LAMPIRAN

LAMPIRAN I (KUESIONER)

Kuesioner Penelitian

Berikut merupakan kuesioner penelitian terkait “Keamanan Data K4IPP Dalam Pertahanan Siber Kemhan dan TNI

Form A

Umum

1. Jenis Kelamin
   - Pria
   - Wanita

2. Umur
   - ≤ 20 tahun
   - 21–30 tahun
   - 31-40 tahun
   - 41-50 tahun
   - ≥51 tahun

3. Strata
   - Perwira
   - Bintara
   - Tamtama
   - PNS/ASN
   - Other ……

4. Pendidikan *
   - SMA

- D3
- S1
- S2
- S3
- Other:_____

5. Satker : *

_____

6. Saya bertugas di bidang: *

- Programmer
- Database Administrator
- System Analyst
- Network Analyst
- Security Analyst
- IT Support
- Other: ……

7. Pernyataan berikut yang sesuai dengan keterkaitan saya dalam K4IPP/CSIRT ataupun pengolahan data dan informasi: *
   - Saya leader/anggota Tim K4IPP, CSIRT ataupun pengolahan data dan informasi Banyak pekerjaan saya terkait dengan K4IPP, CSIRT ataupun pengolahan data dan informasi
   - Beberapa pekerjaan saya terkait dengan K4IPP, CSIRT ataupun pengolahan data dan informasi

- Walau pekerjaan saya tidak terkait K4IPP, CSIRT ataupun pengolahan data daninformasi tapi saya sering diminta pendapat terkait K4IPP ataupun CSIRT
- Saya tidak terlibat apapun dalam K4IPP, CSIRT ataupun pengolahan data daninformasi

Form B

Keterangan :
5 : Sangat baik
4 : Baik
3 : Cukup Baik
2 :Tidak Baik
1 :Sangat Tidak Baik

8. Apakah sistem arsitektur jaringan yang ada sudah mampu mendukung pengolahan data dan informasi, komando dan kendali serta pertahanan siberdengan baik? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

9. Apakah pengembangan sistem keamanan jaringan dilaksanakan secara rutin? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

10. Apakah teknologi yang ada saat ini dapat mendukung K4IPP/CSIRT ataupun pengolahan data dan informasi dengan baik ? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

11. Apakah sistem arsitektur jaringan yang ada mampu meningkatkaninteroperabilitas system dengan baik? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

12. Bagaimanakah dengan teknologi pengamanan data/pertahanan siber yang ada,apakah berpengaruh pada pengolahan data dan informasi ataupun K4IPP? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

13. Sejauh ini bagaimanakah perkembangan teknologi pengolahan data dan informasi serta keamanan data yang sudah di bangun ? apakah berjalan denganbaik dan mampu mendukung operasi? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

14. Apakah ada bagian/unit yang berfungsi sebagai CSIRT dalam menanganikeamanan data/insiden siber? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

15. Apakah SOP dalam menangani keamanan data/insiden siber sudah ada? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

16. Bagaimanakah infrastruktur keamanan data dan informasi dalam pertahanansiber? Apakah sudah dapat diandalkan? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

Keterangan :

5 : Sangat baik

4 : Baik

3 : Cukup Baik

2 :Tidak Baik

1 :Sangat Tidak Baik

Brainware

17. Bagaimana kesiapan pengawak di bidang pengolahan data dan informasi,pertahanan siber ataupun K4IPP? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat baik

18. Apakah rutin diadakan latihan keterampilan penanggulangan insiden siber? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat baik

19. Apakah pengguna sudah memahami penggunaan teknologi pengolahan datadan informasi, pertahanan siber serta K4IPP? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat baik

20. Bagaimana dengan regenerasi pengguna, apakah dapat terlaksana dengan baiktanpa kendala yang berarti? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat baik

21. Bagaimana kesiapan dan keahlian pengguna dalam melaksanakan latihan dukungan data dan informasi dalam suatu operasi serta pertahanan siber dalamskala besar/nasional? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat baik

22. Bagaimana kemampuan pengguna dalam mengikuti perkembangan teknologiinformasi dan pengolahan data serta pertahanan siber pada suatu operasi? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat baik

23. Bagaimana kesiapan pengguna dalam merespon perintah dan informasi melaluiteknologi K4IPP? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat baik

24. Bagaimana kemampuan pengguna dalam mengolah informasi menggunakan bigdata serta machine learning untuk menganalisa dalam pengambilan keputusan?*

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat baik

25. Apakah personel pengguna sudah sesuai dengan jumlah dan kemampuan yangdi tentukan organisasi? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat baik

Keterangan :

5 : Sangat Baik

4 : Baik

3 : Cukup Baik

2 :Tidak Baik

1 :Sangat Tidak Baik

Hardware

26. Seberapa siapkah teknologi pengolahan data dan informasi serta keamanandata dalam fungsi proses pengambilan keputusan? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

27. Bagaimana kemampuan dari arsitektur jaringan yang ada saat ini dalammenghadapi kerentanan insiden siber? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

28. Apakah infrastruktur hardware keamanan jaringan, serta pengolahan data daninformasi telah sesuai kebutuhan? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

29. Apakah spesifikasi hardware yang digunakan telah sesuai dengan kebutuhanoperasional? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

30. Apakah firewall telah digunakan pada semua arsitektur jaringan serta selaluterupdate? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

31. Apakah keamanan server telah diuji dari insiden siber? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

32. Apakah hardware selalu diupgrade secara rutin sesuai dengan perkembanganteknologi dan situasi? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

33. Apakah pengadaan hardware baru yang akan digunakan telah diujikeamanannya dari peretasan? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

34. Bagaimana kesiapan server dalam kondisi darurat, back up manajemen? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

35. Bagaimana tingkat kecepatan penggantian komponen hardware yang rusak? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

Software

Keterangan :

5 : Sangat Baik

4 : Baik

3 : Cukup Baik

2 :Tidak Baik

1 :Sangat Tidak Baik

36. Bagaimana orisinalitas software program aplikasi yang digunakan? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

37. Apakah juga menggunakan software bajakan? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

38. Apakah telah menetapkan antivirus yang resmi digunakan pada organisasi? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

39. Sejauh mana tingkat pengembangan modulasi sistem keamanan dan enkripsisaat ini? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

40. Dalam penggunaan software open source, apakah telah diuji keamanannya? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

41. Apakah software yang digunakan selalu di update secara rutin? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

42. Seberapa besar peran software yang telah dikembangkan dalammempermudah analisa informasi yang ada? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

43. Seberapa besar kemungkinan software yang digunakan dapat diretas? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

44. Apakah software yang dikembangkan saat ini telah memenuhi syarat untukmelakukan interkoneksi dalam K4IPP? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

45. Seberapa jauh software yang ada dapat mendukung keamanan siber sertatingkat Interkoneksi dalam K4IPP? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

Infrastructureware

Keterangan :

5 : Sangat Baik

4 : Baik

3 : Cukup Baik

2 :Tidak Baik

1 :Sangat Tidak Baik

46. Apakah sistem yang ada mampu monitoring jaringan komputer dari potensiVirus, Malware serta insiden siber lainnya? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

47. Apakah sistem Firewall yang ada sudah dapat mengatasi insiden siber? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

48. Apakah pada setiap arsitektur jaringan dipasang IDS (Intrussion Detection System) untuk mendeteksi aktifitas tidak wajar? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

49. Bagaimana kesiapan VPN untuk menjaga kerahasiaan dan komunikasi data? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

50. Apakah sistem Maintenance dalam menjaga performa sistem dilaksanakansecara rutin? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

51. Apakah Sistem audit dilaksanakan dalam meningkatkan efisiensi dan performasistem? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

52. Bagaimana sistem interkoneksi antar sensor dalam K4IPP untuk mendukungketersediaan informasi? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

53. Bagaimana tingkat keamanan data dalam pertukaran informasi dan sistemsharing atau distribusi informasi dalam suatu operasi? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

54. Seberapa baik tingkat keamanan informasi dan komunikasi yang telah dikembangkan? Terutama dalam proses pertukaran data antar satker yangterintegrasi dalam server dan jaringan? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

55. Apakah alokasi kebutuhan bandwith telah sesuai dalam pelaksanaan operasional? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

Firmware

Keterangan :

5 : Sangat Baik

4 : Baik

3 : Cukup Baik

2 :Tidak Baik

1 :Sangat Tidak Baik

56. Tingkat kelengkapan dalam penyediaan dokumen pendukung dalam penyelenggaraan kegiatan keamanan data dan informasi *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

57. Ketersediaan suatu prosedur standar peraturan atau kebijakan terkait keamanandata, informasi dan komunikasi data antar satker *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

58. Dokumen sistem pengamanan data dan informasi mengacu kepada standar keamanan data dan informasi dan dokumen lainnya yang berhubungan denganoperasi *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

59. Seberapa jauh tingkat pengembangan grand design sistem informasi dalampengamanan data dan informasi ? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

60. Perumusan roadmap dan NSF (Network Security Frameworks) untuk keamanandata dan informasi saat ini *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

61. Bagaimana ketersediaan buku petunjuk standar pengoperasian dalam rangkamengelola dan mengamankan satu jaringan sistem informasi dan sistem jaringan komputer? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

62. Tingkat ketersediaan dokumen yang dapat menjamin keamanan data dan informasi dalam melakukan komunikasi dan distribusi data antar satker dalamtingkat interoperabilitas *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

63. Tingkat ketersediaan SOP dalam mengatasi Malfunction ataupun insiden siberketika operasi berjalan, sebagai jaminan keamanan pengguna/operator *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

64. Tingkat pelaksanaan SOP dalam perlindungan data dan informasi dalampertahanan siber *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

Keterangan :

5 : Sangat Baik

4 : Baik

3 : Cukup Baik

2 :Tidak Baik

1 :Sangat Tidak Baik

Budgetware

65. Bagaimana dukungan alokasi anggaran dalam operasional pertahanan siber? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

66. Bagaimana kecukupan sumber daya pendanaan dalam pengembangan sistemdan SDMnya? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

67. Bagaimana manajemen keuangan dalam mengatasi insidental? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

68. Bagaimana kesiapan anggaran dalam mendukung sustainabilitas pengembangan pengolahan data dan informasi, pertahananan siber serta K4IPPsesuai dengan roadmap yang telah ditentukan? *

	1	2	3	4	5	
Sangat Tidak Baik	◯	◯	◯	◯	◯	Sangat Baik

Lampiran 2 Data Responden

Satker	u1	u2	u3	u4	u5	u6	u7	u8	u9
Pusinfolahta TNI	4	5	4	4	4	4	4	2	3
Pusinfolahta TNI	4	2	3	4	4	4	4	4	4
Pusinfolahta TNI	3	3	3	3	3	3	3	3	3
Pusinfolahta TNI	4	5	4	5	5	4	3	5	4
Pushansiber Kemhan	5	5	5	5	5	5	5	5	5
Pushansiber Kemhan	3	4	3	3	3	3	4	3	3
Pushansiber Kemhan	2	2	3	2	3	3	4	2	3
Pushansiber Kemhan	2	2	2	2	2	2	2	2	2
Pushansiber Kemhan	4	4	4	4	4	4	3	4	3
Pushansiber Kemhan	3	4	4	3	4	3	4	3	3
Pushansiber Kemhan	4	4	4	4	4	4	4	4	4
Pushansiber Kemhan	3	3	3	3	3	3	4	4	3
Pusdatin Kemhan	5	5	4	5	4	5	5	4	4
Pushansiber Kemhan	3	4	3	3	3	3	3	3	3
Pushansiber Kemhan	4	5	4	4	4	4	5	5	5
Pushansiber Kemhan	2	2	3	3	3	3	4	3	3
Pusdatin Kemhan	4	4	4	3	3	3	5	3	3
Pusdatin Kemhan	3	4	4	5	4	4	3	3	3
Pusdatin Kemhan	5	4	5	3	4	4	5	3	5
Pusdatin Kemhan	3	2	3	3	3	3	4	2	3

Pusdatin Kemhan	4	4	4	4	4	4	4	4	4
Pusdatin Kemhan	3	2	3	4	4	2	4	3	4
Pusdatin Kemhan	4	4	3	3	3	3	3	3	3
Pusdatin Kemhan	3	4	3	2	3	3	3	4	3
Pusdalops TNI	3	3	3	3	3	3	3	4	3
Pusdalops TNI	4	4	4	4	4	4	4	4	4
Pusdalops TNI	3	2	3	3	4	3	2	4	3
Pusdalops TNI	3	3	3	3	3	3	3	3	3
Pusdalops TNI	3	3	3	3	3	3	3	3	3

Satker	b1	b2	b3	b4	b5	b6	b7	b8	b9
Pusinfolahta TNI	3	3	3	3	3	4	3	2	3
Pusinfolahta TNI	4	3	3	3	3	4	3	3	4
Pusinfolahta TNI	3	3	3	3	3	3	3	3	3
Pusinfolahta TNI	3	3	3	3	5	3	3	3	3
Pushansiber Kemhan	5	5	5	5	5	5	5	5	5
Pushansiber Kemhan	3	2	3	3	2	3	3	3	2
Pushansiber Kemhan	3	3	3	2	2	3	3	3	2
Pushansiber Kemhan	2	2	2	2	2	2	2	2	2
Pushansiber Kemhan	4	4	4	4	4	4	4	4	4
Pushansiber Kemhan	3	2	2	2	3	3	3	3	2
Pushansiber Kemhan	4	3	3	3	4	3	4	4	3
Pushansiber Kemhan	3	2	2	3	3	3	3	3	3

Pusdatin Kemhan	5	4	5	5	4	4	4	4	5
Pushansiber Kemhan	3	3	3	3	3	3	3	3	3
Pushansiber Kemhan	5	5	5	5	5	5	5	5	5
Pushansiber Kemhan	2	2	2	3	2	3	2	3	1
Pusdatin Kemhan	3	4	3	3	3	3	4	4	3
Pusdatin Kemhan	3	3	3	3	3	3	3	4	3
Pusdatin Kemhan	4	2	3	3	1	3	3	4	2
Pusdatin Kemhan	3	3	2	3	2	3	3	2	3
Pusdatin Kemhan	4	4	4	4	4	4	4	4	3
Pusdatin Kemhan	3	3	3	2	3	3	3	4	2
Pusdatin Kemhan	3	3	3	3	3	3	3	3	3
Pusdatin Kemhan	3	3	3	3	2	3	2	2	3
Pusdalops TNI	3	3	3	3	3	3	3	3	3
Pusdalops TNI	4	4	4	3	4	4	4	4	3
Pusdalops TNI	3	4	3	3	2	4	3	3	2
Pusdalops TNI	3	3	3	2	3	3	3	3	2
Pusdalops TNI	3	3	3	3	3	3	3	3	3

Satker	h1	h2	h3	h4	h5	h6	h7	h8	h9	h10
Pusinfolahta TNI	4	4	3	3	5	3	4	3	3	3
Pusinfolahta TNI	4	4	4	4	4	4	4	4	3	3
Pusinfolahta TNI	3	3	3	3	3	3	3	3	3	3
Pusinfolahta TNI	4	4	2	2	5	5	5	1	3	2

Pushansiber Kemhan	4	5	5	5	5	5	5	5	5	5
Pushansiber Kemhan	2	3	3	2	3	4	2	3	2	2
Pushansiber Kemhan	3	3	3	4	4	4	3	3	2	2
Pushansiber Kemhan	2	2	2	2	2	2	2	2	2	2
Pushansiber Kemhan	4	4	4	4	4	4	4	5	4	4
Pushansiber Kemhan	3	3	2	2	3	2	3	3	3	2
Pushansiber Kemhan	4	3	4	3	3	3	3	3	3	3
Pushansiber Kemhan	3	3	3	3	3	3	3	3	3	3
Pusdatin Kemhan	5	5	5	5	5	5	5	5	5	4
Pushansiber Kemhan	3	3	3	3	3	3	3	3	3	3
Pushansiber Kemhan	5	5	5	5	5	5	5	5	5	5
Pushansiber Kemhan	3	3	3	2	3	2	2	3	3	2
Pusdatin Kemhan	5	3	3	4	5	3	4	4	4	3
Pusdatin Kemhan	3	3	4	4	3	4	3	4	3	3
Pusdatin Kemhan	5	3	3	3	3	4	3	5	4	4
Pusdatin Kemhan	3	2	3	3	2	1	1	1	1	1
Pusdatin Kemhan	4	3	3	3	3	3	3	4	4	4
Pusdatin Kemhan	3	3	3	3	3	3	2	2	2	2
Pusdatin Kemhan	3	3	3	3	4	3	3	4	3	3
Pusdatin Kemhan	3	2	2	4	4	3	2	4	2	3
Pusdalops TNI	3	3	3	3	3	3	3	3	3	3
Pusdalops TNI	4	3	3	3	4	3	4	3	4	3

Pusdalops TNI	3	4	3	2	4	4	3	4	3	3
Pusdalops TNI	3	3	3	3	3	3	3	3	3	3
Pusdalops TNI	3	3	3	3	3	3	3	3	3	3

Satker	s1	s2	s3	s4	s5	s6	s7	s8	s9	s10
Pusinfolahta TNI	5	1	1	3	2	5	4	3	3	4
Pusinfolahta TNI	4	3	4	3	4	4	4	4	4	4
Pusinfolahta TNI	3	3	3	3	3	3	3	3	3	3
Pusinfolahta TNI	5	1	5	5	3	5	5	4	3	3
Pushansiber Kemhan	5	5	5	5	5	5	5	5	5	5
Pushansiber Kemhan	4	4	4	3	3	3	3	2	2	3
Pushansiber Kemhan	4	2	4	3	3	3	3	3	3	3
Pushansiber Kemhan	2	2	2	2	2	2	2	2	2	2
Pushansiber Kemhan	4	4	4	4	4	4	4	4	4	4
Pushansiber Kemhan	3	3	3	4	3	3	3	3	3	4
Pushansiber Kemhan	4	4	3	3	3	3	3	3	3	3
Pushansiber Kemhan	4	1	5	3	4	4	3	2	4	3
Pusdatin Kemhan	5	1	5	5	5	5	4	4	5	5
Pushansiber Kemhan	3	1	3	3	3	3	3	3	3	3
Pushansiber Kemhan	5	4	4	3	4	4	4	3	4	5
Pushansiber Kemhan	3	3	4	2	3	3	2	3	1	1
Pusdatin Kemhan	4	1	5	4	4	4	4	3	3	3
Pusdatin Kemhan	3	3	4	4	4	4	3	3	3	3

Pusdatin Kemhan	1	1	1	3	4	3	5	5	2	5
Pusdatin Kemhan	4	1	1	1	3	3	2	2	3	2
Pusdatin Kemhan	4	1	4	4	4	4	4	4	4	4
Pusdatin Kemhan	4	2	3	3	3	3	3	3	3	3
Pusdatin Kemhan	4	2	4	3	3	3	3	3	3	3
Pusdatin Kemhan	4	1	1	2	3	2	4	2	3	3
Pusdalops TNI	3	4	4	4	3	3	4	4	4	4
Pusdalops TNI	4	2	3	3	3	4	4	3	4	4
Pusdalops TNI	5	2	3	4	3	4	4	4	3	4
Pusdalops TNI	3	3	3	3	3	3	3	3	3	3
Pusdalops TNI	3	3	3	3	3	3	3	3	3	3

Satker	i1	i2	i3	i4	i5	i6	i7	i8	i9	i10
Pusinfolahta TNI	3	5	5	5	5	4	4	4	4	4
Pusinfolahta TNI	3	4	3	4	4	4	4	4	4	4
Pusinfolahta TNI	3	3	3	3	3	3	3	3	3	3
Pusinfolahta TNI	5	5	5	5	5	5	5	5	5	5
Pushansiber Kemhan	5	5	5	5	5	5	5	5	5	5
Pushansiber Kemhan	3	3	4	2	2	1	3	2	3	4
Pushansiber Kemhan	4	4	4	4	3	1	4	3	2	4
Pushansiber Kemhan	2	2	2	2	2	2	2	2	2	2
Pushansiber Kemhan	4	4	4	4	4	4	4	4	4	3
Pushansiber Kemhan	3	3	3	3	3	3	3	4	3	3

Pushansiber Kemhan	4	4	3	4	3	4	3	4	4	4
Pushansiber Kemhan	3	3	3	3	3	3	3	3	3	4
Pusdatin Kemhan	5	5	5	5	5	5	5	5	5	4
Pushansiber Kemhan	3	3	3	3	3	3	3	3	3	3
Pushansiber Kemhan	4	5	5	5	5	4	5	5	5	5
Pushansiber Kemhan	3	3	4	3	2	2	1	2	2	3
Pusdatin Kemhan	4	4	4	4	4	4	3	4	4	5
Pusdatin Kemhan	3	3	3	3	3	3	3	3	3	3
Pusdatin Kemhan	4	3	4	5	4	1	3	3	2	4
Pusdatin Kemhan	3	2	3	3	3	3	3	4	3	3
Pusdatin Kemhan	3	3	4	5	4	4	4	4	4	4
Pusdatin Kemhan	3	2	3	3	3	3	3	3	3	3
Pusdatin Kemhan	4	4	4	4	4	4	3	4	4	4
Pusdatin Kemhan	2	3	4	4	4	4	3	4	3	4
Pusdalops TNI	2	3	2	3	3	3	3	3	3	3
Pusdalops TNI	4	4	4	4	4	4	4	4	4	2
Pusdalops TNI	5	5	4	4	4	3	3	3	4	3
Pusdalops TNI	3	3	3	3	3	3	3	3	3	3
Pusdalops TNI	3	3	3	3	3	3	3	3	3	3

Satker	f1	f2	f3	f4	f5	f6	f7	f8	f9
Pusinfolahta TNI	3	2	3	3	3	3	3	3	3
Pusinfolahta TNI	4	4	4	4	4	4	4	4	4

Pusinfolahta TNI	3	3	3	3	3	3	3	3	3
Pusinfolahta TNI	5	5	5	3	2	5	5	3	5
Pushansiber Kemhan	5	5	5	5	5	5	5	5	5
Pushansiber Kemhan	3	2	2	3	2	2	2	2	2
Pushansiber Kemhan	2	2	2	2	3	2	2	2	2
Pushansiber Kemhan	2	2	2	2	2	2	2	2	2
Pushansiber Kemhan	4	4	4	4	4	4	4	4	4
Pushansiber Kemhan	3	3	4	3	3	3	3	3	3
Pushansiber Kemhan	4	3	4	3	4	3	4	3	4
Pushansiber Kemhan	3	3	3	3	3	3	3	3	3
Pusdatin Kemhan	5	4	4	4	5	4	5	4	4
Pushansiber Kemhan	3	3	3	3	3	3	3	3	3
Pushansiber Kemhan	4	5	5	5	5	5	5	5	5
Pushansiber Kemhan	3	3	3	3	2	3	2	2	2
Pusdatin Kemhan	3	3	3	4	3	3	3	4	4
Pusdatin Kemhan	3	3	3	3	3	3	3	3	3
Pusdatin Kemhan	2	1	1	1	1	3	3	2	1
Pusdatin Kemhan	3	2	3	3	3	3	3	3	3
Pusdatin Kemhan	4	3	3	3	3	3	3	4	4
Pusdatin Kemhan	3	3	3	3	3	3	3	3	3
Pusdatin Kemhan	3	3	3	3	3	3	3	3	3
Pusdatin Kemhan	3	4	3	3	3	4	3	3	3

Pusdalops TNI	3	3	3	3	3	3	3	3	3
Pusdalops TNI	3	4	4	4	4	3	4	3	4
Pusdalops TNI	3	4	4	4	4	3	3	4	4
Pusdalops TNI	3	3	3	3	3	3	3	3	3
Pusdalops TNI	3	3	3	3	3	3	3	3	3

Satker	bg1	bg2	bg3	bg4
Pusinfolahta TNI	3	2	2	2
Pusinfolahta TNI	3	3	3	4
Pusinfolahta TNI	3	3	3	3
Pusinfolahta TNI	2	2	2	2
Pushansiber Kemhan	5	5	5	5
Pushansiber Kemhan	1	1	2	1
Pushansiber Kemhan	2	2	2	2
Pushansiber Kemhan	2	2	2	2
Pushansiber Kemhan	4	4	4	4
Pushansiber Kemhan	3	3	3	3
Pushansiber Kemhan	4	3	3	3
Pushansiber Kemhan	2	3	3	3
Pusdatin Kemhan	4	4	5	5
Pushansiber Kemhan	3	3	2	2
Pushansiber Kemhan	5	5	5	5
Pushansiber Kemhan	1	1	2	1

Pusdatin Kemhan	3	3	3	3
Pusdatin Kemhan	3	3	3	3
Pusdatin Kemhan	2	2	2	2
Pusdatin Kemhan	5	5	3	3
Pusdatin Kemhan	4	4	4	4
Pusdatin Kemhan	3	3	3	3
Pusdatin Kemhan	3	3	3	3
Pusdatin Kemhan	4	4	4	3
Pusdalops TNI	3	3	3	3
Pusdalops TNI	3	3	3	3
Pusdalops TNI	3	3	3	3
Pusdalops TNI	3	3	3	3
Pusdalops TNI	3	3	3	3

Lampiran 3 Jawaban Wawancara

1. Terkait dengan K4IPP, keamanan data dan informasi di (Nama lokus), apa saja yang menjadi ancaman baik dari internal maupun eksternal yang berpotensi mengganggu pertahanan siber (Nama lokus)?

   Pusinfolahta TNI :

   Yang menjadi ancaman internal pada keamanan data dan informasi di Pusinfolahta TNI diantaranya adalah berupa virus sedangkan yang menjadi ancaman eksternal yaitu berupa serangan siber terhadap server.

   Pusdalops TNI :

   a. Internal:
      1) *Human error*/manusia/personel; dan
      2) Peralatan/*Hardware*.

   b. External:
      1) Virus;
      2) *Malware*;
      3) *Hacker*; dan
      4) Penyadapan.

   Pusdatin Kemhan :

   Terkait keamanan data dan dan informasi di Pusdatin Kemhan terdiri atas tiga bidang yaitu:

   a. Infrastruktur;
   b. Pengembangan pengelolaan aplikasi;
   c. Pengamanan sistem informasi dan persandian

Adapun ancaman baik dari internal maupun eksternal yang berpotensi mengganggu pertahanan siber di pusdatin Kemhan sebagai berikut:

- Internal
    1) SDM (*Human failure*), harus bisa *security awareness* dalam setiap kegiatan, juga kemampuan pengawak dan administrator yang bertanggung jawab secara keseluruhan sistem di pusat data dan Informasi, harus bisa meminimalisir *human failure.*
    2) *Down time system*, diharapkan tidak terjadi putus jaringan yang cukup lama dan jika terjadi harus bisa diatasi secara langsung dan cepat.

Crash aplikasi yang *existing*, seluruh aplikasi dan jaringan serta pengamanan merupakan bagian dari pusdatin kemhan, sehingga dampak dari *corrupt* pada aplikasi mengakibatkan user tidak dapat mengakses dan membuat permasalahan yang serius, harus ada *back up* dan tim pemulihan yang tanggap.

- Eksternal
    1) Bencana alam, jika terjadi keadaan diluar kemampuan manusia maka harus disiapkan cara pemulihan data yang cepat dan sesuai S.O.P untuk memulihkan layanan semula.
    2) Serangan *hacker/cracker*, *Hacker* dan *Cracker* keduanya tetap melakukan tindakan yang melanggar aturan yaitu menembus pertahanan keamanan sistem komputer karena tidak mendapat hak akses.
    3) Sabotase/pencurian/penerobosan, melakukan serangan di infrastruktur perangkat keras, seperti memotong kabel FO (Fiber Optic), menerobos data center untuk mencuri, dll

Pushansiber Kemhan

- Ancaman Internal yang berpotensi mengganggu pertahanan siber di lingkungan Kemhan secara umum adalah kurangnya kesadaran tentang *security awareness.* Selain itu belum adanya *asset management*, serta kebijakan yang komprehensif tentang pertahanan siber. Hal terpenting yang juga merupakan faktor penting adalah terkait dengan kurang terdukungnya anggaran dalam pengelolaan pertahanan siber.
- Ancaman External yang berpotensi mengganggu pertahanan siber di Pushansiber Bainstrahan Kemhan adalah ancaman secara non-fisik seperti serangan *hacker, malware, virus, trojan horse* dan *ransomware*.

2. Dari jenis ancaman siber yang ada, manakah jenis ancaman yang paling banyak dan berbahaya bagi keamanan siber di (Nama Lokus)? (Dalam komunikasi data dengan alutsista, apakah sudah terintegrasi/interoperabiliti dengan Pusdalops)

Pusinfolahta TNI :

Yang paling banyak dan cukup berbahaya berupa virus. Virus tersebut dapat masuk menyerang diantaranya karena banyak komputer pengguna tidak dilengkapi dengan antivirus yang memadai sehingga pengamanannya hanya mengandalkan kemampuan dari firewall.

Pusdalops TNI :

Data yang terhubung belum bisa terintegrasi secara otomatis masih menggunakan pengiriman secara manual oleh operator.

Pusdatin Kemhan :

Serangan *hacker/cracker, hacker* dan c*racker* keduanya tetap melakukan tindakan yang melanggar aturan yaitu menembus pertahanan keamanan sistem komputer karena tidak mendapat hak akses, kenapa ini sangat berbahaya karena pihak yang diserang tidak mengetahui bahwa sistemnya telah dimasuki oleh pihak yang tidak berkepentingan serta dapat mengambil files maupun data yang berklasifikasi dan terus mengeksploitasi dalam sistem tersebut secara bebas.

Pushansiber Kemhan :

Berdasarkan data yang dikumpulkan dari Siaga Pushansiber, diperoleh data bahwa ancaman siber yang paling banyak menyerang adalah *Ransomware*. Hal ini didukung informasi dari para insinyur dan arsitek keamanan siber organisasi *McAfee Enterprise* serta *FireEye* yang baru saja bergabung, yang memperlihatkan cuplikan dari lanskap keamanan siber di tahun 2022, dan dampak yang mungkin ditimbulkan terhadap organisasi berbagai skala, pemerintahan di berbagai negara, dan juga masyarakat umum. *McAfee Enterprise* bersama *FireEye* mengumumkan prediksi ancaman siber di tahun 2022, yang mengulas ancaman-ancaman siber yang mungkin akan dihadapi berbagai organisasi/organisasi di dunia pada tahun mendatang.

3. Dalam mengembangkan infrastruktur K4IPP, keamanan siber (SIEM, SOC, Network/VPN, sensor, machine learning, big data, bandwith, SOP) di (Nama Lokus), permasalahan apa saja yang sering dihadapi dan resiko yang mungkin ditimbulkan?

Pusinfolahta TNI :

Permasalahan dalam monitoring keamanan siber dilingkungan Mabes TNI diantaranya adanya server dari suatu satker yang tidak ditempatkan di Pusinfolahta sehingga kewenangan dalam pengawasan menjadi tidak maksimal.

Pusdalops TNI :

a. Masalah yang sering dihadapi adalah:
   - *Hardware* (terjadi kerusakan *Boot Sector* pada Harddisk);
   - SDM/Manusia (kurangnya kemampuan personel dalam hal IT;
   - Jaringan (saat ini masih menggunakan pihak lain); dan
   - Keamanan data (belum terpasangnya *Secuirity cyber*).

b. Resiko yang mungkin ditimbulkan:
   - Kehilangan data akibat kerusakan *hardware*;
   - Kurangnya kemampuan personel yang mengakibatkan adanya kesalahan ketika kirim / terima data informasi
   - Ketika ada *trouble* pada *link* jaringan birokrasi untuk perbaikan menjadi lama
   - Kemungkinan data di *hack* dan disadap.

Pusdatin Kemhan :

Permasalahan yang sering dihadapi dan resiko yang mungkin ditimbulkan:

a. Dana anggaran, terkait budget anggaran yang dialokasikan sehingga menyesuaikan dengan kebutuhan di lapangan, resikonya tidak mendapatkan sistem yang terintegrasi secara maksimal

b. Pengawak SDM, dibutuhkan personel yang qualified serta memiliki sertifikasi yang mumpuni, jika tidak terpenuhi maka akan mengakibatkan permasalahan dalam operasional peralatan.
c. Perpanjangan *license*, masa berlaku peralatan yang telah tergelar hanya bisa menggunakan fungsi terbatas

Transfer teknologi, diharapkan ada pelatihan yang memberikan pemahaman yang utuh dan lengkap serta transfer teknologi kepada para personel pengawak

Pushansiber Kemhan :

Permasalahan yang paling sering dihadapi dalam mengembangkan infrastruktur keamanan siber adalah dikarenakan dalam penyelenggaraan infrastruktur jaringan internet dilaksanakan oleh Pusdatin Kemhan sehingga apabila terjadi perubahan terhadap jaringan yang ada maupun gangguan secara fisik terhadap infrastruktur jaringan internet akan berakibat tidak optimalnya perangkat infrastruktur keamanan siber. Selain itu Kendala dan tuntutan bagi Pushansiber dalam mengembangkan infrastruktur keamanan siber antara lain faktor keamanan informasi yang meliputi: a) kerahasiaan (*confidentiality*), b) keutuhan (*integrity*), dan c) ketersediaan (*availability*) dari informasi. Oleh karena hal tersebut, strategi implementasi harus meliputi Sistem Manajemen Keamanan Informasi atau *Information Security Management System* (ISMS) yaitu suatu pendekatan yang sistematis untuk mengelola dan mengamankan informasi yang bersifat rahasia dan sangat penting dalam organisasi, meliputi aspek Sumber Daya Manusia (*people*), prosedur standar (*process*), dan Sistem Teknologi Informasinya (*technology*).

4. Apakah ada gagasan lain yang diperlukan untuk menjaga keamanan data dan informasi serta pertahanan siber (Nama Lokus)? (*brainware, hardware, software, infrastrukturware, firmware, bugdetware*)?

Pusinfolahta TNI :

Dalam menjaga keamanan pertahanan siber di Pusinfolahta TNI yang terutama ada meningkatkan kemampuan dari sumber daya manusia, infrastruktur dan anggaran. Penempatan personel harus sesuai dengan kemampuannya agar tidak sekedar mengisi jabatan yang kosong agar dapat dicapainya profesionalitas dalam bekerja. Dalam pengembangan infrastruktur sebagian masih berdasarkan kebijakan. Keterbatasan anggaran mempengaruhi mempengaruhi pengadaan peralatan yang dipergunakan dalam operasional.

Pusdalops TNI :

- *Brainware* : harus memiliki kemampuan Programer, operator dan administrator sehingga Pusdalops TNI harus selektif dalam membina personel agar terwujudnya SDM yang berkualitas.
- *Hardware* : Mengikuti perkembangan IT yang berkembang saat ini;
- *Software* : Menggunakan Flatform yang bisa terintegrasi dengan perangkat lainnya dan mempermudah untuk operasional serta pengiriman data
- *Infrastrukturware* : Pusdalops TNI harus mempunyai Infrastrukturware yang memenuhi unsur-unsur seperti Komponen *Hardware*, komponen *Software*, Komponen Jaringan, komponen penyimpanan data dan komponen konsultasi integrasi ; dan
- *Firmware* : kedepan Pusdalops TNI harus memiliki *Firmware* yang betul-betul *Up To Date* karena ketika Hardware mengikuti

perkembangan IT maka Firmware juga harus sepadan karena sistem inilah yang mengendalikan perangkat keras/Hardware.

- *Bugdetware* : Penggunaan anggaran harus seefisien mungkin dengan tidak mengesampingkan kemampuan *Hardware* dan *Software* serta perangkat pendukung secara optimal.

Pusdatin Kemhan :

Diperlukan suatu sistem keamanan yang komprehensif dan sentralisasi sehingga seluruh peralatan Pusdatin akan termonitor dan terpantau jika terjadi gangguan dan tim *help desk* akan dapat memberikan perlindungan menyeluruh dan mengambil tindakan cepat dan terukur untuk menyelesaikan permasalahan.

Pushansiber Kemhan :

Konsep *people, process and technology*.

Untuk konsep *six-ware* di atas baru mencakup *people* dan *technology*, namun *process* juga sangat penting untuk diperhatikan karena tanpa adanya process dalam hal ini regulasi ataupun SOP maka proses berjalannya sistem pertahanan siber akan menjadi tidak terarah. Gagasan lain yang lebih implementatif adalah pembuatan perimeter sekuriti atau perimeter Internet. Perimeter ini memastikan akses Internet yang aman untuk para TNI dan PNS yang berada di lokasi dalam jangkauan jaringan organisasi, maupun yang sedang berada pada lokasi jauh (*remote*). Dalam rangka untuk memberikan keamanan tersebut, maka perimeter Internet harus dapat untuk:

a. Melakukan perutean (*routing*) lalu lintas antara organisasi dengan Internet

b. Mencegah file-file *executable* ditransfer melalui lampiran email atau penelusuran web

c. Memantau port-port jaringan internal dan eksterna untuk aktifitas-aktifitas mencurigakan

d. Mendeteksi dan memblokir lalu lintas dari titik-titik internal yang terinfeksi

e. Mengendalikan lalu lintas pengguna dengan Internet

f. Mengidentifikasi dan memblokir lalu lintas aneh dan paket-paket mencurigakan yang diduga berpotensi serangan

g. Mengeliminasi ancaman-ancaman seperti spam email, virus dan worm.

h. Mendorong penerapan kebijakan penyaringan untuk memblokir akses pada website-website yang mengandung malware atau konten-konten yang dicurigai atau meragukan keamanannya.

i. Disamping perimeter Internet, perlu juga diterapkan kontrol perimeter untuk *Virtual Private Network* (VPN), *Wide Area Network* (WAN) dan *Wireless Local Area Networks* (WLAN).

5. Apa sajakah hambatan dalam operasional pada keamanan data dan informasi K4IPP serta sistem pertahanan siber yang ada saat ini dan gagasan yang menjadi opsi penanganan dimasa yang akan datang?

Pusinfolahta TNI :

Hambatan saat ini dalam operasional pertahanan siber yaitu berupa aturan ataupun dasar hukum mengenai pelibatan dalam suatu operasi militer. Dimana saat ini masih hanya berlaku pada operasi milter selain perang (OMSP) sedangkan perkembangan zaman dan situasi telah yang telah melibatkan peperangan siber.

Pusdalops TNI :

a. Hambatan:

- *Hardware;*
- *Software;*
- SDM; dan
- Jaringan.

b. Gagasan untuk di masa mendatang:

- Mengikuti perkembangan IT secara *Up to Date*
- Penggunaan Software harus bisa terintegrasi dengan perangkat lain serta mudah dalam mengoperasionalkan.
- Meningkatkan pembinaan personel sehingga terwujud SDM yang berkualitas
- Pemasangan *Cyber Security* dan penggunaan jaringan sendiri.

Pusdatin Kemhan

Kurangnya SDM yang mampu menangani ancaman siber dan yang memiliki kemampuan teknis yang merata.

Pushansiber Kemhan

Hambatan yang selama ini dialami dalam operasional pertahanan siber yaitu:

- *Budgetware*, dimana anggaran yang ada hanya mencakup belanja operasional sedangkan perangkat yang ada sudah kurang mumpuni bila dihadapkan dengan perkembangan teknologi.
- *Process*, dimana regulasi maupun SOP yang mendukung kegiatan pertahanan siber belum tergelar secara optimal
- *Brainware*, dari DSP yang ada, Pushansiber masih sangat kurang untuk tenaga yang ekspertis seperti security analyst.

Gagasan lain yang dilakukan oleh Kementerian Pertahanan antara lain dengan membentuk Tim Kerja Pusat Operasi Dunia Maya (*Cyber Defence Operation Centre*), yang bertujuan untuk mempertahankan keamanan dan perlindungan internal (Kemenhan) maupun eksternal (nasional) dari berbagai serangan siber.

6. Bagaimana arsitektur keamanan data (Nama Lokus) yang ideal dalam pertahanan siber (Nama Lokus)?

Pusinfolahta TNI :

Saat ini di Pusinfolahta belum memiliki ruangan data *center*, yang sudah ada hanya berupa ruang server sehingga masih belum maksimal dalam monitoring seluruh server dan aplikasi dilingkungan Mabes TNI.

Pusdalops TNI :

- Integrasi dengan *Cyber Security* untuk pengamanan data;
- Mempunyai server sendiri;
- Pemasangan server *Redundant*; dan
- *Update* Antivirus.

Pusdatin Kemhan :

Arsitektur keamanan data Pusdatin yang ideal dengan mengamankan jalur FO dengan secure gateway dan VPN serta menerapkan standar keamanan yang terintegrasi di data center Pusdatin Kemhan.

Pushansiber Kemhan :

Peningkatan penggunaan jaringan Internet menyebabkan beragamnya pemakai di jaringan Internet, sehingga praktisi lapangan serta teknologi yang dipakai tidak mampu melindungi sistem dari serangan orang iseng

atau yang memang punya niat negatif. Untuk melindungi jaringan komputer di dalam jaringan, solusinya adalah dengan mengimplementasikan peranti yang mampu melindungi sistem dengan baik. Peranti tersebut tetap tidak akan bermanfaat jika tidak ada staf yang selalu memantau jaringan dan secepat mungkin mencegah penyerangan serta memperkecil resiko kerusakan jaringan komputer.