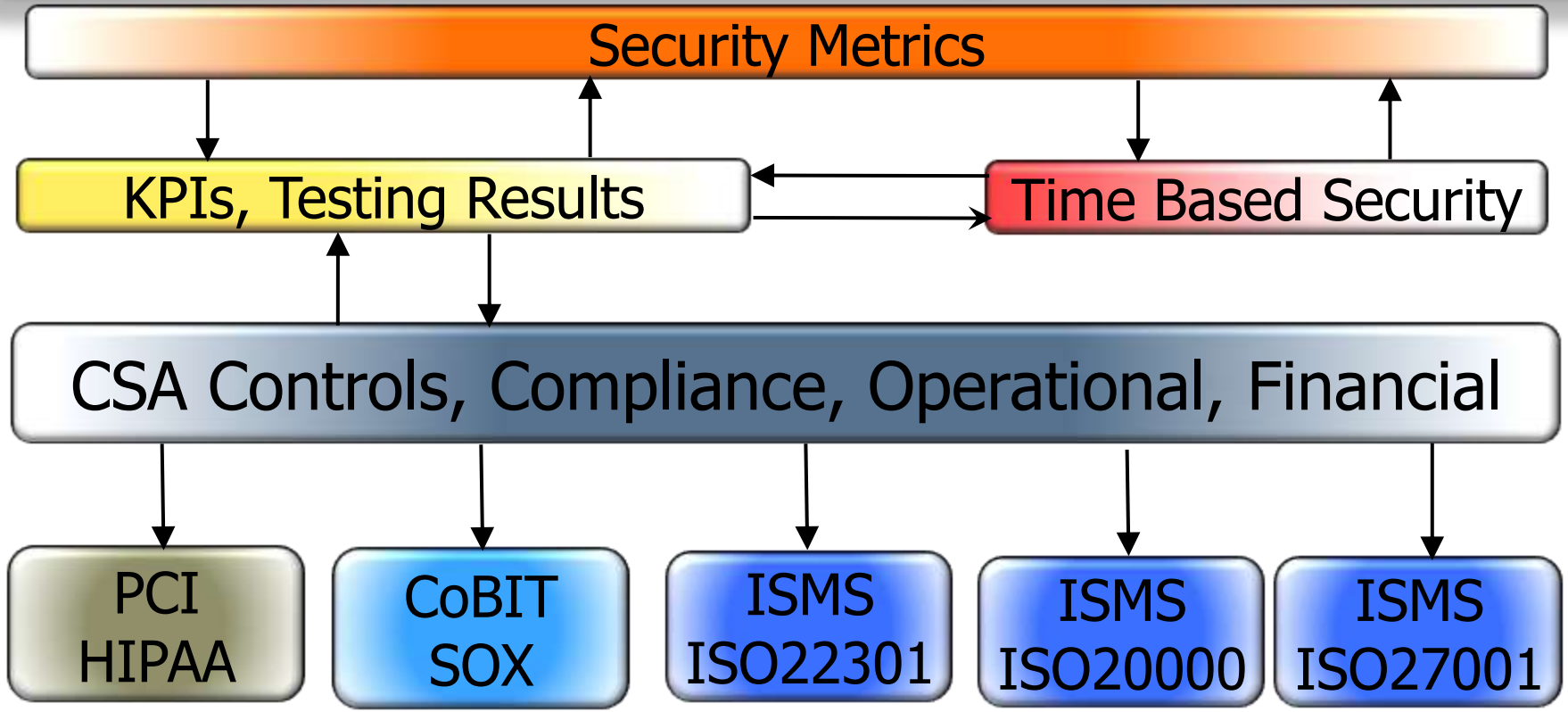
Partners, Vendors, CERT ,…

Internet, Mailing list and other sources

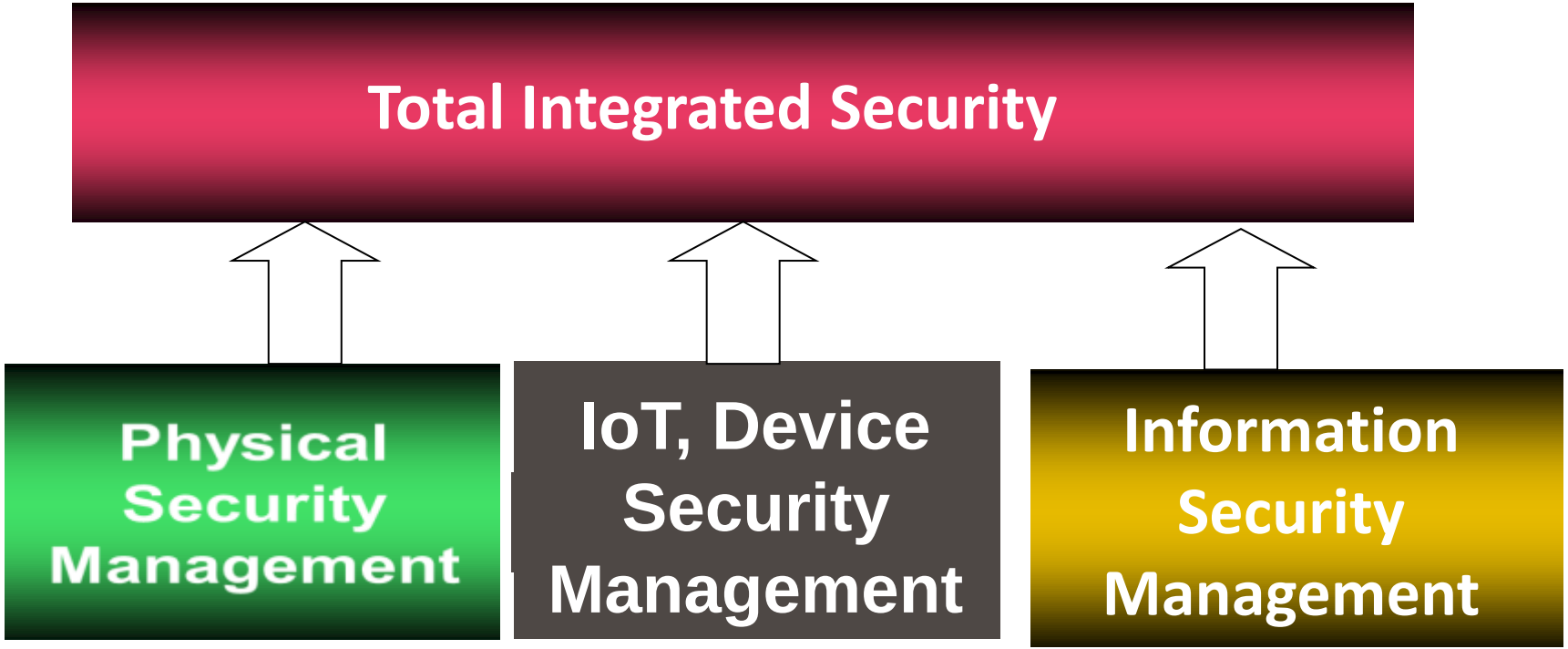
Infosec Knowledge Base Response

Incidence Response

# Road to Security Metrics



# Final Goal Is



# Winning the War

| Red Teaming | Solve Attribution |
| --- | --- |
| Continuous Vulnerability Mgmt | Crowd Sourcing/Bug Bounty |
| Fusing | Crisis Management |
| Vertical CERT Integration | Encryption |
| Exchange Knowledge | Data Leak Prevention |
| Threat Management | Reputation Management |
| Big Data | Honeynets |
| Machine Learning | Sandbox |
| Security Metrics | Empower end users |
| Continuous Training | Attack / Take down |

# Don’t bring a knife to gun fight

RULES FOR A GUNFIGHT

1. Bring a gun. Preferably, bring at least two guns. Bring all of your friends who have guns.

# Questions

**Jorge Sebastiao, CISSP**
**ICT Expert**
**Jorge.sebastiao@huawei.com**

HUAWEI