CENSUS

IT Security Works

”Malicious” Technologies

April 2015, CENSUS S.A.
Infocom Security

www.census-labs.com

> AGENDA

I. Intro

II. Source Code Auditing

III. Vulnerability Research/Bug Hunting

IV. Packing/Crypting

> INTRO

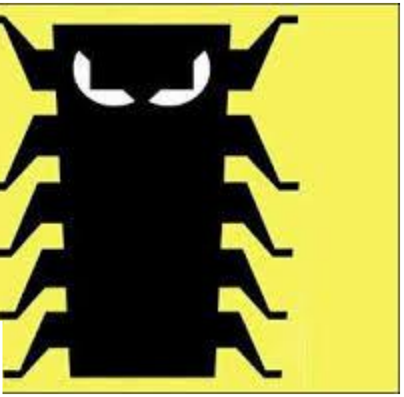
- “Malicious” Technologies?

> INTRO

- Inexistent “Malicious” Technologies?

> INTRO

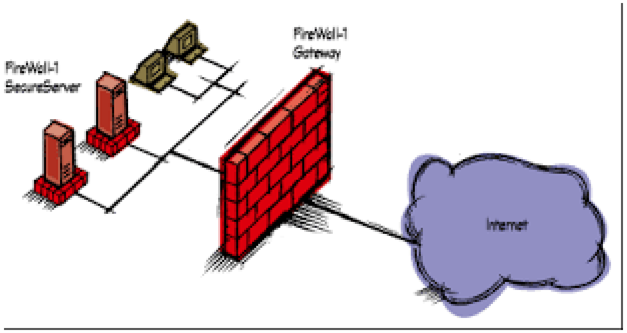
- Bugs



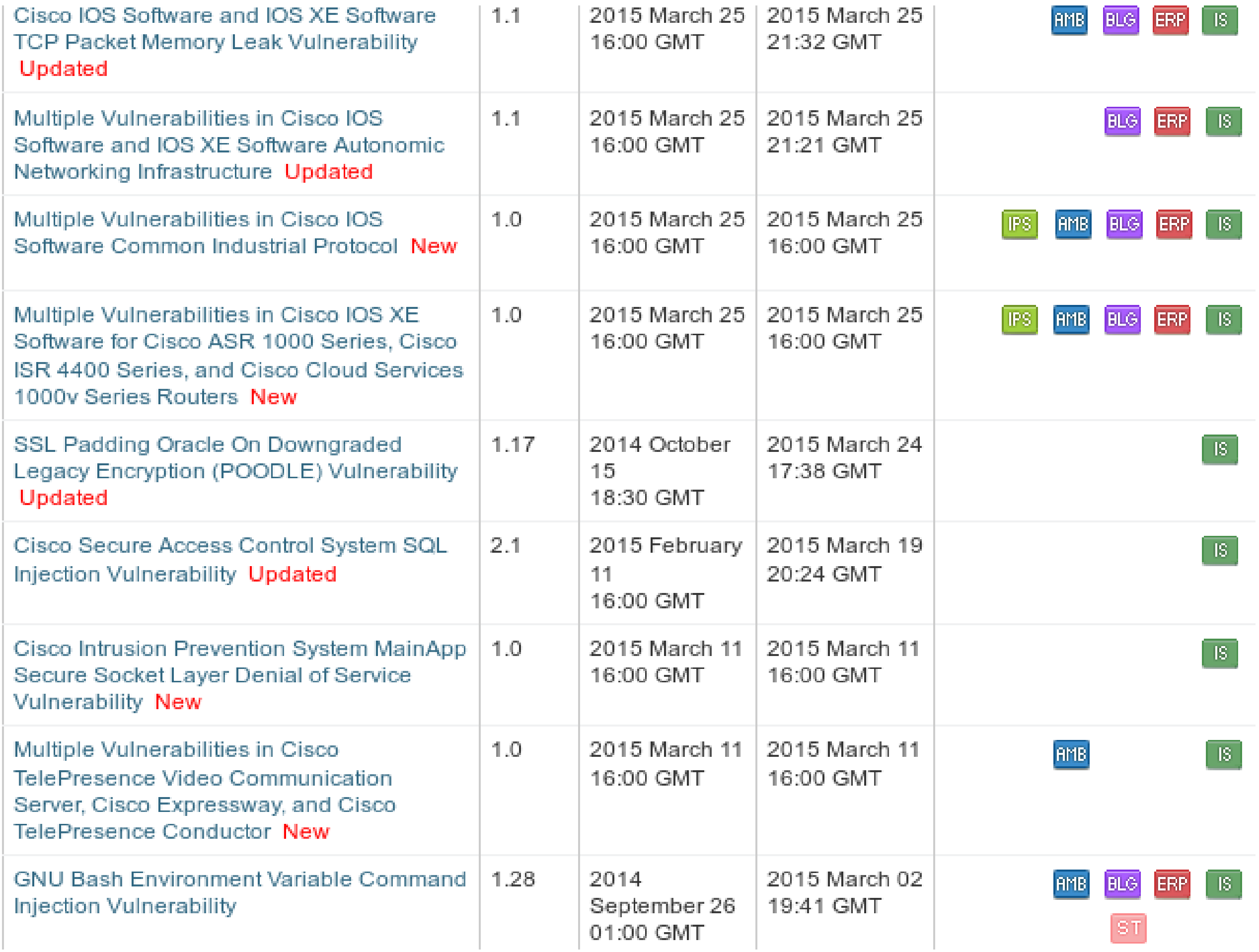
```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this                you've seen this Stop error screen,
restart                this screen appears again, fol
these s

Check t                hardware or software is prope
If this                ion, ask your hardware or soft
for any                u might need.

If prob                ble or remove any newly instal
or soft                memory options such as caching
If you                 de to remove or disable compon
your co                 select Advanced Startup options, and then
select

Technic

*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)

***  SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c
```

> INTRO

- Solution?

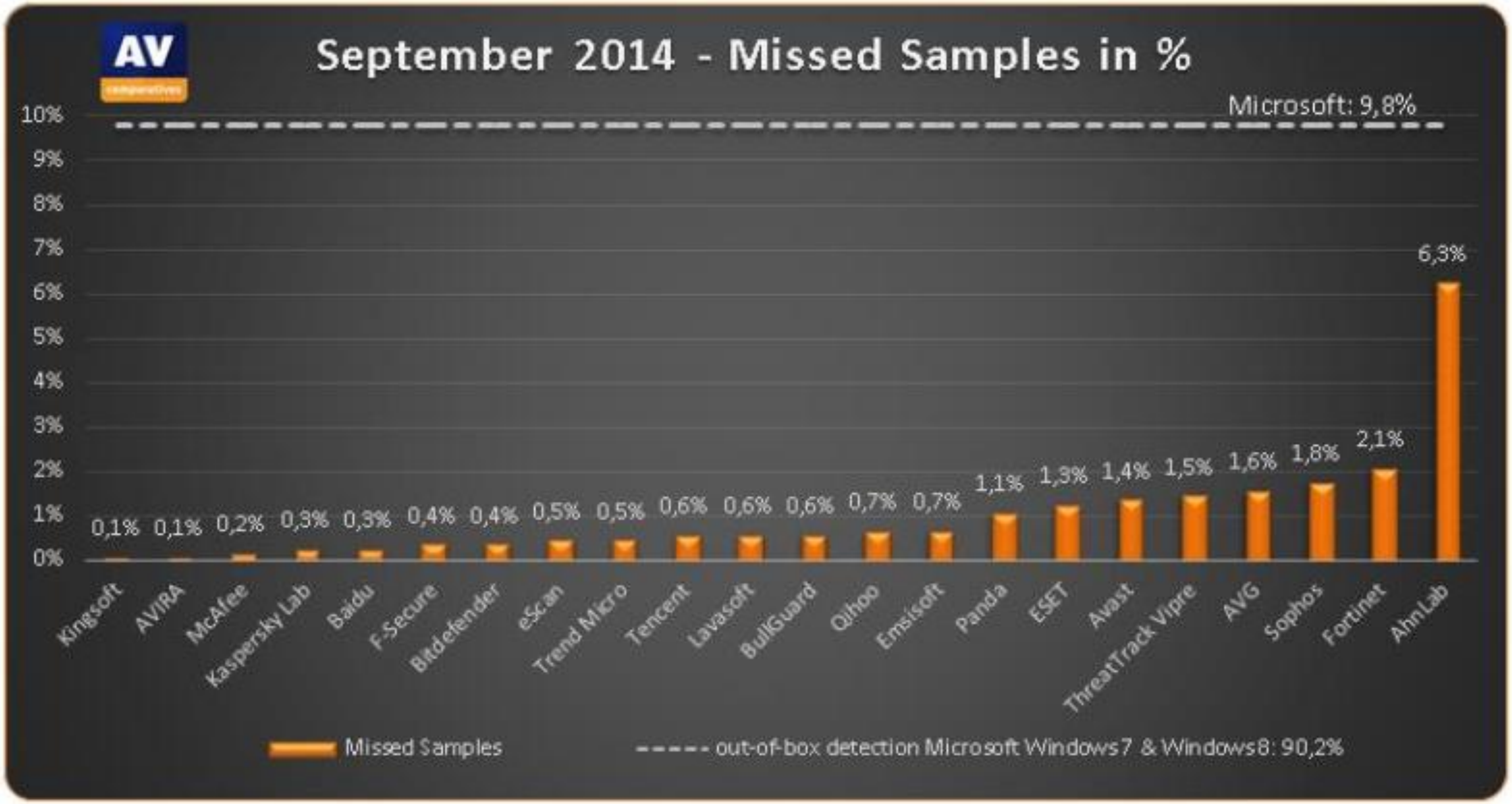


> INTRO

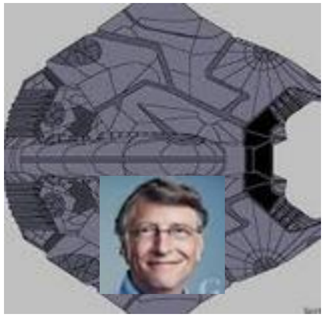


Cisco IOS Software and IOS XE Software TCP Packet Memory Leak Vulnerability Updated	1.1	2015 March 25 16:00 GMT	2015 March 25 21:32 GMT	AMB BLG ERP IS
Multiple Vulnerabilities in Cisco IOS Software and IOS XE Software Autonomic Networking Infrastructure Updated	1.1	2015 March 25 16:00 GMT	2015 March 25 21:21 GMT	BLG ERP IS
Multiple Vulnerabilities in Cisco IOS Software Common Industrial Protocol New	1.0	2015 March 25 16:00 GMT	2015 March 25 16:00 GMT	IPS AMB BLG ERP IS
Multiple Vulnerabilities in Cisco IOS XE Software for Cisco ASR 1000 Series, Cisco ISR 4400 Series, and Cisco Cloud Services 1000v Series Routers New	1.0	2015 March 25 16:00 GMT	2015 March 25 16:00 GMT	IPS AMB BLG ERP IS
SSL Padding Oracle On Downgraded Legacy Encryption (POODLE) Vulnerability Updated	1.17	2014 October 15 18:30 GMT	2015 March 24 17:38 GMT	IS
Cisco Secure Access Control System SQL Injection Vulnerability Updated	2.1	2015 February 11 16:00 GMT	2015 March 19 20:24 GMT	IS
Cisco Intrusion Prevention System MainApp Secure Socket Layer Denial of Service Vulnerability New	1.0	2015 March 11 16:00 GMT	2015 March 11 16:00 GMT	IS
Multiple Vulnerabilities in Cisco TelePresence Video Communication Server, Cisco Expressway, and Cisco TelePresence Conductor New	1.0	2015 March 11 16:00 GMT	2015 March 11 16:00 GMT	AMB IS
GNU Bash Environment Variable Command Injection Vulnerability	1.28	2014 September 26 01:00 GMT	2015 March 02 19:41 GMT	AMB BLG ERP IS ST

> INTRO


AV comparatives
September 2014 - Missed Samples in %
Microsoft: 9,8%
10%
9%
8%
7%
6%
5%
4%
3%
2%
1%
0%
0,1%
0,1%
0,2%
0,3%
0,3%
0,4%
0,4%
0,5%
0,5%
0,6%
0,6%
0,6%
0,7%
0,7%
1,1%
1,3%
1,4%
1,5%
1,6%
1,8%
2,1%
6,3%
Kingsoft
AVIRA
McAfee
Kaspersky Lab
Baidu
F-Secure
Bitdefender
eScan
Trend Micro
Tencent
Lavasoft
BullGuard
Qihoo
Emsisoft
Panda
ESET
Avast
ThreatTrack Vipre
AVG
Sophos
Fortinet
AhnLab
Missed Samples
out-of-box detection Microsoft Windows7 & Windows8: 90,2%

> ATTACKERS



> SOURCE CODE AUDITING

30,229,414,348

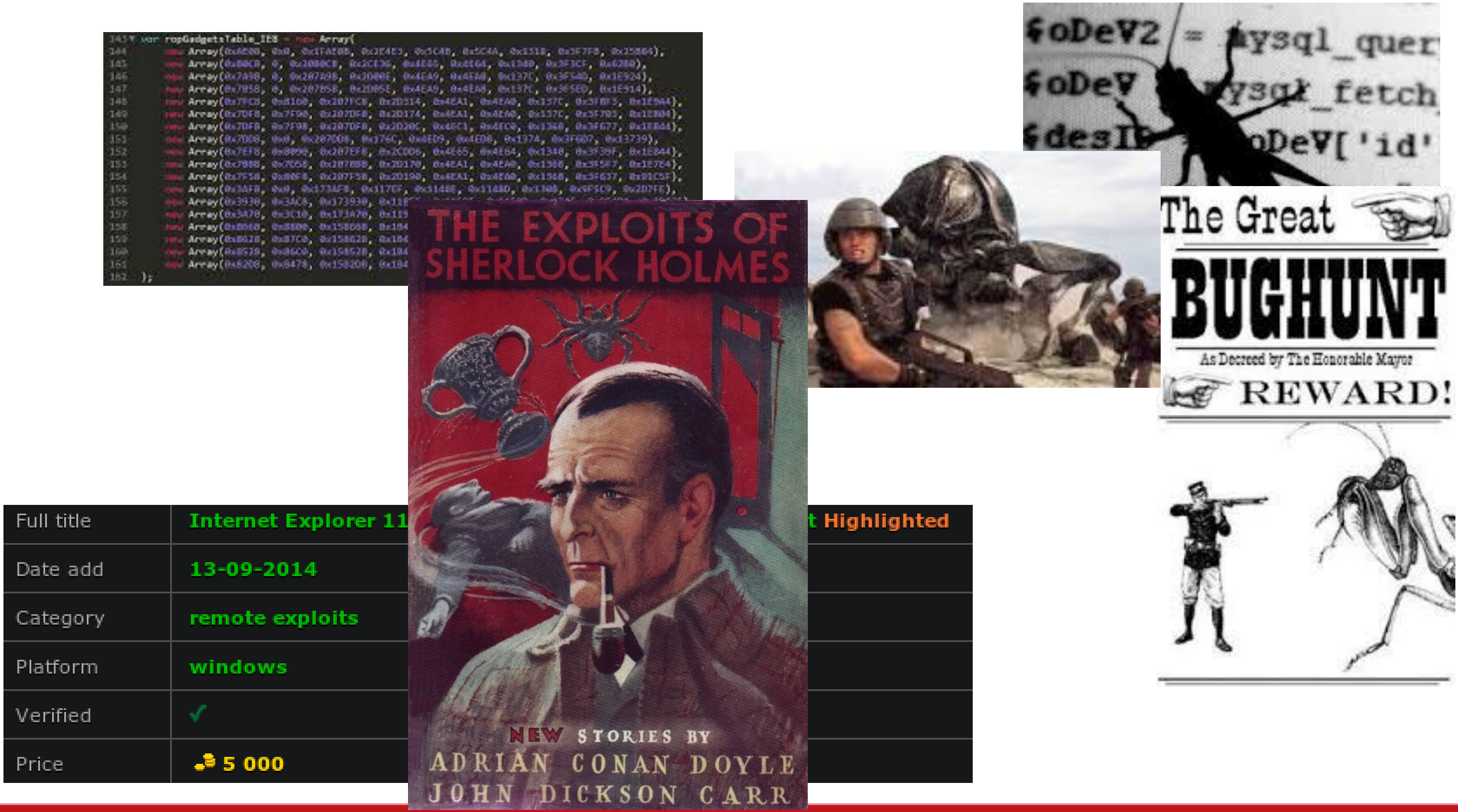
Lines of Code in Open Source Projects

BLACKDUCK | Open HUB

> BUGS?

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this          you've seen this Stop error screen,
restart          this screen appears again, fol
these s

Check t          hardware or software is prope
If this          ion, ask your hardware or soft
for any          u might need.

If prob          ble or remove any newly instal
or soft          memory options such as caching
If you           de to remove or disable compon
your co          select Advanced Startup options, and then
select

Technic

*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)


***  SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c
```

> BUG HUNTING/EXPLOITS

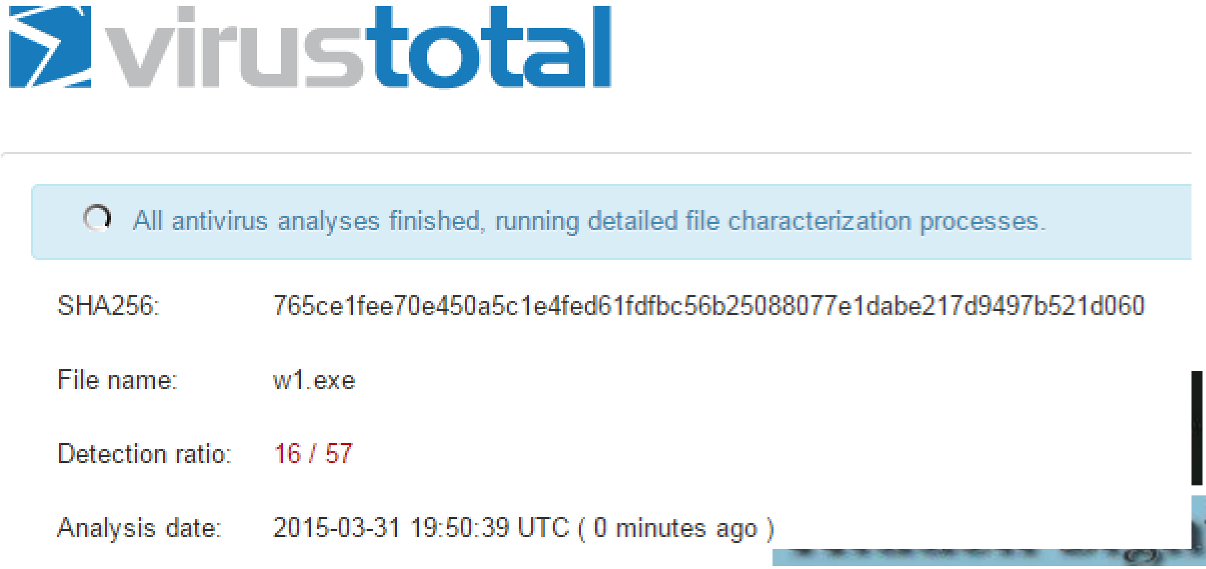


```
var ropGadgetsTable_IE8 = new Array(
        new Array(0xAE00, 0x0, 0x1FAE08, 0x2E4E3, 0x5C4B, 0x5C4A, 0x1318, 0x3F7F8, 0x25804),
        new Array(0xB0C8, 0, 0x2000C8, 0x2CE36, 0x4E66, 0x4E64, 0x1340, 0x3F3CF, 0x6280),
        new Array(0x7A98, 0, 0x207A98, 0x2D00E, 0x4EA9, 0x4EA8, 0x137C, 0x3F5A0, 0x1E924),
        new Array(0x7B58, 0, 0x207B58, 0x2D05E, 0x4EA9, 0x4EA8, 0x137C, 0x3F5ED, 0x1E914),
        new Array(0x7FC8, 0x8100, 0x207FC8, 0x2D314, 0x4EA1, 0x4EA0, 0x137C, 0x3F8F5, 0x1E9A4),
        new Array(0x7DF8, 0x7F90, 0x207DF8, 0x2D174, 0x4EA1, 0x4EA0, 0x137C, 0x3F703, 0x1E804),
        new Array(0x7DF8, 0x7F98, 0x207DF8, 0x2D20C, 0x4EC1, 0x4EC0, 0x1368, 0x3F677, 0x1E844),
        new Array(0x7D08, 0x0, 0x207D08, 0x176C, 0x4ED9, 0x4ED8, 0x1374, 0x3F6D7, 0x13739),
        new Array(0x7EF8, 0x8090, 0x207EF8, 0x2CDD6, 0x4E65, 0x4E64, 0x1348, 0x3F39F, 0x1E844),
        new Array(0x7B88, 0x7D58, 0x207B88, 0x2D170, 0x4EA1, 0x4EA0, 0x1388, 0x3F5F7, 0x1E7E4),
        new Array(0x7F58, 0x80F8, 0x207F58, 0x2D190, 0x4EA1, 0x4EA0, 0x1368, 0x3F637, 0x01C5F),
        new Array(0x3AF8, 0x0, 0x173AF8, 0x117EF, 0x11400, 0x1140D, 0x1308, 0x9F5C9, 0x207FE),
        new Array(0x3930, 0x3AC8, 0x173930, 0x118
        new Array(0x3A70, 0x3C10, 0x173A70, 0x119
        new Array(0x8068, 0x8800, 0x158068, 0x184
        new Array(0x8628, 0x87C0, 0x158628, 0x184
        new Array(0x8528, 0x86C0, 0x158528, 0x184
        new Array(0x8208, 0x8478, 0x158208, 0x184
);
```

Full title	Internet Explorer 11 … t Highlighted
Date add	13-09-2014
Category	remote exploits
Platform	windows
Verified	✓
Price	5 000

> PACKING/CRYPTING

> PACKING/CRYPTING



virustotal

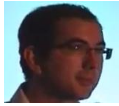
All antivirus analyses finished, running detailed file characterization processes.

SHA256: 765ce1fee70e450a5c1e4fed61fdfbc56b25088077e1dabe217d9497b521d060

File name: w1.exe

Detection ratio: 16 / 57

Analysis date: 2015-03-31 19:50:39 UTC (0 minutes ago)



ZEUS Crypter - 2.2

> USE

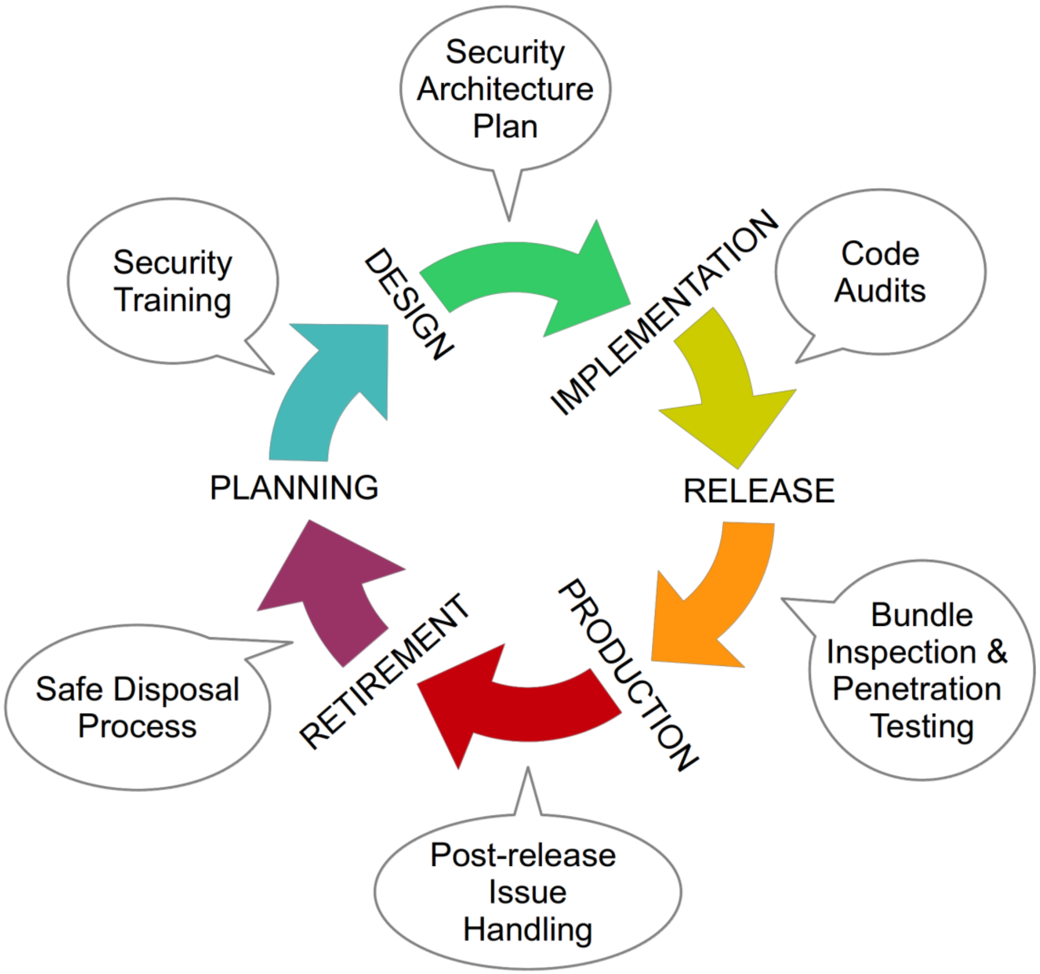
3 Vulnerability Fighting Cases

- Large Public Organization/MDM Solution Installation

- Organization with proper Source Code Audit/SSDLC Process

- SSDLC Implementation on Development House

> SECURITY CONSULTING WITHIN THE SDLC



Thank you!

CENSUS
IT Security Works