LAPORAN RESMI
KEMANAN JARINGAN

Cybersecurity Framework

Dosen :
Dr. Ferry Astika Saputra ST, M.Sc
Oleh :
Septiana Dyah Anissawati
D4 LJ Teknik Informatika B
3122640031

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
TAHUN AJARAN
2022/2023

Jelasakan tentang CSF v2 dengna menggunakan referensi :
https://www.nist.gov/cyberframework

CSF v2 atau *Cybersecurity Framework* Version 2 adalah kerangka kerja (framework) yang dibuat oleh *National Institute of Standards and Technology* (NIST) untuk membantu organisasi dalam membangun dan meningkatkan kemampuan keamanan siber mereka. CSF v2 menggantikan versi sebelumnya, yaitu CSF v1.1 dan dirilis pada tahun 2021. *Cybersecurity framework* dapat membantu organisasi dan perusahaan dalam mengidentifikasi risiko keamanan siber yang mungkin terjadi, mengevaluasi sistem keamanan yang ada, dan mengembangkan strategi dan rencana tindakan yang efektif untuk mengurangi risiko tersebut. Kerangka kerja CSF v2 terdiri dari tiga bagian utama: Core, Implementation Tiers, dan Profiles. Berikut adalah penjelasan singkat tentang masing-masing bagian:

1. **Core**: Core merupakan serangkaian aktivitas yang hasilnya diinginkan dalam bidang keamanan siber untuk mengorganisir kedalam kategori yang disesuaikan dengan referensi infomatif. Framework Core dirancang untuk mudah dipahami sehingga menjadi lapisan penerjemah yang digunakan untuk komunikasi antara tim disiplin dengan menggunakan bahasa sederhana. Core terdiri dari 3 bagian yaitu Fungsi, Kategori dan Subkategori.
   Bagian ini mencakup seperangkat keamanan siber yang terdiri dari lima fungsi utama: Identify, Protect, Detect, Respond, dan Recover. Kelima fungsi ini membentuk dasar dari semua kegiatan keamanan siber yang dilakukan oleh organisasi. Selanjutnya terdapat 23 ktegori yang terbagi di lima fungsi.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

   Kategori-kategori diatas dorancang untuk mencakup tujuan keaman siber secara keseluruhan bagi sebuah organisasi.

Subkategori merupakan tingkat abstraksi yang mana terdapat 108 subkategori yang merupakan pernyataan yang didorong oleh hasil yang memberikan pertimbangan untuk membuat atau meningkatkan program keaman siber.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Kelima Subkategori yang tergambar pada Kategori Lingkungan Bisnis (ID.BE) memberikan contoh pernyataan yang didorong oleh hasil yang ditemukan di seluruh Core Framework. Kolom di sebelah kanan, Referensi Informatif, mendukung Framework dengan menyediakan referensi yang lebih teknis daripada Framework itu sendiri. Organisasi dapat memilih untuk menggunakan beberapa, tidak ada, atau seluruh referensi ini untuk menginformasikan aktivitas yang dilakukan untuk mencapai hasil yang dijelaskan dalam Subkategori.

2. **Implementation Tiers**: Menggambarkan sejauh mana praktik manajemen risiko keamanan siber dalam organisasi yang mana menunjukkan karakteristik yang didefinisikan framework. Bagian ini mencakup empat tingkat kesiapan keamanan siber: Partial, Risk-Informed, Repeatable, dan Adaptive. Tingkat kesiapan ini membantu organisasi untuk mengevaluasi seberapa matang dan efektif upaya keamanan siber mereka dan seberapa baik keputusan resiko keamanan siber terintegrasi ke dalam keputusan resiko yang lebih luas. Tiers tidak selalu mewakili tingkat kematangan. Organisasi harus menentukan Tiers yang diinginkan, memastikan tiers yang dipilih memenuhi tujuan organisasi, mengurangi resiko keamanan siber dan memungkinkan untuk diimplementasi secara fisik dan akuntansi.

3. **Profiles**: Digunakan untuk mengidentifikasi peluang untuk meningkatkan postur keamanan siber dengan membandingkan "Current" Profile and "Target" Profile. Profile berkaitan dengan mengoptimalkan framework keamanan siber untuk melayani organisasi. Salah satu cara untuk mendekati profil adalah dengan memetakan persyaratan keamanan siber, tujuan misi, dan metodologi operasional organisasi, bersama dengan praktik saat ini terhadap subkategori Framework Core untuk membuat "Current" Profile. Pembuatan profil ini dan analisis kesenjangan memungkinkan organisasi untuk membuat rencana implementasi yang diprioritaskan. Prioritas, ukuran

kesenjangan, dan perkiraan biaya dari tindakan perbaikan membantu organisasi merencanakan dan menganggarkan aktivitas peningkatan keamanan siber.

Dalam CSF v2, NIST menekankan pentingnya kolaborasi dan integrasi antara fungsi-fungsi keamanan siber yang berbeda. Organisasi disarankan untuk mengadopsi pendekatan yang terpadu dan holistik dalam membangun kemampuan keamanan siber mereka. Adopsi CSF version 2 (*Cybersecurity Framework Version 2*) memberikan beberapa manfaat bagi organisasi, di antaranya:

1. CSF v2 memberikan panduan yang komprehensif dan terintegrasi untuk membantu organisasi dalam mengevaluasi dan meningkatkan kemampuan keamanan siber mereka. Dengan menggunakan CSF v2, organisasi dapat mengidentifikasi dan mengatasi kelemahan keamanan siber mereka secara sistematis.
2. CSF v2 membantu organisasi dalam menentukan prioritas dan alokasi sumber daya mereka secara efektif untuk meningkatkan kemampuan keamanan siber. Dengan memahami risiko keamanan siber yang dihadapi dan mengadopsi pendekatan yang terpadu, organisasi dapat menghindari pengeluaran yang tidak perlu dan meningkatkan efisiensi dan efektivitas upaya mereka.
3. CSF v2 menyediakan bahasa yang seragam untuk membantu stakeholder dalam berkomunikasi dan bekerja sama dalam konteks keamanan siber. Ini membantu organisasi dalam menciptakan kerja sama yang lebih efektif dan saling mendukung antar departemen, mitra, dan penyedia layanan keamanan siber.
4. CSF v2 membantu organisasi untuk membangun reputasi keamanan siber yang kuat dan meningkatkan kepercayaan pelanggan, investor, dan pemangku kepentingan lainnya. Dengan menunjukkan keseriusan dan kesiapan dalam menghadapi ancaman keamanan siber, organisasi dapat meningkatkan citra dan nilai merek mereka.

Dalam keseluruhan, CSF v2 membantu organisasi untuk meningkatkan kemampuan keamanan siber mereka dengan pendekatan yang terpadu dan sistematis. Hal ini dapat membantu organisasi untuk mengidentifikasi dan mengatasi risiko keamanan siber yang mereka hadapi, menghindari pengeluaran yang tidak perlu, dan meningkatkan efisiensi dan efektivitas upaya keamanan siber mereka. Untuk mengadopsi CSF v2 (*Cybersecurity Framework Version 2*), organisasi perlu melakukan beberapa tahapan, antara lain:

1. **Evaluasi**: Organisasi harus mengevaluasi tingkat kesiapan dan kemampuan keamanan siber mereka dengan menggunakan CSF v2 sebagai panduan. Evaluasi ini dapat membantu organisasi untuk mengidentifikasi area yang perlu ditingkatkan dan membuat rencana aksi yang spesifik.
2. **Penentuan Prioritas**: Organisasi harus menentukan prioritas dan alokasi sumber daya yang tepat untuk meningkatkan kemampuan keamanan siber mereka. Prioritas ini harus didasarkan pada hasil evaluasi risiko keamanan siber dan rekomendasi yang diberikan oleh CSF v2.
3. **Implementasi**: Organisasi harus mengimplementasikan rencana aksi yang telah dibuat untuk meningkatkan kemampuan keamanan siber mereka. Implementasi harus meliputi pengembangan dan penerapan kebijakan dan prosedur keamanan, pemilihan dan penerapan teknologi keamanan, dan pelatihan dan kesadaran keamanan untuk karyawan.

4. **Pemantauan dan Evaluasi**: Organisasi harus memantau dan mengevaluasi efektivitas upaya keamanan siber mereka secara teratur. Hal ini dapat membantu organisasi dalam mengidentifikasi kelemahan dan kebutuhan tambahan serta memastikan bahwa rencana aksi yang telah dibuat tetap relevan dan efektif.

Untuk membantu organisasi dalam mengadopsi CSF v2, NIST menyediakan berbagai sumber daya dan alat bantu, termasuk panduan, model, dan kerangka kerja yang dapat diunduh secara gratis dari situs web mereka. Selain itu, organisasi juga dapat mengambil keuntungan dari layanan konsultan dan vendor yang menawarkan dukungan dan layanan terkait keamanan siber. Dengan mengadopsi CSF v2 dan menerapkan pendekatan yang terpadu dan holistik dalam membangun kemampuan keamanan siber mereka, organisasi dapat mengurangi risiko keamanan siber dan meningkatkan efisiensi dan efektivitas upaya mereka dalam melindungi aset penting dan menjaga kepercayaan pelanggan. CSF v2 (*Cybersecurity Framework Version 2*) adalah pengembangan dari versi sebelumnya, CSF v1.1. Beberapa perbedaan utama antara kedua versi ini adalah sebagai berikut:

1. Penekanan pada kolaborasi dan integrasi: CSF v2 menekankan pentingnya kolaborasi dan integrasi antara fungsi-fungsi keamanan siber yang berbeda. Ini termasuk integrasi antara keamanan siber dan manajemen risiko, serta integrasi antara keamanan siber dan keamanan fisik. Dengan cara ini, CSF v2 membantu organisasi untuk mengadopsi pendekatan yang terpadu dan holistik dalam membangun kemampuan keamanan siber mereka.
2. Adanya Implementation Tiers: CSF v2 menyertakan Implementation Tiers yang memungkinkan organisasi untuk mengevaluasi dan meningkatkan kesiapan keamanan siber mereka. Implementation Tiers terdiri dari empat tingkat, yaitu Partial, Risk-Informed, Repeatable, dan Adaptive. Setiap tingkat menunjukkan tingkat matangnya kemampuan keamanan siber organisasi dan memberikan panduan tentang tindakan yang harus diambil untuk meningkatkan kesiapan keamanan siber mereka.
3. Adanya Profiles: CSF v2 juga memperkenalkan Profiles yang dirancang untuk memenuhi kebutuhan keamanan siber organisasi tertentu. Profiles dibuat berdasarkan pada kriteria-kriteria tertentu, seperti tingkat risiko dan ketersediaan sumber daya. Dengan Profiles, organisasi dapat membuat rekomendasi khusus yang sesuai dengan kebutuhan mereka.
4. Penambahan isi: CSF v2 memperluas isi CSF v1.1 dengan memperkenalkan beberapa fitur baru, seperti panduan tentang identifikasi risiko siber, praktik-praktik terbaik untuk keamanan siber di lingkungan cloud, dan saran untuk implementasi keamanan siber pada perangkat Internet of Things (IoT).

Kesimpulannya, CSF v2 adalah pengembangan dari versi sebelumnya, CSF v1.1, yang menekankan pentingnya kolaborasi dan integrasi, menyertakan Implementation Tiers dan Profiles, serta memperluas isi CSF v1.1 dengan fitur-fitur baru. Dengan CSF v2, organisasi dapat mengadopsi pendekatan yang terpadu dan holistik dalam membangun kemampuan keamanan siber mereka dan mengevaluasi kesiapan keamanan siber mereka secara efektif.