Modul Pelatihan

JUNIOR CYBER SECURITY

Vocational School Graduate Academy
Digital Talent Scholarship
Tahun 2023

KATA PENGANTAR

Dunia saat ini berada pada era industri 4.0 yang lebih banyak menggunakan teknologi digital dan Indonesia telah mempersiapkan diri untuk masuk ke dalam tahap industri 4.0 tersebut melalui agenda percepatan transformasi digital. Salah satu langkah yang dilakukan dalam percepatan transformasi digital adalah penyiapan talenta digital. Laporan Bank Dunia tahun 2019 menyatakan bahwa Indonesia memiliki kekurangan 9 juta pekerja berketerampilan teknologi informasi dan komunikasi, sehingga perlu dilakukan penyiapan talenta digital untuk memenuhi kebutuhan tersebut dengan alokasi 600.000 orang setiap tahun. Upaya penyiapan talenta digital dilakukan oleh berbagai unsur baik pemerintah, institusi pendidikan, industri, komunitas masyarakat, maupun media publik.

Sejak tahun 2018, Kementerian Komunikasi dan Informatika melalui Badan Penelitian dan Pengembangan Sumber Daya Manusia menginisiasi Program Beasiswa Pelatihan Digital bernama *Digital Talent Scholarship* (DTS) yang telah berhasil dianugerahkan kepada lebih dari 300.000 penerima pelatihan bidang teknologi informasi dan komunikasi. Program *Digital Talent Scholarship* ini ditujukan untuk memberikan pelatihan dan sertifikasi berbagai tema pada bidang informatika, komunikasi, dan telekomunikasi, serta diharapkan melengkapi pemenuhan kebutuhan talenta digital Indonesia.

Program DTS tahun 2023 secara garis besar dibagi menjadi delapan akademi, salah satunya Vocational School Graduate Academy (VSGA). VSGA merupakan program pelatihan berbasis kompetensi kerja nasional bagi lulusan pendidikan vokasi SMK/sederajat dan diploma bidang *Science, Technology, Engineering, Mathematics* (STEM) yang belum mendapatkan pekerjaan atau sedang tidak bekerja. Tujuan Program VSGA adalah menyiapkan talenta digital dengan standar kompetensi sesuai Standar Kompetensi Kerja Nasional Indonesia (SKKNI). Oleh karena itu, penyusunan modul pelatihan untuk Program VSGA disusun dengan berbasis pada kompetensi (*Competency Based Training*). Kami berpesan agar modul pelatihan berbasis kompetensi yang telah disusun ini dapat menjadi referensi bagi peserta dan pengajar agar pelatihan berjalan efektif dan efisien.

Selamat mengikuti Pelatihan *Digital Talent Scholarship*, mari persiapkan diri kita menjadi talenta digital Indonesia yang kompeten.

Jakarta, April 2023
Kepala Badan Penelitian dan Pengembangan Sumber Daya Manusia
Kementerian Komunikasi dan Informatika Republik Indonesia

Dr. Hary Budiarto, M.Kom

Pendahuluan

Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam dalam melaksanakan kebijakan keamanan informasi untuk pencegahan, deteksi, dan pengelolaan ancaman keamanan siber.

A. Tujuan Umum

Setelah mempelajari modul ini peserta latih diharapkan mampu dalam melaksanakan kebijakan keamanan informasi dengan benar.

B. Tujuan Khusus

Adapun tujuan mempelajari unit kompetensi melalui buku modul alam mengumpulkan data ini guna memfasilitasi peserta latih sehingga pada akhir pelatihan diharapkan memiliki kemampuan sebagai berikut:

1. Mengidentifikasi aset penting dalam organisasi.
2. Memproteksi aset penting dalam organisasi.
3. Melakukan pemantauan terhadap aktivitas yang rentan ancaman.

Latar belakang

Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengumpulkan data untuk data science. Penilaian dilakukan dengan mengacu kepada Kriteria Unjuk Kerja (KUK) dan dilaksanakan di Tempat Uji Kompetensi (TUK), ruang simulasi atau workshop dengan cara:

1.1 Lisan
1.2 Wawancara
1.3 Tes tertulis
1.4 Demonstrasi
1.5 Metode lain yang relevan.

Deskripsi Pelatihan

Materi Pelatihan ini memfasilitasi pembentukan kompetensi dalam menentukan kebutuhan teknis pelaksanaan kebijakan keamanan informasi.

Tujuan Pembelajaran

Setelah mengikuti pelatihan ini, peserta mampu menentukan kebutuhan teknis pelaksanaan kebijakan keamanan informasi.

Kompetensi Dasar

Mampu menentukan kebutuhan teknis pelaksanaan kebijakan keamanan informasi.

Indikator Hasil Belajar

Ketepatan dalam melakukan proses pengambilan data sesuai dengan tools yang telah disiapkan

INFORMASI PELATIHAN

INFORMASI PELATIHAN	
Akademi	VSGA untuk Junior Cyber Security
Mitra Pelatihan	
Tema Pelatihan	***Junior Cyber Security***
Sertifikasi	Sertifikasi kompetensi BNSP *Junior Cyber Security*
Deskripsi Pelatihan	Pelatihan ini menyiapkan peserta agar kompeten dalam melaksanakan pekerjaan *junior cyber security* yang dapat membantu pekerjaan praktisi *cyber security.* Kualifikasi pada jabatan ini menuntut seseorang memiliki kompetensi dalam menerapkan prinsip perlindungan informasi, menerapkan prinsip keamanan informasi untuk penggunaan jaringan internet, menerapkan prinsip keamanan informasi pada transaksi elektronik, melaksanakan kebijakan keamanan informasi, mengaplikasikan ketentuan/persyaratan keamanan informasi , mengelola log, dan menerapkan kontrol akses berdsarkan konsep/metodologi yang telah ditetapkan
Output Pelatihan	Setelah mengikuti pelatihan peserta akan mampu menganalisis dan memvisualisasikan data sehingga dapat digunakan dalam pengambilan keputusan
Durasi Pelatihan	24 JP (3 hari)

INFORMASI PELATIHAN	
Jenis Pelatihan	**Luring */Offline* (40% Pengetahuan - 60% Praktek)**
Persyaratan Peserta	● Warga Negara Indonesia ● Usia Maksimal 29 Tahun pada saat mendaftar ● Lulus Pendidikan D3 Bidang TIK/SMK Bidang (TKJ/TI/RPL) yang pernah bekerja minimal 3 tahun ● Belum Mendapatkan Pekerjaan Tetap/Pernah Bekerja tapi sedang tidak bekerja ● Lolos Seleksi Administrasi dan Tes Substansi
Persyaratan Sarana Peserta	Laptop/PC dengan spesifikasi: ● RAM minimal 4 GB ● 32/64-bit processor ● Operating System Windows 7,8,10, Linux, atau MAC OSX ● konektivitas WiFi ● Akses Internet Dedicated 256 kbps per peserta per perangkat
Kriteria Pengajar/*Trainer*/ Instruktur:	1. Minimal Lulusan S2 di bidang TIK; atau Memiliki kompetensi Okupasi Nasional "*Junior Cyber Security*". 2. Pengalaman Kerja diutamakan sebagai tenaga pengajar Pelatihan Bidang TIK minimal selama 2 tahun 3. Telah mengikuti pelatihan *training of trainner Junior Cyber Security*
Tim Penyusun:	1. Yan Hadynoer (BSSN) 2. Yoyok Darmanto (BSSN)

INFORMASI PEMBELAJARAN

RENCANA PELATIHAN		
Pertemuan	**Topik**	**Aktivitas**
Hari 1	● Pembukaan dan Penjelasan Rencana Pembelajaran ● Pre test	Pemaparan materi, diskusi dan *hands-on lab live class* 1 JP
	Pengantar *Junior Cyber Security* (Posisi dan peran *junior cyber security)*	Pemaparan materi, diskusi dan *hands-on*

		lab live class 1 JP
	Persiapan alat bantu (tools) pelatihan - Python (Jupiter) kenalkan dengan yang online; numpy, pandas, matplotl, seaborn, folium - MySql (XAMPP)	Pemaparan materi, diskusi dan *hands-on lab live class* 1 JP
	Menerapkan prinsip perlindungan informasi 1. Mendefinisikan prosedur keamanan informasi yang tepat untuk tiap klasifikasi 2. Mengidentifikasi kelemahan dari informasi dalam sistem komunikasi bisnis 3. Menerapkan akses kontrol lingkungan Komputasi yang sesuai 4. Mematuhi dan melaksanakan petunjuk yang terdapat pada dokumen yang diterbitkan khusus oleh pemerintah atau badan-badan resmi terkait untuk mengelola sistem operasi 5. Mengumpulkan dan memelihara data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem.	Pemaparan materi, diskusi dan *hands-on lab live class* 2 JP
	Menerapkan prinsip keamanan informasi untuk penggunaan jaringan internet 1. Mematuhi dan menerapkan kebijakan dan prosedur keamanan informasi yang terkait dengan penggunaan jaringan internet 2. Mengidentifikasi tipe kelemahan dan jenisjenis serangan dalam jaringan internet 3. Mengaplikasikan penggunaan jaringan internet secara aman	Pemaparan materi, diskusi dan *hands-on lab live class* 3 JP

Hari 2	**Menerapkan prinsip keamanan informasi pada transaksi elektronik** 1. Mengidentifikasikan dan memenuhi kebutuhan terkait kerahasiaan, integritas, bukti dari pengguna dokumen kunci dan kontrak yang diakui 2. Menetapkan aspek-aspek transaksi 3. Melaksanakan dan memantau perlindungan keamanan untuk sistem infrastruktur dan penggunaan teknologi informasi sesuai dengan rencana implementasi dan prosedur operasi standar	Pemaparan materi, diskusi dan *hands-on lab live class* 3 JP
	Melaksanakan kebijakan keamanan informasi 1. Mengidentifikasi aset penting dalam organisasi 2. Memproteksi aset penting dalam organisasi 3. Melakukan pemantauan terhadap aktivitas yang rentan ancaman	Pemaparan materi, diskusi dan *hands-on lab live class* 2 JP
	Mengaplikasikan ketentuan/persyaratan keamanan informasi 1. Mengaplikasikan persyaratan untuk program yang spesifik untuk keamanan lingkungan komputasi guna mengidentifikasi kelemahan/kerentanan 2. Menyediakan masukan tentang hal yang terkait dengan persyaratan keamanan untuk dimasukkan dalam laporan pekerjaan dan dokumen-dokumen pengadaan terkait 3. Mengumpulkan dan memelihara data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem 4. Mengindentifikasikan persyaratan keamanan dalam prosedur operasi di lingkungan komputasi 5. Menyusun persyaratan keamanan untuk perangkat keras, piranti lunak, dan penggunaan layanan yang spesifik	Pemaparan materi, diskusi dan *hands-on lab live class* 3 JP

	untuk program keamanan jaringan 6. Mengevaluasi dan/atau menyetujui persyaratan keamanan yang relevanterhadap kemampuan teknologi informasi yang baru	
Hari 3	**Mengelola *log*** 1. Menetapkan kebijakan pencatatan *log* untuk menyertakan peristiwa penting 2. Melakukan kontrol berkas *log* terhadap kemungkinan diubah atau dihapus 3. Melakukan kontrol tempat menyimpan media file pencatatan terhadap kemungkinan penuh sehingga terjadi kegagalan ketika mencatat kejadian yang terjadi	Pemaparan materi, diskusi dan *hands-on lab live class* 4 JP
	Menerapkan kontrol akses berdsarkan konsep/metodologi yang telah ditetapkan 1. Menerapkan kontrol akses lingkungan komputasi yang sesuai 2. Melaksanakan kebijakan organisasi dan kebijakan *password* organisasi 3. Mengelola akun hak jaringan dan hak akses ke sistem jaringan dan infrastrukturnya 4. Mengimplementasikan peringatan secara online untuk menginformasikan para pengguna atas peraturan akses dari seluruh infrastruktur dan penggunaan sistem teknologi informasi 5. Menyusun prosedur untuk memastikan pengguna sistem menyadari tanggung jawab keamanan mereka sebelum memberikan akses ke sistem informasi organisasi 6. Melakukan kontrol dan pengawasan pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan agar menerima pelatihan keamanan dasar dan berkelanjutan serta mendapatkan sertifikasi yang sesuai untuk melaksanakan tugas keamanan	Pemaparan materi, diskusi dan *hands-on lab live class* 4 JP

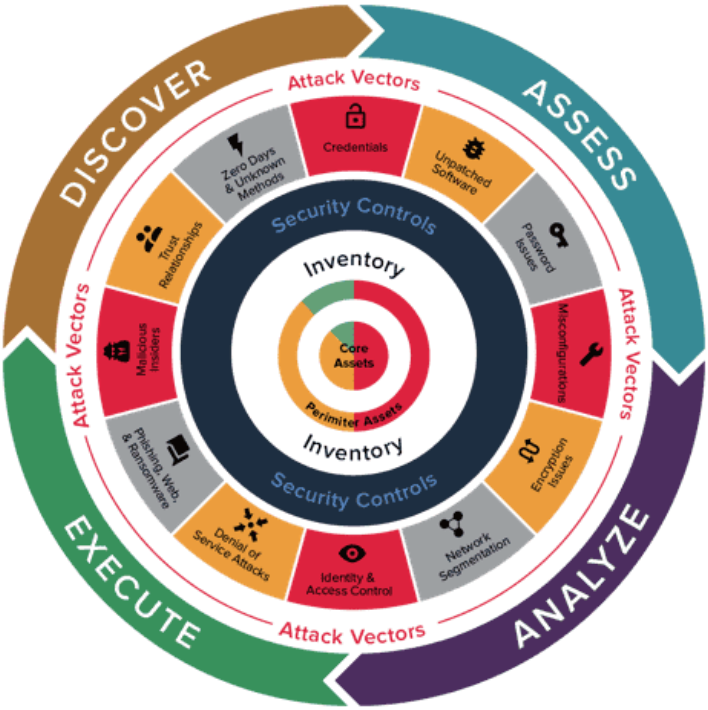
Materi Pokok
1. Mengidentifikasi aset penting dalam organisasi. 2. Memproteksi aset penting dalam organisasi. 3. Melakukan pemantauan terhadap aktivitas yang rentan ancaman.

Sub Materi Pokok
1.1. Manajemen Aset Teknologi Informasi (Aset IT) 2.1. Kerentanan dan Ancaman terhadap Aset IT 2.2. Kontrol Keamanan Aset IT 3.1. *Security Event* 3.2. Pelaporan terhadap *Security Event*

1. MENGIDENTIFIKASI ASET PENTING DALAM ORGANISASI

1.1 Manajemen Aset Teknologi Informasi (Aset IT)

Berbicara tentang *cybersecurity*, akan berkaitan erat dengan bagaimana pengelolaan sumber daya (*people*), tata kelola (*governance*), dan teknologi (*technology*) dijalankan. Dalam bahasan ini akan lebih dalam dijelaskan bagaimana sisi teknologi dikelola dan dipergunakan untuk mendukung keamanan informasi. Salah satu bagian penting di dalam penggunaan teknologi adalah aset, dimana aset merupakan perangkat (baik lunak ataupun keras) yang digunakan dalam lingkungan teknologi informasi untuk mendukung jalannya sebuah layanan sistem elektronik.



Gambar 1. Kerangka Kebijakan dalam Keamanan Aset IT

Aset di dalam lingkungan teknologi informasi perlu dikenali dan dikelola dengan baik dan benar. Mengenali aset IT menjadi bagian penting dalam mewujudkan keamanan informasi sebuah layanan sistem elektronik secara menyeluruh. Hal ini perlu menjadi perhatian, dikarenakan sebagian besar serangan dan ancaman keamanan dilakukan terhadap objek teknologi yang dipergunakan, yang lebih spesifik lagi dijalankan oleh aset-aset yang saling berkorelasi di dalam sistem elektronik. Pengelolaan aset IT, atau yang dikenal dengan istilah menajemen aset IT dilakukan sebagai betuk proteksi terhadap beberapa serangan yang menyasar pada aset IT, diantaranya:

- *Credential Leak*, serangan yang menyasar pada kelemahan dalam pengelolaan nilai kredensial sebuah sistem elektronik.
- *Unpatched Software*, eksploitasi terhadap adanya celah keamanan akibat penggunaan komponen aplikasi yang *obsolete*,
- *Misconfiguration*, eksploitasi terhadap adanya kelemahan akibat konfigurasi aplikasi yang tidak menyesuaikan dengan kaidah keamanan,
- *Lack of Encryption*, serangan pada bagaimana fungsi enkripsi yang tidak diterapkan dengan benar dan aman,
- *Network Attack*, serangan pada pemanfaatan komponen perangkat jaringan,
- *Identity and Access Control Leak*, serangan yang menjadikan identitas dan control akses sebagai objek utama untuk diretas,
- DoS *Attack*, serangan yang mengganggu ketersediaan layanana sistem elektronik,
- *Virus and Malware*, serangan yang memanfaatkan kode program yang dirancang khusus untuk melakukan penetrasi keamanan ke dalam sistem,
- *Insider Attack*, serangan yang memanfaatkan jalur internal sehingga tidak lagi melewati parameter keamanan yang kompleks,

- *Zero-Day Attack*, serangan terbaru yang belum pernah dikenali dan dideteksi sebelumnya.

Setelah mengetahui bagaimana model ancaman yang mengarah pada aset IT, maka selanjutnya menjadi penting untuk dilakukan kontrol terhadap kebijakan keamanan aset IT, mulai dari inventarisasi aset IT, kemudian siapa yang bertanggung jawab dan memiliki hak terhadap aset IT, bagaimana klasifikasi dan siklus hidup informasinya, sampai dengan bagaimana proteksi terhadap aset IT yang telah teridentifikasi.

a. Penanggung Jawab Aset IT

Kebijakan yang digunakan untuk mengidentifikasi aset IT organisasi dan menentukan tanggung jawab perlindungan yang bersesuaian. Terdapat beberapa kontrol keamanan dalam kebijakan ini, diantaranya:

- Inventarisasi Aset, aset yang berkaitan dengan informasi dan perangkat pemrosesannya harus diidentifikasi, diinventarisasi, dikelola dan dipelihara.
- Kepemilikan Aset, aset yang dikelola dalam persediaan merupakan aset yang dimiliki organisasi
- Penggunaan Aset, mengatur bagaimana penggunaan informasi dapat diterima dan aset yang berkaitan dengan informasi atupun yang berkaitan dengan perangkat pemrosesannya harus dapat diidentifikasi, didokumentasikan dan diimplementasikan.
- Pengembalian Aset, mengatur bagaimana aset dikembalikan oleh seluruh pengguna di dalam organisasi, setelah yang bersangkutan sudah tidak memiliki ikatan lagi dengan organisasi.

b. Siklus Hidup dan Klasifikasi Informasi

Kebijakan yang digunakan untuk memastikan bahwa informasi memiliki tingkat pelindungan yang sesuai dengan tingkat kepentingannya bagi proses bisnis organisasi. Terdapat beberapa kontrol keamanan dalam kebijakan ini, diantaranya:

- Klasifikasi Informasi, informasi harus diklasifikasikan berdasarkan pada kebutuhan legal, nilai, tingkat kerawanan, dan sifat sensitifitasnya terhadap pencurian dan modifikasi informasi yang dilakukan secara tidak sah.
- Pelabelan Informasi, rangkaian prosedur dalam melakukan pelabelan informasi yang harus dikembangkan dan diterapkan sesuai dengan klasifikasi informasi yang diadopsi oleh organisasi.
- Penanganan Aset, mengatur bagaimana prosedur penanganan aset dilakukan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi. Selain itu, juga dikendalikan akses terhadap informasi sensitif yang dilakukan oleh pengguna.
- Siklus Hidup Data dan Informasi, mengatur bagaimana pengelolaan siklus hidup data dan informasi harus dilakukan, mulai dari pembuatan, penggunaan, penyimpanan dan penghancuran. Pengaturan ini mencakup dokumentasi waktu retensi untuk kategori data dan bukti prosedur audit ketika penghancuran informasi.
- Daftar Aset Informasi, aset informasi dan pemiliknya harus dikenali dan didokumentasikan dalam daftar aset informasi. Aspek

kerahasiaan, keutuhan dan ketersediaan juga perlu dikenali dan dilakukan penilaian untuk data dan informasi.

c. Proteksi Aset IT

Kebijakan yang digunakan untuk memastikan bahwa informasi dan penyimpanan data dikelola dan dilindungi. Terdapat beberapa kontrol keamanan dalam kebijakan ini, diantaranya:

- Proteksi Data dan Informasi, terdapat sarana (fisik ataupun logik) yang dapat dipergunakan untuk menjalankan fungsi lindungan data dan informasi terhadap ancaman berupa akses tidak sah, pencurian, modifikasi, ataupun penghapusan yang bersifat ilegal. Selain itu, juga dibutuhkan pengamanan dalam penyimpanannya.
- Ketahanan Layanan, terdapat data cadangan (*backup*) yang aman dan selalu tersedia apabila data asli tidak dapat diakses, sehingga kontinuitas layanan dapat tetap berjalan.

Dalam manajemen aset IT perlu diperhatikan mengenai bagaimana mengenali aset yang dimiliki, sehingga inventarisasi dan penyusunan daftar aset menjadi penting untuk dilakukan. Aset IT dapat dikategorikan ke dalam beberapa bagian, mulai dari aset berupa informasi, sumber daya manusia, perangkat keras, perangkat lunak, layanan, sampai pada aset tidak berwujud (*intangible*). Gambar 2 sampai 7 merupakan contoh daftar aset yang dapat dbuat.

No Formulir	xxx/xxx/xxx/xx/x/2022	**DAFTAR ASET**										
Rev	01											
Tanggal Revisi	xxxxxx 2022											
Klasifikasi	**INFORMASI**											
							Klasifikasi Keamanan Informasi					
Kode	**Layanan**	**Nama Aset**	**Sub Klasifikasi**	**Format Penyimpanan**	**Pemilik Aset**	**Masa Berlaku**	**Kerahasiaan**	**Integritas**	**Ketersediaan**	**Nilai**	**Keterangan**
INF-003	DATA CENTER	Dokumentasi jaringan (topologi & Konfigurasi)	Business Process/ Procedure	Dokumen Elektronik		-	3	3	3	3	Tinggi
INF-005	DATA CENTER & SURAT ELEKTRONIK	Dokumen Kontrak	Data Log & Audit	Dokumen Elektronik		-	3	3	3	3	Tinggi
INF-006	DATA CENTER	IP Inventaris	Data Log & Audit	Dokumen Elektronik		-	3	3	3	3	Tinggi
INF-008	DATA CENTER	Database	Database & data files	Dokumen Elektronik		-	3	3	3	3	Tinggi
INF-009	DATA CENTER	Lisensi software	Database & data files	Dokumen Elektronik		-	3	3	3	3	Tinggi
INF-010	DATA CENTER	Laporan Monitoring Performa Jaringan	Data Log & Audit	Dokumen Elektronik		-	3	3	3	3	Tinggi
INF-011	DATA CENTER	Laporan Monitoring Keamanan Jaringan	Data Log & Audit	Dokumen Elektronik		-	3	3	3	3	Tinggi
INF-012	DATA CENTER	Laporan Insiden	Data Log & Audit	Dokumen Elektronik		-	3	3	3	3	Tinggi
INF-013	DATA CENTER & SURAT ELEKTRONIK	Konfigurasi server	Database & data files	Dokumen Elektronik		-	3	3	3	3	Tinggi
INF-014	DATA CENTER	User Manual	Business Process/ Procedure	Dokumen Elektronik		-	3	3	3	3	Tinggi
INF-015	DATA CENTER	Status Real Time Jaringan dan Data Center	Data Log & Audit	Dokumen Elektronik		-	3	3	3	3	Tinggi
INF-018	DATA CENTER	Daftar Aplikasi Operasional	Database & data files	Dokumen Elektronik		-	3	3	3	3	Tinggi
INF-019	DATA CENTER	Daftar Perangkat Data	Database & data files	Dokumen Elektronik		-	3	3	3	3	Tinggi
INF-021	DATA CENTER	Log Change Management	Data Log & Audit	Dokumen Elektronik		-	3	3	3	3	Tinggi
INF-022	DATA CENTER & SURAT ELEKTRONIK & LPSE	Daftar Aset TI	Data Log & Audit	Dokumen Elektronik		-	3	3	3	3	Tinggi
INF-023	DATA CENTER	Master Software	Database & data files	Dokumen Elektronik		-	3	3	3	3	Tinggi
INF-024	DATA CENTER	IT Blue Print	Business Process/ Procedure	Dokumen Elektronik		-	3	3	3	3	Tinggi
INF-025	DATA CENTER	IT SOP & Policy	Business Process/ Procedure	Dokumen Elektronik		-	3	3	3	3	Tinggi
INF-026	DATA CENTER	Kontrak Pekerjaan Personil	Data Log & Audit	Dokumen Elektronik		-	3	3	3	3	Tinggi

Gambar 2. Daftar aset **informasi**

No Formulir	xxx/xxx/xxx/xx/x/2022
Rev	01
Tanggal Revisi	xxxxxx 2022
Klasifikasi	**SUMBER DAYA MANUSIA**

DAFTAR ASET

Kode	Layanan	Nama Personil	Nama Aset	Sub Klasifikasi	No. Identitas/NIP	Pemilik Aset			Jabatan	No. Kontrak/NDA	Atasan Langsung	Kerahasiaan	Integritas	Ketersediaan	Nilai	Keterangan
						Fungsi	Nama Personil	Unit								
SDM-001	Data Center			Management		Penanggung Jawab		Data Center				3	3	3	3	Tinggi
SDM-002	Data Center			Management		Data Center		Data Center				3	3	3	3	Tinggi
SDM-003	Data Center			Management		Data Center		Data Center				3	3	3	3	Tinggi
SDM-004	Data Center			Management		Data Center		Data Center				3	3	3	3	Tinggi
SDM-005	Data Center			Technical		Data Center		Data Center				3	3	3	3	Tinggi
SDM-006	Data Center			Technical		Admin		Data Center				2	2	2	2	Sedang
SDM-007	Data Center			Technical		Admin		Data Center				2	2	2	2	Sedang
SDM-008	Data Center			Technical		Teknisi Jaringan		Data Center				2	2	2	2	Sedang
SDM-009	Data Center			Technical		Teknisi Jaringan		Data Center				2	2	2	2	Sedang
SDM-010	Data Center			Technical		Teknisi Jaringan		Data Center				2	2	2	2	Sedang
SDM-011	Data Center			Technical		Teknisi Jaringan		Data Center				2	2	2	2	Sedang
SDM-012	Data Center			Technical		Teknisi Jaringan		Data Center				2	2	2	2	Sedang

Gambar 3. Daftar aset **sumber daya informasi**

No Formulir	xxx/xxx/xxx/xx/x/202
Rev	01
Tanggal Revisi	xxxxxx 2022
Klasifikasi	**FISIK**

DAFTAR ASET

Kode	Layanan	Nama Aset	Sub Klasifikasi	Jenis Aset	Spesifikasi	Serial number	Pemilik Aset	Penyedia Aset	Pemegang Aset	LOKASI ASET	MASA BERLAKU	Kerahasiaan	Integritas	Ketersediaan	Nilai	Keterangan
FSK-001	DATA CENTER	SWITCH ALLIED TELESIS	Switch	ACCESS SWITCH								3	3	3	3	Tinggi
FSK-076	DATA CENTER	SWITCH ALLIED TELESIS	Switch	ACCESS SWITCH								3	3	3	3	Tinggi
FSK-077	DATA CENTER	CORE SWITCH ALLIED TELESIS	Switch	CORE SWITCH								3	3	3	3	Tinggi
FSK-078	DATA CENTER	CORE SWITCH ALLIED TELESIS	Switch	CORE SWITCH								3	3	3	3	Tinggi
FSK-079	DATA CENTER	Switch Router MikroTik	Switch Router	Router Distribution Firewall								3	3	3	3	Tinggi
FSK-092	DATA CENTER	Switch Router MikroTik	Switch Router	Router Distribution Firewall								3	3	3	3	Tinggi
FSK-093	DATA CENTER	AccesPoint ALLIED TELESIS	AccesPoint	Wereles Accespoint								3	3	3	3	Tinggi
FSK-094	DATA CENTER	AccesPoint ALLIED TELESIS	AccesPoint	Wereles Accespoint								3	3	3	3	Tinggi
FSK-289	DATA CENTER	AccesPoint ALLIED TELESIS	AccesPoint	Wereles Accespoint								3	3	3	3	Tinggi
FSK-290	DATA CENTER	Server SPPTI	Server	Server								3	3	3	3	Tinggi
FSK-291	DATA CENTER	Server Kepaniteraan	Server	Server								3	3	3	3	Tinggi
FSK-292	DRC BALI	Rackmount Server Fujitsu RX 2540M4	Rack	Rack Server								3	3	3	3	Tinggi
FSK-293	DRC BALI	Rackmount Server Fujitsu RX 2540M4	Rack	Rack Server								3	3	3	3	Tinggi
FSK-294	DRC BALI	Storage Amari D30T Starter										3	3	3	3	Tinggi
FSK-295	DRC BALI	Mikrotik CCR 1016 – 12G	Switch Router	Router Distribution Firewall								3	3	3	3	Tinggi
FSK-296	DRC BALI	Close Rack 42U APC AR3100	Rack	Rack Server								3	3	3	3	Tinggi
FSK-298	DRC Duren Tiga	KVM Switch Attens	Switch	ACCESS SWITCH								3	3	3	3	Tinggi
FSK-299	DRC Duren Tiga	Aten Load Balancer	Load Balancer	Load Balancer								3	3	3	3	Tinggi
FSK-300	DRC Duren Tiga	Storage Amari	Storage	Storage								3	3	3	3	Tinggi
FSK-301	DRC Duren Tiga	Storage Amari	Storage	Storage								3	3	3	3	Tinggi
FSK-302	DRC Duren Tiga	Primergy BX900 S2	Server	Server								3	3	3	3	Tinggi
FSK-303	DRC Duren Tiga	Primergy BX2530 M1	Server	Server								3	3	3	3	Tinggi
FSK-304	DRC Duren Tiga	Mikrotik RB 110AH	Switch Router	Router Distribution Firewall								3	3	3	3	Tinggi
FSK-305	DRC Duren Tiga	Net Storage DI01	Storage	Storage								3	3	3	3	Tinggi

Gambar 4. Daftar aset **fisik** (perangkat keras)

No Formulir	xxx/xxx/xxx/xx/x/2022
Rev	01
Tanggal Revisi	xxxxxx 2022
Klasifikasi	**SOFTWARE**

DAFTAR ASET

Kode	Layanan	Nama Aset	Sub Klasifikasi	Pemilik Aset	Pemegang Aset	Lokasi Aset	Masa Berlaku	Metode Penghapusan	Kerahasiaan	Integritas	Ketersediaan	Nilai	Keterangan
SOF-001	DATA CENTER	Website	Aplication Service			Ruang Data Center	-	Delete Normal	3	3	3	3	Tinggi
SOF-002	DATA CENTER	Sistem webmail	Aplication Service			Ruang Data Center	-	Delete Normal	3	3	3	3	Tinggi
SOF-003	DATA CENTER	Sistem mailing list	Aplication Service			Ruang Data Center	-	Delete Normal	3	3	3	3	Tinggi
SOF-005	DATA CENTER	E-Arsip	Aplication Service			Ruang Data Center	-	Delete Normal	3	3	3	3	Tinggi
SOF-006	DATA CENTER	JDIH (Jaringan Dokumentasi Informasi Hukum)	Aplication Service			Ruang Data Center	-	Delete Normal	3	3	3	3	Tinggi
SOF-010	DATA CENTER	E-learning	Aplication Service			Ruang Data Center	-	Delete Normal	3	3	3	3	Tinggi
SOF-012	DATA CENTER	LPSE	Aplication Service			Ruang Data Center	-	Delete Normal	3	3	3	3	Tinggi
SOF-013	DATA CENTER	Active Directory	Aplication Service			Ruang Data Center	-	Delete Normal	3	3	3	3	Tinggi
SOF-017	DATA CENTER	Perpustakaan	Aplication Service			Ruang Data Center	-	Delete Normal	3	3	3	3	Tinggi
SOF-019	DATA CENTER	API	Aplication Service			Ruang Data Center	-	Delete Normal	3	3	3	3	Tinggi

Gambar 5. Daftar aset ***software*** (perangkat lunak)

No Formulir	xxx/xxx/xxx/xx/x/2022
Rev	01
Tanggal Revisi	xxxxxx 2022
Klasifikasi	**LAYANAN**

DAFTAR ASET

Kode	Layanan	Nama Aset	Sub Klasifikasi	Pemilik Aset	Pemegang Aset	Penyedia Aset	Kontrak/SLA			Kerahasiaan	Integritas	Ketersediaan	Nilai	Keterangan
							No. Kontrak/SLA	Deskripsi	Masa Berlaku					
SRV-001	DATACENTER	Perangkat Switch	Maintenance & Support							1	2	3	2	Sedang
SRV-002	DATACENTER	Server	Maintenance & Support							1	2	3	2	Sedang
SRV-003	DATACENTER	PAC/AC	Maintenance & Support							1	2	3	2	Sedang
SRV-004	DATACENTER	Titik Jaringan LAN	Maintenance & Support							1	2	3	2	Sedang
SRV-005	DATACENTER	FirePro FM-200	Maintenance & Support Service							1	2	3	2	Sedang
SRV-006	DATACENTER	Storage	Maintenance & Support							1	2	3	2	Sedang
SRV-007	DATACENTER	Internet Provider	Support							1	2	3	2	Sedang
SRV-008	DATACENTER	Internet Provider	Support							1	2	3	2	Sedang
SRV-009	DATACENTER	Internet Provider	Support							1	2	3	2	Sedang
SRV-010	DATACENTER	UPS	Maintenance & Support							1	2	3	2	Sedang

Gambar 6. Daftar aset **layanan**

No Formulir	xxx/xxx/xxx/xx/x/202	**DAFTAR ASET**							
Rev	01								
Tanggal Revisi	xxxxxx 2022								
Klasifikasi	**INTANGIBLE**								
No	**Layanan**	**Nama Aset**	**Sub Klasifikasi**	**Pemilik Aset**	**Kerahasiaan**	**Integritas**	**Ketersediaan**	**Nilai**	**Keterangan**
INT-001	data center	Standarisasi kualitas Data Center	Reputasi Organisasi		1	3	3	2	Sedang

Gambar 7. Daftar aset tak berwujud (***intangible***)

2. MEMPROTEKSI ASET PENTING DALAM ORGANISASI

2.1 Kerentanan dan Ancaman terhadap Aset IT

Sebelum menerapkan proteksi terhadap aset IT, terlebih dahulu perlu dikenali kerentanan dan ancaman yang dapat mungkin terjadi terhadap aset IT. Berikut adalah kerentanan dan ancaman yang perlu menjadi perhatian dalam penanganan keamanan.

a. Kerentanan

- *Obsolete Component*, penggunaan OS, *webserver*, komponen aplikasi, dan objek di dalam aplikasi lainnya masih banyak ditemukan penerapannya yang menggunakan versi lama yang memiliki banyak celah keamanan yang belum ditutupi. Hal tersebut menimbulkan kerentanan pada aplikasi yang dapat dieksploitasi oleh penyerang.

Vulnerable product	Description	Class	Published	Affected versions	Solution (1)
com_virtuemart	Virtuemart Component	XSS Vulnerability	Dec 04 2017	Version 3.2.4	Update to version 3.2.6
Joomla!	Joomla! LDAP Information Disclosure	Inadequate escaping in the LDAP authentication plugin	Nov 07 2017	Joomla! versions 1.5.0 through 3.8.1	Update to version 3.8.2
com_jsjobs	Js Jobs Component	RCE Vulnerability	Oct 26 2017	Version 1.1.8	Update to version 1.1.9
com_hdwplayer	HDW Player Component	RCE Vulnerability	Oct 26 2017	Version 4.0.0 and all previous	Currently the manufacturer does not provide patches or upgrades
plugin_googlemap3	Google Maps by Reumer	Malicious update	Oct 21 2017	Version 3.5	Update to version 3.5.2
com_ajaxquiz	Ajax Quiz Component	SQL Injection Vulnerability	Oct 18 2017	Version 1.8.0	Currently the manufacturer does not provide patches or upgrades
com_price_alert	Price Alert for Virtuemart Component	SQL Injection Vulnerability	Oct 18 2017	Version 3.0.4 and previous	Currently the manufacturer does not provide patches or upgrades
com_zhyandexmap	Zh YandexMap Component	SQL Injection Vulnerability	Oct 01 2017	Version 6.1.1.0	Update to version 6.2.0.0
com_ns_downloadshop	NS Download Shop Component	SQL Injection Vulnerability	Oct 01 2017	Version 2.2.6	Currently the manufacturer does not provide patches or upgrades

Gambar 8. Contoh daftar komponen aplikasi yang *obsolete* dan rentan

- *Weak Password*, penggunaan kata sandi yang lemah, *default*, dan mudah ditebak. Pemilihan kata sandi merupakan kata-kata yang umum, missal yang terdapat dalam kamus, nama seseorang, atau kata-kata yang memiliki makna umum, sehingga hal tersebut menyebabkan timbulnya kerentanan terhadap dimungkinkannya dilakukan percobaan serangan bruteforce terhadap kata sandi yang digunakan untuk akses masuk ke dalam sistem atau aplikasi.

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Gambar 9. Kompleksitas *password* dan waktu yang dibutuhkan untuk meretasnya

- *Public Remote Access*, akses jarak jauh diperlukan untuk menghubungkan sistem pusat dengan pengguna di luar jaringan sistem pusat, sehingga kontrol kendali tetap dapat dilakukan walaupun berada di luar lingkungan sistem pusat. Meskipun memiliki manfaat dalam adaptivitas, namun akses jarak jauh ini beresiko tinggi apabila tidak dikelola dengan aman. Kerentanan seperti pengambil alihan sistem akibat dibukanya akses melalui jaringan publik, ataupun pencurian data dan informasi akibat tidak adanya perlindungan dalam penerapan akses jarak jauh dapat terjadi setiap saat.
- *Security Misconfiguration*, pengaturan keamanan tidak diterapkan secara memadai dalam operasional layanan aplikasi, sehingga menimbulkan kerentanan dalam bagian konfigurasi sistem yang dapat terjadi pada setiap tingkatan komponen penyusun sebuah sistem , seperti jaringan, OS, *webserver*, *database*, *framework*, kode sumber, lingkungan virtual, ataupun media penyimpanan. Kerentanan ini dapat dengan mudah dikenali dan dieksploitasi oleh pihak penyerang.
- *Unprotected Sharing Object*, integrasi antar komponen penyusun aplikasi menggunakan jaringan dapat menimbulkan kerentanan dalam penyediaan *sharing object* apabila tidak diterapkan dengan fungsi keamanan yang memadai.
- *Virus/Malware Infection*, tidak adanya dukungan antivirus ataupun anti-malware yang memadai menjadikan sebuah aplikasi atau sistem rentan terhadap masuknya kode program jahat. Selain itu, tidak dilakukannya pembaharuan pada versi aplikasi antivirus juga dapat menimbulkan kerentanan yang sama.

b. Ancaman

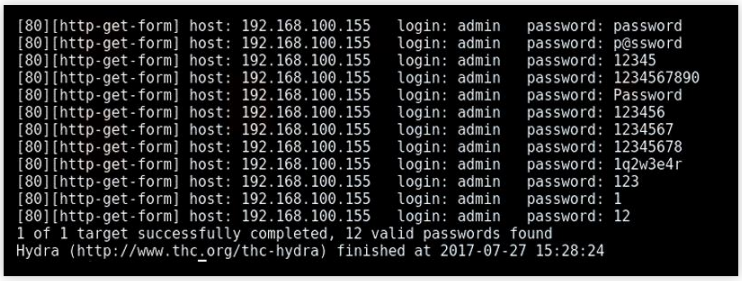
- *Vulnerability Attack*, kerentanan-kerentanan yang dimiliki oleh sebuah aplikasi ataupun sistem, selanjutnya dapat dimanfaatkan untuk dieksploitasi. Teknik dan metode yang dapat digunakan banyak dikenalkan dan selalu disajikan setiap saat, sehingga pihak penyerang dapat dengan mudah dan cepat dalam melakukan serangannya dengan memanfaatkan celah keamanan yang ada.

Date	D	A	V	Title	Type	Platform
2023-03-25				PHPGurukul Online Birth Certificate System V 1.2 - Blind XSS	WebApps	PHP
2023-03-25				Composr-CMS Version <=10.0.39 - Authenticated Remote Code Execution	WebApps	PHP
2023-03-25				MODX Revolution v2.8.3-pl - Authenticated Remote Code Execution	WebApps	PHP
2023-03-25				Abantecart v1.3.2 - Authenticated Remote Code Execution	WebApps	PHP
2023-03-25				SimpleMachinesForum v2.1.1 - Authenticated Remote Code Execution	WebApps	PHP
2023-03-25				ImpressCMS v1.4.3 - Authenticated SQL Injection	WebApps	PHP
2023-03-25				Password Manager for IIS v2.0 - XSS	WebApps	ASP
2023-03-25				Bus Pass Management System 1.0 - Cross-Site Scripting (XSS)	WebApps	PHP
2023-03-25				DLink DIR 819 A1 - Denial of Service	DoS	Hardware
2023-03-25				GuppY CMS v6.00.10 - Remote Code Execution	WebApps	PHP
2023-03-25				NVFLARE < 2.1.4 - Unsafe Deserialization due to Pickle	Remote	Python
2023-03-25				Lavalite v9.0.0 - XSRF-TOKEN cookie File path traversal	WebApps	PHP
2023-03-25				Employee Performance Evaluation System v1.0 - File Inclusion and RCE	WebApps	PHP
2023-03-25				Yoga Class Registration System v1.0 - Multiple SQLi	WebApps	PHP
2023-03-25				Human Resources Management System v1.0 - Multiple SQLi	WebApps	PHP

Gambar 10. *Online repository* celah keamanan terkini

- *Bruteforce Attack*, serangan yang menggunakan metode *trial and error* untuk menebak parameter login, penggunaan kunci enkripsi, atau mencari URL sensitif yang disembunyikan. *Brutefoce* dilakukan dengan

mencoba semua kemungkinan kombinasi dengan harapan ditemukan parameter yang tepat untuk masuk ke dalam sistem. Secara kriptografis, *bruteforce* dapat dikatakan sebagai sebuah teknik serangan pada sistem komputer yang menggunakan percobaan terhadap semua kemunngkinan kunci yang benar dengan melakukan pemeriksaan kemungkinan kata sandi yang benar. Metode serangan seperti ini merupakan teknik yang sudah sejak lama dilakukan, namun masih efektif karena masih banyak praktik pada penggunaan kata sandi yang lemah.



Gambar 11. Contoh serangan *bruteforce*

- *Remote Code Execution* (RCE), serangan yang memanfaatkan terbukanya fasilitas akses jarak jauh untuk mengakses sebuah komputer atau sistem secara *remote*. RCE memungkinkan penyerang untuk melakukan eksekusi perintah dari luar sistem yang berdampak pada terambil alihnya kontrol (peretasan) terhadap sebuah komputer atau sistem. Selain itu, RCE juga dapat menyebabkan terjadinya pencurian data dan informasi, DoS, ataupun penyebaran virus dan malware.
- *Virus* dan *Malware*, kode program yang dibuat untuk masuk ke dalam sebuah komputer secara tidak sah dengan tujuan untuk merusak, mengubah, ataupun menghapus file atau data yang ada di dalamnya. *Virus* dapat menggandakan diri dan dinilai lebih berbahaya daripada *worm*, karena *worm* hanya mereplikasi dirinya sendiri tanpa membuat perubahan data atau file di dalam komputer yang diinfeksi. Sedangkan *malware* merupakan "*malicious software*" yang dibuat untuk menyebabkan kerusakan pada sistem komputer atau jaringan komputer. *Virus*, *worm* dan *trojan* merupakan bagian dari penggunaan istilah *malware*.

2.2 Kontrol Keamanan Aset IT

Kerentanan dan ancaman yang telah didefinisikan dapat diminimalisir risiko keamanan yang akan timbul dengan menerapkan kontrol keamanan yang tepat. Kontrol keamanan berbeda-beda dan disesuaikan untuk masing-masing kerentanan dan ancaman yang teridentifikasi.

Tabel 1. Kontrol Keamanan

Kerentanan	Ancaman	Kontrol Keamanan
Obsolete Component	*Vulnerability Attack*	- Lakukan *security update/patch* - Mencatat dan mendokumentasikan setiap aktivitas update

Kerentanan	Ancaman	Kontrol Keamanan
		- Membuat daftar aset hardware, firmware, dan software dengan informasi masa berlakunya
Weak Password	*Bruteforce Attack*	- Terapkan penggunaan *password* yang aman - Buat kebijakan dalam penggunaan *password* - Sosialisasi dan edukasi seluruh pengguna mengenai kebijakan penggunaan *password* yang aman
Public Remote Access	*Remote Code Execution*	- Batasi penggunaan akses *remote* - Terapkan penggunaan VPN untuk akses *remote* - Lakukan pemantauan lalu lintas jaringan, khususnya untuk aset yang kritis - Terapkan kebijakan dalam permohonan penggunaan akses *remote*
Security Misconfiguration	*Exploitation*	- Terapkan *security hardening* - Lakukan *security update/patch* - Secara berkala lakukan pemeriksaan keamanan - Terapkan enkripsi untuk data yang disimpan - Sosialisasi dan edukasi pemilik sistem mengenai keamanan konfigurasi - Terapkan akses kontrol berdasar tingkat risiko keamanan
Unprotected Sharing Object	*Unwanted Access*	- Terapkan akses kontrol jaringan - Gunakan *active directory* - Melakukan pemantauan terhadap lalu lintas jaringan
Virus/Malware Infection	*Virus/Malware*	- Gunakan *Antivirus* - Gunakan *anti-malware*

Kerentanan	Ancaman	Kontrol Keamanan
		- Membuat dan menerapkan kebijakan BYOD - Melakukan pemantauan terhadap lalu lintas jaringan

3. MELAKUKAN PEMANTAUAN TERHADAP AKTIVITAS YANG RENTAN ANCAMAN

3.1 *Security Event*

a. `sudo` *command*, merupakan istilah untuk "**superuser do**" atau "**substitute do**" yang berarti bahwa sebuah eksekusi perintah dijalankan oleh otoritas dengan hak akses paling tinggi dalam sebuah sistem operasi, sehingga seluruh perintah yang dituliskan dapat dijalankan. Aktifitas `sudo` *command* perlu dikenali dan diperhatikan di dalam sistem dikarenakan beberapa serangan yang berhasil masuk ke dalam sistem akan menjalankan perintah-perintah dengan hak akses tertinggi ini agar dapat tereksekusi. Serangan seperti RCE, *virus*, *malware*, *backdoor*, dan *trojan* bisa saja menggunakan `sudo` *command* untuk melakukan eksploitasi lebih dalam kepada sistem.

b. Syslog, merupakan sebuah protokol dasar untuk menjalankan *system logging* yang digunakan untuk mengumpulkan berbagai macam *log* dari perangkat ataupun aplikasi yang berbeda-beda ke sebuah server terpusat untuk dapat dipantau dan ditinjau. *Log* pada perangkat, seperti *router*, *switch*, *firewall*, *scanner*, *printer*, ataupun *log* pada OS, aplikasi, *database* dan *webserver*.

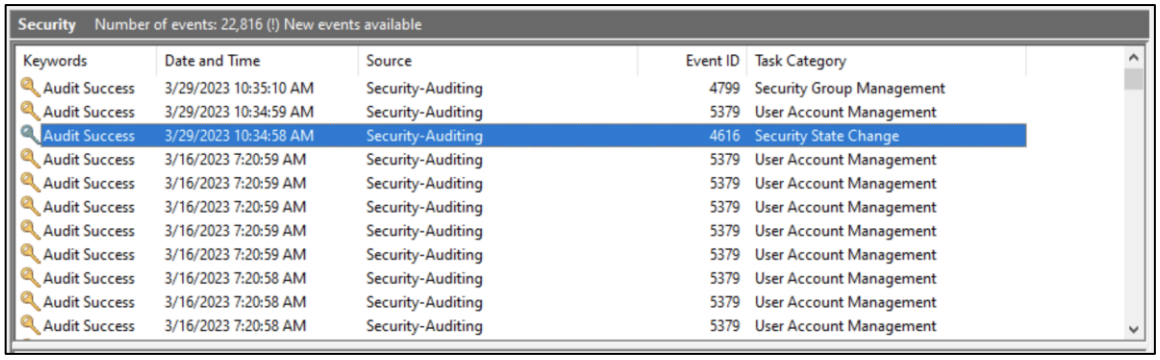
c. Aktifitas *login*, sebagai sebuah akses kontrol untuk otentikasi pengguna, umumnya diterapkan mekanisme *login*. Riwayat dalam mekanisme *login* ini perlu dicatat, untuk mengenali dan mengidentifikasi pengguna yang berhasil ataupun gagal melakukan *login*. Pada aktifitas *login* ini, dapat terlihat adanya indikasi serangan yang terjadi berupa akses illegal yang dilakukan oleh penyerang untuk masuk ke dalam sistem.

d. Anomali keamanan lainnya, merupakan aktifitas yang sudah lebih spesifik mengarah pada ancaman keamanan dan serangan terhadap sistem atau aplikasi.

- *Network scanning*, proses identifikasi dan enumerasi seluruh *host* di dalam jaringan untuk melihat karakteristik jaringan yang dimiliki masing-masing *host*. Dengan *network scanning*, dapat dikenali postur keamanan dari sisi jaringan yang dimiliki masing-masing host yang terhubung di dalam jaringan.
- *Web scanning*, proses pemindaian terhadap sebuah aplikasi web untuk mengenali adanya kerentanan keamanan di dalam sebuah aplikasi, seperti *cross-site scripting* (XSS), *database injection*, ataupun *cross-site request forgery* (CSRF).
- *Multiple authentication failed*, kegagalan *login* secara berulang dalam waktu yang berdekatan mengindikasikan adanya percobaan serangan *bruteforce*.
- DoS *attack*, serangan di dalam jaringan yang memungkinkan penyerang untuk mengganggu atau meniadakan layanan jaringan, sehingga jaringan terputus dan tidak dapat dilakukan komunikasi apapun yang lewat melalui jaringan. Beberapa cara yang dilakukan untuk menjalankan serangan DoS, antara lain adalah dengan menghabiskan *bandwith* yang tersedia di dalam jaringan, membanjiri jaringan dengan lalu lintas dengan paket yang besar, melakukan akses secara terus-menerus ke sebuah perangkat jaringan, ataupun dengan mengeksploitasi kelemahan yang ada di dalam jaringan.

3.2 Pelaporan terhadap *Security Event*

Setiap riwayat yang berkaitan dengan seluruh aktifitas yang terjadi pada sebuah sistem atau aplikasi, khususnya yang berpotensi menimbulkan kerentanan keamanan, perlu didokumentasikan untuk kebutuhan pelaporan sebagai bahan dasar bagi pihak manajemen dalam menentukan bagaimana penguatan dan pengembangan kebijakan keamanan dapat diterapkan. Berikut merupakan contoh pelaporan terhadap *security event* yang terjadi pada sebuah sistem operasi Windows.



Gambar 12. *Security event* pada sistem operasi Windows

Keywords	Date and Time	Source	Event ID	Task Category	
Audit Success	3/29/2023 1:48:33 PM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	3/29/2023 1:04:06 PM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	3/29/2023 12:00:07 PM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	3/29/2023 11:34:34 AM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	3/29/2023 10:50:37 AM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	3/29/2023 10:34:58 AM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	3/16/2023 7:18:55 AM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	3/15/2023 10:40:02 PM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	3/15/2023 11:57:13 AM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	3/15/2023 9:04:46 AM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	3/14/2023 7:57:43 AM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	3/13/2023 4:37:29 PM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	3/13/2023 3:39:13 PM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	3/13/2023 11:20:48 AM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	3/11/2023 9:32:00 PM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	3/11/2023 9:14:34 PM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	2/24/2023 5:55:30 PM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	3/11/2023 9:11:42 PM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	2/24/2023 5:17:37 PM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	2/24/2023 2:32:53 PM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	2/24/2023 2:13:16 PM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.
Audit Success	2/24/2023 8:48:32 AM	Microsoft-Windows-Security-Auditing	4616	Security State Change	The system time was changed.

Gambar 13. Dokumentasi pelaporan *security event*

Latihan 1

Melakukan penyusunan daftar aset IT organisasi

Latihan 2

Mengidentifikasi kerentanan keamanan terhadap daftar aset IT organisasi

Latihan 3

Melakukan penerapan kontrol keamanan pada aset IT organisasi

A. Pengetahuan yang diperlukan untuk melaksanakan kebijakan keamanan informasi

1. Pengetahuan tentang aspek keamanan informasi (CIA triad)
2. Pengetahuan tentang ancaman keamanan siber
3. Pengetahuan tentang beberapa kebijakan keamanan dan standar keamanan yang berlaku
4. pengetahuan tentang pengelolaan aset IT

B. Keterampilan yang diperlukan untuk melaksanakan kebijakan keamanan informasi

1. Kemampuan menjalankan sistem operasi komputer
2. Kemampuan menjalankan program komputer sederhana untuk keamanan informasi
3. Kemampuan mengenali aset IT

C. Sikap Kerja yang diperlukan untuk melaksanakan kebijakan keamanan informasi

1. Harus cermat dalam menjalankan program komputer untuk keamanan informasi
2. Memiliki *security awareness* (kesadaran akan ancaman keamanan informasi)
3. Teliti

Tugas Dan Proyek Pelatihan
1. Kerjakan Latihan 1 sampai dengan latihan 3

Link Referensi Modul
https://www.exploit-db.com

Link Pertanyaan Modul

Bahan Tayang
Bisa berupa Link/ Screen Capture Slide pelatihan

Link room Pelatihan dan Jadwal live sesi bersama instruktur
Zoom, Meets

Penilaian
Komposisi penilaian Kuis 1 Mengumpulkan data: Nilai 10 (Range 0 -10)

Target Penyelesaian Modul
1hari/sampai 2 JP

KOMINFO digitalent

VSGA Vocational School Graduate Academy

2023

#JadiJagoanDigital

digitalent.kominfo.go.id