情 報 保 護 學 會 誌
第 15 卷 第 1 號, 2005. 2

조기 경보와 위협관리

채 현 주*

요 약

웜, 바이러스, 해킹 등 아직 일어나지 않은 사이버 위협을 예측하여 조기 예·경보를 통해 능동적으로 방어할 수 있는 위협관리시스템(TMS; Threat Management System)이 보안업계의 새로운 관심분야로 떠오르고 있다. 본 논문에서는 이 위협관리시스템의 개념과 기능에 대해 설명하고, 이를 통한 조기 경보의 방법을 논의하고자 한다.

Ⅰ. 서 론

인터넷은 정보통신기술의 발전과 더불어 사회 전반적인 분야를 크게 변화시키고 있으며 일상생활의 필수 요소로 자리잡게 되었다. 그러나, 현재의 인터넷은 정보 공유나 생산성 향상과 같은 순기능 이외에도 1.25 대란과 같은 사이버 테러나 개인정보를 악용한 사이버 범죄로의 악용이라는 양면성을 보여주고 있다.

이러한 현재 사이버 위협은 점차 복잡하고 지능적으로 진화하고 있으며 공격기법이 다양해지고(Blended Attack) 네트워크 서비스 가용성에 대한 위협이 증대되고 있다. 즉, 위협의 파괴력이 커지고, 피해 범위가 넓어짐에 따라 이에 대응하는데 제약이 많아진다.

기존의 보안 솔루션들은 알려진 공격에 대해서만 대응이 가능하기 때문에 제로 데이 위협에 대해 처리할 수 없는 단점을 갖는다. 결국은 이 위협이 확산돼, 네트워크 장애나 트래픽 폭증 등의 현상이 나타나기 전까지는 인식하기도 어려운 경우가 발생한다. 제로 데이 공격은 취약점에 대한 패치, 탐지와 차단 패턴이 개발되고 배포되기 전에, 이 취약점을 이용한 공격이 실행되는 위협을 의미한다.

또한, 최근 웜이나 바이러스는 기술적인 공격 제약을 극복하기 위해 피싱(Phishing)과 같은 사회공학적인 방법을 사용하므로 탐지를 위한 패턴을 정의할 수 없다. 이 같은 이유로 사이버 위협에 대처하기 위해 새로운 보안 개념들이 연구되고 있다. 사이버 위협

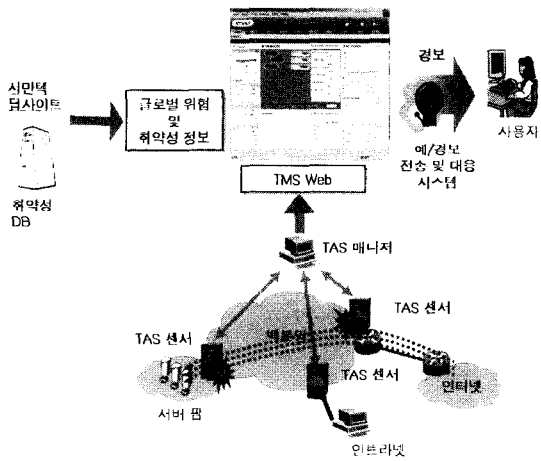


그림 1. 위협관리시스템의 구성도

에 효과적으로 대처하기 위한 새로운 보안 개념들은 다가오는 위협을 조기에 감지하고 발생한 위협을 완화하거나 확산을 막고, 피해를 최소화 하는 것이 궁극적인 목적이다. 그 중에 가장 대표적인 시스템이 바로 위협관리 시스템(Threat Management System)이다.

위협관리 시스템은 보안에 대한 새로운 방향성을 가지고 보안 위협에 대응한다. 첫째는 기술과 정보를 융합시켜 단위 솔루션이 갖는 한계를 극복하는 것이고, 둘째는 관리의 방향이 자산이 아닌 위협으로 향하고 있다.

2장에서는 위협관리 시스템의 필요성과 기능 등에

* 정보보호 기술 취약성 분석팀 (nunchuk@infosec.co.kr)
한국정보보호학회 조기경보시스템연구회 WG02 "사이버 공격수준 평가 및 경보단계 운영" 운영자

대해 서술하고 3장에서는 조기 경보와 관련된 위협관리 시스템의 기능을 중점적으로 논의할 것이다. 4장은 위협관리 시스템의 구축 사례를 통해 실제 위협관리가 어떻게 활용되는지 살펴볼 것이다.

II. 위협관리시스템의 개요

위협관리 시스템은 이미 알려져 있거나 알려지지 않은 공격에 대하여 조기에 감지하고, 발생한 위협을 완화시키거나 확산을 막고, 피해를 최소화 할 수 있도록 지원한다. 위협관리 시스템은 잠재적인 위협의 발견, 위협의 활성화, 위협의 확산에서 소멸 단계까지 위협에 대한 라이프 사이클을 관리한다. 또한, 신규 취약점과 웜 바이러스와 같은 악성코드 그리고 글로벌 위협 정보를 수집하고 로컬의 침입 탐지와 이상징후 탐지 결과를 종합하여 '잠재적인 위협', '활성화된 위협'(Active Threat), '상승하는 위협', '감소하는 위협' 등으로 분류하여 적절한 대응에 필요한 의사결정을 지원한다.

위협관리 시스템은 필요에 따라 자동화되고 능동적인 대응 수단을 제공하기도 하지만, 많은 제로 데이 위협의 경우 사람이 막아야 하는 현실을 고려하고 있다. 또한 위협관리 시스템의 관리 대상은 위협 그 자체로, 네트워크 자산이나 보안시스템으로 보는 NMS (Network Management System. 네트워크의 전반적인 상황을 모니터하고 문제점을 알려주는 기능을 수행하는 소프트웨어나 하드웨어)나 ESM(Enterprise Security Management. IDS 방화벽, VPN 등 각종 네트워크 보안 제품의 통합 관리와 개별 침입에 대한 종합적인 대응을 위한 통합보안 관리시스템)과 분명히 다른 방향성을 가지고 있다.

본 장에서는 위협관리 시스템의 구성과 구현 방법에 관하여 서술한다.

1. 위협관리 시스템의 방향

위협관리 시스템은 '예측성', '적시성', '신뢰성', '적합성'에 맞게 구성된다. 사람은 스스로 자신의 인프라에 미칠 외부의 위협을 감지하거나 분석할 수 없다. 따라서 위협관리 시스템은 외부로부터 미칠 위협에 관한 국내외 각종 정보들과 실제 위협관리 시스템의 보호 대상 인프라에 미치는 영향을 상호 연관 분석해 현재 그리고 앞으로 다가올 위협을 예측할 수 있어야 한다.

위협관리 시스템은 네트워크에 영향을 주는 위협을 포착한 순간 적시에 위협 경고를 관리자에게 전달해 관리자로 하여금 적절한 조치를 위할 수 있도록 한다. 이는 위협이 나타나는 시기를 판단하고 대형 사고로 전이되는 것을 방지하는 것이다.

2. 위협관리 시스템의 구현

현재 개발 완료된 위협관리 시스템은 인터넷 웜, 바이러스, 해킹 등의 사이버 공격에 대한 침입탐지, 트래픽 분석과 상관관계를 분석해 종합적인 '위협분석시스템(Threat Analysis System), '글로벌 위협정보 및 취약성 정보', '조기 예경보 전송 및 실시간 대응 시스템'을 통합하는 체계적인 사이버 위협에 대한 관제 및 대응 기능을 제공한다.

2.1 위협의 분류

위협관리 시스템은 시점에 따라 위협을 조직 인프라에 아직 비활성화된 위협과 이미 활성화된 위협 등의 두 단계로 구분한다. 비활성화 위협은 새로운 취약점이 발견되고 이를 이용한 악성코드가 출현해 보안사고가 발생하는 등 아직까지 조직 인프라에는 영향을 주지 않지만 급박하게 발생할 수 있는 위협으로, 다가오는 위협 또는 잠재적인 위협이다.

글로벌 위협은 이와 같이 아직 활성화되지 않았지만 다가오거나 잠재적인 위협을 총칭하며, 로컬 위협은 실질적으로 조직에 유입되는 위협을 말한다. 대부분의 사이버 공격은 국내가 아닌 해외로부터 유입되기 때문에, 국내 유입 초기 또는 조직 인프라에 유입되기 이전에 사전 탐지한다면, 효과적으로 위협을 완화시킬 수 있다. 이런 측면에서 글로벌 위협에 대비하기 위한 조기 경보 체계는 위협을 완화하기 위한 위협관리 시스템의 핵심 기능이다.

2.2 위협관리시스템의 구성

위협관리 시스템은 조직 내의 네트워크 위협을 탐지하고 탐지된 이벤트를 분석하는 '위협분석시스템', 위협분석 결과 예경보를 담당하는 '예경보와 대응시스템', 그리고 조직 외부의 글로벌 위협 정보를 수집하는 '글로벌위협 정보 수집 시스템' 등 4가지로 구성된다. 각 구성요소들은 정보 공유를 통해 네트워크 상태와 위협분석 결과를 효율적으로 전달하게 된다.

2.2.1 위협분석시스템

위협분석시스템은 네트워크의 모든 트래픽을 실시

간으로 모니터링하여 공격 시도를 탐지한다. 탐지 센서는 네트워크에 미치는 영향을 최소화하여 설치되며, 각종 해킹 탐지, 비정상트래픽 탐지, 이벤트 탐지 기능이 있다. 위협분석 시스템은 탐지 기능 이외에 탐지된 대량의 이벤트를 축약하고 분석하여 예경보 대응 시스템으로 정보를 전송한다.

2.2.2 글로벌위협 정보 수집 시스템

글로벌위협 정보 수집 시스템은 아직까지 활성화되지 않은 잠재적인 위협 정보를 수집하는 시스템이다. 국내외 신종 바이러스의 출현이나 최신 해킹기법, 보안 취약점이 발표되면, 그 취약점 유형을 분류하고 위험도를 산정해 피해가 우려될 경우 예경보 대응 시스템으로 정보를 전달한다.

2.2.3 예경보와 대응시스템

'예경보와 대응시스템'은 글로벌 위협 정보와 로컬 네트워크에서의 위협 분석 정보를 종합적으로 활용하여 예보 및 경보를 지원한다. 예경보 방식으로는 전자 메일이나 SMS(단문 메시지 서비스) 등을 이용하고 있다.

Ⅲ. 위협관리의 핵심, 조기 경보와 실시간 분석

1. 위협을 완화하기 위한 조기 경보 체계

위협관리 시스템을 통한 조기 예경보 기능을 살펴보기에 앞서, 조직 인프라 보호를 위한 조기 경보 체계는 최근 들어 필수적인 요소이다. 조기 경보 체계는 위협이 조직 인프라에 임박하기 전에, 위협을 인지하고 방지한다는 차원에서, 보다 능동적인 대응 방법이다. 정보보호 홈페이지에서 정보보호 동향, 논문, 보고서, 패치 및 업데이트 프로그램 등을 수집하고, 바이러스 백신업체와는 바이러스 예·경보(신규 바이러스, 웜 정보 백신 업데이트 및 패치)를 실행하며, 국내외 CERT (Computer Emergency Response Team), ISAC (Information Sharing & Analysis Center)와 침해사고에 대한 협력(해킹사고, 신규 해킹기술 공유) 등 다양한 방법으로 위협 징후 발견을 위한 능동적인 정보 수집이 필요하다. 임박한 위협을 인지하기 위해서, 조직 인프라에 유입될 수 있는 주요 구간에서 보안 이벤트와 트래픽 정보를 수집하고 분석하는 것이 필수적이지만, 이 같은 조직의 인프라를 감시하는 수동적 차원의 단독대응을 넘어서, 수직, 수평 조직 간에 연계를 통한 공동 대응이 필요하다. 독자적인 조기 경보 체계를 구축하기 어려운 일반 기업의 경우, 기업 CERT나 국내외 ISAC에 편입해, 각종 위협 정보를 공유하는 방법, 공동 대규모 관제센터 또는 글로벌 보안 업체들과 상시 정보를 공유하는 예·경보 서비스를 받는 방법 등을 선택할 수 있다. 참고로, 정부 차원에서는 이미 국가정보원 산하 국가사이버안전센터, 국방부 산하 국방정보전대응센터, 정보통신부 산하 침해사고대응지원센터 등 3개 센터를 두고 있다. 또한 한국(KRCERT), 중국(CNCERT), 일본(JPCERT)이 상호 연계해 활동하고 있으며 미국, 호주 등을 포함한 APEC 회원국으로 상호 연계 범위를 점차 확대하고 있다. 이외에도 보안 업체 중 시만텍은 전 세계 180여 개국의 2만여 개의 딥사이트(DeepSight) 센서들을 통해 수집된 정보를 분석해 신속한 조기 경보 서비스를 제공하고 있다. 국내외 신종 바이러스의 출현이나 최신 해킹기법, 보안 취약점이 발표되면, 그 취약점 유형을 분류하고 위험도를 산정해 피해가 우려될 경우 예보를 발령한다. 국내외 사이버 피해가 발생하거나 조직 인프라에서 이상징후 탐지 또는 피해 상황이 접수될 경우, 상황을 종합, 분석해 단계에 맞는 경보를 발령한다.

2. 핵심 위협 분류로 시작하는 이상징후 탐지

조직의 인프라에 해를 끼치는 위협이나 활성화된 위협을 조기에 차단하거나 완화시키기 위해서는, 네트워크 이상징후 탐지와 이를 분석해 우선적으로 처리해야 할 핵심 위협을 분류하는 작업은 매우 중요하다. 이상징후 탐지는 아직 알려지지 않은 위협을 탐지하기 위한 수단으로, 일정한 패턴을 가지고 탐지할 수 없다.

정의되지 않은 이상징후를 탐지하기 위해서 네트워크 트래픽과 이벤트 분석을 통해 네트워크의 상태 변화를 감지해야 한다. 이상징후 탐지 기준을 위해서 요일별, 시간대별 이벤트 및 트래픽 특성을 고려해 기간별 네트워크 상태 추이를 예측해 프로파일을 생성한다.(그림 2 참조) 이상징후 탐지 기능은 실시간으로 이벤트와 트래픽이 프로파일에 정의된 정상 행위 패턴과 비교해 이상징후 여부를 판단한다.

일반적으로 최신 취약점이나 웜이 전파되는 과정에서 또는 웜의 감염으로 생성된 백도어 포트로부터 트래픽이 생성된다. 백도어 포트는 주기적인 접속 시도 또는 감염 경로 포트로 사용되기 때문에 이 같은 트래픽 분석을 통해 네트워크 사용 상황을 파악함으로써

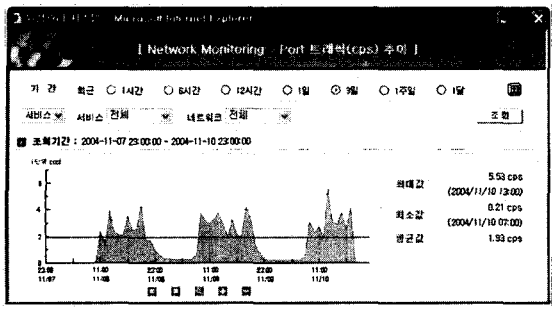


그림 2. 주기별로 특정한 패턴을 갖는 네트워크 트래픽

상태 변화를 감지할 수 있다. 또한 조직 인프라에 발생한 이벤트들 간에 '유형별', '포트별', 'IP별' 상관관계 분석을 통해 이상징후를 감지할 수 있다. 그림 3은 공격 유형별 통계 분석을 통해, 새롭게 증가하는 이벤트, 상승하거나 감소하는 이벤트를 분류해 네트워크 상태 변화의 징후를 분석한 결과다. 발생한 이벤트가 정확한지 아닌지는 중요하지 않다. 극단적으로 오탐지 이벤트가 평상시에 단위시간당 100여 개 발생하던 것이 1000여 개로 증가했다면, 분명한 네트워크 상태 변화의 징후로 간주하고 심층적인 분석이 필요하다는 뜻이다. 또한 발생한 이벤트들로 인한 유해 트래픽을 산정해, 이로 인한 네트워크에 대한 영향을 파악하는 것도 중요하다.

3. 상관 분석을 통한 위협 분석

이상 징후가 발생하면 신속한 위협 분석을 통해, 원인 분석과 위협이 조직 인프라에 미치는 영향을 분석해 위협을 차단하거나 완화하는 조기 경보 대응 방안을 수립해야 한다. 특정 취약점을 이용하는 이벤트가 증가하는 이벤트 이상징후의 경우, 동일 취약성을 이용한 새로운 변종이 발생할 가능성을 분석해야 하고, ICMP/서비스 스캔이 비정상적으로 증가하는 경우 정의되지 않은 웜이 확산될 가능성 여부를 파악할 필요가 있다. 위협관리 시스템은 신속하고 정확한 위협분

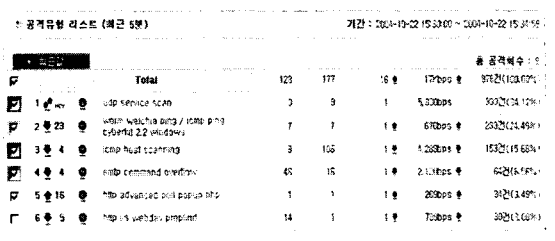


그림 3. 실시간 이벤트 통계 분석

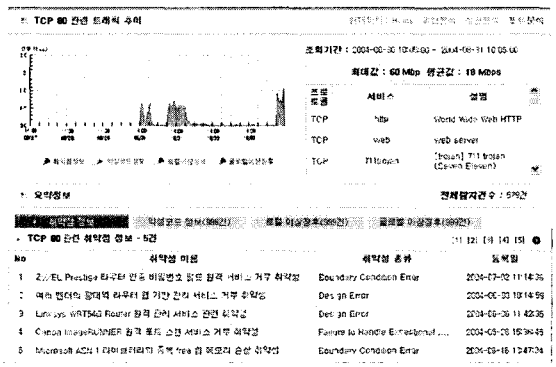


그림 4. 포트 분석 화면

석을 위해서, IP 중심의 상관 분석과 서비스 포트 중심의 상관 분석 및 판단이 가능한 직관적인 사용자 인터페이스를 제공한다.

- IP 중심의 상관 분석 : 이상징후를 발생시키는 IP를 중심으로 해당 IP 관련 이벤트와 트래픽 발생 이력, 블랙리스트 등록 여부 등을 상관 분석 기능을 제공한다.
- 서비스 포트 중심의 상관 분석 : 이상징후 발생 포트를 중심으로 글로벌 취약점, 악성코드, 침입탐지 이벤트간의 상관 분석 기능을 제공한다.

위협관리 시스템은 필요에 따라, 보다 상세한 이상징후의 원인 분석을 위해서 프로토콜, 서비스, 프레임 크기, 유해 트래픽, 비정상 트래픽들을 분석할 수 있는 트래픽 분석 기능, 공격유형별, 공격 IP별, 피해 IP별 이벤트 분석 기능과 트래픽 패킷 단위로 분석할 수 있는 기능 등 다양한 분석 기능을 제공한다.

Ⅳ. 위협관리시스템 구축 사례

위협관리시스템의 개념과 필요성은 1.25 대란 직후부터 대두됐고, 그 이후로 정부 CERT 기관이나 ISP와 같이 사이버 위협이 발생했을 때 초기에 빠르게 대응이 필요한 기관들을 중심으로 수요가 확산되고 있다. 현재 행정자치부, 정보통신부 등을 포함한 주요 정부 중앙 부처들, 공공 및 민간 CERT 기관들과 대형 ISP가 위협관리시스템 또는 조기 예·경보 시스템의 형태로 운영되고 있거나, 구축 사업을 진행하고 있다.

최근에는 대형 ISP와 공공 분야 뿐만 아니라 인터넷 환경에 민감한 비즈니스 모델을 가진 기업을 중심으로 그 수요가 확대되고 있다. 본 장에서는 대형 웹

포털 서비스 업체인 K사의 구축 사례를 통해 위협관리시스템의 활용사례를 살펴본다.

1. 위협관리의 도입

대형 포털 서비스 업체인 K사는 웹 포털 서비스를 제공하고 있다. 많은 사용자가 접속하는 네트워크에는 대용량 트래픽이 항상 흐르고 있어 빠른 감염 속도로 네트워크에 영향을 미치는 웜, 바이러스, 봇(Bot) 등에 의한 DoS(Denial of Service), 대량 전자우편을 통해 전파되는 다양한 위협들로부터 서비스 가용성을 확보해야 한다.

따라서 기존 보안 솔루션에서 제공할 수 없었던 프로토콜, 포트, 프레임 크기 등 정상 트래픽과 유해 트래픽을 상세히 분석할 솔루션과 분석한 정보를 기반으로 글로벌 위협 상황과 내부 서비스 네트워크로 유입되는 유해 트래픽 등 로컬 위협 상황을 비교 분석해 빠르게 의사 결정할 수 있는 분석시스템도 필요했다.

K사는 번번히 발생되는 위협 상황을 빠르게 분석하고 예경보하기 위해 위협관리시스템을 도입하였다. 또한 주요 사업인 웹 포털 서비스의 위협분석 목적뿐만 아니라, URL, IP 그룹에 대한 트래픽을 분석하고 해당 정보를 기반으로 시스템 확장과 같은 정책 결정에 활용할 계획을 갖고 프로젝트를 추진했다.

K사에서 도입한 위협관리시스템은 위협분석 센서 5식과 위협분석 통합 매니저 1식, DBMS, 위협관리시스템 웹 서비스 등으로 구축되었다. 위협분석 센서들은 인터넷에 연결된 6개의 기가비트급 회선에 탭(TAP) 장비를 연결하고 해당 패킷을 로드밸런싱해 패킷을 수집하고 분석처리할 수 있도록 했다. 위협분석 통합 매니저는 위협분석 센서들에서 수집된 정보를 이용하고 트래픽 통계와 이상징후 탐지에 사용한다.

2. 트래픽 사용량 분석을 통한 조기 경보

초기 도입 설치 후 내부 네트워크의 유해트래픽 발생량과 각 포트별 트래픽 사용량을 분석해, 프로파일을 작성하고 이상징후 탐지에 적용할 수 있도록 했으며, 내부 네트워크에서 발생되는 웜·바이러스 등을 파악하고 조치할 수 있도록 구축되었다. 그 밖에도 K사가 웹 포털 서비스가 주요 사업임을 감안해 특히 웹 트래픽 분석 기능을 특화하여 'URL', 'IP 그룹별' 트래픽 분석 기능을 강화하였다.

URL 분석 기능은 각종 침입 이벤트와 트래픽 분

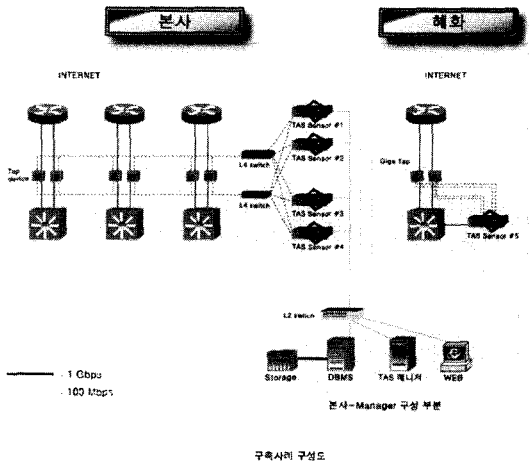


그림 5. K사 위협관리시스템 구성도

류를 URL별로 상세히 분석할 수 있어 위협 분석 뿐만 아니라 현재 서비스에 대한 가용성도 분석할 수 있고, CPS(Connection Per Second) 분석을 통해 현재 URL별 접속량도 분석한다. 넷스카이와 같은 대량 메일 전송 웜·바이러스를 탐지하고, 웹 로그인 브루트포스(Web login bruteforce) 공격 등으로부터 안전하게 포털 서비스를 운영하기 위한 주요 기능이 통합돼 있다.

V. 결 론

어떤 보안 솔루션도 완벽한 보안을 이뤄낼 수는 없다. 한 예로 바이러스 백신을 보면, 생물학적 바이러스와 사이버 바이러스는 유사점을 많이 가지고 있다. 사스(SARS), 조류 독감, 에볼라, 에이즈 등 아직 완전한 백신이 없는 생물학적 바이러스에 대한 대응을 백신에 의존할 수 없는 현실이다. 따라서 바이러스의 확산 정도, 확산 지역 등에 대한 정보를 기반으로 격리, 방역 등의 조치로 대응할 수 밖에 없다.

사이버 바이러스도 이와 크게 다르지 않다. 한 달 동안 400건 이상 신고되는 신종 및 변종 바이러스를 기존 백신 소프트웨어가 모두 탐지하기 어렵고, 특히 사회공학적 공격에는 대응할 수 없다. 이렇듯 기술(Technology)와 정보(Information)가 상호 보완적으로 결합돼, 활성화된 위협의 형태, 원인, 네트워크 상태 및 현상에 따라 적절하게 보안 수단을 적용할 수 있도록 의사 결정 수단을 제공해야 한다.

위협관리 시스템은 실질적으로 기술은 제품(Product 또는 Solution) 형태로, 정보는 서비스(Ser-

vice) 형태로 구체화시키며, 이를 융합시켜 목적을 이룬다. 실제로 위협관리의 생명력은 기술과 정보의 적시성에 있다. 위협으로 인해 내부에 발생하는 이상 징후나 상태변화를 조기 감지할 수 있어야 하고 활성화된 글로벌 위협정보의 신뢰성과 신속함이 있어야 유지할 수 있다.

위협관리 시스템이 조기에 확산될 수 있었던 가장 큰 원인은 현재의 상황을 직관적으로 파악할 수 있도록 위협분석의 결과를 형상화시키고 조기 예경보 대응을 통해 운영자의 빠른 판단이 가능하도록 했기 때문이다. 앞으로 위협관리 시스템이 조기 예경보 서비스를 통해 사회 전분야로 확산되어 안전한 정보보호와 네트워크의 지속적인 인프라 보호를 위해 중요한 핵심 요소가 될 것으로 기대한다.

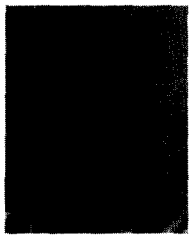
Ⅳ. WG 2 소개

한국조기경보포럼의 WG 2는 사이버 공격수준을 평가하고 경보단계 운영과 관련한 분과이다. 이 분과에서는 전세계의 사이버 공격 수준을 평가하는 방법 및 경보 단계에 대한 벤치마킹을 통해 합리적이고 효율적인 공격 수준 평가 방법론에 대해 연구하며 국내의 보안 위협에 대한 경보단계 운영에 대한 실태 조사 및 장/단점 분석 및 현재 사이버 공격 수준 평가에 있어서의 문제점과 이를 해결하기 위한 방안을 연구한다.

⊙ 연구 방향
- 국내외 조기 예/경보 발령시 이용되고 있는 경보 단계 운영 실태 조사
- 사이버 공격 수준 평가 방법론과 이에 대한 문제점 및 해결 방안 연구
- 공격 수준 평가 및 경보 단계 운영에서의 국내외 산학 협력 방안
- 기타 조기 예/경보와 관련된 논문 및 최근 동향 연구

⊙ 분과 운영
- 월 1회 오프라인 모임 및 온라인 모임을 갖고 연구 주제를 토론
- 희망 과제를 부여하고 자유롭게 발표

〈著 者 紹 介〉



채 현 주 (Chae Hyun Joo)
정회원

1997년 2월 : 동국대학교 컴퓨터공학과 졸업
2000년 8월~2003년 1월 : 정보보호기술 침입탐지시스템 엔진 개발
2003년 1월~현재 : 정보보호기술 취약성 분석팀장
〈관심분야〉 정보보호, 컴퓨터공학