MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA

KEPUTUSAN MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA
NOMOR 391 TAHUN 2020
TENTANG
PENETAPAN STANDAR KOMPETENSI KERJA NASIONAL INDONESIA
KATEGORI INFORMASI DAN KOMUNIKASI
GOLONGAN POKOK AKTIVITAS PEMROGRAMAN, KONSULTASI KOMPUTER
DAN KEGIATAN YANG BERHUBUNGAN DENGAN ITU
BIDANG *SECURITY OPERATIONS CENTER*

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI KETENAGAKERJAAN REPUBLIK INDONESIA,

Menimbang : a. bahwa untuk melaksanakan ketentuan Pasal 31 Peraturan Menteri Ketenagakerjaan Nomor 3 Tahun 2016 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia, perlu menetapkan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang *Security Operations Center*;

b. bahwa Rancangan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas pemrograman, Konsultasi Komputer dan Kegiatan YBDI Bidang *Security Operations Center* telah disepakati melalui Konvensi Nasional pada tanggal 26 September 2020 di Jakarta;

c. bahwa sesuai dengan Surat Deputi Bidang Pemantauan dan Pengendalian Badan Siber dan Sandi Negara Nomor 2996/BSSN/D4/PP.01.02/11/2020 tanggal 9 November 2020 perihal permohonan penetapan Rancangan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan YBDI Bidang *Security Operations Center*;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b dan huruf c, perlu ditetapkan dengan Keputusan Menteri;

Mengingat : 1. Undang-Undang Nomor 13 Tahun 2003 tentang Ketenagakerjaan (Lembaran Negara Republik Indonesia Tahun 2003 Nomor 39, Tambahan Lembaran Negara Republik Indonesia Nomor 4279);

2. Peraturan Pemerintah Nomor 31 Tahun 2006 tentang Sistem Pelatihan Kerja Nasional (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 67, Tambahan Lembaran Negara Republik Indonesia Nomor 4637);

3. Peraturan Presiden Nomor 8 Tahun 2012 tentang Kerangka Kualifikasi Nasional Indonesia (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 24);

4. Peraturan Presiden Nomor 95 Tahun 2020 tentang Kementerian Ketenagakerjaan (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 213);

5. Peraturan Menteri Ketenagakerjaan Nomor 21 Tahun 2014 tentang Pedoman Penerapan Kerangka Kualifikasi Nasional Indonesia (Berita Negara Republik Indonesia Tahun 2014 Nomor 1792);

6. Peraturan Menteri Ketenagakerjaan Nomor 3 Tahun 2016 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia (Berita Negara Republik Indonesia Tahun 2016 Nomor 258);

MEMUTUSKAN:

Menetapkan : KEPUTUSAN MENTERI KETENAGAKERJAAN REPUBLIK INDONESIA TENTANG PENETAPAN STANDAR KOMPETENSI KERJA NASIONAL INDONESIA KATEGORI INFORMASI DAN KOMUNIKASI GOLONGAN POKOK AKTIVITAS PEMROGRAMAN, KONSULTASI KOMPUTER DAN KEGIATAN YANG BERHUBUNGAN DENGAN ITU BIDANG *SECURITY OPERATIONS CENTER*.

KESATU : Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan YBDI Bidang *Security Operations Center*, sebagaimana tercantum dalam Lampiran dan merupakan bagian yang tidak terpisahkan dari Keputusan Menteri ini.

KEDUA : Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU menjadi acuan dalam penyusunan jenjang kualifikasi nasional, penyelenggaraan pendidikan dan pelatihan serta sertifikasi kompetensi.

KETIGA : Pemberlakuan Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU dan penyusunan jenjang kualifikasi nasional sebagaimana dimaksud dalam Diktum KEDUA ditetapkan oleh Kepala Badan Siber dan Sandi Negara dan/atau kementerian/ lembaga teknis terkait sesuai dengan tugas dan fungsinya.

KEEMPAT : Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU dikaji ulang setiap 5 (lima) tahun atau sesuai dengan kebutuhan.

KELIMA : Keputusan Menteri ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 30 Desember 2020

MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA,

IDA FAUZIYAH

LAMPIRAN
KEPUTUSAN MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA
NOMOR 391 TAHUN 2020
TENTANG
PENETAPAN STANDAR KOMPETENSI KERJA NASIONAL INDONESIA KATEGORI INFORMASI DAN KOMUNIKASI GOLONGAN POKOK AKTIVITAS PEMROGRAMAN, KONSULTASI KOMPUTER DAN KEGIATAN YBDI BIDANG *SECURITY OPERATIONS CENTER* (SOC)

BAB I
PENDAHULUAN

A. Latar Belakang

Pesatnya perkembangan komputer serta teknologi informasi dan komunikasi telah mendorong perusahaan di dunia untuk melakukan adaptasi dan perubahan dalam berbisnis diantaranya melalui pemanfaatan *cloud computing*, *artificial intelligence*, maupun *big data* untuk mengolah aset informasi yang meningkat pesat. Akan tetapi disamping banyaknya manfaat yang diperoleh, penggunaan teknologi juga menimbulkan risiko terjadinya serangan. Serangan tersebut dapat menyebabkan kebocoran dan kerugian data yang dapat menimbulkan masalah hukum dan kerugian finansial, serta merusak reputasi dan kepercayaan publik.

Pada 2018, pencurian data menyumbang 63,5% dari semua serangan siber yang teridentifikasi. Pencurian data umumnya melanda sektor manufaktur, layanan kesehatan, transportasi, ritel, dan layanan keuangan. Diperkirakan dua juta serangan siber pada tahun 2018 mengakibatkan kerugian lebih dari $ 45 miliar di seluruh dunia.

Online Trust Alliance (OTA) *Internet Society*, pada tahun 2018 merilis Laporan Tren Insiden dan Pelanggaran Siber, yang menemukan bahwa dampak kerugian finansial dari serangan *ransomware* meningkat 60%, kerugian dari *Business Email Compromise* (BEC) dua kali lipat, dan insiden *cryptojacking* lebih dari tiga kali lipat. Dalam laporan tersebut, OTA mencatat peningkatan tajam insiden keamanan siber diantaranya *supply chain attacks*, *Business Email Compromise* (BEC) dan

cryptojacking. Beberapa jenis serangan, seperti *ransomware*, bukanlah hal baru tetapi terus menguntungkan para penjahat. Lainnya, seperti *cryptojacking*, menunjukkan bahwa penjahat mengalihkan fokus mereka ke target baru.[1]

Sepanjang tahun 2016 – 2019, di Indonesia tercatat adanya peningkatan jumlah serangan siber setiap tahunnya sebagaimana dapat dilihat pada grafik berikut:

Merujuk Laporan Tahunan Pusat Operasi Keamanan Siber Nasional Badan Siber dan Sandi Negara pada tahun 2018 dan 2019, selama dua tahun berturut-turut Indonesia menjadi negara tujuan serangan terbanyak di dunia. Dimana serangan yang terbesar adalah serangan percobaan pembocoran data, diikuti dengan serangan menggunakan metode *malware*.

Selain data tersebut di atas, pada Laporan *Microsoft Security Endpoint Threat* 2019, Persentase serangan *malware* di Indonesia mencapai 10,68 persen dari total kasus di regional dan menyebabkan Indonesia menjadi negara dengan kasus *malware* tertinggi di Asia Pasifik. Sementara itu, tingkat kasus *ransomware* Indonesia juga berada di peringkat kedua tertinggi di wilayah Asia Pasifik, yaitu 0,14 persen

[1]Online Trust Alliance (OTA) Internet Society (https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf, diakses pada tanggal 3 November 2020 pukul 10.00)

dari total kasus. Nilai tersebut menurun sebesar 46 persen dibanding tahun lalu. akan tetapi, 2,8 kali lebih tinggi dari rata-rata regional. Indonesia tercatat memiliki tingkat serangan *drive-by* yang tinggi, yaitu 0,12 persen dari total kasus pada tahun lalu. Nilai tersebut lebih tinggi 1,5 kali dibanding rata-rata regional dan global.

Selain bertumbuh dalam jumlah dan jenis, ancaman juga bertumbuh di sisi kualitas dan kompleksitas. Salah satunya jenis serangan *Advanced Persistent Threats* (APT). APT secara sederhana adalah ancaman keamanan tingkat canggih yang dilakukan secara gigih. APT dirancang untuk satu tujuan sama yaitu, akses yang tidak terdeteksi ke informasi sensitif. APT menggunakan teknik *hacking* terus menerus untuk mendapatkan akses ke sistem komputer dan dapat tetap di dalam jaringan selama berbulan-bulan sebelum dapat ditemukan.

Serangan-serangan APT terus berkembang cepat. Hal ini mendorong perusahaan-perusahaan besar berada menjadi siaga. Para penyerang telah berkembang pesat dari skala kecil menjadi skala raksasa dengan kepemilikan senjata *malware* yang super canggih. Ditambah lagi jumlah pemain yang mengembangkan APT terus tumbuh pesat dari individu-individu menjadi lembaga besar hingga pemerintahan negara-negara besar di dunia.

Mengingat tingginya ancaman serangan siber saat ini, maka organisasi/perusahaan perlu mengembangkan pemahaman di lingkungannya terkait pengelolaan risiko keamanan siber untuk jaringan, sumber daya, informasi, dan kapasitas. Untuk memenuhi fungsi ini, diperlukan visibilitas penuh atas aset digital dan fisik serta interkoneksinya. Dalam hal ini penetapan peran dan tanggung jawab, pemahaman risiko dan eksposur, dan penerapan kebijakan dan prosedur untuk mengelola risiko tersebut sangat penting.

Bagi suatu organisasi, keamanan siber merupakan aktivitas untuk melakukan pengamanan dan melindungi informasi atau sumber daya teknologi informasi yang esensial dalam upaya mencapai visi, misi dan tujuannya baik untuk kepentingan bisnis maupun layanan yang bersifat sosial demi mencegah terjadinya serangan siber.

Mengacu dari fakta tersebut, diperlukan solusi keamanan yang efektif dan relevan. Untuk dapat mencapai keamanan siber yang optimal maka diperlukan visibilitas terhadap kemungkinan serangan di segala aspek. Hal ini dapat dipenuhi oleh *Security Operations Center* (SOC) yang dapat melakukan korelasi antara informasi yang dikumpulkan dari berbagai solusi keamanan siber yang ada dan melakukan analisis terhadap *incident security* yang sedang terjadi. Secara rinci, dalam suatu organisasi SOC memiliki peran sebagai berikut:

1. Melakukan pencegahan insiden keamanan siber melalui analisis ancaman berkelanjutan, pemindaian aset Teknologi Informasi untuk mendeteksi kerentanan, optimalisasi penerapan kontrol keamanan, dan penyediaan rekomendasi kebijakan keamanan dan arsitektur keamanan siber yang dibutuhkan organisasi.
2. Melakukan monitoring, untuk mendeteksi, dan menganalisis potensi gangguan secara *real time* dan melalui tren historis pada sumber data yang relevan.
3. Melakukan *incident response* terhadap insiden yang dikonfirmasi, dengan mengoordinasikan sumber daya dan mengarahkan penggunaan tindakan pencegahan yang tepat waktu dan tepat.
4. Memberikan kesadaran situasional dan pelaporan tentang status keamanan siber, insiden, dan tren serangan kepada pihak organisasi.

Ada tiga komponen inti yang perlu diperhatikan dalam membangun sebuah SOC, yaitu *people, process,* dan *technology*. Ketiga komponen tersebut perlu saling mendukung dan terintegrasi, guna membangun SOC yang efektif dan optimal. Tentunya tidak mudah untuk membangun ketiga komponen tersebut, banyak tantangan yang perlu dihadapi. Karenanya, disamping memenuhi kebutuhan dalam aspek teknologi dan tata kelolanya hal penting yang harus menjadi perhatian adalah bagaimana menyiapkan aspek *people* di Indonesia untuk melaksanakan fungsi-fungsi SOC.

Dari aspek *people*, kita dihadapkan pada tantangan ketersediaan *security professional* yang relatif masih sedikit. Sementara itu, diperlukan *effort* yang besar untuk merekrut, melatih, dan *maintain*

tenaga ahli SOC, hingga tenaga ahli tersebut memiliki *skill* dan *experience* yang cukup untuk memonitor, menganalisis, dan memberikan rekomendasi terhadap terkait *incident* keamanan siber yang akan dan sedang terjadi.

Dengan demikian, kualitas SOC menentukan kesuksesan suatu organisasi. SOC mencakup banyak sisi mulai dari bagaimana keamanan siber bisa dioperasikan dengan sadar atau tidak, direkam dan disimpan secara lokal atau di media penyimpanan *online* (*cloud*), kemungkinan mempunyai struktur yang berbeda-beda, dari berbagai sumber yang berbeda dan untuk kepentingan yang berbeda-beda. Kualitas SOC yang baik semakin diperlukan jika pemanfaatan keamanan siber mengharuskan pengamanan data dan informasi serta aset teknologi informasi yang diambil dari berbagai lokasi, dalam berbagai format keamanan, dengan menggunakan berbagai alat perekam atau pengidentifikasian atau investigasi keamanan siber.

SOC meliputi kegiatan yang luas sesuai dengan banyaknya dimensi (aspek) keamanan siber yang harus ditangani, karena itu diperlukan kompetensi-kompetensi yang mampu merepresentasikan semaksimal mungkin aktivitas-aktivitas dalam SOC. Upaya memenuhi amanah peraturan perundangan yang berlaku dan mengakomodasi semua pihak yang berkepenting terhadap aspek-aspek pengamanan siber, maka disusun Standar Kompetensi Kerja Nasional Indonesia (SKKNI) SOC ini.
Standar kompetensi SOC ini disusun sebagai upaya untuk:

1. Mengidentifikasi kompetensi-kompetensi yang dibutuhkan dalam mengelola SOC.
2. Menghasilkan referensi acuan penyelenggaraan aktivitas sertifikasi kompetensi yang berbasis pada skema okupasi nasional maupun Kerangka Kualifikasi Nasional Indonesia (KKNI);
3. Menghasilkan referensi acuan pengembangan kurikulum pendidikan tinggi di bidang informatika yang mengacu pada KKNI sesuai dengan peraturan perundang-undangan yang berlaku;
4. Menghasilkan referensi acuan penyusunan *job description* berbagai fungsi teknologi informasi dan komunikasi yang ada dalam sebuah organisasi komersial maupun nirlaba;

5. Menghasilkan referensi acuan pemetaan profil kebutuhan dan ketersediaan sumber daya manusia informatika Indonesia dalam berbagai okupasi dan fungsi kunci; dan
6. Menghasilkan referensi acuan pembuatan berbagai modul dan desain instruksional berbasis kompetensi yang dibutuhkan oleh lembaga pendidikan dan pelatihan di seluruh wilayah Indonesia.

Setiap kompetensi kerja dirumuskan ke dalam SKKNI yang disusun berdasarkan kebutuhan industri. Oleh karena itu, dalam setiap proses penyusunannya SKKNI SOC ini diusahakan semaksimal mungkin melibatkan kalangan industri dan asosiasi profesi yang relevan. SKKNI juga diusahakan menyesuaikan pasar kerja baik nasional maupun internasional serta perkembangan ilmu pengetahuan dan teknologi. Penyusunan SKKNI juga melibatkan kalangan akademisi untuk mengakomodasi kepentingan kurikulum pendididikan formal.

Tersedianya standar kompetensi kerja merupakan salah satu bagian penting yang harus disiapkan dalam pengembangan sumber daya manusia yang berkualitas. Standar kompetensi kerja pada dasarnya merupakan gambaran atau informasi tentang pengetahuan, ketrampilan dan sikap yang harus dimiliki untuk melaksanakan suatu tugas atau pekerjaan sebagaimana dipersyaratkan.

Unit Kompetensi yang diperoleh dari standar internasional dapat dilakukan dengan metode adopsi atau adaptasi. Selain berdasarkan masukan dari kalangan industri, asosiasi, pemerintah, maupun akademisi penyusunan SKKNI SOC juga mengadaptasi dari berbagai sumber acuan yang bersifat global.

B. Pengertian

1. *Security Operations Center* (SOC) adalah salah satu komponen utama keamanan siber dalam sebuah perusahaan/organisasi dalam mengelola risiko siber untuk mencapai tingkat yang dapat diterima oleh perusahaan. SOC berfungsi meningkatkan postur keamanan siber perusahaan/organiasi dalam mengidentifikasi, mendeteksi, melindungi, dan merespon berbagai ancaman dan serangan siber terhadap perusahaan/organisasi.

2. Keamanan siber adalah upaya yang dilakukan untuk melakukan pengamanan dan melindungi informasi atau sumber daya teknologi informasi demi mencegah terjadinya serangan siber.
3. Aset Teknologi Informasi (TI) atau Aset TI meliputi informasi, perangkat keras, perangkat lunak dan sumber daya manusia yang bernilai dan bermanfaat untuk mencapai tujuan perusahaan/organisasi. Aset perangkat keras dapat mencakup *workstation* dan komponennya, perangkat jaringan, printer, *smartphone*, dan lain-lain. Aset perangkat lunak dapat mencakup lisensi, instalasi, *Operating System* (OS), dan lain-lain.
4. *Threat modelling framework* adalah *framework* untuk memahami berbagai teknik, taktik dan prosedur yang digunakan dalam melakukan serangan siber.
5. Insiden Keamanan Siber adalah satu atau beberapa peristiwa keamanan siber yang terkait dan teridentifikasi yang dapat membahayakan organisasi misalnya akses tidak sah terhadap sistem, perubahan tanpa otorisasi atau sistem tidak melayani pengguna aset atau membahayakan operasinya.
6. Risiko siber merupakan risiko operasional terhadap aset informasi dan teknologi yang berdampak buruk terhadap kerahasiaan, ketersediaan, atau integritas informasi atau sistem informasi.

C. Penggunaan SKKNI

Standar Kompetensi dibutuhkan oleh beberapa lembaga/institusi yang berkaitan dengan pengembangan sumber daya manusia, sesuai dengan kebutuhan masing- masing:

1. Untuk institusi pendidikan dan pelatihan
   a. Memberikan informasi untuk pengembangan program dan kurikulum.
   b. Sebagai acuan dalam penyelenggaraan pelatihan, penilaian, dan sertifikasi.
2. Untuk dunia usaha/industri dan penggunaan tenaga kerja
   a. Membantu dalam rekrutmen.
   b. Membantu penilaian unjuk kerja.

c. Membantu dalam menyusun uraian jabatan.
d. Membantu dalam mengembangkan program pelatihan yang spesifik berdasar kebutuhan dunia usaha/industri.

3. Untuk institusi penyelenggara pengujian dan sertifikasi
   a. Sebagai acuan dalam merumuskan paket-paket program sertifikasi sesuai dengan kualifikasi dan levelnya.
   b. Sebagai acuan dalam penyelenggaraan pelatihan penilaian dan sertifikasi.

D. Komite Standar Kompetensi

Susunan komite standar kompetensi pada Rancangan Standar Kompetensi Kerja Nasional Indonesia (RSKKNI) Bidang *Security Operations Center* melalui keputusan Kepala Badan Siber dan Sandi Negara Nomor 61 Tahun 2020 tentang Pembentukan Komite, Tim Perumus, Tim Verifikasi, dan Sekretariat Penyusunan Standar Kompetensi Kerja Nasional Indonesia Bidang Keamanan Siber Tahun Anggaran 2020 tanggal 14 April 2020 dapat dilihat pada Tabel 1.

Tabel 1. Susunan komite standar kompetensi RSKKNI Bidang *Security Operation Center*

NO	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Dr. Suharyanto, S.E., M.M.	Badan Siber dan Sandi Negara	Pengarah
2.	Dame Ria Munthe, S.E.	Badan Siber dan Sandi Negara	Ketua
3.	Asri Setyowati, S.Si., M.M.	Badan Siber dan Sandi Negara	Sekretaris
4.	Christyanto Noviantoro, S.H., M.H.	Badan Siber dan Sandi Negara	Anggota
5.	Anton Setiawan, S.Si., M.M.	Badan Siber dan Sandi Negara	Anggota
6.	Victor Prihatino Tobing	Badan Siber dan Sandi Negara	Anggota

NO	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
7.	Akhmad Toha	Badan Siber dan Sandi Negara	Anggota
8.	Hasto Prastowo, S.Kom	Badan Siber dan Sandi Negara	Anggota
9.	Purwadi, S.Kom	Asosiasi Pengusaha TIK Nasional (APTIKNAS)	Anggota
10.	Satriyo Wibowo S.T., MBA, M.H., IPM, CERG, CCISO	Indonesia Cyber Security Forum (ICSF)	Anggota
11.	Eva Marlina	Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)	Anggota

Tabel 2. Susunan tim perumus RSKKNI Bidang *Security Operation Center*

NO	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Prof. Dr. Eko Kuswardono Budiardjo, Ir., M.Sc.	Universitas Indonesia	Pengarah
2.	Dr. rer. nat. I Made Wiryana, S.Si, S.Kom, M.Sc.	Universitas Gunadarma	Ketua
3.	Dr. Rudi Lumanto, M.Eng.	ID Care	Sekretaris
4.	Yan Adikusuma, S.Kom., M.Eng.	Kantor Staf Presiden	Anggota
5.	Edy Nuryanto	Kementerian Keuangan	Anggota
6.	Tri Budiarta	Kementerian Keuangan	Anggota
7.	Dr. Charles Lim, BSc., M.Sc., CTIA, CHFI, EDRP, ECSA, ECSP, ECIH, CEH, CEI	Swiss German University	Anggota
8.	Dr. Ir. M. Amin Soetomo, M.Sc.	Swiss German University	Anggota
9.	Elysabeth Damayanti	PT. Telkom Indonesia, Tbk.	Anggota
10.	Much Rif 'an	Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)	Anggota

NO	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
11.	M. Novel Ariyadi, ST, MPM, CISSP, CISA, CDPSE, ECIH.	Indonesia Cyber Security Forum (ICSF)	Anggota
12.	Thata Apriatin	Asosiasi Forensik Digital Indonesia (AFDI)	Anggota
13.	Dr. Toto Alfin Atmojo	PT. Defender Nusa Semesta (Defenxor)	Anggota
14.	Digit Oktavianto	Independent Security pada Industri Keamanan Informasi	Anggota
15.	Purnama Sulfa	PT. Bank Mandiri, Tbk.	Anggota
16.	Teguh Wahyono, M.T	Badan Siber dan Sandi Negara	Anggota
17.	Taufik Arianto, S.ST., M.Kom	Badan Siber dan Sandi Negara	Anggota
18.	Wildan, S.ST., M.Si.	Badan Siber dan Sandi Negara	Anggota
19.	Didit Hari Kuncoro Raharjo, S.ST	Badan Siber dan Sandi Negara	Anggota
20.	Yogha Restu Pramadi, S.Kom., M.T.	Politeknik Siber dan Sandi Negara	Anggota

Tabel 3. Susunan Tim verifikasi RSKKNI Bidang *Security Operation Center*

NO	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	2	3	4
1.	Ir. Siswanto, M.M., M.Kom.	Universitas Budi Luhur/ Ikatan Ahli Informatika Indonesia (IAII)	Ketua
2.	Lucia Sri Istiyowati, M.Kom.	Institut Perbanas	Anggota
3.	Irmawanti, S.E	Badan Siber dan Sandi Negara	Anggota
4.	Anas Hilal, S.Pd.	Badan Siber dan Sandi Negara	Anggota
5.	Mita Pramihapsari, S.ST.MP.	Badan Siber dan Sandi Negara	Anggota

BAB II
STANDAR KOMPETENSI KERJA NASIONAL INDONESIA

A. Pemetaan Standar Kompetensi

TUJUAN UTAMA	FUNGSI KUNCI	FUNGSI UTAMA	FUNGSI DASAR
Melakukan perlindungan terhadap seluruh aset organisasi secara terpusat dan kontinyu terus menerus	Merencanakan strategi perlindungan	Menyiapkan perencanaan dan pembangunan infrastruktur pemantauan dan memperbaruinya secara berkala	Membuat model operasi dan strategi *Security Operations Center* (SOC) yang diinginkan
			Merancang kapabilitas *Security Operations Center* (SOC)
		Merencanakan penanggulangan insiden keamanan siber	Menyusun prosedur penanganan insiden keamanan siber
			Mengelola tim penanganan insiden keamanan siber
			Melakukan analisis keamanan siber terhadap insiden kemanan siber untuk menentukan kendali
	Melakukan pemantauan ancaman, serangan dan insiden keamanan siber	Mengindentifikasi dan mendeteksi adanya ancaman dan anomali keamanan	Melakukan deteksi kerentanan aset Teknologi Informasi (TI)
			Menganalisis ancaman/anomali keamanan siber (*threat intelligence*) pada perimeter keamanan
			Melakukan pemantauan aset Teknologi Informasi (TI) terhadap aktivitas ancaman siber
		Mengidentifikasi dan mendeteksi serangan dan insiden keamanan siber yang berkelanjutan	Mengelompokkan insiden keamanan siber yang terjadi sesuai dengan tingkat kegentingan
			Memberikan tiket terhadap insiden keamanan siber

TUJUAN UTAMA	FUNGSI KUNCI	FUNGSI UTAMA	FUNGSI DASAR
			Menganalisis *log* pada *Security Operations Center* (SOC)
	Melakukan respon terhadap insiden keamanan siber	Melakukan koordinasi tanggap insiden keamanan siber	Melakukan pencadangan Data *Security Operations Center* (SOC)
			Mengkomunikasikan penanganan insiden keamanan siber dan manajemen krisis
		Melakukan analisis insiden keamanan siber	Melakukan investigasi modus operandi insiden keamanan siber
			Mengidentifikasi solusi teknis terhadap insiden keamanan siber yang terjadi
		Melakukan mitigasi insiden keamanan siber	Mengisolasi aset Teknologi Informasi (TI) yang terdampak untuk menghentikan insiden keamanan siber
			Melakukan terminasi layanan aset Teknologi Informasi (TI) terdampak insiden untuk perbaikan
		Memberikan rekomendasi hasil analisis untuk tindak lanjut perbaikan/ pemulihan	Menganalisis dampak insiden keamanan siber
			Mengakhiri proses respon terhadap Insiden keamanan siber
			Membuat rekomendasi perbaikan setelah insiden keamanan siber

B. Daftar Unit Kompetensi

NO	Kode Unit	Judul Unit Kompetensi
1	*2*	*3*
1.	J.62SOC00.001.1	Membuat Model Operasi dan Strategi *Security Operations Center* (SOC) yang Diinginkan
2.	J.62SOC00.002.1	Merancang Kapabilitas *Security Operations Center* (SOC)
3.	J.62SOC00.003.1	Menyusun Prosedur Penanganan Insiden Keamanan Siber
4.	J.62SOC00.004.1	Mengelola Tim Penanganan Insiden Keamanan Siber
5.	J.62SOC00.005.1	Melakukan Analisis Keamanan Siber terhadap Insiden Kemanan Siber untuk Menentukan Kendali
6.	J.62SOC00.006.1	Melakukan Deteksi Kerentanan Aset Teknologi Informasi (TI)
7.	J.62SOC00.007.1	Menganalisis Ancaman/Anomali Keamanan Siber (*Threat Intelligence*) pada Perimeter Keamanan
8.	J.62SOC00.008.1	Melakukan Pemantauan Aset Teknologi Informasi (TI) terhadap Aktivitas Ancaman Siber
9.	J.62SOC00.009.1	Mengelompokkan Insiden Keamanan Siber yang Terjadi sesuai dengan Tingkat Kegentingan
10.	J.62SOC00.010.1	Memberikan Tiket terhadap Insiden Keamanan Siber
11.	J.62SOC00.011.1	Menganalisis *Log* pada *Security Operations Center* (SOC)
12.	J.62SOC00.012.1	Melakukan Pencadangan Data *Security Operations Center* (SOC)
13.	J.62SOC00.013.1	Mengkomunikasikan Penanganan Insiden Keamanan Siber dan Manajemen Krisis
14.	J.62SOC00.014.1	Melakukan Investigasi Modus Operandi Insiden Keamanan Siber
15.	J.62SOC00.015.1	Mengidentifikasi Solusi Teknis terhadap Insiden Keamanan Siber yang Terjadi
16.	J.62SOC00.016.1	Mengisolasi Aset Teknologi Informasi (TI) yang Terdampak untuk Menghentikan Insiden Keamanan Siber

NO	Kode Unit	Judul Unit Kompetensi
1	*2*	*3*
17.	J.62SOC00.017.1	Melakukan Terminasi Layanan Aset Teknologi Informasi (TI) Terdampak Insiden untuk Perbaikan
18.	J.62SOC00.018.1	Menganalisis Dampak Insiden Keamanan Siber
19.	J.62SOC00.019.1	Mengakhiri Proses Respon terhadap Insiden Keamanan Siber
20.	J.62SOC00.020.1	Membuat Rekomendasi Perbaikan setelah Insiden Keamanan Siber

C. Uraian Unit Kompetensi

KODE UNIT : **J.62SOC00.001.1**

JUDUL UNIT : **Membuat Model Operasi dan *Strategi Security Operations Center* (SOC) yang Diinginkan**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam membuat strategi dan model operasi pada *Security Operations Center* (SOC) yang diinginkan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengumpulkan informasi terkait ancaman dan *best practice* pembangunan dan pengelolaan SOC yang ada	1.1 Informasi terkait **ancaman** terdahulu yang berpengaruh terhadap organisasi dan pemangku kepentingannya dianalisis berdasarkan **profil risikonya**. 1.2 Informasi terkait terkait tren **serangan siber** dalam dan luar negeri baik secara nasional atau sektoral dikumpulkan berdasarkan jenis dan sumbernya. 1.3 Informasi ***best practice*** pembangunan dan pengelolaan SOC dianalisis berdasarkan jenis dan sifat organisasi.
2. Melakukan analisis kesenjangan (*gap analysis*) terhadap kondisi keamanan informasi saat ini dan yang ingin dicapai	2.1 Aset dan pemangku kepentingan yang berpotensi terdampak ancaman dikumpulkan dan diidentifikasi berdasarkan profil risikonya. 2.2 Informasi potensi kerugian akibat ancaman secara bisnis, reputasi, dan legal serta kemungkinan kejadiannya berulang kembali dikumpulkan berdasarkan *best practice* dan dokumen pembelajaran. 2.3 Kondisi keamanan informasi yang ingin dicapai dianalisis berdasarkan jenis dan sifat organisasi. 2.4 Langkah-langkah untuk menutupi kesenjangan kondisi keamanan informasi diidentifikasi berdasarkan *best practice*.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
	2.5 Prioritas peningkatan kondisi keamanan informasi ditentukan berdasarkan profil risiko siber dan selera risiko *(risk appetite)*.
3. Mengidentifikasi strategi dan model operasi SOC	3.1 **Strategi pembangunan dan operasional** SOC diidentifikasi berdasarkan analisis kesenjangan. 3.2 **Model operasi** diidentifikasi berdasarkan strategi penanganan dan kecukupan akan sumber daya yang ada. 3.3 Alternatif model operasional diverifikasi berdasarkan *best practice*.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Ancaman adalah ancaman keamanan siber yang menyebabkan insiden keamanan siber yang dapat berakibat buruk terhadap aset TI atau organisasi.
   1.2 Profil risiko adalah jenis-jenis risiko yang diakibatkan oleh ancaman siber, yang mungkin terjadi dan berakibat buruk secara spesifik terhadap sebuah aset atau organisasi.
   1.3 Serangan siber adalah semua bentuk serangan yang menargetkan aset-aset sebuah organisasi melalui perantara atau media siber.
   1.4 *Best practice* dalam konteks SOC adalah metode atau teknik dalam pembangunan dan pengelolaan SOC yang secara umum dianggap paling efektif dan efisien.
   1.5 Strategi pembangunan dan operasional adalah sebuah rencana yang berisi target akhir (kondisi yang akan dicapai) beserta tindakan dan sumber daya yang diperlukan untuk mencapai tujuan dari pembangunan dan operasional SOC tersebut.
   1.6 Model operasi adalah bagaimana SOC dari sebuah organisasi beroperasi. Dapat berupa SOC mandiri yaitu SOC yang dibangun dan dioperasikan secara mandiri, lalu SOC yang dijalankan oleh pihak ketiga melalui layanan alih daya (*outsourcing*) maupun kombinasi keduanya (*hybrid*).

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat keras komputer
      2.1.2 Perangkat lunak pengolah kata
   2.2 Perlengkapan
      2.2.1 Media penyimpanan
      2.2.2 *Printer*

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 sebagaimana diubah dengan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)
   4.2 Standar
      4.2.1 SNI ISO/IEC 27005:2008 Teknologi informasi - Teknik Keamanan - Manajemen Risiko Keamanan Informasi
      4.2.2 SNI ISO/IEC 27035-1:2016 Teknologi informasi - Teknik Keamanan - Manajemen Insiden Keamanan Informasi - Bagian 1: Prinsip Manajemen Insiden
      4.2.3 SNI ISO/IEC 27035-2:2016 Teknologi informasi - Teknik Keamanan - Manajemen Insiden Keamanan Informasi - Bagian 2: Pedoman Perencanaan dan Persiapan respon Insiden

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan

konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.

1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan, serta fasilitas asesmen yang dibutuhkan.

1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara, serta metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Sistem Manajemen Keamanan Informasi (SMKI)

3.1.2 Manajemen risiko teknologi informasi

3.1.3 Manajemen insiden keamanan siber

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan perangkat lunak

3.2.2 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah diidentifkasi

3.2.3 Melakukan analisis kesenjangan (*gap analysis*)

4. Sikap kerja yang diperlukan

4.1 Teliti

4.2 Objektif

4.3 Tanggung jawab

4.4 Integritas

5. Aspek kritis
    5.1 Kecermatan dalam menganalisis kondisi keamanan informasi yang ingin dicapai berdasarkan jenis dan sifat organisasi
    5.2 Kemampuan dalam mengidentifikasi model operasi berdasarkan strategi penanganan dan kecukupan akan sumber daya yang ada

KODE UNIT : **J.62SOC00.002.1**
JUDUL UNIT : **Merancang Kapabilitas *Security Operations Center* (SOC)**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam merancang kapabilitas *Security Operations Center* (SOC), agar berfungsi sesuai tujuan yang telah ditetapkan organisasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menyusun rancangan aspek pengelolaan SOC	1.1 **Struktur SOC** dirancang sesuai dengan kebutuhan dan keterbatasan organisasi. 1.2 **Target dan metrik kinerja SOC** dirancang sesuai dengan tujuan, kebutuhan dan keterbatasan organisasi. 1.3 Proses monitoring dan pemberian peringatan/*alerting* terhadap potensi serangan siber dirancang sesuai dengan kebijakan organisasi. 1.4 Proses penanganan insiden keamanan siber dirancang sesuai kebijakan organisasi. 1.5 Isi, format, dan frekuensi pelaporan SOC dirancang sesuai kebutuhan organisasi.
2. Menyusun rancangan aspek sumber daya manusia SOC	2.1 Kebutuhan Sumber Daya Manusia (SDM) dirancang sesuai dengan struktur organisasi SOC dan proses-proses internal. 2.2 Uraian kerja dan **indikator kinerja** SDM dirancang sesuai kebutuhan organisasi. 2.3 Kebutuhan peningkatan kompetensi bagi SDM dirancang sesuai kapabilitas SOC. 2.4 Pola kerja dan pola komunikasi tim dirancang untuk kegiatan SOC sehari-hari sesuai dengan kebijakan yang berlaku.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
3. Menyusun rancangan aspek teknologi SOC	3.1 Daftar **aset TI** yang dalam ruang lingkup tanggung jawab SOC dibuat berdasarkan jenis dan kapabilitasnya. 3.2 Sumber-sumber ***event*** yang akan dikelola dalam SOC ditentukan berdasarkan *best practice*. 3.3 **Kapabilitas perangkat** diestimasi berdasarkan *best practice* dan dokumen pembelajaran. 3.4 Aspek teknis format pelaporan dan *dashboard* yang akan digunakan oleh SOC dibuat berdasarkan kebijakan yang berlaku.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Struktur SOC adalah hierarki organisasi dalam pengelolaan SOC yang menunjukkan wewenang, tanggung jawab, dan ruang lingkup pekerjaan.
   1.2 Target dan metrik kinerja SOC adalah sasaran operasional yang hendak dicapai dan indikator pengukuran keberhasilannya.
   1.3 Indikator kinerja diukur berdasarkan parameter waktu deteksi dan waktu penyelesaian, efektivitas solusi, pembatasan dampak insiden keamanan siber, dan efektivitas komunikasi serta koordinasi tim.
   1.4 Aset TI berupa data, aplikasi, sistem operasi, dan perangkat keamanan siber adalah aset yang dibutuhkan agar kegiatan operasional pada SOC dapat berjalan sesuai rencana untuk mencapai target yang ditentukan.
   1.5 *Event* berupa *security event*, *system event,* dan *application events* adalah berbagai kejadian yang direkam dan dimonitor oleh SOC.
   1.6 Kapabilitas perangkat meliputi prakiraan *event* serta kapasitas *management log,* kemampuan pengumpulan *event* oleh *log management,* kemampuan korelasi dan analisis *event,* dan sebagainya.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat keras komputer
      2.1.2 Perangkat lunak pengolah kata
   2.2 Perlengkapan
      2.2.1 Media penyimpanan
      2.2.2 *Printer*
      2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 sebagaimana diubah dengan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
      4.2.1 SNI ISO/IEC 27001:2013 Teknologi informasi - Teknik keamanan Sistem manajemen keamanan informasi - Persyaratan
      4.2.2 SNI ISO/IEC 27035 - 1:2016 Teknologi informasi - Teknik Keamanan - Manajemen insiden keamanan informasi - Bagian 1: Prinsip manajemen insiden
      4.2.3 SNI ISO/IEC 27035 - 2:2016 Teknologi informasi - Teknik Keamanan - Manajemen insiden keamanan informasi - Bagian 2: Pedoman perencanaan dan persiapan respon insiden

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.
   1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan, serta fasilitas asesmen yang dibutuhkan.
   1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara, serta metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Sistem Manajemen Keamanan Informasi (SMKI)
      3.1.2 Manajemen insiden keamanan informasi
      3.1.3 Prinsip dan kebijakan perlindungan informasi
      3.1.4 Penerapan kontrol keamanan informasi
      3.1.5 Manajemen SDM
      3.1.6 Proses bisnis organisasi sesuai fungsionalitas yang akan digunakan sebagai basis dalam menentukan kapabilitas SOC
   3.2 Keterampilan
      3.2.1 Menggunakan aplikasi pengolah kata serta aplikasi deskripsi proses dan organisasi

3.2.2 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah diidentifkasi

3.2.3 Membaca dokumen peta okupasi dan Standar Kompetensi Kerja Nasional Indonesia untuk perancangan kebutuhan SDM

4. Sikap kerja yang diperlukan
   4.1 Teliti
   4.2 Objektif
   4.3 Tanggung jawab

5. Aspek kritis
   5.1 Ketepatan dalam menyusun pola kerja dan pola komunikasi tim dalam melaksanakan kegiatan SOC sehari-hari sesuai dengan kebijakan yang berlaku
   5.2 Ketepatan dalam melakukan estimasi kapabilitas perangkat berdasarkan *best practice* dan dokumen pembelajaran

KODE UNIT : **J.62SOC00.003.1**
JUDUL UNIT : **Menyusun Prosedur Penanganan Insiden Keamanan Siber**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam membantu implementasi pengelolaan penanganan insiden keamanan siber.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasikan proses bisnis penanganan insiden keamanan siber	1.1 Standar dan *best practice* penanganan insiden keamanan siber dipilih berdasarkan kesesuaian dengan model operasi dan rancangan kapabilitas *Security Operations Center* (SOC). 1.2 Rekomendasi perubahan proses bisnis disusun berdasarkan laporan operasional dan **daftar pembelajaran**. 1.3 Proses bisnis penanganan insiden keamanan siber ditentukan berdasarkan standar dan *best practice.*
2. Mengidentifikasi prosedur yang dibutuhkan dalam setiap tahap penanganan insiden keamanan siber	2.1 Proses bisnis dianalisis berdasarkan tahapan, kewenangan, dan ruang lingkupnya. 2.2 Kebutuhan ragam **prosedur** pada setiap tahapan proses bisnis diidentifikasi berdasarkan standar dan *best practice*.
3. Membuat prosedur penanganan insiden keamanan siber	3.1 Langkah-langkah penanganan insiden keamanan siber diidentifikasi berdasarkan ruang lingkup prosedur yang telah ditentukan. 3.2 Kewenangan dan **kebutuhan** dalam prosedur diverifikasi kepada pihak yang berwenang. 3.3 Prosedur disusun berdasarkan langkah-langkah yang sistematis dan pemberian kewenangan yang jelas.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Daftar pembelajaran antara lain meliputi pengkajian ulang, identifikasi, dan perbaikan terhadap *information security control, risk assessment,* dan evaluasi manajemen.
   1.2 Prosedur yang digunakan dalam rangka penanganan insiden keamanan siber pada SOC antara lain, namun tidak terbatas pada:
      1.2.1 Prosedur pemantauan terhadap aktivitas ancaman siber
      1.2.2 Prosedur pencadangan data SOC
      1.2.3 Prosedur pengelolaan tiket
      1.2.4 Prosedur *vulnerability assessment*
      1.2.5 Prosedur pemulihan data SOC
      1.2.6 Prosedur penentuan kendali insiden keamanan siber
      1.2.7 Prosedur komunikasi penanganan insiden keamanan siber
      1.2.8 Prosedur komunikasi manajemen krisis
      1.2.9 Prosedur investigasi modus operandi insiden keamanan siber
      1.2.10 Prosedur isolasi insiden keamanan siber
      1.2.11 Prosedur terminasi aset TI
      1.2.12 Prosedur *digital evidence first response*
      1.2.13 Prosedur pengakhiran insiden keamanan siber
      1.2.14 Prosedur *information sharing*
      1.2.15 Prosedur pengelompokkan insiden keamanan siber
      1.2.16 Prosedur pembuatan laporan/dokumen
   1.3 Kebutuhan pada prosedur yang dimaksud meliputi formulir, peralatan, akses, dll

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat keras komputer
      2.1.2 Perangkat lunak pengolah kata
   2.2 Perlengkapan
      2.2.1 Media penyimpanan

2.2.2 *Printer*

2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 sebagaimana diubah dengan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27001:2013 Teknologi informasi - Teknik keamanan Sistem manajemen keamanan informasi - Persyaratan

4.2.2 SNI ISO/IEC 27035 -1:2016 Teknologi informasi - Teknik Keamanan - Manajemen insiden keamanan informasi - Bagian 1: Prinsip manajemen insiden

4.2.3 SNI ISO/IEC 27035 - 2:2016 Teknologi informasi - Teknik Keamanan - Manajemen insiden keamanan informasi - Bagian 2: Pedoman perencanaan dan persiapan respon insiden

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.

1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan, serta fasilitas asesmen yang dibutuhkan.

1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara, serta metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Sistem Manajemen Keamanan Informasi (SMKI)

3.1.2 Manajemen insiden keamanan siber

3.1.3 Proses bisnis organisasi sesuai fungsionalitas yang akan digunakan sebagai basis dalam menentukan kapabilitas SOC

3.1.4 Tata aturan, standar, dan *best practice* yang terkait dengan *security operation and incident management*

3.2 Keterampilan

3.2.1 Menggunakan notasi untuk menjabarkan prosedur kerja

3.2.2 Menggunakan perangkat lunak diagram dan pengolah kata untuk menjabarkan prosedur kerja

4. Sikap kerja yang diperlukan

4.1 Teliti

4.2 Objektif

4.3 Tanggung jawab

5. Aspek kritis

   5.1 Kecermatan dalam mengidentifikasi kebutuhan ragam prosedur pada setiap tahapan proses bisnis berdasarkan standar dan *best practice*

KODE UNIT : **J.62SOC00.004.1**

JUDUL UNIT : **Mengelola Tim Penanganan Insiden Keamanan Siber**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengelola tim penanganan insiden keamanan siber.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi kebutuhan organisasi akan tim penanganan insiden keamanan siber	1.1 Kebutuhan Sumber Daya Manusia (SDM) *Security Operations Center* (SOC) diidentifikasi berdasarkan model operasi, kapabilitas, dan strategi. 1.2 Kebutuhan kompetensi ditentukan sesuai dengan SDM pada SOC.
2. Mengelola tim penanganan insiden keamanan siber	2.1 Tugas pokok dan target kinerja anggota tim diusulkan berdasarkan fungsi dan tujuan organisasi SOC. 2.2 Kesenjangan kompetensi diidentifikasi sesuai dengan kebutuhan kompetensinya. 2.3 Tim pendukung internal dari **divisi lain** untuk antisipasi insiden keamanan siber yang kritis, berprioritas tinggi, dan berdampak pada operasional bisnis diusulkan kepada **pihak terkait.**
3. Menjaga kolaborasi dengan para pihak eksternal	3.1 **Tim pendukung eksternal** diidentifikasi untuk antisipasi insiden keamanan siber yang kritis, berprioritas tinggi, dan berdampak bisnis operasi. 3.2 Hubungan dan pola kerja sama dengan tim pendukung eksternal dibuat sesuai aturan dan kesepakatan.
4. Menentukan kesiapsiagaan tim	4.1 **Aspek kendali keamanan informasi** ditentukan berdasarkan *best practice*. 4.2 Jadwal audit keamanan untuk mengkaji tingkat keamanan dan pemantauan kerentanan dari sistem ditetapkan berdasarkan **laporan**. 4.3 **Latihan insiden keamanan siber** dilaksanakan sesuai dengan kompleksitas yang berbeda.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Divisi lain termasuk di antaranya hukum, *public relation*, SDM, dan keuangan.
   1.2 Pihak terkait yaitu pihak internal yang mempunyai wewenang untuk menyetujui pembentukan tim penanganan insiden keamanan siber.
   1.3 Tim pendukung eksternal di antaranya vendor, konsultan, pemerintahan, industri, akademis, komunitas keamanan informasi, dan seterusnya.
   1.4 Aspek kendali keamanan informasi di antaranya pengelolaan kerentanan, *security updates and patches,* risiko teknologi baru, *Intrusion Detection System* (IDS), anomali dalam perangkat jaringan, dan antisipasi *zero day*.
   1.5 Laporan di antaranya, namun tidak terbatas pada laporan insiden keamanan siber, daftar pembelajaran, hasil audit, informasi pihak ketiga, dan sebagainya.
   1.6 Parameter latihan insiden keamanan siber di antaranya menguji proses, prosedur, kemampuan tim, kerja sama dengan pihak lain, komunikasi, dan pengambilan keputusan.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat keras komputer
      2.1.2 Perangkat lunak pengolah kata
   2.2 Perlengkapan
      2.2.1 Media penyimpanan
      2.2.2 *Printer*
      2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 sebagaimana diubah dengan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

3.3 Keputusan Kepala BSSN Nomor: 563.1 tahun 2019 tentang Penetapan Peta Okupasi Nasional dalam Kerangka Kualifikasi Nasional Indonesia pada Area Fungsi Keamanan Siber

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27001:2013 Teknologi informasi - Teknik keamanan Sistem manajemen keamanan informasi - Persyaratan

4.2.2 SNI ISO/IEC 27004:2013 Teknologi informasi - Teknik keamanan - Manajemen keamanan informasi - Pengukuran

4.2.3 SNI ISO/IEC 27035 -1:2016 Teknologi informasi - Teknik Keamanan - Manajemen insiden keamanan informasi - Bagian 1: Prinsip manajemen insiden

4.2.4 SNI ISO/IEC 27035 - 2:2016 Teknologi informasi - Teknik Keamanan - Manajemen insiden keamanan informasi - Bagian 2: Pedoman perencanaan dan persiapan respon insiden

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.

1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan, serta fasilitas asesmen yang dibutuhkan.

1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara, serta metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Organisasi dan proses bisnis

3.1.2 Manajemen insiden keamanan informasi

3.1.3 Sistem Manajemen Keamanan Informasi (SMKI)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan perangkat lunak untuk berkomunikasi dan berkolaborasi

3.2.2 Memanfaatkan Peta Okupasi dan Standar Kompetensi Kerja Nasional Indonesia untuk menentukan kompetensi dan karakterstik SDM yang diperlukan

3.2.3 Melaksanakan persiapan Latihan insiden keamanan siber

3.2.4 Melakukan negosiasi

4. Sikap kerja yang diperlukan

4.1 Teliti

4.2 Objektif

4.3 Tanggung jawab

4.4 Komunikatif

4.5 Kolaboratif

5. Aspek kritis

5.1 Kecermatan dalam menentukan kebutuhan kompetensi sesuai dengan SDM pada SOC

5.2 Kecermatan dalam penyusunan tugas pokok dan target kinerja

KODE UNIT : **J.62SOC00.005.1**

JUDUL UNIT : **Melakukan Analisis Keamanan Siber terhadap Insiden Keamanan Siber untuk Menentukan Kendali**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan investigasi awal untuk menentukan kendali terhadap insiden keamanan siber.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengumpulkan informasi terkait efek dari insiden keamanan siber	1.1 Informasi terkait efek dari insiden keamanan siber ke dalam organisasi dikumpulkan sesuai prosedur. 1.2 Informasi terkait efek dari insiden keamanan siber ke luar organisasi dikumpulkan sesuai prosedur. 1.3 Pembaruan informasi insiden keamanan siber susulan dilakukan sesuai prosedur.
2. Mengidentifikasi dampak insiden keamanan siber	2.1 Seluruh **pemangku kepentingan** yang kemungkinan terdampak insiden keamanan siber diidentifikasi berdasarkan ruang lingkupnya. 2.2 **Risiko kerugian** akibat insiden keamanan siber didefinisikan berdasarkan analisis risiko. 2.3 Langkah mitigasi dan prioritas ditentukan berdasarkan ***risk appetite***.
3. Menentukan kendali terhadap insiden keamanan siber	3.1 Rencana penanganan insiden keamanan siber dibuat berdasarkan prosedur. 3.2 Ketersediaan akan sumber daya internal dalam penanganan insiden keamanan siber dipastikan sesuai kebutuhan. 3.3 Eskalasi pengambilan keputusan berdasarkan kewenangan dilakukan sesuai prosedur. 3.4 Laporan kegiatan investigasi awal untuk menentukan kendali terhadap insiden keamanan siber didokumentasikan sesuai prosedur.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Pemangku kepentingan di antaranya, namun tidak terbatas pada internal organisasi, aparat penegak hukum, pelanggan, pemasok, masyarakat, dan komunitas Teknologi Informasi dan Komunikasi (TIK).
   1.2 Risiko kerugian di antaranya, namun tidak terbatas pada kebocoran dan kerugian data, permasalahan hukum, kerugian finansial, rusaknya reputasi, dan kepercayaan publik.
   1.3 *Risk appetite* merupakan jumlah dan jenis risiko yang disiapkan oleh sebuah organisasi untuk dipertahankan, dipelihara atau diambil/sejumlah risiko, pada tingkatan manajemen/*board*, dimana sebuah organisasi bersedia menerima risiko tersebut.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat keras komputer
      2.1.2 Perangkat lunak pengolah kata
   2.2 Perlengkapan
      2.2.1 Media penyimpanan
      2.2.2 *Printer*
      2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah terakhir pada Undang-Undang Nomor 19 Tahun 2016
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik sebagaimana diubah terakhir pada Peraturan Pemerintah Nomor 71 Tahun 2019

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27001:2013 Teknologi Informasi - Teknik Keamanan - Sistem Manajemen Keamanan Informasi - Persyaratan

4.2.2 SNI ISO/IEC 27035-1:2016 Teknologi informasi – Teknik Keamanan – Manajemen Insiden Keamanan Informasi – Bagian 1: Prinsip Manajemen Insiden

4.2.3 SNI ISO/IEC 27035-2:2016 Teknologi informasi – Teknik Keamanan – Manajemen Insiden Keamanan Informasi – Bagian 2: Pedoman Perencanaan dan Persiapan respon Insiden

4.2.4 NIST SP 800-171 *Revision 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.

1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan.

1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara, serta metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
    3.1. Pengetahuan
        3.1.1 Organisasi dan proses bisnis
        3.1.2 Kontrak/*Service Level Agreement* (SLA)
        3.1.3 Rencana keberlangsungan bisnis
        3.1.4 Analisis insiden keamanan siber
    3.2. Keterampilan
        3.2.1 Mengoperasikan perangkat keras dan perangkat lunak pengolah kata
        3.2.2 Melakukan analisis terhadap permasalahan dan *vulnerabities* yang sudah berhasil di eksploitasi sehingga menemukan sebuah solusi/jalan keluar untuk menangani permasalahan insiden keamanan siber.
        3.2.3 Melakukan *Layer of Protection Analysis* (LOPA)
        3.2.4 Melakukan komunikasi dan negosiasi

4. Sikap kerja yang diperlukan
    4.1 Teliti
    4.2 Objektif
    4.3 Tanggung jawab
    4.4 Integritas

5. Aspek kritis
    5.1 Ketepatan dalam membut eskalasi pengambilan keputusan berdasarkan kewenangan dilakukan sesuai prosedur

KODE UNIT : **J.62SOC00.006.1**

JUDUL UNIT : **Melakukan Deteksi Kerentanan Aset Teknologi Informasi (TI)**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan deteksi kerentanan pada Aset TI.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi ruang lingkup deteksi kerentanan aset TI	1.1 Aset TI yang akan dideteksi kerentanannya diidentifikasi berdasarkan **dokumen kesepakatan**. 1.2 Ruang lingkup deteksi kerentanan diidentifikasi berdasarkan dokumen kesepakatan. 1.3 Jadwal dan lokasi pelaksanaan dikoordinasikan kepada pihak terkait sesuai dokumen kesepakatan.
2. Mengidentifikasi kerentanan pada aset TI	2.1 Deteksi kerentanan aset TI dilaksanakan sesuai dengan **tahapan *vulnerability assessment***. 2.2 Rekomendasi mitigasi disusun sesuai dengan laporan hasil *vulnerability assessment*.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Dokumen kesepakatan yang dimaksud dapat berupa *Service Level Agreement* (SLA) maupun *Non Disclosure Agreement* (NDA). Pada dokumen tersebut memuat target/dokumen prioritas, jadwal, teknik dan kustomisasi, pelaksana dan keahlian, lokasi pelaksanaan.
   1.2 Tahapan *vulnerability assessment* terdiri atas tahapan *reconnaissance, scanning, enumeration, vulnerability analysis*, dan pelaporan.
      1.2.1 *Recoinnaisance* adalah tahapan awal untuk melakukan evaluasi keamanan postur dari target organisasi di mana

penguji mengumpulkan data tentang organisasi tersebut seperti teknologi yang digunakan, berapa perangkat yang terkoneksi, hingga arsitektur jaringan dari target.

1.2.2 *Scanning* adalah proses pengumpulan informasi tambahan yang lebih detail mengenai target menggunakan teknik *reconnaissance* aktif untuk mendeteksi target aktif, *port*, dan *service* pada jaringan.

1.2.3 *Enumeration* adalah tahapan yang mirip dilakukan pada *reconnaissance*, namun biasanya pada *enumeration* dilakukan pencarian data yang lebih spesifik atau ketika sudah berhasil masuk pada *service* tententu.

1.2.4 *Vulnerability analysis* adalah tahapan deteksi dan analisis terhadap kerentanan yang ditemukan. Proses analisis dapat dilakukan berdasarkan pengalaman penguji dengan informasi-informasi yang telah didapatkan sebelumnya atau dapat menggunakan v*ulnerability assessment tools* seperti Nessus, OWASP Zap, Acunetix, dan *tools* lain sejenis.

2. Peralatan dan perlengkapan
   - 2.1 Peralatan
     - 2.1.1 Komputer atau server
     - 2.1.2 Perangkat lunak deteksi kerentanan
     - 2.1.3 Perangkat lunak pengolah kata
   - 2.2 Perlengkapan
     - 2.2.1 Media Penyimpanan
     - 2.2.2 *Printer*
     - 2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   - 3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah terakhir pada Undang - Undang Nomor 19 Tahun 2016

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik sebagaimana diubah terakhir pada Peraturan Pemerintah Nomor 71 Tahun 2019

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
      4.2.1 SNI ISO/IEC 27001:2013 Teknologi informasi - Teknik keamanan Sistem manajemen keamanan informasi - Persyaratan

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.
   1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.
   1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan.
   1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara, serta metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
    3.1. Pengetahuan
        3.1.1 Sistem Manajemen Keamanan Informasi (SMKI)
        3.1.2 Proses dan cara kerja sistem operasi komputer
        3.1.3 Manajemen insiden keamanan informasi
        3.1.4 Teknik *vulnerability assessment*
    3.2. Keterampilan
        3.2.1 Mengoperasikan perangkat keras dan perangkat lunak *vulnerability assessment*
        3.2.2 Melakukan identifikasi risiko kerentanan aset TI
        3.2.3 Menjalankan alat evaluasi kerentanan (*vulnerability assessment*) aset TI

4. Sikap kerja yang diperlukan
    4.1 Teliti
    4.2 Objektif
    4.3 Tanggung jawab
    4.4 Integritas

5. Aspek kritis
    5.1 Kecermatan dalam mengidentifikasi ruang lingkup deteksi kerentanan berdasarkan dokumen kesepakatan
    5.2 Ketepatan dalam mendeteksi kerentanan aset TI sesuai dengan tahapan *vulnerability assessment*

KODE UNIT : **J.62SOC00.007.1**

JUDUL UNIT : **Menganalisis Ancaman/Anomali Keamanan Siber *(Threat Intelligence)* pada Perimeter Keamanan**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengidentifikasi ancaman yang terjadi pada aset Teknologi Informasi (TI).

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan parameter kewajaran	1.1 Ruang lingkup aset TI diidentifikasi berdasarkan jenis dan kapabilitasnya. 1.2 Parameter kewajaran didefinisikan berdasarkan **kenormalan** aset TI terkini yang dimonitor, pembelajaran insiden keamanan siber sebelumnya, dan hasil ***threat intelligence*** dari eksternal.
2. Melakukan pemeriksaan terhadap *log*	2.1 Anomali *log* dianalisis berdasarkan **parameter kewajaran**. 2.2 **Tipe *log*** dan notifikasi dari aset TI diidentifikasi berdasarkan *event*. 2.3 *Log* dari aset TI yang masuk dianalisis berdasarkan parameter kewajaran. 2.4 *Log* dari aset TI yang menjadi target ancaman dianalisis secara berkala berdasarkan parameter kewajaran.
3. Menentukan tingkat ancaman	3.1 **Jenis-jenis ancaman** di ranah siber diinventaris berdasarkan *best practice*. 3.2 Rincian *payload* serangan terhadap target yang masuk ke dalam aset TI ditinjau ulang berdasarkan parameter kewajaran. 3.3 Rincian *payload* serangan diverifikasi untuk memastikan keabsahan serangan berdasarkan aset TI yang dipantau.
4. Melakukan penelusuran terhadap *threat intelligence* data terhadap ancaman yang masuk untuk mendapatkan informasi mengenai ancaman yang datang	4.1 Sumber data *threat intelligence* yang *valid* ditentukan berdasarkan **tipe organisasi**. 4.2 Sumber yang menjadi ancaman dianalisis berdasarkan data *threat intelligence*.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
	4.3 Jenis ancaman yang masuk beserta tipenya dianalisis berdasarkan data *threat intelligence.*
5. Melakukan pengecekan korelasi dari beberapa *log* aset TI	5.1 *Log* dari aset TI yang terkait dievaluasi berdasarkan parameter kewajaran. 5.2 Laporan evaluasi *log* dari aset TI yang terkait dibuat berdasarkan parameter kewajaran.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Kenormalan dimaksud pada proses, indikator dan cara kerja sistem operasi pada *end point.*
   1.2 *Threat intelligence* adalah informasi yang diatur, dianalisis, dan disaring yang berkaitan tentang potensi atau serangan terkini yang mengancam organisasi. *Threat intelligence* merupakan sebuah teknologi modern dalam dunia siber untuk membantu suatu organisasi untuk mengumpulkan *cyber threat data* yang berasal dari berbagai sumber-sumber terpercaya seperti *Trusted Partner Intelligence*, *Open Source Inteligence*, *Internet Service Provider*, dan *International Internet Gateways*.
   1.3 Parameter kewajaran adalah kenormalan operasi dalam aset TI seperti *login*, waktu akses, proses yang berjalan, koneksi jaringan, lokasi mengakses, frekuensi akses, dan sebagainya.
   1.4 Tipe *log* meliputi *log* yang tidak terbatas pada sistem operasi, jaringan, perangkat lunak, perangkat keras, dan peralatan *network security.*
   1.5 Jenis-jenis ancaman ditentukan berdasarkan tingkat kerentanan disandingkan dengan tingkat strategis atau kegentingan aset.
   1.6 Tipe organisasi di antaranya meliputi, namun tidak terbatas pada sektor pemerintahan, sektor finansial, BUMN, sektor perminyakan, sektor energi, sektor swasta, sektor kesehatan, dan sektor telekomunikasi.

2. Peralatan dan perlengkapan
    2.1 Peralatan
        2.1.1 Perangkat keras komputer
        2.1.2 Perangkat lunak analisis *threat intelligence*
        2.1.3 Sumber data *threat intelligence*
    2.2 Perlengkapan
        2.2.1 Media penyimpanan
        2.2.2 *Printer*
        2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
    3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah terakhir pada Undang - Undang Nomor 19 Tahun 2016
    3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik sebagaimana diubah terakhir pada Peraturan Pemerintah Nomor 71 Tahun 2019

4. Norma dan standar
    4.1 Norma
        (Tidak ada.)
    4.2 Standar
        4.2.1 SNI ISO/IEC 27035 -1:2016 Teknologi informasi - Teknik Keamanan - Manajemen insiden keamanan informasi - Bagian 1: Prinsip manajemen insiden
        4.2.2 SNI ISO/IEC 27035 - 2:2016 Teknologi informasi – Teknik Keamanan – Manajemen insiden keamanan informasi – Bagian 2: Pedoman perencanaan dan persiapan respon insiden
        4.2.3 NIST *Cyber Security Framework Version 1.1 Framework for Improving Critical Infrastructure Cybersecurity*

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.
   1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.
   1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan.
   1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara, serta metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 *Threat modelling framework*
      3.1.2 *Threat intelligence framework*
      3.1.3 Analisis *malware*
      3.1.4 Teknik pengumpulan dan akuisisi data
   3.2 Keterampilan
      3.2.1 Mengoperasikan *threat intelligence platform*
      3.2.2 Menjalankan *sandboxing/enrichment*
      3.2.3 Membaca *log* dan *payload*
      3.2.4 Melakukan analisis dengan berbagai pendekatan strategis dan teknis
      3.2.5 Membuat laporan yang efektif

4. Sikap kerja yang diperlukan
    4.1 Teliti
    4.2 Objektif
    4.3 Tanggung jawab
    4.4 Integritas

5. Aspek kritis
    5.1 Kecermatan menganalisis anomali *log* berdasarkan parameter kewajaran
    5.2 Kecermatan dalam meninjau ulang rincian *payload* serangan terhadap target yang masuk ke dalam aset TI berdasarkan parameter kewajaran
    5.3 Kecermatan dalam menganalisis sumber yang menjadi ancaman berdasarkan data *threat intelligence*

KODE UNIT : **J.62SOC00.008.1**

JUDUL UNIT : **Melakukan Pemantauan Aset Teknologi Informasi (TI) terhadap Aktivitas Ancaman Siber**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan pemantauan terhadap aktivitas yang rentan ancaman siber.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi daftar aset TI yang rentan terhadap ancaman siber	1.1 Daftar aset TI diidentifikasi berdasarkan tingkat kegentingan. 1.2 Daftar **aktivitas siber** yang mencurigakan diidentifikasi berdasarkan **informasi ancaman**. 1.3 **Daftar kerentanan** aset TI secara umum dikumpulkan berdasarkan informasi internal dan eksternal
2. Memantau aktivitas yang dapat menyebabkan ancaman siber	2.1 Aktivitas siber yang teridentifikasi dianalisis sesuai prosedur 2.2 **Dokumentasi aktivitas** dibuat berdasarkan temuan

BATASAN VARIABEL

1. Konteks variabel
   1.1 Aktivitas siber yang dimaksud di antaranya, namun tidak terbatas pada *information security event, information security vulnerability,* dan *network activity.*
   1.2 Informasi ancaman yang dimaksud adalah informasi yang dapat digunakan untuk mengindetifikasi, menganalisis, memonitor dan merespon adanya suatu ancaman siber. Informasi ancaman terdiri namun tidak terbatas pada *Indicator of Compromises* (IOC), teknik, taktik dan prosedur yang didapat dari berbagai macam sumber (*threat intelligence).*
   1.3 Daftar kerentanan yang dibuat terdiri atas informasi mengenai kerentanan (*vulnerability*) yang didapat dari pemasok, MITRE CVE (*Common Vulnerability Exposure*), MITRE CWE (*Common Weakness*

Enumeration), NVD (*National Vulnerability Database*), *Security Advisory* Badan Siber dan Sandi Negara (BSSN), laporan *pentest* dan laporan *bug hunter.*

1.4 Dokumentasi aktivitas berisi bukti (*evidence)* anomali dan serangan.

2. Peralatan dan perlengkapan

4.1 Peralatan

2.1.1 Komputer atau server

2.1.2 Perangkat lunak sistem pemantauan

2.1.3 Perangkat lunak pengolah kata

4.2 Perlengkapan

2.2.1 Media Penyimpanan

2.2.2 *Printer*

2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana terakhir diubah pada Undang-Undang Nomor 19 Tahun 2016

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik sebagaimana terakhir diubah pada Peraturan Pemerintah Nomor 71 Tahun 2019

4. Norma dan standar

2.1 Norma

(Tidak ada.)

2.2 Standar

4.2.1 SNI ISO/IEC 27035 -1:2016 Teknologi informasi - Teknik Keamanan - Manajemen insiden keamanan informasi - Bagian 1: Prinsip manajemen insiden

4.2.2 SNI ISO/IEC 27035 - 2:2016 Teknologi informasi – Teknik Keamanan – Manajemen insiden keamanan informasi –

Bagian 2: Pedoman perencanaan dan persiapan respon insiden

4.2.3 NIST *Cyber Security Framework Version 1.1 Framework for Improving Critical Infrastructure Cybersecurity*

4.2.4 MITRE ATT&CK *Matrix for Enterprise*

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.

1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan.

1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara, serta metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang konsep dasar keamanan informasi (pengelolaan risiko; ketersediaan, integritas dan kerahasiaan; orang, proses dan teknologi; keamanan fisik)

3.1.3 Pengetahuan dasar tentang teknologi keamanan informasi fundamental (kontrol akses, *patch management*, anti

malware, anti spam, *firewall, Intrusion Prevention Systems* (IPS))

3.1.4 Pengetahuan dasar perlindungan informasi (*backup* dan enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan perangkat lunak

3.2.2 Mendeteksi potensi pelanggaran keamanan

3.2.3 Mengaplikasikan petunjuk operasional perangkat pemantauan *traffic*

4. Sikap kerja yang diperlukan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

4.4 Integritas

5. Aspek kritis

5.1 Kecermatan dalam mengidentifikasi aktivitas siber yang mencurigakan berdasarkan informasi ancaman

5.2 Kecermatan dalam menganalisis aktivitas siber yang sudah teridentifikasi sesuai prosedur

KODE UNIT : **J.62SOC00.009.1**

JUDUL UNIT : **Mengelompokkan Insiden Keamanan Siber yang Terjadi Sesuai dengan Tingkat Kegentingan**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengelompokkan insiden keamanan siber yang terjadi sesuai dengan tingkat kegentingan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan dampak (*impact*) dari sebuah insiden keamanan siber	1.1 Pengguna yang terdampak diidentifikasi berdasarkan **data pengguna sistem**. 1.2 Aset TI yang terdampak diidentifikasi berdasarkan **katalog layanan**. 1.3 Nilai dampak ditetapkan berdasarkan pengguna dan aset terdampak yang telah diidentifikasi.
2. Menentukan tingkat urgensi dari sebuah insiden keamanan siber	2.1 Layanan terdampak diidentifikasi berdasarkan acuan pada suatu organisasi. 2.2 Tingkat urgensi ditetapkan berdasarkan layanan terdampak.
3. Menentukan level prioritas	3.1 Level prioritas ditetapkan berdasarkan ***priority matrix*** yang menjadi acuan. 3.2 Waktu respon ditetapkan berdasarkan level prioritas.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Data pengguna sistem merupakan daftar entitas yang menggunakan atau mengakses layanan yang dikelola oleh organisasi.
   1.2 Katalog layanan merupakan dokumen yang dapat berisi rekaman semua data misalnya terkait daftar aset, daftar konfigurasi, layanan operasional, layanan teknis, dan layanan bisnis yang dikelola oleh organisasi.

1.3 *Priority matrix* merupakan matriks yang digunakan untuk memetakan sebuah insiden keamanan siber dengan tingkat kegentingan berdasarkan variabel dampak dan urgensi insiden tersebut guna mendapatkan keputusan insiden mana yang lebih diprioritaskan untuk direspon.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat keras komputer
      2.1.2 Perangkat lunak pengolah kata
      2.1.3 Koneksi jaringan
   2.2 Perlengkapan
      2.2.1 Daftar pengguna dan katalog layanan (*service catalog*)
      2.2.2 *Priority Matrix*
      2.2.3 Media penyimpanan
      2.2.4 Printer
      2.2.5 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 sebagaimana diubah dengan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
      4.2.1 SNI ISO/IEC TR 20000 - 1:2013 Teknologi informasi - Manajemen layanan - Bagian 1: Persyaratan sistem manajemen layanan

4.2.2 SNI ISO/IEC 27035 -1:2016 Teknologi informasi - Teknik Keamanan - Manajemen insiden keamanan informasi - Bagian 1: Prinsip manajemen insiden

4.2.3 SNI ISO/IEC 27035 - 2:2016 Teknologi informasi – Teknik Keamanan – Manajemen insiden keamanan informasi – Bagian 2: Pedoman perencanaan dan persiapan respon insiden

PANDUAN PENILAIAN

1. Konteks penilaian

   1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

   1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja/Tempat Uji Kompetensi (TUK)/pada tempat yang disimulasikan.

   1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitasi asesmen yang dibutuhkan.

   1.4 Metode asesmen yang diterapkan dapat meliputi kombinasi dari metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan/atau wawancara serta metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

   3.1 Pengetahuan

      3.1.1 Standar yang berlaku terkait dengan keamanan informasi

      3.1.2 Pengetahuan dasar tentang keamanan informasi

3.1.3 *Security-to-Business Integration* – pengetahuan bagaimana insiden keamanan mempengaruhi proses bisnis, pemodelan ancaman, dan penilaian serangan

3.1.4 Dasar-dasar protokol jaringan komputer pemahaman dasar HTTP, DNS, SMB, SMTP, dan *tools* terkait

3.1.5 Pengelolaan Insiden Keamanan Informasi

3.1.6 Sistem Manajemen Keamanan Informasi (SMKI)

3.2 Keterampilan

3.2.1 Mengumpulkan dan menganalisis informasi yang diperoleh

3.2.2 Mengoperasikan perangkat keras dan perangkat lunak

3.2.3 Menyusun laporan dan presentasi yang efektif

3.2.4 Membuat ringkasan pengetahuan teknis

4. Sikap kerja

4.1 Cermat

4.2 Objektif

4.3 Tanggung jawab

5. Aspek Kritis

5.1 Ketepatan dalam menetapkan nilai dampak berdasarkan pengguna dan aset terdampak yang telah diidentifikasi

5.2 Ketepatan dalam menetapkan tingkat urgensi berdasarkan layanan terdampak

KODE UNIT : **J.62S0C00.010.1**

JUDUL UNIT : **Memberikan Tiket terhadap Insiden Keamanan Siber**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam memberikan tiket terhadap insiden keamanan siber.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Memproses tiket terhadap insiden keamanan siber	1.1 **Jenis tiket** diidentifikasi sesuai kebutuhan. 1.2 Tiket ditentukan sesuai dengan **parameter.**
2. Mendistribusikan tiket terhadap insiden keamanan siber	2.1 Sistem tiket diidentifikasi sesuai kebutuhan. 2.2 **Layanan tiket** dilaksanakan sesuai hasil identifikasi sistem tiket.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Jenis tiket dapat dikategorikan:
      1.1.1 Berdasarkan obyek terkena insiden keamanan siber:
         a. Server.
         b. Perangkat jaringan.
         c. Perangkat komputer/laptop/HP.
         d. Aplikasi.
         e. Dan lain-lain.
      1.1.2 Berdasarkan jenis spesifik insiden keamanan siber:
         a. *Account compromise.*
         b. *Data theft.*
         c. *Exploitation of weak configuration.*
         d. *Exploitation of weak architecture.*
         e. *Patched software exploitation.*
         f. *Network penetration.*
         g. *Service disruption.*

h. *Vulnerability.*
i. *Phising.*
j. Dan lain-lain.

1.1.3 Dan jenis lain sesuai kebutuhan organisasi.

1.2 Parameter tiket meliputi:

1.2.1 Jenis tiket.

1.2.2 Deskripsi.

1.2.3 Tingkat kegentingan dari insiden keamanan siber (*Low, Medium, High).*

1.2.4 Tingkat sensitivitas insiden keamanan siber.

1.2.5 Dapat menggunakan protokol *Traffic Light Protocol* (TLP) yang umum digunakan respon insiden keamanan siber dalam kategori *sharing information* (RED, AMBER, GREEN, WHITE).

1.2.6 Tujuan/pihak pelaksana tiket ditentukan (merujuk struktur organisasi SOC terkait).

1.2.7 Dan lain-lain.

1.3 Layanan tiket mencakup bisnis proses dari organisasi, sistem tiket, dan distribusinya.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Perangkat keras komputer

2.1.2 Perangkat lunak sistem tiket

2.2 Perlengkapan

2.2.1 Media Penyimpanan

2.2.2 *Printer*

2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 sebagaimana diubah dengan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
      4.2.1 SNI ISO/IEC 27035 -1:2016 Teknologi informasi - Teknik Keamanan - Manajemen insiden keamanan informasi - Bagian 1: Prinsip manajemen insiden
      4.2.2 SNI ISO/IEC 27035 - 2:2016 Teknologi informasi – Teknik Keamanan – Manajemen insiden keamanan informasi – Bagian 2: Pedoman perencanaan dan persiapan respon insiden

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.
   1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja/Tempat Uji Kompetensi (TUK)/pada tempat yang disimulasikan.
   1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitasi asesmen yang dibutuhkan.
   1.4 Metode asesmen yang diterapkan dapat meliputi kombinasi dari metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan/atau wawancara serta metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
    3.1 Pengetahuan
        3.1.1 Pengetahuan mengenai penentuan jenis tiket, parameter tiket, tingkat kegentingan insiden keamanan siber, dan tingkat sensitivitas insiden keamanan siber
        3.1.2 Pengetahuan mengenai organisasi dan proses bisnis
        3.1.3 Sistem Manajemen Keamanan Informasi (SMKI)
    3.2 Keterampilan
        3.2.1 Mengoperasikan perangkat keras dan perangkat lunak pengelolaan tiket
        3.2.2 Memilah atau mengklasifikasikan insiden keamanan siber
        3.2.3 Mengelola insiden keamanan siber
        3.2.4 Penanganan atau respon terhadap insiden keamanan siber

4. Sikap kerja yang diperlukan
    4.1 Teliti
    4.2 Objektif
    4.3 Tanggung jawab

5. Aspek kritis
    5.1 Kecermatan dalam memberikan layanan tiket sesuai hasil identifikasi sistem tiket

KODE UNIT : **J.62S0C00.011.1**

JUDUL UNIT : **Menganalisis *Log* pada *Security Operations Center* (SOC)**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menganalisis *log* yang berkaitan dengan insiden keamanan siber.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan jenis *log*	1.1 Salinan *log* disiapkan sesuai kebutuhan. 1.2 **Jenis *log*** diidentifikasi berdasarkan kebutuhan.
2. Memeriksa *log*	2.1 **Parameter kewajaran** ditentukan sesuai kebutuhan. 2.2 ***Log* artefak** diidentifikasi sesuai parameter kewajaran.
3. Mendokumentasikan kegiatan analisis *log*	3.1 Hasil pemeriksaan *log* didokumentasikan sesuai kebutuhan. 3.2 Laporan analisis *log* disusun sesuai format laporan.

BATASAN VARIABEL

1. Konteks variabel
    1.1 Jenis log dikategorikan menjadi:
        1.1.1 *Security Software logs*:
            a. *Antimalware software.*
            b. *Intrusion detection and intrusion prevention systems.*
            c. *Remote access software.*
            d. *Web proxies.*
            e. *Vulnerability management software.*
            f. *Authentication servers.*
            g. *Routers.*
            h. *Firewalls.*
            i. *Network quarantine servers.*
            j. Dan lain-lain.

1.1.2 *Operating system logs.*

1.1.3 *Application logs.*

1.2 *Log* artefak merupakan salinan *log* yang sudah disiapkan untuk dilakukan analisis.

1.3 Parameter kewajaran merupakan poin yang perlu diperiksa dalam rangka melakukan analisis *log*, meliputi:

1.3.1 Informasi *severity log* (*Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug*).

1.3.2 Statistik *log.*

1.3.3 Linimasa *log.*

1.3.4 Karakteristik *log* (sub konten/*field*/*metadata log*).

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Perangkat keras komputer

2.1.2 Perangkat lunak olah *data*/*log*

2.1.3 Perangkat lunak pengolah kata

2.2 Perlengkapan

2.2.1 Media penyimpanan (*imaging*/*copy log*)

2.2.2 *Printer*

2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 sebagaimana diubah dengan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27001:2013 Teknologi informasi - Teknik keamanan Sistem manajemen keamanan informasi - Persyaratan

4.2.2 NIST 800-92 *Guide to Computer Security Log Management*

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja/Tempat Uji Kompetensi (TUK)/pada tempat yang disimulasikan.

1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitasi asesmen yang dibutuhkan.

1.4 Metode asesmen yang diterapkan dapat meliputi kombinasi dari metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan/atau wawancara serta metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Manajemen *log security*

3.1.2 Jaringan komputer organisasi dan proses bisnis

3.1.3 Teknis yang mendalam tentang jaringan, titik akhir, intelijensi ancaman, forensik, rekayasa balik *malware*, dan fungsi dari aplikasi spesifik atau infrastruktur TI yang mendasarinya

3.1.4 Sistem Menajemen Keamanan Informasi (SMKI)

3.2 Keterampilan

3.2.1 Mengumpulkan dan mengolah data terkait *log*

3.2.2 Mengoperasikan alat *Security Information and Event Management* (SIEM)

3.2.3 Menganalisis data berdasarkan hasil temuan pada SIEM

3.2.4 Mengidentifikasi jenis *log*

3.2.5 Menentukan *device config*

3.2.6 Mengolah data yang bersumber dari *traffic capture*

3.2.7 Melakukan *performance monitoring*

3.2.8 Melakukan *device monitoring*

3.2.9 Melakukan dan membuat penetapan rekomendasi tindak lanjut penyelidikan

4. Sikap kerja yang diperlukan

4.1 Teliti

4.2 Objektif

4.3 Tanggung jawab

5. Aspek kritis

5.1 Kecermatan dalam menentukan parameter kewajaran sesuai kebutuhan

5.2 Kecermatan dalam mengidentifikasi *log* artefak sesuai parameter kewajaran

KODE UNIT : **J.62SOC00.012.1**

JUDUL UNIT : **Melakukan Pencadangan Data *Security Operations Center* (SOC)**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam pencadangan data untuk memastikan ketersediaan data yang berkaitan dengan *Security Operations Center* (SOC).

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menyiapkan pencadangan data	1.1 Pencadangan **data SOC** diidentifikasi berdasar kebijakan retensi data. 1.2 Interval waktu dan retensi penyimpanan data ditentukan sesuai dengan kebijakan retensi data. 1.3 Perangkat pencadangan disiapkan sesuai dengan prosedur. 1.4 **Aspek kecukupan** perangkat pencadangan diidentifikasi berdasarkan kebutuhan.
2. Melaksanakan pencadangan data	2.1 **Prosedur pencadangan** dilakukan berdasarkan kebijakan yang ditentukan. 2.2 Pencadangan data dilaporkan kepada pihak terkait sesuai prosedur.
3. Melaksanakan pemulihan pencadangan data	3.1 Prosedur pemulihan cadangan data dilakukan sesuai ketentuan. 3.2 **Pemulihan pencadangan data** dilaporkan kepada pihak terkait.
4. Melaksanakan penghapusan data yang sudah melalui masa retensi	4.1 Data pencadangan yang telah lewat masa retensinya diidentifikasi sesuai kebijakan. 4.2 Penghapusan data cadangan dilakukan sesuai prosedur. 4.3 **Penghapusan pencadangan data** dilaporkan kepada pihak terkait.

BATASAN VARIABEL

1. Konteks variabel
   2.1 Data SOC adalah semua data yang terkait dengan kegiatan SOC, mulai dari data sensor, data informasi hasil proses analisis keamanan, dan data konfigurasi perangkat SOC.
   2.2 Pencadangan Data dalam konteks SOC adalah kegiatan pencadangan data SOC yang ada pada media penyimpanan jangka pendek dan masa hidupnya telah melewati kebijakan retensi data sehingga harus dicadangkan ke media penyimpanan jangka panjang.
   2.3 Aspek Kecukupan adalah tercukupinya media penyimpanan jangka panjang untuk melakukan pencadangan data yang melingkupi seluruh data SOC yang harus dicadangkan sesuai kebijakan retensi data.
   2.4 Prosedur Pencadangan Data, Pemulihan Data, dan Penghapusan data SOC adalah prosedur operasional standar yang telah dibakukan dan disahkan dalam lingkup organisasi yang berisi panduan atau langkah-langkah instruksi dalam melakukan pencadangan data, pemulihan data, dan penghapusan data yang harus ditaati.
   2.5 Pemulihan Pencadangan Data dalam konteks SOC adalah kegiatan memulihkan data cadangan yang diminta oleh pihak lain dalam SOC untuk kepentingan seperti (namun tidak terbatas pada) forensik digital, analisis keamanan, maupun pemulihan operasional SOC.
   2.6 Penghapusan Data dalam konteks SOC adalah kegiatan penghapusan data SOC yang telah melewati masa retensinya sesuai kebijakan retensi data dan harus dihapus dengan cara yang aman sehingga data tidak bisa ditampilkan kembali dan media penyimpanan dapat digunakan kembali untuk data baru.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer

2.1.2 Media penyimpanan data

2.2 Perlengkapan

2.2.1 Kebijakan retensi data organisasi

2.2.2 Prosedur pencadangan data

2.2.3 Prosedur pemulihan data

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 sebagaimana diubah dengan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27001:2013 Teknologi informasi - Teknik keamanan Sistem manajemen keamanan informasi - Persyaratan Annex A 12 3

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja/Tempat Uji Kompetensi (TUK)/pada tempat yang disimulasikan.

1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitasi asesmen yang dibutuhkan.

1.4 Metode asesmen yang diterapkan dapat meliputi kombinasi dari metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan/atau wawancara serta metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Dasar arsitektur komputer
      3.1.2 Manajemen data
      3.1.3 Teknologi pencadangan dan penghapusan data
      3.1.4 Klasifikasi data
      3.1.5 Sistem Manajemen Keamanan Informasi (SMKI)
   3.2 Keterampilan
      3.2.1 Melaksanakan pencadangan dan pemulihan data sesuai prosedur
      3.2.2 Mengoperasikan perangkat keras dan perangkat lunak pencadangan dan pemulihan data
      3.2.3 Menyusun laporan sesuai format

4. Sikap kerja yang diperlukan
   4.1 Teliti
   4.2 Objektif
   4.3 Tanggung jawab
   4.4 Cermat

5. Aspek kritis
   5.1 Kecermatan dalam mengidentifikasi pencadangan data SOC berdasarkan kebijakan retensi data organisasi
   5.2 Ketepatan melakukan prosedur pencadangan berdasarkan kebijakan yang ditentukan

KODE UNIT : **J.62SOC00.013.1**

JUDUL UNIT : **Mengkomunikasikan Penanganan Insiden Keamanan Siber dan Manajemen Krisis**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengkomunikasikan penanganan insiden keamanan siber dan manajemen krisis.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melaksanakan prosedur komunikasi penanganan insiden keamanan siber yang telah ditentukan	1.1 Langkah-langkah komunikasi penanganan insiden keamanan siber kepada **pihak terkait** dilaksanakan sesuai **prosedur komunikasi**. 1.2 Komunikasi rutin antar petugas SOC untuk mendapatkan informasi terbaru dilaksanakan sesuai prosedur.
2. Melakukan komunikasi penanganan insiden keamanan siber kepada pihak terkait	2.1 Komunikasi penanganan insiden keamanan siber dilaksanakan berdasarkan pihak terkait dan **tujuan komunikasi**. 2.2 Laporan komunikasi penanganan insiden keamanan siber kepada pihak terkait dibuat sesuai prosedur.
3. Melaksanakan prosedur komunikasi manajemen krisis apabila keadaan tidak terkendali	3.1 Langkah-langkah komunikasi **manajemen krisis** dilaksanakan sesuai prosedur komunikasi manajemen krisis. 3.2 Laporan pelaksanaan komunikasi manajemen krisis dibuat sesuai prosedur.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Pihak terkait adalah seluruh pihak baik internal maupun eksternal yang merupakan pemangku kepentingan (*stakeholder*) dari kegiatan komunikasi penanganan insiden keamanan siber dan manajemen krisis.

1.2 Prosedur komunikasi adalah tata cara yang disusun dalam rangka pelaksanaan komunikasi penanganan insiden keamanan siber dan manajemen krisis.

1.3 Tujuan komunikasi merupakan hasil akhir dan harapan dari pelaksanaan komunikasi.

1.4 Manajemen krisis adalah proses organisasi dalam menangani kejadian yang mengganggu dan tidak terduga yang dapat mengancam dan membahayakan organisasi atau para pemangku kepentingan.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Peralatan komunikasi

2.1.2 Aplikasi penanganan insiden keamanan siber

2.1.3 Perangkat komputer

2.1.4 Perangkat jaringan

2.2 Perlengkapan

2.2.1 Media penyimpanan

2.2.2 Printer

2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

(Tidak ada.)

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27035-1:2016 Teknologi informasi – Teknik Keamanan – Manajemen Insiden Keamanan Informasi – Bagian 1: Prinsip Manajemen Insiden

4.2.2 SNI ISO/IEC 27035-2:2016 Teknologi informasi – Teknik Keamanan – Manajemen Insiden Keamanan Informasi –

Bagian 2: Pedoman Perencanaan dan Persiapan respon Insiden

4.2.3 ISO 22301:2019 *Security and Resilience – Business Continuity Management System – Requirements*

4.2.4 Standar Operasional Prosedur (SOP) atau petunjuk teknis komunikasi penanganan insiden dalam organisasi

4.2.5 Standar Operasional Prosedur (SOP) atau petunjuk teknis komunikasi manajemen krisis dalam organisasi

PANDUAN PENILAIAN

1. Konteks penilaian

   1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

   1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.

   1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan.

   1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

   3.1 Pengetahuan

      3.1.1 Organisasi dan proses bisnis

      3.1.2 Komunikasi manajemen krisis

      3.1.3 Sistem Manajemen Keamanan Informasi (SMKI)

3.2 Keterampilan

3.2.1 Melaksanakan prosedur komunikasi penanganan insiden keamanan siber secara tepat

3.2.2 Melaksanakan prosedur komunikasi manajemen krisis secara tepat

4. Sikap kerja yang diperlukan

4.1 Teliti

4.2 Objektif

4.3 Tanggung jawab

4.4 Integritas

5. Aspek kritis

5.1 Kemampuan komunikasi penanganan insiden keamanan siber kepada pihak terkait yang berdasarkan tujuan komunikasi

5.2 Ketepatan menentukan langkah-langkah komunikasi manajemen krisis sesuai prosedur komunikasi manajemen krisis

KODE UNIT : **J.62SOC00.014.1**

JUDUL UNIT : **Melakukan Investigasi Modus Operandi Insiden Keamanan Siber**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan investigasi terhadap modus operandi insiden keamanan siber yang terjadi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melaksanakan prosedur awal penanganan insiden keamanan siber	1.1 Alat investigasi berupa perangkat keras dan perangkat lunak disiapkan berdasarkan prosedur. 1.2 **Informasi** terkait dengan insiden dikumpulkan berdasarkan prosedur.
2. Melakukan analisis modus serangan	2.1 *Log* dan *traffic* dari aset TI yang terdampak dianalisis berdasarkan **parameter kewajaran**. 2.2 **Informasi *live*** yang terkait dengan insiden keamanan siber dianalisis berdasarkan parameter kewajaran. 2.3 **Modus operandi** ditentukan sesuai dengan hasil analisis.
3. Mendokumentasikan kegiatan	3.1 Modus serangan didokumentasikan sesuai prosedur. 3.2 Laporan kegiatan investigasi sistem terdampak disusun sesuai format laporan.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Informasi mencakup konfigurasi awal, aset yang terdampak, jenis insiden, parameter insiden (waktu, sumber, tipe), infrastruktur yang terdampak, dan analisis *log*.
   1.2 Parameter kewajaran merupakan poin yang perlu diperiksa dalam rangka melakukan analisa *log*, meliputi:
      1.2.1 Informasi *severity log (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug*)
      1.2.2 Statistik *log*

1.2.3 Linimasa *log*

1.2.4 Karakteristik *log* (sub konten/*field*/*metadata log*)

1.3 Informasi *live* berupa lalu lintas data dari dan ke arah aset TI (perangkat keamanan TI, dan perangkat *endpoint* terdampak), dan Karakteristik program jahat (*malware*, *trojan*, virus, *backdoor*).

1.4 Modus operandi adalah cara yang dilakukan oleh pelaku dalam melakukan serangan siber (memuat target/sumber kerentanan, jalur serangan, dan pola serangan).

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Perangkat keras komputer

2.1.2 Perangkat jaringan

2.1.3 Perangkat lunak alat bantu investigasi

2.1.4 Perangkat lunak pengolah kata

2.2 Perlengkapan

2.2.1 Media penyimpanan

2.2.2 *Printer*

2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

(Tidak ada.)

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27032:2014 Teknologi Informasi - Teknik Keamanan - Pedoman Keamanan Siber

4.2.2 SNI ISO/IEC 27035-1:2016 Teknologi informasi – Teknik Keamanan – Manajemen Insiden Keamanan Informasi – Bagian 1: Prinsip Manajemen Insiden

4.2.3 SNI ISO/IEC 27035-2:2016 Teknologi informasi – Teknik Keamanan – Manajemen Insiden Keamanan Informasi –

Bagian 2: Pedoman Perencanaan dan Persiapan respon Insiden

4.2.4 SNI ISO/IEC 27037:2014 Teknologi Informasi - Teknik Keamanan - Pedoman Identifikasi, Pengumpulan, Akuisisi, dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.
   1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.
   1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan.
   1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Manajemen insiden keamanan informasi
      3.1.2 Infrastruktur jaringan
      3.1.3 Prosedur penanganan insiden keamanan siber
      3.1.4 Sistem Manajemen Keamanan Informasi (SMKI)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan perangkat lunak investigasi siber

3.2.2 Menganalisis informasi yang dimiliki

4. Sikap kerja yang diperlukan

4.1 Teliti

4.2 Objektif

4.3 Tanggung jawab

4.4 Bekerjasama dalam tim

5. Aspek kritis

5.1 Ketepatan dalam menganalisis *log* dan *traffic* dari aset TI yang terdampak berdasarkan parameter kewajaran

5.2 Ketepatan dalam menentukan modus operandi sesuai dengan hasil analisis

KODE UNIT : **J.62SOC00.015.1**

JUDUL UNIT : **Mengidentifikasi Solusi Teknis terhadap Insiden Keamanan Siber yang Terjadi**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengidentifikasi solusi teknis terhadap insiden keamanan siber yang terjadi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melakukan analisis terhadap insiden keamanan siber yang terjadi berdasarkan data yang dikumpulkan	1.1 Penyebab atau sumber insiden diidentifikasi berdasarkan informasi insiden keamanan siber. 1.2 Prakiraan dampak insiden keamanan siber dinilai berdasarkan kerugian yang ditimbulkan.
2. Memberikan rekomendasi solusi teknis	2.1 **Alternatif solusi** dikembangkan berdasarkan jenis insiden keamanan siber yang terjadi. 2.2 Alternatif solusi yang ada dinilai berdasarkan kecukupan **sumber daya** yang ada. 2.3 Rekomendasi solusi teknis diajukan berdasarkan hasil analisis kepada **pihak terkait**.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Alternatif solusi antara lain isolasi, terminasi, format, *restore,* dan sebagainya.
   1.2 Sumber daya mencakup Sumber Daya Manusia (SDM), teknologi, dan anggaran.
   1.3 Pihak terkait yang dimaksud adalah manajemen internal organisasi/perusahaan.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat keras komputer

2.1.2 Perangkat jaringan

2.1.3 Perangkat lunak pengolah kata

2.2 Perlengkapan

2.2.1 Media penyimpanan

2.2.2 Printer

2.2.3 Alat Tulis Kantor (ATK)

2.2.4 *Log* kejadian/simulasi insiden keamanan siber

3. Peraturan yang diperlukan

3.1 Undang–Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaiman diubah terakhir pada Undang–Undang Nomor 19 Tahun 2016

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik sebagaimana diubah terakhir pada Peraturan Pemerintah Nomor 71 Tahun 2019

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.4 SNI ISO/IEC 27035-1:2016 Teknologi informasi – Teknik Keamanan – Manajemen Insiden Keamanan Informasi – Bagian 1: Prinsip Manajemen Insiden

4.2.5 SNI ISO/IEC 27035-2:2016 Teknologi informasi – Teknik Keamanan – Manajemen Insiden Keamanan Informasi – Bagian 2: Pedoman Perencanaan dan Persiapan respon Insiden

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan

peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.

1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan.

1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 *Log security*

3.1.2 Manajemen insiden keamanan informasi

3.1.3 Karakteristik dan jenis-jenis insiden keamanan siber

3.1.4 Solusi teknis terhadap insiden keamanan siber

3.1.5 Sistem Manajemen Keamanan Informasi (SMKI)

3.2 Keterampilan

3.2.1 Membuat prakiraan dampak insiden keamanan siber

3.2.2 Menghitung kecukupan sumber daya

3.2.3 Mengoperasikan *tools* analisis

4. Sikap kerja yang diperlukan

4.1 Teliti

4.2 Objektif

4.3 Tanggung jawab

5. Aspek kritis
    5.1 Ketepatan dalam mengidentifikasi penyebab atau sumber insiden yang terjadi berdasarkan informasi insiden keamanan siber
    5.2 Ketepatan dalam memberikan rekomendasi solusi teknis berdasarkan hasil analisis kepada pihak terkait

KODE UNIT : **J.62SOC00.016.1**

JUDUL UNIT : **Mengisolasi Aset Teknologi Informasi (TI) yang Terdampak untuk Menghentikan Insiden Keamanan Siber**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan isolasi terhadap aset TI yang terdampak untuk menghentikan insiden keamanan siber.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan apakah insiden keamanan siber dapat diisolasi	1.1 **Informasi** terkait insiden dianalisis berdasarkan keterhubungannya dengan aset TI lainnya. 1.2 Insiden keamanan siber yang dapat diisolasi ditentukan berdasarkan hasil analisis.
2. Melakukan isolasi terhadap aset TI terdampak	2.1 **Isolasi** terhadap aset TI yang terdampak dilakukan berdasarkan prosedur dan kewenangan. 2.2 Isolasi terhadap **aset TI yang terdampak** insiden keamanan siber disampaikan kepada **pihak terkait**.
3. Melakukan penghentian insiden keamanan siber	3.1 Insiden keamanan siber dihentikan berdasarkan prosedur dan kewenangan. 3.2 Melakukan *monitoring* pada aset TI yang diisolasi untuk memastikan insiden keamanan siber telah berhasil dihentikan berdasarkan informasi.
4. Melakukan pencabutan isolasi terhadap aset TI yang terdampak insiden	4.1 Informasi pencabutan isolasi dikomunikasikan kepada pihak terkait. 4.2 Pencabutan isolasi dilakukan sesuai dengan prosedur.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Informasi terkait insiden mencakup deskripsi aset TI yang terdampak, dampak yang ditimbulkan pada aset TI, jenis insiden,

modus serangan, ketersediaan cadangan, informasi *live*, *log* dan *traffic* dari aset TI yang terdampak, dan lainnya.

1.2 Isolasi mencakup *server*, *client*/*work station*, jaringan dan perangkatnya, jangka waktu, dan lainnya.

1.3 Aset TI yang terdampak yang dimaksud meliputi informasi, perangkat keras, perangkat lunak, dan sumber daya manusia yang rusak, hilang, dan/atau tidak dapat berfungsi secara normal karena insiden keamanan siber.

1.4 Pihak terkait adalah bisnis manajer dan tim tanggap insiden keamanan siber.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Perangkat keras komputer

2.1.2 Perangkat jaringan

2.1.3 Perangkat lunak pengolah kata

2.2 Perlengkapan

2.2.1 Media penyimpanan

2.2.2 Printer

2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

3.1 Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaiman diubah terakhir pada Undang – Undang Nomor 19 Tahun 2016.

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik sebagaimana diubah terakhir pada Peraturan Pemerintah Nomor 71 Tahun 2019

4. Norma dan standar

4.1 Norma

(Tidak ada)

4.2 Standar

4.2.1 SNI ISO/IEC 27035 -1:2016 Teknologi informasi - Teknik Keamanan - Manajemen insiden keamanan informasi - Bagian 1: Prinsip manajemen insiden

4.2.2 SNI ISO/IEC 27035 - 2:2016 Teknologi informasi – Teknik Keamanan – Manajemen insiden keamanan informasi – Bagian 2: Pedoman perencanaan dan persiapan respon insiden

4.2.3 Standar Operasional Prosedur (SOP) isolasi aset TI yang terdampak insiden keamanan siber pada organisasi

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.

1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan.

1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Infrastruktur teknologi informasi

3.1.2 Perangkat jaringan

3.1.3 Manajemen insiden keamanan informasi

3.1.4 Aset TI yang terdampak

3.1.5 Sistem Manajemen Keamanan Informasi (SMKI)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat jaringan yang terhubung dengan aset TI terdampak dalam hubungannya perlakuan dan pencabutan isolasi

3.2.2 Mengoperasikan sistem operasi dan perangkat lunak yang berhubungan dengan aktivitas penghentian insiden

4. Sikap kerja yang diperlukan

4.1 Teliti

4.2 Objektif

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam melakukan isolasi terhadap aset TI yang terdampak berdasarkan prosedur dan kewenangan sesuai dengan kesepakatan antara bisnis manajer dengan tim tanggap insiden keamanan siber

KODE UNIT : **J.62SOC00.017.1**

JUDUL UNIT : **Melakukan Terminasi Layanan terhadap Aset Teknologi Informasi (TI) yang Terdampak untuk Perbaikan**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan terminasi untuk perbaikan sistem.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan titik awal insiden keamanan siber	1.1 Titik awal (*entry point*) terhadap insiden keamanan siber diidentifikasi berdasarkan hasil investigasi modus operandi insiden keamanan siber. 1.2 *Log* internal dan *log* eksternal pada aset TI yang terdampak insiden keamanan siber dianalisis berdasarkan hasil investigasi modus operandi insiden keamanan siber. 1.3 Setiap ***indicator of compromise*** dikorelasikan berdasarkan hasil investigasi modus operandi insiden keamanan siber.
2. Melakukan terminasi terhadap aset TI yang terdampak	2.1. Terminasi terhadap aset TI yang terdampak dilakukan berdasarkan prosedur dan kewenangan yang diberikan. 2.2. *System restore/cleanup* yang terdampak diidentifikasi berdasarkan *back up system* yang tersedia. 2.3. Pengamanan terhadap hasil identifikasi terhadap titik awal insiden keamanan siber diterapkan sesuai prosedur respon insiden keamanan siber. 2.4. Informasi terminasi dikomunikasikan kepada **pihak terkait**.
3. Melakukan proses pencabutan terminasi	3.1 Informasi pencabutan terminasi dikomunikasikan kepada pihak terkait. 3.2 Pencabutan terminasi dilakukan sesuai dengan prosedur.

BATASAN VARIABEL

1. Konteks variabel
   1.1 *Indicator of Compromise* adalah indikasi-indikasi yang menginformasikan telah terjadinya suatu insiden keamanan siber.
   1.2 Pihak terkait adalah penanggung jawab aset TI, pemilik aset TI, dan pemilik bisnis.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat keras dan perangkat lunak yang menjadi objek terminasi
      2.1.2 Perangkat jaringan
      2.1.3 Perangkat lunak pengolah kata
      2.1.4 Perangkat lunak utilitas
   2.2 Perlengkapan
      2.2.1 Media penyimpanan
      2.2.2 *Printer*
      2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah terakhir pada Undang-Undang Nomor 19 Tahun 2016
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik sebagaimana diubah terakhir pada Peraturan Pemerintah Nomor 71 Tahun 2019

4. Norma dan standar
   4.1 Norma
      (Tidak ada)

4.2 Standar

4.2.1 SNI ISO/IEC 27035 -1:2016 Teknologi informasi - Teknik Keamanan - Manajemen insiden keamanan informasi - Bagian 1: Prinsip manajemen insiden

4.2.2 SNI ISO/IEC 27035 - 2:2016 Teknologi informasi – Teknik Keamanan – Manajemen insiden keamanan informasi – Bagian 2: Pedoman perencanaan dan persiapan respon insiden

4.2.3 *Information Technology Infrastructure Library* (ITIL): *Service Operation*

4.2.4 COBIT 2019 *Framework: Governance and Management Objectives*

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.

1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan.

1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada)

3. Pengetahuan dan keterampilan yang diperlukan
    3.1 Pengetahuan
        3.1.1 Manajemen insiden keamanan informasi
        3.1.2 Sistem Manajemen Keamanan Informasi (SMKI)
        3.1.3 Infrastruktur teknologi informasi dan komputer
        3.1.4 Perangkat jaringan
        3.1.5 Pengetahuan bisnis yang berhubungan dengan layanan aset TI yang terdampak
    3.2 Keterampilan
        3.2.1 Menentukan dan menganalisis *Indicator of Compromise* berdasarkan hasil investigasi insiden keamanan siber
        3.2.2 Mengoperasikan sistem operasi dan perangkat lunak yang berhubungan dengan aktivitas penghentian dan pemulihan layanan

4. Sikap kerja yang diperlukan
    4.1 Teliti
    4.2 Objektif
    4.3 Tanggung jawab

5. Aspek kritis
    5.1 Ketepatan dalam melakukan terminasi terhadap aset TI yang terdampak berdasarkan prosedur dan kewenangan yang diberikan

KODE UNIT : **J.62SOC00.018.1**

JUDUL UNIT : **Menganalisis Dampak Insiden Keamanan Siber**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam analisis profil insiden keamanan siber terhadap aset Teknologi Informasi (TI) organisasi beserta dengan penilaian dampak finansial dan nonfinansial yang diakibatkan dari insiden keamanan siber dalam rangka pemulihan sistem dalam organisasi terkait.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melakukan analisis profil insiden keamanan siber yang terjadi	1.1 Kerusakan dan/atau kehilangan pada aset dianalisis berdasarkan **informasi profil insiden keamanan siber** dan aset TI. 1.2 Aset TI/sistem terdampak insiden keamanan siber ditentukan berdasarkan hasil analisis.
2. Menilai kerugian finansial yang diakibatkan insiden keamanan siber yang terjadi	2.1. **Biaya langsung** dihitung berdasarkan biaya yang ditimbulkan agar sistem yang terdampak insiden keamanan siber dapat beroperasi kembali. 2.2. **Biaya tidak langsung** dihitung berdasarkan besarnya kerugian nonoperasional yang timbul karena sistem terdampak insiden keamanan siber. 2.3. **Biaya pemulihan** untuk setiap sistem terdampak insiden keamanan siber dihitung berdasarkan jumlah biaya langsung dan biaya tidak langsung.
3. Mengidentifikasi kerugian nonfinansial yang diakibatkan insiden keamanan siber yang terjadi	3.1 Dampak kerugian nonfinansial diidentifikasi berdasarkan analisis jangka panjang. 3.2 **Dampak terhadap industri** diidentifikasi berdasarkan laporan terkait.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Informasi profil insiden keamanan siber berupa nama, deskripsi, ancaman, *threat agent*, kerentanan, *Indicator of Compromise* (IoC), dan aset TI yang terdampak insiden keamanan siber.
   1.2 Biaya langsung adalah biaya yang langsung dapat dihitung sesuai dengan nilai kerusakan akibat insiden keamanan siber, termasuk biaya penggantian kerusakan dan/atau kehilangan aset, biaya perangkat baru yang harus dibeli, biaya konsultan untuk pemulihan, dan biaya langsung lainnya.
   1.3 Biaya tidak langsung termasuk biaya akibat rusaknya reputasi, kehilangan kesempatan bisnis, kehilangan data pribadi, kehilangan produktifitas karyawan, dan biaya terhadap pelanggaran kode etik, dan biaya tidak langsung lainnya.
   1.4 Biaya pemulihan adalah biaya yang dibutuhkan untuk melakukan pemulihan terhadap sistem sampai dalam kondisi sebelum insiden keamanan siber terjadi.
   1.5 Dampak terhadap industri di antaranya meningkatnya risiko investasi dan premi asuransi, tata kelola kebijakan baru serta kebutuhan industri untuk membangun *Computer Security Incident Response Team* (CSIRT), *Information Sharing and Analysis Center* (ISAC), dan *Honeynet.*

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat keras dan perangkat lunak komputer
      2.1.2 Perangkat jaringan
      2.1.3 Perangkat lunak pengolah kata
      2.1.4 Perangkat lunak utilitas
      2.1.5 Media komunikasi
   2.2 Perlengkapan
      2.2.1 Formulir survei atau interviu
      2.2.2 Media penyimpanan
      2.2.3 *Printer*
      2.2.4 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

   3.1 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik sebagaimana diubah terakhir pada Peraturan Pemerintah Nomor 71 Tahun 2019

   3.2 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik

4. Norma dan standar

   4.1 Norma

   (Tidak ada.)

   4.2 Standar

      4.2.1 SNI ISO/IEC 27035-1:2016 Teknologi informasi – Teknik Keamanan – Manajemen insiden keamanan informasi – Bagian 1: Prinsip manajemen insiden

      4.2.2 SNI ISO/IEC 27035-2:2016 Teknologi informasi – Teknik Keamanan – Manajemen insiden keamanan informasi – Bagian 2: Pedoman perencanaan dan persiapan respon insiden

      4.2.3 NIST SP 800–61 *Revision* 2 *Computer Security Incident Handling Guide*

      4.2.4 *Information Technology Infrastructure Library* (ITIL): *Service Operation*

      4.2.5 COBIT 2019 *Framework: Governance and Management Objectives*

PANDUAN PENILAIAN

1. Konteks penilaian

   1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.

1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan.

1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Sistem Manajemen Keamanan Informasi (SMKI)

3.1.2 Proses bisnis organisasi dan struktur organisasi

3.1.3 Manajemen risiko

3.1.4 Aspek finansial untuk pemulihan

3.1.5 *Disaster Recovery Plan* (DRP)

3.2 Keterampilan

3.2.1 Mampu bekerjasama dan berkomunikasi dengan tim di bawahnya maupun tim terkait yang memberikan dukungan dalam proses perhitungan dampak

3.2.2 Mampu mengumpulkan informasi dengan baik lewat proses interviu dan survei untuk menentukan biaya keseluruhan sistem terdampak

3.2.3 Mampu mengumpulkan temuan-temuan dari sebuah insiden keamanan siber dan mendokumentasikan dengan baik

4. Sikap kerja yang diperlukan
    4.1 Teliti
    4.2 Bertanggung jawab
    4.3 Integritas

5. Aspek kritis
    5.1 Ketepatan dalam menghitung biaya pemulihan untuk setiap sistem terdampak insiden keamanan siber
    5.2 Ketepatan mengidentifikasi dampak kerugian nonfinansial berdasarkan analisis jangka panjang

KODE UNIT : **J.62S0C00.019.1**

JUDUL UNIT : **Mengakhiri Proses Respon terhadap Insiden Keamanan Siber**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menutup proses respon terhadap insiden keamanan siber.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melakukan monitor terhadap pengetesan ulang aset TI untuk memastikan tidak ada kerentanan yang tersisa	1.1 Dampak insiden keamanan siber yang terjadi sebelumnya dimonitor ulang sesuai prosedur. 1.2 Uji fungsi dari aset TI dimonitor sesuai dengan fungsionalitas aset TI. 1.3 Uji kinerja dari aset TI dimonitor sesuai dengan **data historis**
2. Mengidentifikasi dokumen-dokumen terkait insiden keamanan siber	2.1. **Dokumentasi dan laporan** dikumpulkan berdasarkan tahapan penanganan insiden keamanan siber. 2.2. Bukti elektronik dari insiden keamanan siber dikelola sesuai **prosedur *digital evidence first response*** jika diperlukan investigasi lebih lanjut.
3. Melakukan pengakhiran proses penanganan insiden keamanan siber	3.1. Laporan linimasa insiden keamanan siber dan penanganannya disiapkan berdasarkan dokumentasi dan laporan. 3.2. Informasi mengenai pengakhiran proses penanganan insiden keamanan siber dikomunikasikan kepada **pihak terkait**.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Data historis adalah informasi mengenai aset TI terdampak sebelum terjadinya insiden keamanan siber.
   1.2 Dokumentasi dan laporan meliputi hasil analisis *log*, dokumen solusi penanganan insiden keamanan siber, dokumen sistem dan topologi jaringan, serta kebijakan dan prosedur.

1.3 Prosedur *digital evidence first response* meliputi identifikasi, koleksi, akuisisi, dan preservasi barang bukti elektronik.

1.4 Pihak terkait adalah penanggung jawab aset TI, pemilik aset TI, dan pemilik bisnis.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.2.1 Perangkat keras dan perangkat lunak komputer

2.2.2 Perangkat jaringan

2.2.3 Perangkat lunak pengolah kata

2.2.4 Perangkat lunak utilitas

2.2.5 Perangkat forensik digital

2.2 Perlengkapan

2.2.1 Media penyimpanan

2.2.2 *Printer*

2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

1.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah terakhir pada Undang-Undang Nomor 19 Tahun 2016

1.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik sebagaimana diubah terakhir pada Peraturan Pemerintah Nomor 71 Tahun 2019

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27037:2014 Teknologi Informasi - Teknik keamanan - Pedoman identifikasi, pengumpulan, akuisisi dan preservasi bukti digital

4.2.2 SNI ISO/IEC 27035 -1:2016 Teknologi informasi - Teknik Keamanan - Manajemen insiden keamanan informasi - Bagian 1: Prinsip manajemen insiden

4.2.3 SNI ISO/IEC 27035 - 2:2016 Teknologi informasi – Teknik Keamanan – Manajemen insiden keamanan informasi – Bagian 2: Pedoman perencanaan dan persiapan respon insiden

4.2.4 *Information Technology Infrastructure Library* (ITIL): *Service Operation*

4.2.5 COBIT 2019 *Framework: Governance and Management Objectives*

PANDUAN PENILAIAN

1. Konteks penilaian

   1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

   1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.

   1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan.

   1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
    3.1 Pengetahuan
        3.1.1 Manajemen insiden keamanan informasi
        3.1.2 Sistem Manajemen Keamanan Informasi (SMKI)
        3.1.3 Layanan aset TI yang terdampak insiden keamanan siber
        3.1.4 Prosedur *digital evidence first response*
    3.2 Keterampilan
        3.2.1 Mengkomunikasikan proses respon terhadap insiden keamanan siber secara lisan dan tulisan dengan baik
        3.2.2 Mengoperasikan perangkat keras dan perangkat lunak yang mendukung proses pengambilan keputusan pengakhiran proses
        3.2.3 Mengoperasikan perangkat forensik digital

4. Sikap kerja yang diperlukan
    4.1 Teliti
    4.2 Objektif
    4.3 Tanggung jawab

5. Aspek kritis
    5.1 Ketepatan dalam mengelola bukti elektronik dari insiden keamanan siber sesuai prosedur *digital evidence first response* jika diperlukan investigasi lebih lanjut
    5.2 Kemampuan mengkomunikasikan informasi mengenai pengakhiran proses penanganan insiden keamanan siber kepada pihak terkait

KODE UNIT : **J.62S0C00.020.1**

JUDUL UNIT : **Membuat Rekomendasi Perbaikan setelah Insiden Keamanan Siber**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menyusun dokumen rekomendasi dalam perbaikan sistem dengan pembelajaran dari insiden keamanan siber yang terjadi yang diotorisasi oleh pihak yang mempunyai kewenangan pengelolaan keamanan siber.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengukur efektivitas dari strategi yang disiapkan dalam menghadapi insiden keamanan siber	1.1. Laporan diidentifikasi berdasarkan tahapan penanganan insiden keamanan siber. 1.2. Laporan penanganan insiden keamanan siber dianalisis/dinilai berdasarkan **indikator kinerja**. 1.3. Strategi penerapan perbaikan sistem setelah insiden keamanan siber dianalisis berdasarkan tingkat keberhasilan.
2. Mengidentifikasi kebutuhan perbaikan strategi penanganan insiden keamanan siber	2.1. Referensi ***best practice*** dalam strategi penerapan perbaikan diidentifikasi sesuai profil insiden keamanan siber. 2.2. Identifikasi kebutuhan perbaikan strategi penanganan insiden keamanan siber dianalisis berdasarkan *best practice*. 2.3. Langkah-langkah perbaikan strategi penanganan insiden keamanan siber disusun berdasarkan *best practice.*
3. Membuat rekomendasi perbaikan setelah insiden keamanan siber	3.1 **Daftar pembelajaran** dibuat berdasarkan penanganan insiden keamanan siber sebelumnya. 3.2 **Informasi insiden keamanan siber** disebarkan secara aman kepada pihak terkait yang tepercaya sesuai prosedur. 3.3 Rekomendasi hasil analisis yang paling sesuai untuk perbaikan sistem setelah insiden keamanan siber disusun berdasarkan hasil identifikasi kebutuhan perbaikan strategi penanganan insiden keamanan siber.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Indikator kinerja diukur antara lain berdasarkan parameter waktu deteksi dan waktu penyelesaian, efektivitas solusi, pembatasan dampak insiden keamanan siber, dan efektivitas komunikasi serta koordinasi tim.
   1.2 *Best practice* dalam konteks *Security Operations Center* merupakan metode atau teknik dalam penanganan insiden keamanan siber yang secara umum dianggap paling efektif dan efisien.
   1.3 Daftar pembelajaran antara lain merupakan pengkajian ulang, identifikasi, dan perbaikan terhadap *information security control, risk assessment* dan evaluasi manajemen.
   1.4 Informasi insiden keamanan siber yang dimaksud antara lain pola serangan, langkah penanganan, dan pemulihan insiden keamanan siber yang disebarkan dengan format tertentu dengan tidak membongkar informasi kritis sistem organisasi.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat keras dan perangkat lunak komputer
      2.1.2 Perangkat jaringan
      2.1.3 Perangkat lunak pengolah kata
      2.1.4 Perangkat lunak utilitas
   2.2 Perlengkapan
      2.2.1 Media penyimpanan
      2.2.2 *Printer*
      2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah terakhir pada Undang-Undang Nomor 19 Tahun 2016

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik sebagaimana diubah terakhir pada Peraturan Pemerintah Nomor 71 Tahun 2019

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27035 -1:2016 Teknologi informasi - Teknik Keamanan - Manajemen insiden keamanan informasi - Bagian 1: Prinsip manajemen insiden

4.2.2 SNI ISO/IEC 27035 - 2:2016 Teknologi informasi – Teknik Keamanan – Manajemen insiden keamanan informasi – Bagian 2: Pedoman perencanaan dan persiapan respon insiden

4.2.3 *Information Technology Infrastructure Library* (ITIL): *Service Operation*

4.2.4 COBIT 2019 *Framework: Governance and Management Objectives*

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.

1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan.

1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat

kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Manajemen insiden keamanan informasi
      3.1.2 Sistem Manajemen Keamanan Informasi (SMKI)
      3.1.3 Protokol *information sharing* antara lain *traffic light protocol*
   3.2 Keterampilan
      3.2.1 Mengoperasikan perangkat keras dan perangkat lunak yang berhubungan dengan penyusunan rekomendasi dan pembelajaran
      3.2.2 Menganalisis perbaikan strategi melalui pendekatan strategis dan teknis
      3.2.3 Mengkomunikasikan hasil rekomendasi dan pembelajaran secara lisan dan tulisan dengan baik

4. Sikap kerja yang diperlukan
   4.1 Teliti
   4.2 Objektif
   4.3 Tanggung jawab

5. Aspek kritis
   5.1 Ketepatan menganalisis strategi penerapan perbaikan sistem setelah insiden keamanan siber berdasarkan tingkat keberhasilan
   5.2 Kemampuan dalam membuat daftar pembelajaran berdasarkan penanganan insiden keamanan siber sebelumnya

BAB III

PENUTUP

Dengan ditetapkannya Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berkaitan Dengan Itu (YBDI) Bidang *Security Operations Center,* maka SKKNI ini menjadi acuan dalam penyusunan jenjang kualifikasi nasional, penyelenggaraan pendidikan dan pelatihan serta sertifikasi kompetensi.

MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA,

IDA FAUZIYAH