

Protect Your Online Business

Cyber Security Seminar & Workshop

Yohanes Syailendra, CEH, ECSCA

16 May 2017 | Marquee, Cyber 2 Tower 17th | Jakarta, Indonesia



Indonesia HoneyNet Project



Who Am I



**Singer
Wannabe**



**Programmer and
System Integrator**



**3x Indonesia Cyber Defense
Competition Winner +
DoD Cyber Security Team**




Indonesia Honeynet Project



Recycle Bin



malware




Privacy Protection

designed to protect

[Home Page](#)
[Full PC Scan](#)
[Privacy Keeper](#)
[Firewall](#)
[Update Settings](#)
[Global Settings](#)

WARNING!


 **Privacy Protection has found 31 useless and UNWANTED files on your computer!**

Information on removal
Potentially dangerous files were found on your system during the last scan!
It is strongly recommended that you remove them immediately

- Serious threats were detected
 - ▶ 28 items are critical privacy compromising content
 - ▶ 1 items is medium privacy threats
 - ▶ 2 items are junk content of low privacy threats

Potential risks:

- ▶ Exposure of your private data, including credit card information, etc.
- ▶ Slow web-surfing and malware downloads while visiting websites
- ▶ Windows running slow and system crashes

 Activation is highly recommended

[Activate Now](#)

[Help & Support](#)

Your PC might be at risk.
Activate the software to protect it.


[Get full time protection now](#)

FIREWALL WARNING

Hidden file transfer to remote host has been detected

Detection has detected a leak of your files though
We strongly recommend that you block the
immediately

▶ Remote host transfer IP:	43.111.238.84
▶ Remote user computer name:	MAINUSER-PC
▶ User name:	Main User
	150.158.237.91

 **Security Warning!**
Malicious program has been detected.
Click here to protect your computer.

[Block attack](#)

[Allow](#)

9:01 AM

2/24/2013

Two of the biggest Telco in Indonesia got Hacked at the same day



Tiket.com Hacked?

**HACKER REMAJA
INI SUKSES BOBOL
SITUS
TIKET.COM
DI SERVER
CITILINK,
KERUGIAN
DITAKSIR RP 4,1
MILIAR**



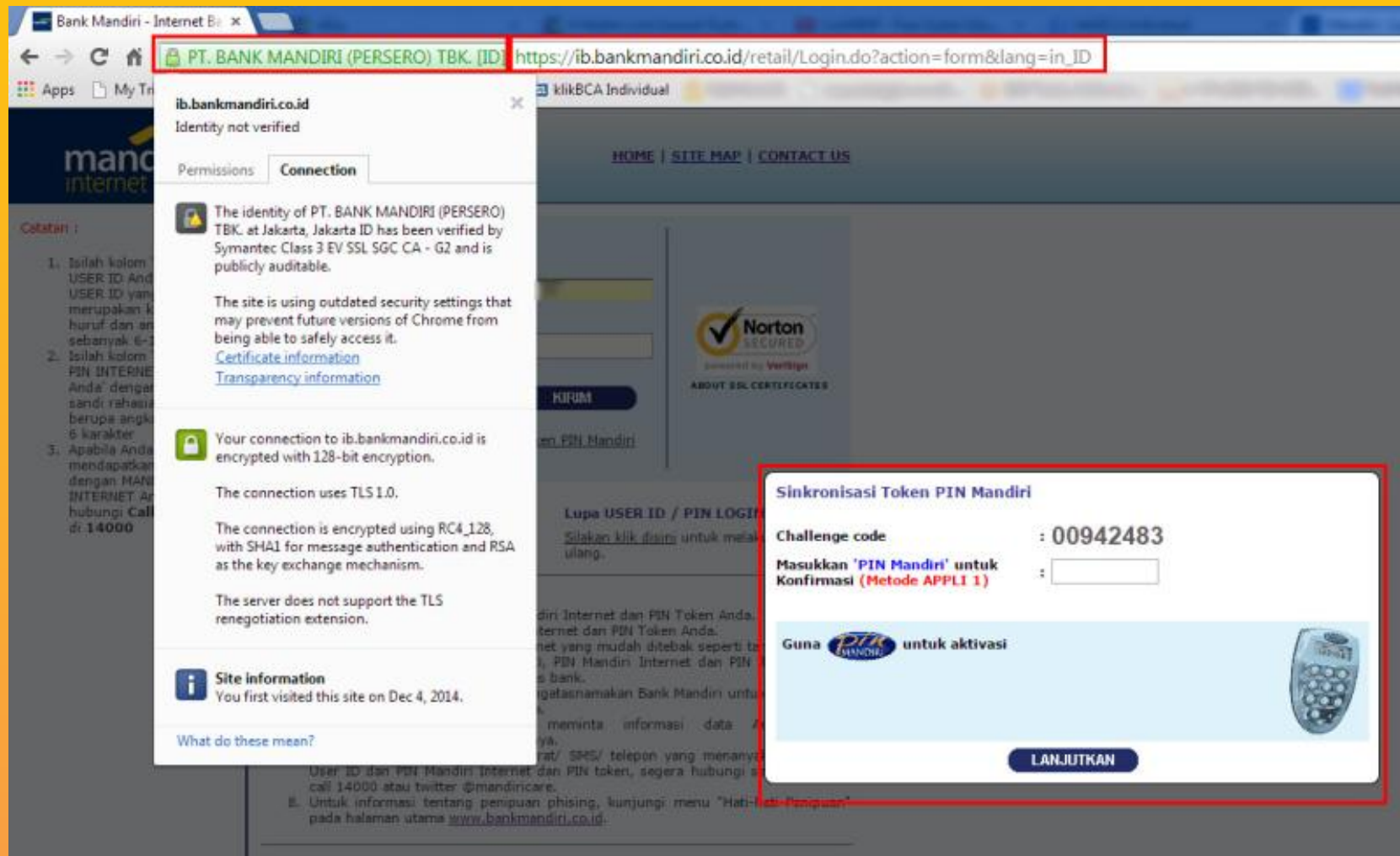
Saksikan Video Berita Terupdate Hari Ini



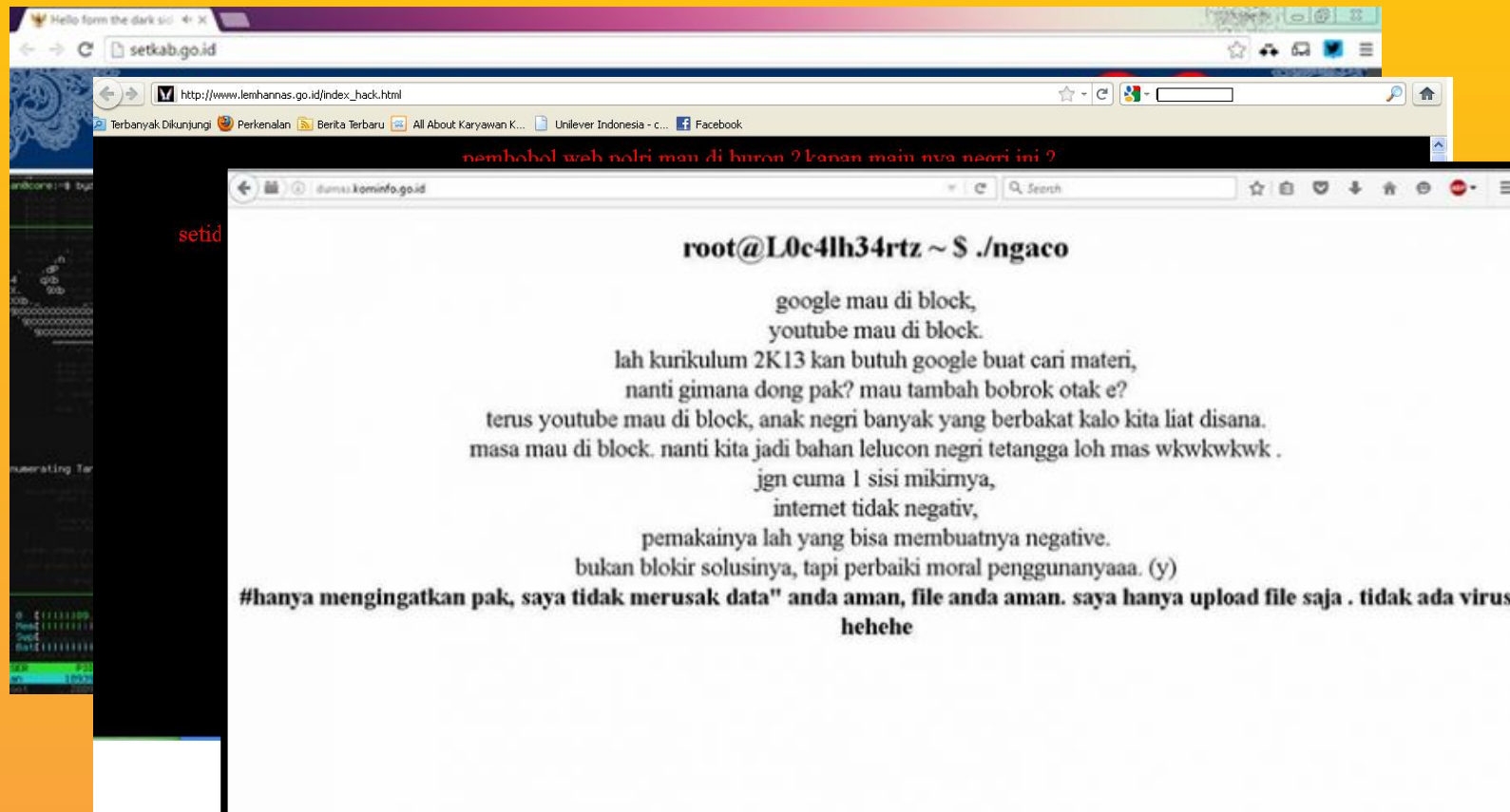
Indonesia HoneyNet Project



“Sinkronisasi Token” and Malware trying to spoof destination account



Hundreds of Government sites aren't Secured



Hacked website by Blackhat group

1. www.langaitz.com/bannerrak/index.php
2. <http://emeralda-golfclub.com/system>
3. <http://www.suplemengki.com/stampe>
4. <http://pjinformatics.com/About-Us.htm>
5. <http://ciptakarya.pu.go.id/v3/search.php>
6. www.ibighit.com
7. <http://divine-order.cba.pl/>
8. <http://www.bentleyscafe.co.uk/news/>
9. <http://izumino.jp/Security/analyze/26/>
10. <http://www.kopditswastiastu.co.id/inc>
11. <http://www.clinicasdeconduccion.com>
12. <http://breukelaar-brands.nl/index.php>
13. <http://thelclub.com.br/editor/images/>
14. <http://marc.info/?l=horde-commits&n>
15. <http://szkolachelmce.pl/var.php>
16. <http://daycare.starsphere.jp/>
17. <http://kaschkonzept.de/>
18. http://www.hack-mirror.com/mirror_3
19. <http://pdb.ma-mifa.sch.id/>
20. <http://digilib.stainponorogo.ac.id/files>
21. <http://www.methodist2mdn.sch.id/An>
22. <http://thewaster.com/x.php>
23. <http://www.elicadavlumbaz.com/E.ph>
24. <http://otomas.co.id/login.php>
25. <https://www.defacer.id/2221.html>
26. <http://pokemongonobrasil.com/>
27. Site : <http://adomahangom.hu/Qs.php>
28. Site : <http://awm-hungary.com/Qs.php>
29. Site : <http://azorr.hu/Qs.php> Defaced
30. Site : <http://babparavan.hu/Qs.php> Defaced
31. Site : <http://bakman.hu/Os.php> Defaced
32. Site : <http://beasmink.hu/>
33. Site : <http://beaszalon.hu/>
34. Site : <http://bolcsodes.hu/>
35. Site : <http://botiteamk.hu/>
36. Site : <http://chrys.hu/C>
37. Site : <http://codefactor.hu/>
38. Site : <http://compassw.hu/>
39. Site : <http://cursorinsig.hu/>
40. Site : <http://edentars.hu/>
41. Site : <http://electro-he.hu/>
42. Site : <http://evotrend.hu/>
43. Site : <http://fedoracorr.hu/>
44. Site : <http://feketesaph.hu/>
45. Site : <http://fruttanatu.hu/>
46. Site : <http://fussteis.hu/>
47. Site : <http://gleams.hu/>
48. Site : <http://ha1ya.hu/>
49. Site : <http://hungaryin.hu/>
50. Site : <http://iseum.com/>
51. Site : <http://kacs.hu/>
52. Site : <http://kolyokruhi.hu/>
53. Site : <http://miellqualit.hu/>
54. Site : <http://motorordo.hu/>
55. Site : <http://naraykft.hu/>
56. Site : <http://nextent.hu/>
57. Site : <http://nyeregben.hu/>
58. Site : <http://oladplato.hu/>
59. Site : <http://party.fish/qz.php> Defaced
60. Site : <http://profieskuvo.hu/Qs.php> Defaced
61. Site : <http://saltstack.hu/Qs.php> Defaced
62. Site : <http://sesg.h.hu/Qs.php> Defaced
63. Site : <http://slackware.hu/Qs.php> Defaced
64. Site : <http://szentendreitelek.hu/Qs.php> Defaced
65. Site : <http://szentpeterfa-alapitvany.com/Qs.php> Defaced
66. Site : <http://szombathely.hu/Qs.php> Defaced
67. Site : <http://szombathelyizsidohitkozseg.hu/Qs.php> Defaced
68. Site : <http://tomsymon.com/Qs.php> Defaced
69. Site : <http://travelgoo.hu/Qs.php> Defaced
70. Site : <http://ungvarikft.hu/Qs.php> Defaced
71. Site : <http://unicornis97.hu/Qs.php> Defaced
72. Site : <http://vday.hu/Qs.php> Defaced
73. Site : <http://vinfo.hu/Qs.php> Defaced
74. Site : <http://vitorlas.com/Qs.php> Defaced
75. <http://www.oyunoloji.tk/>
76. <http://numismaticaxxl.altervista.org/blog/>
77. <http://www.gherardovitalirosati.it/IMG/html/index.html>
78. <http://marcrenaud.me/wp-content/ubh/>
79. <http://www.dwp-grupo.com/>



Half of Internet Down in 2016

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

Dyn estimated that the attack had involved '100,000 malicious endpoints', and the company said there had been reports of an extraordinary attack strength of 1.2 terabits (1,200 gigabytes) per second. Photograph: Alamy

The [cyber-attack](#) that brought down much of America's internet last week was caused by a new weapon called the Mirai botnet and was likely the largest of its kind in history, experts said.

The victim was the servers of Dyn, a company that controls much of the internet's domain name system (DNS) infrastructure. It was hit on 21 October and remained under sustained assault for most of the day, bringing down sites including Twitter, the Guardian, Netflix, Reddit, CNN and many others in Europe and the US.



Is This a Hacker ?



Indonesia HoneyNet Project





They are around us..

All activities should
be anonymous



Indonesia HoneyNet Project

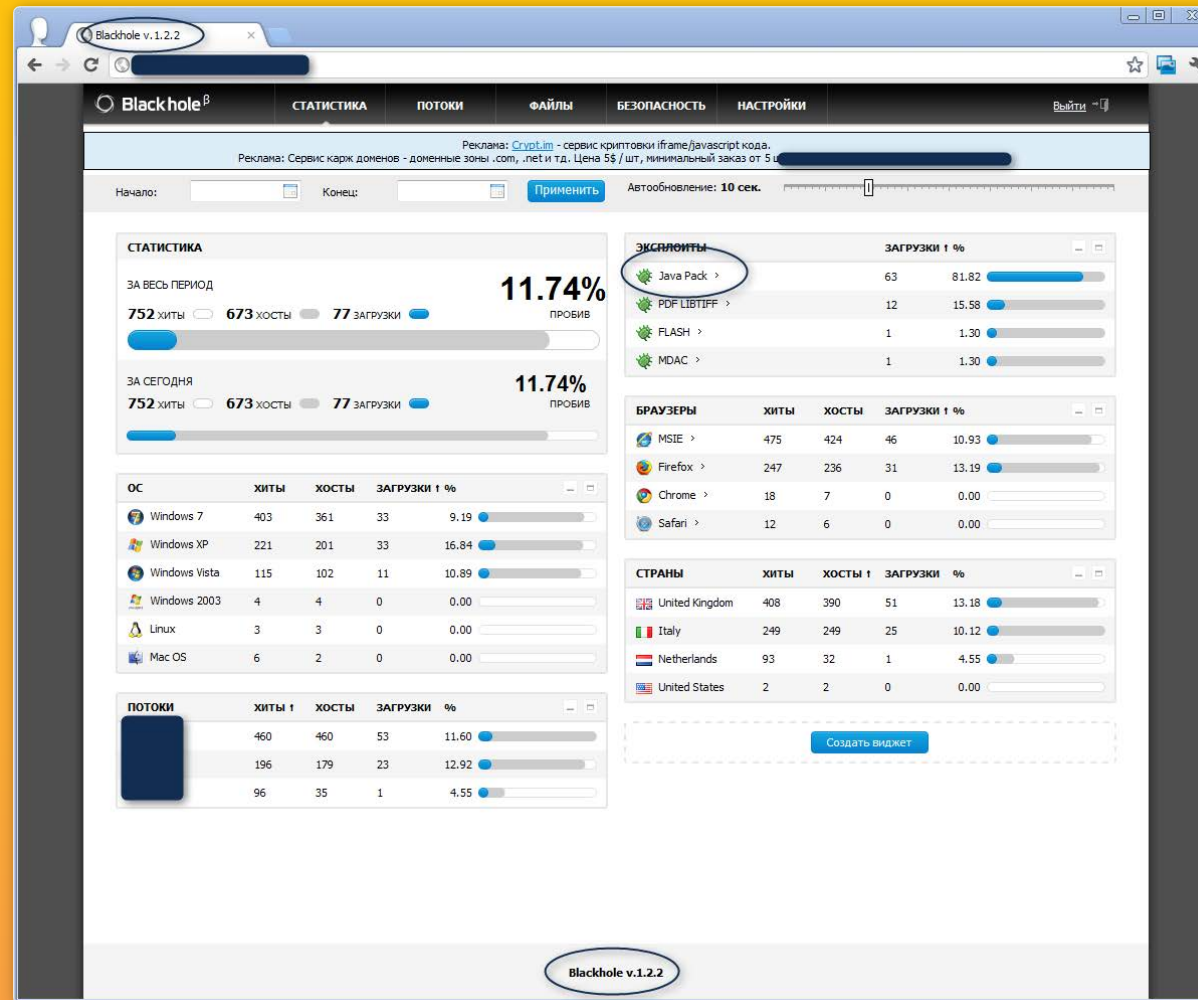




Indonesia HoneyNet Project



Botnet Command and Control



Advanced Persistent Threat (APT): The Uninvited Guest

How attackers remain in your network harvesting information and avoiding detection over time

1. INCURSION

Attackers break into network by using social engineering to deliver targeted malware to vulnerable systems and people.

2. DISCOVERY

Once in, the attackers stay "low and slow" to avoid detection. They then map the organization's defenses from the inside and create a battle plan and deploy multiple parallel kill chains to ensure success.

3. CAPTURE

Attackers access unprotected systems and capture information over an extended period. They may also install malware to secretly acquire data or disrupt operations.

4. EXFILTRATION

Captured information is sent back to attack team's home base for analysis and further exploitation fraud—or worse.



Indonesia Honeynet Project





So, How to Protect?

**Know Your Enemy, Know Yourself, And Victory is
Never in Doubt, not in a hundred battles**

- Sun Tzu, The Art of War -



Indonesia HoneyNet Project





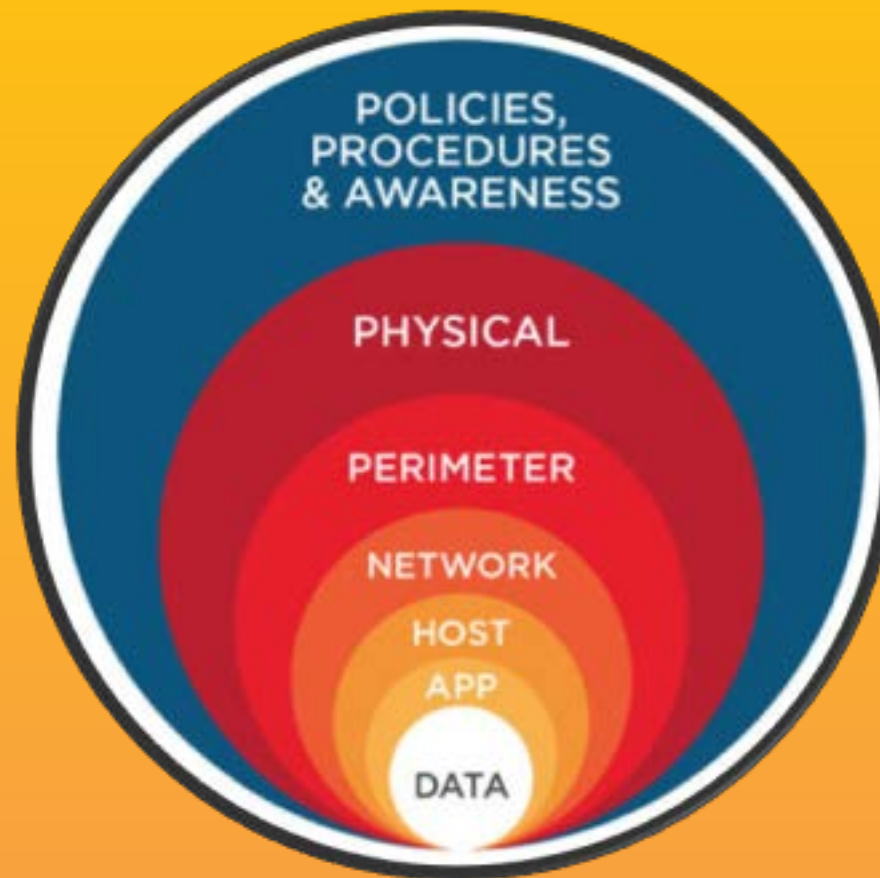
Indonesia Honeynet Project



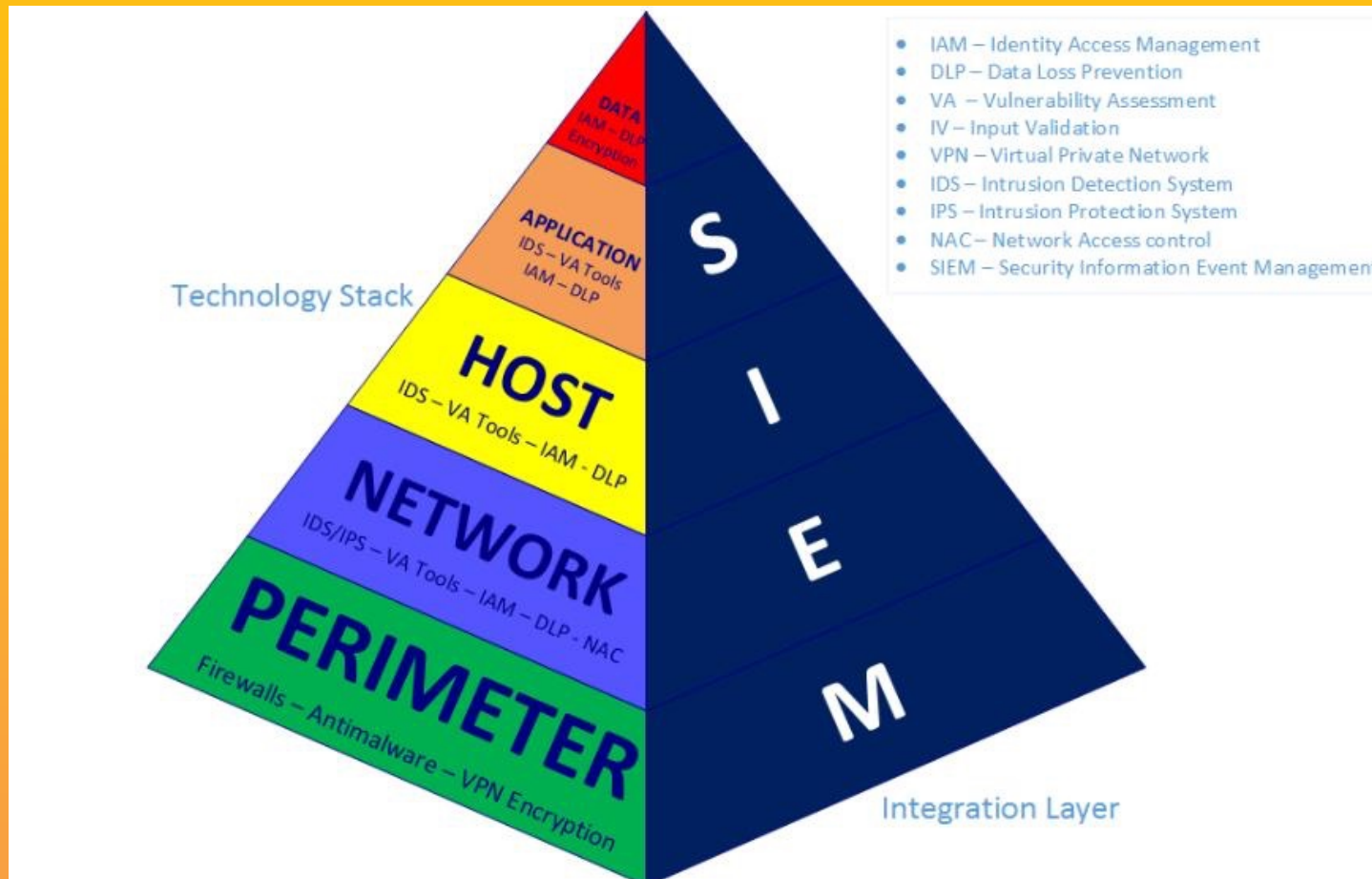
1. Conduct a **Security Assessment to measure the **Security Risks** and **Maturity Level****



2. Implement **Layered Security Protection**

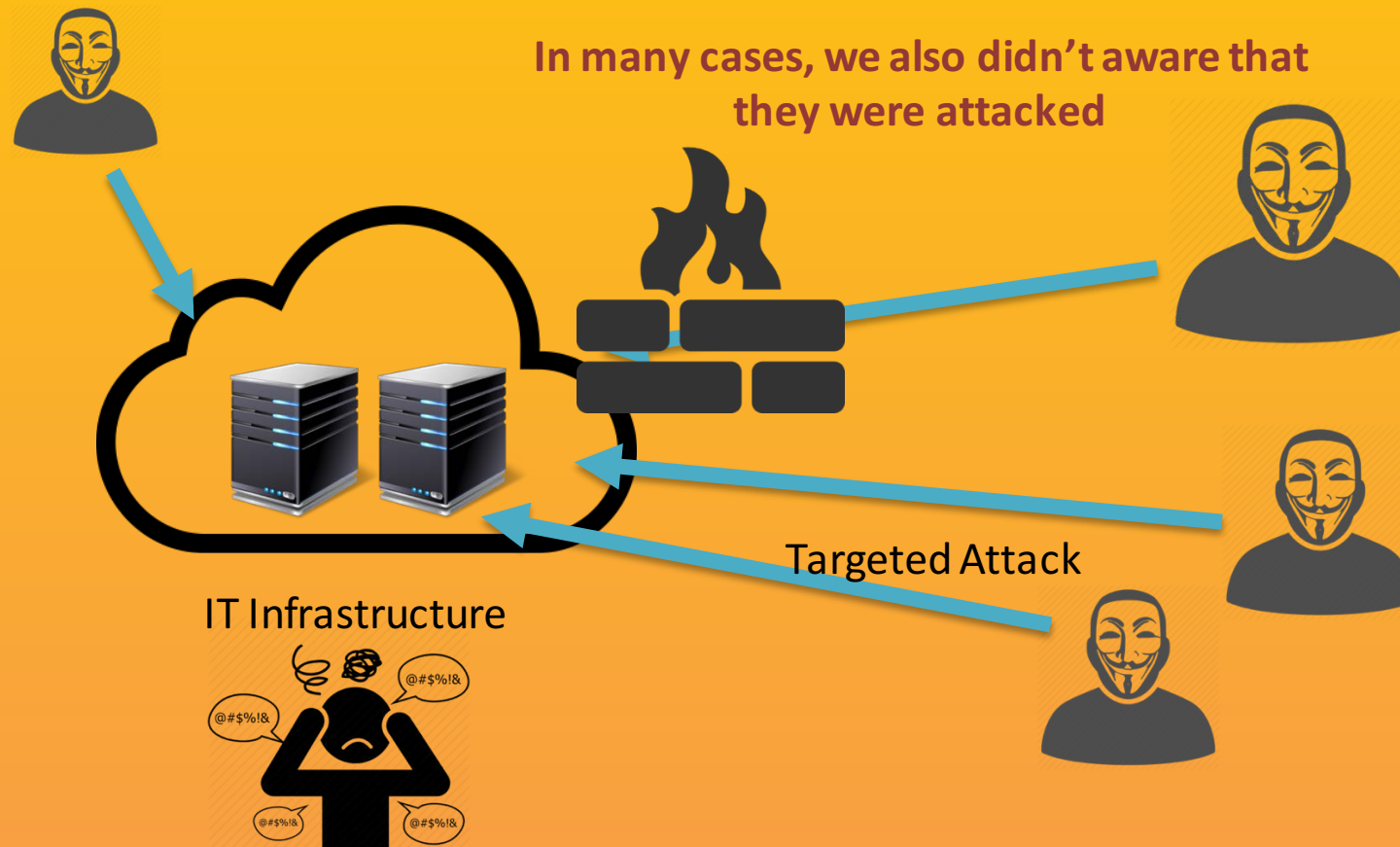


Layered Security Model



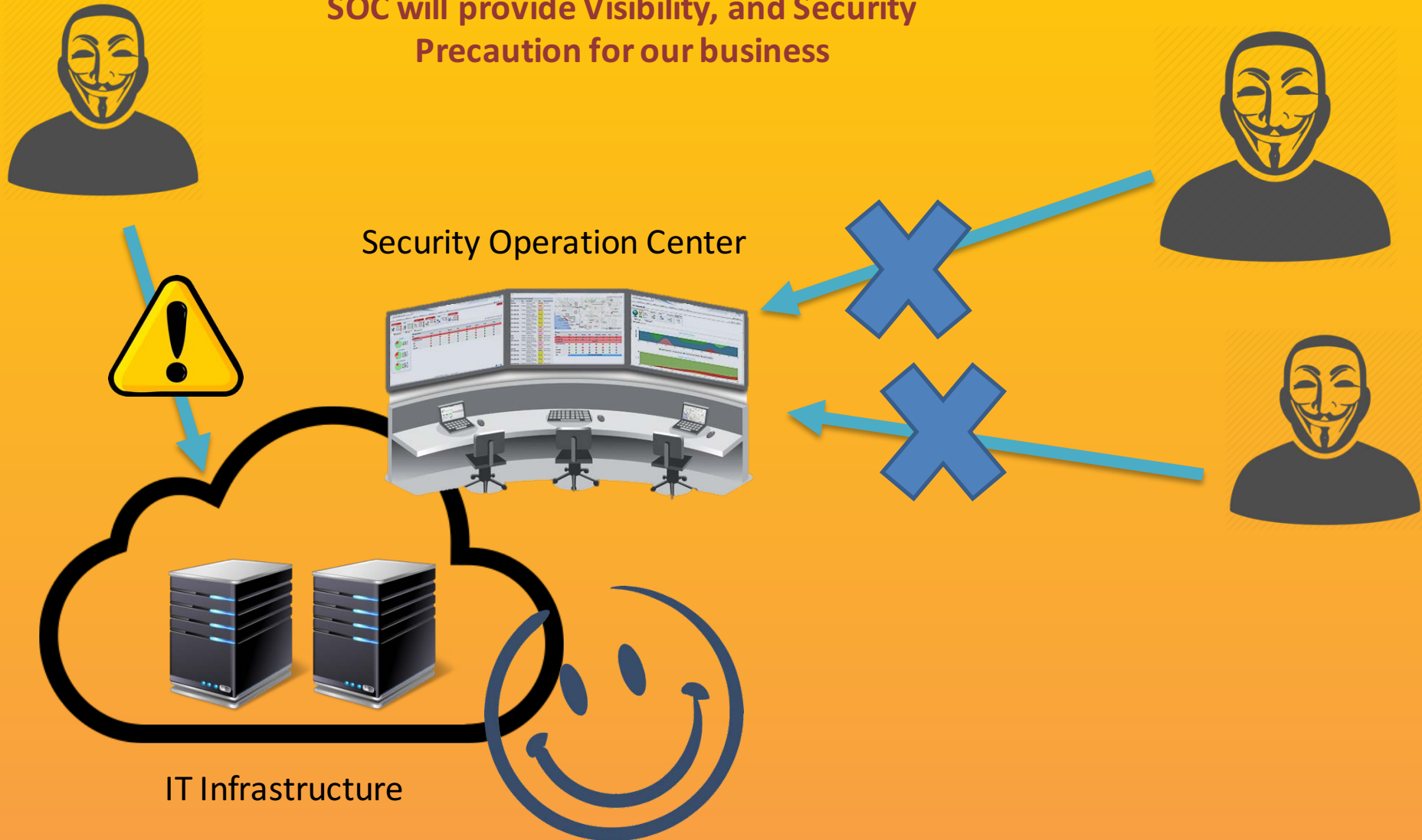
Targeted Attack Landscape

Current Security System cannot guarantee to protect you from ANY Attacks, especially when you are TARGETED



3. Implement Monitoring TEAM

SOC will provide Visibility, and Security
Precaution for our business



Common **Mistakes** on Security Implementation



**CyberSecurity is a SHARED RESPONSIBILITY,
And it boils down to this: In CyberSecurity,
THE MORE SYSTEMS WE SECURE, THE
MORE SECURE WE ALL ARE**

**- Jen Johnson -
(Secretary of Homeland Security)**



Indonesia Honeynet Project





Indonesia HoneyNet Project

