

THE NATIONAL CSIRT/CC OF INDONESIA

Id-SIRTII/CC



Mata Garuda

An advanced Network Monitoring System

The *S.L.A.D* Network Security Framework

FIRST Conference
Berlin, 19 June 2015

Security in Real Life





Setting off a
FALSE ALARM
Can Cost You!

A red fire alarm pull station with a silver handle and the text 'PULL IN CASE OF FIRE' and 'FIRE ALARM' on it.



Car Alarms

=

Network Security Alarms

**Intrusion Detection System
(IDS)**

Our responsibility : Indonesia CERT/CC

Vision

Build Indonesia Internet within safe, comfortable and conducive environment

Mission

Improves the Nation's cyber security posture, and proactively manages cyber risks to the Nation's cyberspace.

40 Network Access Providers

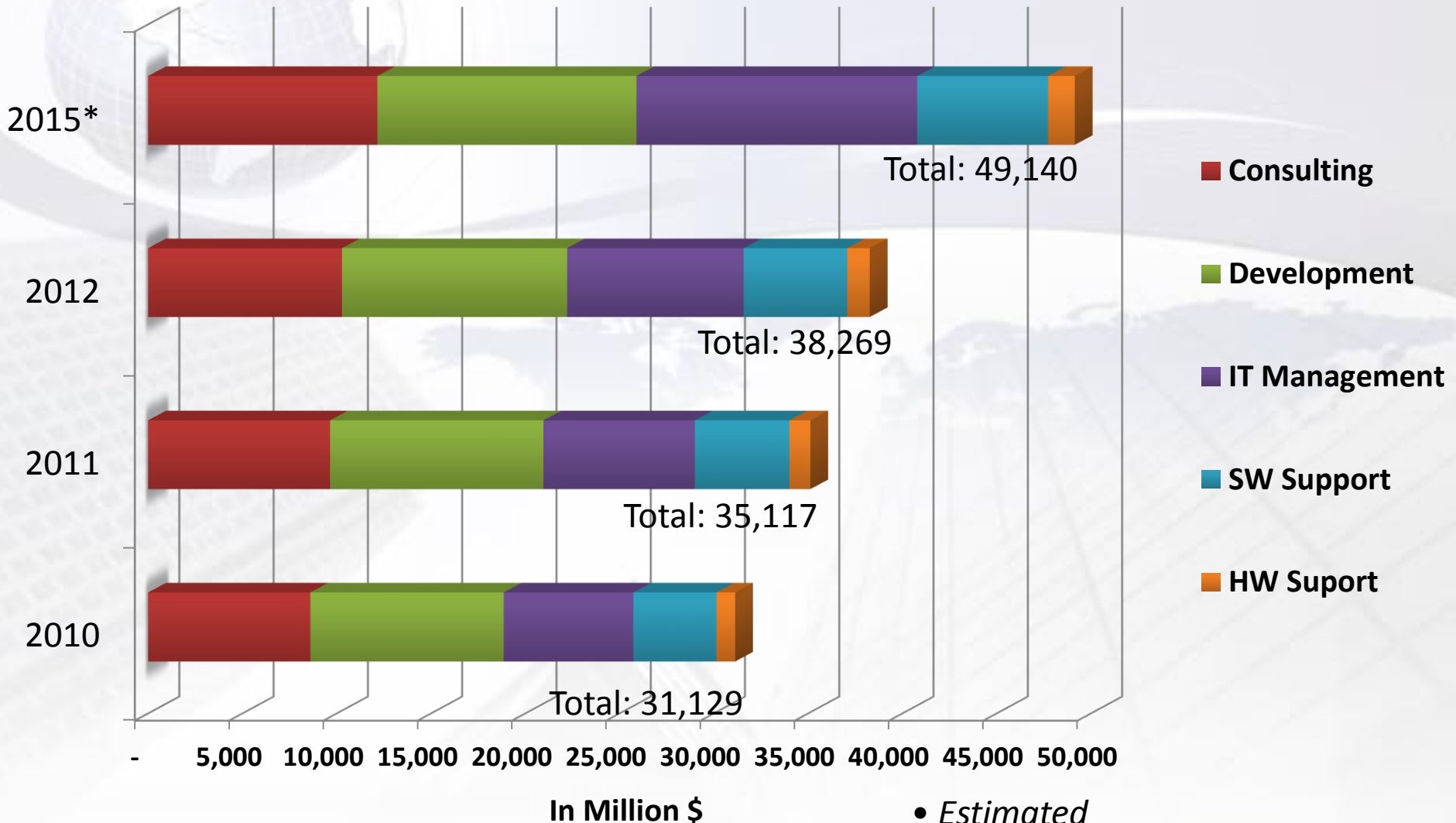
300 Internet Service Providers

12 Telco's with 110.000 BTS
3G/4G

23 Million ICT ready
companies

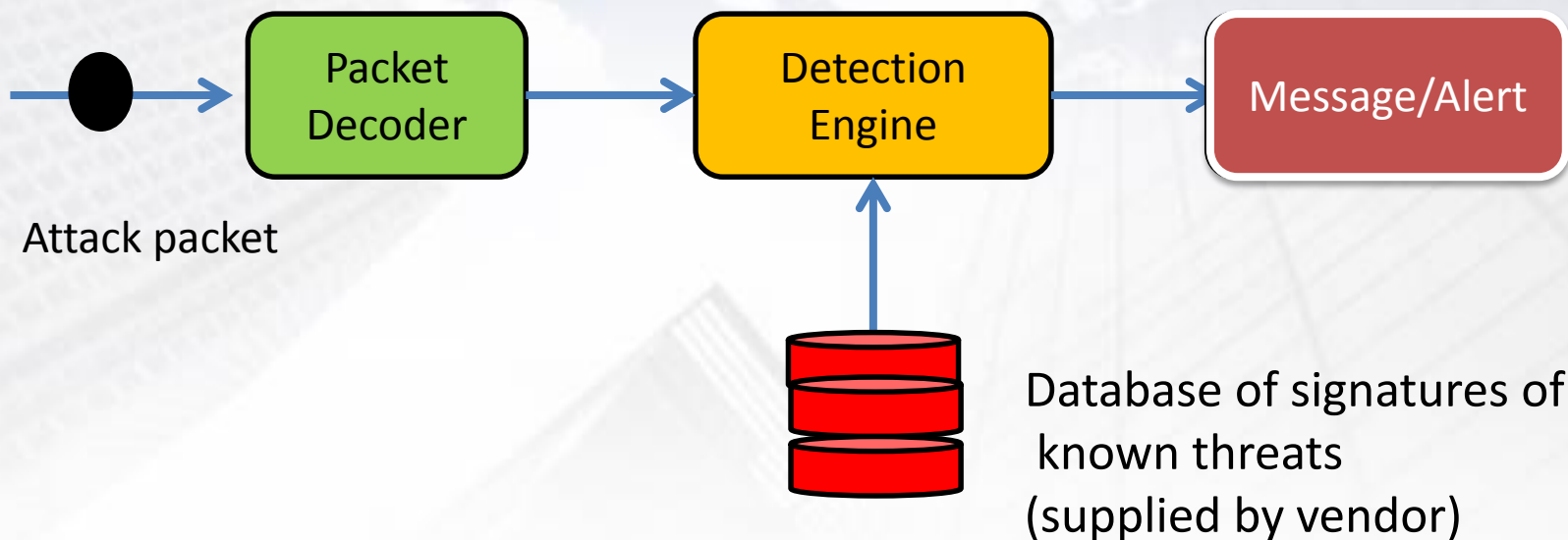
75 Million Internet User

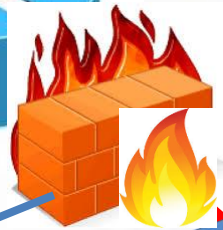
Worldwide Security Service Spending



Common **IDS** Technology

Signature based IDS





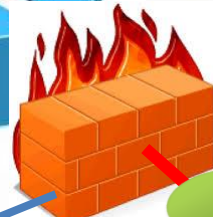
Everything i\$ OK



Bad packet



True Positive

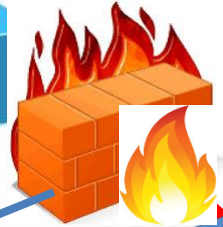


Good packet



Everything i\$ OK

False Positive

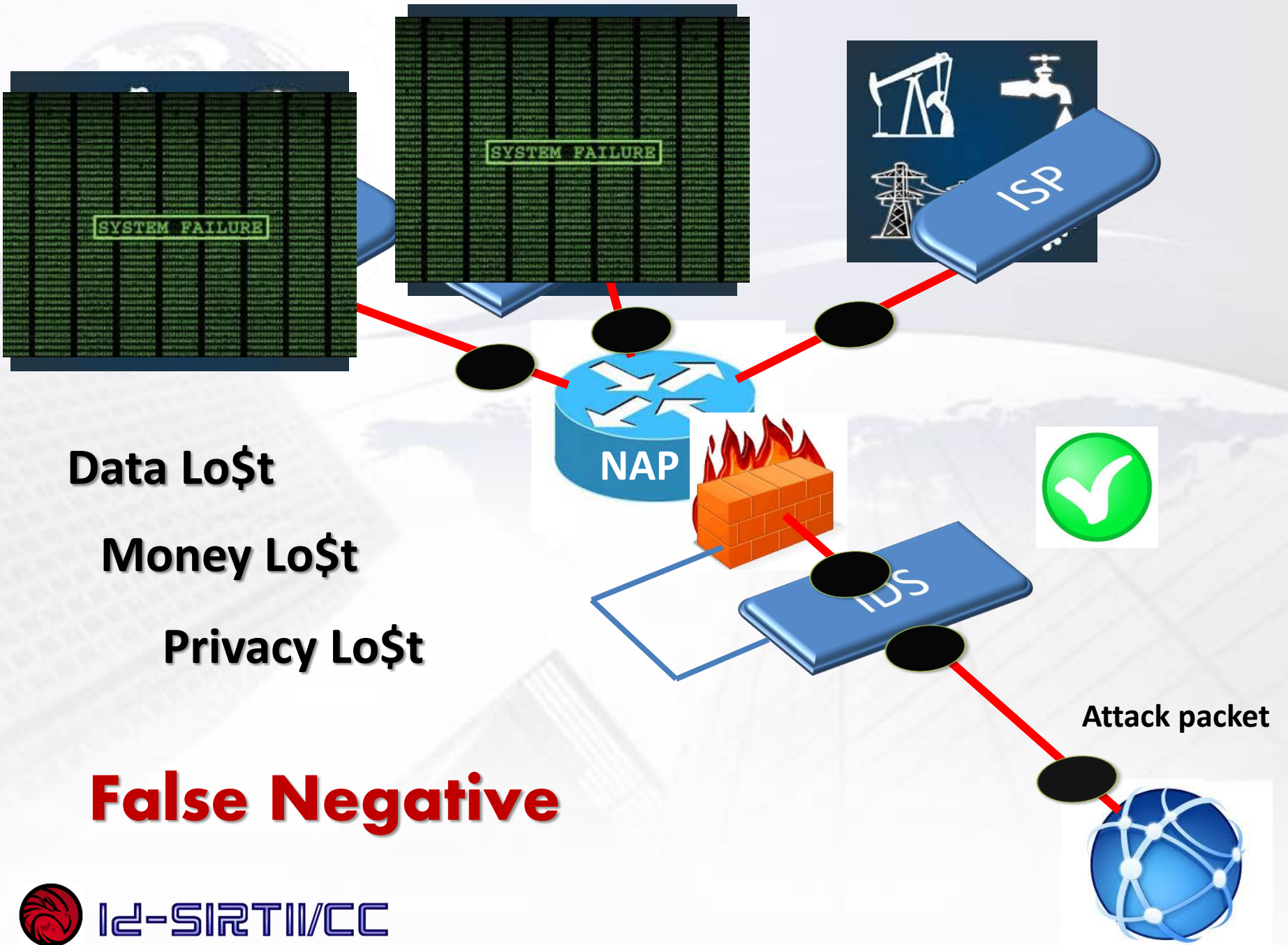


Good packet



**Valuable Net
Activity get Lo\$t**

True Negative



Data Lo\$

Money Lo\$

Privacy Lo\$

False Negative

Detection State of IDS

A legitimate attacks
which trigger alarms

True
positive

False
Positive

Alarms are generated,
But no attacks have
taken place

No attack has taken place
and no alarm is raised

True
Negative

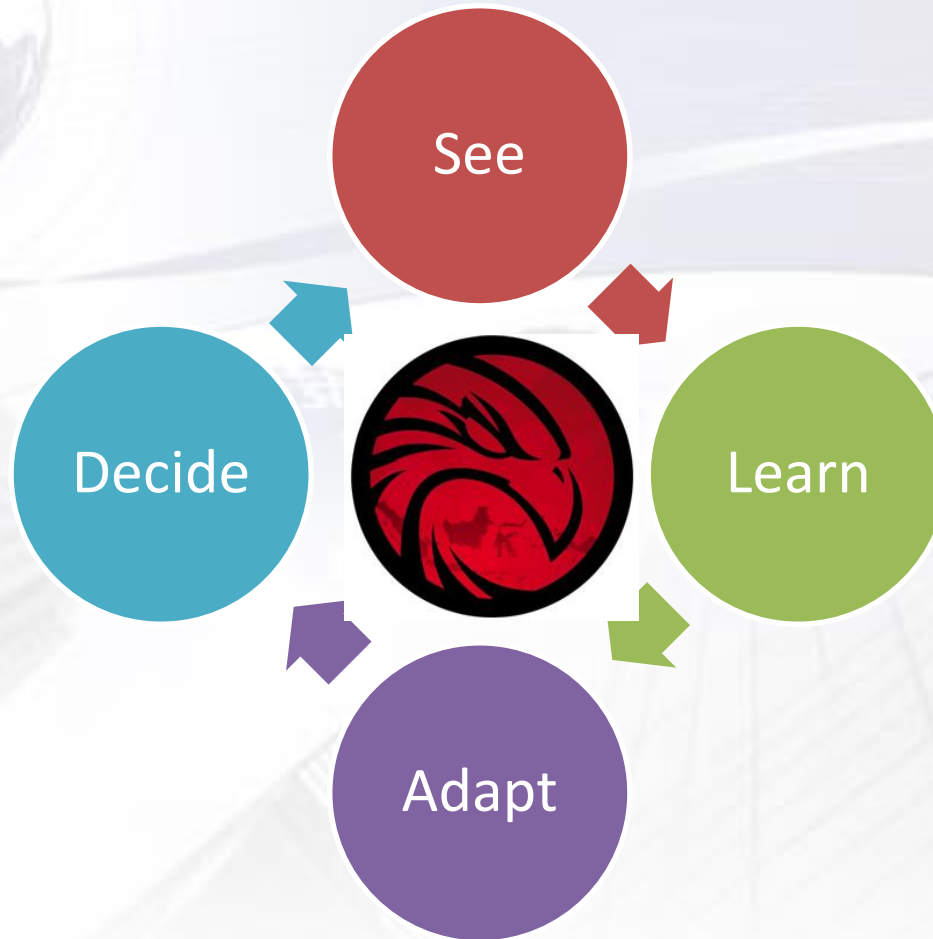
False
Negative

A failure of an IDS
to detect actual attacks

Threats change –
Common IDS Technology Have not



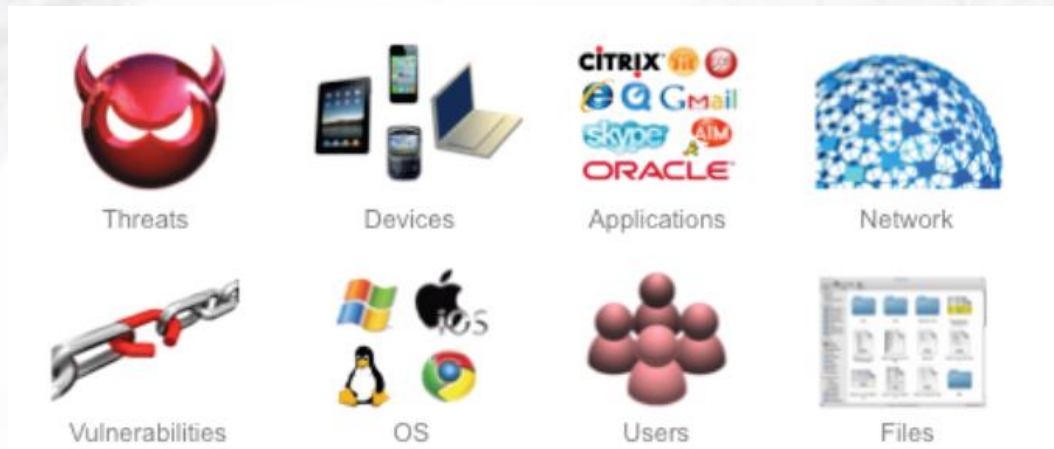
What the Cyber Security Needs is



...a continuous process to responds to continuous change

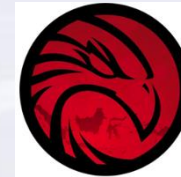


- **See** everything in one place – depth seeing
- **Learn** - Gain insight into your **local** traffic characteristic by **Intelligent engine**
- **Adapt** - Change is constant : leverage open architecture
- **Decide** - Reduce the “false noise” to make better decision



Mata Garuda Network Monitoring Solutions

Common IDS
Technology



Technology

Closed / blind

SEE

See not only
the attacking phase

Black box / inflexible

LEARN

Intelligence about
Local traffic with
machine learning tech.

Fixed analysis tools

ADAPT

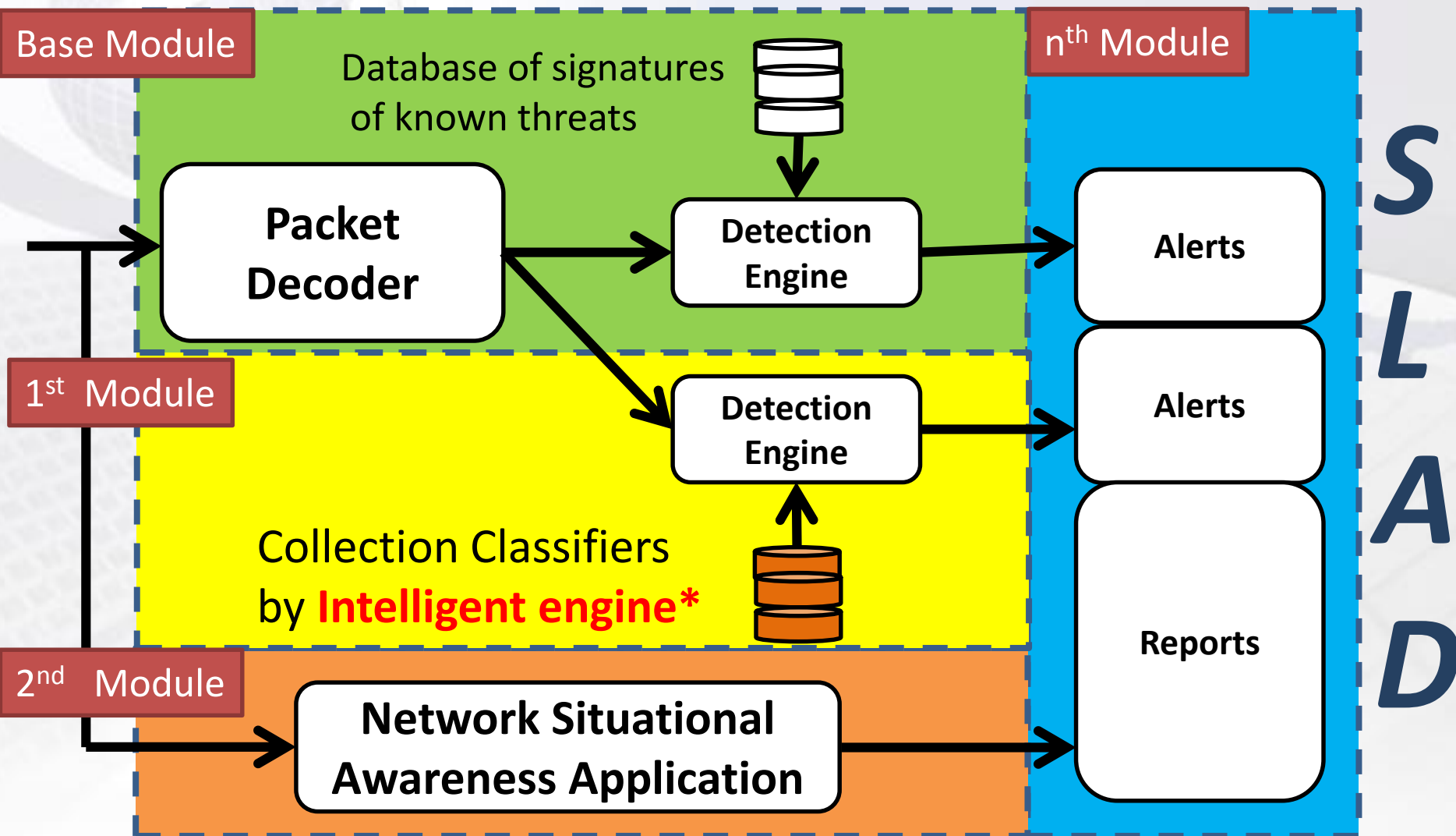
Modularity analysis tools

Many “false alarms”

DECIDE

Reducing false alarms with
intelligence technology ¹⁶

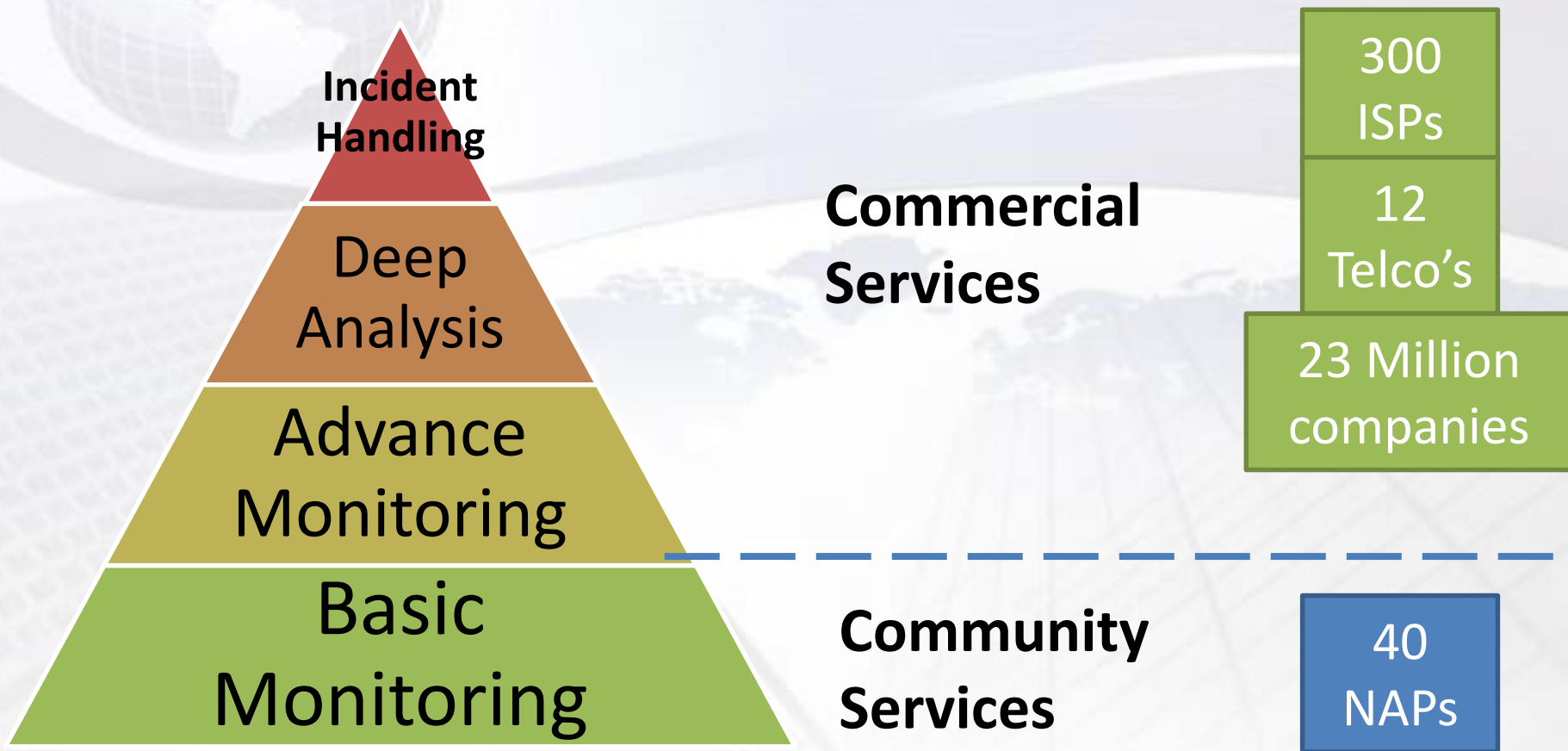
How it works?



Value to Government, Public and Private Sectors



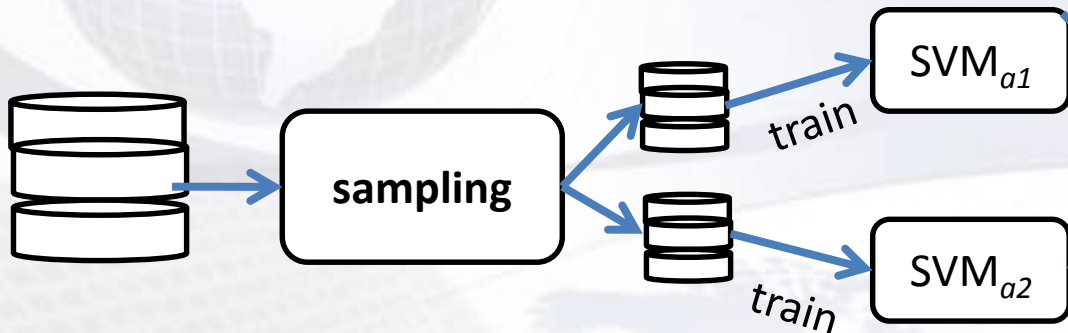
Community vs. Commercial Services



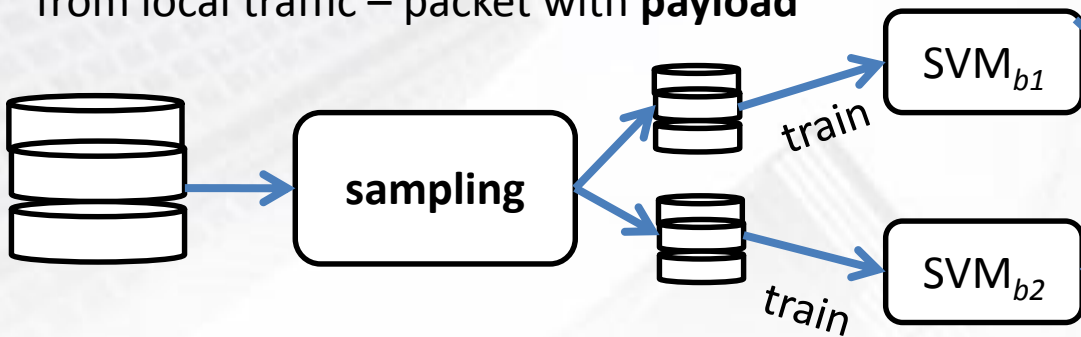
Intelligence detection engine based on Machine Learning tech

- Machine Learning as second classification engine
- It is based on Support Vector Machine (SVM)
 - It has been proven to be one of the best classification method
 - We have done benchmarking by using data from DARPA (Defense Advanced Research Projects Agency). By using 8 features *It can give 99% detection rate*

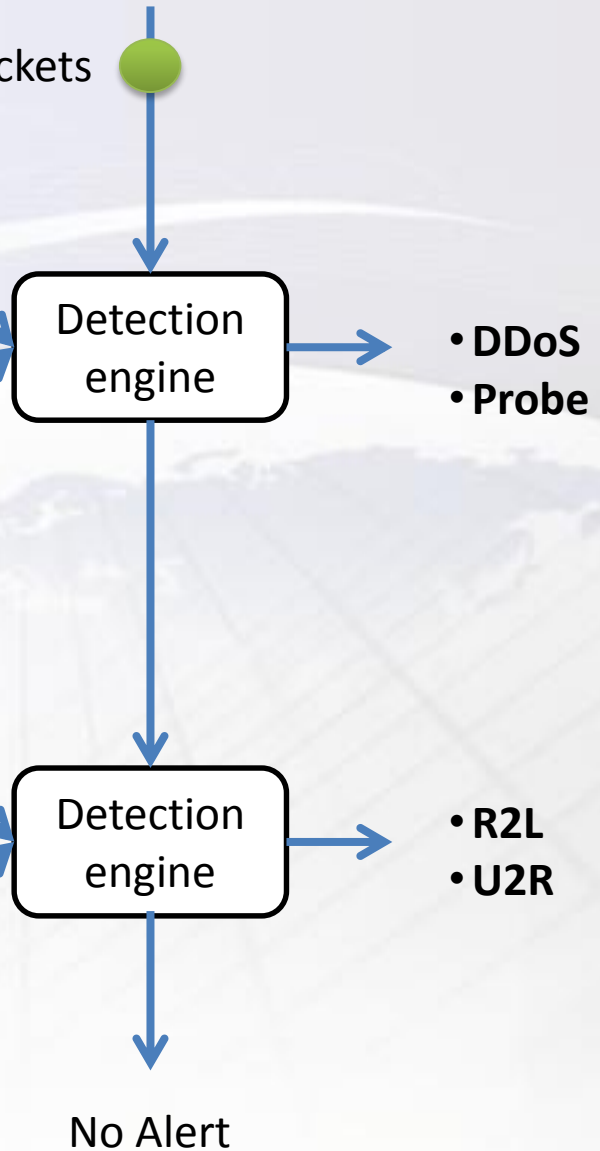
Train data set
from local traffic – packet **without payload**



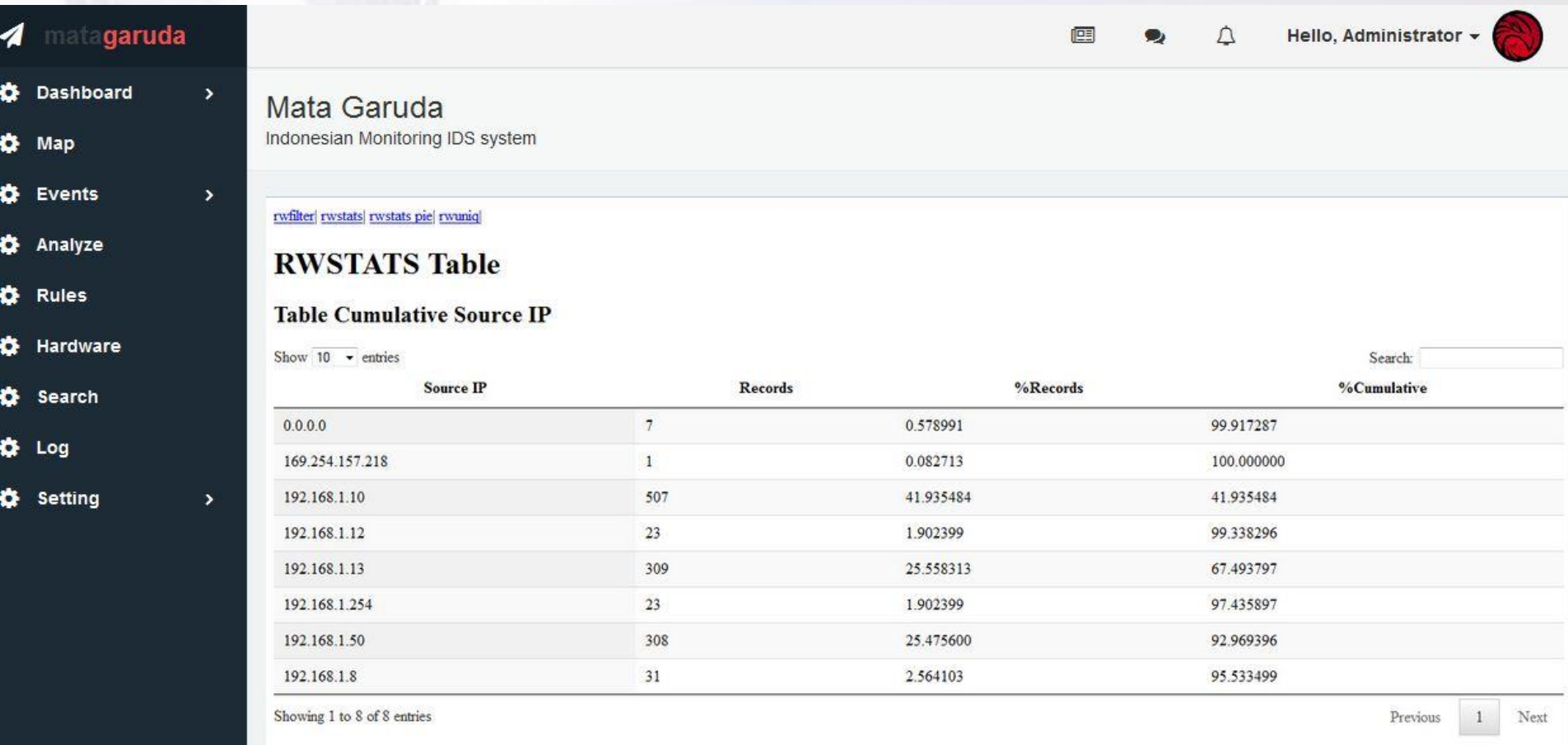
Train data set
from local traffic – packet with **payload**



Incoming packets



See not only the attacking phase – log of packet header



The screenshot displays the Mata Garuda web interface, an Indonesian Monitoring IDS system. The left sidebar contains navigation options: Dashboard, Map, Events, Analyze, Rules, Hardware, Search, Log, and Setting. The main content area shows the 'RWSTATS Table' with a sub-section for 'Table Cumulative Source IP'. A search bar is present at the top right of the table area. The table lists source IP addresses, the number of records, the percentage of records, and the cumulative percentage. The data is as follows:

Source IP	Records	%Records	%Cumulative
0.0.0.0	7	0.578991	99.917287
169.254.157.218	1	0.082713	100.000000
192.168.1.10	507	41.935484	41.935484
192.168.1.12	23	1.902399	99.338296
192.168.1.13	309	25.558313	67.493797
192.168.1.254	23	1.902399	97.435897
192.168.1.50	308	25.475600	92.969396
192.168.1.8	31	2.564103	95.533499

Showing 1 to 8 of 8 entries

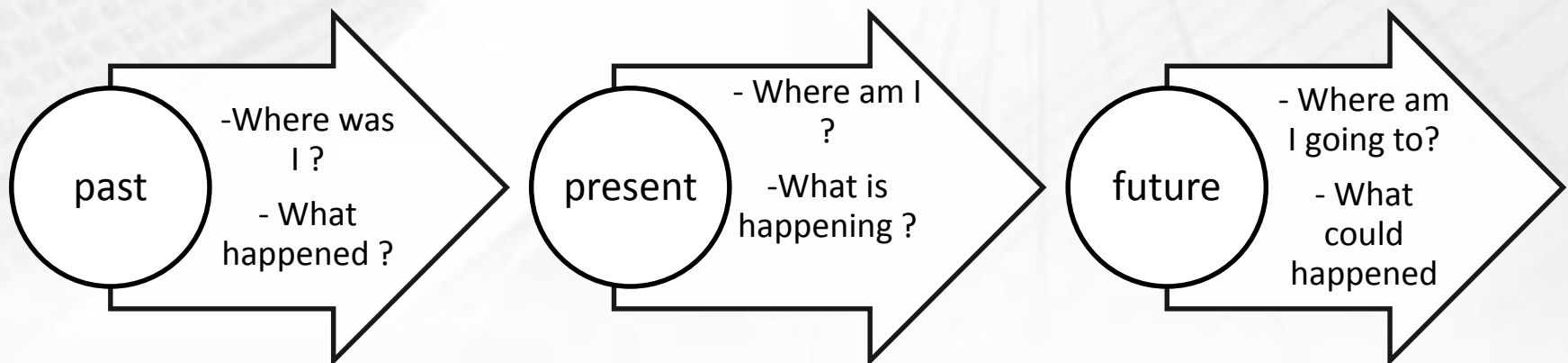
Navigation: Previous 1 Next

Cyber Situational Awareness System

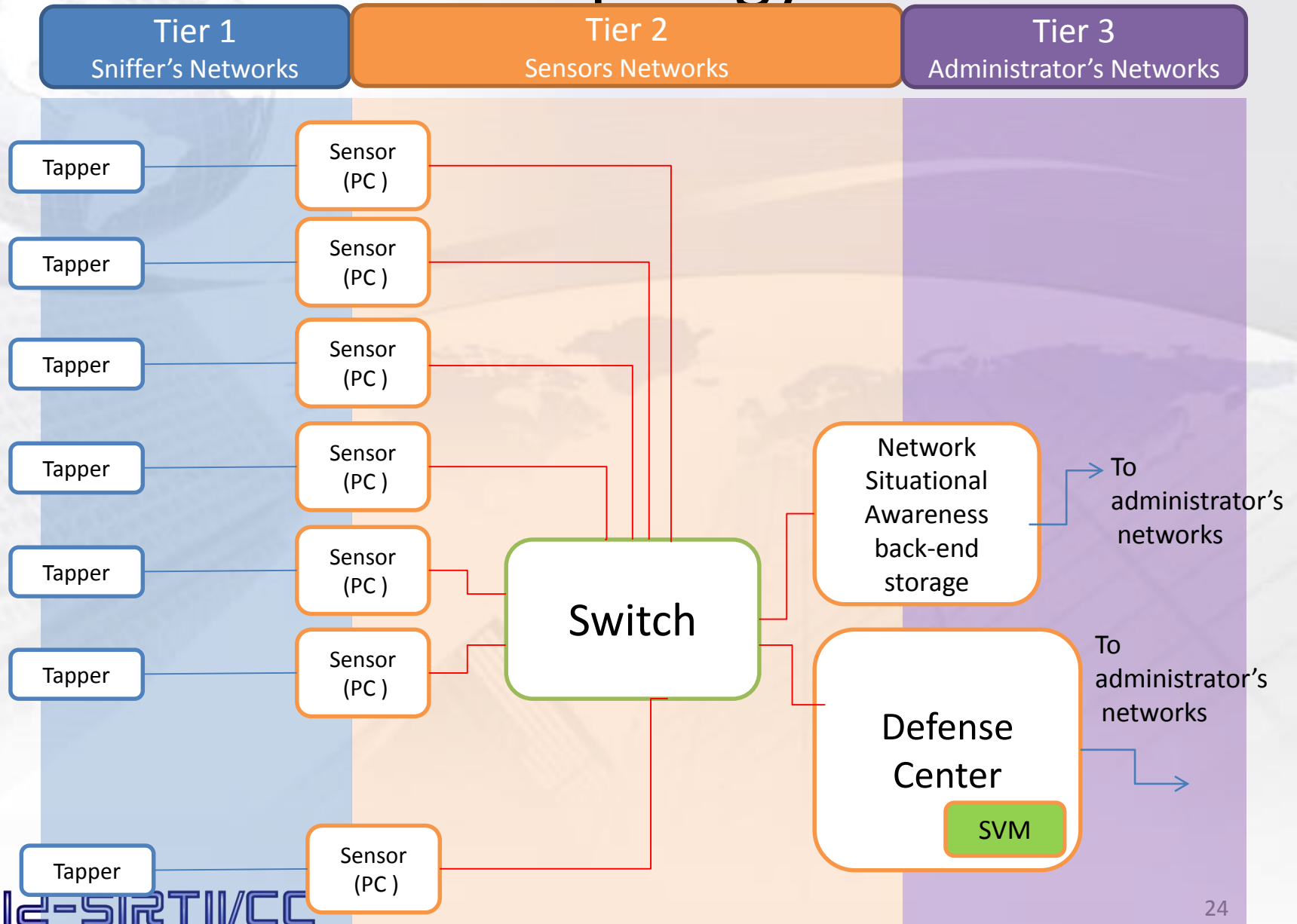
- Packet Header Forensic :

- Before
- Current
- After

} Attacking Phase



The Topology





Thank You

Id-SIRTII/CC

Ravindo Tower 17th Floor

Jalan Kebon Sirih Kav. 75

Central Jakarta, 10340

Phone +62 21 3192 5551

Fax +62 21 3193 5556

Email info@idsirtii.or.id

Website <http://www.idsirtii.or.id>

