Pertemuan 4

Keamanan Informasi dan Internet

Information Security and Internet

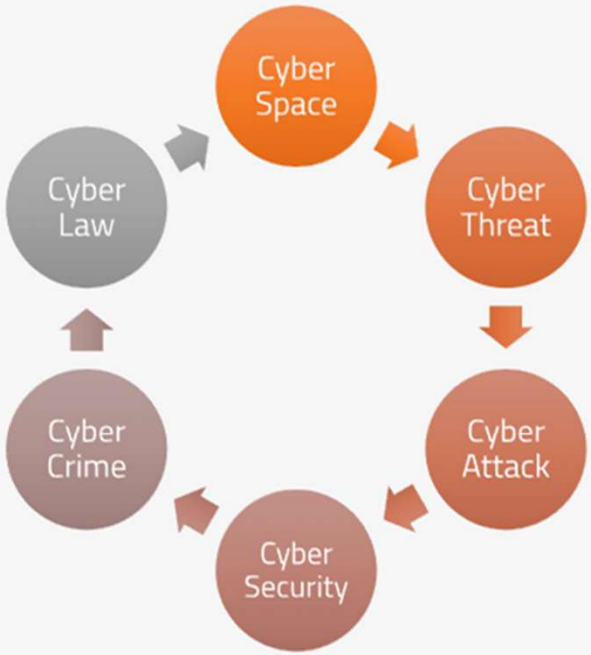
- Tim Pengawas Keamanan Internet
- Menyusun Kebijakan dan Prosedur Keamanan

Tim Pengawas Keamanan Internet

Bagaimana cara mengamankan Informasi dan Keamanan Internet?

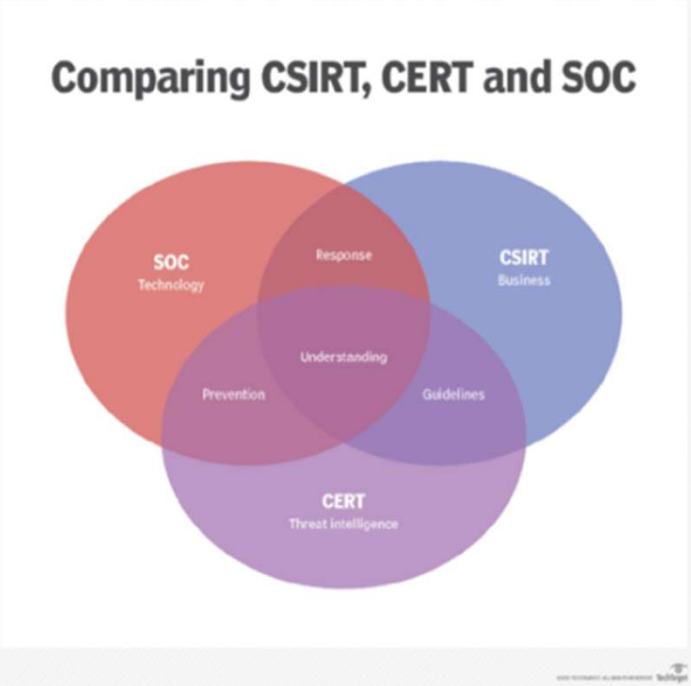
Membentuk Tim Respon Siber

CSIRT/CERT



CSIRT/CERT

- CERT (Tim Tanggap Darurat Komputer)
- Istilah CERT awalnya diterapkan pada tim pemadam kebakaran di Amerika Serikat karena kesamaan tugas dan tanggung jawab mereka.
- CSIRT (Tim Respons Insiden Keamanan Komputer)
- Universitas Carnegie Mellon, yang pertama memperkenalkan konsep CERT/CC



CSIRT - computer security incident response team

CERT - computer emergency response (or readiness) team

Pendirian CSIRT di Indonesia

- Bermula dari kasus pemilu tahun 2004
- Inisiatif komunitas Keamanan Internet dan Informasi: APJII, Mastel, AWARI dan Pemerintah: Polri dan Kominfo
- Menteri Komunikasi dan Informatika Nomor : 26/PER/M.KOMINFO/5/2007

ID-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure) + Lemsaneg

BSSN (Badan Siber dan Sandi Negara) 2017

Tugas ID-SIRTII

- Sosialisasi keamanan pemanfaatan Jaringan Telekomunikasi Internet
- Pemantauan, deteksi dini dan peringatan dini ancaman dan gangguan internet
- Membangun dan/atau menyediakan, mengoperasikan, memelihara dan mengembangkan sistem pemantauan basis data.

Task ID-SIRTII

- Melaksanakan fungsi layanan informasi terhadap ancaman dan gangguan keamanan internet
- Menyediakan laboratorium simulasi dan pelatihan kegiatan keamanan internet
- Melakukan layanan konsultasi dan bantuan teknis
- Menjadi contact point dengan institusi terkait baik dalam negeri maupun luar negeri.

4 Jenis CERT

4 Jenis CERT

- Sector CERT
- Internal CERT
- Vendor CERT
- Commercial CERT

Sector CERT

- Institusi yang didirikan untuk mengelola keamanan komputer/internet untuk lingkungan tertentu
- seperti militer, rumah sakit, universitas dll.

Internal CERT

- Suatu lembaga yang dibentuk oleh suatu perusahaan yang mempunyai cakupan geografis di seluruh nusantara
- seperti : pertamina, Bank Nasional, PLN, TELKOM dll.

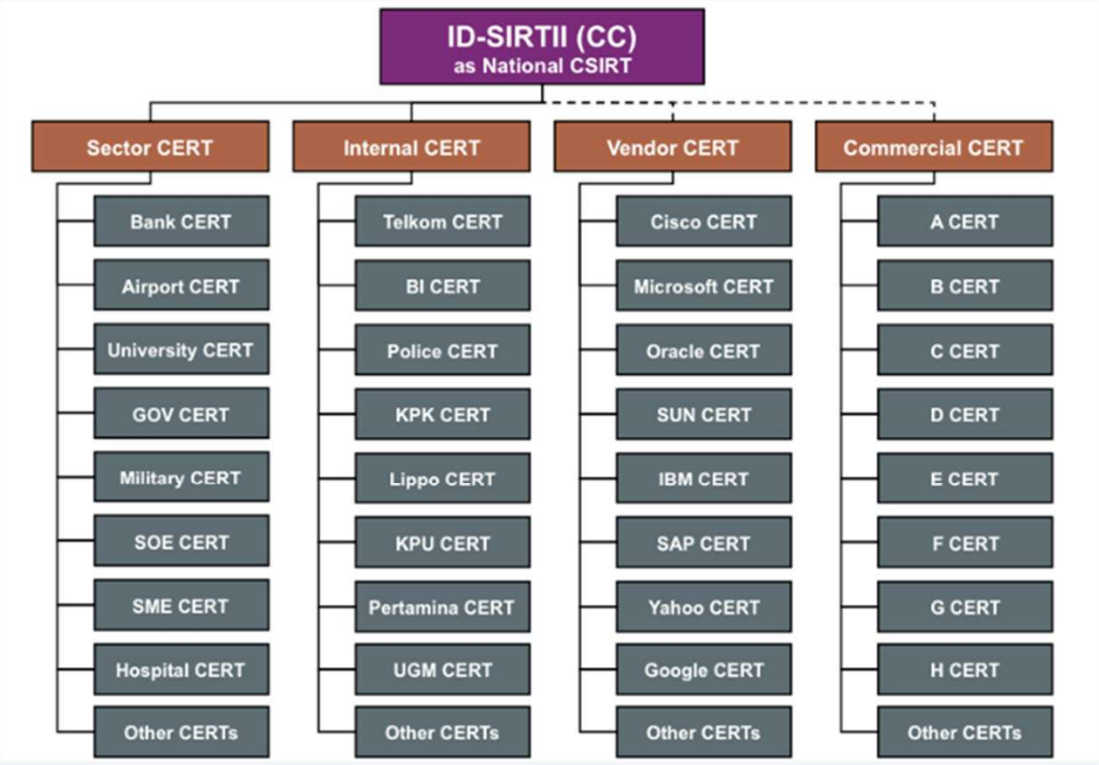
Vendor CERT

- Lembaga manajemen keamanan yang dimiliki oleh vendor teknologi untuk melindungi kepentingan pengguna teknologi terkait,
- seperti: Google, Cisco, Microsoft, Oracle, IBM dll.

Commercial CERT

- Lembaga yang biasanya dibentuk oleh sejumlah praktisi dan pakar keamanan komputer/internet yang menawarkan berbagai produk/jasa kepada pihak lain terkait dengan tawaran membantu proses keamanan TI secara komersial.

Hubugan antara ID-SIRTII dan CERT

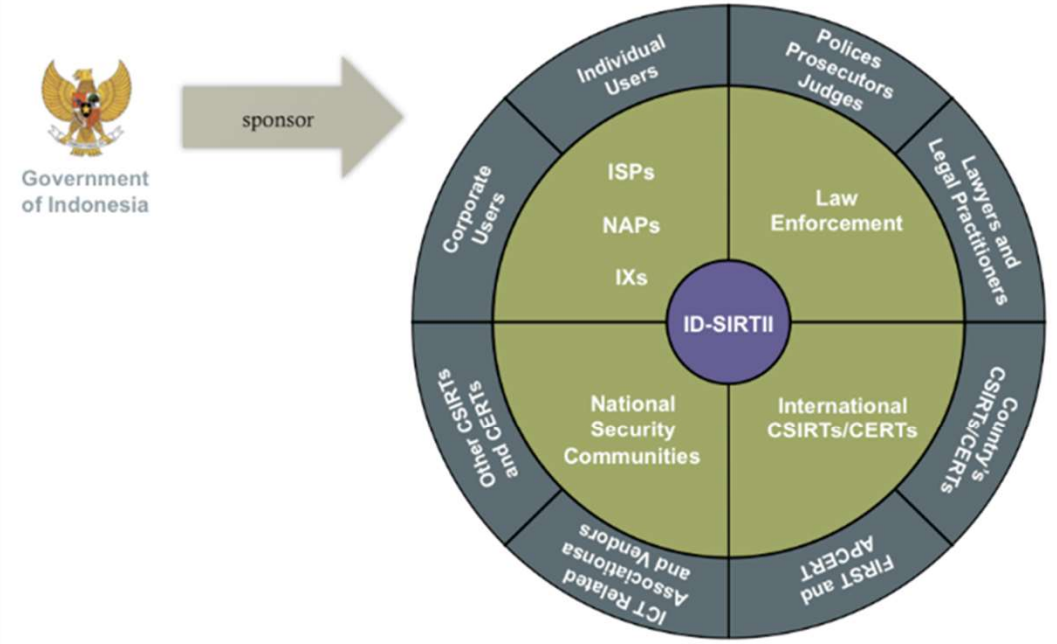


Klasifikasi ruang lingkup keamanan Internet

INCIDENT HANDLING DOMAIN and ID-SIRTII MAIN TASKS	Reactive Services	Proactive Services	Security Quality Management Services
1. Monitoring traffic	Alerts and Warnings	Announcements Technology Watch Intrusion Detection Services	x
2. Managing log files	Artifact Handling	x	x
3. Educating public	x	x	Awareness Building
4. Assisting institutions	Security-Related Information Dissemnination Vulnerability Handling Intrusion Detection Services	Security Audit and Assessment Configuration and Maintenenace of Security Tools, Applications, and Infrastructure	Security Consulting
5. Provide training	x	X	Education Training
6. Running laboratory	x	x	Risk Analysis BCP and DRP
7. Establish collaborations	Incident Handling	x	Product Evaluation

ID-SIRTII Constituents

- Konstituen Internal
  - Penyedia layanan internet
  - Poin Pertukaran Internet
  - Titik Akses Jaringan
  - Penegakan hukum
  - CSIRT/CERT Internasional
  - Komunitas Keamanan Nasional
- Konstituen Eksternal
  - Pengguna Korporasi
  - Pengguna Perorangan
  - Hakim Jaksa Polisi
  - CERT/CSIRT Negara
  - APCERT
  - Terkait dan Vendor ICT



Incident Handling Priority Level

TYPE OF INCIDENT AND ITS PRIORITY	Public Safety and National Defense (Very Priority)	Economic Welfare (High Priority)	Political Matters (Medium Priority)	Social and Culture Threats (Low Priority)
1. Interception	Many to One	One to Many	Many to Many	Automated Tool (KM-Based Website)
2. Interruption	Many to One	One to Many	Many to Many	Automated Tool (KM-Based Website)
3. Modification	Many to One	One to Many	Many to Many	Automated Tool (KM-Based Website)
4. Fabrication	Many to One	One to Many	Many to Many	Automated Tool (KM-Based Website)

Menyusun Kebijakan dan Prosedur Keamanan

ISO/IEC 27001 dan ISO/IEC 27002: Meskipun ISO/IEC 27001 lebih berfokus pada Sistem Manajemen Keamanan Informasi (ISMS), ISO/IEC 27002 memberikan panduan rinci tentang kontrol teknis dan tindakan keamanan yang dapat diimplementasikan dalam organisasi.

NIST SP 800-53: Standar Pengamanan Data Federal (NIST) SP 800-53 memberikan panduan yang komprehensif untuk mengelola risiko keamanan informasi dalam lingkup pemerintah federal AS. Ini mencakup kontrol dan tindakan keamanan yang dapat diadopsi oleh berbagai organisasi.

Center for Internet Security (CIS) Controls: Ini adalah seperangkat kontrol keamanan informasi yang disusun oleh Center for Internet Security. CIS Controls memberikan daftar langkah-langkah praktis untuk meningkatkan keamanan informasi secara keseluruhan.

Menyusun Kebijakan dan Prosedur Keamanan

ISF Standard of Good Practice for Information Security: Diterbitkan oleh Information Security Forum (ISF), standar ini memberikan panduan praktis dan rekomendasi untuk mengelola risiko keamanan informasi.

HIPAA Security Rule: Merupakan standar yang mengatur keamanan informasi kesehatan di Amerika Serikat. Meskipun khusus untuk industri kesehatan, beberapa prinsip keamanan dapat diterapkan di berbagai sektor.

PCI DSS (Payment Card Industry Data Security Standard): Standar ini mengatur keamanan informasi terkait dengan pengolahan data kartu pembayaran. Meskipun fokus pada industri pembayaran, beberapa prinsip keamanan dapat diterapkan secara umum.

ISO/IEC 27001 dan ISO/IEC 27002

	From ISO/IEC 27002:2013	To ISO/IEC 27002:2022
Number	**Security control clause**	**Security control clause**
5	Information security policies	Organizational controls (37)
6	Organization of information security	People controls (8)
7	Human resource security	Physical controls (14)
8	Asset management	Technological controls (34)
9	Access control	
10	Cryptography	
11	Physical and environmental security	
12	Operations security	
13	Communications security	
14	System acquisition, development and maintenance	
15	Supplier relationships	
16	Information security incident management	
17	Information security aspects of BCM	
18	Compliance	

NIST SP 800-53 control families

TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Reference

- Certified Ethical Hacker CEH v9 - v10
- https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf
- Pandi

THANK YOU

Assignment

- Cari dan Pilih CSIRT/CERT dari berbagai negara, Pilih 1 (selain Indonesia)
  - Mengetahui latar belakang berdirinya CSIRT/CERT
  - Jelaskan tugas dan tanggung jawab CSIRT/CERT
  - Lacak Insiden yang ditangani oleh CSIRT/CERT

- Carikanlah Perusahaan dan Negara yang menggunakan standar keamanan berikut ini, kemudian jelaskan implementasi yang mereka lakukan terhadap standar tersebut
  - ISO/IEC 27001 dan ISO/IEC 27002 untuk perusahaan
  - NIST SP 800-53 untuk negara