Keamanan Jaringan
(Cyber Security Framework)

Oleh:

Aldo Faiz Winarno (3122640039)

D4 LJ IT B

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

TAHUN 2023

Cyber Security Framework v2.0

▪ Pendahuluan

The NIST Cybersecurity Framework (CSF or Framework) memberikan panduan kepada organisasi untuk memahami, mengelola, mengurangi, dan mengomunikasikan risiko keamanan siber dengan lebih baik. Ini adalah pondasi penting yang digunakan oleh semua sektor di seluruh dunia. Meskipun risiko keamanan siber terus berkembang, namun CSF tetap efektif dalam mengatasi risiko keamanan siber dengan memfasilitasi program tata kelola dan manajemen risiko dan meningkatkan komunikasi di dalam dan di seluruh organisasi.

CSF dimaksudkan sebagai dokumen hidup yang disempurnakan dan ditingkatkan dari waktu ke waktu. Dengan keterlibatan masyarakat yang luas dengan keterlibatan masyarakat yang luas, NIST awalnya membuat Kerangka Kerja 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 *workshop*, tinjauan, komentar publik, dan bentuk keterlibatan lainnya.

▪ Potensi Perubahan Signifikan dalam CSF 2.0

1. CSF 2.0 akan secara eksplisit mengakui penggunaan CSF secara luas untuk memperjelas potensi aplikasinya.
   - **Mengubah judul dan teks CSF untuk mencerminkan tujuan penggunaannya oleh semua organisasi.**
     CSF 2.0 akan menggunakan nama yang lebih luas dan umum digunakan, "Cybersecurity Framework" sebagai gantinya dari "Framework for Improving Critical Infrastructure Cybersecurity".
   - **Cakupan CSF memastikan bermanfaat bagi organisasi terlepas dari sektor, jenis, atau ukuran.**
     Memastikan Framework ini membantu organisasi - terlepas dari sektor, jenis, atau ukurannya - dalam menangani tantangan keamanan siber dan mendorong semua pihak yang berkepentingan untuk berpartisipasi dalam proses tersebut.
   - **Meningkatkan kolaborasi dan keterlibatan internasional.**
     Memprioritaskan pertukaran dengan pemerintah dan industri asing sebagai bagian dari pengembangan CSF 2.0 serta berpartisipasi dalam kegiatan standar internasional yang memanfaatkan CSF sebagai bagian dari upaya dan prioritas yang lebih luas untuk terlibat secara strategis dalam pekerjaan standar internasional organisasi yang sedang berkembang.

2. CSF 2.0 akan tetap menjadi kerangka kerja, memberikan konteks dan koneksi yang standar pada sumber daya yang ada.
   - **Mempertahankan tingkat detail CSF saat ini.**
     Mempertahankan tingkat detail dan kekhususan saat ini dalam CSF 2.0 untuk memastikannya tetap terukur dan fleksibel untuk berbagai organisasi.

- **Menghubungkan CSF dengan jelas ke kerangka kerja NIST lainnya.**
  Framework terkait keamanan siber dan privasi NIST lainnya, seperti the Risk Management Framework, the Privacy Framework, the National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity, dan the Secure Software Development Framework masing-masing akan akan tetap menjadi kerangka kerja yang terpisah. Masing-masing berfokus pada topik-topik spesifik yang layak untuk panduan khusus.
- **Memanfaatkan Alat Referensi Keamanan Siber dan Privasi untuk inti CSF 2.0 secara online.**
  Selain format PDF dan Excel, Cybersecurity and Privacy Reference Tool (CPRT) menawarkan format yang dapat dibaca oleh mesin dan antarmuka pengguna yang konsisten untuk mengakses data referensi dari standar, pedoman, dan kerangka kerja keamanan siber dan privasi NIST, serta pendekatan yang fleksibel untuk mengkarakterisasi hubungan antara standar, pedoman, dan kerangka kerja, serta berbagai aplikasi dan teknologi.
- **Menggunakan Referensi Informatif online yang dapat diperbarui.**
  Pada CSF 2.0, NIST akan bergerak ke arah penggunaan referensi online yang dapat diperbarui yang ditampilkan melalui CPRT.
- **Menggunakan Referensi Informatif untuk memberikan panduan lebih lanjut untuk mengimplementasikan CSF.**
  NIST akan bekerja sama dengan komunitas untuk mendorong dan memungkinkan produksi pemetaan yang mendukung CSF 2.0.
- **Tetap netral terhadap teknologi dan vendor, tetapi mencerminkan perubahan dalam keamanan siber praktik keamanan siber.**
  CSF dapat terus dimanfaatkan oleh organisasi terlepas dari teknologi atau layanan yang mereka gunakan, termasuk layanan TI, IoT, OT, dan Cloud.

3. CSF 2.0 (dan sumber daya pendamping) akan mencakup panduan yang diperbarui dan diperluas dengan implementasi Framework.
   - **Menambahkan contoh implementasi untuk Subkategori CSF.**
     CSF 2.0 akan menyertakan contoh implementasi nosional dari proses dan aktivitas yang ringkas dan berorientasi pada tindakan untuk membantu mencapai hasil dari Subkategori CSF, di samping panduan yang disediakan dalam Referensi Informatif CSF.
   - **Mengembangkan templat Profil CSF.**
     Profil khusus sektor dan ancaman yang dapat dimanfaatkan oleh organisasi untuk membangun Profil organisasinya. Contoh Profil ini memudahkan organisasi untuk menerapkan CSF dengan memprioritaskan dan menyelaraskan hasil CSF dengan risiko dan standar sektor dan ancaman tertentu.
   - **Memperbaiki situs web CSF untuk menyoroti implementasi sumber daya.**
     Situs web CSF NIST berisi banyak informasi dan panduan tambahan tentang penerapan CSF. Ini termasuk berbagai sumber daya yang dikembangkan oleh NIST dan organisasi eksternal, termasuk contoh Profil CSF, pemetaan, panduan, alat bantu,

studi kasus, kisah sukses, publikasi terkait (seperti Panduan Memulai Cepat CSF), dan webinar.

4. CSF 2.0 akan menekankan pentingnya tata kelola keamanan siber.
   - **Menambahkan Fungsi Pengaturan baru.**
     NIST, CSF 2.0 akan menyertakan Fungsi "Kelola" baru untuk menekankan hasil tata kelola manajemen risiko keamanan siber. Meskipun lima Fungsi CSF telah mendapatkan adopsi luas dalam kebijakan nasional dan internasional, termasuk standar ISO, NIST percaya bahwa ada banyak manfaat untuk memperluas pertimbangan tata kelola dalam CSF 2.0.
   - **Meningkatkan diskusi mengenai hubungan dengan manajemen risiko.**
     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, memindahkan, menghindari), dan berbagai contoh proses manajemen risiko yang dapat digunakan untuk mendukung implementasi CSF.

5. CSF 2.0 akan menekankan pentingnya manajemen risiko rantai pasokan keamanan siber (C-SCRM).
   - **Memperluas cakupan rantai pasokan**
     Dengan meningkatnya globalisasi, outsourcing, dan perluasan penggunaan layanan teknologi (seperti komputasi awan), CSF 2.0 harus memperjelas pentingnya organisasi untuk mengidentifikasi, menilai, dan mengelola risiko pihak pertama dan ketiga.

6. CSF 2.0 akan memajukan pemahaman tentang pengukuran keamanan siber dan penilaian.
   - **Memperjelas bagaimana memanfaatkan 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 dari upaya pengukuran dan penilaian mereka, terlepas dari proses manajemen risiko yang mendasarinya.
   - **Memberikan contoh pengukuran dan penilaian menggunakan CSF.**
     Risiko, prioritas, dan sistem setiap organisasi adalah unik, sehingga metode dan tindakan yang digunakan untuk mencapai hasil yang dijelaskan oleh Kerangka Kerja Inti berbeda-beda. Dengan demikian, pengukuran dan penilaian hasil juga bervariasi tergantung pada konteksnya.
   - **Memperbarui Panduan Pengukuran Kinerja NIST untuk Keamanan Informasi.**
     Memberikan panduan kepada organisasi tentang penggunaan ukuran untuk meningkatkan pengambilan keputusan, kinerja, dan akuntabilitas program keamanan siber atau sistem informasi.

- **Memberikan panduan tambahan tentang Tingkatan Implementasi Kerangka Kerja.**

  Tingkatan CSF menyediakan mekanisme bagi organisasi untuk melihat dan memahami

  pendekatan mereka terhadap risiko keamanan siber serta proses dan program yang ada untukmengelola risiko tersebut. Tingkatan tersebut memiliki tingkat ketelitian dan kecanggihan yang semakin meningkat dalam menggambarkan 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.