Resume Cyber Security Framework V2
Keamanan Jaringan

Dosen Pembimbing :

Dr. Ferry Astika Saputra, ST., M.Sc.

Disusun Oleh :

Lula Rania Salsabilla (3122640045)

1 D4 – IT B LJ

D4 TEKNIK INFORMATIKA

DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

2023

Resume Cyber Security Framework V2

Pendahuluan

- Kerangka Keamanan Siber NIST (CSF atau Framework) memberikan panduan kepada organisasi untuk lebih memahami, mengelola, mengurangi, dan mengomunikasikan risiko keamanan siber.
- Merupakan sebuah dasar dan sumber daya penting yang digunakan oleh semua sektor di seluruh dunia. Meskipun risiko keamanan siber berkembang, banyak responden NIST Cybersecurity RFI melaporkan bahwa CSF tetap efektif di menangani risiko keamanan siber dengan memfasilitasi tata kelola dan program manajemen risiko dan meningkatkan komunikasi di dalam dan lintas organisasi.
- CSF telah diadopsi secara sukarela dan dalam kebijakan dan mandat pemerintah di semua tingkatan di seluruh dunia, mencerminkan sifatnya yang tahan lama dan fleksibel untuk melampaui risiko, sektor, teknologi, dan batas negara.
- CSF dimaksudkan untuk menjadi dokumen hidup yang disempurnakan dan diperbaiki dari waktu ke waktu.
- Dengan ekstensif keterlibatan masyarakat, NIST awalnya menghasilkan Framework pada tahun 2014 dan memperbaruinya pada tahun 2018 dengan CSF 1.1. CSF diperbarui secara terbuka dengan masukan dari pemerintah, akademisi, dan industri, termasuk melalui lokakarya, tinjauan dan komentar publik, dan lainnya bentuk-bentuk keterlibatan.
- Dengan pembaruan ini, NIST terbuka untuk membuat perubahan yang lebih substansial daripada di pembaruan sebelumnya. Versi “CSF 2.0” mencerminkan lanskap keamanan siber yang berkembang— tetapi kebutuhan masyarakat akan mendorong luas dan isi perubahan.

Potensi Perubahan Signifikan dalam CSF 2.

- Bagian ini menguraikan usulan perubahan pada CSF 2.0 dan sumber daya terkait. NIST mencari umpan balik atau feedback pada masing-masing pendekatan yang dijelaskan di bawah ini.
- Dalam beberapa bagian di bawah ini yang menguraikan usulan perubahan dalam CSF dan kegiatan terkait, NIST mengidentifikasi "Ajakan Bertindak" yang memilih cara-

cara di mana komunitas dapat berkontribusi peningkatan CSF 2.0 dan sumber daya terkait.

1. **CSF 2.0 akan secara eksplisit mengenali penggunaan luas CSF untuk mengklarifikasi aplikasi potensialnya.**

❖ **Mengubah judul dan teks CSF untuk mencerminkan tujuan penggunaannya oleh semua organisasi.**

- Meskipun CSF pada awalnya dikembangkan untuk mengatasi risiko keamanan siber dari infrastruktur penting terlebih dahulu, CSF telah digunakan secara lebih luas. Sebagai pengakuan atas hal ini, CSF 2.0 akan menggunakan nama yang lebih luas dan umum digunakan, yaitu "Cybersecurity Framework" setalah sebelumnya bernama "Kerangka Kerja untuk Meningkatkan Keamanan Siber Infrastruktur Kritis".
- Cakupan CSF 2.0 akan mencakup semua organisasi lintas pemerintahan, industri, dan akademisi, termasuk namun tidak terbatas pada infrastruktur penting. Referensi ke infrastruktur penting dalam CSF dapat dipertahankan sebagai contoh, tetapi teks Framework akan ditinjau untuk penerapan yang luas.
- Kategori dan Subkategori Inti CSF yang khusus untuk infrastruktur kritis, seperti ID.BE-2 dan ID.RM-3, akan diperluas. Perubahan ini tidak dimaksudkan untuk mengurangi relevansi CSF dengan organisasi infrastruktur penting, termasuk pentingnya memastikan keamanan dan ketahanan infrastruktur kritis bangsa kita, tetapi untuk merangkul dan meningkatkan penggunaannya secara lebih luas.

❖ **Memastikan lingkup CSF bermanfaat bagi organisasi terlepas dari sektor, jenis, atau ukurannya.**

- Sejak melakuakan publikasi CSF 1.1, Kongres mengarahkan NIST untuk mempertimbangkan masalah bisnis kecil dan kebutuhan keamanan social media. Selain itu, CSF adalah sumber daya yang diakui untuk organisasi negara bagian dan lokal di bawah Program Hibah Keamanan Siber Negara

Bagian dan Lokal Departemen Keamanan Dalam Negeri (DHS) dan telah dirujuk secara luas oleh banyak asosiasi serta lembaga pemerintah di berbagai tingkatan.

- Menanggapi hal tersebut, NIST akan meningkatkan upayanya untuk memastikan kerangka ini bermanfaat bagi organisasi – dan juga sektor, jenis, atau ukurannya dalam mengatasi tantangan keamanan siber dan mendorong semua pihak yang berkepentingan untuk berpartisipasi dalam proses tersebut.

❖ **Meningkatkan kerjasama dan keterlibatan internasional.**

- RFI menyerukan peningkatan kolaborasi dan keterlibatan internasional sebagai tema penting untuk pembaruan CSF 2.0. Sejak peluncuran pengembangan CSF pada tahun 2013, banyak organisasi telah memperjelas bahwa penggunaan CSF secara internasional akan meningkatkan efisiensi dan efektivitas upaya keamanan siber mereka.
- CSF 1.1 sering dirujuk dalam strategi, kebijakan, dan panduan yang dikembangkan oleh negara lain. Beberapa negara, di seluruh wilayah di dunia, telah mengadopsi atau mengadaptasi kerangka tersebut, dan beberapa menganggap penggunaan kerangka tersebut wajib untuk sektor publik dan swasta mereka.
- NIST akan terus berpartisipasi dalam kegiatan standar internasional yang memanfaatkan CSF sebagai bagian dari upaya dan prioritas yang lebih luas untuk terlibat secara strategis dalam pekerjaan organisasi pengembangan standar internasional.

2. CSF 2.0 akan tetap menjadi kerangka kerja, menyediakan konteks dan koneksi ke standar dan sumber daya yang ada.

❖ **Mempertahankan tingkat detail CSF saat ini**

- Secara keseluruhan, responden RFI memperjelas bahwa atribut utama kerangka – termasuk sifatnya yang fleksibel, sederhana, dan mudah

digunakan – telah bermanfaat untuk implementasi oleh organisasi dari berbagai ukuran, jenis, dan sektor.

- Merefleksikan masukan ini, NIST bertujuan untuk mempertahankan tingkat detail dan spesifisitas saat ini dalam CSF 2.0 untuk memastikannya tetap dapat diskalakan dan fleksibel untuk berbagai organisasi.
- Framework ini akan terus menyediakan struktur pengorganisasian umum untuk berbagai pendekatan keamanan siber, termasuk dengan memanfaatkan dan menghubungkan ke, tetapi tidak menggantikan, standar dan pedoman yang diakui secara global.

❖ **Mengaitkan CSF dengan jelas ke kerangka kerja NIST lainnya.**

- Kerangka kerja terkait keamanan siber dan privasi NIST lainnya – Kerangka Manajemen Risiko, Kerangka Privasi, Prakarsa Nasional untuk Kerangka Kerja Pendidikan Keamanan Siber untuk Keamanan Siber, dan Kerangka Pengembangan Perangkat Lunak Aman – masing-masing akan tetap menjadi kerangka kerja yang terpisah. Masing-masing berfokus pada topik tertentu yang layak untuk panduan khusus.
- Namun, setiap kerangka kerja memiliki hubungan dengan CSF, sehingga akan dirujuk sebagai pedoman baik dalam CSF 2.0 maupun dalam materi pendamping, seperti pemetaan.

❖ **Memanfaatkan Cybersecurity dan Alat Referensi Privasi untuk CSF 2.0 Core online.**

- Selain format PDF dan Excel, CSF 2.0 akan dipamerkan melalui NIST Cybersecurity and Privacy Reference Tool (CPRT) yang baru diluncurkan. CPRT menawarkan format yang dapat dibaca mesin dan antarmuka pengguna yang konsisten untuk mengakses data referensi dari standar keamanan siber dan privasi NIST, pedoman, dan kerangka kerja, serta pendekatan yang fleksibel untuk mengkarakterisasi hubungan antara standar, pedoman, dan kerangka kerja serta berbagai aplikasi dan teknologi.

❖ **Gunakan Referensi Informatif online yang dapat diperbarui.**

- CSF 1.1 Core mengidentifikasi serangkaian hasil keamanan siber berdasarkan dan terhubung ke Referensi Informatif – standar, pedoman, dan praktik keamanan siber yang sudah ada dan diterima secara luas untuk memberikan panduan implementasi tambahan.
- Sementara konsep referensi informatif diterima dengan baik, beberapa Referensi Informatif CSF menjadi usang karena dokumen sumber tersebut diperbarui. Selain itu, kolom Referensi Informatif di CSF 1.1 hanya mewakili sebagian kecil dari contoh standar yang dapat dimanfaatkan oleh organisasi dalam menggunakan CSF.
- Banyak komentator RFI menunjuk pada nilai Referensi Informatif dan menyatakan ketertarikannya pada pemetaan tambahan. Dalam CSF 2.0, NIST akan beralih ke penggunaan referensi online yang dapat diperbarui yang dipamerkan melalui CPRT.

❖ **Gunakan Referensi Informatif untuk memberikan lebih banyak panduan untuk menerapkan CSF**

- NIST akan bekerja dengan masyarakat untuk mendorong dan mengaktifkan pembuatan pemetaan yang mendukung CSF 2.0. Ada minat masyarakat yang kuat terhadap pemetaan tambahan; responden RFI meminta pemetaan ke hampir 50 standar keamanan siber, pedoman, dan kerangka kerja lainnya, banyak di antaranya ditulis oleh organisasi lain. Dengan menggunakan referensi online, CSF dapat dipetakan ke sumber daya yang lebih spesifik untuk memberikan panduan tambahan, seperti untuk mengamankan informasi rahasia yang terkendali, komputasi awan, Internet of Things (IoT) dan keamanan siber teknologi operasional (OT), arsitektur tanpa kepercayaan (ZTA), dan lainnya.

3. **CSF 2.0 (dan sumber daya pendamping) akan menyertakan panduan yang diperbarui dan diperluas tentang implementasi Framework.**

❖ **Tambahkan contoh penerapan untuk Subkategori CSF**

- CSF 2.0 akan mencakup contoh global implementasi 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. Menambahkan contoh global yang disarankan dalam tanggapan RFI dan telah berhasil dimanfaatkan dalam kerangka NIST lainnya seperti kerangka Pengembangan Perangkat Lunak Aman dan Draf Playbook Kerangka Kerja Manajemen Risiko Kecerdasan Buatan.

❖ **Kembangkan template Profil CS**

- Sehubungan dengan pengembangan CSF 2.0, NIST akan menghasilkan template dasar opsional untuk Profil CSF yang menyarankan format dan area untuk dipertimbangkan dalam Profil. Sementara organisasi dapat terus menggunakan format yang berbeda untuk Profil berdasarkan kebutuhan khusus mereka, penggunaan template diharapkan dapat meningkatkan produksi Profil khusus sektor dan organisasi dan membuat pengembangan Profil lebih mudah bagi pengguna. NIST mencari umpan balik tentang konten apa yang harus dimanfaatkan dalam template Profil CSF, termasuk organisasi konten yang saat ini disertakan dalam Profil CSF mereka.

❖**Tingkatkan situs web CSF untuk menyoroti sumber daya implementasi**

- Untuk meningkatkan kesadaran, pemahaman, dan penggunaan CSF, NIST telah mengembangkan dan bekerja sama dengan pihak lain untuk menghasilkan ringkasanKisah Sukses CSF menjelaskan bagaimana beragam organisasi telah menggunakan CSF untuk meningkatkan manajemen risiko keamanan siber mereka. Ada banyak peluang untuk memperluas jumlah kisah sukses karena koleksi saat ini terbatas – seperti yang ditunjukkan oleh banyaknya organisasi yang memberikan pernyataan dan indikasi penggunaan CSF secara produktif.

4. CSF 2.0 akan menekankan pentingnya tata kelola keamanan siber.

❖ **Tambahkan Fungsi Pemerintahan baru**

- Mencerminkan masukan substansial untuk NIST, CSF 2.0 akan menyertakan Fungsi "Pemerintah" baru untuk menekankan hasil tata kelola manajemen risiko keamanan siber. Sementara lima Fungsi CSF telah diadopsi secara luas dalam kebijakan nasional dan internasional, termasuk standar ISO, NIST percaya bahwa ada banyak manfaat untuk memperluas pertimbangan tata kelola dalam CSF 2.0.
- Fungsi lintas sektor baru ini akan menyoroti bahwa tata kelola keamanan siber sangat penting untuk mengelola dan mengurangi risiko keamanan siber. Tata kelola keamanan siber dapat mencakup penentuan prioritas dan toleransi risiko organisasi, pelanggan, dan masyarakat yang lebih luas; penilaian risiko dan dampak keamanan siber; penetapan kebijakan dan prosedur keamanan siber; dan pemahaman tentang peran dan tanggung jawab keamanan siber.
- Kegiatan ini sangat penting untuk mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan di seluruh organisasi, serta dalam mengawasi pihak lain yang melakukan aktivitas keamanan dunia maya untuk organisasi, termasuk dalam rantai pasokan organisasi. Mengangkat aktivitas tata kelola ke suatu Fungsi juga akan mendorong penyelarasan aktivitas keamanan siber dengan risiko perusahaan dan persyaratan hukum.

❖ **Meningkatkan pembahasan hubungan dengan manajemen risiko**

- Merevisi CSF menawarkan kesempatan untuk mengklarifikasi hubungan antara tata kelola dan manajemen risiko keamanan siber di seluruh narasi dan Inti CSF. CSF 2.0 akan menjelaskan bagaimana proses manajemen risiko yang mendasari sangat penting untuk mengidentifikasi, menganalisis, memprioritaskan, merespons, dan memantau risiko, bagaimana hasil CSF mendukung keputusan respons risiko (menerima, memitigasi, mentransfer, menghindari), dan berbagai contoh proses

manajemen risiko (misalnya, Kerangka Kerja Manajemen Risiko, ISO 31000) yang dapat digunakan untuk mendukung implementasi CSF.

5. **CSF 2.0 akan menekankan pentingnya cybersecurity supply chain risk management (C-SCRM).**

❖ **Memperluas cakupan rantai pasokan**

- Mengelola keamanan dunia maya dalam rantai pasokan adalah salah satu tambahan utama dalam pembaruan terakhir CSF. Sejak saat itu, lebih banyak perhatian telah diberikan untuk mengembangkan panduan guna meningkatkan kepercayaan dan jaminan dalam produk dan layanan teknologi, termasukpanduan dikembangkan berdasarkan Perintah Eksekutif, "Meningkatkan Keamanan Siber Bangsa" (EO 14028). CSF 1.1 menambahkan Kategori CSF "Supply Chain Risk Management" (ID.SC); diperluas Bagian 3.3, Mengkomunikasikan Persyaratan Keamanan Siber dengan Pemangku Kepentingan untuk lebih memahami C-SCRM; menambahkan Bagian 3.4 baru, Keputusan Pembelian untuk menyoroti penggunaan Kerangka dalam memahami risiko yang terkait dengan produk dan layanan siap pakai; dan memasukkan kriteria C-SCRM ke dalam CSF Tiers. Selain itu, manajemen pihak ketiga disertakan sebagai pertimbangan sebagai bagian dari hasil CSF yang lebih luas di seluruh Fungsi Kerangka Kerja.

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

Pengukuran dan penilaian program dan strategi manajemen risiko keamanan siber terus menjadi area penting dalam penggunaan CSF. Tanggapan RFI menunjukkan responden mencari panduan dan sumber daya CSF tambahan untuk mendukung pengukuran dan penilaian penggunaan CSF oleh organisasi. Keinginan terkait adalah agar CSF menjelaskan dengan jelas bagaimana organisasi dapat menggunakan Tingkatan Implementasi, dan bagaimana mereka berhubungan dengan pengukuran.

- **Memperjelas bagaimana pemanfaatan CSF dapat mendukung pengukuran dan penilaian program keamanan siber.**
    - CSF 2.0 akan memperjelas bahwa dengan memanfaatkan CSF, organisasi memiliki taksonomi dan leksikon yang sama untuk mengkomunikasikan hasil upaya pengukuran dan penilaian mereka, terlepas dari proses manajemen risiko yang mendasarinya. Di semua organisasi, tujuan utama pengukuran dan penilaian keamanan siber adalah untuk menentukan seberapa baik mereka mengelola risiko keamanan siber, dan jika serta bagaimana mereka terus meningkat. Aktivitas yang mendukung pengukuran dan penilaian – mulai dari tingkat sistem hingga keseluruhan organisasi – merupakan input untuk menentukan maturitas dan mendukung keputusan manajemen risiko.
- **Memberikan contoh pengukuran dan penilaian menggunakan CSF.**
    - Setiap risiko, prioritas, dan sistem organisasi adalah unik, sehingga metode dan tindakan yang digunakan untuk mencapai hasil yang dijelaskan oleh Framework Core bervariasi.
    - Dengan demikian, pengukuran dan penilaian hasil bervariasi tergantung pada konteksnya. Karena tidak ada pendekatan tunggal untuk mengukur dan menilai CSF, NIST tidak akan mengedepankan satu pendekatan penilaian dalam CSF 2.0 untuk melanjutkan fleksibilitas dalam bagaimana organisasi dapat mengimplementasikan Kerangka tersebut.
    - Alih-alih satu pendekatan, CSF 2.0 akan menyertakan contoh bagaimana organisasi telah menggunakan CSF untuk menilai dan mengomunikasikan kemampuan keamanan siber mereka. Ini mungkin termasuk contoh bagaimana organisasi dapat memanfaatkan CSF, dikombinasikan dengan strategi manajemen risiko dan model kematangan, untuk mengomunikasikan jawaban atas pertanyaan tentang keefektifan keamanan siber mereka.