2020

LAPORAN

HASIL PENILAIAN

CYBER SECURITY MATURITY (CSM)

DINAS KOMUNIKASI DAN INFORMATIKA
PROVINSI DAERAH ISTIMEWA YOGYAKARTA

PENDAHULUAN

I. Tujuan Kegiatan

Kegiatan ini bertujuan untuk mengetahui tingkat maturitas keamanan siber di lingkungan Dinas Komunikasi dan Informatika Provinsi Daerah Istimewa Yogyakarta. Dengan adanya tingkat maturitas ini diharapkan dapat memberikan gambaran mengenai apa yang harus menjadi tindak lanjut baik oleh *stakeholder* maupun Badan Siber dan Sandi Negara (BSSN) untuk meningkatkan maturitas keamanan siber.

II. Ruang Lingkup Kegiatan

Kegiatan yang dilaksanakan meliputi pemetaan aspek penanganan insiden meliputi :

1. Aspek Tata Kelola
2. Aspek Identifikasi
3. Aspek Proteksi
4. Aspek Deteksi
5. Aspek Respon

III. Metodologi Kegiatan

Metodologi yang digunakan berdasarkan hasil pengisian instrumen *Cyber Security Maturity* (CSM), wawancara/diskusi, dan melihat ketersediaan dokumen keamanan siber. Hasil diberikan dalam bentuk Indeks Kematangan, Level Kematangan dan bagan berbentuk radar yang menjelaskan maturitas setiap aspek keamanan siber.

Penentuan Level Kematangan diukur berdasarkan Indeks Kematangan yang didapat. Konversi Indeks Kematangan menjadi Level Kematangan menggunakan formula:

$$Level\ Kematangan\ (\%) = \frac{Indeks\ Kematangan}{5}\ x\ 100\%$$

Nilai Level Kematangan dikategorikan menjadi :

- Level 1 (*Initial*) : Penerapan keamanan siber tidak ada proses yang terorganisir, bersifat informal, tidak dilakukan secara konsisten, dan tidak dilakukan secara berkelanjutan.
- Level 2(*Repeatable*): Penerapan keamanan siber proses yang dilakukan sudah terorganisir, bersifat informal, dilakukan secara berulang namun belum konsisten, serta belum dilakukan secara berkelanjutan.
- Level 3 (*Defined*) : Penerapan keamanan siber proses yang dilakukan sudah terorganisir dengan jelas, bersifat formal, dilakukan secara berulang, dilakukan reviu berkala, dan konsisten. Namun penerapan perubahan belum dilakukan secara berkelanjutan.
- Level 4 (*Managed*) : Penerapan keamanan siber proses yang dilakukan sudah terorganisir dengan baik namun belum dilakukan proses otomatisasi, bersifat formal, dilakukan secara berulang dan direviu secara berkala, serta implementasi perbaikan dilakukan secara berkelanjutan.
- Level 5 (*Optimized)*: Penerapan keamanan siber proses yang dilakukan sudah terorganisir dengan baik, diterapkan proses otomatisasi, bersifat formal, dilakukan secara berulang secara konsisten, direviu berkala, serta penerapan perbaikan dilakukan secara berkelanjutan.

IV. Pelaksanaan Kegiatan

1. Pengisian Instrumen CSM oleh internal stakeholder (*self assessment*)

   Pengisian Instrumen oleh internal stakeholder dilakukan pada 7 Desember 2020.

2. Validasi Pemetaan CSM

   Validasi Pemetaan CSM dilaksanakan untuk pengecekan hasil *self assessment* isian instrumen. Kegiatan validasi dilakukan dengan metode wawancara/diskusi dan melihat ketersediaan dokumen keamanan siber. Kegiatan validasi dilaksanakan pada 8 Desember 2020.

HASIL KEGIATAN

I. Informasi *Stakeholder*

Nama Instansi/Lembaga : Diskominfo Provinsi D.I. Yogyakarta
Alamat : Jl. Brigjen Katamso, Keparakan, Kec. Mergangsan, Kota Yogyakarta, D.I. Yogyakarta 55152
Nomor Telp./Fax. : (0274) 373444
Email : diskominfo@jogjaprov.go.id
Narasumber Instansi/Lembaga :

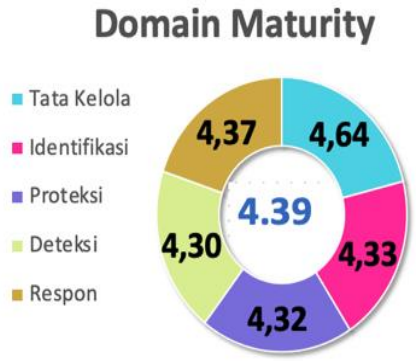
1. Dr. Sayuri Egaravanda, S.Kom., M.Eng.
   Kepala Bidang Keamanan Informasi dan Persandian
2. Anik Budiati, S.Kom., M.Eng.
   Kepala Seksi Keamanan Informasi
3. Raden Setya Legawa, S.IP
   Kepala Seksi Persandian
4. Mohamad Zainuri, S.Kom., M.Eng.

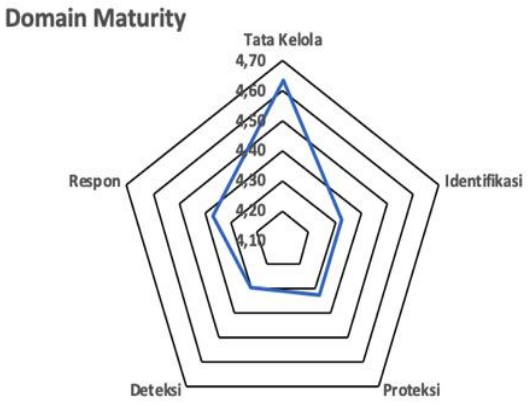
II. Deskripsi Ruang Lingkup Penilaian

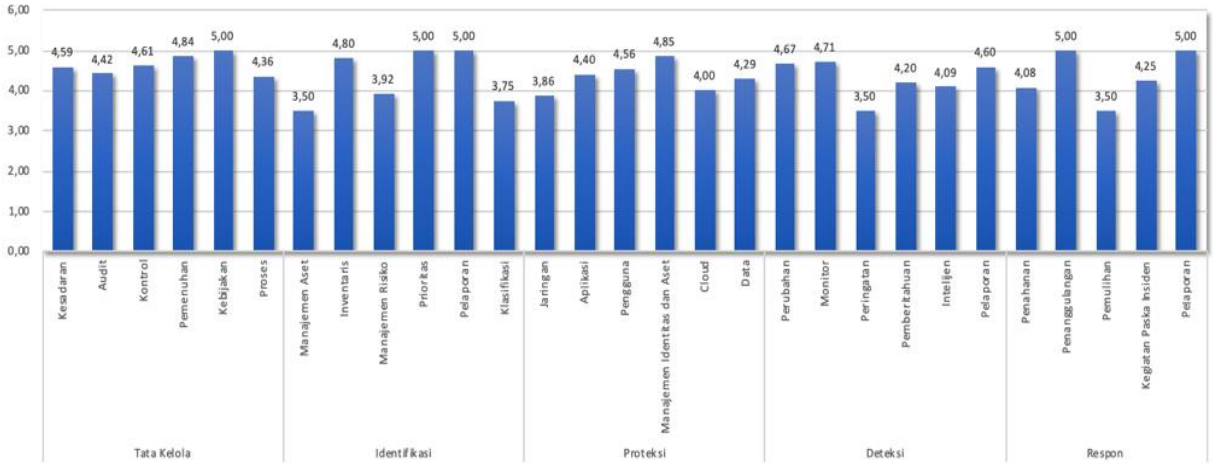
1. Ruang Lingkup Penilaian :
   ☐ Organisasi Keseluruhan ☐ Regional, Kanwil, Cabang √ Unit Kerja ☐ Lainnya
2. Instansi/Unit Kerja* : Dinas Komunikasi dan Informatika Provinsi D.I. Yogyakarta

III. Hasil Penilaian CSM

Tata Kelola		Identifikasi		Proteksi		Deteksi		Respon	
4,64		4,33		4,32		4,30		4,37	
Kesadaran	4,59	Manajemen Aset	3,50	Jaringan	3,86	Perubahan	4,67	Penahanan	4,08
Audit	4,42	Inventaris	4,80	Aplikasi	4,40	Monitor	4,71	Penanggulangan	5,00
Kontrol	4,61	Manajemen Risiko	3,92	Pengguna	4,56	Peringatan	3,50	Pemulihan	3,50
Pemenuhan	4,84	Prioritas	5,00	Manajemen Identitas dan Aset	4,85	Pemberitahuan	4,20	Kegiatan Paska Insiden	4,25
Kebijakan	5,00	Pelaporan	5,00	Cloud	4,00	Intelijen	4,09	Pelaporan	5,00
Proses	4,36	Klasifikasi	3,75	Data	4,29	Pelaporan	4,60		
LEVEL MATURITAS					4,39				







Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut:

Total Score Kematangan: 4,39

Sehingga perhitungan penentuan Level Kematangan didapatkan level kematangan sebagai berikut :

Level Kematangan Tingkat IV+

IV. Kekuatan/Kematangan

Berdasarkan hasil validasi penilaian kematangan keamanan siber (*Cyber Security Maturity*), dapat disimpukan kondisi kekuatan keamanan siber pada Dinas Komunikasi dan Informatika Provinsi D.I. Yogyakarta sebagai berikut:

Aspek Tata Kelola

1. Organisasi telah memilik program kesadaran keamanan informasi yang telah dilakukan dan direview secara berkala.
2. Peningkatan kompetensi keamanan informasi telah terjadwal.
3. Organisasi telah memberikan pelatihan kepada karyawan tentang *secure authentication, social engineering, pengelolaan data sensitive*.
4. Organisasi telah melakukan manajemen kerentanan siber.
5. Organisasi telah melakukan pemeriksaan background pada karyawan baru.
6. Organisasi telah memiliki *tool vulnerability scanning* secara mandiri.
7. Organisasi menggunakan akun khusus untuk melakukan *vulnerability scanning*, dan akan dihapus jika sudah tidak terpakai.
8. Organisasi telah memiliki *risk assessment, risk treatment*, internal audit keamanan informasi.
9. Organisasi telah memiliki WAFs, *firewall* pada *end user*, NAT, DMARC, *filter* terhadap seluruh jenis file lampiran *email*.

10. Organisasi telah melakukan konfigurasi *firewall* secara berkala dan telah didokumentasikan.
11. *Vulnerability assessment* dan *penestration testing* telah dilakukan dengan melibatkan pihak internal dan eksternal.
12. Organisasi sudah memiliki gap analisis kemampuan sehingga organisasi tidak dapat membuat baseline pelatihan keamanan informasi.
13. Organisasis sudah memiliki pelatihan secure code untuk personel yang terlibat dalam pengembangangan aplikasi.
14. Organisasi sudah memiliki kebijakan terkait perlindungan data pribadi.
15. Organisasi sudah mereviu izin akses dari akun pengguna.
16. Organisasi sudah memiliki red team dan blue team.
17. Organisasi sudah memiliki pemisahan environment antara sistem production dan development.
18. Organisasi sudah menggunakan DLP (Data Loss Prevention) atau NAC (Network Access Control).
19. Organisasi sudah menerapkan metode sandbox terhadap seluruh lampiran email guna mencegah dan analisis keamanan lebih lanjut terhadap malicious behaviour.
20. Organisasi Anda suah memiliki kebijakan yang menetapkan sanksi yang dijatuhkan terhadap karyawan yang tidak patuh pada kebijakan yang berkaitan dengan keamanan siber.
21. Organisasi sudah memiliki kebijakan terkait SSO dan tenggat waktu kadaluarsa sebuah akun.

Aspek Identifikasi

1. Organisasi telah melakukan manajemen aset secara optimal, dengan menerapkan update perencanaan kapasitas dan *update patch* terhadap semua aset.
2. Organisasi telah melakukan inventarisasi data yang ada pada semua aset perangkat keras maupun perangkat lunak. Dan aset yang diidentifikasi telah disusun berdasarkan klasifikasi kritikalitas.
3. Organisasi telah melakukan manajemen resiko berupa retensi data sensitif.
4. Aspek keamanan mempertimbangkan kapasitas *server* dan perangkat jaringan secara menyeluruh.
5. Organisasi telah memiliki standar untuk melakukan klasifikasi *cyber threat*.
6. Organisasi sudah memiliki system configuration management tools untuk otomatisasi konfigurasi perangkat keras dan perangkat lunak.
7. Aset yang diidentifikasi sudah dilakukan klasifikasi kritikalitas dan sudah ditetapkan siapa penanggungjawabnya.
8. sudah dilakukan identifikasi maupun pembatasan akses perangkat yang tidak diizinkan.
9. Analisis keterkaitan antara keamanan dan kenyamanan dari pengguna aset perangkat dan aplikasi sudah dilakukan dalam rangkan penyusunan standar keamanan informasi.
10. sudah ada kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.
11. Karyawan tidak diiizinkan memiliki akses sebagai administrator pada perangkat (laptop, personal computer, dll) milik organisasi.
12. Pihak ketiga tidak diizinkan untuk menggunakan aset mereka pada jaringan organisasi.
13. sudah ada dokumentasi mengenai alur informasi yang memproses data stakeholder termasuk yang dikelola oleh pihak ketiga.
14. Pemrosesan data stakeholder (dicatat, dimonitoring, dilaporkan) sudah dilakukan reviu.

15. Organisasi sudah menon-aktifkan aset perangkat dan aplikasi yang tidak diperlukan.
16. Risk Register sudah didokumentasikan untuk semua aplikasi.
17. Organisasi sudah memperbaharui roadmap keamanan TI organisasi dalam jangka waktu tertentu.
18. Organisasi sudah memiliki Business Impact Analysis terhadap perangkat dan aplikasi TI.
19. Organisasi sudah memiliki metode/standar klasifikasi aset TI dan cyber threats yang ditemukan.
20. Organisasi sudah memprioritaskan Langkah proteksi keamanan siber dalam perlindungan data dan aset kritis.

Aspek Proteksi

1. Penggunaan IDS dan IPS dengan menggunakan Sangfor.
2. Memanfaatkan sistem enkripsi dalam akses nirkabel.
3. Koneksi ke *server* dan jaringan sudah menggunakan protocol enkripsi.
4. Penggunaan *firelwall* telah di konfigurasi dengan baik seperti *implicit* atau *explicit deny any/any rule, inbound network traffic* dan *outbound network traffic*.
5. Sudah menggunakan DNS *Filtering*.
6. Beberapa aplikasi sudah mulai dilakukan pemisahan sebagian besar *server* fisik maupun virtual.
7. Pada *email system* dilakukan pengecekan secara otomatis terhadap *spam/phishing/malware* menggunakan *magic spam* dan *mail server*
8. Sudah ada *white list* aplikasi dalam memastikan *authorized software library* dan *signed script*.
9. Sudah dilakukan *updating* secara berkala dalam penggunaan *web browser*, dan *email client* dalam organisasi;

10. Sistem manajemen identitas dan akses telah digunakan untuk seluruh sistem operasi.
11. *Multi-Factor Authentication* (MFA) telah digunakan pada akses LAN dan VPN serta untuk mengakses data sensitive (dengan menggunakan otentikasi dan captcha).
12. Penggunaan *password* telah digunakan pada semua akses login dan dilakukan penggantian berkala secara manual.
13. Penggunaan akses data telah diatur hak akses dan penerapan *white list* untuk memverifikasi alamat IP yang mempunyai hak akses.
14. Anomali transaksi oleh karyawan/stakeholder/klien dapat diidentifikasi dan dilakukan pelacakan/pendeteksian.
15. Organisasi sudah memiliki *cloud* internal yang memiliki proses otorisasi.
16. Data penting telah dilakukan *backup* secara berkala.
17. Penyimpanan log sudah dilakukan dalam rangka audit dan forensik.
18. Penyimpanan data *backup* sudah dilindungi baik secara fisik dan non fisik.
19. Perangkat jaringan belum menggunakan otentifikasi terpusat.
20. Inbound network traffic belum di filter untuk memeriksa malware dan mencegah eksplotasi terhadap kerentanan.
21. Organisasi sudah menerapkan port access control sebagai pengendalian terhadap otentifikasi perangkat yang terhubung ke jaringan.
22. Sudah diterapkan firewall filtering antar segmen jaringan local.
23. Sudah ada pembatasan aplikasi yang diunduh, diinstal, dan dioperasikan.
24. Sudah dilakukan pembatasan penggunaan scripting tools.
25. Master image sudah dilakukan penyimpanan.
26. Sudah ada batasan fitur auto-run content dan pengaturan akses read/write pada perangkat USB.
27. Semua perangkat endpoints termasuk server sudah menggunakan antivirus.
28. Informasi identitas dan akses pengguna sudah digunakan untuk membatasi hak akses dari dalam jaringan.
29. Sudah ada penerapan SSO, pembatasan IP dan MMA pada akses cloud.

30. Sudah ada Data Center Redudancy terkait cloud yang ada di organisasi.
31. Organisasi belum memiliki kebijakan penanganan insiden dan selaras dengan kebijakan pengaturan kesinambungan organisasi atau business continuity planning (BCP).
32. Organisasi belum memiliki skema penilaian insiden dan prioritas berdasarkan potensial dampak.
33. Organisasi belum melakukan reviu terhadap rekap laporan insiden siber yang pernah terjadi untuk melihat apakah prosedur insiden respon sudah sesuai dengan standar yang ditetapkan.
34. Organisasi belum merancang standar terkait waktu yang diperlukan bagi administrator sistem dan karyawan lainnya untuk melaporkan kejadian yang tidak wajar kepada tim penanganan insiden, mekanisme pelaporan tersebut, dan jenis informasi yang harus dimasukkan dalam pemberitahuan insiden.

Aspek Deteksi

1. Organisasi melakukan *monitoring* terhadap *log* dari perangkat *security control*, jaringan, dan aplikasi selama 24 jam.
2. Organisasi Anda mengaktifkan *Enable Detailed Logging* yang mencakup informasi terperinci seperti *event source*, tanggal, *user*, *timestamp*, *source addresses*, *destination addresses*, dan komponen lainnya.
3. Setiap orang yang tergabung dalam tim *monitoring* pada organisasi mendapatkan peningkatan keterampilan.
4. Organisasi memantau akses fisik terhadap perangkat yang berada di dalam ruangan data center untuk mendeteksi potensi kejadian keamanan siber.
5. Organisasi memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal.
6. Organisasi memiliki *contact tree* untuk mengeskalasi dalam merespon suatu kejadian.

7. Organisasi telah memiliki mekanisme *sharing* informasi baik internal maupun eksternal.
8. Organisasi telah memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat untuk menangani kejadian prioritas tinggi dan mampu mendeteksi anomali.
9. Organisasi sudah memiliki Change Advisory Board (CAB).
10. Organisasi memiliki mekanisme monitoring terhadap akses dan perubahan pada data sensitif (seperti File Integrity Monitoring atau Event Monitoring).
11. Organisasi memiliki mekanisme monitoring dan deteksi terhadap penggunaan enkripsi yang tidak sah.
12. Organisasi memiliki sistem untuk memonitoring dan mencegah kehilangan data sensitif.
13. Organisasi sudah menerapkan SIEM atau Log Analytic Tools untuk keperluan dokumentasi, korelasi, dan analisis log
14. Organisasi sudah dapat mendeteksi Wireless Access Point yang terhubung ke jaringan LAN.
15. Organisasi sudah menjamin alokasi kapasitas penyimpanan log sesuai dengan kebutuhan.
16. Organisasi memantau aktifitas pihak ketiga untuk mendeteksi adanya potensi kejadian keamanan siber.
17. Organisasi sudah memiliki ticketing system untuk melacak progress suatu kejadian.
18. Organisasi sudah menerapkan event notification yang berbeda-beda untuk setiap jenis eskalasi.
19. Organisasi memperoleh informasi dari multiple threat intelligence feeds untuk mendeteksi serangan siber.
20. Organisasi menjalankan vulnerability scanning tools secara otomatis untuk mendeteksi kerentanan siber.
21. Organisasi sudah memiliki Metrik Security Event.

Aspek Respon

1. Organisasi memiliki SOP pelaporan insiden, SOP penanganan insiden, dan *disaster recovery plan* yang telah direview secara berkala.
2. Organisasi melakukan simulasi penanganan insiden kepada karyawan secara rutin.
3. Organisasi memiliki rencana respon insiden dan daftar kontak tim penanganan insiden internal dan eksternal.
4. Organisasi mendesain jaringan yang dapat memastikan apabila *server* DMZ terkena serangan siber, penyerang tidak dapat mengakses server yang lain.
5. Tim respon insiden telah memiliki peralatan sumber daya analisis insiden (misalkan *packet sniffer*, diagram jaringan, alat digital forensik, dll).
6. Ketika organisasi mengalami insiden, tim respon insiden dengan mudah mendapat bantuan dari rim manajemen kritis.
7. Hasil review dan rekap laporan pengangan insiden telah dilaporkan ke *top management*.
8. Laporan insiden di organisasi Anda dilaporkan ke *top management* dan ke pihak eksternal yang berkepentingan/wajib dilaporkan sesuai regulasi.

V. Kelemahan/Kekurangan

Berdasarkan hasil validasi penilaian kematangan keamanan siber (*Cyber Security Maturity*), dapat disimpukan kondisi kelemahan/kekurangan keamanan siber pada Dinas Komunikasi dan Informatika Provinsi D.I. Yogyakarta sebagai berikut:

Aspek Tata Kelola

1. Organisasi belum mengimplementasikan anti virus dan anti malware pada *end point* secara terpusat.

Aspek Identifikasi

1. Organisasi belum melakukan Vulnerability Scanning dan atau Penetration Testing terhadap semua perangkat dan aplikasi.

Aspek Proteksi

1. Organisasi belum melakukan *disable peer-to-peer* pada *wireless client* di perangkat *endpoint*.
2. Belum memanfaatkan metode otentikasi pada saluran yang terenkripsi dan juga penambahan OTP.
3. Organisasi belum menonaktifkan kounikasi antar workstation untuk mencegah potensi terjadinya serangan siber dalam satu jaringan yang sama
4. Organisasi belum memastikan penggunaan add-on dan plugin aplikasi sudah sesuai dengan ketentuan atau belum
5. Organisasi belum menggunakan *Next Generation Endpoint Protection*, hanya menggunakan anti virus.

Aspek Deteksi

1. Organisasi belum memiliki sistem untuk melakukan Malicious Code Detection untuk mendeteksi, menghapus, dan melindungi dari Malicious Code.
2. Log hasil hasil deteksi malware belum terhubung dengan perangkat anti malware administration dan event log server sehingga dapat digunakan untuk log analysis.
3. Organisasi memiliki perangkat anti-malware tapi belum secara otomatis melakukan scanning terhadap removable media yang terhubung ke perangkat.
4. Organisasi belum menyimpan semua log terhadap url yang diakses oleh karyawan.
5. Threat Intellegence feeds belum dikonfirmasi secara otomatis untuk memperbarui kontrol pencegahan, seperti pembaruan signature IPS, Update Rules, dan konfigurasi linnya.
6. Organisasi belum melakukan *vulnerability scanning* secara otomatis menggunakan aplikasi yang diinstall pada *endpoint*.
7. Organisasi belum mengaktifkan *DNS Query logging* dalam mendeteksi *hostname lookups* untuk mengetahui adanya *malicious domain*.

Aspek Respon

1. Organisasi belum melaksanakan pelatihan respon insiden yang mencakup pengujian saluran komunikasi, pengambilan keputusan, dan kemampuan teknis pelaporan insiden dengan menggunakan alat dan data yang tersedia..
2. Organisasi belum melakukan backup data pada aptop karyawan ke cloud.

VI. Rekomendasi

1. Untuk meningkatkan aspek tata Kelola, organisasi diharapkan:
   a. Menerapkan anti virus dan anti *malware* pada *end point* secara terpusat.

2. Aspek Identifikasi dapat ditingkatkan dengan hal-hal sebagai berikut:
   a. Organisasi turut serta menerapkan kebijakan *Penetration Testing* terhadap semua perangkat dan aplikasi yang digunakan selain mekanisme *Vulnerability Scanning* yang sudah berjalan.

3. Untuk meningkatkan Aspek Proteksi dapat dilakukan dengan cara:
   a. Organisasi melakukan *disable peer-to-peer* pada *wireless client* di perangkat *endpoint*.
   b. Organisasi memanfaatkan metode otentikasi pada saluran yang terenkripsi dan juga penambahan OTP.
   c. Organisasi membatasi atau menonaktifkan komunikasi antar *workstation* untuk mencegah potensi terjadinya serangan siber dalam satu jaringan yang sama
   d. Organisasi menerapkan *Next Generation Endpoint Protection* yang tidak terbatas pada penggunaan anti virus.

4. Aspek Deteksi ditingkatkan dengan hal-hal berikut:
   a. Penerapan koneksitas Log hasil deteksi malware dengan perangkat anti malware administration dan event log server.
   b. Penyimpanan semua log terhadap url guna mendukung proses investigasi.
   c. Penerapan otomatisasi *Threat Intellegence feeds* untuk memperbarui kontrol pencegahan, seperti pembaruan *signature IPS*, *Update Rules*, dan konfigurasi linnya.
   d. Pengaktifkan *DNS Query logging* dalam mendeteksi *hostname lookups* untuk mengetahui adanya *malicious domain*.

5. Aspek Respon ditingkatkan dengan cara:
   a. Pemrograman dan pelaksanaan pelatihan respon insiden siber yang mencakup pengujian saluran komunikasi, pengambilan keputusan, dan kemampuan teknis pelaporan insiden dengan menggunakan alat dan data yang tersedia.
   b. Penyediaan *Space Storage* yang cukup untuk penyimpanan hasil *backup* data dinas yang tersimpan pada Komputer Pegawai.

PENUTUP

Demikian disampaikan laporan kegiatan penilaian maturitas keamanan siber pada Dinas Komunikasi dan Informatika Pemerintah Provinsi D.I. Yogyakarta, sebagai bahan masukkan bagi pimpinan dalam menentukan kebijakan lebih lanjut.

Yogyakarta, 10 Desember 2020

Kepala Bidang Keamanan Informasi dan Persandian	Kepala Subdirektorat Penanggulangan dan Pemulihan Pemerintah Daerah Wilayah II
	Ditandatangani secara elektronik oleh : KASUBDIT PPPDW II, DEPUTI III **Agustinus Toad, S.E.** Pembina (IV/a)
Dr. Sayuri Egaravanda, S.Kom., M.Eng	Agustinus Toad, S.E