TUGAS KEAMANAN JARINGAN

“Cyber Security Framework”

Nama : Akhmad Mufti Ali Wafa

Kelas : D4 LJ IT B

NRP 3122640048

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

TAHUN AJARAN 2022/2023

A. CSF 2.0 akan secara eksplisit mengenali penggunaan luas CSF untuk memperjelas potensinya aplikasi

1. Ubah judul dan teks CSF untuk mencerminkan tujuan penggunaannya oleh semua organisasi

   Cybersecurity Framework (CSF) awalnya dikembangkan untuk mengatasi risiko keamanan siber dalam infrastruktur penting, tetapi sejak saat itu telah digunakan secara lebih luas. Akibatnya, CSF 2.0 akan menggunakan nama yang lebih luas dan umum digunakan, "Cybersecurity Framework", bukan "Framework for Improving Critical Infrastructure Cybersecurity" yang asli.

   CSF 2.0 akan mencakup semua organisasi di pemerintahan, industri, dan akademisi, termasuk di luar infrastruktur kritis. Referensi ke infrastruktur penting masih dapat disertakan sebagai contoh, tetapi teks kerangka kerja akan ditinjau untuk penerapan yang luas. Kategori dan subkategori CSF Core yang dikhususkan untuk infrastruktur kritis akan diperluas, seperti ID.BE-2 dan ID.RM-3.

2. Lingkup CSF untuk memastikannya bermanfaat bagi organisasi terlepas dari sektor, jenis, atau ukuran

   Kongres telah mengarahkan NIST untuk mempertimbangkan bisnis kecil dan institusi pendidikan tinggi dalam Cybersecurity Framework (CSF). CSF adalah sumber daya yang diakui untuk organisasi negara bagian dan lokal di bawah Program Hibah Keamanan Siber Negara Bagian dan Lokal DHS. NIST akan meningkatkan upaya untuk memastikan kerangka kerja ini bermanfaat bagi semua ukuran organisasi dan mendorong partisipasi dari semua pihak yang berkepentingan.
3. Meningkatkan kerjasama dan keterlibatan internasional
   Banyak organisasi menyerukan peningkatan kolaborasi dan keterlibatan internasional dalam pengembangan CSF 2.0. NIST akan memprioritaskan pertukaran dengan pemerintah dan industri asing untuk memfasilitasi kolaborasi ini, serta bekerja untuk mengembangkan terjemahan CSF 2.0. NIST akan terus berpartisipasi dalam kegiatan standar internasional dan berbagi informasi tentang keterlibatan internasionalnya melalui situs International Cybersecurity and Privacy Resources. Beberapa negara telah mengadopsi atau mengadaptasi CSF 1.1, dan beberapa menganggap penggunaan Kerangka ini wajib untuk sektor publik dan swasta mereka.

B . CSF 2.0 akan tetap menjadi kerangka kerja, menyediakan konteks dan koneksi dengan yang sudah ada

1. Pertahankan tingkat detail CSF saat ini
   Tanggapan RFI menyoroti atribut CSF yang bermanfaat, termasuk fleksibilitas, kesederhanaan, dan kemudahan penggunaannya, yang memungkinkan organisasi dengan berbagai ukuran, jenis, dan sektor untuk menerapkannya secara efektif. Untuk menjaga fleksibilitas ini, NIST bertujuan untuk mempertahankan tingkat detail dan spesifisitas saat ini di CSF 2.0. Fungsi CSF akan terus memberikan struktur pengorganisasian umum untuk berbagai pendekatan keamanan siber, dan Kerangka Kerja akan memanfaatkan dan terhubung ke standar dan pedoman yang diakui secara global tanpa menggantinya.
2. Tautkan CSF dengan jelas ke kerangka kerja NIST lainnya

Kerangka kerja terkait keamanan siber dan privasi NIST lainnya, termasuk Kerangka Kerja Manajemen Risiko, Kerangka Privasi, Prakarsa Nasional untuk Kerangka Kerja Pendidikan Keamanan Siber untuk Keamanan Siber, dan Kerangka Pengembangan Perangkat Lunak Aman, akan tetap menjadi kerangka kerja terpisah. Namun, mereka akan dirujuk sebagai pedoman dalam CSF 2.0 atau dalam materi pendamping seperti pemetaan, karena setiap kerangka memiliki hubungan dengan CSF. Misalnya, CSF 2.0 dapat membahas bagaimana Kerangka Privasi dapat dimanfaatkan saat menerapkan CSF, membangun hubungan antara kedua kerangka tersebut.

3. Memanfaatkan Cybersecurity and Privacy Reference Tool untuk CSF 2.0 Core online
   CSF 2.0 akan disajikan dalam format PDF dan Excel, serta melalui NIST Cybersecurity and Privacy Reference Tool (CPRT) yang baru saja diluncurkan. CPRT menyediakan format yang dapat dibaca mesin dan antarmuka pengguna untuk mengakses data referensi dari keamanan dunia maya dan standar privasi, pedoman, dan kerangka kerja NIST, dan menawarkan pendekatan yang fleksibel untuk mengkarakterisasi hubungan antara standar, pedoman, kerangka kerja, dan berbagai aplikasi dan teknologi ini
4. Gunakan Referensi Informatif online yang dapat diperbarui
   CSF 1.1 menggunakan Referensi Informatif sebagai cara untuk memberikan panduan implementasi tambahan, tetapi beberapa referensi menjadi usang karena dokumen sumber diperbarui. Kolom Referensi Informatif di CSF 1.1 juga hanya mewakili sebagian kecil dari contoh standar yang dapat digunakan dengan CSF. Dalam CSF 2.0, NIST akan beralih ke penggunaan referensi online yang dapat diperbarui yang dipamerkan melalui CPRT. Beberapa sumber telah dipetakan ke CSF di luar yang termasuk dalam CSF 1.1 Core, dan pemetaan lebih lanjut dapat ditemukan di Profil sampel CSF dan publikasi NIST.
5. Gunakan Referensi Informatif untuk memberikan panduan lebih lanjut untuk menerapkan CSF
   NIST akan bekerja dengan komunitas untuk menghasilkan pemetaan guna mendukung CSF 2.0. Responden RFI meminta pemetaan ke hampir 50 standar keamanan dunia maya, pedoman, dan kerangka kerja lainnya, dan NIST bertujuan untuk memanfaatkan referensi online yang dapat diperbarui untuk memberikan panduan tambahan. Ini akan memungkinkan pemetaan pada tingkat Fungsi dan Kategori selain tingkat Subkategori, dan dapat memberikan gambaran yang lebih baik tentang hubungan antara sumber daya. Penambahan contoh penerapan juga harus memudahkan pengguna untuk menemukan lebih banyak panduan tentang cara mencapai hasil CSF.
6. Tetap netral teknologi dan vendor, tetapi mencerminkan perubahan dalam keamanan siber praktik
   CSF 2.0 akan tetap netral teknologi dan vendor, memungkinkannya untuk dimanfaatkan oleh organisasi terlepas dari teknologi atau layanan yang mereka gunakan. NIST sedang meninjau CSF untuk memastikan hasil yang luas dapat terus berlaku, sementara panduan tambahan untuk menyesuaikan teknologi atau aplikasi tertentu mungkin paling baik dicapai melalui profil sampel, pemetaan standar atau panduan khusus, atau contoh implementasi. NIST berkolaborasi dengan komunitas untuk mengembangkan pemetaan khusus teknologi untuk menjelaskan hubungan antara kapabilitas keamanan yang dapat dicapai dengan mengonfigurasi atau mengaktifkan fitur keamanan dalam kumpulan teknologi dan hasil yang diinginkan yang dijelaskan dalam CSF. NIST percaya bahwa tidak ada perubahan pada Subkategori CSF yang diperlukan untuk mengakomodasi prinsip Zero Trust Architecture (ZTA), dan NIST mendorong peninjauan dan

komentar pada pemetaan ini di Volume E paling lambat 6 Februari 2023. Pemetaan hubungan CSF khusus teknologi lainnya sedang dikembangkan sebagai bagian proyek NCCoE lainnya, termasuk Trusted IoT Device Network-Layer Onboarding dan Lifecycle Management, 5G Cybersecurity, dan Migrasi ke Post-Quantum Cryptography.

C. CSF 2.0 (dan sumber daya yang menyertainya) akan mencakup panduan yang diperbarui dan diperluas Implementasi kerangka

1. Menambahkan contoh penerapan untuk Subkategori CSF
   CSF 2.0 akan memberikan contoh implementasi gagasan dari proses dan kegiatan yang ringkas dan berorientasi pada tindakan untuk membantu mencapai hasil dari Subkategori CSF, selain panduan yang diberikan dalam Referensi Informatif CSF. Penambahan contoh nosional disarankan dalam tanggapan RFI dan telah berhasil digunakan dalam kerangka kerja NIST lainnya. Inti CSF akan tetap tingkat tinggi dan ringkas, dengan sejumlah kecil contoh nosional. Contoh-contoh tersebut akan membantu mengklarifikasi arti dan maksud dari setiap Subkategori dan memberikan gagasan implementasi dalam Inti CSF bagi mereka yang tidak terbiasa dengan standar keamanan siber terperinci yang diidentifikasi dalam Referensi Informatif. Contoh-contoh tersebut juga dapat membahas sifat teknologi dan teknik keamanan siber yang berkembang dengan menyoroti kemungkinan perbedaan dalam implementasi untuk platform seperti TI, IoT, OT, dan komputasi awan. Contoh penerapan lebih lanjut dapat dicakup oleh sumber daya CSF terkait, seperti Profil CSF yang disediakan oleh NIST dan organisasi lain serta Panduan Praktik Keamanan Siber NIST (seri SP 1800). Umpan balik diterima mengenai apakah contoh penerapan ini harus disertakan sebagai kolom di Inti CSF, yang disorot dalam Alat Referensi Keamanan dan Privasi Siber, atau dalam panduan pendamping terpisah.
2. Mengembangkan template Profil CSF
   Banyak tanggapan RFI meminta panduan tambahan dan template untuk mengembangkan Profil CSF. Profil CSF adalah cara bagi organisasi untuk mengimplementasikan CSF dengan menyelaraskan fungsi, kategori, dan subkategorinya dengan persyaratan misi, toleransi risiko, dan sumber daya mereka. NIST telah menghasilkan contoh Profil khusus sektor dan ancaman, yang dapat digunakan oleh organisasi untuk membangun Profil mereka. Dalam CSF 2.0, NIST berencana untuk menghasilkan template dasar opsional untuk Profil CSF untuk menyarankan format dan area yang perlu dipertimbangkan. Meskipun organisasi dapat menggunakan format yang berbeda, penggunaan template diharapkan dapat meningkatkan produksi Profil khusus sektor dan organisasi serta mempermudah pengembangannya. NIST mencari umpan balik tentang konten apa yang harus disertakan dalam template.
3. Tingkatkan situs web CSF untuk menyoroti sumber daya implementasi
   Situs web CSF NIST memiliki berbagai sumber daya, seperti Profil sampel, panduan, alat, studi kasus, kisah sukses, publikasi, dan webinar, yang dapat digunakan organisasi untuk mengimplementasikan kerangka kerja. NIST akan mengubah situs web untuk meningkatkan konten dan kegunaan, serta menghapus sumber daya yang sudah usang. Selain itu, NIST berencana untuk meningkatkan kesadaran akan sumber daya yang ada dan mengidentifikasi yang baru.

D. CSF 2.0 akan menekankan pentingnya tata kelola keamanan siber

1. Penambahan Fungsi Tata Kelola baru

CSF 2.0 akan menyertakan Fungsi "Pemerintah" baru untuk menyoroti pentingnya hasil tata kelola manajemen risiko keamanan siber. Fungsi baru ini akan menekankan bahwa tata kelola keamanan siber sangat penting untuk mengelola dan mengurangi risiko keamanan siber. Kegiatan yang berada di bawah tata kelola keamanan siber dapat mencakup penentuan prioritas dan toleransi risiko, menilai risiko dan dampak keamanan siber, menetapkan kebijakan dan prosedur keamanan siber, dan memahami peran dan tanggung jawab keamanan siber.

Fungsi Tata Kelola yang baru di CSF 2.0 akan menginformasikan dan mendukung Fungsi lainnya, dan mempromosikan penyelarasan aktivitas keamanan siber dengan risiko perusahaan dan persyaratan hukum. Kategori saat ini di CSF 1.1 yang mencakup tata kelola akan dipindahkan ke Fungsi Tata Kelola yang baru, termasuk Lingkungan Bisnis (ID.BE), Tata Kelola (ID.GV), dan Strategi Manajemen Risiko (ID.RM).

CSF 2.0 juga akan memperluas pertimbangan topik terkait tata kelola di Fungsi baru. Subkategori saat ini di bawah Pemerintahan (ID.GV) masing-masing dapat diangkat ke kategori terpisah di bawah Pemerintahan. NIST menerima umpan balik tentang Kategori dan Subkategori apa yang harus digabungkan dalam Fungsi ini, dan akan meninjau kerangka kerja NIST lainnya dengan tata kelola sebagai fungsi yang sudah ada.

2. Meningkatkan pembahasan hubungan dengan manajemen risiko
   Revisi CSF 2.0 akan memperkenalkan Fungsi "Tata Kelola" baru yang menekankan hasil tata kelola manajemen risiko keamanan siber. Fungsi lintas sektor baru ini akan mendorong penyelarasan aktivitas keamanan siber dengan risiko perusahaan dan persyaratan hukum, serta mendukung lima fungsi CSF lainnya. Kategori saat ini di CSF 1.1 yang mencakup tata kelola akan dipindahkan ke Fungsi Tata Kelola yang baru, dan subkategori di bawah Tata Kelola akan diangkat ke kategori terpisah di bawah Tata Kelola di CSF 2.0. Revisi juga menawarkan kesempatan untuk mengklarifikasi hubungan antara tata kelola dan manajemen risiko keamanan siber di seluruh narasi CSF dan Core, menekankan sifat penting dari proses manajemen risiko yang mendasari untuk mengidentifikasi, menganalisis, memprioritaskan, merespons, dan memantau risiko. CSF 2.0 akan menjelaskan bagaimana hasil CSF mendukung keputusan respons risiko dan memberikan contoh proses manajemen risiko yang dapat digunakan untuk mendukung penerapan CSF, seperti Kerangka Kerja Manajemen Risiko dan ISO 31000.

E. CSF 2.0 akan menekankan pentingnya manajemen risiko rantai pasokan keamanan siber (C-SCRM)

1. Memperluas cakupan rantai pasokan
   Responden RFI setuju bahwa risiko keamanan siber dalam rantai pasokan dan pihak ketiga merupakan risiko utama di seluruh organisasi. CSF 1.1 telah menambahkan Kategori "Manajemen Risiko Rantai Pasokan" CSF dan memperluas bagian terkait C-SCRM. Namun, ada beragam pendapat tentang bagaimana masalah ini harus ditangani dalam pembaruan CSF. NIST percaya bahwa CSF 2.0 harus memberikan panduan tambahan untuk mengidentifikasi, menilai, dan mengelola risiko pihak pertama dan ketiga. NIST mengundang umpan balik tentang cara menangani C-SCRM di CSF 2.0, termasuk integrasi lebih lanjut di seluruh Inti CSF, membuat Fungsi baru yang berfokus pada C-SCRM, atau memperluas hasil C-SCRM dalam Kategori ID.SC saat ini. Selain itu, NIST mengundang umpan balik tentang potensi penanganan pengembangan perangkat lunak yang aman sebagai bagian dari hasil C-SCRM.

F. CSF 2.0 akan memajukan pemahaman tentang pengukuran dan penilaian keamanan siber

1. Mengklarifikasi bagaimana memanfaatkan CSF dapat mendukung pengukuran dan penilaian program keamanan dunia maya
   CSF 2.0 akan menekankan bahwa dengan menggunakan CSF, organisasi dapat memiliki bahasa dan cara yang sama untuk mengkomunikasikan hasil penilaian dan upaya pengukurannya, terlepas dari proses manajemen risikonya. Tujuan utama pengukuran dan penilaian keamanan siber adalah untuk menentukan seberapa baik organisasi mengelola risiko keamanan siber dan terus meningkatkannya. Aktivitas ini, mulai dari tingkat sistem hingga keseluruhan organisasi, merupakan masukan untuk menentukan maturitas dan mendukung keputusan manajemen risiko.
2. Memberikan contoh pengukuran dan penilaian menggunakan CSF
   CSF 2.0 mengakui bahwa setiap organisasi memiliki risiko, prioritas, dan sistem unik yang memerlukan pendekatan berbeda untuk mencapai hasil Inti Kerangka Kerja. Oleh karena itu, NIST tidak akan memberikan pendekatan tunggal untuk penilaian di CSF 2.0, melainkan menawarkan contoh bagaimana organisasi telah menggunakan CSF untuk menilai dan mengkomunikasikan kemampuan keamanan siber mereka. CSF 2.0 juga akan menyertakan contoh bagaimana organisasi dapat memanfaatkan CSF, dikombinasikan dengan strategi manajemen risiko dan model maturitas, untuk mengomunikasikan postur keamanan siber mereka kepada khalayak non-keamanan siber dan menilai efektivitas program keamanan siber mereka. Panelis Lokakarya #1 CSF 2.0 telah memberikan contoh bagaimana organisasi menyelaraskan implementasi CSF mereka dengan misi atau kebutuhan bisnis tertentu dengan memanfaatkan kerangka kerja manajemen risiko dan model maturitas lainnya.
3. Perbarui Panduan Pengukuran Kinerja NIST untuk Keamanan Informasi
   NIST sedang memperbarui Panduan Pengukuran Kinerja untuk Keamanan Informasi (SP 800-55r2), yang memberikan panduan kepada organisasi dalam menggunakan langkah-langkah untuk meningkatkan pengambilan keputusan, kinerja, dan akuntabilitas program keamanan siber atau sistem informasi. Panduan ini berlaku untuk pengukuran berbagai aktivitas program keamanan siber dan mungkin berguna bagi mereka yang memanfaatkan CSF. Dasar-dasar proses dan implementasi pengukuran keamanan siber tidak akan disertakan dalam CSF 2.0 tetapi dalam NIST SP 800-55.
4. Berikan panduan tambahan tentang Kerangka Implementasi Tiers
   Tingkat CSF digunakan oleh organisasi untuk memahami pendekatan mereka terhadap risiko keamanan siber dan proses yang ada untuk mengelola risiko tersebut. Tingkatan memiliki berbagai tingkat ketelitian dalam menjelaskan praktik manajemen risiko keamanan siber secara keseluruhan, termasuk proses manajemen risiko, integrasi program manajemen risiko, dan partisipasi aktif dalam ekosistem keamanan siber yang lebih luas. Organisasi menggunakan Tingkatan dalam berbagai cara, mulai dari menetapkan tujuan internal hingga mengomunikasikan postur keamanan siber organisasi dan mengukur kematangan program keamanan siber. CSF 2.0 akan mengklarifikasi ruang lingkup dan penerapan Tingkatan, menjelaskan dengan lebih baik hubungan antara Tingkatan dan model kematangan, dan dapat mengalihkan fokus Tingkatan ke tujuan dan sasaran dalam konteks tata kelola. NIST mencari

umpan balik tentang nilai dari perubahan tersebut, serta umpan balik tentang cara organisasi menggunakan Tingkatan. CSF 2.0 tidak akan memberikan model maturitas yang berbeda, namun dapat menyertakan sumber daya tambahan untuk menggunakan Tingkatan dalam Profil CSF dan berbagi pemetaan antar Tingkatan, proses manajemen risiko, dan model maturitas. Panduan Pengukuran Kinerja untuk Keamanan Informasi (SP 800-55r2) memberikan panduan tentang pengukuran berbagai aktivitas program keamanan siber dan mungkin sangat berguna bagi mereka yang memanfaatkan CSF.