



FastResponder: New Open Source weapon to detect and understand a large scale compromise

“About us”

French Company in Cyber Security

Cert Sekoia

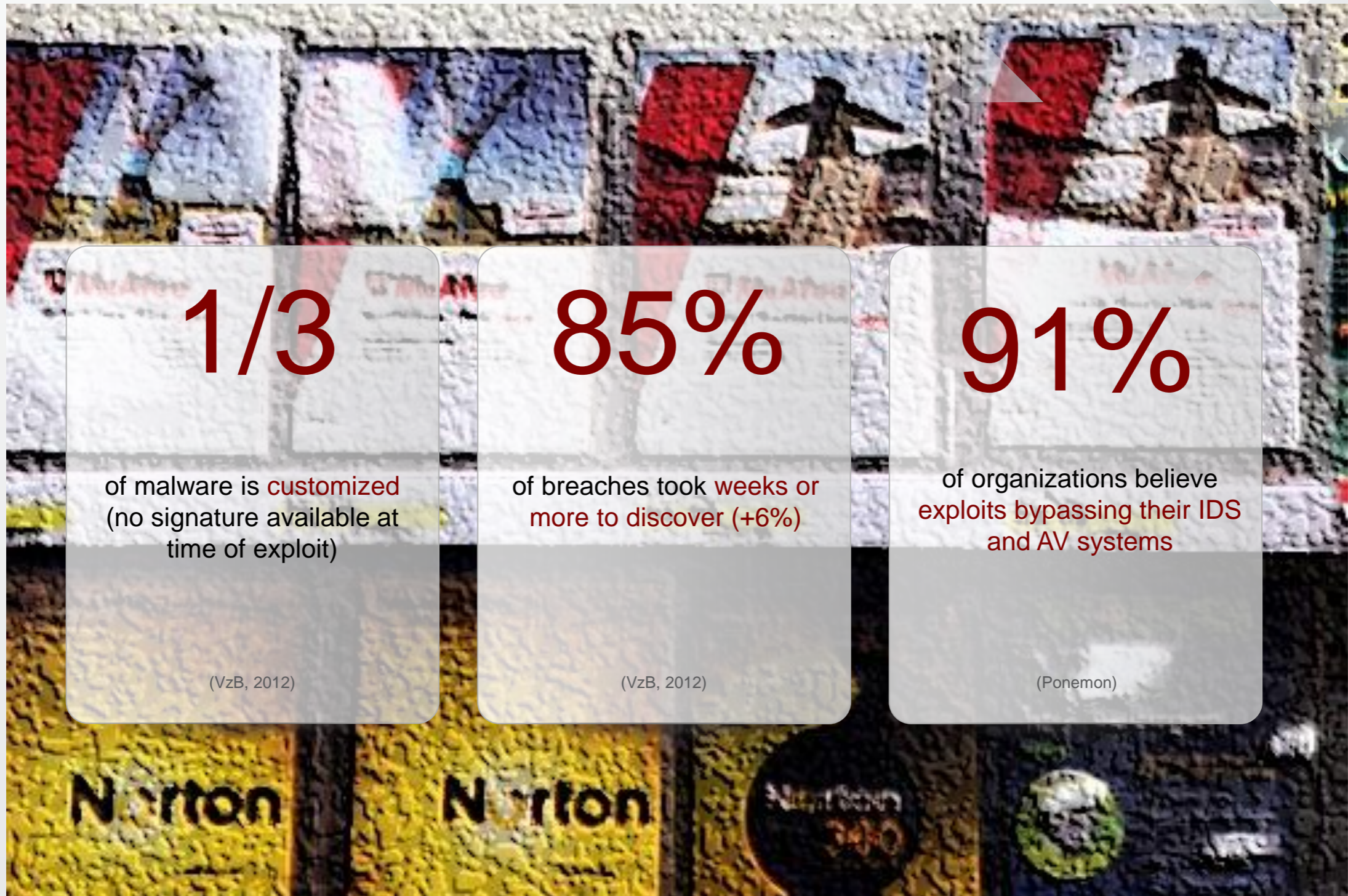
Detection Intrusion experts

Digital Forensics and Incidence Response

Co-Organizer of #BotConf

Members of Honeynet Project

“Symantec Executive Says Antivirus is Dead”



Wall Street Journal 2014, May 4th - Brian Dye, senior vice-president Symantec



Our 3 objectives

Fast Data Acquisition for Detection of compromissions

Fast Analysis of an attack

Fast Incident Response to mitigate the impact

Common denominator after an attack ?

CSI: NY

Traditional
Forensic
investigation



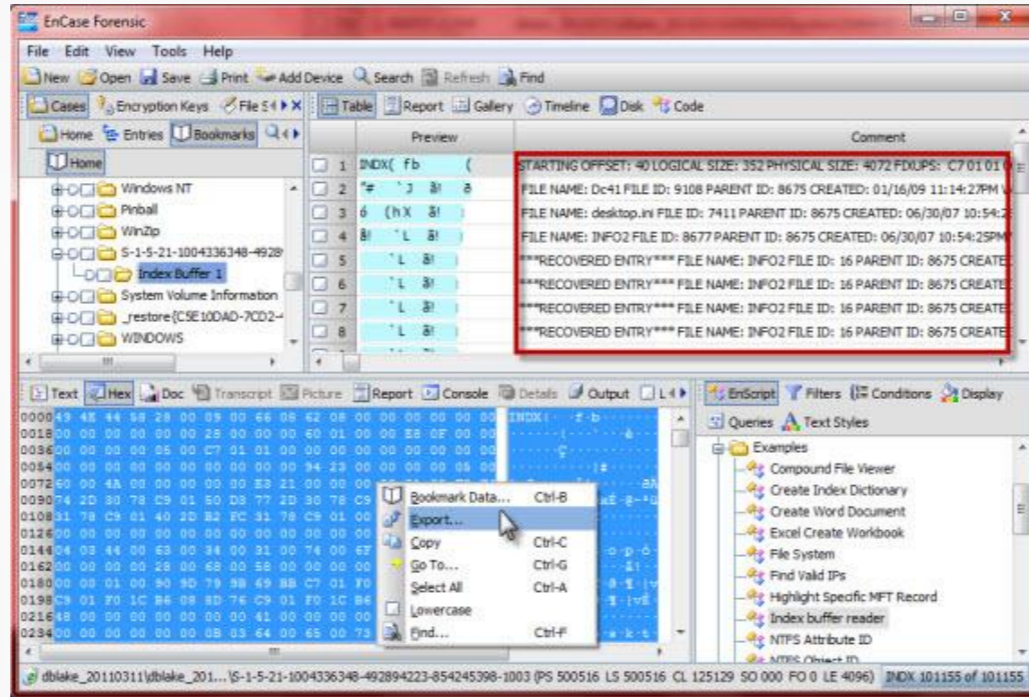
Nicholas...

Common denominator of traditional forensic?

Slow
Painful
Expensive
Business
independent



Old fashioned holistic approach tools



Software for data acquisition



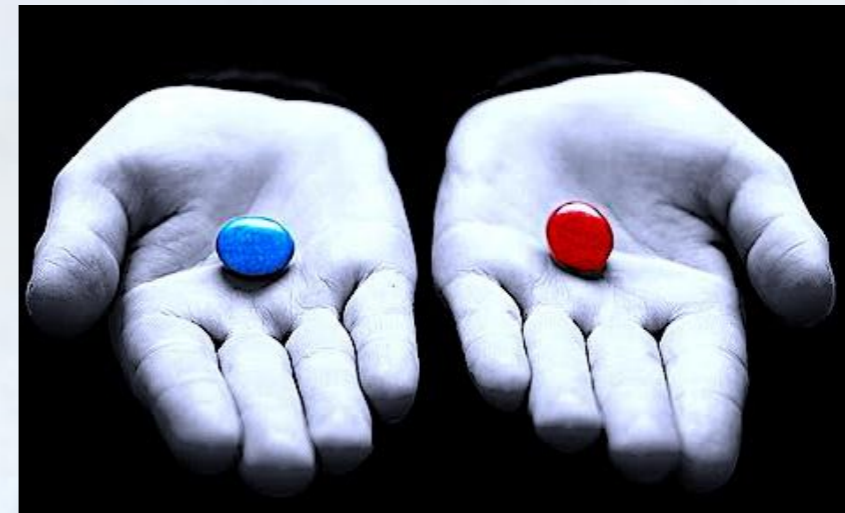
Hardware for data acquisition

1	date	time	MACB	source	Description
2948	2/1/2012	3:00:02	ACB	WEBHIST	URL:http://www.staples.com/sbd/img/bg/bg_flyoutcloser.gif cache stored in: 3ASVQIE8/bg_flyoutcloser[1].gif - HTTP/1.1 200 OK - ETag: "a3db0-19f-49b2c2
2949	2/1/2012	3:00:02	ACB	WEBHIST	URL:http://www.staples.com/sbd/img/bg/bg_car-arrows[1].gif - HTTP/1.1 200 OK - ETag: "48cf3-956-49b2c27d5
2950	2/1/2012	3:00:02	ACB	WEBHIST	URL:http://www.staples.com/sbd/reviews/engine/images/stars_small.gif cache stored in: PY8WR6ZU/stars_small[1].gif - HTTP/1.1 200 OK - ETag: "b5cb-9f
3221	2/1/2012	3:00:19	ACB	WEBHIST	URL:http://www.staples.com/sbd/img/bg/bg_d01_hover.gif cache stored in: 3ASVQIE8/bg_d01_hover[1].gif - HTTP/1.1 200 OK - ETag: "48cfa-147-49b2c27d5
3284	2/1/2012	3:07:24	MACB	WEBHIST	URL:http://www.staples.com/office/supplies/StaplesSearch?catalogId=10051&langId=-1&storeId=10001&searchComparisonSkus=8&sortBy=Value%20price%20asc
3285	2/1/2012	3:07:25	MACB	WEBHIST	URL:http://www.staples.com/office/supplies/StaplesSearch?searchkey=envelope¤tUrl=http%3A%2Fwww.staples.com%2Fink-Toner-Finder%2Ffc
3286	2/1/2012	3:08:00	MACB	OXML	- Application: Microsoft Office Word - Company: Microsoft - AppVersion: 12.0000 - Invoice-#233-Staples-Office-Supplies.docx
3299	2/1/2012	3:08:40	CB	LNK	C:/Drivers/video/Invoice-#233-Staples-Office-Supplies.docx - C:/vsc12/Users/harrell/AppData/Roaming/Microsoft/Office/Recent/Invoice-#233-Staples-Offi
3300	2/1/2012	3:08:40	M...	LNK	C:/Drivers/video<-C:/vsc12/Users/harrell/AppData/Roaming/Microsoft/Windows/Recent/video.Ink- which is stored on a local vol type - Fixed- SN 0x4ce702
3301	2/1/2012	3:08:40	A...	LNK	C:/Drivers/video<-C:/vsc12/Users/harrell/AppData/Roaming/Microsoft/Windows/Recent/video.Ink- which is stored on a local vol type - Fixed- SN 0x4ce702
3302	2/1/2012	3:08:40	...	MACTIME	C:/Drivers/video/Invoice-#233-Staples-Office-Supplies.docx
3303	2/1/2012	3:08:41	A...	Jump Lists	C:/Drivers/video/Invoice-#233-Staples-Office-Supplies.docx
3304	2/1/2012	3:08:41	MACB	WEBHIST	URL:file:///C:/Drivers/video/Invoice-
3305	2/1/2012	3:08:41	M...	LNK	C:/Drivers/video/Invoice-#233-Staples-Office-Supplies.docx - C:/vsc12/Users/harrell/AppData/Roaming/Microsoft/Office/Recent/Invoice-#233-Staples-Offi
3306	2/1/2012	3:08:41	A...	LNK	C:/Drivers/video/Invoice-#233-Staples-Office-Supplies.docx - C:/vsc12/Users/harrell/AppData/Roaming/Microsoft/Office/Recent/Invoice-#233-Staples-Offi
3309	2/1/2012	3:08:41	MAC	MACTIME	C:/Drivers/video/Invoice-#233-Staples-Office-Supplies.docx
3310	2/1/2012	3:08:41	...	MACTIME	C:/Users/harrell/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012012013120120201
3311	2/1/2012	3:08:41	...	MACTIME	C:/Users/harrell/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012012013120120201/index.dat
3312	2/1/2012	3:08:41	MAC	MACTIME	C:/Users/harrell/AppData/Roaming/Microsoft/Office/Recent
3313	2/1/2012	3:08:41	M.C.	MACTIME	C:/Users/harrell/AppData/Roaming/Microsoft/Office/Recent/index.dat
3314	2/1/2012	3:08:41	MACB	MACTIME	C:/Users/harrell/AppData/Roaming/Microsoft/Office/Recent/Invoice-#233-Staples-Office-Supplies.docx.LNK
3315	2/1/2012	3:08:41	MACB	MACTIME	C:/Users/harrell/AppData/Roaming/Microsoft/Office/Recent/video.LNK
3316	2/1/2012	3:08:41	MAC	MACTIME	C:/Users/harrell/AppData/Roaming/Microsoft/Windows/Recent
3317	2/1/2012	3:08:41	M.C.	MACTIME	C:/Users/harrell/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/1b4dd6729cb1962a.automaticDestinations-ms
3318	2/1/2012	3:08:41	M.C.	MACTIME	C:/Users/harrell/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/adeafb853d77462a.automaticDestinations-ms
3319	2/1/2012	3:08:41	MACB	MACTIME	C:/Users/harrell/AppData/Roaming/Microsoft/Windows/Recent/Invoice-#233-Staples-Office-Supplies.docx.LNK
3320	2/1/2012	3:08:41	MACB	MACTIME	C:/Users/harrell/AppData/Roaming/Microsoft/Windows/Recent/video.LNK
3321	2/1/2012	3:08:41	MAC	MACTIME	C:/Users/harrell/AppData/Roaming/Microsoft/Word

Spreadsheet macro for data analysis

What is #FastForensic ?

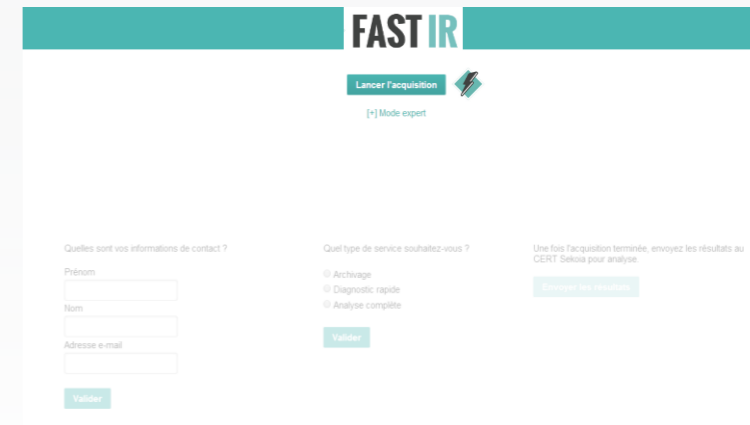
Easy to use
Focused
Fast
Context aware



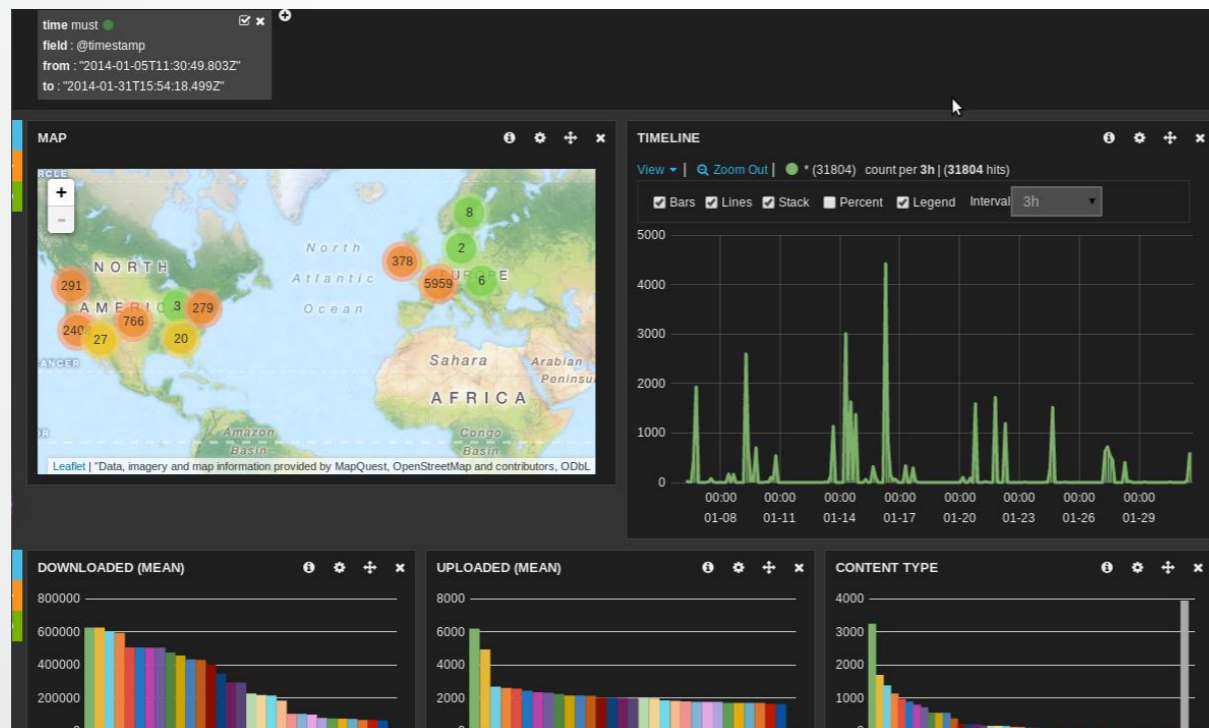
#FastForensic : a all new approach



Specialized hardware for data acquisition

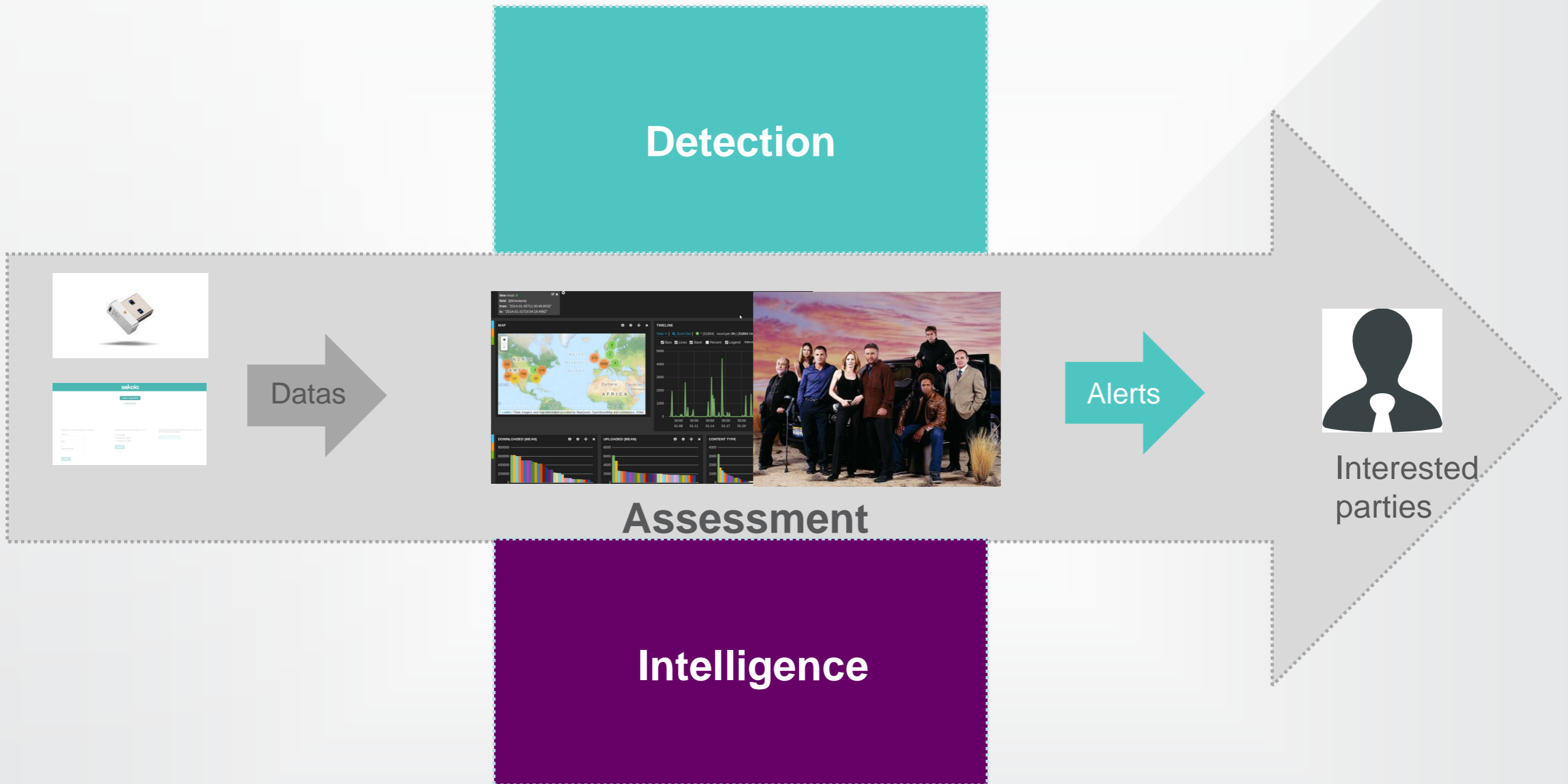


1 click software for data acquisition



« Big data » technologies for data analysis

Process



Detection

Datan

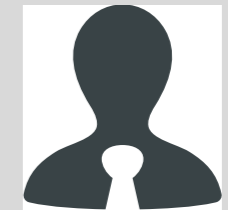
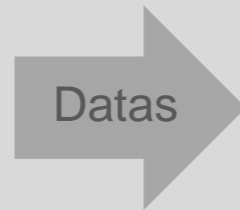
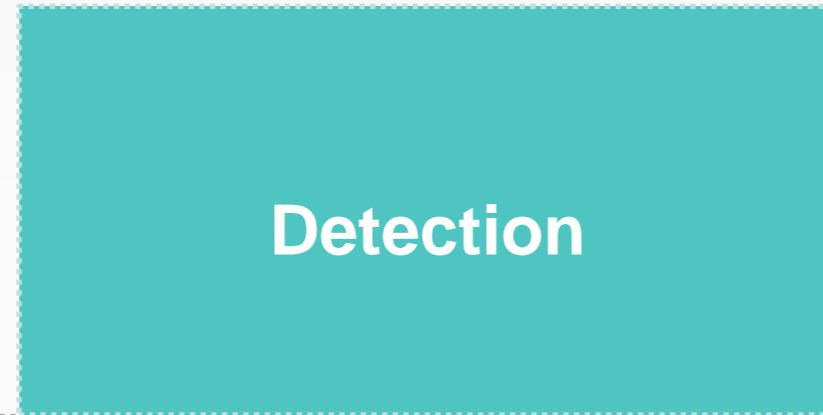
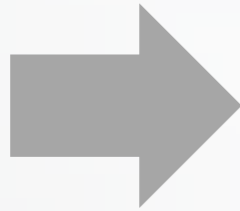
Assessment

Alerts

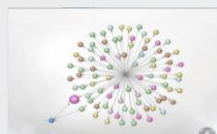
Interested parties

Intelligence

Process | A Lean Cybersecurity approach



Interested partie



Large company integrated model

Information sources

AV

IDS

AD

...

Logs collection / correlation

collection

correlation

SOC L1

Referentiels,
HR
CMDB
Interested parties

1. Event recording

2. Event assessment

3. Threat intelligence

4. Remediation

5. Feedback

6. workshop, reporting

SOC L2
CERT

Sec
community

Business
Lines

Large company integrated model

Information sources

AV IDS AD ...

Logs collections / correlation

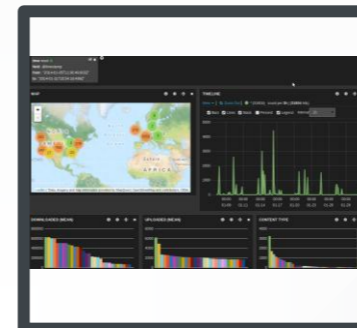
collection → correlation

SOC L1

Referentiels,
HR
CMDB
Interested Parties

1. Event recording
2. Event assessment
3. Threat intelligence
4. Remediation
5. feedback
6. workshop, reporting

Malware Intl



SOC L2
CERT

Security
community

Business
Lines

O Mail

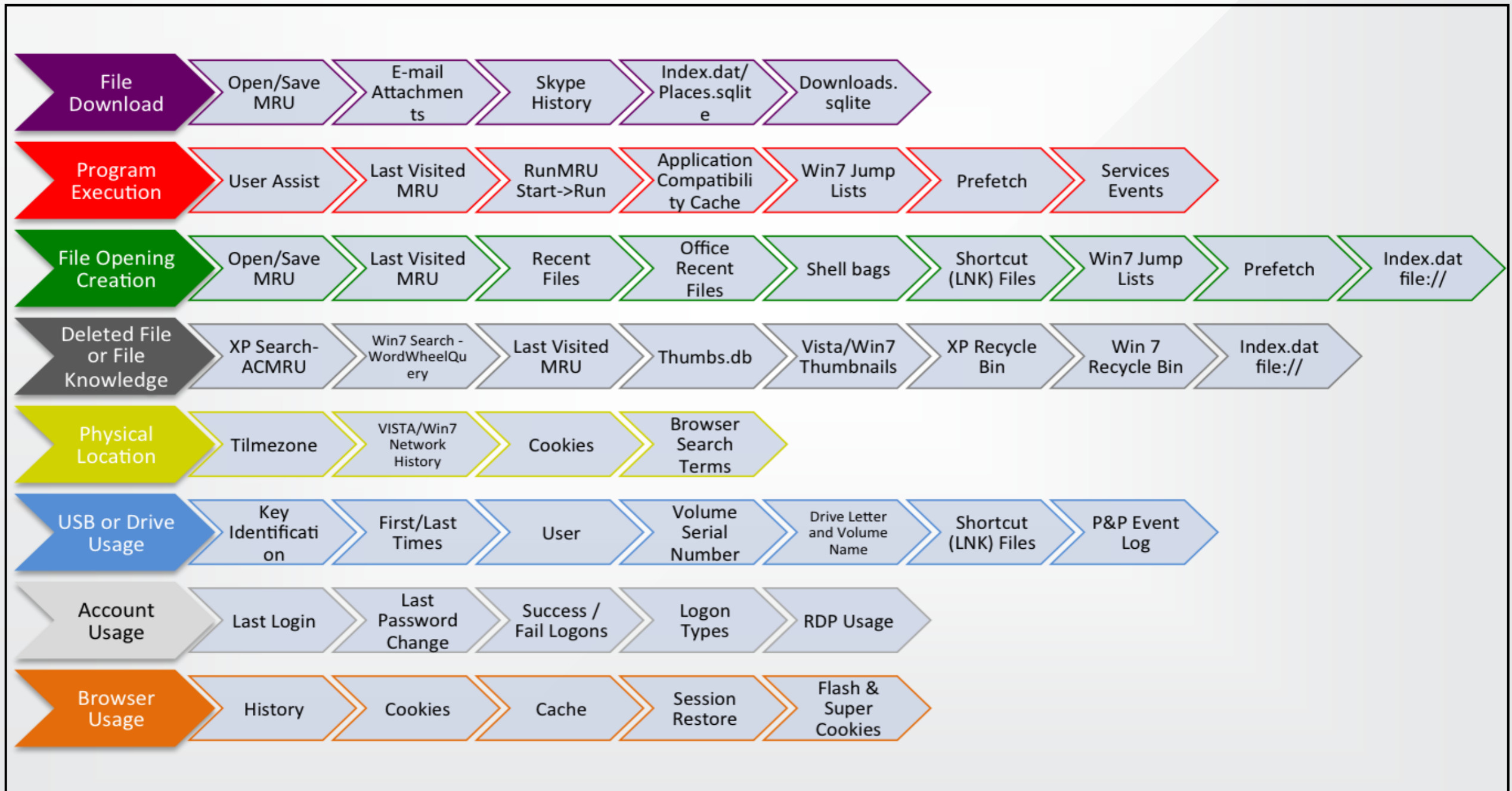


So we have develop FastResponder

```
u_int64_t u64;
/* file can be accessed using pread/pwrite */
int entry_size;
* Feb 24, 2000 Nenad Corbic Added support for socket based x25api
#define __SO_SIZE(c) ((c) & 0x3fff)
/* really a separate operation, and should be modified via sysctl
* at page-private, with BUILD_BUG_ON to make sure that this will not
struct videobuf_queue *q;
#define V4L2_STD_SECAM_L ((v4l2_std_id)0x00400000)
/* these are the normal masks */
int (*reset)(struct irda_task *task);
#define get_cpu() ((preempt_disable)
#ifndef IRDA_MIN /* Lets not mix this MIN with other header files */
#define FALSE management overhead than the whole mess
*/
struct timer_list pgdir_timer; do {
#define PUD_MASK u_int16_t u16;
* Author: Fred M. van Kempen (swa1@uut.nl)
int (*v4l2_copy_to_user)(struct videobuf_queue *q,
struct sk_buff *skb,
spinlock_t *spinlock;
/* part because of use for some possible hardware use when for hack around
int videobuf_streamoff(struct videobuf_queue *q,
transactions */
#define CONFIG_DEBUG_IRDA
unsigned long nrecvdata;
int (*copy_to_user)(struct videobuf_queue *q,
#define EBT_DESTMAC 0x4001
#define XT_CONTINUE 0xfffff
#define XT_RETURN (-NF_REPEAT - 1)
#define FMODE_NDELAY unsigned int nentries; mode_t mode;
int (*copy_to_user)(struct videobuf_queue *q,
size_t videobuf_read;
/* Hack to do small buffers when setting media bus in IrLAP */
/* modify it under the terms of the GNU General Public License
* If it's used for something else, it should be published by the Free Software Foundation
#define V4L2_STD_BTSC_8VSB ((v4l2_std_id)0x02000000)
* different techniques for packing the packet and such, so that some appear
* ebt_encode;
#define TRB_ENTRY struct videobuf_queue *q;
int (*copy_to_user)(struct videobuf_queue *q,
struct videobuf_queue *q;
int amplifier;
Steve Whitehouse <gw7rrm@eeshack3.swin.me.uk>
#define V4L2_STD_SECAM_L ((v4l2_std_id)0x00400000)
* Addition HACK: follow perms without
* makes switch up to break to, there's a hack defining ATM_NO_PAR
#define __SO_NUMBERS
/* THIS will go away
* Remove it when
* Copied in_suspend; 1995-2000 Sangoma Technology;
#define V4L2_STD_SECAM_L ((v4l2_std_id)0x00400000)
* Jun 02, 1999 Gideon Hackack added support for the 5514
/* This is a hack but seems sufficient for the
NetBSD/OpenBSD headers
* here. We ought to some special case hackery that add
```

Focus on FastResponder

Need for a fast artefact acquisition tool, easy to use and robust



Source : SANS Windows Forensic FOR 408



Focus on FastResponder

- *Decoding MBR and BootSector*
- *Dump MFT*
- *MD5 files of drive system*
- *Detect malicious files with yara signatures*

FastResponder: Enter the code

Python 2.7 + ctypes

PyWin32

WMI requests

Psutils

Events logs new chanel

Export CSV

CLI or Config File

Detect encoding of Operating System

FastResponder: On IR

- *Very simple to distribute and collect the results*
- *Very simple to use*
- *The program doesn't crash of an decoding artefact*
- *Easy to add a artefact source*
- *Fast Collector*

FastResponder: On IR

- *Profile collector like volatility*
- *Choose an artefact to collect to minimize and concentrate searching*
- *One module, one source of artefacts*
- *With CSV, you can index in ELK or Splunk results*
- *You can deploy by script or GPO the .exe*
- *MD5 of all files to compare with your threat intel data base*
- *You can use your threat intel signatures with yara integration*

FastResponder: Demo time





FastResponder: Future Features

Ram Dump and analyses

DNS Cache

Embedded Certificates in PE

Multi Browser history

Windows 8.1/10

Console collect like Viper or Meterpreter

For the community



Thanks to CERT team





Sébastien Larinier

Sebastien.larinier@sekoia.fr

@sebdraven

SEKOIA

16, Place de la Madeleine

75008 Paris

www.sekoia.fr