

C DEF | Bulletin

Jakarta, 28 November 2017

Tujuan

- ▶ Mencerdaskan kehidupan bangsa - sesuai pembukaan UUD 1945
- ▶ Regenerasi
- ▶ Amalan yang tidak pernah terputus



CDEF Bulletin Contents

- Pengenalan sejarah& Tokoh di bidang keamanan siber
- Sharing experience

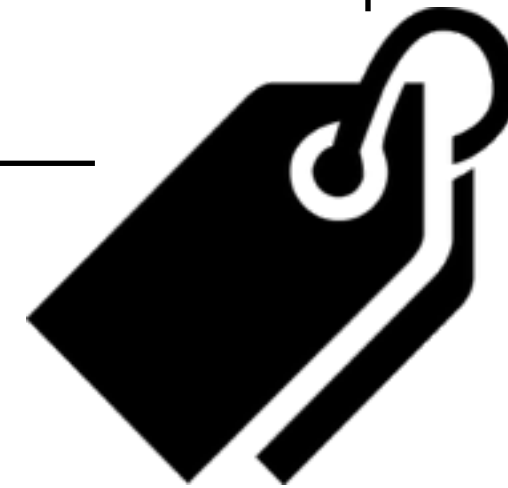


Figures

- Tips & Trick to hardening the network, forensic, malware analysis, dll
- Playbook



- Latest Issues
- IOC Shares



Category



- Tutorial
- Challenges

• **Monthly ?? Quarterly ?**

• **Contributors ??**

• **Board Reviewer ??**

Our Github

<https://github.com/cdefcomm>

Secure <https://github.com/cdefcomm/cdef-edr/wiki/Log-Data-&-Log-Management>

Log Data & Log Management

jonitampn edited this page on Sep 26 · 1 revision

Apa itu Log Data?

Log data is the intrinsic meaning that a log message has. Or put another way, log data is the information pulled out of a log message to tell you why the log message generated.

Sebuah contoh, pada sebuah web server yang dikunjungi oleh user, user akan otomatis mengakses resources didalamnya (web pages, gambar, file, dll.). Jika user mengakses halaman tersebut, web server akan menulis log kedalam sistem nya. Salah satunya source IP Address dari user yang telah mengunjungi halaman tersebut.

Idealnya, untuk sebuah log data harus bisa kurang lebih menjelaskan 5W1H. Namun untuk detail (how,why) sangat jarang ditulis dan dimasukkan kedalam log. Hal ini mungkin akan kita temui untuk jenis log Debug. Atau yang jenis log yang lain dengan level verbose yang tinggi itu akan memberikan banyak informasi.

Untuk isi dasar log itu sendiri biasanya mengandung :

- Waktu.
- Sumber.
- Data.

Penggunaan Log


Secure <https://github.com/cdefcomm/meetup/wiki/1st-Meetup-%7C-20-Oktober-2017>

1st Meetup | 20 Oktober 2017

C|DEF {Cyber Defense} Community edited this page on Oct 24 · 9 revisions

1st Meetup - 20 Oktober 2017

Pada meetup yang pertama ini, kegiatan diselenggarakan di salah kantor penyedia jasa e-commerce terbesar di Indonesia, yakni BliBli.com, Grha Niaga Thamrin, Jakarta Pusat pada tanggal 22 Oktober 2017. Di luar dugaan ternyata kegiatan yang diselenggarakan komunitas C|DEF ini mendapat sambutan positif dari kalangan kegiatan keamanan siber di Indonesia. Hal ini tercermin dari cukup banyaknya peserta kegiatan yang hadir pada meetup kali ini, latar belakang peserta kegiatan berasal dari berbagai latar belakang dan berbagai institusi baik sektor private, pemerintahan ataupun individual researcher.



▼ Pages 2

[Home](#)

[1st Meetup | 20 Oktober 2017](#)

+ Add a custom sidebar

Clone this wiki locally

<https://github.com/cdefcomm>

Clone in Desktop

Ada idekah ??