MATERI L1 SOC ANALYST

UNIT KOMPETENSI 5

Melakukan Analisis Keamanan Siber terhadap Insiden Keamanan Siber untuk Menentukan Kendali

MEDIA PEMBELAJARAN L1 SOC ANALYST

Unit Kompetensi

Melakukan Analisis Keamanan Siber terhadap Insiden Keamanan Siber untuk Menentukan Kendali

Hasil Pembelajaran

Setelah mengikuti pembelajaran peserta didik diharapkan mampu melakukan analisis terhadap keamanan siber untuk menentukan kendali

Indikator Hasil Belajar

- Mengumpulkan informasi terkait efek dari insiden kemanan siber
- Mengidentifikasi dampak insiden siber
- Menentukan kendali terhadap insiden keamanan siber

Elemen Kompetensi

1. Mengumpulkan info terkait efek dari insiden keamanan siber
    a. Informasi terkait efek dari insiden keamanan siber ke dalam organisasi dikumpulkan sesuai prosedur.
    b. Informasi terkait efek dari insiden keamanan siber ke luar organisasi dikumpulkan sesuai prosedur.
    c. Pembaruan informasi insiden keamanan siber susulan dilakukan sesuai prosedur.
2. Mengidentifikasi dampak insiden kemanan siber
    a. Seluruh pemangku kepentingan yang kemungkinan terdampak insiden keamanan siber diidentifikasi berdasarkan ruang lingkupnya.
    b. Risiko kerugian akibat insiden keamanan siber didefinisikan berdasarkan analisis risiko.
    c. Langkah mitigasi dan prioritas ditentukan berdasarkan risk appetite.
3. Menentukan kendali terhadap insiden keamanan siber
    a. Rencana penanganan insiden keamanan siber dibuat berdasarkan prosedur.
    b. Ketersediaan akan sumber daya internal dalam penanganan insiden keamanan siber dipastikan sesuai kebutuhan.
    c. Eskalasi pengambilan keputusan berdasarkan kewenangan dilakukan sesuai prosedur.
    d. Laporan kegiatan investigasi awal untuk menentukan kendali terhadap insiden keamanan siber didokumentasikan sesuai prosedur.

A. IDENTIFIKASI DAMPAK INSIDEN SIBER

Definisi & Terminologi dalam Insiden Siber

- Aset
  Segala sesuatu yang berharga bagi organisasi dan perlu dilindungi, seperti informasi, perangkat keras, perangkat lunak, atau infrastruktur.
- Ancaman / *Threat*
  Potensi tindakan yang dapat membahayakan sistem atau data, seperti malware, phishing, DDoS, ransomware, dll
- Kerentanan / *Vulnerability*
  Kelemahan dalam sistem atau perangkat lunak yang dapat dieksploitasi oleh ancaman, seperti konfigurasi yang tidak aman, bug pada perangkat lunak, celah keamanan, dll
- Serangan / *Attack*
  Upaya untuk mengeksploitasi kerentanan dan menyebabkan kerusakan, seperti peretasan, pencurian data, penipuan *online*.
- *Incident*
  Kejadian yang tidak terduga dan tidak diinginkan yang dapat membahayakan keamanan sistem atau jaringan, seperti serangan siber, pelanggaran data, dan kegagalan sistem
- *Event*
  Segala hal yang terjadi di lingkungan organisasi.
- *Security Incident*
  Peristiwa yang dikonfirmasi telah melanggar kebijakan keamanan dan menimbulkan dampak negatif berkaitan dengan kerahasiaan, integritas, atau ketersediaan sistem informasi, jaringan, program, atau data, serta berimplikasi pada pelanggaran data atau pelanggaran privasi.
- *Security Event*
  Setiap kejadian dalam sistem atau jaringan yang membutuhkan perhatian atau penyelidikan karena berpotensi menimbulkan risiko keamanan.
- Risiko
  Potensi terjadinya peristiwa yang dapat membahayakan aset informasi organisasi, seperti data, perangkat keras, perangkat lunak, infrastruktur jaringan, dan reputasi organisasi.
- *Security Control*
  Tindakan, proses, dan teknologi yang diterapkan untuk mengurangi risiko dan melindungi aset informasi dari berbagai ancaman.
- Mitigasi
  Upaya untuk mengurangi risiko dan/atau dampak insiden keamanan siber.
- Manajemen Risiko

Proses yang sistematis untuk mengidentifikasi, menganalisis, mengevaluasi, dan mengendalikan risiko yang berkaitan dengan aset informasi dan sistem teknologi informasi.

- Respons Insiden / *Incident Response*
  Proses menanggapi dan menangani insiden keamanan siber untuk meminimalkan dampak insiden, melindungi aset organisasi, dan memulihkan operasi secepat mungkin.
- Penanganan Insiden / *Incident Handling*
  Proses menyeluruh untuk mengidentifikasi, mengendalikan, menyelidiki, melaporkan, menangani, merespons serta mempelajari insiden keamanan siber untuk meminimalkan dampak insiden, memulihkan layanan, dan mencegah insiden serupa di masa mendatang.

Event vs Incident

Kategori	***Event***	***Incident***
Definisi	Kejadian yang terdeteksi dalam sistem yang belum tentu berdampak negatif.	Insiden keamanan yang telah dikonfirmasi berdampak negatif terhadap organisasi.
Contoh	Upaya login dengan password salah.	Akun pengguna berhasil diretas dan data dicuri.
	Antivirus mendeteksi file mencurigakan.	Situs web organisasi menjadi target serangan DDoS dan tidak dapat diakses.
	Sistem jaringan mendeteksi peningkatan lalu lintas tidak biasa.	Karyawan mengirim email berisi informasi sensitif ke pihak tidak berwenang.
	Sistem keamanan mendeteksi beberapa upaya login gagal.	Sistem organisasi dienkripsi oleh *ransomware*.
Dampak	Belum tentu menyebabkan gangguan atau kerugian.	Menyebabkan gangguan operasional, kebocoran data, atau ancaman lainnya.
Tindakan	Biasanya hanya perlu dipantau atau dianalisis lebih lanjut.	Membutuhkan respons segera dan tindakan mitigasi.

RESPON INSIDEN VS PENANGANAN INSIDEN

kategori	Penanganan Insiden	Respons Insiden
Definisi	Tindakan jangka panjang untuk memulihkan dan mencegah insiden serupa terjadi di masa depan.	Tindakan segera yang diambil untuk mengurangi dampak insiden keamanan yang sedang terjadi.
Tujuan	Memulihkan sistem dan memperkuat keamanan untuk mencegah insiden berulang.	Menghentikan atau mengurangi dampak insiden secepat mungkin.
Contoh	Memulihkan data yang hilang akibat ransomware.	Mengisolasi sistem yang terinfeksi malware.
	Mengidentifikasi dan menambal kerentanan yang dieksploitasi dalam serangan siber.	Mengubah password akun yang disusupi.
	Melatih karyawan tentang kesadaran dan respons insiden.	Memblokir alamat IP yang berbahaya.
Dampak	Bersifat strategis dan dilakukan setelah insiden dikendalikan.	Bersifat taktis dan dilakukan secara langsung saat insiden terjadi.

Sumber Serangan Siber

1. Sumber Internal dan Eksternal
    - Sumber internal dapat berasal dari dalam organisasi seperti karyawan atau vendor yang memiliki akses ke sistem, sebagai contoh yaitu terdapat karyawan yang menjual data pengguna.
    - Sumber eksternal berasal dari luar organisasi baik individu maupun kelompok seperti kelompok *hacker* yang menargetkan sistem.
2. Kekecewaan

Serangan yang dilakukan oleh penyerang atas dasar ketidakpuasan akan organisasi, sebagai contoh mantan karyawan yang masih memiliki akses terhadap sistem menghapus data organisasi.

3. Persaingan, Permusuhan & Konflik
   Serangan dilakukan oleh pesaing bisnis, negara maupun kelompok tertentu yang memiliki kepentingan tertentu seperti perusahaan A mempekerjakan *hacke*r untuk menyerang perusahaan B agar kepercayaan masyarakat kepada perusahaan B hancur.
4. *Hacktivitists*
   Serangan yang dilakukan hacktivist dilakukan untuk menyuarakan pesan politik atau sosial seperti kelompok anonymus melakukan defacement terhadap website pemerintah dengan isi kritik terhadap pemerintah.
5. Grup Kejahatan Terorganisir
   Serangan yang dilakukan oleh kelompok maupun perseorangan dengan tujuan mendapatkan keuntungan finansial dari serangan seperti *hacker* membuat *ransomware* dan meminta tebusan kepada korban.
6. Organisasi Ekstrimis
   Kelompok dengan pemikiran tertentu melakukan serangan untuk menyebarkan propaganda atau teror
7. Kegiatan Intelijen
   Serangan yang dilakukan pihak negara asing dalam mendapatkan informasi strategis seperti pencurian data terhadap aset pertahanan nasional.
8. Teknologi
   Serangan yang bersalah dari penggunaan teknologi yang tidak sesuai atau memliki celah keamanan seperti penggunaan *access point* tanpa *password*

Dampak Serangan Siber

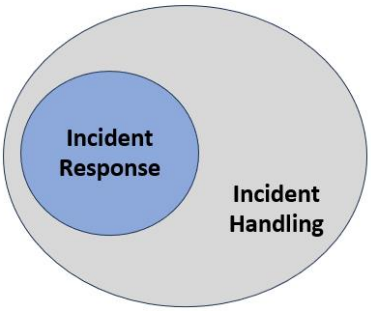
1. Dampak Finansial
   Kerugian finansial seperti biaya tambahan untuk pemulihan data, biaya forensik, dan denda.
2. Dampak Reputasi
   Kerusakan reputasi dan kredibilitas perusahaan akibat insiden keamanan siber
3. Dampak Operasional
   Gangguan pada operasi bisnis dan layanan TI akibat kerusakan sistem dan *downtime*
4. Dampak Psikologis Individu
   Ketakutan, stres, pencurian identitas, penipuan keuangan, dan kerugian pribadi lainnya.
5. Dampak Legal/Hukum

Risiko tuntutan hukum dan denda akibat pelanggaran privasi dan regulasi

B. Respons Insiden

Kebutuhan *Incident Response* dan *Incident Handling*

Incident Handling adalah proses menyeluruh dalam mengelola insiden dari awal hingga akhir, termasuk pencegahan, deteksi, respons, pemulihan, dan evaluasi sedangkan *incident response* adalah bagian dari Incident Handling yang berfokus pada tindakan langsung saat insiden terjadi.




Incident Response

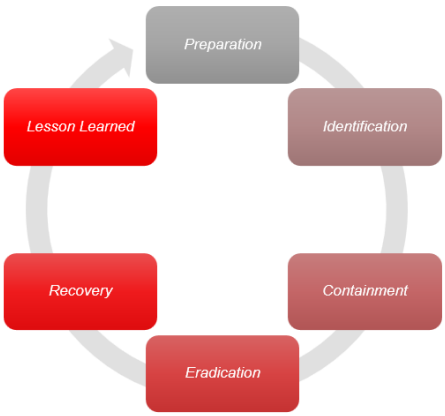

Incident Handling

Jika dianalogikan dalam insiden kebakaran maka *incident handling* dapat berupa menyediakan *hydrant*, alat pemadam api ringan dan pelatihan personel dalam menghadapi kebakaran sedangkan *incident response* dapat berupa pemadam kebakaran memadamkan api agar tidak menyebar.

Incident handling dan *incident response* dibutuhkan untuk

1. Meningkatkan kesiapan organisasi untuk merespons insiden dengan cepat dan terkoordinasi.
2. Meminimalkan kerusakan yang disebabkan oleh insiden.
3. Memungkinkan organisasi untuk pulih dari insiden dengan cepat dan efektif.
4. Membantu organisasi mengidentifikasi kelemahan dan mencegah insiden serupa di masa depan.
5. Membantu organisasi mematuhi peraturan dan undang-undang yang relevan.
6. Membantu melindungi aset organisasi (data, sistem, dan reputasi)

Incident Respone Framework



SANS
Sysadmin, Audit, Network, and Security Institute

NIST
National Institute of Standards and Technology

1. *Preparation* (Persiapan)
   Mengembangkan rencana respons insiden, menguji rencana tersebut, dan memastikan tim IR memiliki pelatihan dan sumber daya yang diperlukan.
   - Mendefinisikan kebijakan dan prosedur IR.
   - Mengidentifikasi tim IR dan peran/tanggung jawab.
   - Mengembangkan rencana komunikasi insiden.
   - Menerapkan kontrol keamanan untuk mencegah insiden.
2. *Identification* (Identifikasi)
   Mendeteksi insiden keamanan siber dan menentukan ruang lingkup serta dampaknya
   - Mendeteksi aktivitas mencurigakan yang mungkin menunjukkan insiden
   - Menganalisis insiden untuk memahami sifat dan ruang lingkupnya.
   - Mendokumentasikan bukti digital
   - Mengumpulkan informasi terkait insiden
   - Melakukan identifikasi kategori/jenis insiden
   - Menentukan sifat dan potensial serangan (Dampak, Urgensi, SLA)
   - Melakukan koordinasi dengan *stakeholder* yang terkait

   Setelah insiden diidentifikasi maka insiden dapat diprioritaskan berdasarkan dampak dan urgensi sesuai gambar berikut:

Urgensi	Dampak		
	High	Medium	Low
High	High	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

Urgensi:

- *High* berarti Insiden mempengaruhi seluruh layanan yang mengakibatkan ketidak mampuan untuk menjalankan fungsi layanan
- *Medium* berarti Insiden cukup memengaruhi kemampuan pengguna untuk melakukan pekerjaan, namun terdapat solusi alternative
- *Low* berarti Insiden tidak menghalangi kemampuan untuk melakukan pekerjaan atau menyediakan fungsi layanan

Dampak:

- *High* berarti Insiden yang mempengaruhi seluruh pengguna dalam internal organisasi
- *Medium* berarti Insiden yang mempengaruhi sebagian besar pengguna dalam internal organisasi
- *Low* berarti Insiden yang mempengaruhi satu atau beberapa pengguna

Waktu penyelesaian insiden dapat dilihat dari tabel service level agreement:

Service Level Agreement		
Kategori	**Respon**	**Waktu Penyelesaian**
High	Segera	8 jam
Medium	24 jam	3 x 24 jam
Low	N/A	N/A

3. *Containment* (Penahanan)

Mengisolasi sistem yang terinfeksi untuk mencegah penyebaran insiden

- memblokir lalu lintas dari alamat tertentu atau pada port tertentu,
- mengubah entri DNS, mengubah konfigurasi IDS / IPS atau firewall,
- menonaktifkan akun tertentu

- menghapus perangkat individu atau seluruh sistem dari jaringan, atau mematikan sebagian jaringan
- Menonaktifkan layanan yang tidak digunakan untuk memperkuat sistem serangan lebih lanjut

4. *Eradication* (Penghapusan)
   Menghapus malware atau sumber serangan dari sistem yang terinfeksi
   - Membersihkan *malwar*e atau kerentanan yang dieksploitasi
   - Melakukan pengecekan dan membersihkan sistem dari celah-celah yang digunakan untuk masuk ke sistem, misal *backdoor*
   - Melakukan *scanning* terhadap celah keamanan yang mungkin masih ada sebelum sistem di-*deploy* kembali
   - Melakukan patching pada sistem
5. *Recovery* (Pemulihan)
   Mengembalikan sistem dan data yang terdampak ke keadaan normal
   - Melakukan *restore* sistem
   - Memastikan sistem berjalan kembali secara normal
   - Melakukan pengujian, pemantauan, dan validasi system serta melakukan verifikasi sistem agar tidak terinfeksi kembali atau disusupi dengan cara lain
6. *Lesson Learned* (Pembelajaran & Peningkatan)
   Menganalisis insiden untuk mengidentifikasi kelemahan dan menerapkan langkah-langkah perbaikan untuk mencegah insiden serupa di masa mendatang
   - Melakukan analisis lebih lanjut dan evaluasi insiden untuk mengidentifikasi penyebab dan kelemahan.
   - Melakukan identifikasi pelajaran yang didapat dari insiden
   - Meninjau efektifitas proses, prosedur dan menjelaskan perubahan yang diperlukan
   - Memperbarui kebijakan dan prosedur IR berdasarkan pelajaran yang didapat.
   - Mengkomunikasikan dan membagikan hasil tinjauan dalam komunitas tepercaya.

Laporan *Incident Response*

Dalam melakukan *incident response*, pelaksana kegiatan wajib melakukan dokumentasi dan pembuatan laporan agar dapat digunakan sebagai kepatuhan terhadap regulasi seperti ISO 27001 dan NIST. Dengan laporan yang baik, tim dapat menganalisis pola serangan, mengidentifikasi celah keamanan, serta melakukan perbaikan agar insiden serupa tidak terulang. Laporan *incident response* terdiri dari beberapa bab sebagai berikut:

I. Informasi Pelaporan Insiden Keamanan Siber
- ✓ Waktu pelaporan insiden
- ✓ Sumber pelaporan (pengguna, sistem monitoring, dll)
- ✓ Identitas pelapor
- ✓ Hal pelaporan (singkat dan deskriptif)
- ✓ Aset terdampak (server, workstation, dll)
- ✓ Bukti insiden

II. Deskripsi Insiden

Detail kronologi kejadian, identifikasi aset yang terdampak, dan dampak insiden terhadap proses bisnis (gangguan layanan, kehilangan data, dll)

III. Analisis dan Investigasi

Menjelaskan hasil analisis dan investigasi insiden, seperti sumber dan penyebab insiden, perkiraan waktu terjadinya insiden, bukti dan temuan yang relevan, serta analisis risiko untuk menilai potensi dampak insiden.

IV. Mitigasi

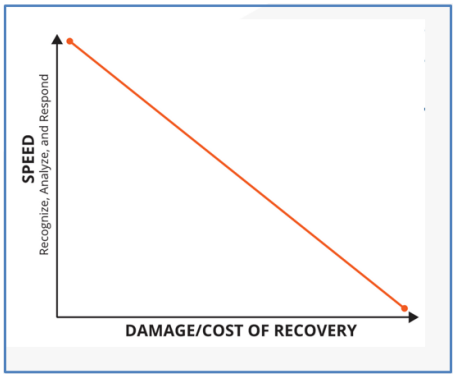
Menjelaskan tindakan penanganan (langkah *containment* dan pemulihan) yang telah dilakukan untuk mengurangi dampak insiden dan memulihkan aset terdampak

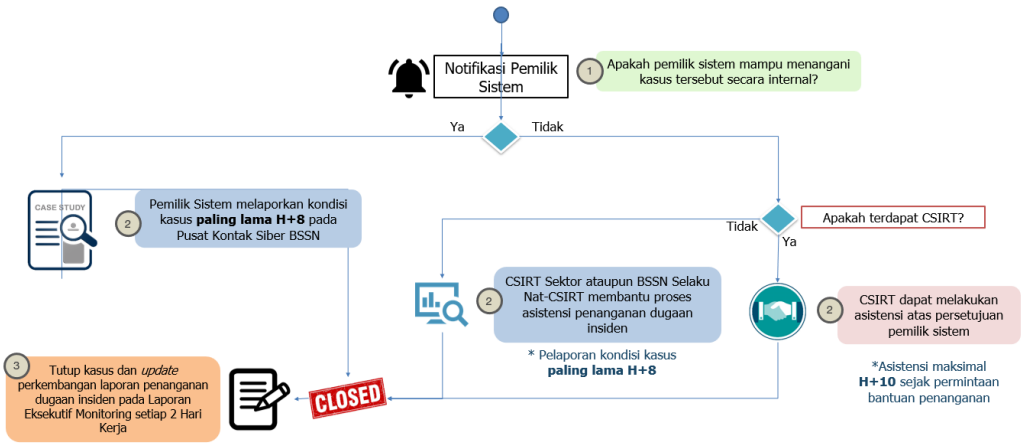
V. Kesimpulan dan Rekomendasi
- ✓ Kesimpulan
- ✓ Rekomendasi

Lampiran
- ✓ Dokumentasi teknis (mis. log, screenshot, laporan forensik)
- ✓ Daftar kontak tim yang terlibat dalam penanganan insiden

Alur Asistensi Penanganan Siber di Indonesia

Kecepatan suatu organisasi dapat mengenali, menganalisis, dan menanggapi suatu insiden membatasi kerusakan yang terjadi dan menurunkan biaya pemulihan.





CISRT (*Computer Security Incident Response Team*)

Tim yang bertugas menangani insiden keamanan siber pada suatu organisasi atau institusi. Memiliki istilah lain diantaranya CERT atau CERT/CC (*Computer Emergency Response Team/Coordination Center*), IRT (*Incident Response Team*), CIRT (*Computer Incident Response Team*), SERT (*Security Emergency ResponseTeam*).

CISRT memiliki fungsi utama sebagai berikut:

1. Menerima dan menangani laporan insiden keamanan siber.
2. Melakukan investigasi dan analisis terhadap insiden.
3. Melakukan koordinasi dengan pihak terkait untuk mengatasi insiden.
4. Memberikan rekomendasi dan solusi untuk mencegah insiden serupa di masa depan.
5. Meningkatkan kesadaran dan edukasi tentang keamanan siber.

Manfaat Memiliki CSIRT

1. Meminimalkan dampak insiden keamanan siber
2. Meningkatkan kesiapsiagaan dan kemampuan organisasi dalam menangani insiden keamanan siber
3. Meningkatkan kepercayaan dan reputasi organisasi
4. Memenuhi peraturan dan undang-undang terkait keamanan siber

CISRT VS SOC

Aspek	CSIRT	SOC
Sifat	Reaktif – Merespons insiden setelah terjadi	Proaktif – Mencegah insiden terjadi
Fokus Utama	Menangani dan merespons insiden keamanan yang telah terjadi	Melakukan pemantauan dan pencegahan ancaman keamanan
Monitoring	Tidak termasuk dalam tugas utama	Bertanggung jawab atas monitoring sistem keamanan
Pemimpin Tim	*Team Leader* – Mengarahkan dan bertanggung jawab atas prosedur respons	CISO (*Chief Information Security Officer*) – Menentukan strategi keamanan dan kepatuhan organisasi
Koordinator	*Incident Leader* – Mengoordinasikan respons terhadap insiden spesifik	Manager – Mengawasi semua aktivitas SOC dan membuat kebijakan baru
Anggota Tim	IT: Ahli infrastruktur IT	*Security Engineer*: Mengelola alat monitoring dan membangun arsitektur keamanan

	Management: Berkomunikasi dengan manajemen terkait insiden	*Security Analyst*: Menganalisis dan merespons ancaman
	PR: Mengelola komunikasi dengan publik dan pelanggan	
	Legal: Memberikan saran hukum terkait insiden	

C. Manajemen Risiko Keamanan Siber

Manajemen Risiko

Proses berkelanjutan untuk mengidentifikasi, menilai, dan mengendalikan risiko keamanan informasi yang dihadapi oleh suatu organisasi.

Tujuan manajemen resiko sebagai berikut:

1. Meminimalkan dampak negatif dari risiko
2. Memaksimalkan peluang yang dapat dihasilkan dari risiko
3. Meningkatkan efisiensi dan efektivitas organisasi

Manajemen resiko memiliki manfaat diantaranya:

1. Membantu organisasi dalam mencapai tujuannya
2. Meningkatkan kesiapsiagaan organisasi dalam menghadapi situasi yang tidak terduga
3. Meningkatkan kepercayaan dan reputasi organisasi
4. Memenuhi peraturan dan undang-undang terkait manajemen risiko

Risk Assement

Risk assessment (penilaian resiko) adalah proses mengidentifikasi, mengukur, dan mengevaluasi risiko potensial dalam organisasi. Tujuan utama dari penilaian risiko adalah untuk memahami sumber risiko, probabilitas terjadinya risiko, serta dampak yang mungkin timbul dari risiko tersebut.

Risk assement terbagi menjadi tahapan sebagai berikut:

1. *Identifikasi Vulnerability*
    - Kerentanan dapat menimbulkan bahaya jika dibarengi dengan adanya ancaman
    - Penerapan pengendalian yang tidak dilakuan secara tepat dapat menjadi kerentanan
2. Identifikasi *Threa*t
    - Informasi tentang ancaman diperoleh dari meninjau insiden dan dari sumber terbuka lainnya
    - Sumber ancaman baik sengaja atau tidak sengaja harus diidentifikasi
    - Sumber ancaman internal atau eksternal
3. *Risk Analysis*

- Analisis terhadap potensi level risiko meliputi analisis kemungkinan dan dampak
- Mempertimbangkan kontrol yang sudah ada.

4. *Risk Evaluation*
    - Proses evaluasi hasil analisis risiko
    - Menjaga basis dalam penentuan risk treatment terhadap risiko

Pendekatan Risk Assesment

Aprroach :

$$Risk = Likelihood \times Impact$$

Risk (Risiko)
Risiko adalah potensi kerugian atau dampak negatif yang bisa terjadi dalam suatu sistem atau organisasi. Risiko dapat berupa kebocoran data, serangan siber, atau kegagalan sistem.
Likelihood (Kemungkinan)
Seberapa besar kemungkinan suatu risiko terjadi. Faktor-faktor yang mempengaruhi diantaranya seberapa sering ancaman muncul, seberapa rentan sistem terhadap ancaman, apakah ada kontrol keamanan.
Impact (Dampak)
Jika risiko terjadi, seberapa besar dampaknya terhadap organisasi atau sistem. Dapat berupa kerugian finansial, hilangnya reputasi, kehilangan data atau gangguan layanan

Matriks Risiko

Overall Risk Severity				
Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Note	Low	Medium
		Low	Medium	High
	Likelihood			

matriks risiko yang mengklasifikasikan tingkat risiko berdasarkan kemungkinan (*likelihood*) dan dampak (*impact*):

1. *Low* (Rendah) – Hijau: Risiko dapat diabaikan atau tidak memerlukan tindakan segera.
2. *Medium* (Sedang) – Kuning: Risiko perlu diperhatikan, tetapi tidak mendesak.
3. *High* (Tinggi) – Merah: Risiko serius yang membutuhkan tindakan segera.
4. *Critical* (Kritis) – Ungu: Risiko sangat berbahaya dan harus segera ditangani.

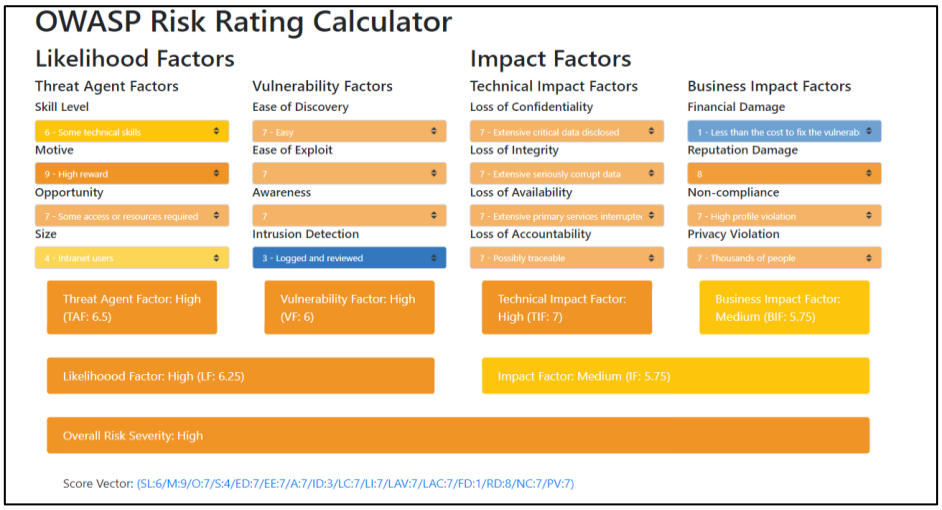
Risk Register

Dokumen yang digunakan untuk mendokumentasikan, melacak, dan mengelola risiko yang dihadapi oleh suatu organisasi.

NO.	Daftar Aset	Deskripsi Resiko			CURRENT ACTIONS/CONTROLS TO MANAGE THE RISK				*RISK TREATMENT*	RISK MITIGATION	Penanggung Jawab
		LOSS EVENTS		DAMPAK RESIKO							
	Nama Aset	Kerentanan (*Vulnerability*)	Ancaman (*Threat*)	Uraian Dampak	Pengendalian yang ada	Likelihood	Impact	Nilai Risiko	Mitigasi / Terima / Transfer / Hindari	Rekomendasi & Pengendalian Baru	PIC
ASET											
1	Web Server Aplikasi Kepegawaian	CVE-2021-41617	Penggunaan konfigurasi non-default tertentu pada sshd OpenSSH 6.2 s.d. sebelum 8.8, memungkinkan peningkatan hak istimewa (privilege escalation) karena grup tambahan tidak diinisialisasi seperti yang diharapkan. Privilege escalaton dapat dilakukan melalui AuthorizedKeysCommand dan AuthorizedPrincipalsCommand, sehingga Penyerang dapat mengeksploitasi kerentanan ini untuk mendapatkan hak akses root pada sistem yang terdampak.	- Penyerang dapat melakukan eskalasi hak istimewa ke member dari grup yang berhubungan dengan proses sshd - Penyerang dapat mengambil alih kontrol pada sistem yang terdampak - Penyerang dapat mengeksekusi perintah pada perangkat korban dan membaca data sensitif	None	High	Medium	High	Mitigasi	- Melakukan upgrade OpenSSH ke versi terbaru - Memonitor log SSH pada server untuk mengetahui aktivitas mencurigakan - Melakukan Blocking IP penyerang - Melakukan penggantian port ssh - Mengimplementasikan IDS - Memberikan security awareness pada karyawan dan sistem admin - Me-nonaktifkan AuthorizedKeysCommand dan AuthorizedPrincipalsCommand jika tidak diperlukan - Membatasi akses sudo hanya kepada pengguna dan grup yang diperlukan	Tim Pusdatin

1. *Likelihood*
   Probabilitas atau kemungkinan terjadinya suatu risiko (High, Medium, Low)
2. *Risk rating*
   proses untuk menentukan tingkat keparahan suatu risiko (*High, Medium, Low*)
   Tingkat Risiko = *Likelihood X Impact*
3. *Control*
   Tindakan atau langkah-langkah yang diambil untuk mengurangi risiko.
4. *Risk treatment*
   Proses untuk memilih dan menerapkan kontrol untuk mengurangi risiko sesuai dengan situasi dan toleransi risiko organisasi
   - *Avoidance*
   - *Mitigation*
   - *Transfer*
   - *Acceptance*
5. *Risk residual*
   Risiko yang tersisa setelah organisasi menerapkan kontrol atau tindakan mitigasi untuk mengurangi risiko.

Menghitung Resiko dengan OWASP Risk Calculator



Likelihood Factor

Menilai seberapa besar kemungkinan suatu kerentanan akan dieksploitasi oleh penyerang.

1. *Threat Agent* (Faktor Penyerang)
    - *Skill* (Tingkat Keahlian)
      Seberapa ahli penyerang dalam mengeksploitasi sistem. Semakin tinggi keahlian, semakin besar kemungkinan serangan berhasil.
    - *Motive* (Motivasi)
      Seberapa besar keinginan atau insentif bagi penyerang untuk mengeksploitasi kerentanan (misalnya, keuntungan finansial atau politik).
    - *Opportunity* (Kesempatan)
      Seberapa mudah bagi penyerang untuk menemukan dan mengeksploitasi kerentanan tanpa terdeteksi.
    - *Size* (Ukuran Kelompok Penyerang)
      Seberapa banyak penyerang yang memiliki akses dan kemampuan untuk mengeksploitasi kerentanan tersebut.
2. *Vulnerability* (Faktor Kerentanan)
    - *Ease of Discovery* (Kemudahan Ditemukan)
      Seberapa mudah kerentanan dapat diidentifikasi, misalnya melalui scanning otomatis atau eksploitasi manual.
    - *Ease of Exploit* (Kemudahan Eksploitasi)
      Seberapa sederhana atau kompleks teknik yang diperlukan untuk mengeksploitasi kerentanan.
    - *Awareness* (Kesadaran Pengembang/Sistem)
      Apakah organisasi menyadari adanya kerentanan dan sudah mengambil langkah mitigasi atau belum.
    - *Intrusion Detection* (Kemampuan Deteksi Intrusi)
      Seberapa baik sistem keamanan dapat mendeteksi atau mencegah eksploitasi sebelum terjadi dampak besar.

Impact Factor

Menilai tingkat keparahan potensi jika kerentanan berhasil dieksploitasi.

1. *Technical Impact* (Dampak Teknis)
    - *Loss of Confidentiality* (Kehilangan Kerahasiaan)
      Seberapa besar risiko kebocoran data sensitif jika kerentanan dieksploitasi.
    - *Loss of Integrity* (Kehilangan Integritas)
      Seberapa besar kemungkinan data atau sistem diubah tanpa izin, merusak validitasnya.
    - *Loss of Availability* (Kehilangan Ketersediaan)
      Apakah eksploitasi dapat menyebabkan layanan atau sistem tidak tersedia (misalnya melalui serangan DDoS).
    - *Loss of Accountability* (Kehilangan Akuntabilitas)

Apakah eksploitasi memungkinkan seseorang untuk menyembunyikan identitas atau bertindak tanpa dapat dilacak.

Business Impact (Dampak Bisnis)

- *Financial Damage* (Kerugian Finansial)
  Seberapa besar kerugian ekonomi yang dapat ditimbulkan (misalnya pencurian data pelanggan atau penipuan transaksi).
- *Reputation Damage* (Kerusakan Reputasi)
  Apakah eksploitasi dapat menyebabkan hilangnya kepercayaan pelanggan atau merusak citra perusahaan.
- *Non-Compliance* (Ketidakpatuhan Regulasi)
  Apakah eksploitasi dapat membuat organisasi melanggar regulasi seperti GDPR, HIPAA, atau standar keamanan lainnya.
- *Privacy Violation* (Pelanggaran Privasi)
  Apakah data pribadi pengguna dapat terekspos atau dicuri akibat eksploitasi kerentanan ini.