보안솔루션, 그 관리의 중요성

(최대의 효과를 위한 실천적 보안솔루션 운영방안)

네트워크의 미래를 제시하는 세미나 **NetFocus 2003 :**

IT 관리자를 위한 네트워크 보안 방법론

on the NET
Network Intelligence for Leading Networkers

인포섹㈜ / **CERT**팀장

이 정 환

Junghlee@skinfosec.co.kr

AGENDA

I. 보안솔루션 관리 필요성

II.보안솔루션 운영전략

III.보안솔루션 현황

IV.보안강화

V.관리 및 보호

VI.결 론

I. 보안솔루션의 관리 필요성

배 경

- 기업의 Internet Technology 의존도가 심화됨
- 안전한 네트워크 관리를 위한 보안정책이 도입됨
- 보안정책의 실천을 위하여 보안솔루션 도입되어 운영되고 있음

목 적

- 기 운영중인 보안솔루션을 효과적으로 관리 운영함으로써
  기업 정보시스템의 C.I.A.를 확보하고자 함

※ C.I.A. : Confidentiality, Integrity, Availability

II. 보안솔루션 운영 전략

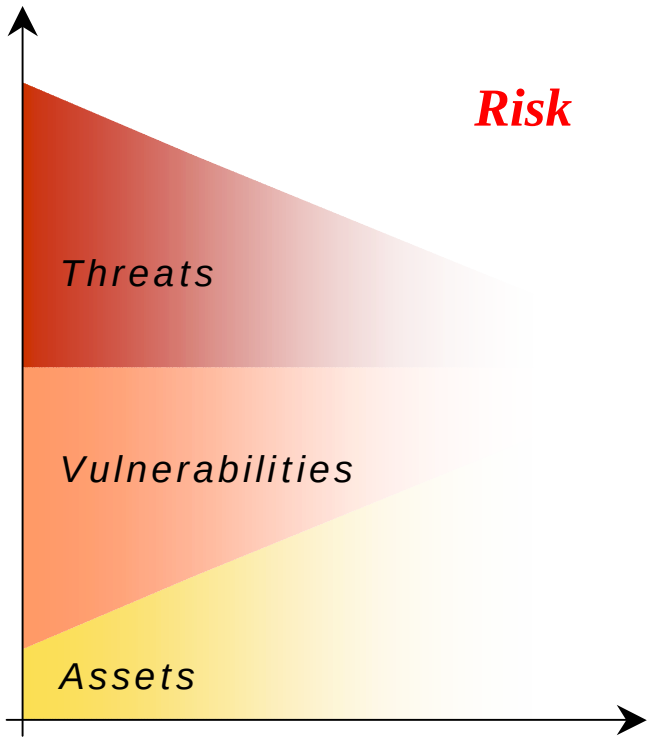
1. 전 략 목 표 RISK REDUCTION(계속)

가. 기업 정보시스템의 보호
- 보안 취약점 인지 및 제거
- 위협 인지

나. 효과적인 관리
- 확장성
- 중앙 집중식 관리

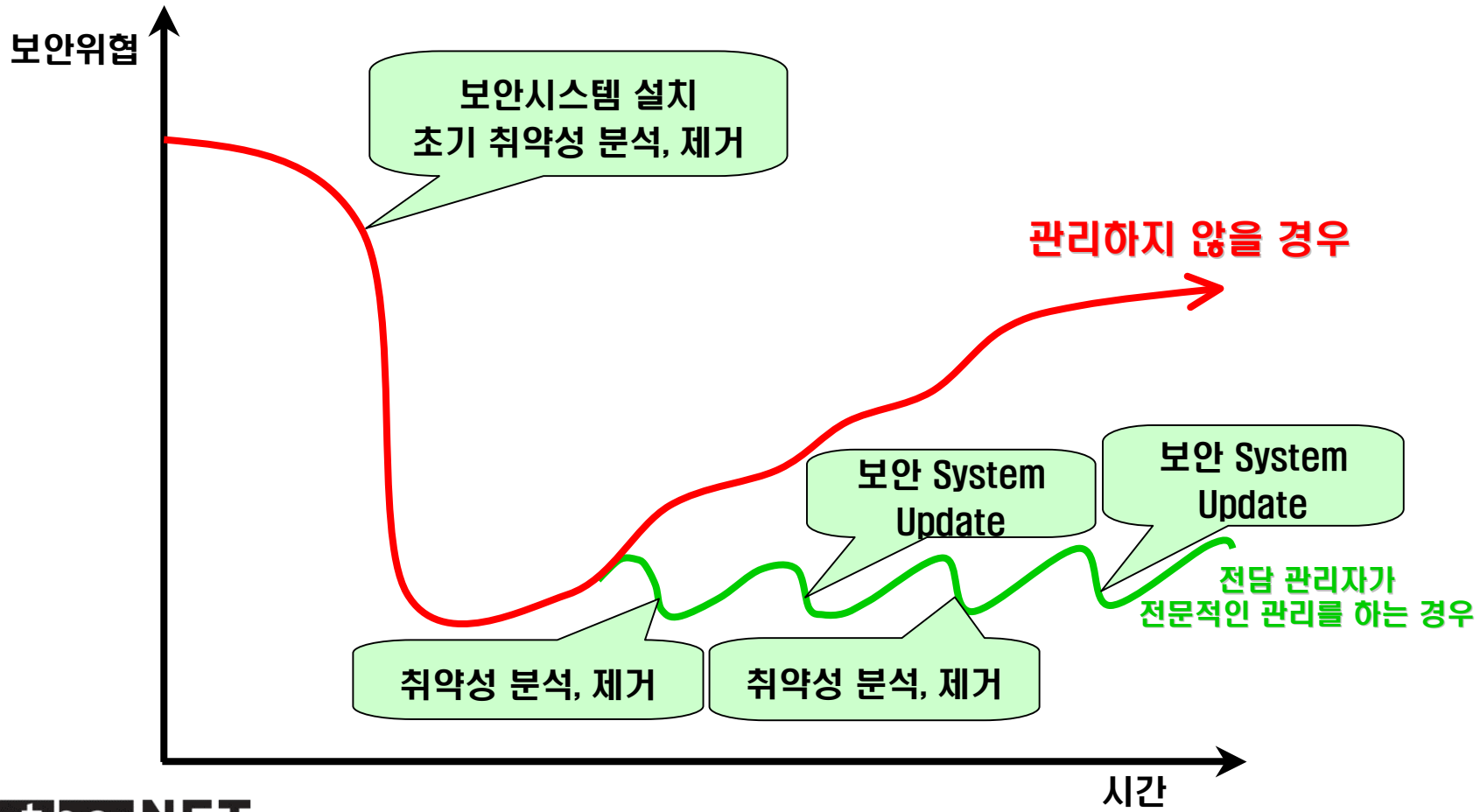
다. 보안솔루션 운영 절차
- 환경에 맞는 운영 절차
- 위험 관리 절차

라. 기업 수입과 평판 보호



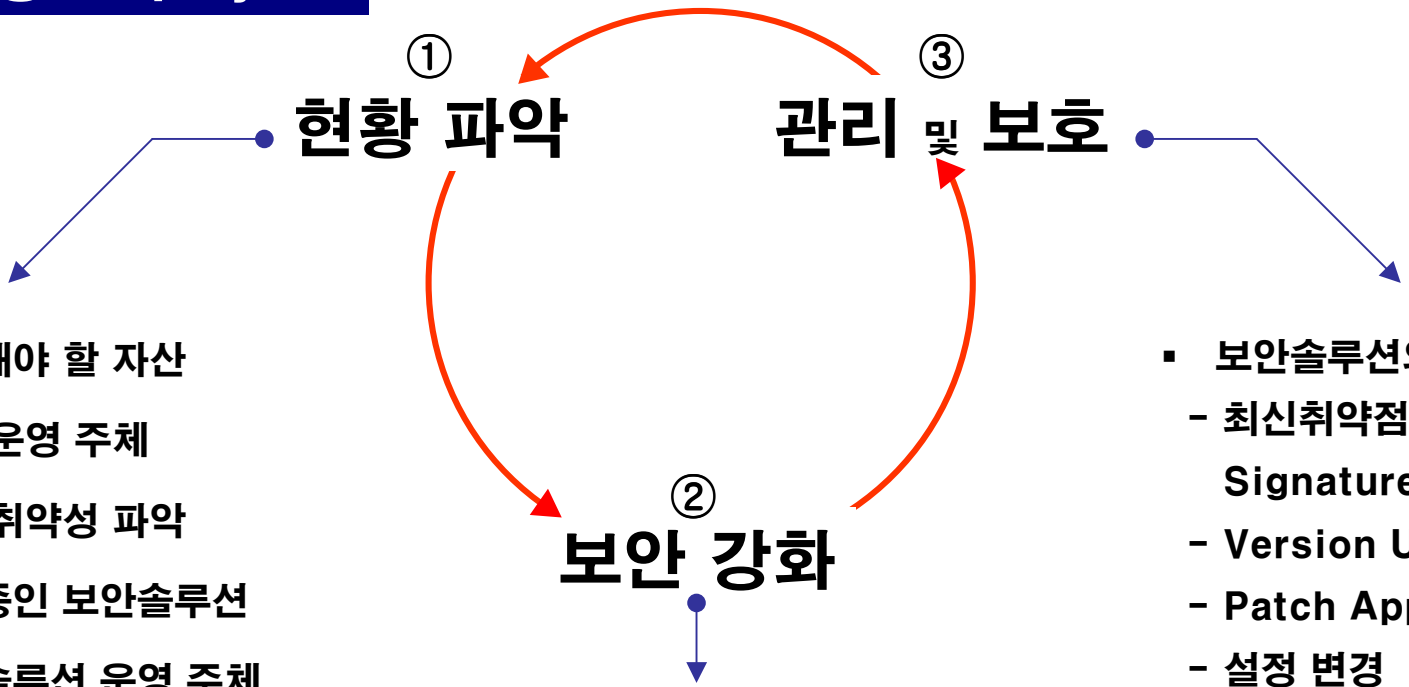
II. 보안솔루션 운영 전략

1. 전 략 목 표 *RISK REDUCTION*



II. 보안솔루션 운영 전략

2. 운영 전략 Cycle



- 보호해야 할 자산
- 자산 운영 주체
- 자산 취약성 파악
- 운영중인 보안솔루션
- 보안솔루션 운영 주체

- 자산별 보안강화
  - Hardening
- 보안권고사항 준수
  (사전보안강화)

- 보안솔루션의 관리
  - 최신취약점 탐지
    Signature Update
  - Version Update
  - Patch Apply
  - 설정 변경
  - Performance 측정
  - Rule Optimize

III. 보안솔루션 현황

1. 현황 파악 (계속)

Q1. 도입된 보안솔루션은 무엇인가 ?

Q2. 보안솔루션 운영주체는 누구인가 ?

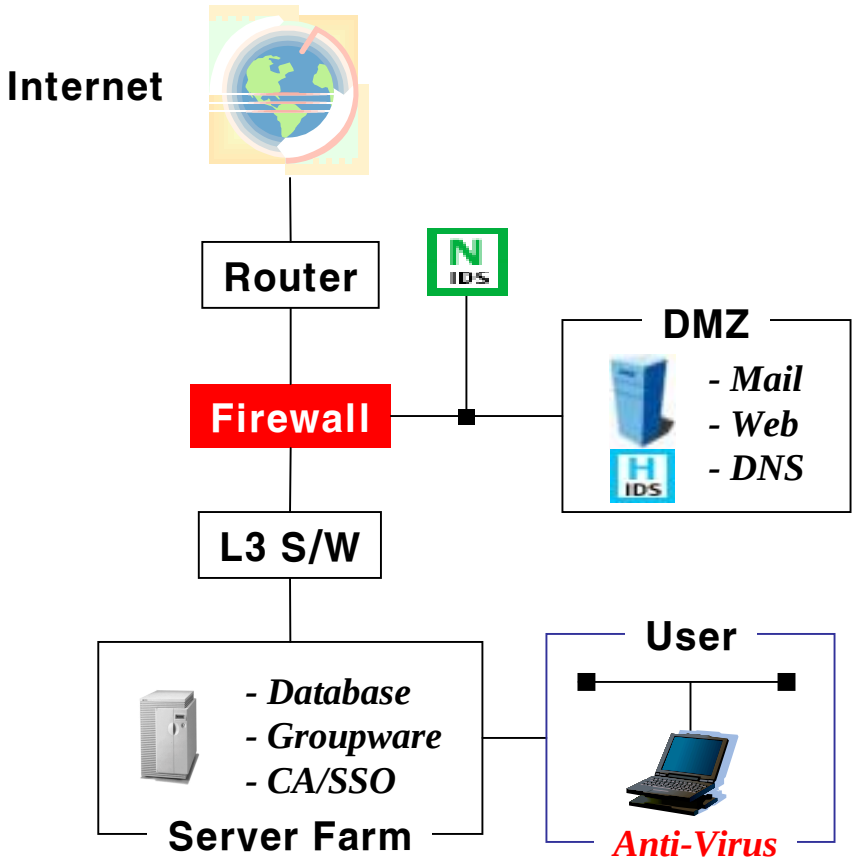
Q3. 보안솔루션이 보호하고자 하는 자산(Asset)은 무엇인가 ?

Q4. 자산 운영 주체는 누구인가 ?

Q5. 자산의 알려진 보안 취약점(Vulnerability)을 파악하고 있는가 ?

III. 보안솔루션 현황

1. 현황 파악

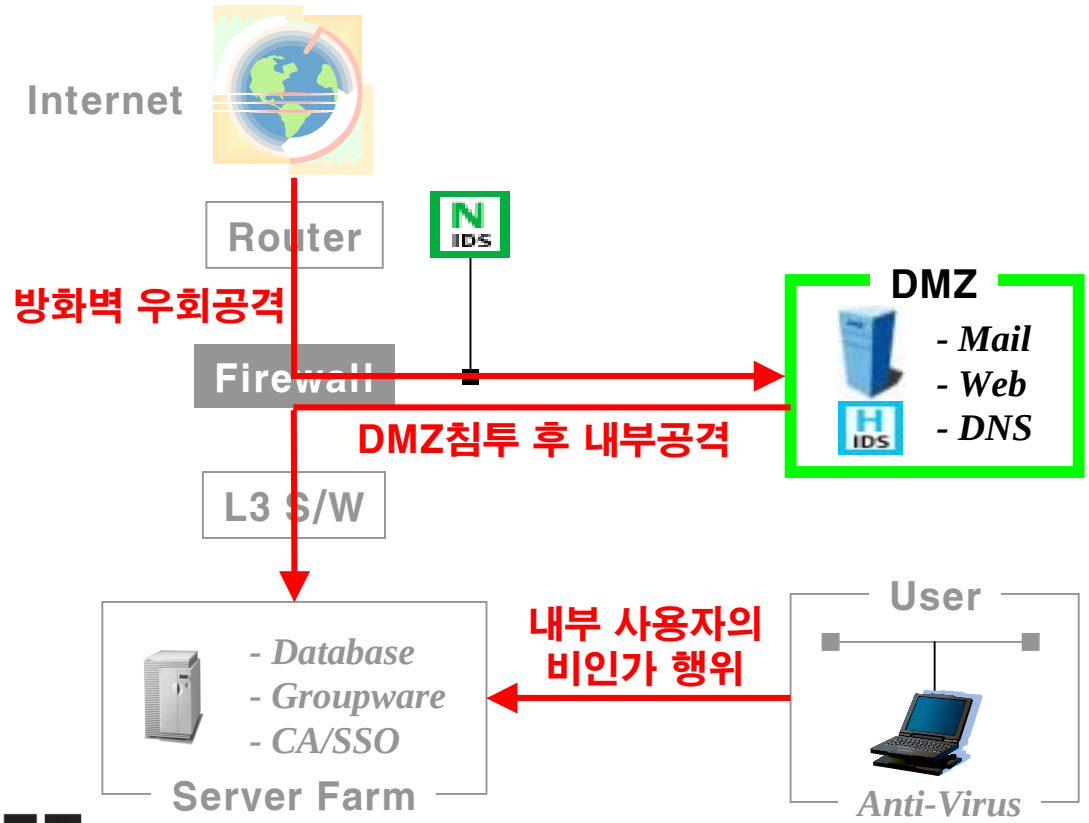


- 도입된 보안솔루션
  - Network IDS
  - Host IDS
  - Firewall
  - Anti-Virus
- 보호해야 할 자산
  DMZ,Server Farm Segment내 의 주요 정보시스템
- 존재하는 취약점
  - Network 설정 취약점
  - 침입차단시스템 정책 취약점
  - 정보시스템 취약점

III. 보안솔루션 현황

2. 침입탐지시스템 (IDS)

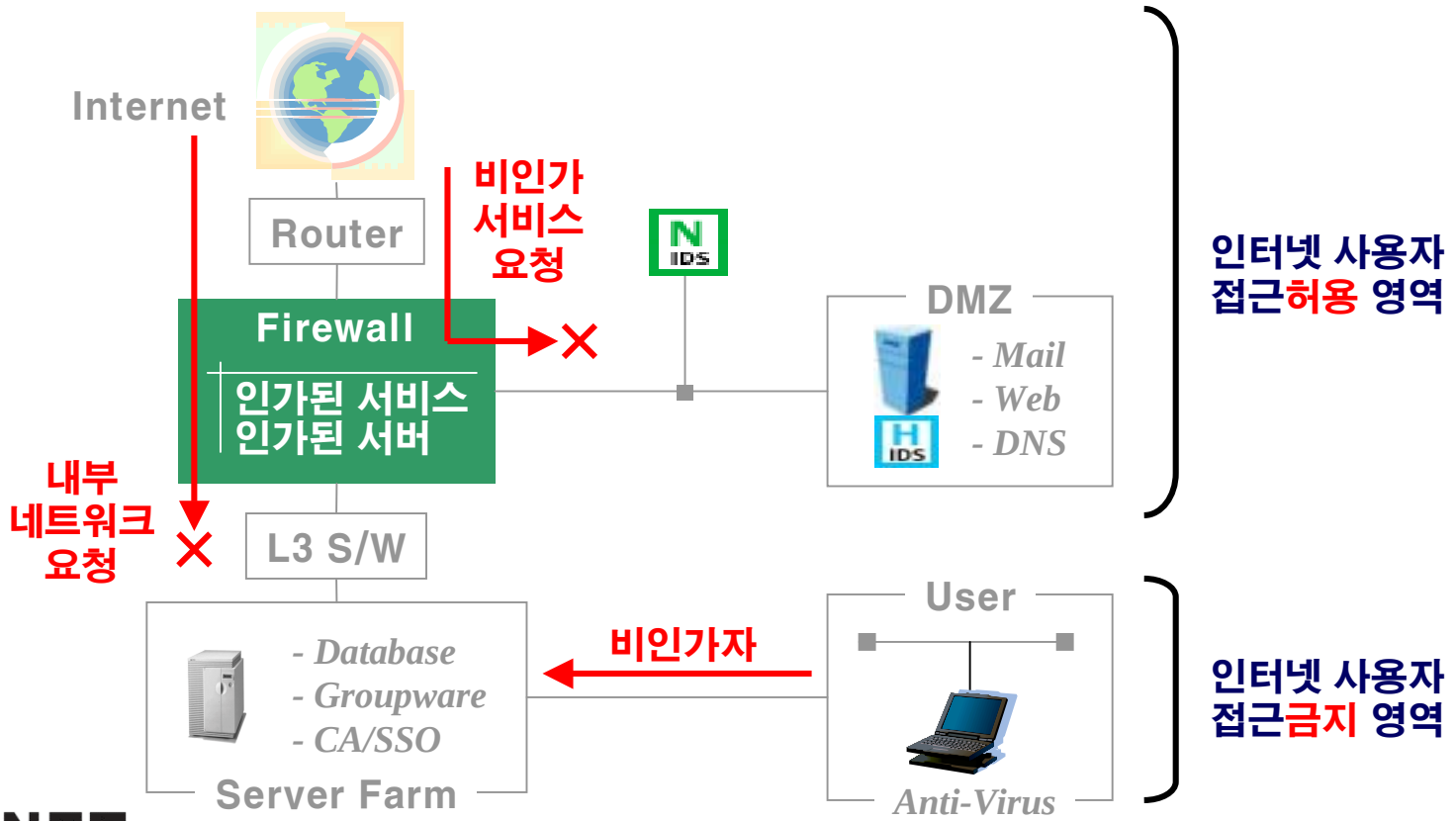
- 내/외부 사용자의 비인가 행위의 탐지(Detect)범위가 DMZ로 한정돼 있음
- Server Farm 및 User 망의 비인가 행위 및 공격 탐지 불가능



III. 보안솔루션 현황

3. 침입차단시스템 (Firewall)

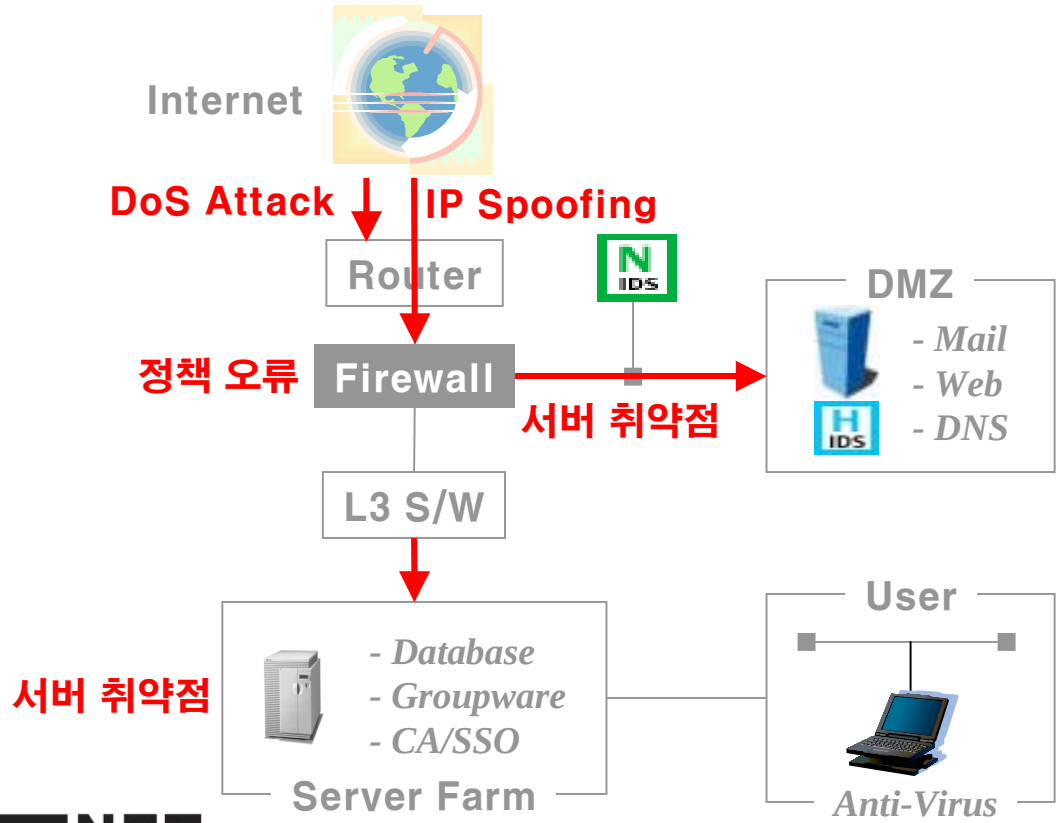
- 내부 사용자의 비인가 접속 제한이 불가능함



III. 보안솔루션 현황

4. 취약점 점검 (Vulnerability Assessment)

- 네트워크 장비 및 침입차단시스템의 보안 강화 설정 적용이 필요함
- 서버 및 네트워크의 보안 취약점 정기적으로 파악하여 보안강화 적용이 필요함



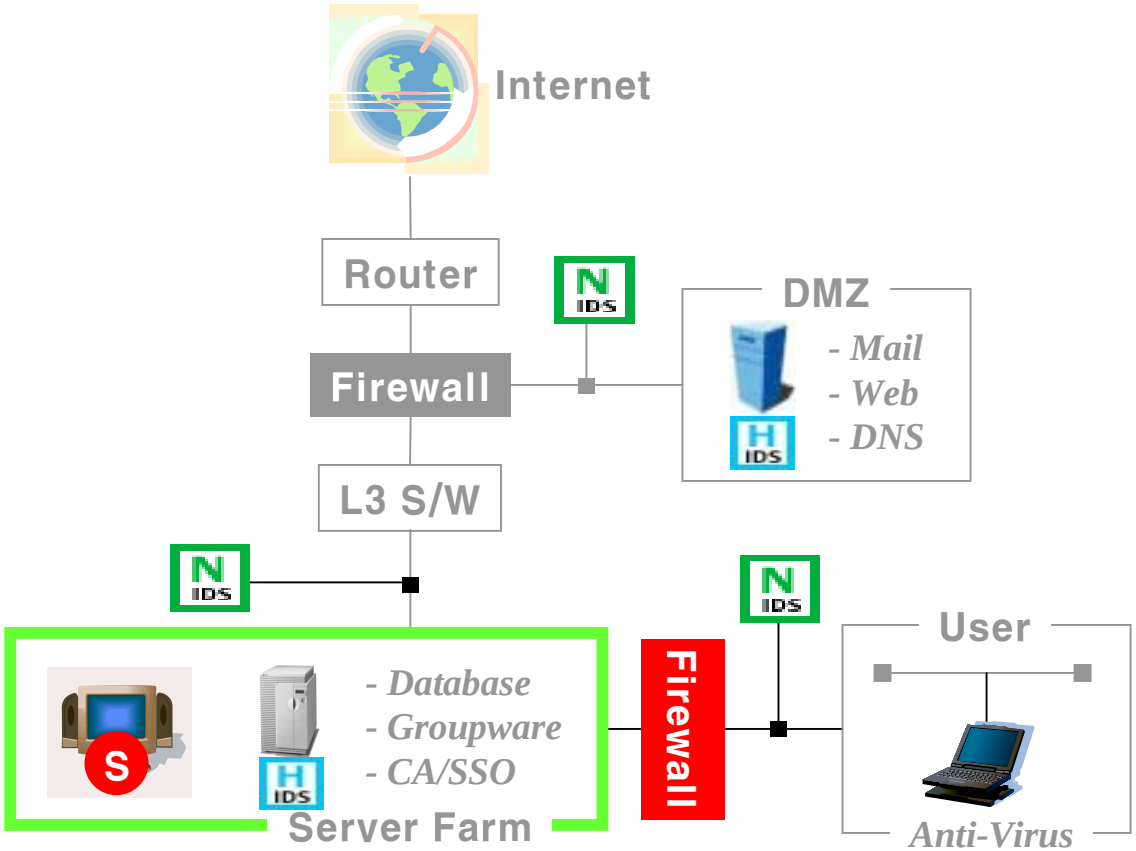
서버 보안수준 측정

네트워크 보안수준 측정

IV. 보안 강화(Hardening)

1. Security Hole 제거

- 기업 정보시스템의 Security Hole를 제거하기 위하여 추가적으로 보안솔루션을 도입함



- 침입차단시스템 (Firewall)
  User망에서 Server Farm으로 접근 제한
- 침입탐지시스템 (N IDS, H IDS)
  비인가 행위 및 공격탐지 범위 확대
- Scanner (S)
  정보시스템의 보안 취약점 파악 (정기/비정기)

IV. 보안 강화(Hardening)

2. 네트워크 장비 보안 강화 (계속)

- **Enable Secret 사용**

  Cisco 라우터의 경우 운영자(Privileged) Mode로 접근하기 위하여 사용되는 Password는 Secret Password 사용을 권장

  ▸ **조치방법**

  Privileged-mode로 들어간다.

  enable secret [level *level*] {password | *encryption-type encrypted-password*} ↵

- **Service password-encryption 사용**

  이 명령어를 사용할 경우 enable password의 패스워드를 암호화하여 저장함

  ▸ **조치방법**

  Global configuration mode로 들어간다.

  service password-encryption ↵

IV. 보안 강화(Hardening)

2. 네트워크 장비 보안 강화 (계속)

- **Username 사용**

  Username을 사용할 경우, 접근할 수 있는 계정과 패스워드를 알아야 함으로써 접근 보안성을 향상시킬 수 있으므로 사용하기를 권장

  ▸ **조치방법**

  Global configuration mode로 들어간다.

  username ID password 7 *password_strings* ↵

IV. 보안 강화(Hardening)

2. 네트워크 장비 보안 강화 (계속)

- **SNMP Default Community String 변경**

  SNMP의 Public, Private와 같은 Default Community String을 변경하지 않고 사용할 경우, 보안상 매우 위험성이 크기 때문에 추측하기 어려운 String으로 변경하기를 권장

  ▸ **조치방법**

  Global configuration mode로 들어간다.

  snmp-server community *string* RO ↵

- **SNMP Agent 관리 ACL 사용**

  SNMP Manager를 지정할 경우 접속 대상 Manager를 지정하여 접근이 가능한 IP를 제한하는 것이 권장

  ▸ **조치방법 (192.168.xxx.xxx에서만 해당 네트워크 장비로 접속가능)**

  Global configuration mode로 들어간다.

  snmp-server community community_string RO 5 ↵

  access-list 5 permit 192.168.xxx.xxx ↵

IV. 보안 강화(Hardening)

2. 네트워크 장비 보안 강화 (계속)

- **HTTP 원격 관리 사용**

  HTTP를 통한 원격 관리는 지양해야 한다. 단순 사용자 인증방식에 따라 Brute Force 공격이 가능하며, HTTP에 대한 보안취약점이 발표되고 있는 사용하지 않는 것이 권장

  ▸ **조치방법**

  Global configuration mode로 들어간다.

  no ip http server ↵

- **원격관리 대상 제한 필요**

  Default로 모든 네트워크에서 접속(telnet)이 가능하도록 되어 있는 보안상 위험성이 존재함으로 원격 접속은 관리자 PC나 특정 Segment내에서만 접속할 수 있도록 제한하는 것이 권장

  ▸ **조치방법**

  Global configuration mode로 들어간다.

  ip access-class 1-199 in (필요한 segment에서만 접속하도록 ACL을 적용) ↵

IV. 보안 강화(Hardening)

2. 네트워크 장비 보안 강화 (계속)

- **원격관리 시 IDLE할 경우, 접속 종료 설정**

  네트워크를 통한 원격 접속 시 관리자가 일정 시간동안 키 입력이 없을 경우 연결된 접속을 종료시키는 기능을 사용하는 것이 권장됨

  ▸ **조치방법**

  Global configuration mode로 들어간다.

  exec-timeout 분 [초] ↵

- **Warning Banner 사용**

  네트워크 장비에 대한 Telnet 접속 시 적당한 Warning Banner를 삽입하여 불법적인 접속자에게 경고를 주는 것이 필요함

  ▸ **조치방법**

  Global configuration mode로 들어간다.

  banner motd *Warning_Banner* ↵

IV. 보안 강화(Hardening)

2. 네트워크 장비 보안 강화 (계속)

- **SNMP, SYSLOG 로깅 설정**

  SNMP TRAP이나 SYSLOG를 이용하여 네트워크 장비의 시스템 정보, 트래픽 정보 등을 지정된 Logging Server로 보내어 실시간으로 로깅 및 관리하는 것이 보안상이나 운영상 필요함

  ▸ **조치방법**

  Global configuration mode로 들어간다.

  logging xxx.xxx.xxx.xxx (Logging 서버 지정) ↵

IV. 보안 강화(Hardening)

2. 네트워크 장비 보안 강화 (계속)

- **Directed Broadcast 제한**

  IP Directed Broadcast는 DoS(Denial of Service)의 일종인 “Smurf” 공격에 방어하기 위하여 반드시 적용할 것을 권고함

  ▸ **조치방법**

  Global configuration mode로 들어간다.

  no ip directed-broadcast ↵

- **IP Source Routing 제한**

  내부의 라우팅 경로를 파악하여 라우팅이 되지 않는 주요서버로 접근을 할 수 있기 때문에 소스 라우팅을 기본적으로 사용하지 않는 것이 권고됨

  ▸ **조치방법**

  Global configuration mode로 들어간다.

  no ip source-route ↵

IV. 보안 강화(Hardening)

2. 네트워크 장비 보안 강화 (계속)

- **TCP/UDP Small Service 제한**

  DoS 공격의 대상이 될 수 있는 기본적인 서비스(echo, discard, daytime, chargen)를 제거하여 사용하지 않도록 하는 것을 권고함

  ▸ 조치방법

  Global configuration mode로 들어간다.

  no service tcp-small-servers ↵

  no service udp-small-servers ↵

- **Finger 서비스 사용 제한**

  Finger 서비스를 사용할 경우 기본적인 접속 상태가 노출될 수 있어 이 서비스를 제한 것을 권고함

  ▸ 조치방법

  Global configuration mode로 들어간다.

  no service finger ↵

IV. 보안 강화(Hardening)

2. 네트워크 장비 보안 강화

- **Anti-Spoofing with RPF 적용**

  Cisco 제품에서 지원하는 CEF(Cisco Express Forwarding)의 경우 라우터를 통과하는 패킷 헤더의 출발지 주소를 체크할 수 있으며, 그 패킷이 유효하지 않을 경우 해당 패킷을 Drop시킬 수 있어 CEF를 사용하는 경우 RPF(Reverse Path Forwarding) 진단 적용하는 것이 권장됨

  ▸ **조치방법**

  Global configuration mode로 들어간다.

  ip verify unicast reverse-path ↵

IV. 보안 강화(Hardening)

3. 침입차단시스템 정책 강화 (계속)

- **Basic Security Policy 이해**

  일반 네트워크 보안 정책을 정확히 확인하는 것이 필요하다. Internal Network에서의 인터넷 Access 및 웹 서버 등의 운영 등에 대한 기본적인 보안 정책을 이해하고 이 정책에 맞도록 침입차단시스템을 적용하는 것이 필요함

- **Security Architecture 이해**

  DMZ, Internal DNS 서버, External DNS 서버 운영, VPN이나 외부 Client의 정근 구성 등의 네트워크 구성 및 특성을 정확히 이해하는 것이 침입차단시스템의 보안 정책 적용 시 기술적인 문제 해결 및 적용을 효율화하는데 필수적임

- **기본 Performance(CPU, Memory) & Session 수 확인**

  침입차단시스템에 보안 정책이 적용되었을 경우 시스템의 CPU, Memory 증가와 평균 및 최대 Session 수를 확인하고 관리하는 것이 안전한 침입차단시스템 관리에 필요함

IV. 보안 강화(Hardening)

3. 침입차단시스템 정책 강화 (계속)

- **Change Control 관리**

  모든 Rule의 Change가 이루어 질 때에는 다음과 같은 항목에 대한 관리가 필요함
  - Name of Person modifying rule
  - Date/Time of rule Change
  - Reason for rule Change

- **Audit 상황 점검**

  일단 침입차단시스템 Rule이 완성되면, Rule에 대한 외부와 내부에서의 Audit가 필요하며 이를 주기적으로 진행하는 것이 필요함

- **침입차단시스템 자체 보안강화**

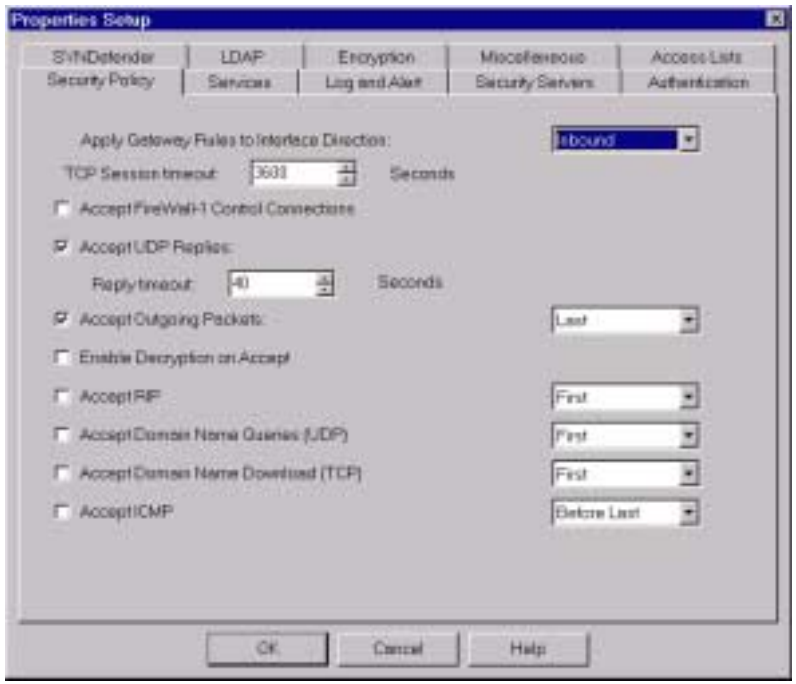
  1차적으로 네트워크 보호하는 장비이며, 외부에 노출되어 있기 때문에 침입차단시스템이 설치되어 있는 OS 보안 강화를 위하여 Hardening 작업을 반드시 수행할 필요가 있음

IV. 보안 강화(Hardening)

3. 침입차단시스템 정책 강화 (계속)

- **Default Properties**

  침입차단시스템은 Default Policy로 많은 서비스들이 Open되어 있어, 해당 환경에 알맞은 보안 설정해 주는 것이 필요함



IV. 보안 강화(Hardening)

3. 침입차단시스템 정책 강화 (계속)

- **Internal Outbound**

  Internal 네트워크의 모든 사용자가 인터넷에 Access할 때, HTTP, DNS Query 등과 같은 특정 필요서비스만 Open되어 있거나 Proxy를 사용하는 것이 필요함

IV. 보안 강화(Hardening)

3. 침입차단시스템 정책 강화 (계속)

- **LockDown**

  침입차단시스템으로 접근하는 모든 Access를 Block하는 Rule이 필요함

IV. 보안 강화(Hardening)

3. 침입차단시스템 정책 강화 (계속)

- **Drop All**

  Default로 Rule에 해당되지 않는 모든 Packet들을 Drop시켜야 하며, 필요성에 따라 Drop & Long LOG Rule 적용을 고려할 필요가 있음

IV. 보안 강화(Hardening)

3. 침입차단시스템 정책 강화 (계속)

- **No Logging**

Windows PC가 많은 Intranet에서는 Broadcast Traffic이 많이 있어, BetBIOS(NBT)와 Mail Server에 의한 사용자 Identify를 위해 사용되는 IDENT를 침입차단시스템으로 오는 것을 "Reject" Type으로 막고 Log를 남기지 않는 것이 권장됨

No.	Source	Destination	Service	Action	Track	Install On	T
1	fw-admin	firewall	FireWall1	accept	Long	Gateways	A
2	Any	firewall	NBT ident	reject		Gateways	A
3	Any	firewall	Any	drop	Long	Gateways	A
4	internal	Any	Any	accept	Long	Gateways	A
5	Any	Any	Any	drop	Long	Gateways	A

IV. 보안 강화(Hardening)

3. 침입차단시스템 정책 강화 (계속)

- **DNS Access**

  인터넷 DNS Access(Strictly 53/UDP)는 Internal 네트워크를 제외하고 모든 사용자가 접근할 수 있도록 하며 로그를 남기지 않도록 설정하는 것을 권장함
  (Internet Network는 Internal DNS Server를 사용하는 것이 일반적임)

3	Any	firewall	Any	drop	Long	Gateways	A
4	internal	dns-server	domain-udp	accept		Gateways	A
5	internal	Any	Any	accept	Long	Gateways	A

IV. 보안 강화(Hardening)

3. 침입차단시스템 정책 강화 (계속)

- **SMTP/HTTP Access**

  모든 사용자가 해당 서비스를 이용할 수 있도록 설정해야 함

IV. 보안 강화(Hardening)

3. 침입차단시스템 정책 강화 (계속)

- **Blocking DMZ**

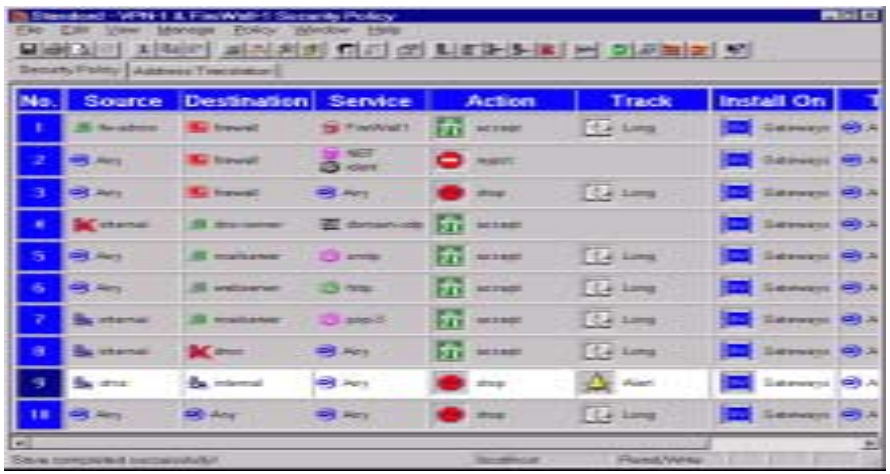
  Internal 사용자가 DMZ로의 접근을 막는 것이 내부자 보안에 매우 필요함으로 반드시 적용해야 함

IV. 보안 강화(Hardening)

3. 침입차단시스템 정책 강화 (계속)

- **Sneaky Rule**

  DMZ의 한 서버가 해킹 당해 Internal Network로 공격 시도할 경우 정책에 Drop 뿐만 아니라 관리자에게 Mail 또는 SNMP 등으로 Alert를 해 주는 것이 반드시 필요함
  (일반적인 상황에서 DMZ에서 Internal Network 접근이 없는 경우)

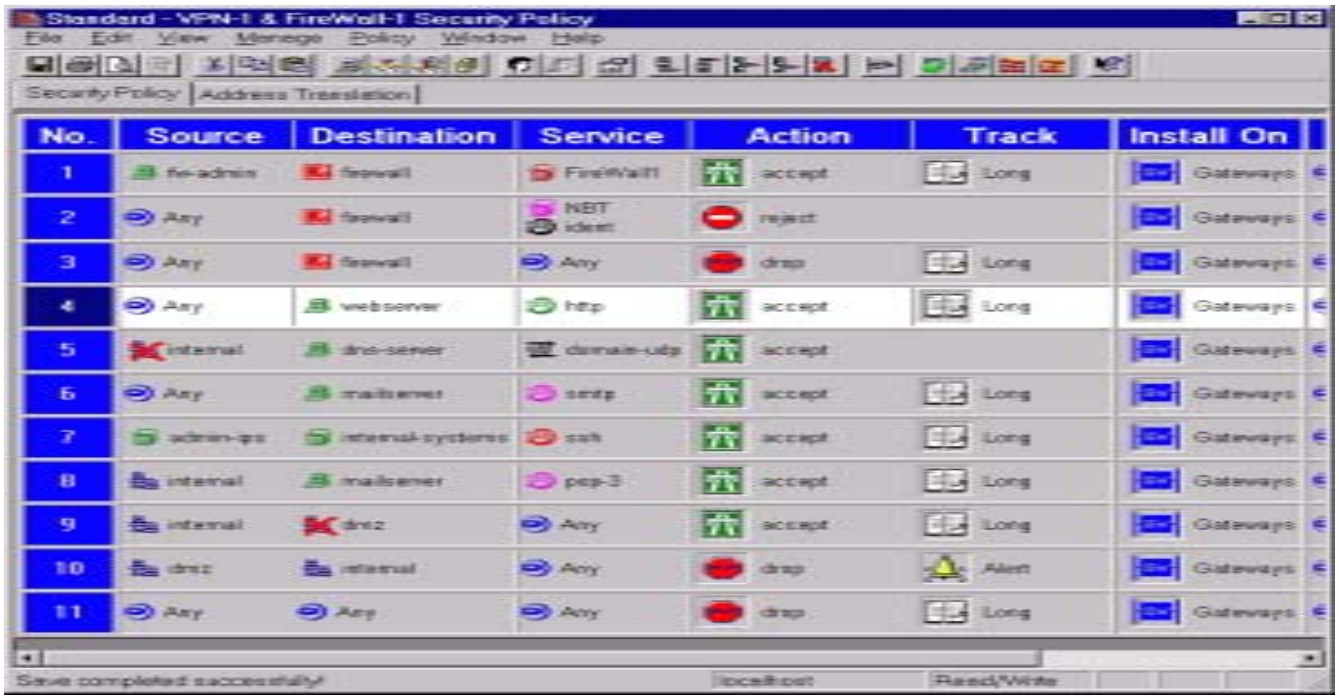


IV. 보안 강화(Hardening)

3. 침입차단시스템 정책 강화

- **Performance**

  Performance를 위하여 가장 일반적으로 사용되는 Rule은 RuleBase의 상위에 위치시키는 것이 필요함



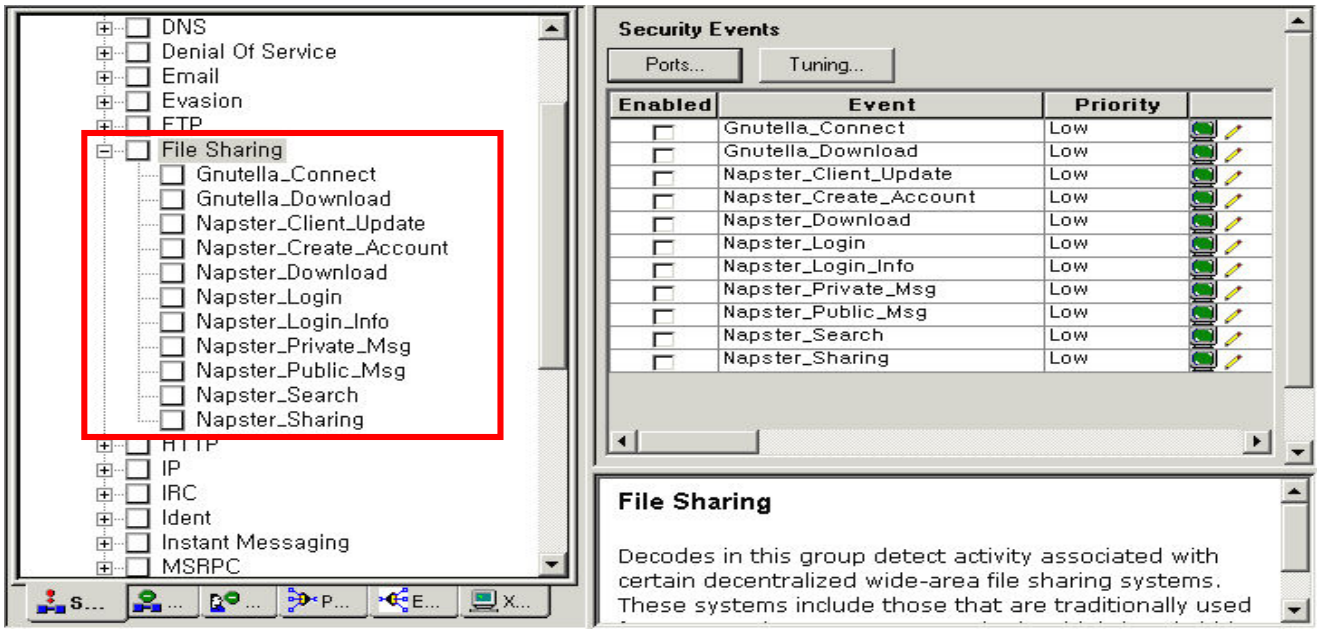
IV. 보안 강화(Hardening)

4. 침입탐지시스템 탐지 정책 (계속)

- **침입차단시스템 정책과 연관**

침입차단시스템의 정책에 따른 허용되지 않은 서비스(or 서버)에 대한 "탐지 정책"을 변경

(Example : P2P 서비스(Napster/Gnutella 사용 금지 정책에 따른 "탐지 정책" 제거)



IV. 보안 강화(Hardening)

4. 침입탐지시스템 탐지 정책 (계속)

- **탐지 위치에 따른 정책 적용**

  침입탐지시스템의 설치 위치(탐지 위치)에 따라 탐지 정책을 다르게 적용하는 것을 권장함
  (Example : DMZ Segment, Server Farm Segment, User Segment)

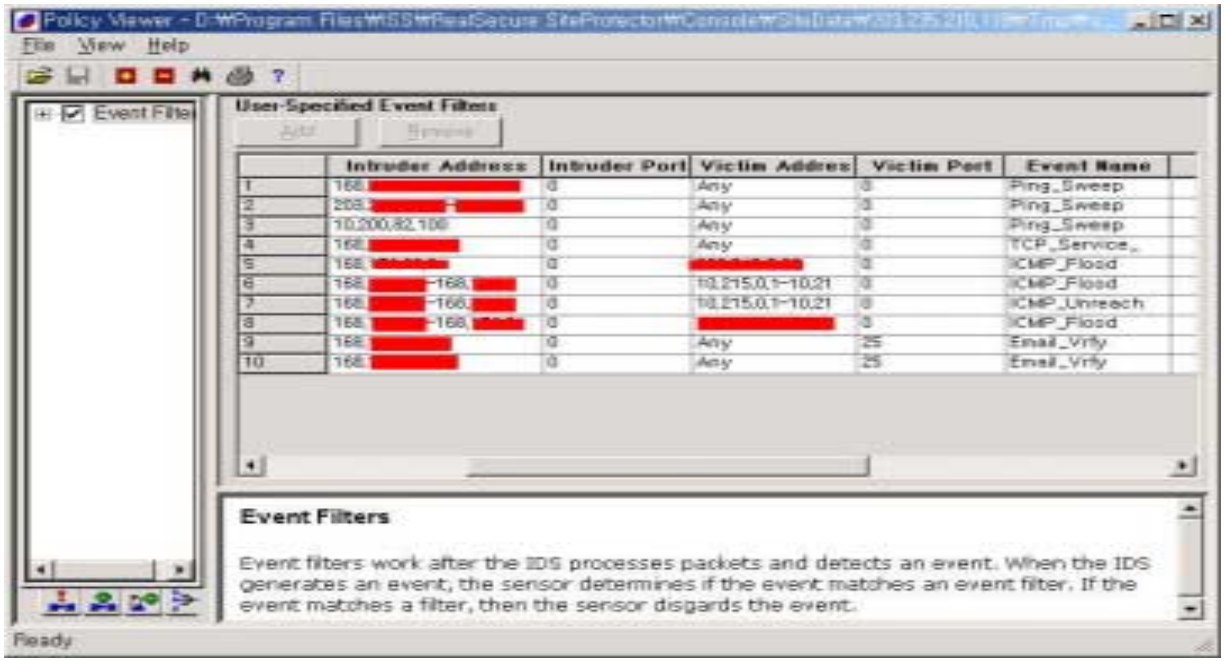
IV. 보안 강화(Hardening)

4. 침입탐지시스템 탐지 정책 (계속)

- **False Positive 제거**

정상적인 네트워크 행위를 공격으로 오판하는 "False Positive" Event를 제거하는 것이 필요함

(Example : 네트워크 장비의 Heartbeat Check로 사용되는 ICMP Protocol : ping 10.215.0.*)

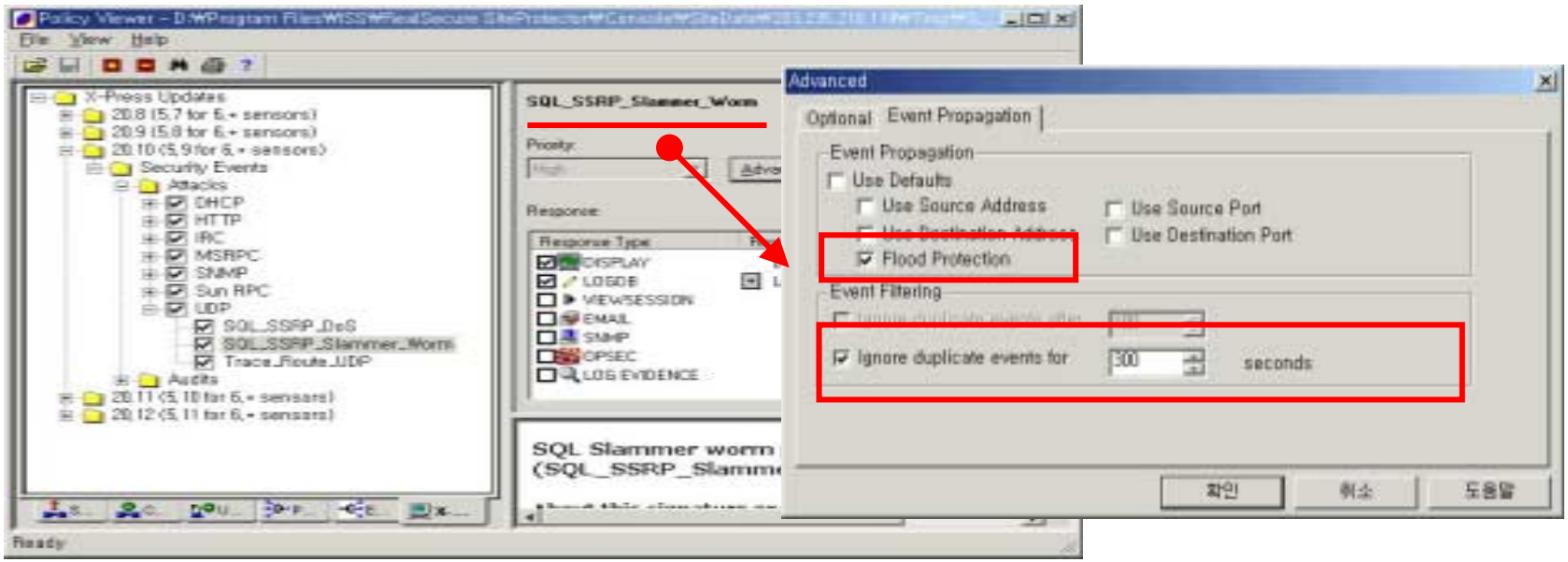


IV. 보안 강화(Hardening)

4. 침입탐지시스템 탐지 정책 (계속)

- **Flood Protection 설정**

Worm이 확산 활동하는 동안 Network에 Scanning, 공격 Packet 등과 같은 많은 행위를 수행함에 따라 탐지되는 Event가 많아진다. 따라서 **침입탐지시스템에 부하**를 줄 수 있어 Flood Protection을 적용해야 함 (Example : **SQL Slammer Worm**(UDP Protocol 이용 확산)

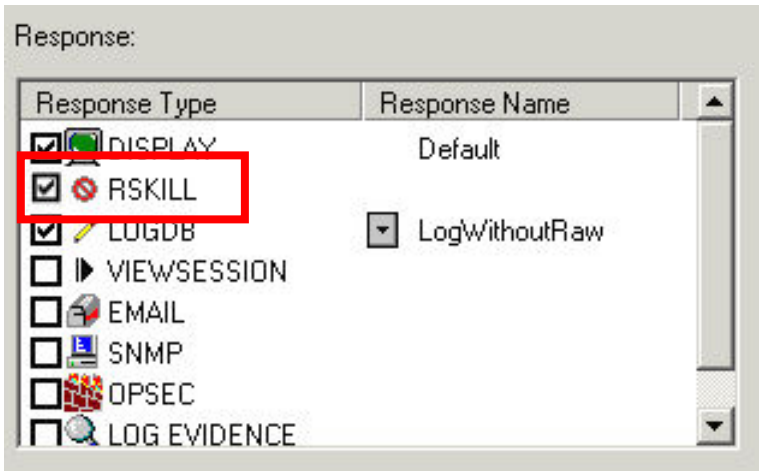


IV. 보안 강화(Hardening)

4. 침입탐지시스템 탐지 정책

- **Session Kill 설정**

비 인가자에 의한 공격을 차단하기 위하여 공격자의 Session을 끊을 필요가 있을 때, Session Kill 설정을 적용할 수 있으나 **매우 신중하게 적용**해야 한다. 왜냐하면 Worm과 같이 Traffic을 유발하는 공격에 대해 Session Kill 설정할 경우 **Worm Traffic과 IDS Traffic(Reset Packet)이 합해져 네트워크 Traffic 상황을 더 악화**시킬 수 있기 때문이다.

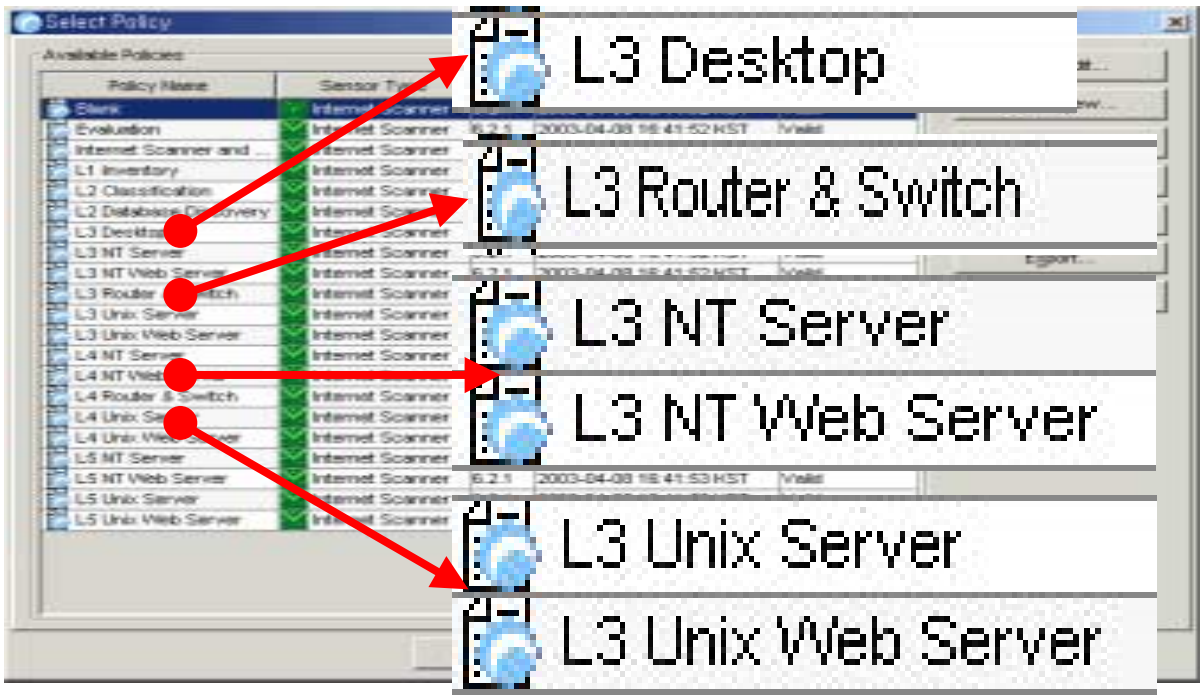


IV. 보안 강화(Hardening)

5. Scanner (계속)

- **정보시스템에 맞는 취약성 점검 정책**

  현재 정보시스템이 가지고 있는 보안 취약성을 파악하기 위해서는 정보시스템 타입에 특화된 정책을 적용하여 관리하는 것이 필요함

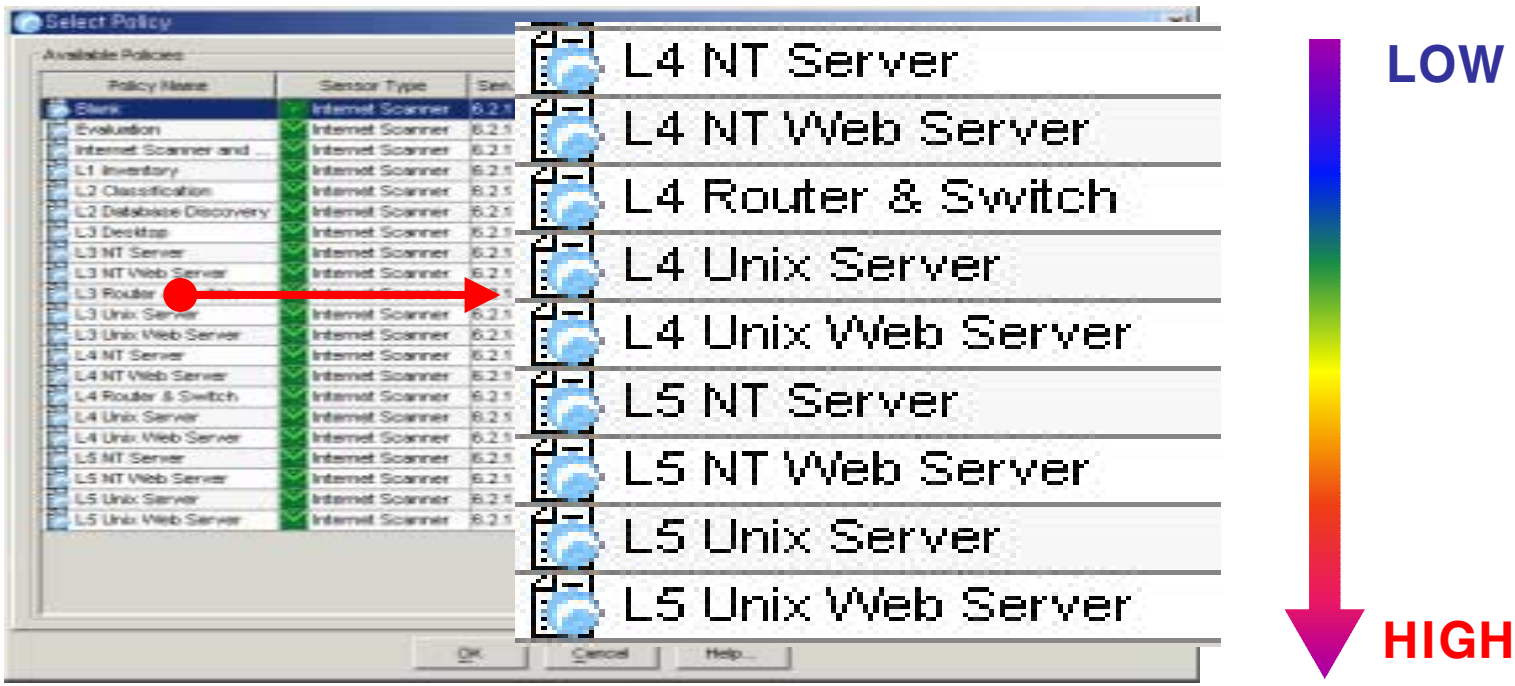


IV. 보안 강화(Hardening)

5. Scanner (계속)

- **취약성 점검 수위에 따른 정책**

다수의 정보시스템에 대한 보안 취약성을 점검하는 수위는 점검 주기, 점검 소요시간, 관리자 기대치 등에 따라 유동적으로 적용할 필요가 있기 때문에 점검 수위를 조절해야 함



IV. 보안 강화(Hardening)

5. Scanner

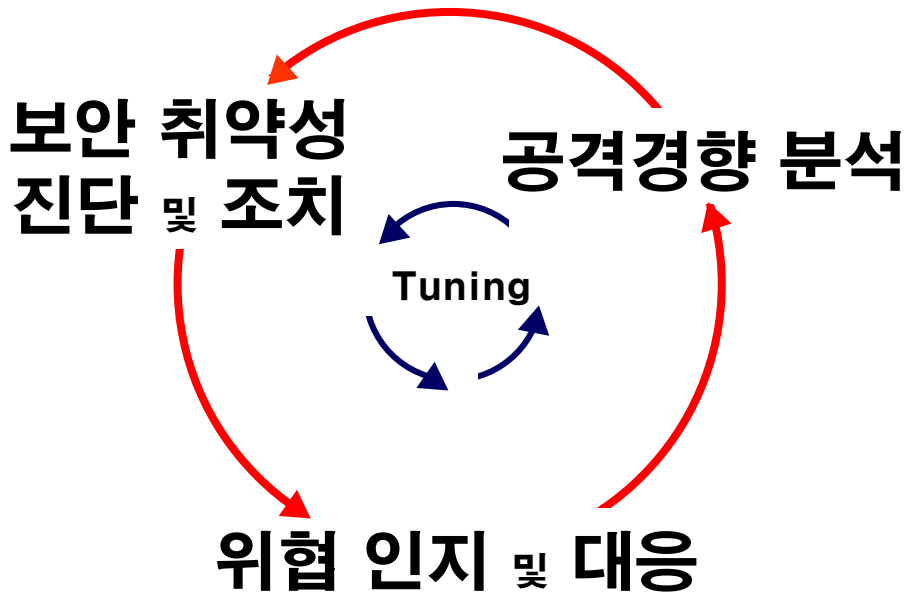
- **취약성 점검결과에 따른 조치**

Scanner를 이용하여 나온 정보시스템의 보안 취약성 점검 결과를 살펴보고, 그에 해당되는 조치 권고 사항을 인지하여 적용여부를 결정할 필요가 있음

조치 권고안

V. 관리 및 보호

- 효과적으로 기업 정보시스템을 보호하고, 지속적으로 정보보호 수준을 높은 수준으로 유지하기 위해서는 "보안 취약성 진단"을 수행하여 "자산이 가지고 있는 취약성"에 대한 "위협을 인지하여 대응"하여야 함
- 또한 위협(공격)에 대한 경향 파악/분석하여 "사전 예방활동"을 수행해야 함
- 이를 반복하여 "Process Tuning"을 계속 수행해야 함



V. 관리 및 보호

1. 보안취약성 진단 및 조치 (계속)

- 보안 취약성 진단이란 ?

  정보시스템이 지니고 있는 보안상의 문제점 파악하고 내/외부 침해행위로 인하여 발생할 수 있는 위험 수준을 진단하는 작업

- 왜 정기적인 정보시스템 보안 취약성 진단을 수행해야 하는가 ?

  - 사전에 침해사고를 예방할 수 있는 적극적 행위 (Pro-Activity)

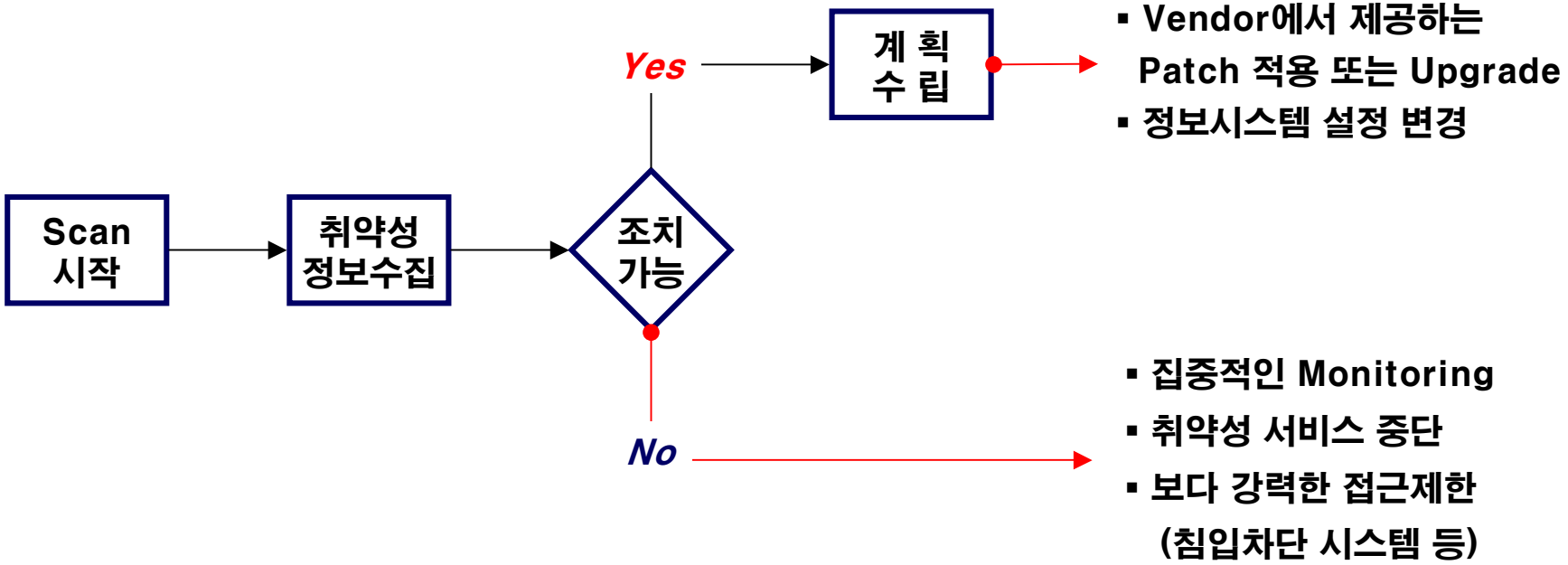
    Anti-Virus 제품 : 웜/바이러스와 같은 침해행위를 할 수 있는 악성프로그램에 대한 사후 조치 프로그램(제품)

  - 정보시스템의 가용성(Availability) 및 무결성(Integrity) 추구의 방법

V. 관리 및 보호

1. 보안취약성 진단 및 조치

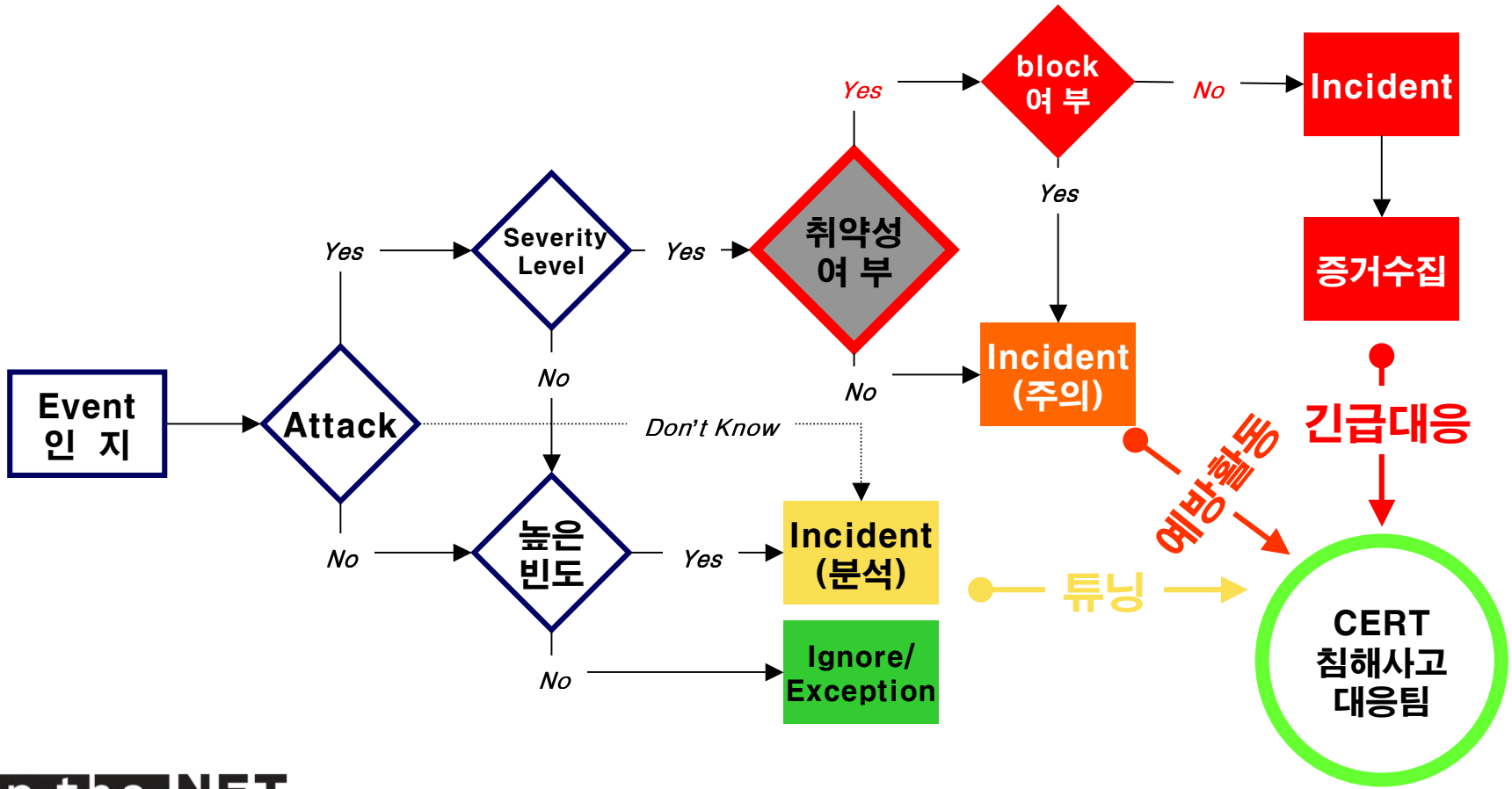
- 기업 정보시스템의 운영 환경에 맞게 "보안 취약성 진단 주기"를 적정수준으로 조정하여 지속적으로 취약성 정보를 관리해야 함



V. 관리 및 보호

2. 위협인지 및 대응 (계속)

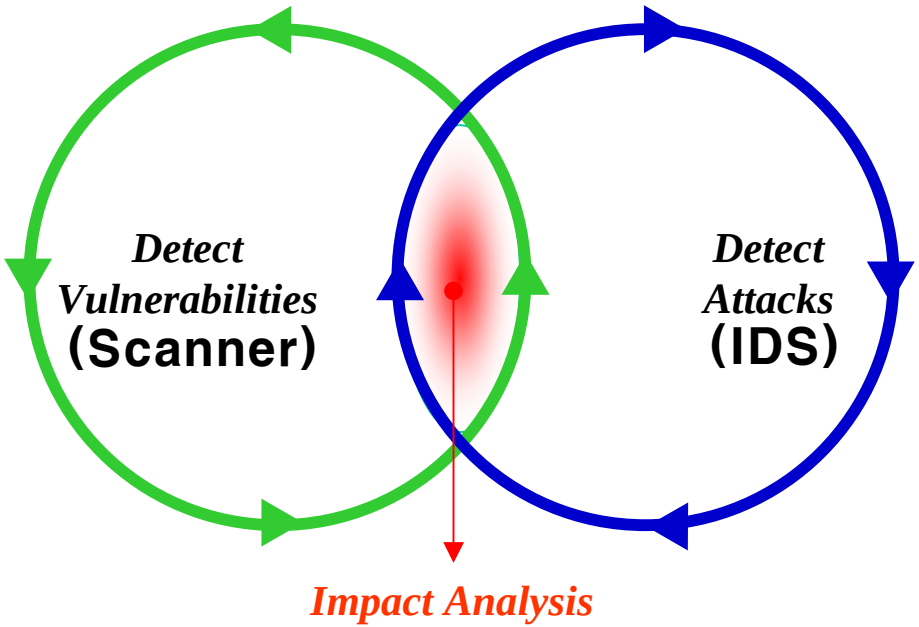
- 아래와 같은 절차로 "위협 인지 및 대응 업무"를 수행함



V. 관리 및 보호

2. 위협인지 및 대응 (계속)

- 단순한 “Attack” 탐지가 아닌 “Impact Analysis”가 핵심
- “정보시스템에 존재하는 취약성”을 파악한 후, 해당 “정보시스템의 취약성에 대한 공격”을 탐지하여 Attack에 대한 Impact Analysis를 수행 함



V. 관리 및 보호

2. 위협인지 및 대응

- 명확한 Impact Analysis를 통하여 "정확한 사건인지"를 하며 그에 대한 "조치방안"을 제시하여 간단 명료한 사건처리 가능

Time	Source IP	Target IP	Tag Name	Status	Severity
2003-03-03 15:00:00 KST	192.168.117.34	192.168.117.39	smtp-expn	Failure likely (no vulnerability)	Medium
2003-03-03 15:00:00 KST	[illegible]	[illegible]	[illegible]	[illegible]	High
2003-03-03 15:00:00 KST	192.168.117.24	192.168.117.39	solaris-ftp-shadow-recovery	Success likely (target vulnerable)	Medium

조치방안

V. 관리 및 보호

3. 공격 경향 분석 (계속)

A1. 최근 발표된 보안 취약성은 무엇인가 ?

A2. 정보시스템에 발견된 보안 취약성 증감 변화가 있었는가 ?

A3. "A1" 취약성에 대한 공격들은 있었는가 ?

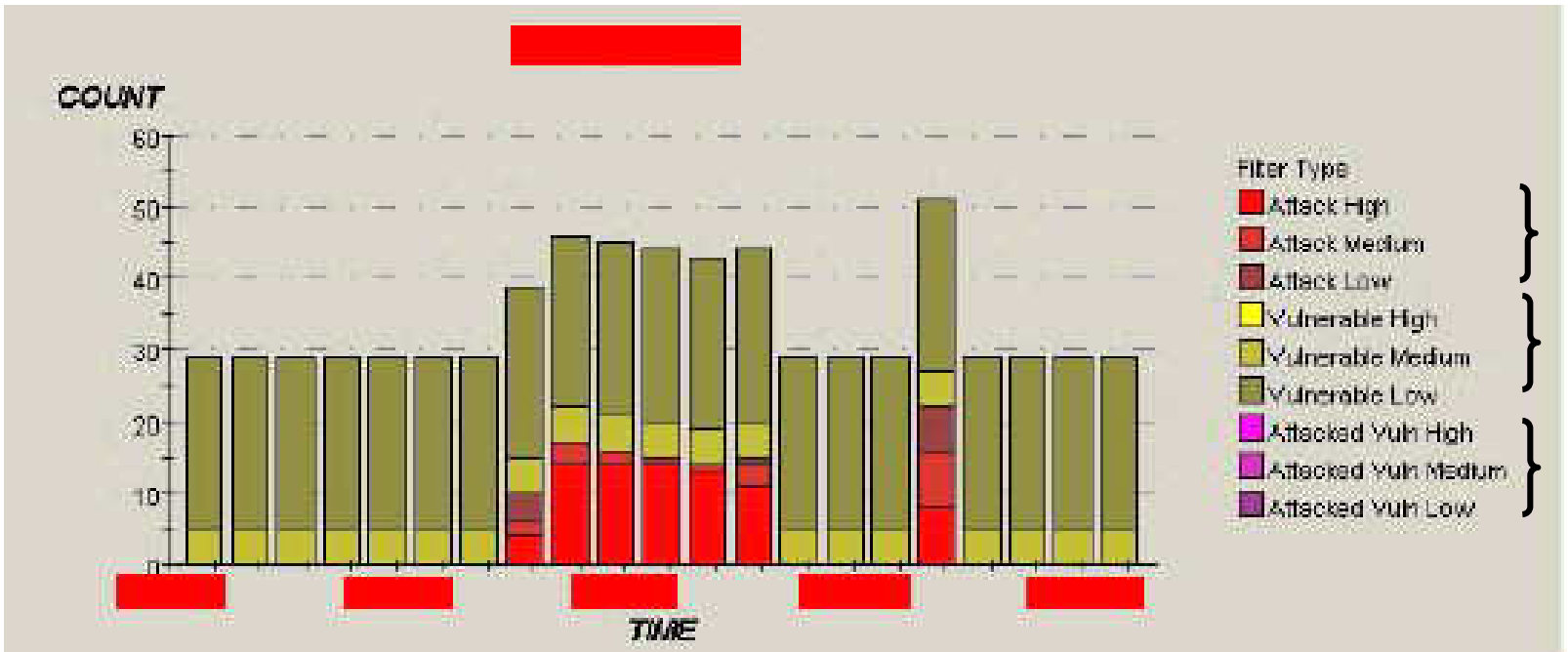
A4. 높은 빈도의 공격은 어떠한 것이며, 어떤 변화가 있는가 ?

A5. 높은 빈도의 공격자는 누구이며, 해당 공격지로부터 공격은 어떠한 것인가 ?

V. 관리 및 보호

3. 공격 경향 분석 (계속)

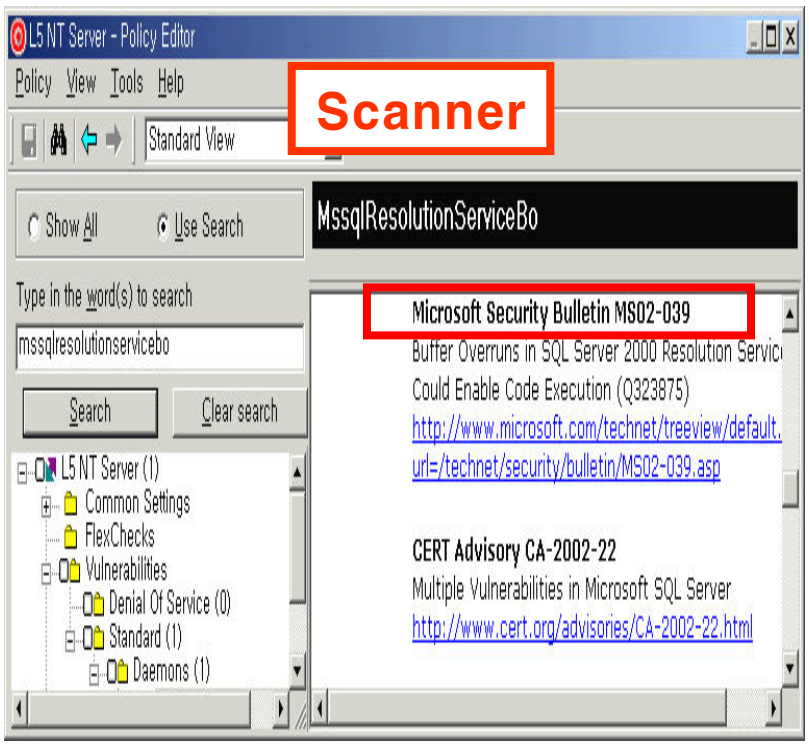
- 아래의 표와 같이 시간에 따른 공격 성향, 정보시스템 취약성 개수 그리고 취약성에 대한 공격 성향 등을 분석할 수 있음

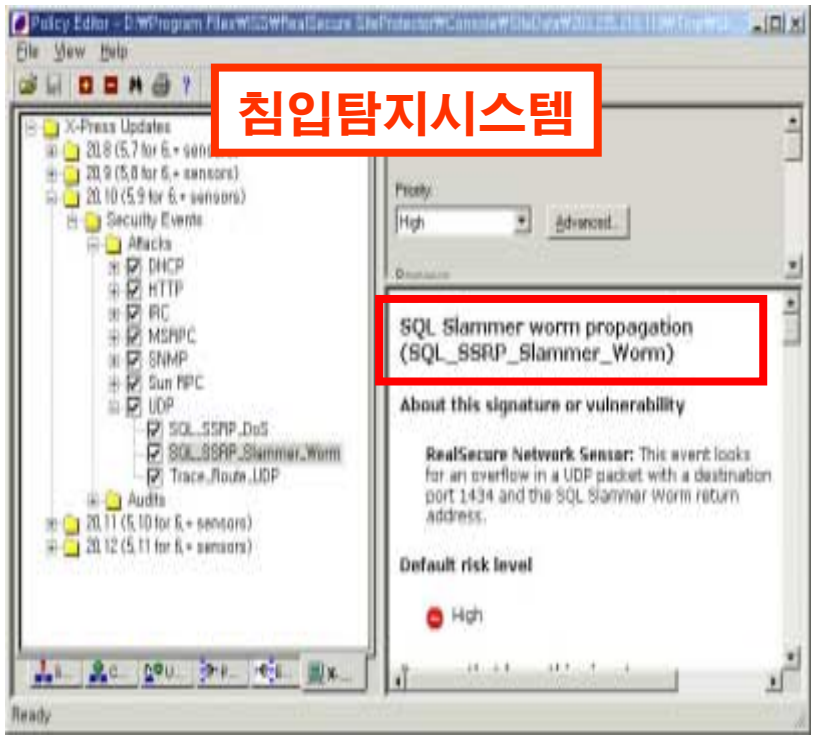


V. 관리 및 보호

3. 공격 경향 분석

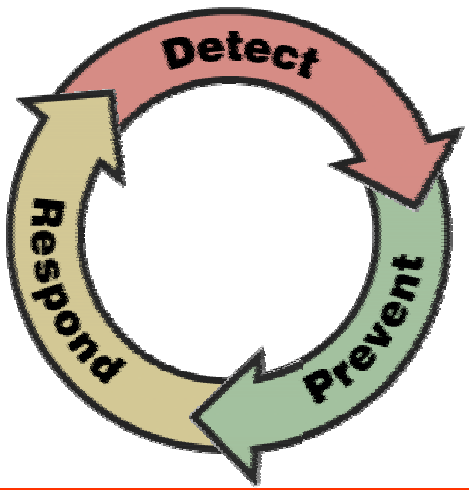
- 최근 발견된 취약성이 정보시스템에도 존재하는지 점검할 필요가 있으며, 취약성에 대한 공격 탐지 방법 및 대응 조치방법까지 파악하는 것이 필요 (Example : Slammer)
  - Scanner : 취약점 정보 Update, 침입탐지시스템 : 공격 Signature Update





VI. 결 론

- 기업 정보시스템을 안전하게 보호하기 위해서는 체계적인 보안정책이 필요함
  - 네트워크/시스템 운영자 및 보안운영조직 간의 명확한 Role & Responsibility 정립
- 하나의 보안솔루션으로 모든 보안 위협 요소에 대해서 해결할 수 없음을 인지하며 여러 보안솔루션을 통합해 운영하는 Know-How가 필요함
- 계속해서 발생하고 있는 위협(공격)에 대해 탐지(Detect), 대응(Respond), 예방(Prevent) Activity를 24시간 365일 지속적으로 수행해야 할 필요가 있음
  - 전문 보안 기술자에 의한 관리 (Outsourcing)



VI. 결 론

- '보안'을 단순히 기술적 문제로 판단하면 안됨
  - IT담당자의 꾸준한 보안패치 설치, 확인되지 않은 사람들에게는 내부의 정보를 제공하지 않는 것, 개인의 e-mail이나 PC의 보안에 주의를 기울이는 것
- 다양한 위험 시나리오를 분석하고 관련된 위험 측정
  - 다양한 침입 시나리오를 통한 보안의 위험 측정 및 보안에 대한 효과분석과 우선순위 설정 및 위험에 근거해 우선순위 대책을 수립해야 함
- 주기적인 평가와 측정 그리고 지속적인 관리
  - 주기적인 평가와 측정을 통해 보안수준이 어느 정도 상승했는지, 보안위험이 어느 정도 감소했는지 측정하고 이러한 보안활동이 지속성을 유지할 수 있도록 해야 함
- 조직내의 동의와 참여
  - 보안활동의 궁극적인 목표는 "강력한 보안 시스템 구축' 이 아니라 모든 임직원의 총체적인 동의와 참여를 통한 '자연스러운 보안문화 정착'을 시켜야 함