Indonesia Honeynet Project

Building the National Honeynet-based Cyber Security Threat Intelligence – Raising the bar on Cyber Situational Awareness

Dr. Charles Lim, Msc., CTIA, CHFI, EDRP, ECSA, ECSP, ECIH, CEH, CEI

Chapter Lead

Telkom University, Bandung, 12 November 2019

AGENDA

- About Me
- Honeynet Project
- Indonesia Honeynet Project (IHP)
- Our Contributions
- Monitoring Statistics
- Early Warning Systems
- Cyber Situational Awareness
- Honeynet-based Threat Sharing Platform
- IHP Workshop & Research Sharing
- Thank You

About Me

Dr. Charles Lim, Msc., CTIA, CHFI, EDRP, ECSA, ECSP, ECIH, CEH, CEI
Researcher – Information Security Research Group and Lecturer
Swiss German University
Charles.lims [at] gmail.com *and* ***charles.lim [at] sgu.ac.id***
http://people.sgu.ac.id/charleslim

Research Interest

Malware, Intrusion Detection, Threats Intelligence, Digital Forensics, Cloud Security

Community

Indonesia Honeynet Project - Chapter Lead
Academy CSIRT – member
Asosiasi Digital Forensik Indonesia - member

Indonesia Honeynet Project

AFDI
ASOSIASI FORENSIK DIGITAL INDONESIA

CSIRT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Honeynet Project Mission

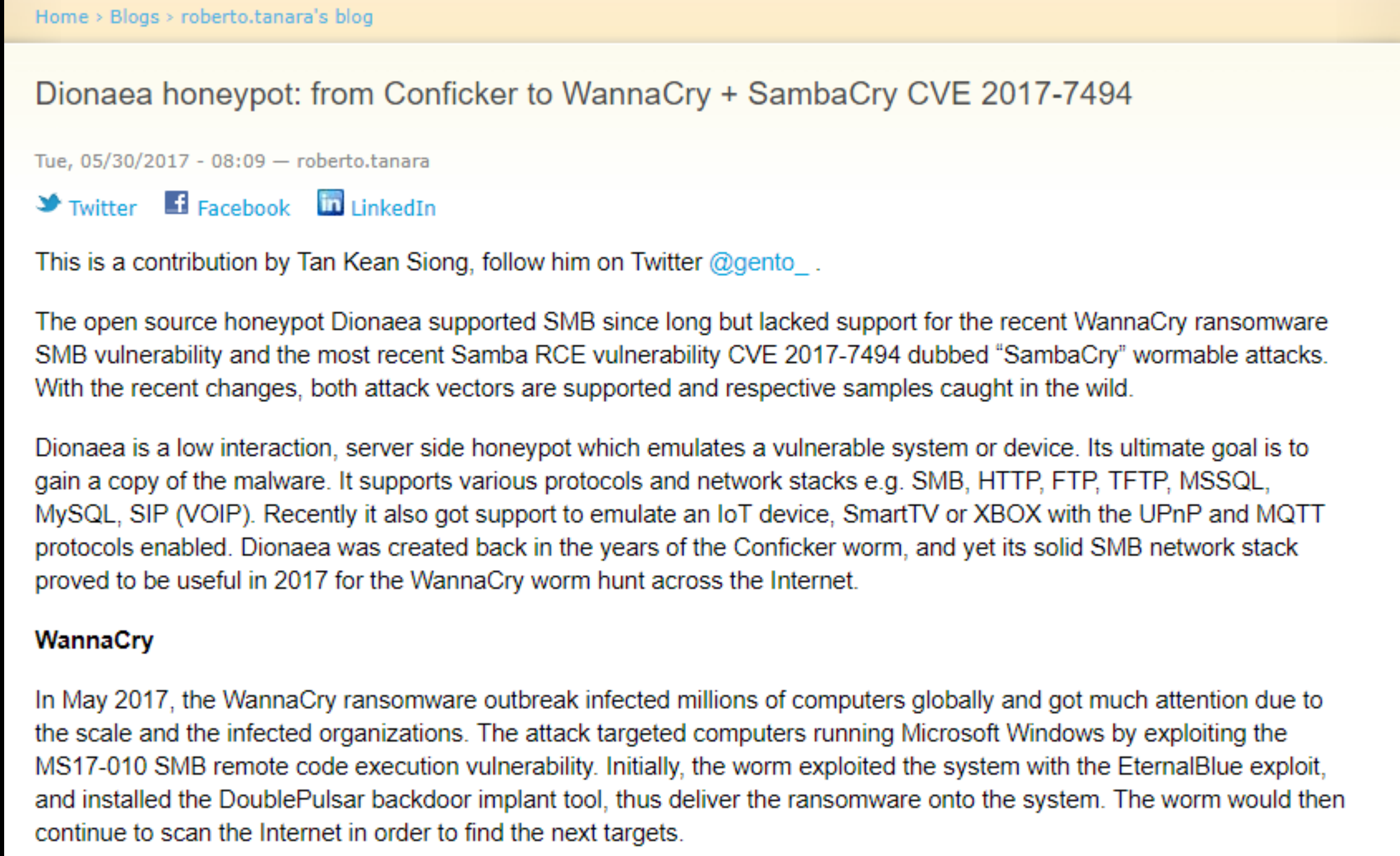
ESTABLISHED

Volunteer open source computer security research organization since 1999 (US 501c3 non-profit)

MISSION

learn the tools, tactics and motives involved in computer and network attacks, and share the lessons learned

Honeynet Project – Know Your Tools



Home › Blogs › roberto.tanara's blog

Dionaea honeypot: from Conficker to WannaCry + SambaCry CVE 2017-7494

Tue, 05/30/2017 - 08:09 — roberto.tanara

Twitter Facebook LinkedIn

This is a contribution by Tan Kean Siong, follow him on Twitter @gento_ .

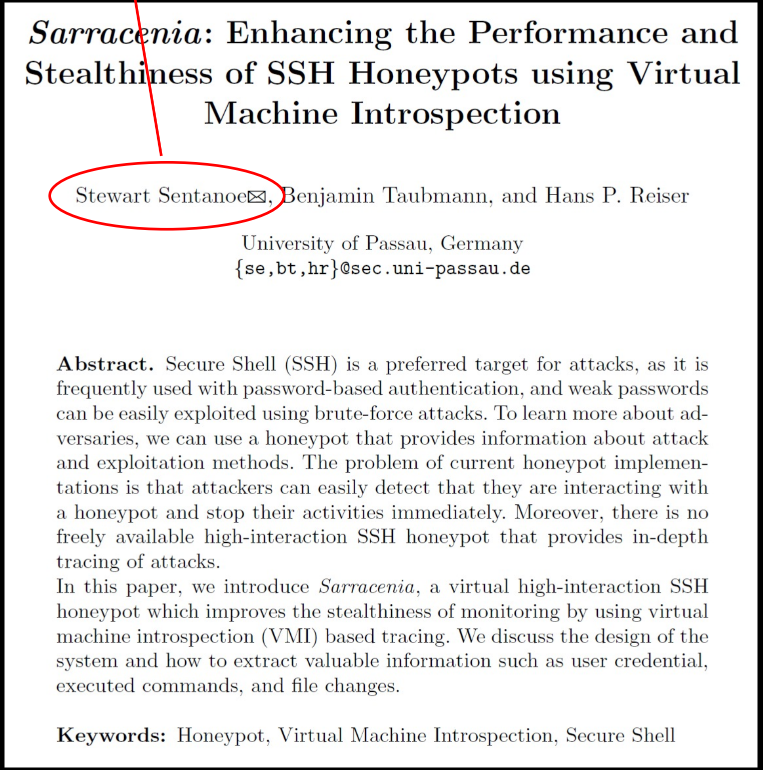
The open source honeypot Dionaea supported SMB since long but lacked support for the recent WannaCry ransomware SMB vulnerability and the most recent Samba RCE vulnerability CVE 2017-7494 dubbed "SambaCry" wormable attacks. With the recent changes, both attack vectors are supported and respective samples caught in the wild.

Dionaea is a low interaction, server side honeypot which emulates a vulnerable system or device. Its ultimate goal is to gain a copy of the malware. It supports various protocols and network stacks e.g. SMB, HTTP, FTP, TFTP, MSSQL, MySQL, SIP (VOIP). Recently it also got support to emulate an IoT device, SmartTV or XBOX with the UPnP and MQTT protocols enabled. Dionaea was created back in the years of the Conficker worm, and yet its solid SMB network stack proved to be useful in 2017 for the WannaCry worm hunt across the Internet.

WannaCry

In May 2017, the WannaCry ransomware outbreak infected millions of computers globally and got much attention due to the scale and the infected organizations. The attack targeted computers running Microsoft Windows by exploiting the MS17-010 SMB remote code execution vulnerability. Initially, the worm exploited the system with the EternalBlue exploit, and installed the DoublePulsar backdoor implant tool, thus deliver the ransomware onto the system. The worm would then continue to scan the Internet in order to find the next targets.

MEMBER IHP



Sarracenia: Enhancing the Performance and Stealthiness of SSH Honeypots using Virtual Machine Introspection

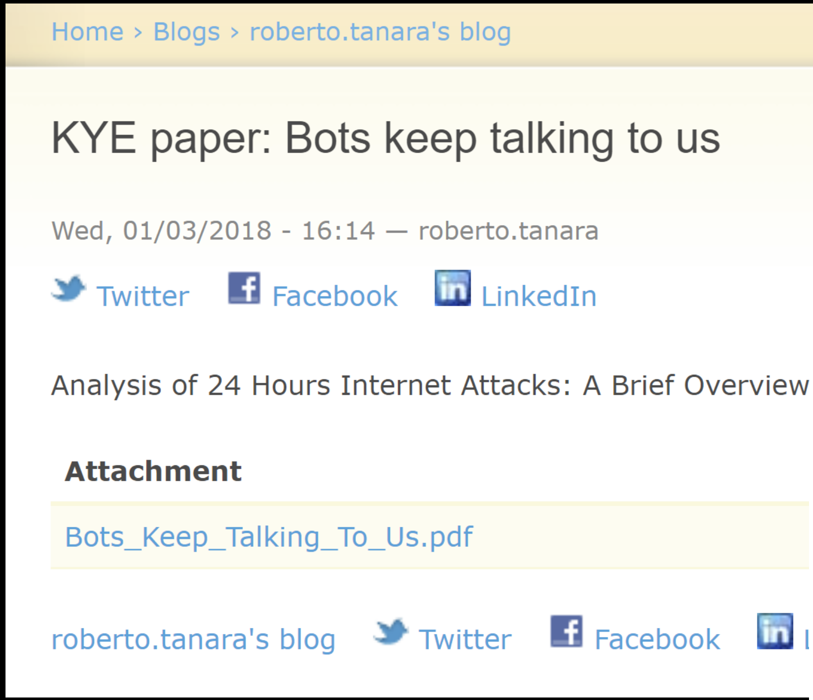
Stewart Sentanoe✉, Benjamin Taubmann, and Hans P. Reiser

University of Passau, Germany
{se,bt,hr}@sec.uni-passau.de

Abstract. Secure Shell (SSH) is a preferred target for attacks, as it is frequently used with password-based authentication, and weak passwords can be easily exploited using brute-force attacks. To learn more about adversaries, we can use a honeypot that provides information about attack and exploitation methods. The problem of current honeypot implementations is that attackers can easily detect that they are interacting with a honeypot and stop their activities immediately. Moreover, there is no freely available high-interaction SSH honeypot that provides in-depth tracing of attacks.
In this paper, we introduce *Sarracenia*, a virtual high-interaction SSH honeypot which improves the stealthiness of monitoring by using virtual machine introspection (VMI) based tracing. We discuss the design of the system and how to extract valuable information such as user credential, executed commands, and file changes.

Keywords: Honeypot, Virtual Machine Introspection, Secure Shell

Honeynet Project – Know Your Enemy



Home › Blogs › roberto.tanara's blog

KYE paper: Bots keep talking to us

Wed, 01/03/2018 - 16:14 — roberto.tanara

Twitter Facebook LinkedIn

Analysis of 24 Hours Internet Attacks: A Brief Overview of Malicious Traffic Targeting Featureless Servers on the

Attachment

Bots_Keep_Talking_To_Us.pdf

roberto.tanara's blog Twitter Facebook

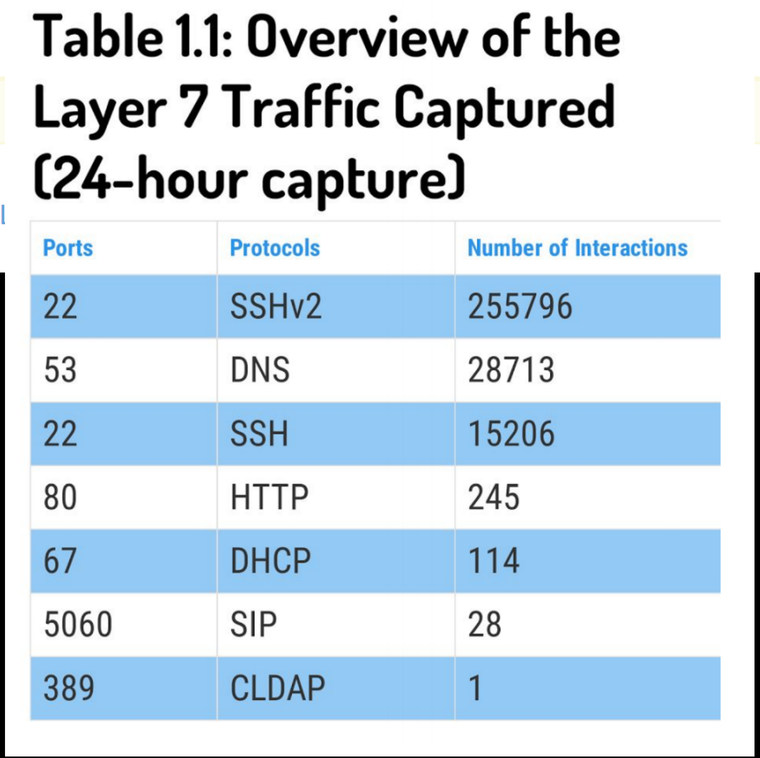


Table 1.1: Overview of the Layer 7 Traffic Captured (24-hour capture)

Ports	Protocols	Number of Interactions
22	SSHv2	255796
53	DNS	28713
22	SSH	15206
80	HTTP	245
67	DHCP	114
5060	SIP	28
389	CLDAP	1

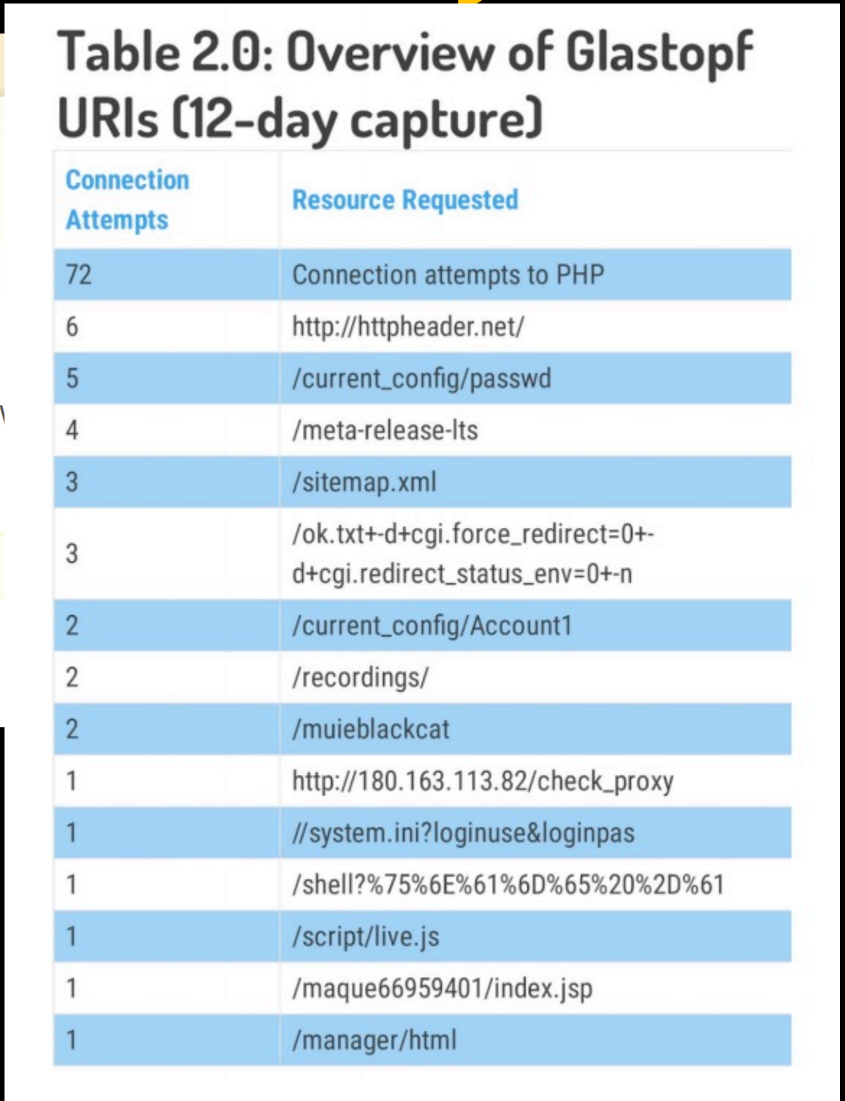


Table 2.0: Overview of Glastopf URIs (12-day capture)

Connection Attempts	Resource Requested
72	Connection attempts to PHP
6	http://httpheader.net/
5	/current_config/passwd
4	/meta-release-lts
3	/sitemap.xml
3	/ok.txt+-d+cgi.force_redirect=0+-d+cgi.redirect_status_env=0+-n
2	/current_config/Account1
2	/recordings/
2	/muieblackcat
1	http://180.163.113.82/check_proxy
1	//system.ini?loginuse&loginpas
1	/shell?%75%6E%61%6D%65%20%2D%61
1	/script/live.js
1	/maque66959401/index.jsp
1	/manager/html

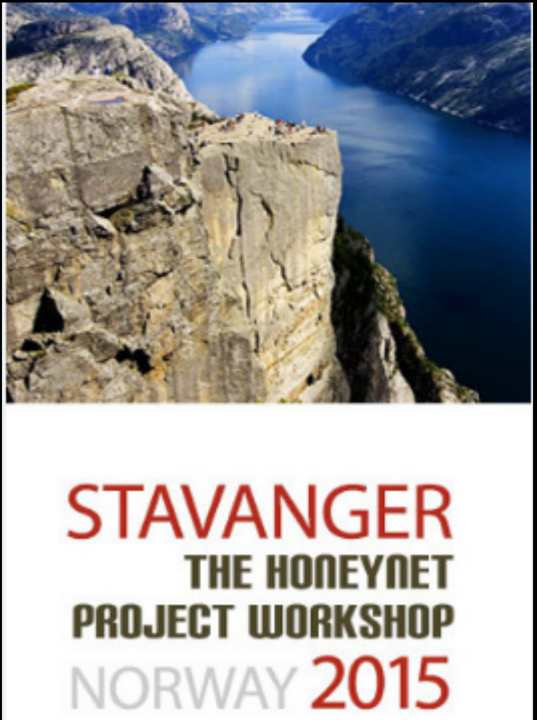
Indonesia Honeynet Project

Honeynet Project Workshop 2012 - 2015

San Francisco 2012

Dubai 2013

Warsaw 2014

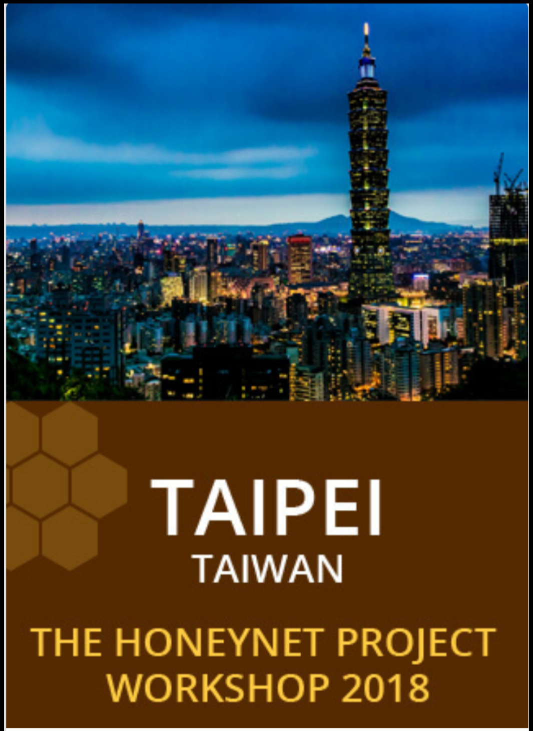


Stavanger 2015

Honeynet Project Workshop 2016 - 2018

San Antonio 2016

Canberra 2017



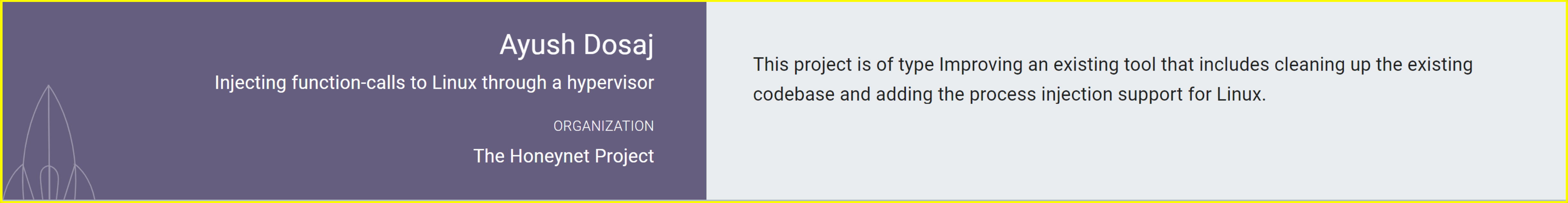
Taipei 2018

Honeynet Project Workshop 2019

The Honeynet Project Annual Workshop 2019

Innsbruck, Austria — July 1st–3rd, 2019

Honeynet Project – 2019 Google Summer of Code



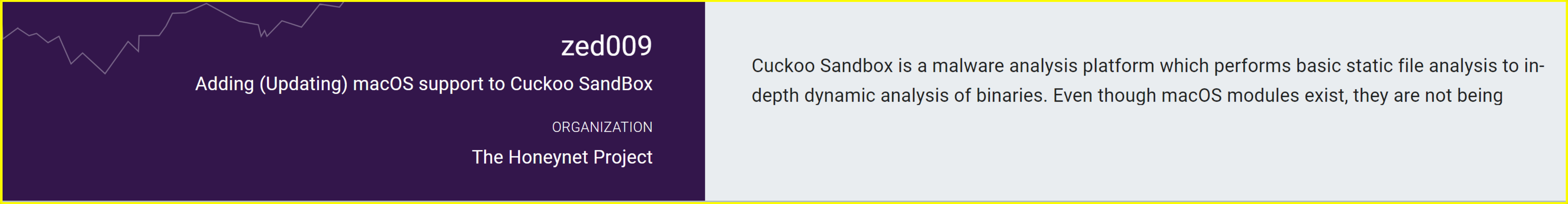
Ayush Dosaj

Injecting function-calls to Linux through a hypervisor

ORGANIZATION

The Honeynet Project

This project is of type Improving an existing tool that includes cleaning up the existing codebase and adding the process injection support for Linux.



zed009

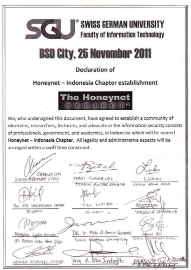
Adding (Updating) macOS support to Cuckoo SandBox

ORGANIZATION

The Honeynet Project

Cuckoo Sandbox is a malware analysis platform which performs basic static file analysis to in-depth dynamic analysis of binaries. Even though macOS modules exist, they are not being

Indonesia Honeynet Project (IHP)



SWISS GERMAN UNIVERSITY
Faculty of Information Technology

BSD City, 25 November 2011

Declaration of

Honeynet – Indonesia Chapter establishment

The Honeynet PROJECT®

We, who undersigned this document, have agreed to establish a community of observers, researchers, lecturers, and advocate in the information security consists of professionals, government, and academics, in Indonesia which will be named **Honeynet – Indonesia Chapter**. All legality and administrative aspects will be arranged within a swift time constraint.

CHARLES LIM
SWISS GERMAN UNIV

MADI SYAHRIAL
STMIK ANTAR BANGSA

LUKAS
UNIKA ATMA JAYA

DWI ADE HANDAYANI CAPAH
ID-SIRTII

Tita Latifah
ID-SIRTII

MUSTAFA
UNISSULA SEMARANG

Margaret Lydia Kewalo
UPT Puskom Unika Atma Jaya

DR. Ir. Moh. A. Amin Soetomo
Swiss German University

Edwin Adi
BINUS INTERNATIONAL

HOGAN KUSNADI, CISSP

Prof. R. Eko Indrajit

MAKSUDI TW. KUSUMO
PERBANAS

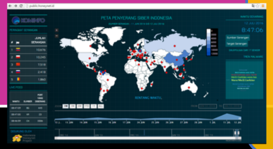
2011

- 15 people signed petition to establish Indonesia Chapter
- First Malware Analysis workshop for students
- First International Presentation @SecureAsia

2012-2016

- Seminar and Workshops funded by KOMINFO
- More than 700 participants over 6 cities
- Grown into 5 key research areas
- Indonesia Honeynet map become available to public

IHPCON 2017
INDONESIA HONEYNET PROJECT CONFERENCE



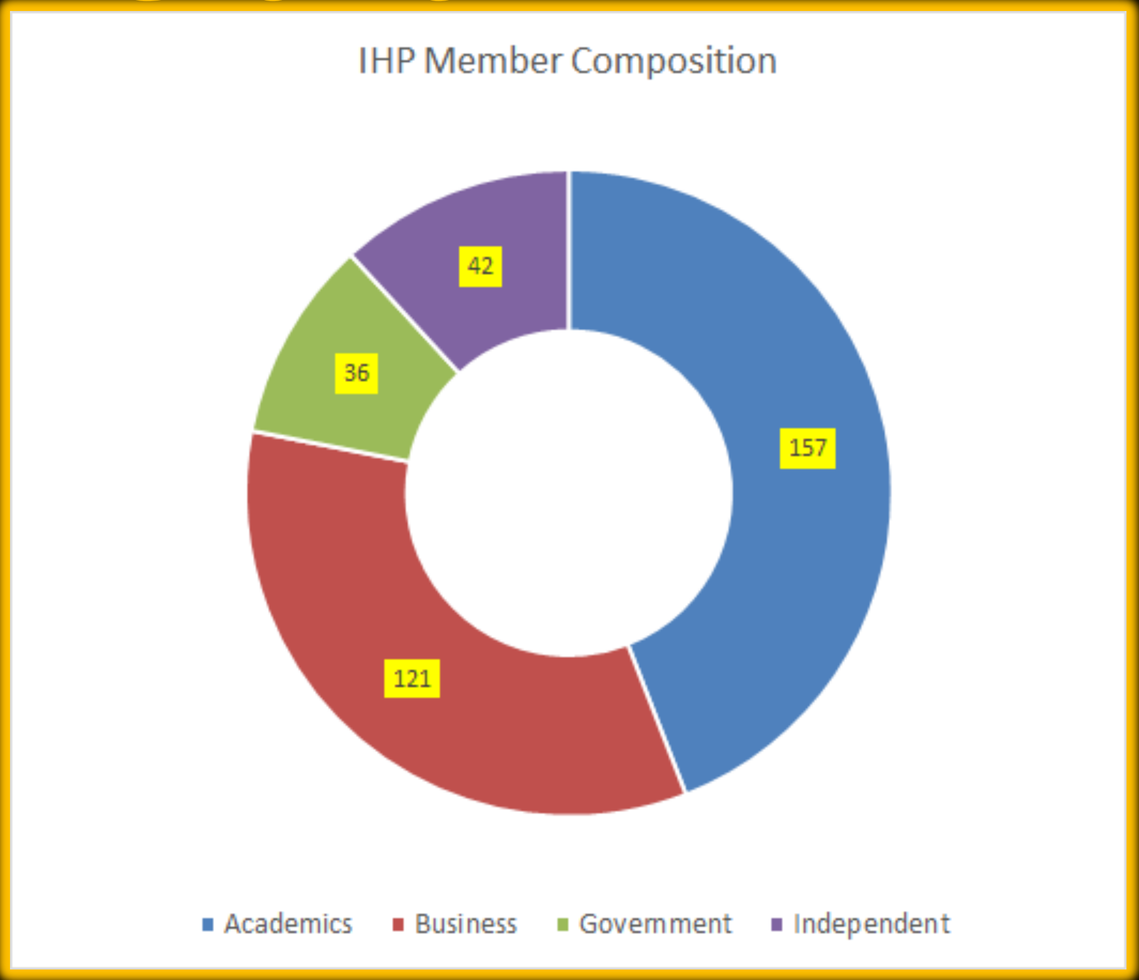
#	JUMLAH SERANGAN
1	10,676
2	10,245
3	7,518
4	2,418
5	1,860

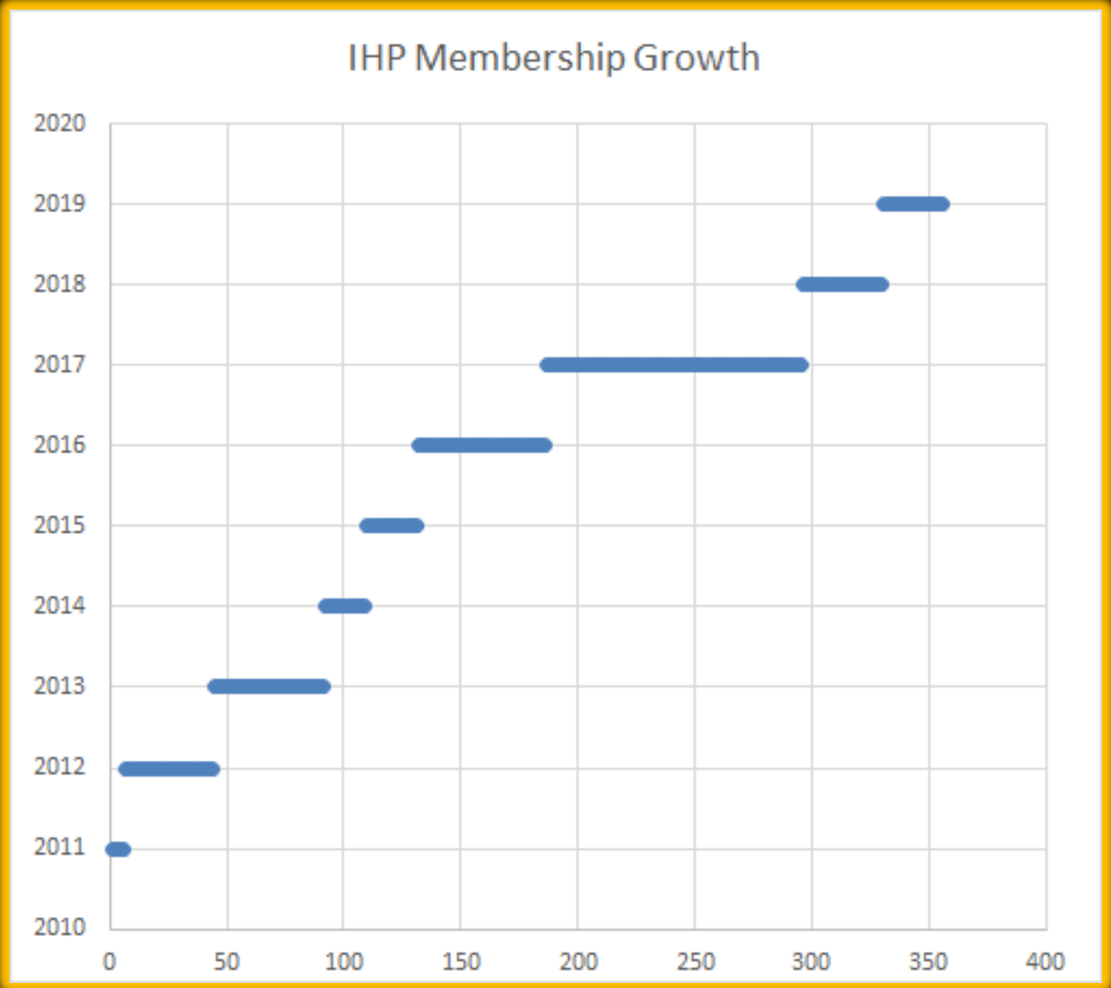
2017

- More than 350+ members and growing
- More than 21 honeypots installed in 6 provinces
- Close to 3100+ unique malware samples captured

Indonesia Honeynet Project

IHP Members – Composition & Growth





Indonesia Honeynet Project

IHP Activities

KOPDAR

- Half day
- Members Only
- Research-oriented
- Every 1-2 months

Workshop

- One Day
- Public
- Sponsorship
- Sharing Knowledge
- Every 1-2 months

Seminar

- One Day
- Public
- Sponsorship
- Sharing and Update
- Every 3-6 months

IHPCON

- 2-4 Days
- Public
- Sponsorship
- Exchange and Update
- Yearly

Honeynet Seminar and Workshop

Masuk
Seminar & Workshop
Peningkatan Cyber Situational Awareness
dengan Memanfaatkan Sistem Deteksi Dini Nasional
PEMBICARA
Didukung oleh:
amandata
HUAWEI

10 September 2019 | Depok, Indonesia

Honeynet Seminar and Workshop

23-24 October 2018 | Banda Aceh, Indonesia

24 November 2018 | Tangerang, Indonesia

Indonesia Honeynet Project

KOPDAR 2017

KOPI DARAT | January 2017 | Jakarta, Indonesia

IHPCON 2017 – C Level Breakfast

IHPCON 2017 | 5-6 September 2017 | Jakarta, Indonesia

Indonesia Honeynet Project

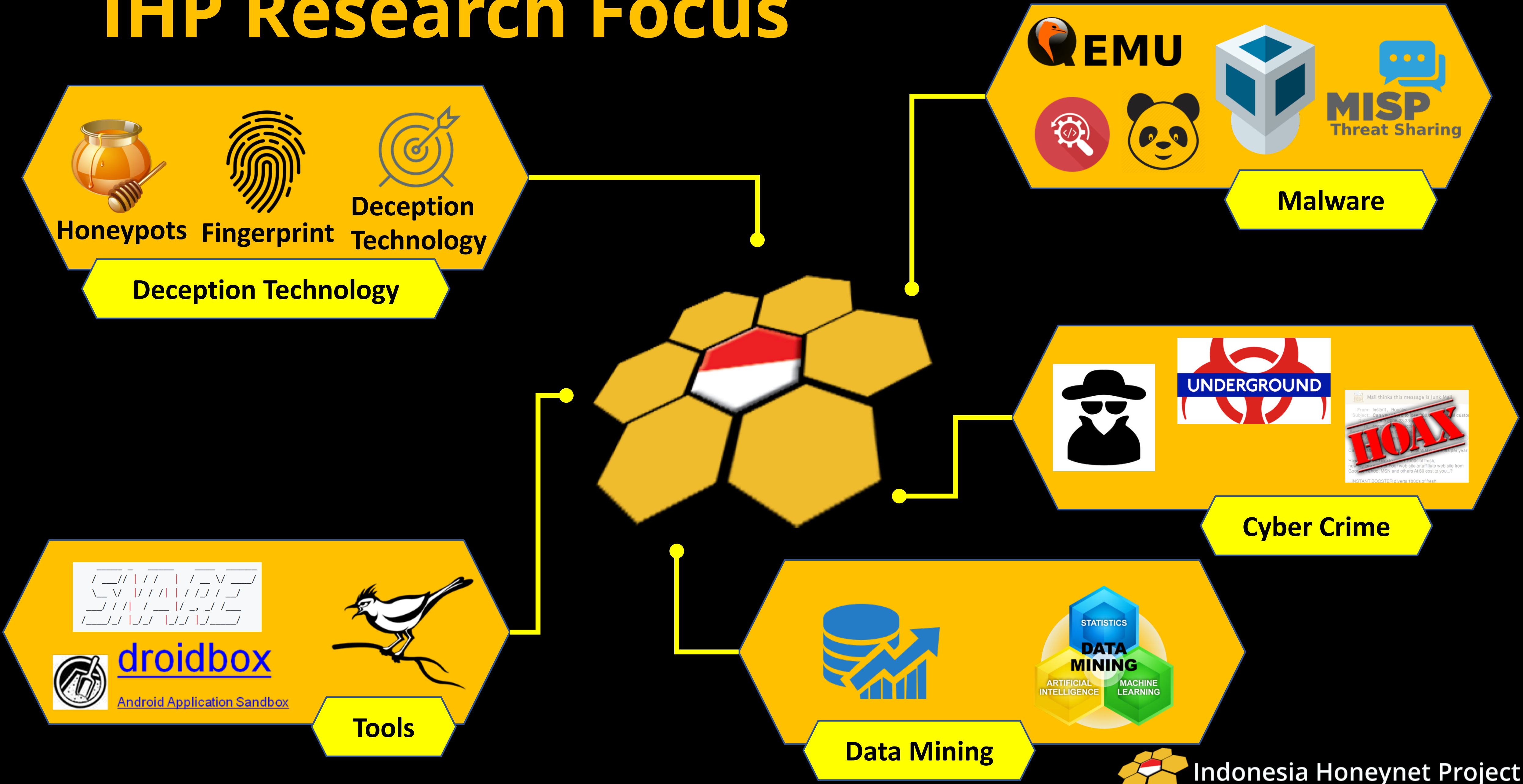
IHPCON 2017 - Conference

Cyber Crime
IHPCON 2017
INDONESIA HONEYNET PROJECT CONFERENCE
aruba
Tugas dan Fungsi Id-GovCSIRT

IHPCON 2017 | 5-6 September 2017 | Jakarta, Indonesia

Indonesia Honeynet Project

IHP Research Focus



Honeypots

Fingerprint

Deception Technology

Deception Technology

Malware

Cyber Crime

Tools

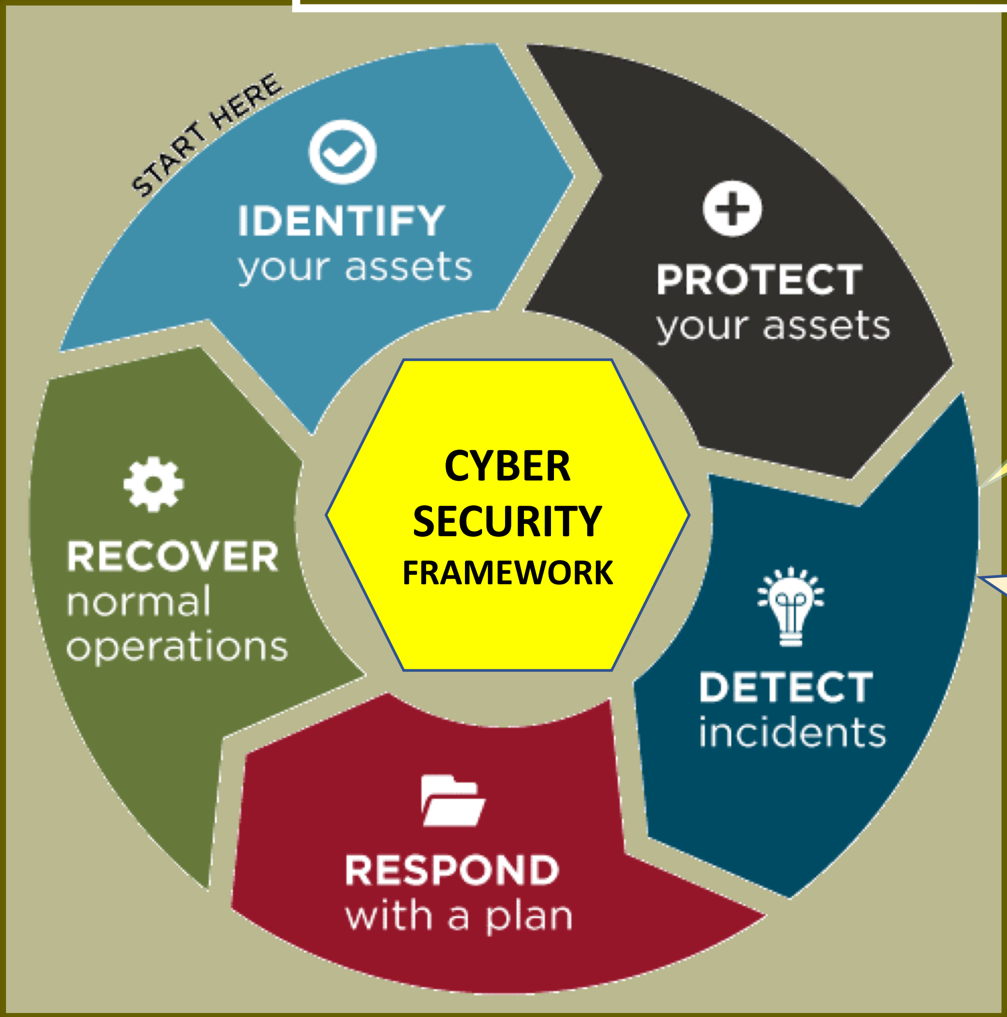
Data Mining

CYBER SECURITY

RESEARCH AND DEVELOPMENT

VALUE-ADDED SERVICES

BUSINESS AND GOV SERVICES



RESEARCH FOCUS

DECEPTION TECH

TOOLS

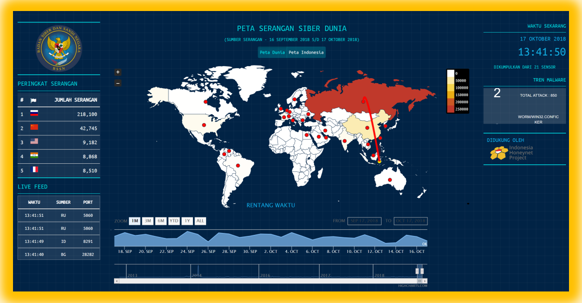
DATA MINING

CYBER CRIME

MALWARE

IHP CONTRIBUTIONS

Indonesia Honeynet Project



THREATS MAP

MALICIOUS DOMAINS

ject

IHP Partners

- SGU®
- INFORMATICS & BUSINESS INSTITUTE DARMAJAYA
- STIKOM BALI
- UNIVERSITAS SYIAH KUALA
- ITS Institut Teknologi Sepuluh Nopember
- UNIVERSITAS ISLAM SULTAN AGUNG UNISSULA
- UNIVERSITAS MUHAMMADIYAH MALANG
- UNIVERSITAS ISLAM INDONESIA
- ATMA JAYA
- Universitas Bina Darma

- Id-SIRTII
- EZ.net.id the Internet Service Provider
- id.cert
- CBN
- LayerSpeed
- netciti

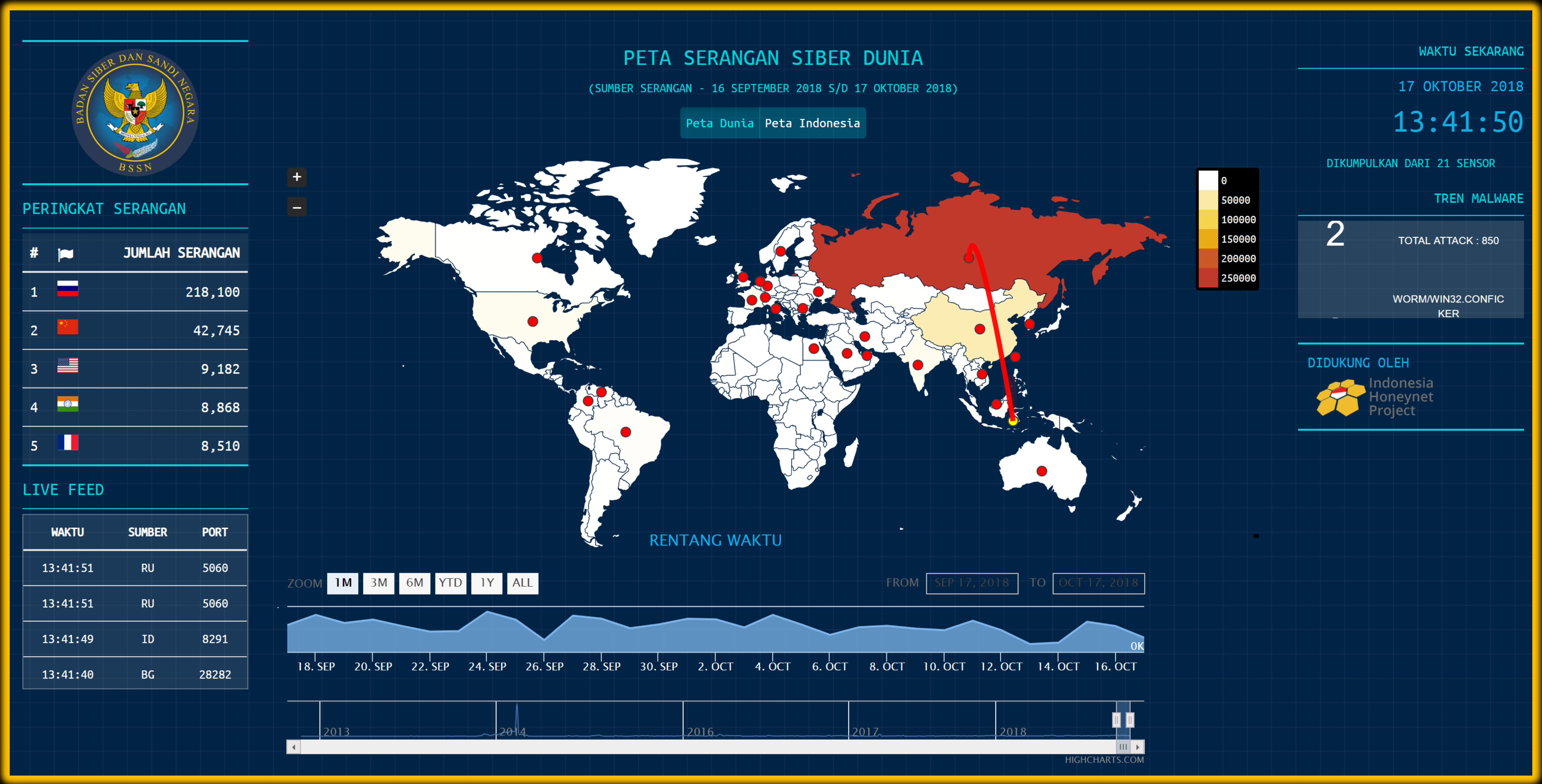
- BPPT
- KOMINFO
- BADAN SIBER DAN SANDI NEGARA BSSN
- KEMENTERIAN PERTAHANAN REPUBLIK INDONESIA

- COMPUTER SECURITY INCIDENT RESPONSE TEAM CSIRT
- EC-Council
- AFDI ASOSIASI FORENSIK DIGITAL INDONESIA
- OWASP Open Web Application Security Project
- ISACA® Trust in, and value from, information systems
- (ISC)²

- datacomm
- SOLUSI AM
- aruba a Hewlett Packard Enterprise company
- XecureIT "Your IT Security, Our Passion"
- RSA®
- ADVANCED TECHNOLOGIES PACIFIC
- amandata
- Course-Net Empowering IT People
- A10®
- paloalto NETWORKS®

Indonesia Honeynet Project

Our Contribution



BADAN SIBER DAN SANDI NEGARA
BSSN

PETA SERANGAN SIBER DUNIA

(SUMBER SERANGAN - 16 SEPTEMBER 2018 S/D 17 OKTOBER 2018)

Peta Dunia | Peta Indonesia

WAKTU SEKARANG

17 OKTOBER 2018

13:41:50

DIKUMPULKAN DARI 21 SENSOR

TREN MALWARE

2

TOTAL ATTACK : 850

WORM/WIN32.CONFICKER

DIDUKUNG OLEH

Indonesia Honeynet Project

PERINGKAT SERANGAN

#	🏳	JUMLAH SERANGAN
1	🇷🇺	218,100
2	🇨🇳	42,745
3	🇺🇸	9,182
4	🇮🇳	8,868
5	🇫🇷	8,510

LIVE FEED

WAKTU	SUMBER	PORT
13:41:51	RU	5060
13:41:51	RU	5060
13:41:49	ID	8291
13:41:40	BG	28282

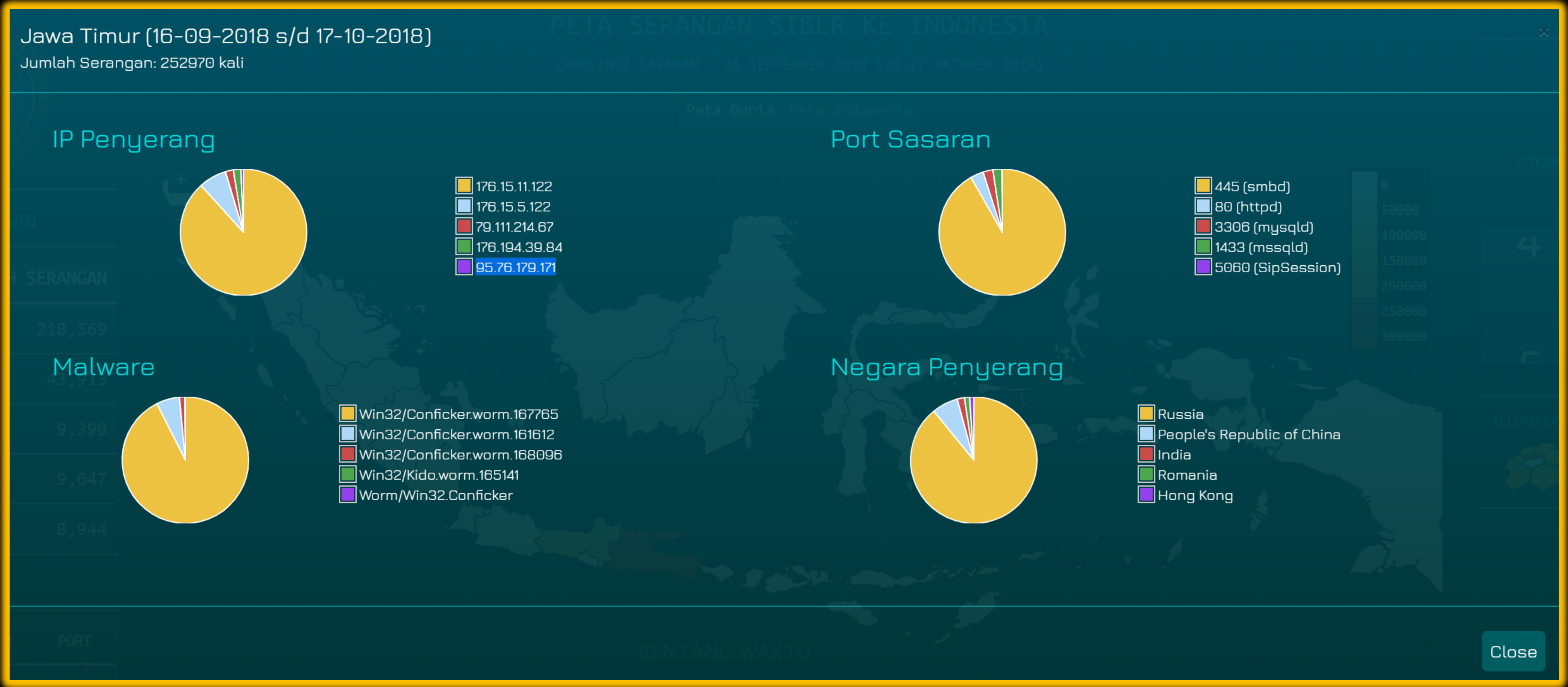
RENTANG WAKTU

ZOOM 1M 3M 6M YTD 1Y ALL

FROM SEP 17, 2018 TO OCT 17, 2018

Honeynet Map Portal untuk public: http://honeynet.bssn.go.id

Indonesia Honeynet Project



Jawa Timur (16-09-2018 s/d 17-10-2018)

Jumlah Serangan: 252970 kali

IP Penyerang

- 🟨 176.15.11.122
- 🟦 176.15.5.122
- 🟥 79.111.214.67
- 🟩 176.194.39.84
- 🟪 95.76.179.171

Port Sasaran

- 🟨 445 (smbd)
- 🟦 80 (httpd)
- 🟥 3306 (mysqld)
- 🟩 1433 (mssqld)
- 🟪 5060 (SipSession)

Malware

- 🟨 Win32/Conficker.worm.167765
- 🟦 Win32/Conficker.worm.161612
- 🟥 Win32/Conficker.worm.168096
- 🟩 Win32/Kido.worm.165141
- 🟪 Worm/Win32.Conficker

Negara Penyerang

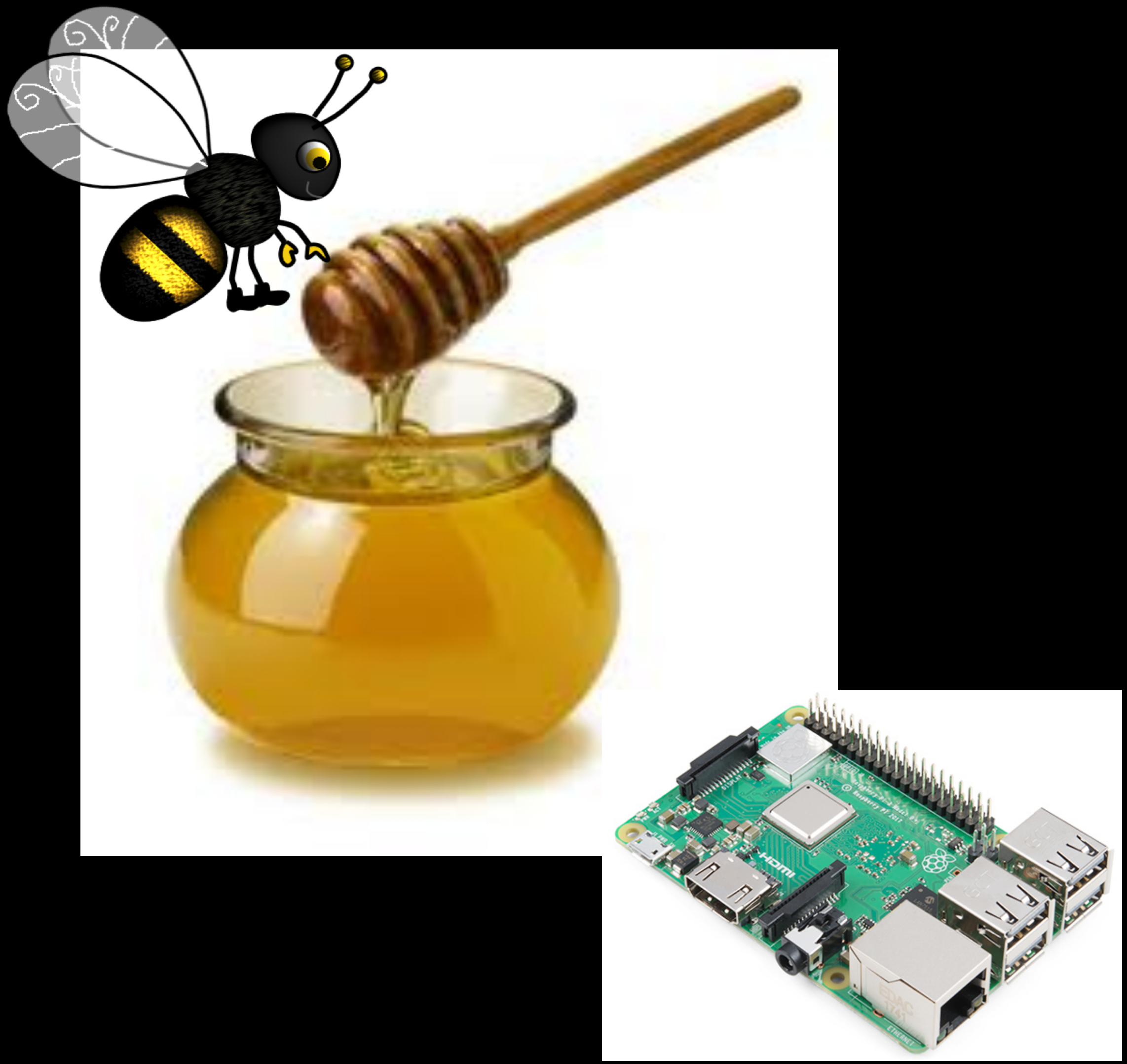
- 🟨 Russia
- 🟦 People's Republic of China
- 🟥 India
- 🟩 Romania
- 🟪 Hong Kong

Honeynet Map Portal untuk publik

http://public.honeynet.id

Indonesia Honeynet Project

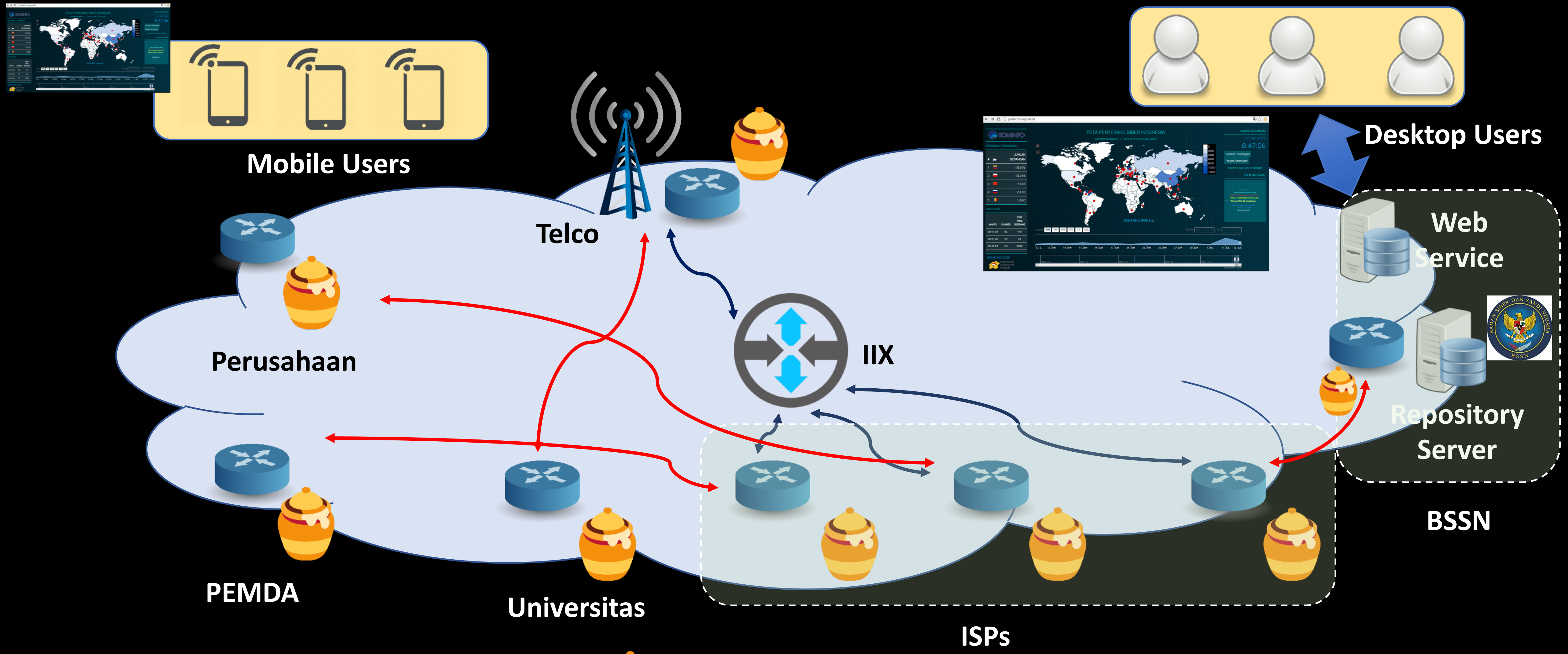
Honeypot



Honeypot adalah sistem keamanan (dibuat mirip dengan sistem sebenarnya) yang sengaja dirancang rentan untuk diserang.

Honeynet adalah sistem yang terdiri dari kumpulan honeypot, yang sengaja dibuat mirip dengan sever produksi.

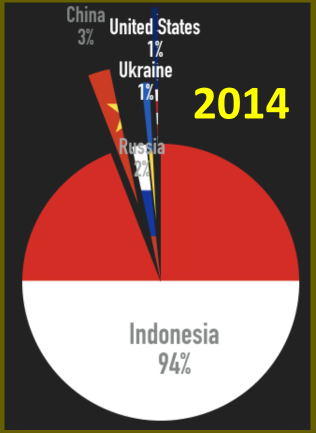
National Honeynet Infrastructure

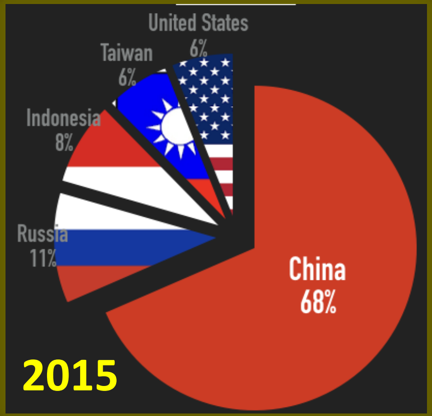


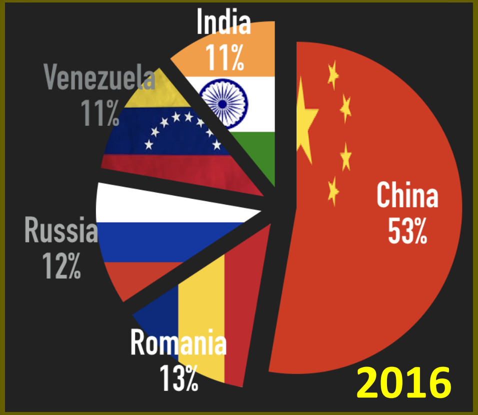
Honeypot
Installed on unused IPs

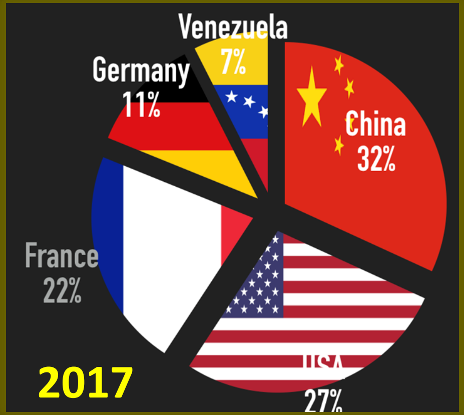
Indonesia Honeynet Project

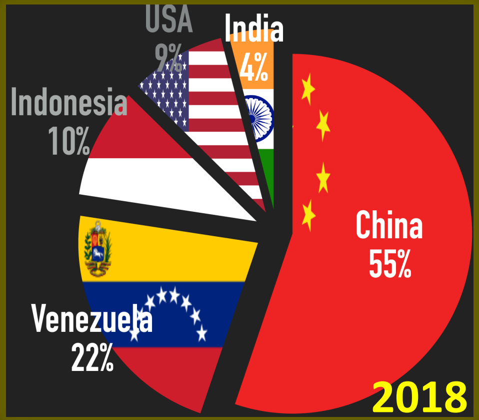
Monitoring Stats

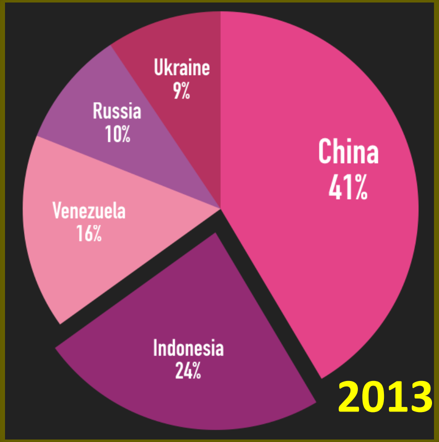


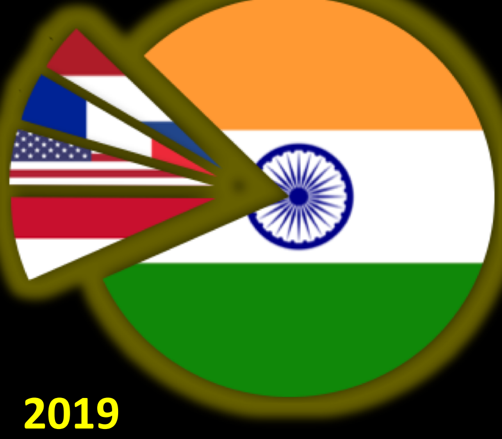


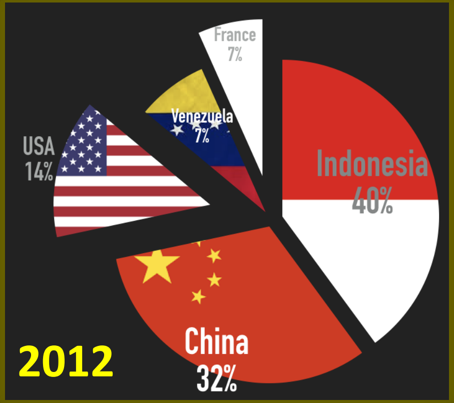












3.101 UNIQUE MALWARE
ATTACK SUMATRA, JAVA, AND BALI

33.856.720
Connection Attacks

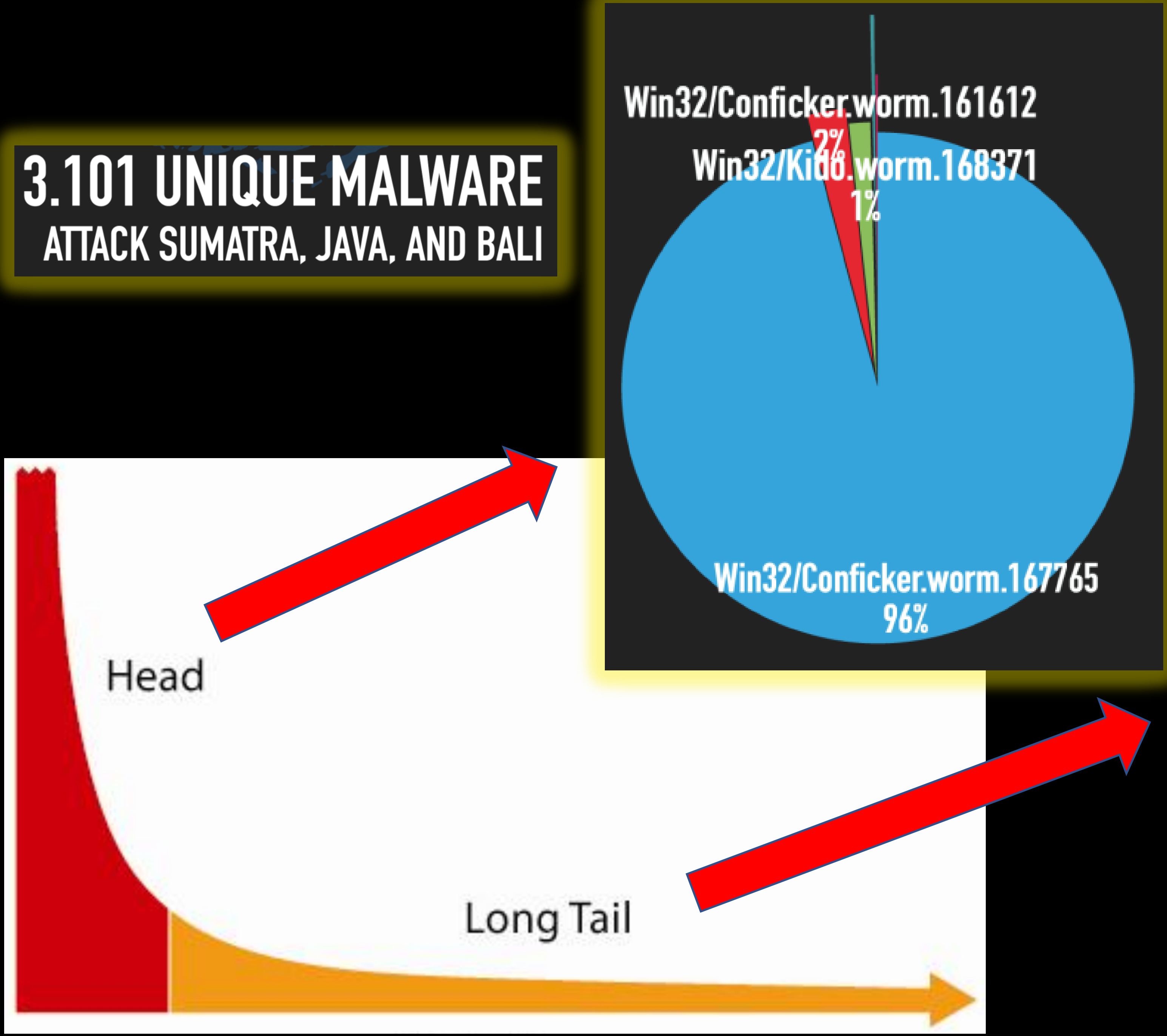
21 Honeypots
In Sumatra, Jawa & Bali

Indonesia Honeynet Project

Malware Stats (2019)

3.101 UNIQUE MALWARE

ATTACK SUMATRA, JAVA, AND BALI



Malware	Hit
Win-Trojan/Agent.33128.B	98
Win-Trojan/Agent.22458	13
Win-Trojan/Starman.Gen	1
Worm/Win32.IRCBot	1

Early Warning System

Early Warning System Components

Risk Knowledge

Monitoring System

Signals

Response

RISKS

Factors that lead to higher risks

Monitoring

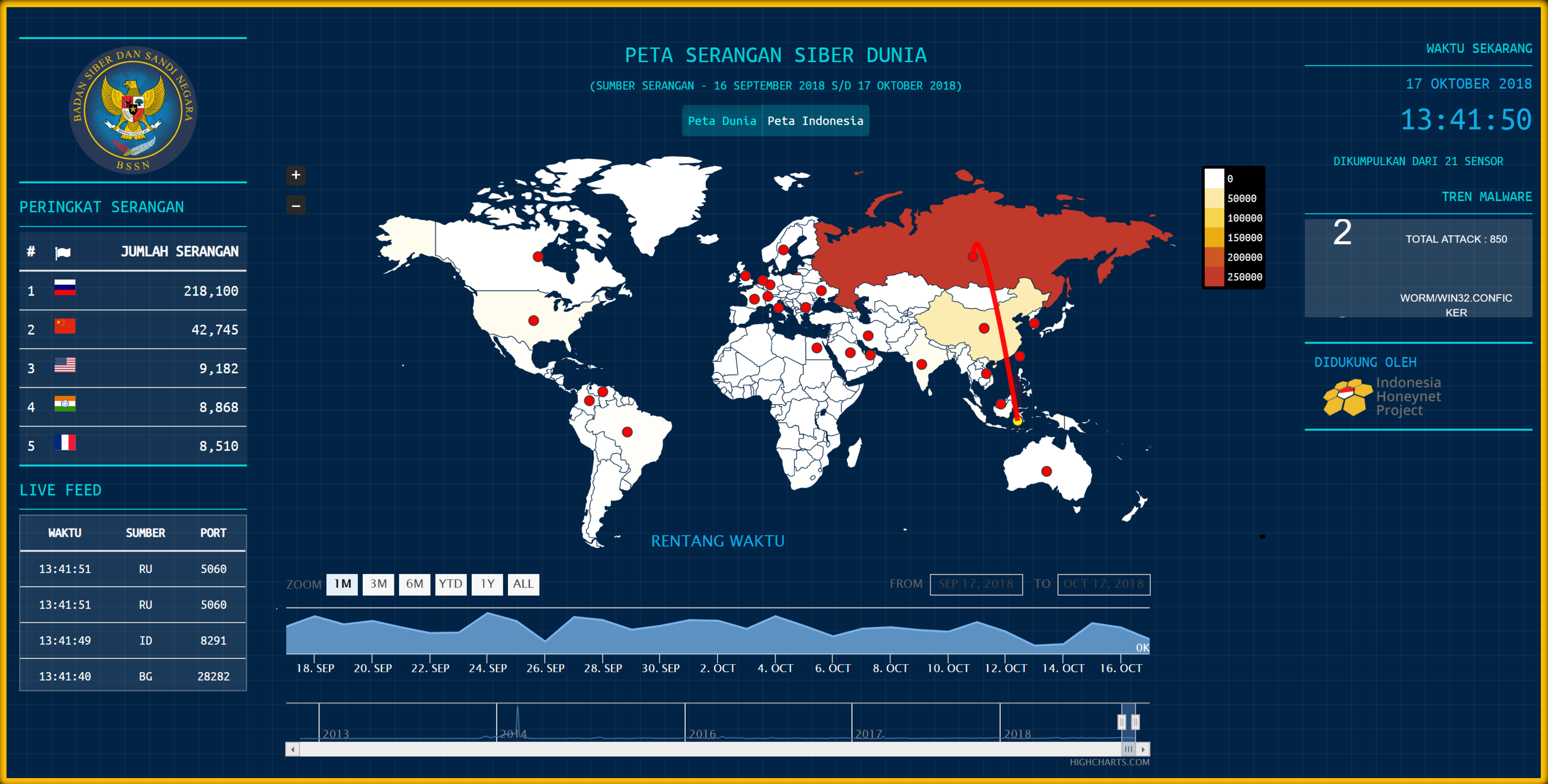
Monitoring sensors for meaningful changes

Signals

What signals provide me the best insight

Response

What actions will be taken



PETA SERANGAN SIBER DUNIA

(SUMBER SERANGAN - 16 SEPTEMBER 2018 S/D 17 OKTOBER 2018)

Peta Dunia | Peta Indonesia

PERINGKAT SERANGAN

#	🏳	JUMLAH SERANGAN
1	🇷🇺	218,100
2	🇨🇳	42,745
3	🇺🇸	9,182
4	🇮🇳	8,868
5	🇫🇷	8,510

LIVE FEED

WAKTU	SUMBER	PORT
13:41:51	RU	5060
13:41:51	RU	5060
13:41:49	ID	8291
13:41:40	BG	28282

WAKTU SEKARANG

17 OKTOBER 2018

13:41:50

DIKUMPULKAN DARI 21 SENSOR

TREN MALWARE

2

TOTAL ATTACK : 850

WORM/WIN32.CONFICKER

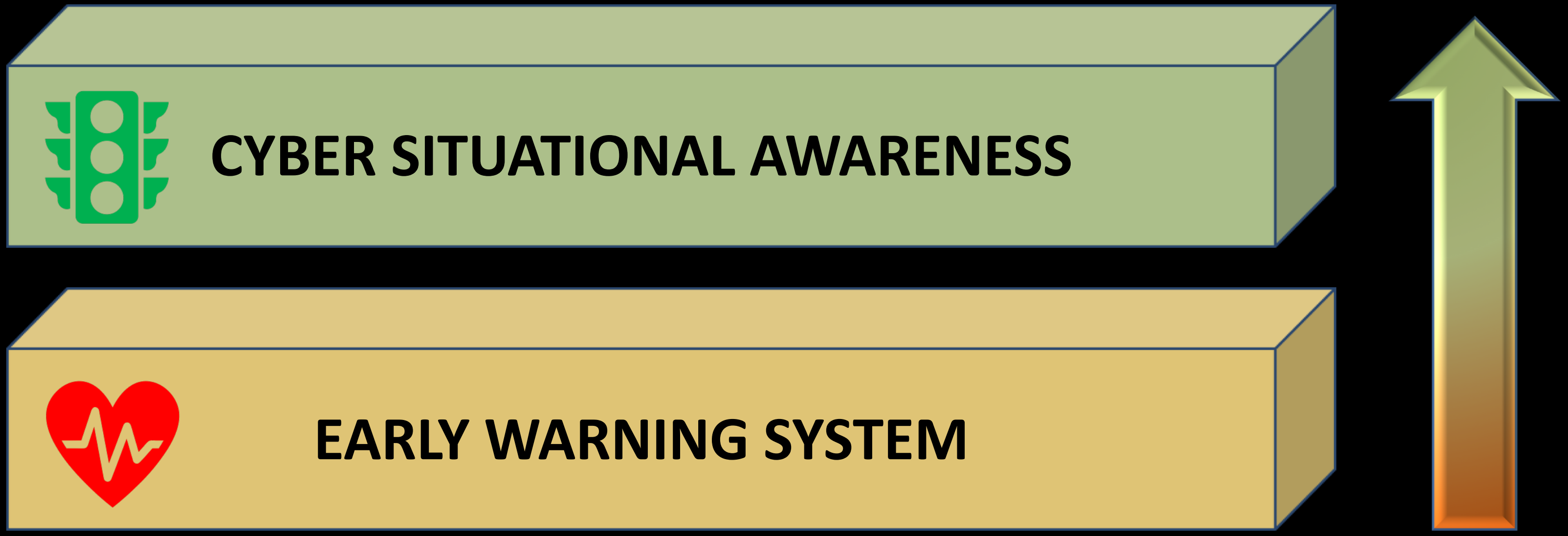
DIDUKUNG OLEH

Indonesia Honeynet Project

Honeynet Map Portal untuk public: http://honeynet.bssn.go.id

Indonesia Honeynet Project

From Early Warning System To Cyber Security Situational Awareness

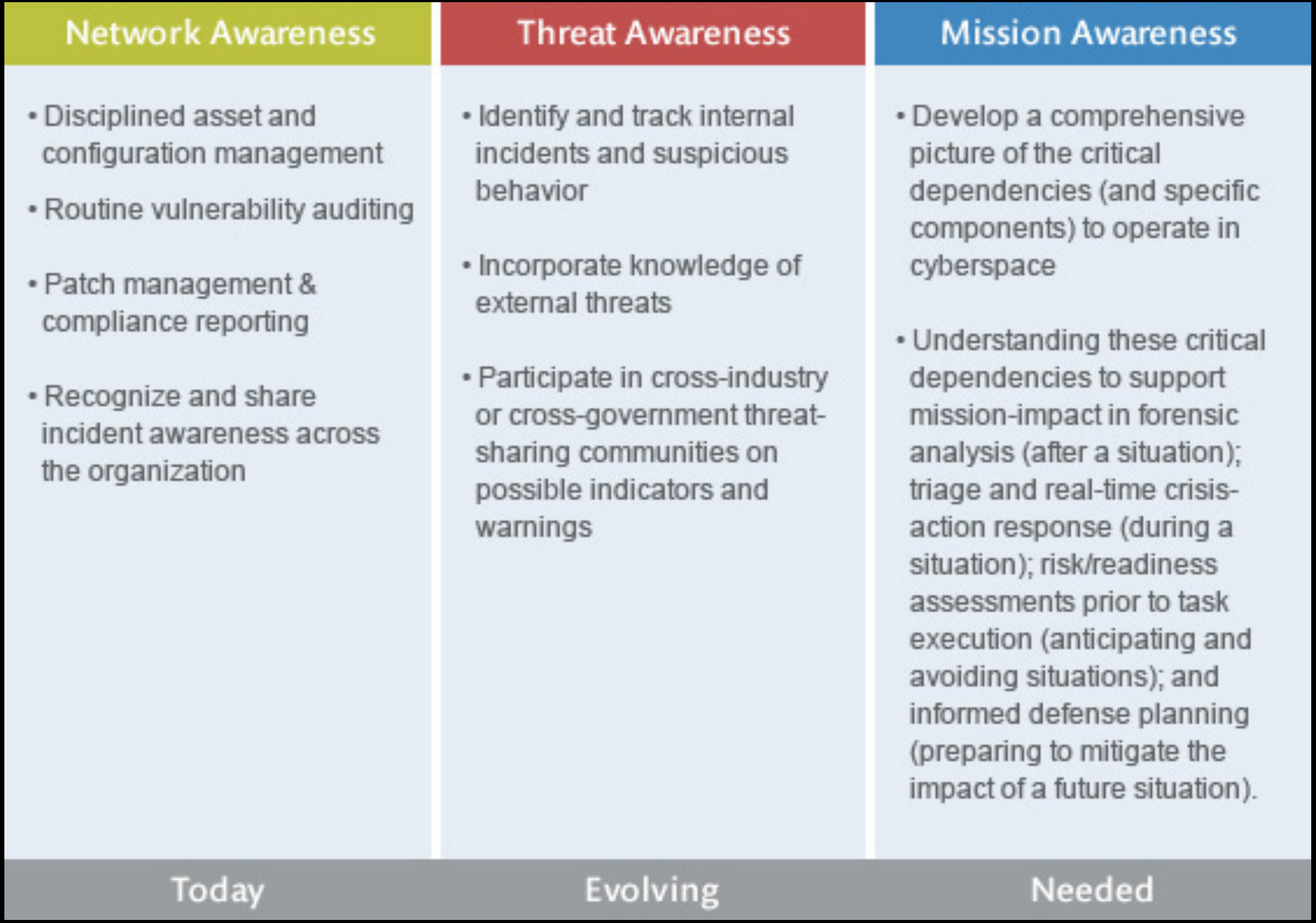


CYBER SITUATIONAL AWARENESS

EARLY WARNING SYSTEM

Cyber Situational Awareness

- Do we know our **assets**?
- Do we know our **security threats**?
- Do we have a **holistic** view of our defense on these assets?

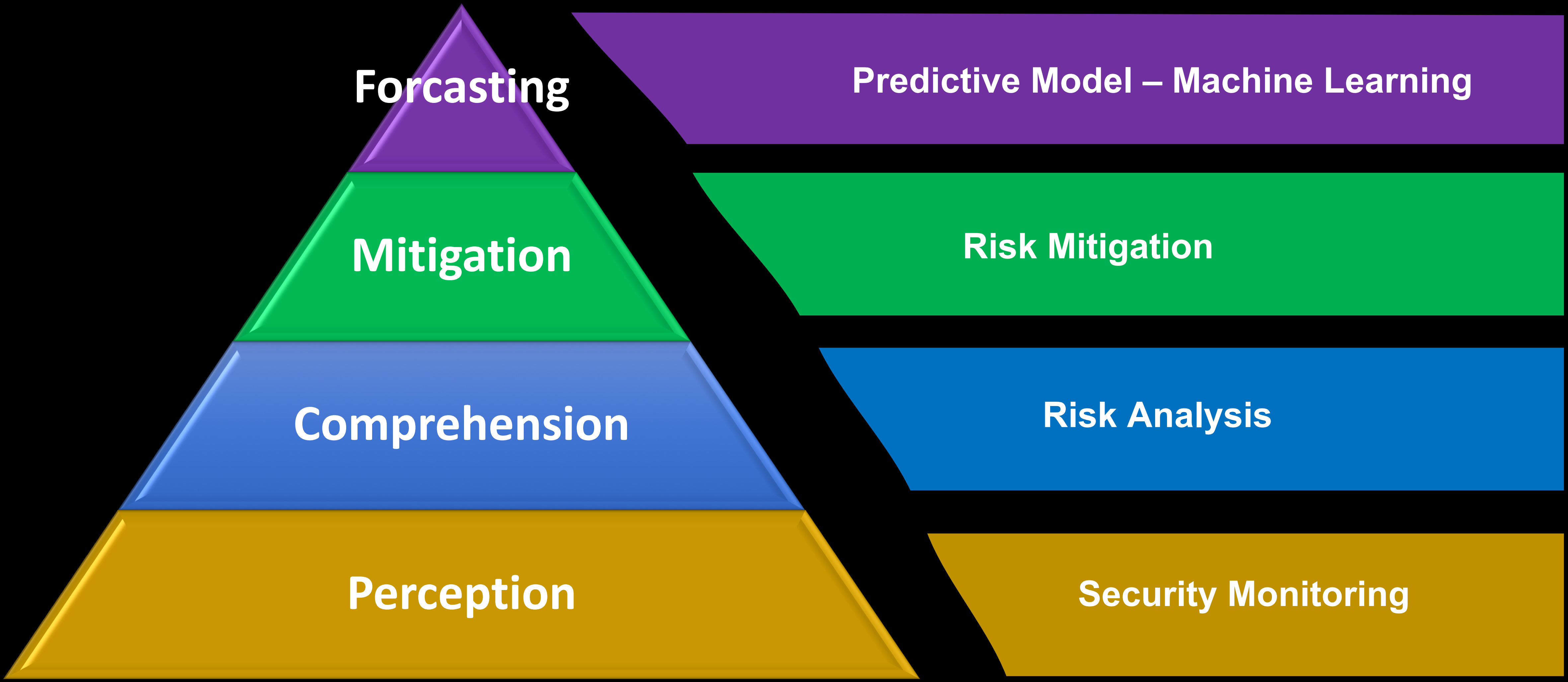


Network Awareness	Threat Awareness	Mission Awareness
• Disciplined asset and configuration management • Routine vulnerability auditing • Patch management & compliance reporting • Recognize and share incident awareness across the organization	• Identify and track internal incidents and suspicious behavior • Incorporate knowledge of external threats • Participate in cross-industry or cross-government threat-sharing communities on possible indicators and warnings	• Develop a comprehensive picture of the critical dependencies (and specific components) to operate in cyberspace • Understanding these critical dependencies to support mission-impact in forensic analysis (after a situation); triage and real-time crisis-action response (during a situation); risk/readiness assessments prior to task execution (anticipating and avoiding situations); and informed defense planning (preparing to mitigate the impact of a future situation).
Today	Evolving	Needed

Source: https://www.mitre.org/capabilities/cybersecurity/situation-awareness

Indonesia Honeynet Project

Cyber Situational Awareness



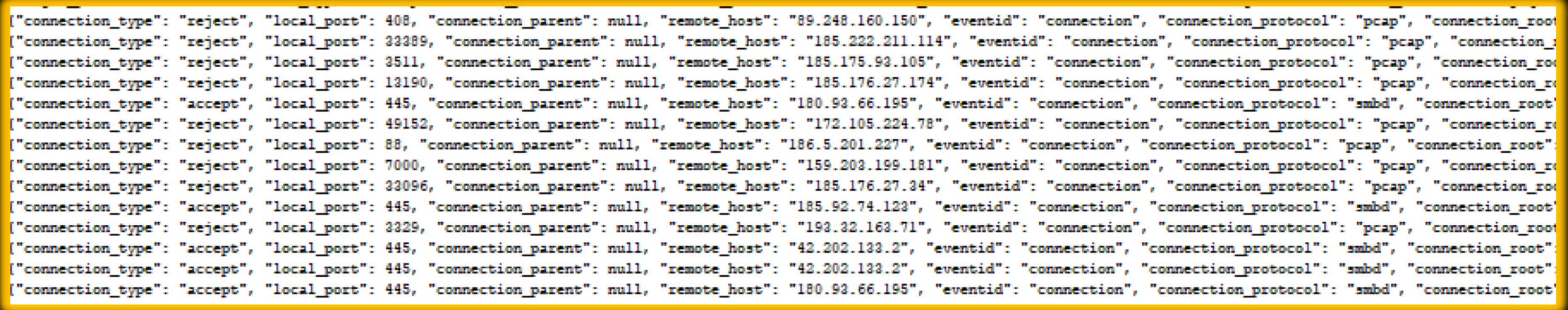
Forcasting – Predictive Model – Machine Learning

Mitigation – Risk Mitigation

Comprehension – Risk Analysis

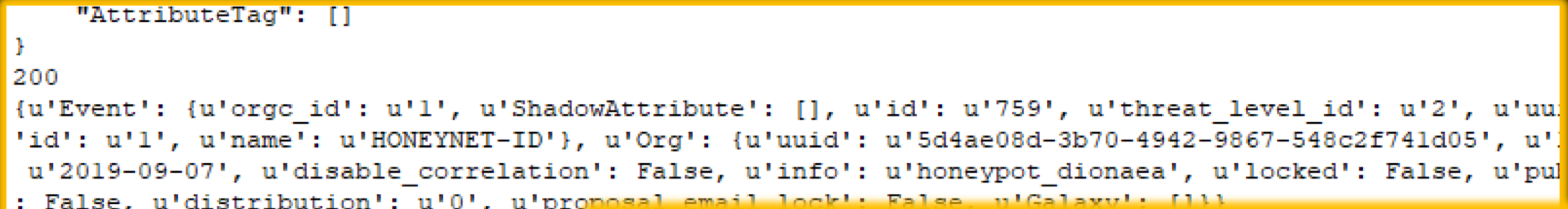
Perception – Security Monitoring

Cyber Situational Awareness – Honeypot Data



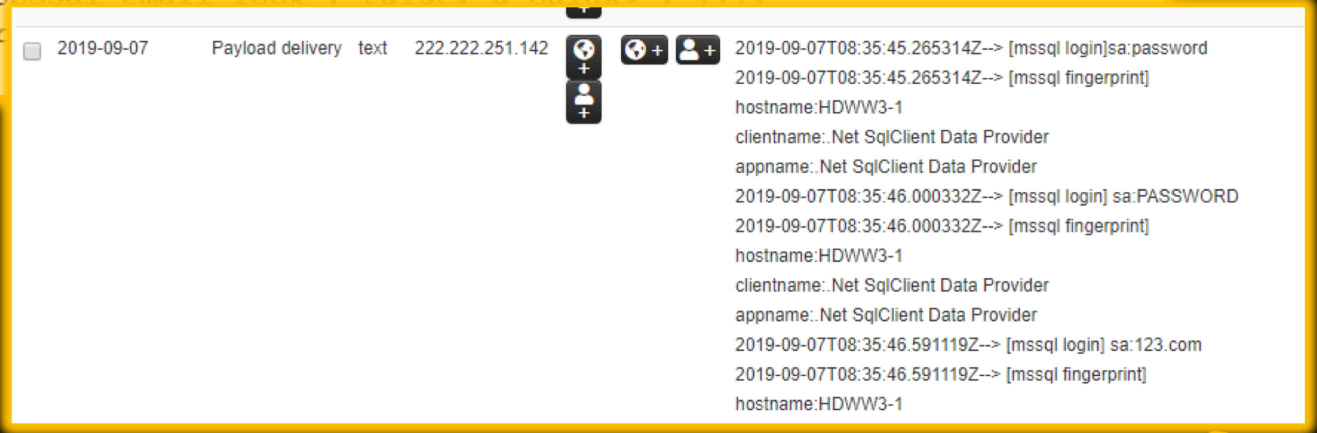
Honeypot Log

```
["connection_type": "reject", "local_port": 408, "connection_parent": null, "remote_host": "89.248.160.150", "eventid": "connection", "connection_protocol": "pcap", "connection_root
["connection_type": "reject", "local_port": 33389, "connection_parent": null, "remote_host": "185.222.211.114", "eventid": "connection", "connection_protocol": "pcap", "connection_
["connection_type": "reject", "local_port": 3511, "connection_parent": null, "remote_host": "185.175.93.105", "eventid": "connection", "connection_protocol": "pcap", "connection_roo
["connection_type": "reject", "local_port": 13190, "connection_parent": null, "remote_host": "185.176.27.174", "eventid": "connection", "connection_protocol": "pcap", "connection_r
["connection_type": "accept", "local_port": 445, "connection_parent": null, "remote_host": "180.93.66.195", "eventid": "connection", "connection_protocol": "smbd", "connection_root"
["connection_type": "reject", "local_port": 49152, "connection_parent": null, "remote_host": "172.105.224.78", "eventid": "connection", "connection_protocol": "pcap", "connection_r
["connection_type": "reject", "local_port": 88, "connection_parent": null, "remote_host": "186.5.201.227", "eventid": "connection", "connection_protocol": "pcap", "connection_root":
["connection_type": "reject", "local_port": 7000, "connection_parent": null, "remote_host": "159.203.199.181", "eventid": "connection", "connection_protocol": "pcap", "connection_r
["connection_type": "reject", "local_port": 33096, "connection_parent": null, "remote_host": "185.176.27.34", "eventid": "connection", "connection_protocol": "pcap", "connection_roo
["connection_type": "accept", "local_port": 445, "connection_parent": null, "remote_host": "185.92.74.123", "eventid": "connection", "connection_protocol": "smbd", "connection_root"
["connection_type": "reject", "local_port": 3329, "connection_parent": null, "remote_host": "193.32.163.71", "eventid": "connection", "connection_protocol": "pcap", "connection_root
["connection_type": "accept", "local_port": 445, "connection_parent": null, "remote_host": "42.202.133.2", "eventid": "connection", "connection_protocol": "smbd", "connection_root":
["connection_type": "accept", "local_port": 445, "connection_parent": null, "remote_host": "42.202.133.2", "eventid": "connection", "connection_protocol": "smbd", "connection_root":
["connection_type": "accept", "local_port": 445, "connection_parent": null, "remote_host": "180.93.66.195", "eventid": "connection", "connection_protocol": "smbd", "connection_root"
```



JSON File

```
    "AttributeTag": []
}
200
{u'Event': {u'orgc_id': u'1', u'ShadowAttribute': [], u'id': u'759', u'threat_level_id': u'2', u'uu
'id': u'1', u'name': u'HONEYNET-ID'}, u'Org': {u'uuid': u'5d4ae08d-3b70-4942-9867-548c2f741d05', u'
 u'2019-09-07', u'disable_correlation': False, u'info': u'honeypot_dionaea', u'locked': False, u'pu
: False, u'distribution': u'0', u'proposal_email_lock': False, u'Galaxy': []}}
{"name":"An Internal Error Has Occurr
500
```

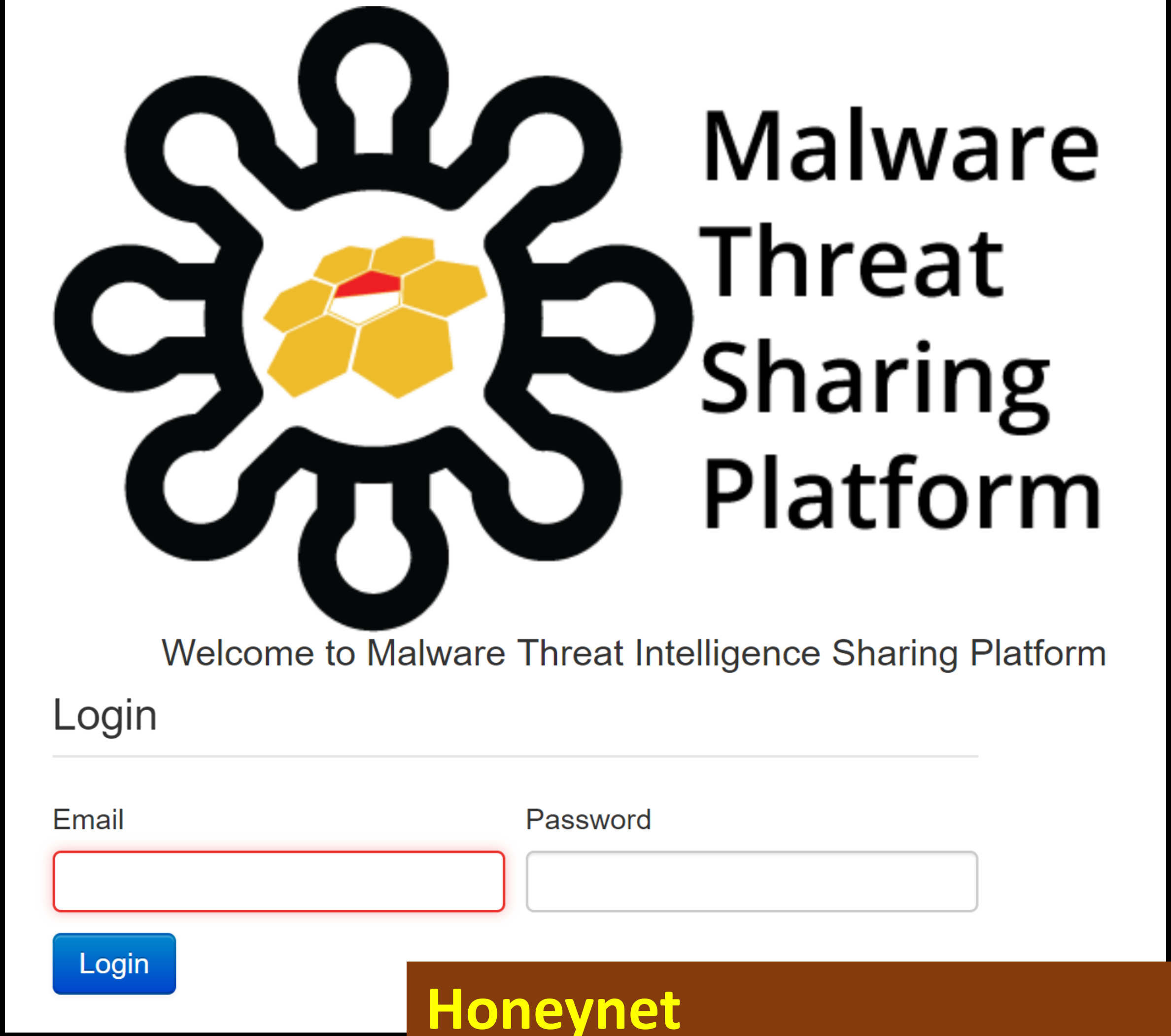


MISP Records

□ 2019-09-07 Payload delivery text 222.222.251.142

2019-09-07T08:35:45.265314Z--> [mssql login]sa:password
2019-09-07T08:35:45.265314Z--> [mssql fingerprint]
hostname:HDWW3-1
clientname:.Net SqlClient Data Provider
appname:.Net SqlClient Data Provider
2019-09-07T08:35:46.000332Z--> [mssql login] sa:PASSWORD
2019-09-07T08:35:46.000332Z--> [mssql fingerprint]
hostname:HDWW3-1
clientname:.Net SqlClient Data Provider
appname:.Net SqlClient Data Provider
2019-09-07T08:35:46.591119Z--> [mssql login] sa:123.com
2019-09-07T08:35:46.591119Z--> [mssql fingerprint]
hostname:HDWW3-1

Cyber Situational Awareness – Threat Sharing Platform



Malware Threat Sharing Platform

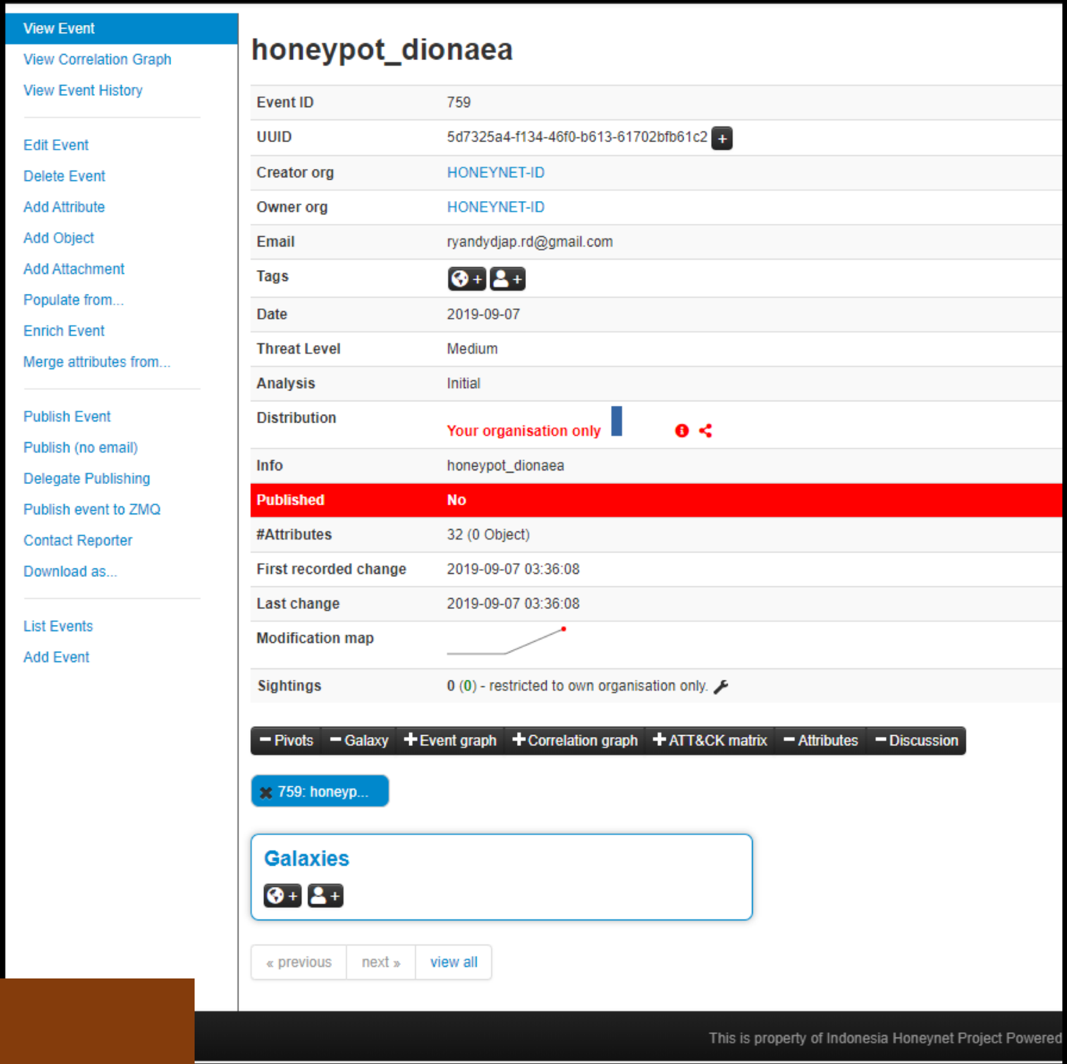
Welcome to Malware Threat Intelligence Sharing Platform

Login

Email

Password

Login



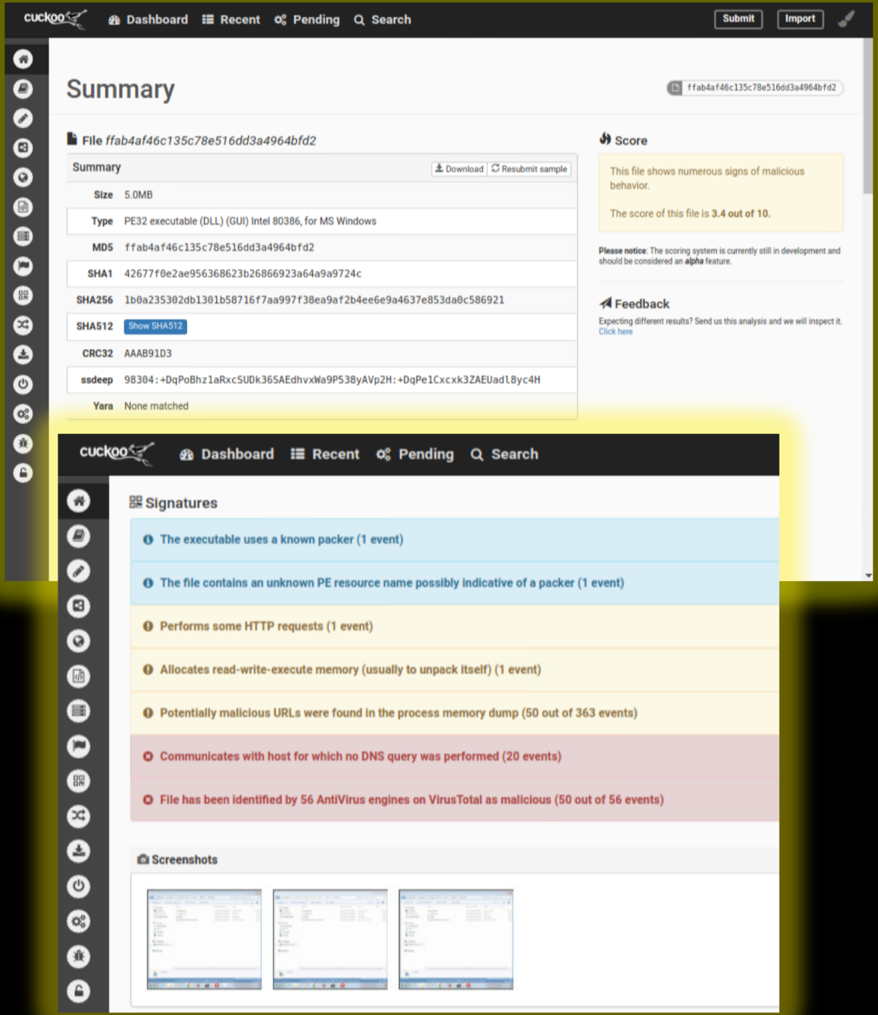
honeypot_dionaea

Event ID	759
UUID	5d7325a4-f134-46f0-b613-61702bfb61c2 +
Creator org	HONEYNET-ID
Owner org	HONEYNET-ID
Email	ryandydjap.rd@gmail.com
Tags	+ +
Date	2019-09-07
Threat Level	Medium
Analysis	Initial
Distribution	Your organisation only
Info	honeypot_dionaea
Published	No
#Attributes	32 (0 Object)
First recorded change	2019-09-07 03:36:08
Last change	2019-09-07 03:36:08
Modification map	
Sightings	0 (0) - restricted to own organisation only.

This is property of Indonesia Honeynet Project Powered

Honeynet
Malware Threat Sharing Platform

Cyber Situational Awareness – Threat Sharing Platform



Summary

ffab4af46c135c78e516dd3a4964bfd2

File *ffab4af46c135c78e516dd3a4964bfd2*

Summary — Download | Resubmit sample

Size	5.0MB
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	ffab4af46c135c78e516dd3a4964bfd2
SHA1	42677f0e2ae956368623b26866923a64a9a9724c
SHA256	1b0a235302db1301b58716f7aa997f38ea9af2b4ee6e9a4637e853da0c586921
SHA512	Show SHA512
CRC32	AAAB91D3
ssdeep	98304:+DqPoBhz1aRxcSUDk36SAEdhvxWa9P538yAVp2H:+DqPe1Cxcxk3ZAEUadl8yc4H
Yara	None matched

Score

This file shows numerous signs of malicious behavior.

The score of this file is **3.4 out of 10.**

Please notice: The scoring system is currently still in development and should be considered an ***alpha*** feature.

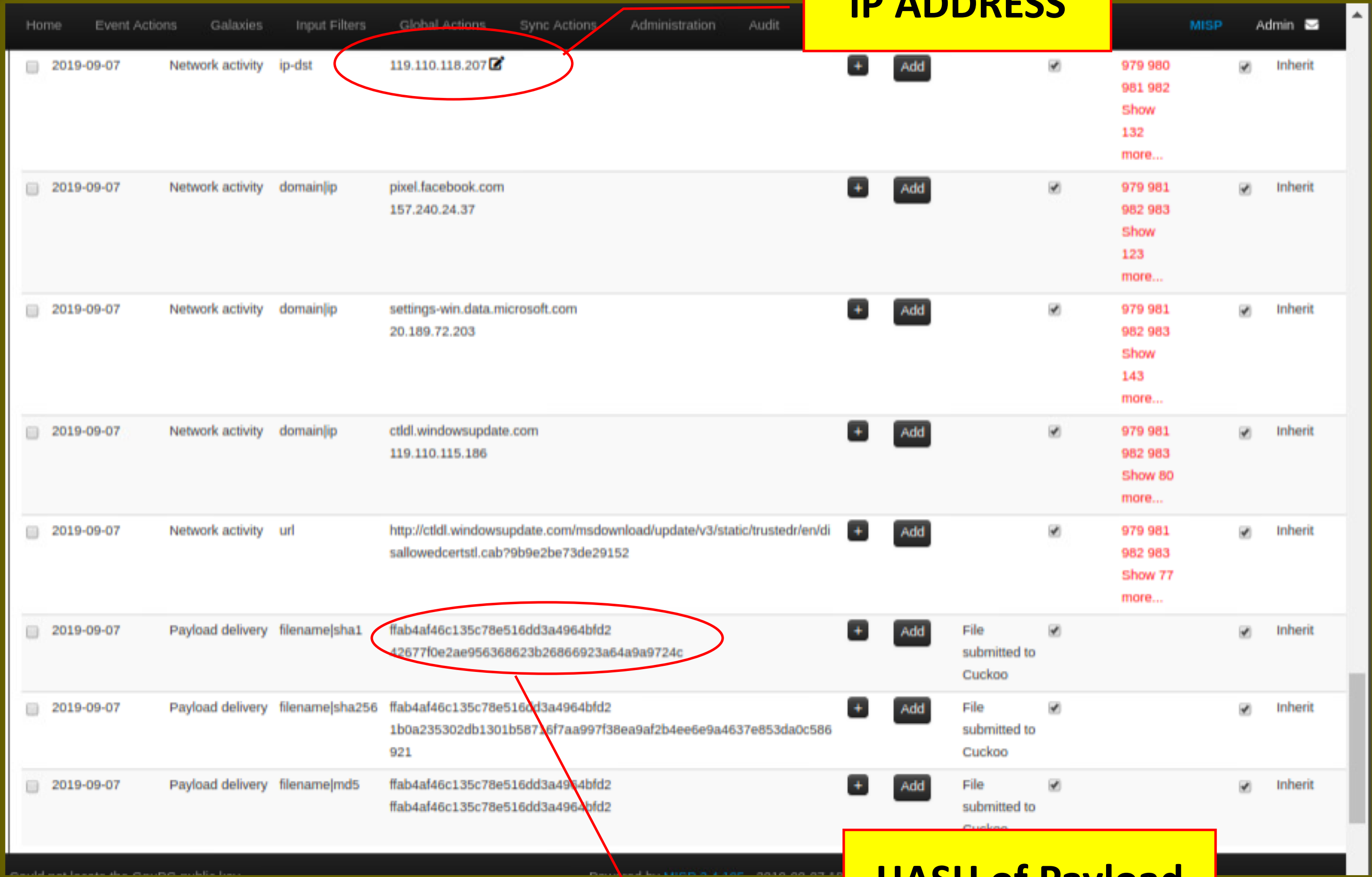
Feedback

Expecting different results? Send us this analysis and we will inspect it. Click here

Signatures

- The executable uses a known packer (1 event)
- The file contains an unknown PE resource name possibly indicative of a packer (1 event)
- Performs some HTTP requests (1 event)
- Allocates read-write-execute memory (usually to unpack itself) (1 event)
- Potentially malicious URLs were found in the process memory dump (50 out of 363 events)
- Communicates with host for which no DNS query was performed (20 events)
- File has been identified by 56 AntiVirus engines on VirusTotal as malicious (50 out of 56 events)

Screenshots



☐	2019-09-07	Network activity	ip-dst	119.110.118.207	+ Add		☑	979 980 981 982 Show 132 more...	☑	Inherit
☐	2019-09-07	Network activity	domain|ip	pixel.facebook.com 157.240.24.37	+ Add		☑	979 981 982 983 Show 123 more...	☑	Inherit
☐	2019-09-07	Network activity	domain|ip	settings-win.data.microsoft.com 20.189.72.203	+ Add		☑	979 981 982 983 Show 143 more...	☑	Inherit
☐	2019-09-07	Network activity	domain|ip	ctldl.windowsupdate.com 119.110.115.186	+ Add		☑	979 981 982 983 Show 80 more...	☑	Inherit
☐	2019-09-07	Network activity	url	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9b9e2be73de29152	+ Add		☑	979 981 982 983 Show 77 more...	☑	Inherit
☐	2019-09-07	Payload delivery	filename|sha1	ffab4af46c135c78e516dd3a4964bfd2 42677f0e2ae956368623b26866923a64a9a9724c	+ Add	File submitted to Cuckoo	☑		☑	Inherit
☐	2019-09-07	Payload delivery	filename|sha256	ffab4af46c135c78e516dd3a4964bfd2 1b0a235302db1301b58716f7aa997f38ea9af2b4ee6e9a4637e853da0c586921	+ Add	File submitted to Cuckoo	☑		☑	Inherit
☐	2019-09-07	Payload delivery	filename|md5	ffab4af46c135c78e516dd3a4964bfd2 ffab4af46c135c78e516dd3a4964bfd2	+ Add	File submitted to Cuckoo	☑		☑	Inherit

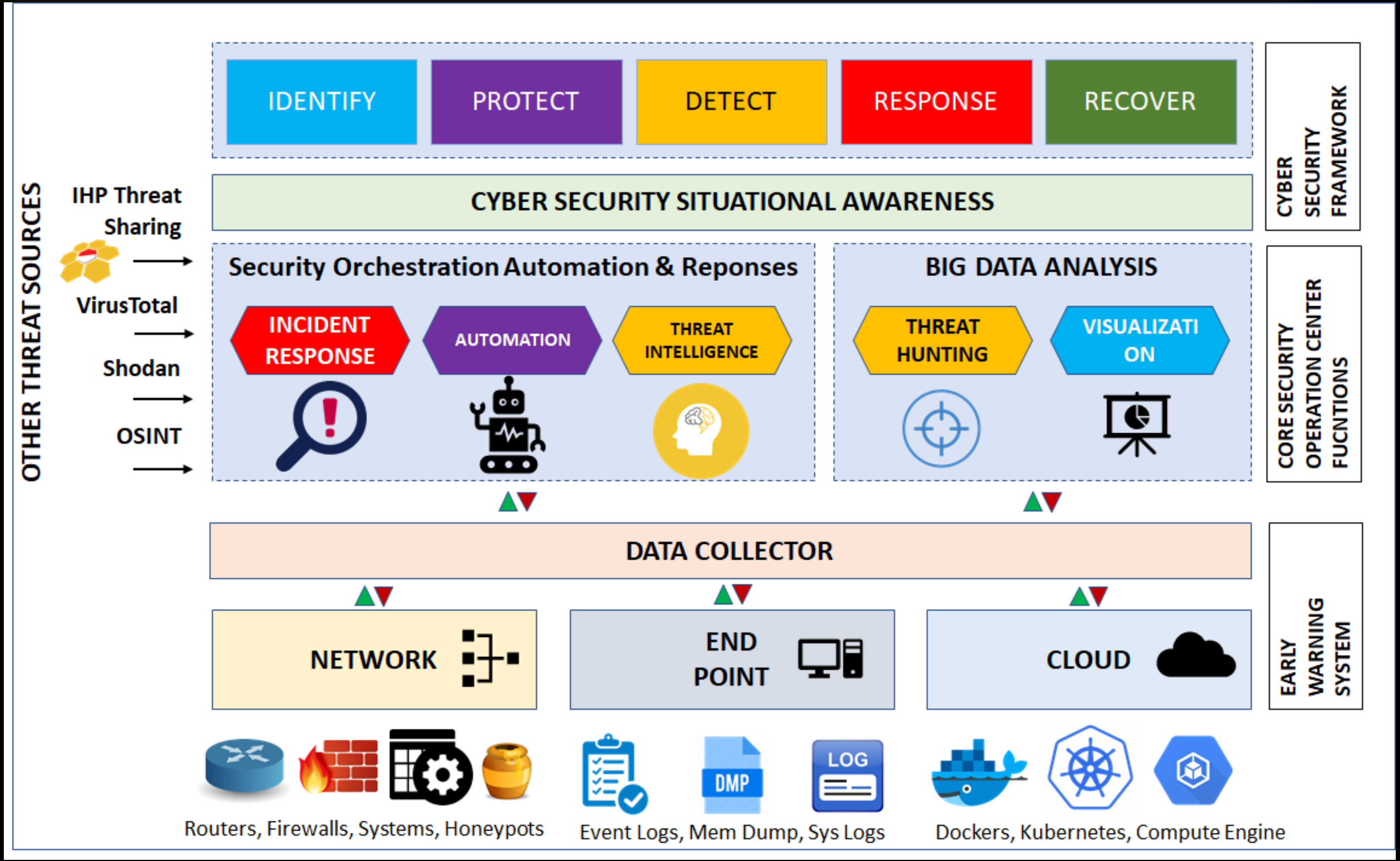
IP ADDRESS

HASH of Payload

Malware Analysis (Cuckoo) ➔ MISP

Indonesia Honeynet Project

Cyber Situational Awareness in Action

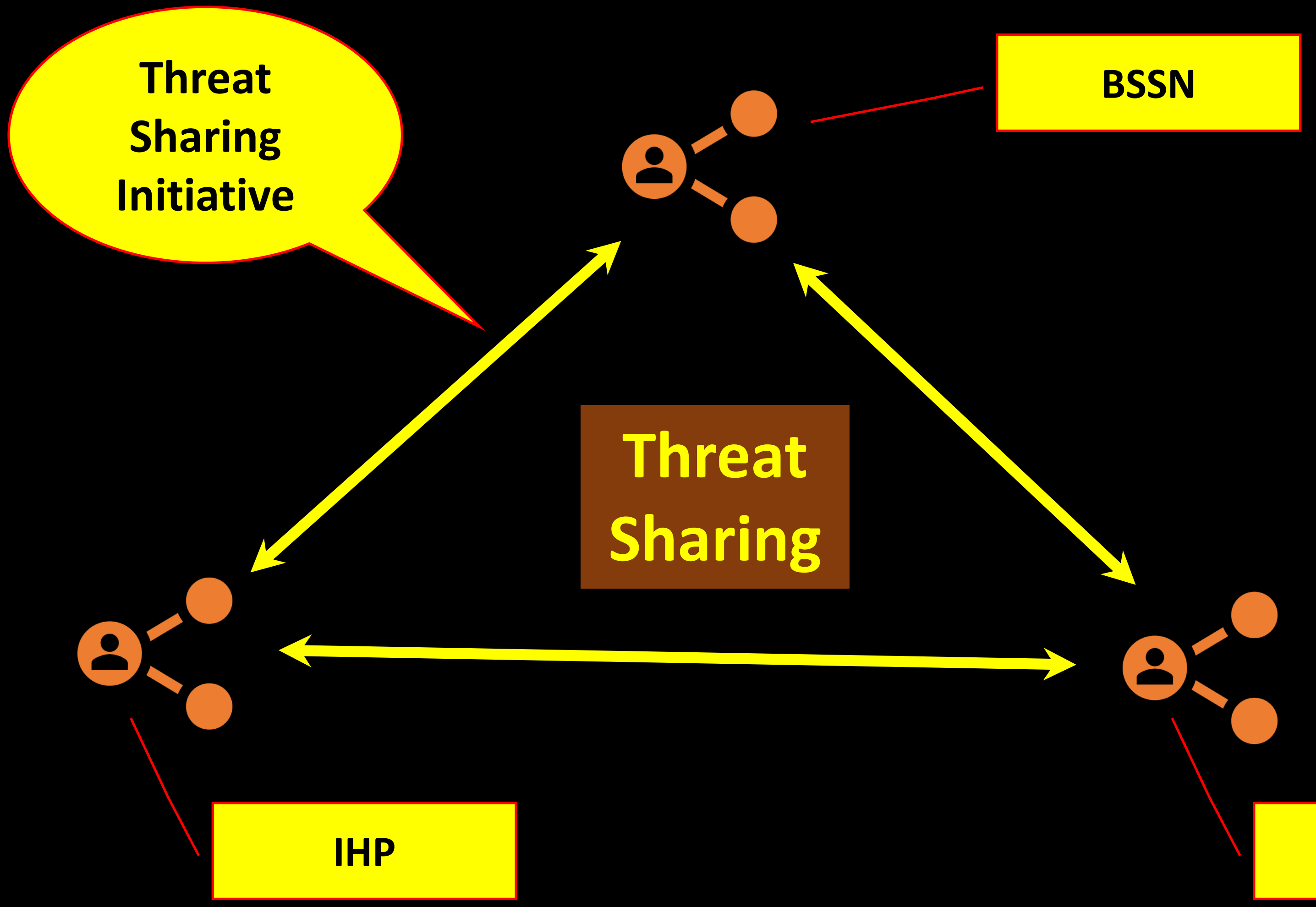


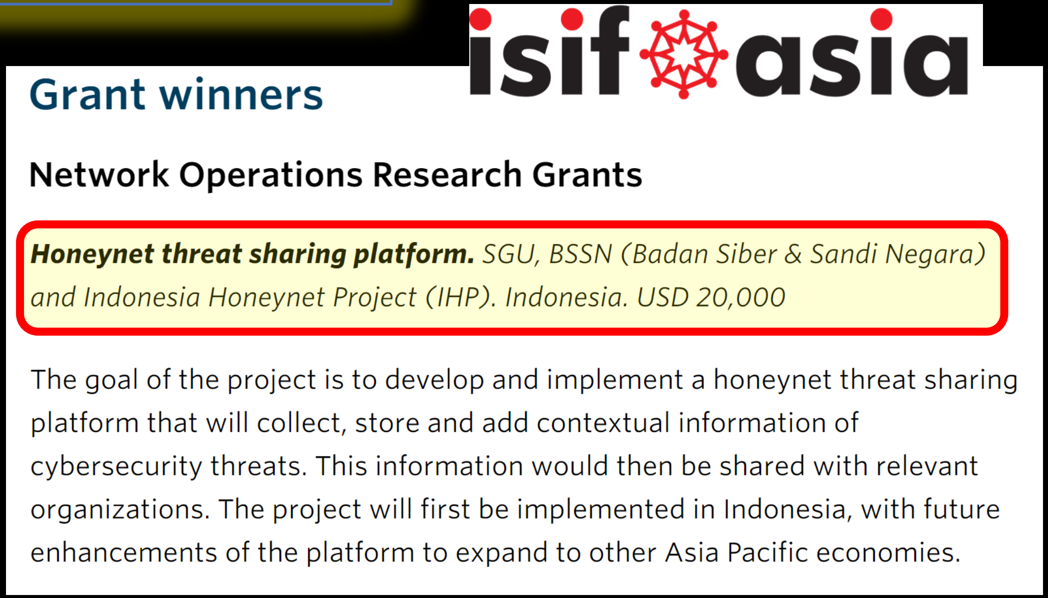
SOC:

- Incident Response
- Automation
- Threat Intelligence
- Threat Hunting
- Visualization

Indonesia Honeynet Project

Honeynet-based Threat Sharing Platform




isif asia

Grant winners

Network Operations Research Grants

Honeynet threat sharing platform. *SGU, BSSN (Badan Siber & Sandi Negara) and Indonesia Honeynet Project (IHP). Indonesia. USD 20,000*

The goal of the project is to develop and implement a honeynet threat sharing platform that will collect, store and add contextual information of cybersecurity threats. This information would then be shared with relevant organizations. The project will first be implemented in Indonesia, with future enhancements of the platform to expand to other Asia Pacific economies.

IHP Workshop 2019

IHP-BSSN Workshop

Track A
BSSN-IHP

- Deception Technology
- Visualizing & Sharing Threats
- Threat Intelligence

Track B
BSSN-IHP

- Malware Threat Sharing
- Windows Malware Analysis
- Hardening Azure Cloud

Track C
IHP-Palo

- Incident Response
- Detect, Investigate, dan Respond Cortex XDR
- Threat Hunting

Track D
ARUBA-TelU

- Aruba 360 Security Exchange
- Technological Advance in Crypto
- Digital Forensics

IHP Research Sharing

👉 **Ruang P 213**

Join Us!

Terima Kasih

Deception Technology | Malware | Data Mining | Cyber Crime | Tools

@IDHoneynet

Indonesia Honeynet Project

groups.google.com/group/id-honeynet