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;

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.62SOC00.008.1**

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.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.62SOC00.018.1**

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