

RENCANA KERJA 2016

*PERTEMUAN TAHUNAN VIII
ID-CERT 2016*

GMP TELKOM
BANDUNG, 03/03/2016

ID-CERT

Event Report Tools

- Mengolah data *log* yang dikirim melalui tiket penanganan insiden ID-CERT.
- Dibuat laporan kostumasi untuk setiap Anggota Korporat
- Durasi: sesuai permintaan
- *SEGERA HADIR*

Survey Malware

- Mengetahui tren top 10 malware di Indonesia
- Perbaiki Parser
- Akan kembali aktif pada bulan Maret 2016.

Keyserver PGP Indonesia

- Berinisiatif membuat Keyserver Mirror untuk PGP di Indonesia
- Sedang dalam masa ujicoba:
<http://keyserver.cert.or.id/>

Malware Scanner Indonesia

- Tengah dalam pembuatan Malware Scanner untuk aplikasi berbasis Windows, Linux hingga Android
- Akan melibatkan lebih banyak vendor AV lokal

Rencana Pelatihan

- Latar belakang:
 - Munculnya banyak pertanyaan seputar hal-hal mendasar terkait PGP Key
 - Perlu lebih banyak sosialisasi terkait masalah IT Security
- Target:
 - Engineer
 - High Level
 - Sektor: ISP, Instansi Pemerintahan, Pendidikan, Penmegak Hukum dan Finansial
- Kapasitas dan biaya:
 - 20 peserta per pelatihan
 - Peserta tidak dikenakan biaya
- Kendala:
 - Tidak pernah dianggarkan dalam kegiatan ID-CERT
 - Perlu dukungan sponsor terhadap aktifitas ini

Rencana Pelatihan dan Pertemuan

- ID-CERT Gathering IX: PENS Surabaya (SEPTEMBER 2016)
 - Pertemuan sosialisasi ID-CERT membahas:
 - Perkembangan terbaru seputar IT Security di Indonesia
 - Aktivitas Rutin ID-CERT
 - Temu Komunitas

Rencana Pelatihan dan Pertemuan

- Pertemuan sosialisasi ID-CERT bersama LiteBig di Bandar Lampung (dalam konfirmasi)
- membahas:
 - Perkembangan terbaru seputar IT Security di Indonesia
 - Aktifitas Rutin ID-CERT
 - Temu Komunitas

Pelatihan yang sudah berjalan

- Dengan JCLEC di Semarang sebanyak 5 kali pada tahun 2015.
- Akan meminta dukungan dari berbagai pihak ditahun 2016.

Pelatihan Dasar (1 Hari)

- Pengenalan Information Security, Tren IT Security 2015/2016 per Sektor
 - Security Audit Methodology
 - Pengenalan ID-CERT
 - Incident Monitoring Report
 - Secure Email
- Topik Pembicara lainnya Per Sektor: GovCSIRT, AcadCSIRT, dsb
- Tanggal Tentative:
 - 23 Juni 2016: sektor ISP
 - 18 Agustus 2016: Sektor penegak hukum
 - 9 September 2016: Sektor Pemerintahan

Pelatihan Lanjutan (2 Hari)

- Pengenalan Information Security, Tren IT Security 2016 per Sektor
 - 10 Domains of Security
 - Security Audit Methodology
 - Pengenalan ID-CERT
 - Incident Monitoring Report
 - Secure Email
 - Penetration Testing
 - Teknologi Pengamanan
 - Diskusi
- Tanggal Tentative:
 - 19-20 Mei, sektor Pemerintahan
 - 13-14 Okt, sektor ISP
 - 17-18 Nov, sektor Penegak Hukum
 - 8-9 Des, sektor Finansial

PERTANYAAN, SARAN & MASUKAN?

Kontak Desk **ID-CERT:**

www.cert.or.id

Telpon: (+62)889-1400-700

cert@cert.or.id

Ahmad Alkazimy (Manajer **ID-CERT**)

ahmad@cert.or.id

Rahmadian L. Arbianita (Helpdesk **ID-CERT**)

rahmadian@cert.or.id

Mailing List:

diskusi@MILIS.cert.or.id

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM

id.cert

*DISKUSI: Tantangan, Kendala CSIRT di
Indonesia (Curhat CSIRT)*

*PERTEMUAN TAHUNAN VIII
ID-CERT 2016*

GMP TELKOM
BANDUNG, 03/03/2016

ID-CERT

CERT/CSIRT DI INDONESIA

- ID-CERT (1998), sektor umum dan berbasis aduan;
www.cert.or.id
- ID-SIRTII (2007), berbasis monitoring log dan memberikan bukti Digital bila diminta penegak hukum;
www.idsirtii.or.id
- Acad-CSIRT (2010), sektor Akademik, berbasis aduan;
<http://www.acad-csirt.or.id/>
- GovCSIRT / KAMINFO (2012), sektor Pemerintahan, berbasis aduan dan Monitoring log.
<http://govcsirt.kominfo.go.id/>
- BPPT CERT (2014): <http://www.csirt.bppt.go.id/>
- Jogja-PGCSIRT (SEP 2015), SubSektor Pemerintahan provinsi DIY, berbasis aduan dan monitoring
- JabarProvCSIRT (DES 2015), SubSektor Pemerintahan provinsi Jawa Barat.

Siapa kontak CSIRT tsb?

- Sesi Perkenalan diri dan Tim CSIRT:
 - Sebutkan nama dan Jabatan?
 - Sebutkan nama Tim?
 - Jumlah personel?
 - Sebutkan Tupoksi/RFC2350
 - Jenis CSIRT: Independen, non-profit, “Plat Merah”, “Plat Kuning”?
 - Sektor CSIRT: Sektoral, Sub-Sektoral, Wilayah Geografis?
 - Biaya Operasional CSIRT: Sponsor, Mitra, Pemerintah atau gabungan?

CSIRT di Indonesia

- Akan bertambah?
- Tupoksi/Cakupan Kerja (RFC2350)?
- Konstituen?

Apa saja Kendala, Tantangan yang dihadapi?

- Beberapa kendala yang umum dihadapi:
 - Kesulitan penanganan insiden
 - Kesulitan menghubungi pihak terkait
 - Kurang SDM?
 - Skill SDM yang kurang?
 - Pendanaan?
 - Kesulitan berkoordinasi dengan pihak Luar/dalam Negeri?

Sesi Diskusi

- [Masing-masing CSIRT mengutarakan pandangan, keluhan kesah, curhat, seputar operasional CSIRT]
- Solusi/bantuan seperti apa yang diharapkan?
- Apakah ada CSIRT lain yang bersedia membantu?

15 Tim CERT/CSIRT di Indonesia yang terdata

Melalui pertemuan ini

A. CSIRT Publik Terbuka:

1. ID-CERT
2. ID-SIRTII

B. CSIRT Publik Terbatas berbasis wilayah/Sektor:

3. Jabar-CSIRT
4. JabarAcad-CSIRT
5. JabarProv-CSIRT
6. Jatim-CSIRT
7. AcadCSIRT
8. ID.GovCSIRT

C. CSIRT Internal

9. BPPT-CSIRT
10. CSOC-Telkom
11. Tim IT Security Bank Mandiri
12. XL-CSIRT

D. Tim yang memiliki fungsi sejenis CSIRT

13. Sektor Pertahanan Negara
14. PUSTEKKOM KEMDIKBUD
15. Direktorat Pengamanan Perdagangan - KEMDAG