*Total Solution Provider for Information Security*

VECTRA™
Security that thinks.™

# 머신런닝과 데이터 사이언스기반의 CYBER ATTACK 탐지 및 모니터링

## -VECTRA 제품 소개서-

**2016. 06**

wiki
주식회사 위키시큐리티
Information Security Solution Provider

# 보안침해대응 및 보안관제 기술동향

## ➢ 인공지능 기반 위협탐지 및 예측

**침해사고 유사도분석, 유사침해자원 패턴매칭, 네트워크 기반 이상징후 탐지/분석 등 다양한 방식을 통한 침해사고 위협탐지는 많으나 딥러닝, 머신러닝 등 인공지능기반 위협탐지, 예측기술 필요성 대두**

## ➢ 악성코드 게놈프로젝트

**개별 악성코드 자동분석 및 악성코드 간 유사성분석 기술을 연구하여 악성코드 프로파일링 및 대량의 유사 악성코드 그룹 분류기술과 학습기반의 악성코드 분석/분류기술들이 연구되고 있음**

## ➢ 사이버 블랙박스 및 Intelligence분석 프로젝트

**네트워크 트래픽을 수집, 관리 및 무결성 보장기술과 Semantic기반 침해사고 원인분석 및 공격재현 기술, 침해공격 정보연동 및 정보공유기술이 연구되고 있음**

## ➢ 침해사고 역추적 기술

**다중소스 기반의 장기간 침해사고 분석을 통한 특징추출 및 연관된 공격 근원지 탐지/침해사고 원인분석 기술과 공격자 그룹식별 및 자동 역추적 기술이 연구되고 있음**

*) 출처: 2016년 ICT R&D 전략포럼 미래부/IITP

# CONTENTS

SINCE
2010

- 사이버공격 대응전략 대변혁의 필요성
- VECTRA의 진화된 사이버공격 대응전략
- VECTRA가 제공하는 주요기능 및 화면
- VECTRA 제품군과 CASE별 구성방안

wiki
주식회사 위키시큐리티
Information Security Solution Provider

# CONTENTS

SINCE
2010

- **사이버공격 대응전략 전환의 필요성**
- VECTRA의 진화된 사이버공격 대응전략
- VECTRA가 제공하는 주요기능 및 화면
- VECTRA 제품군과 CASE별 구성방안

wiki
주식회사 위키시큐리티
Information Security Solution Provider

# 사이버공격 대응전략 전환의 필요성

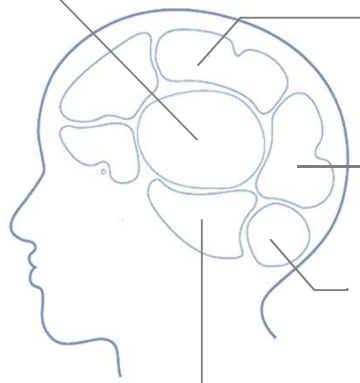
**보안시스템들의 과도한 이벤트**

**시그니처와 탐지룰 기반의 각종 보안시스템들이 띄우는 수많은 보안 이벤트들을 분석하고 판단하는데 한계를 느끼고 계시지 않으십니까?**

## 보안전담조직의 불편한 현실

- 과도하게 발생하는 보안경보로 보안관리자의 보안 이벤트 중요성 인식 저하
- 다양한 단위보안 도구에서 발생하는 다량의 경보와 이벤트에 대한 연관성 파악 부재로 시스템이 어떤 위험에 노출되어 있는지 파악이 용이하지 않음
- 침입탐지 솔루션의 최대 단점인 과도한 false alarm의 발생 및 로그의 발생으로 인해 보안관리자들이 전체 단위보안 솔루션들을 효율적으로 관리할 수 없음
- 보안 도구/콘솔의 독립적인 운영 및 관리로 보안관리자의 생산성 저하
- 단위보안 툴에서 발생하는 로그의 분산 저장으로 감사대비책 미비

## 현재 보안대책 중 가장 어려운 점(2016,아이티비즈)

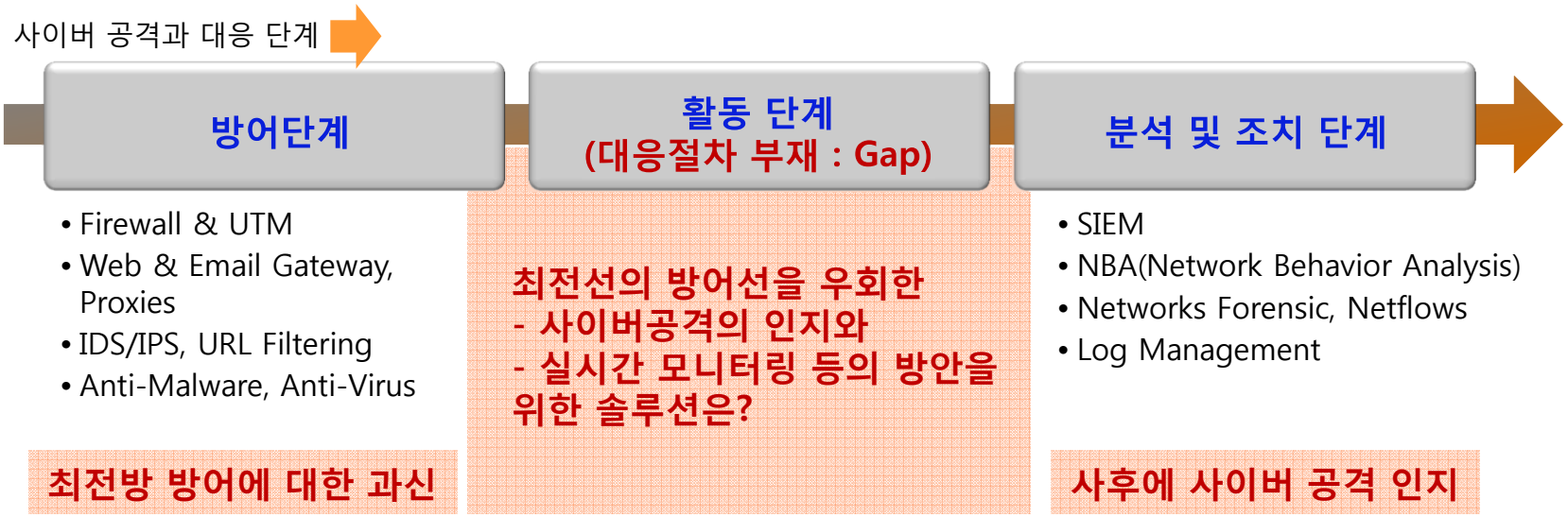


- **26%** 보안기술 및 모니터링인력 부족
- **19%** 문제의 진짜 근본원인 해결을 위한 솔루션 미비
- **18%** 임직원의 보안인식 부족
- **14%** BOYD 등 사이버공격 접점이 늘어나는 기업환경
- **10%** 단 하나의 약점으로도 뚫리는 보안현실

# 사이버공격 대응전략 전환의 필요성

**경계선 보안을 우회한 내부공격**

**Firewall, ESM, IDS/IPS, WAF와 같은 경계선 보안의 우회공격에 성공하여 주변시스템으로 공격을 확장 및 전이하고 있는 내부공격들을 어떻게 탐지하고 모니터링하고 계십니까?**



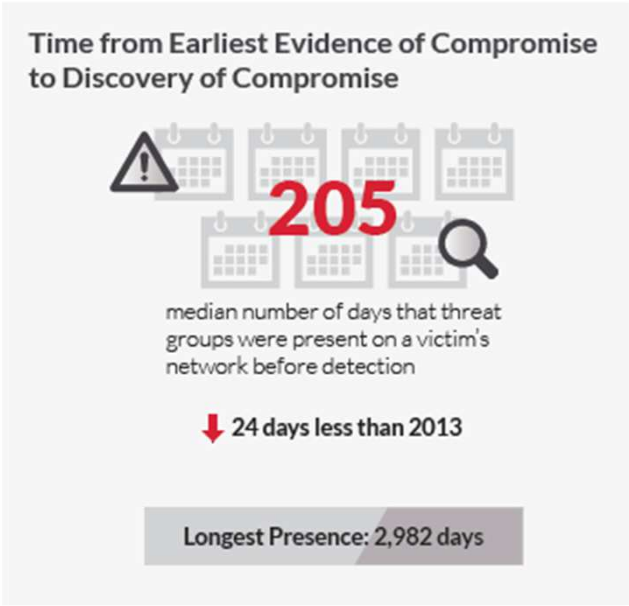

▪ **여러 가지 보안시스템을 갖추고 있지만,**
- **보안 침해사고의 69%는 외부(고객 또는 기관)에서 발견**
- **보안 침해사고의 31%는 내부에서 발견되고 있음**

(*) 출처: 2015, www.mandiant.com

**지속성 공격의 탐지와 예측 필요**

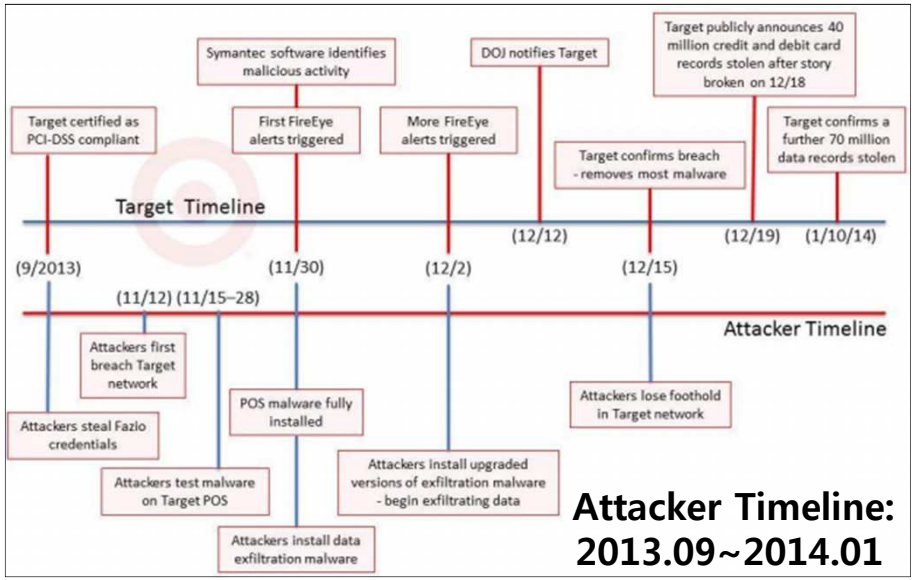
**단편적 공격탐지가 아니라 지속적이고 장기적인 형태의 공격 현황을 탐지하고 이를 시계열적으로 분석하여 향후 공격을 예측할 수 있는 시스템을 갖추고 있습니까?**

**사이버 공격을 발견하기까지 최대 2,982일, 평균 205일 소요**




(*) 출처: 2015, www.mandiant.com

**미국 대형 유통할인마트 Target사 POS 카드결재정보 유출해킹(>1억천만 건)는 공격부터 데이터유출까지 약 5개월간 동안 이뤄짐**



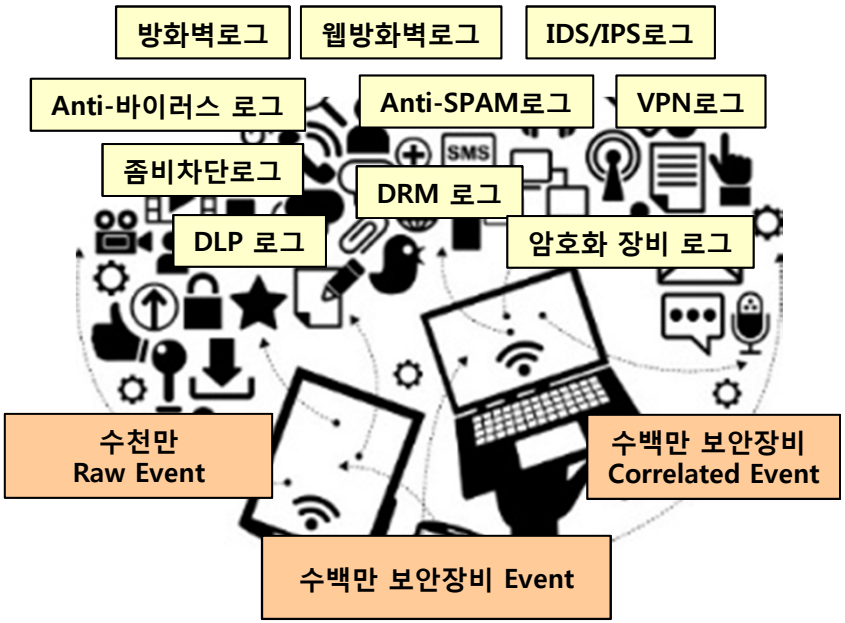

(*) 출처: 2014, USA Committee on Commerce, Science, and Transportation

# 사이버공격 대응전략 전환의 필요성

**제한된 리소스와 증가하는 데이터**

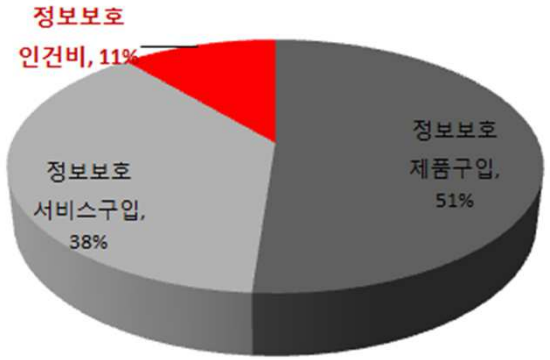
**보안팀의 리소스는 한정되어 있는데, 늘어나는 각종 보안시스템 운영과 늘어나는 데이터의 분석, 새로운 기술과 기법에 대한 분석 및 연구 이슈는 어떻게 해결하고 계십니까?**

## 수천만 Raw Event, 수백만 보안장비 Event




## 기업의 정보보호 예산지출(2015, 미래부)

- 기업의 정보보호 예산은 '14년 대비 18.6% 증가하였으나, 제품(51.2%) > 서비스(37.7%) > 인건비(11.2%) 순
- 증액되지 않는 정보보호 인력 인건비 투자



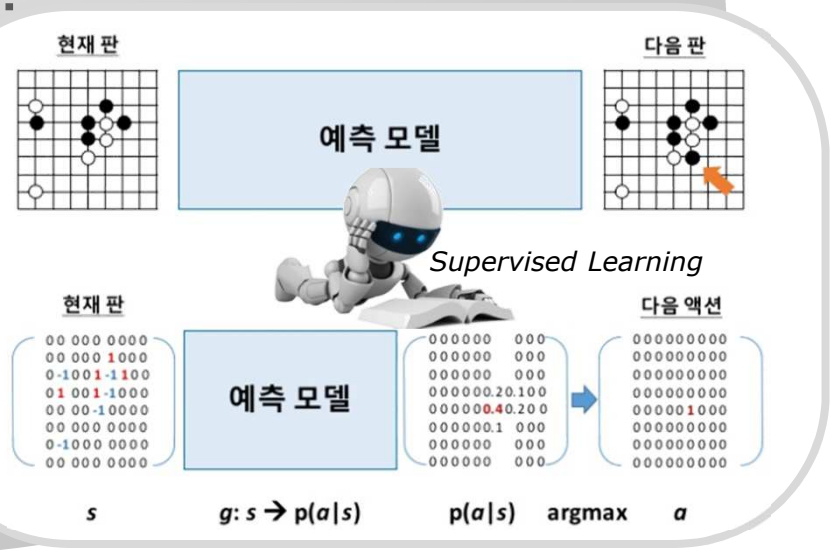

(*) 출처: 2015년 정보보호 실태조사(미래부)

# 사이버공격 대응전략 전환의 필요성

**알파고와 같은 머신런닝을 활용해서**
**Cyber Attack을 효율적으로 대응할 수 있을까?**

**데이터 사이언스 기법으로 수많은**
**공격들을 정확하게 분석할 수 있을까?**

**실시간으로 Cyber Attack 현황을**
**정확하게 모니터링하고 TOC를**
**줄일 수 있는 방안을 무엇일까?**



# CONTENTS

SINCE
2010

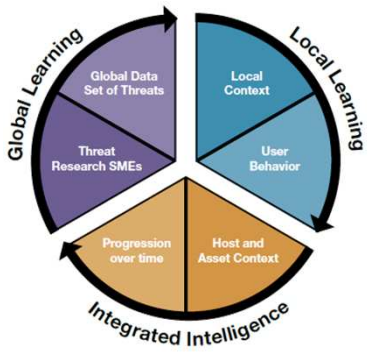
- 사이버공격 대응전략 전환의 필요성
- **VECTRA의 진화된 사이버공격 대응전략**
- VECTRA가 제공하는 주요기능 및 화면
- VECTRA 제품군과 CASE별 구성방안

주식회사 위키시큐리티
Information Security Solution Provider

# 1 Machine Learning과 Data Science 알고리즘 기반

전세계 Cyber attack정보의 학습(Global Supervised Learning Algorithm)과 고객사 현장의 비정상적 행위 학습(Local Unsupervised Learning Algorithm)과정을 지속적으로 병행하고, 통합상관분석 알고리즘을 이용하여 고객사를 장시간 프로파일링 함으로써 비정상행위들을 정확하게 탐지하여 정보를 제공

**[ Vectra의 ML, DS Algorithm ]**




정확한 Cyber Attack 탐지를 위한 Vectra의 지속적 기계학습 병행과 상관분석을 통합한 알고리즘

- Global Learning
- Local Learning
- Integrated Intelligence

## 전세계 사이버공격 학습 알고리즘

- Global Supervised Learning
- 전세계 Cyber Attack 데이터, 기법, 사례들을 분석, 공통특징 축출
- Vectra Threat Labs(Data Scientists, Cyber Security Experts group)의 알고리즘화
- 예) Random forest Algorithm 등

## 고객사 현황 현장학습 알고리즘

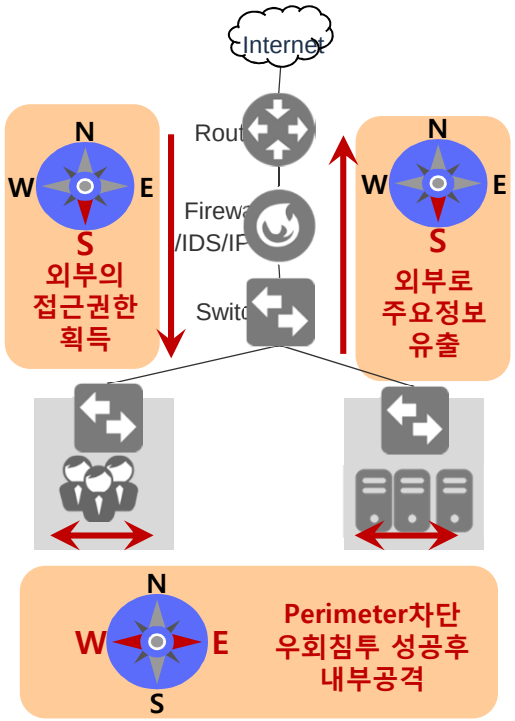
- Local Unsupervised Learning
- 기업의 내부 모든 IP의 행위를 학습 및 분석, 정상/비 정상 행위를 식별
- Vectra의 ATM(Automated Threat Manage -ment) model의 알고리즘화
- 예) K-means clustering, outlier analysis 등

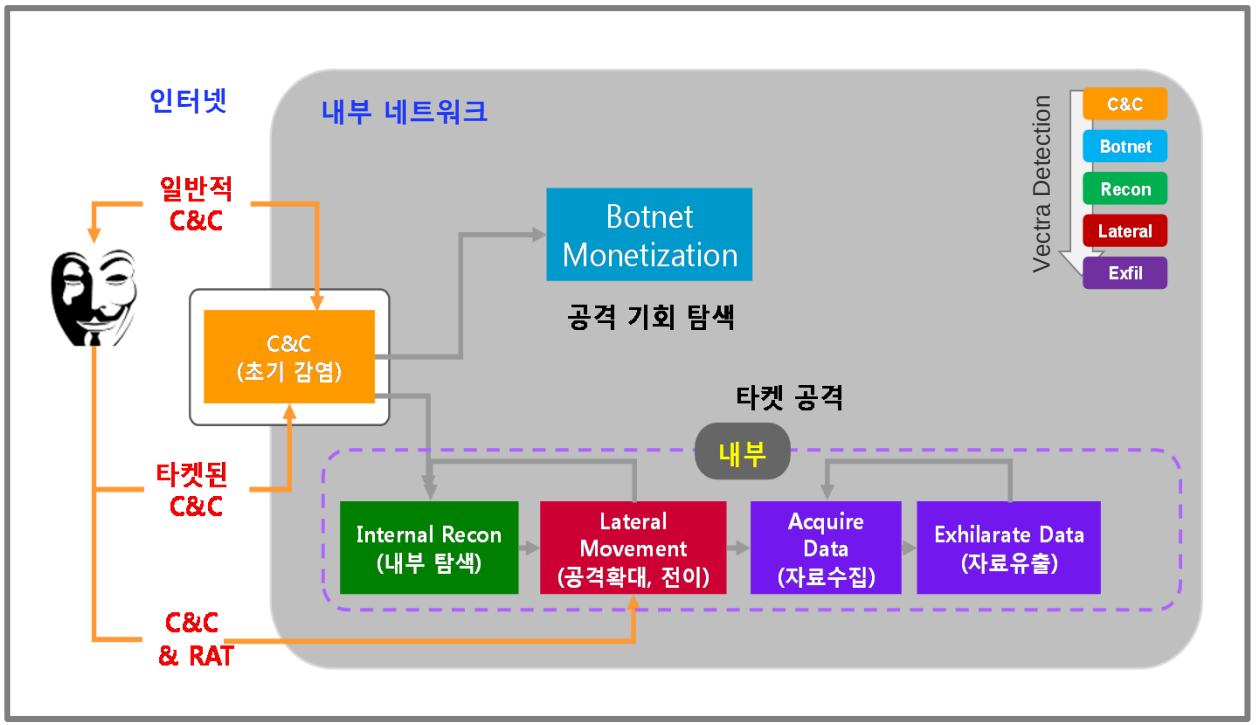
## 통합 상관분석 알고리즘

- Integrated Intelligence
- 장시간의 고객사 현장학습의 프로파일링과 탐지 알고리즘을 바탕으로 공격형태를 상관분석하여 정확한 탐지
- 예) Bayesian networks 등

## 2 인터넷+내부네트워크의 Cyber Kill Chain 공격탐지

일반적인 Cyber Attack의 공격단계(기업외부 > 내부공격 > 데이터유출)를 Vectra는 5개 유형(Cyber Kill Chain)으로 구분하고 유형별 탐지 알고리즘을 적용함으로써, Perimeter Security를 우회하여 내부로 공격을 확대 전이하고 외부C&C서버와 통신하며 데이터를 유출하는 모든 공격을 정확하게 탐지함



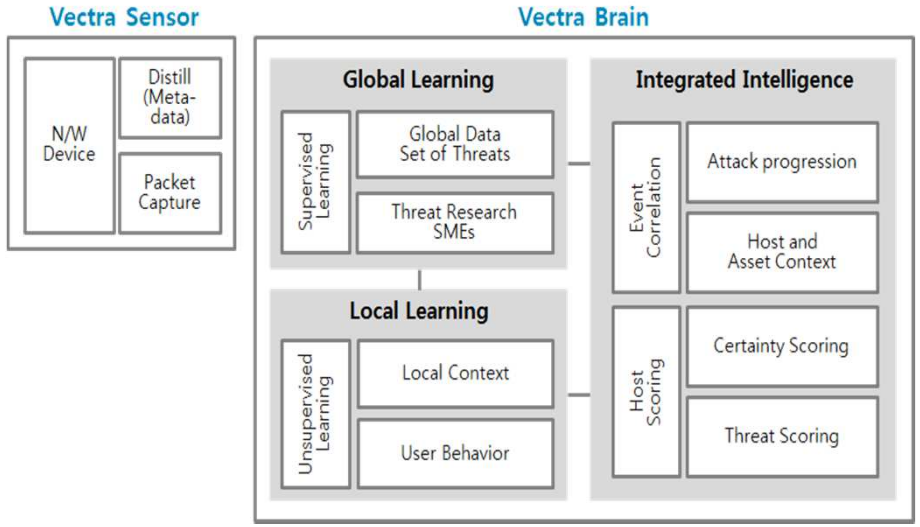



# 3 No Signature, No Rule, No Configuration

Vectra는 Machine Learning과 Data Science 알고리즘을 기반으로 고객사 네트워크를 장시간 Profiling하여 위협을 탐지함으로써, Signature또는 Rule에 의존하는 기존 Cyber attack 탐지 방식의 한계를 극복하여 고객사의 Cyber Attack들을 정확하게 탐지하여 모니터링정보를 제공함

**[ Vectra의 개념 아키텍처 ]**

Vectra Sensor에서 수집된 Packet은 Vectra Brain에 전송, 장기간 Profiling 하여 Vectra의 탐지알고리즘에 의해 Cyber Attack을 자동으로 탐지




**장기간 로컬네트워크를 Profiling (6~9개월간)**

- No Filters
- No Configurations
- No Signatures
- No reputation lists

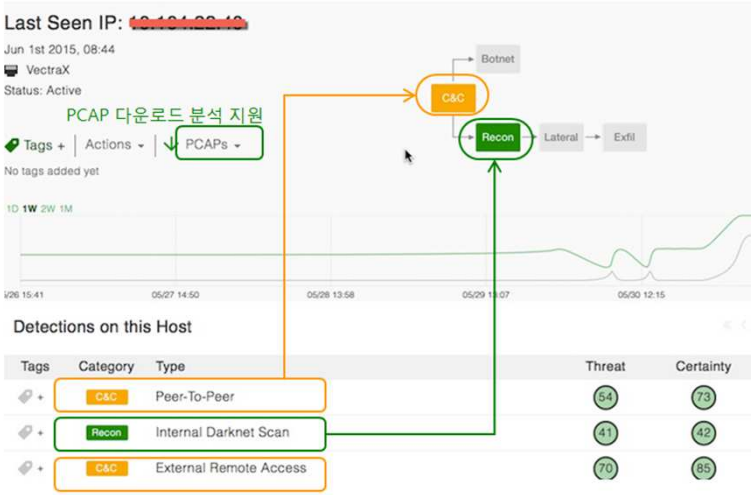
- **신종 공격기법을 정확하게 탐지 (예: Duqu 2.0 등)**
- **타킷형의 장기,지속 공격의 전확한 탐지**
- **탐지 룰셋 추가 및 최적화 작업 필요없는 자동 탐지**
- **전문 분석가 없는 기업도 최고수준의 탐지 환경 구축**

# 4 시계열 분석기능과 정확도 높은 스코어링

Vectra는 모니터링대상에서 이뤄지는 Cyber Attack 단계별 탐지현황을 지속적으로 기록관리하여, 현재의 단편적인 위협상황뿐만 아니라 그간의 모든 공격탐지 이력과 정확도를 Scoring하여 제공함으로써, 현재와 향후 주요 모니터링 대상 또는 조치방법을 판단하기 위한 신뢰성 높은 의사결정 지표를 제공함

**[ Vectra가 탐지한 내부 호스트의 공격단계별 연관화면 ]**

Vectra에서 탐지된 이 호스트는 외부에서 공격시도(External Remote Access)와 내부 스캔(Internal Darknet Scan) 및 Peer-to-peer 접속 등 Cyber Attack이 단계적으로 이뤄지고 있는 이력을 확인할 수 있음




**[ Vectra의 Tracking the attack progression over time ]**

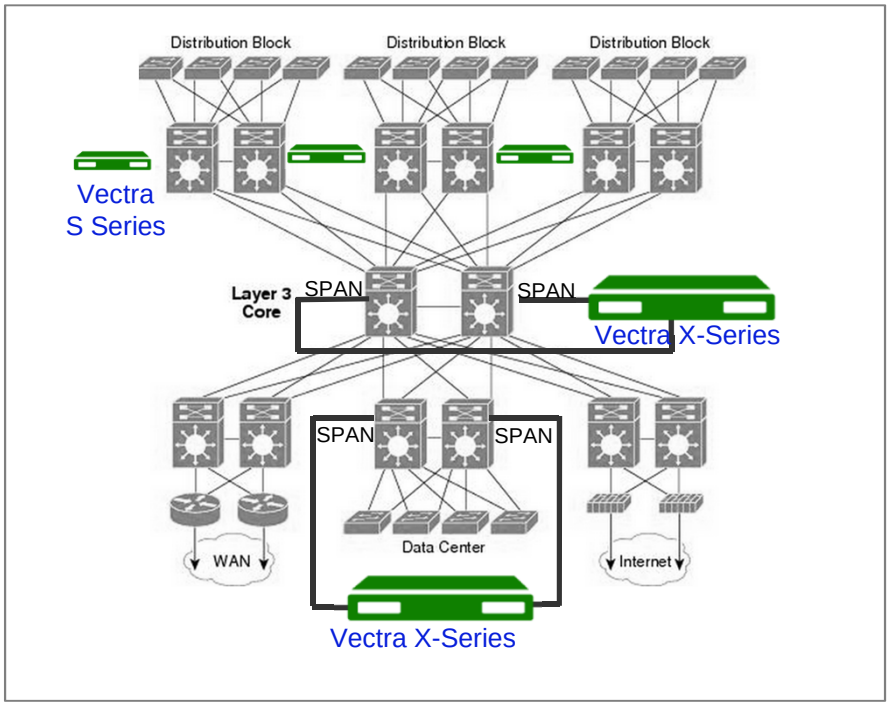
Vectra에서 탐지된 이 호스트는 5/20부터 27까지 Port Scan공격이 있었고, 의심스러운 HTTP통신 Malware업데이트가 6월5일까지 이뤄졌으며, 현재는 내부 포트스캐닝 공격이 이뤄지고 있음

| Tags | Category | Type | Threat | Certainty | First Seen | Last Seen |
|---|---|---|---|---|---|---|
| + | Recon | Port Scan | 60 | 80 | Jun 5th 2016 23:50 | Jun 6th 2016 00:39 |
| + | Recon | Port Sweep | 60 | 80 | Jun 5th 2016 23:49 | Jun 6th 2016 00:34 |
| + | Recon | Internal Darknet Scan | 52 | 49 | Jun 5th 2016 23:49 | Jun 6th 2016 00:00 |
| + | C&C | Suspicious HTTP | 55 | 76 | Jun 5th 2016 23:41 | Jun 5th 2016 23:44 |
| (2) | C&C | Suspicious HTTP | 57 | 90 | May 26th 2016 23:58 | Jun 5th 2016 23:40 |
| (2) | C&C | Malware Update | 75 | 96 | May 26th 2016 23:58 | Jun 5th 2016 23:38 |

# 5 네트워크 기반의 실시간 사이버공격 탐지

Vectra는 Brain역할을 하는 X-Series를 Core Switch에 연결하고 각 Workgroup Switch에 S-Series의 Sensor를 Packet Mirroring으로 설치하여, 단일기업형 뿐만 아니라 분산형, 그룹사형, Cloud Network형 등 다양한 환경에 대하여 Cyber Attack현황을 실시간으로 모니터링 할 수 있음

**[ 기존환경에 유연하고 간편한 Vectra의 설치구성 ]**




**< Vectra Model >**

- X-Series, S-Series
- Virtual Sensor
- Brain/Sensor/Mixed Mode

**< Vectra Model >**

- Packet Mirroring
- >1%의 패킷정제
- Real-time detection

**< Vectra Target >**

- 모든 IP Devices
- 모든 Protocols
- IoT Device
- Cloud Computing Network

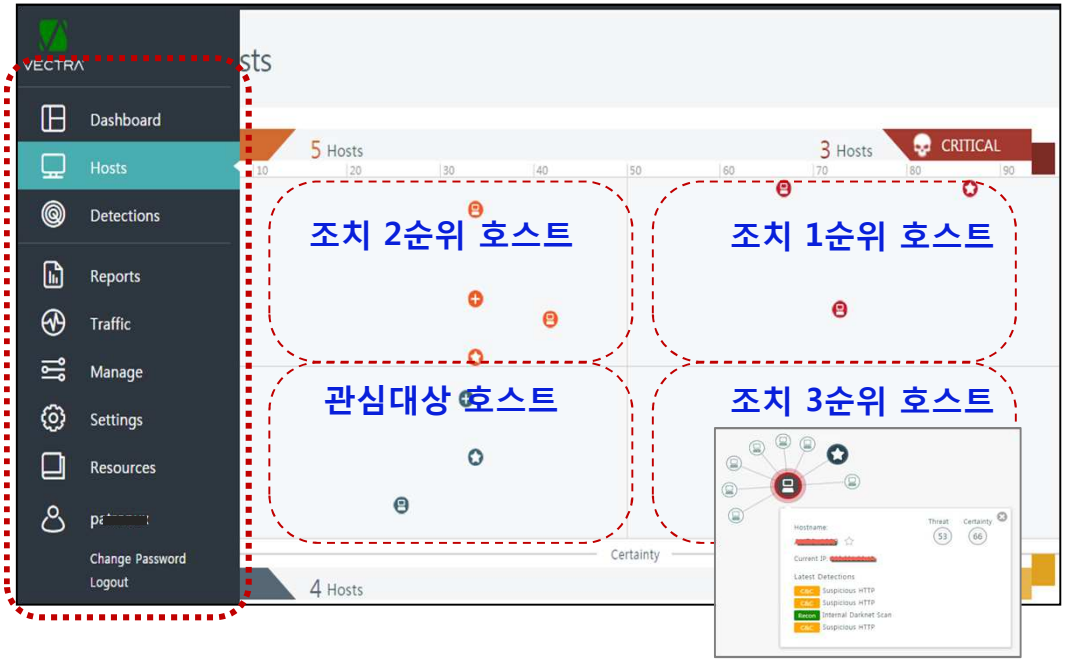
**Vectra의 X-Series, S-Series의 유연한 분산구성과 간편한 설치로 실시간 모니터링**

- 단일 기업형
- 분산 기업형
- 그룹사 구성형
- Cloud Network형

# 6 직관적이고 간결한 관리자 화면

Vectra의 간결하고 직관적인 화면 구성은 관리자가 판단해야 할 신속한 의사결정지원을 위하여 단순한 메뉴구성과 조치우선순위별 4/4분면 표시, 긴급조치 대상 호스트, 핵심자산 호스트에 대한 1개월 또는 24시간 동안의 간략한 Cyber Attack현황 및 이력표시, 급격하게 변화된 호스트의 공격 현황 등을 제공함

**[ Vectra의 Dashboard 화면-1개월간의 공격탐지현황 ]**




**[ 관리자의 직관화를 위한 간결한 화면 ]**

Vectra의 대쉬보드는 조치의 긴급성에 따라 관리자가 직관적으로 알 수 있도록 4/4분 면으로 긴급조치의 우선순위별 호스트 현황을 표시

**[ 조치 우선순위별 4/4분 면에 직관화 ]**

Vectra의 대쉬보드는 조치의 긴급성에 따라 관리자가 직관적으로 알 수 있도록 4/4분 면으로 긴급조치의 우선순위별 호스트 현황을 표시

**[ 긴급조치 대상 호스트의 요약표시 ]**

한번의 클릭으로 호스트별 Cyber Attack현황을 손쉽게 간략한 현황을 확인할 수 있어서, 조치여부 판단을 위한 신속한 의사결정을 지원

# 7 기존 보안시스템과의 유연한 연동기능

Vectra는 SIEM, Sandboxing 형태의 APT, IPS 등과 같은 기존 보안시스템을 대체하기 보다는 활용목적에 따라 상호보완 할 수 있는 보안시스템으로써, Big Data, 악성코드 분석, 침해사고 역추적 등의 보안기술 동향에 따라 타 보안 시스템과 유기적으로 연동하여 목적을 달성할 수 있는 다양한 연동기술은 제공함

**[ Syslog를 이용한 연동 ]**

Vectra벡트라는 표준 시스템 로그 또는 HP ArcSight의 공통 이벤트 형식(CEF)의 시스템 로그를 사용할 수 있도록 간단한 Vectra 설정으로 제공함


**[ RESTFUL API 기반의 연동 ]**

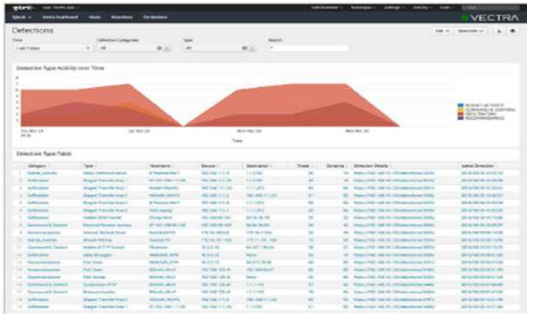
Vectra가 제공하는 RESTFUL API는 개방형 표준 API로써, Vectra가 탐지한 정확한 정보를 다른 보안시스템에서 손쉽게 이용할 수 있도록 JSON 형태로 제공함 (필요시 연동개발을 지원함)

| URL | Method | Data to Query |
|---|---|---|
| /api/settings | GET | Platform configuration |
| /api/rules | GET | Triage rule configuration |
| /api/detections | GET | Security detection events |
| /api/hosts | GET | Host information |
| /api/health | GET | System health statistics |
| /api/sensors | GET | Sensor configuration |

| Detection Category | URL |
|---|---|
| Command and control | /api/detections?category=command |
| Botnet | /api/detections?category=botnet |
| Reconnaissance | /api/detections?category=reconnaissance |
| Lateral movement | /api/detections?category=lateral |
| Exfiltration | /api/detections?category=exfiltration |

**[ Splunk를 이용한 연동 ]**

Vectra는 Big Data분석 등을 목적으로 Splunk 개발자가 Real-time으로 Vectra의 탐지정보를 연동할 수 있도록 Vectra App for Splunk를 제공함(필요시 연동개발을 지원함)



# Vectra의 진화된 사이버공격 대응전략

1. Machine Learning과 Data Science 알고리즘 기반
2. 인터넷+내부네트워크의 Cyber Kill Chain 공격탐지
3. No Signature, No Rule, No Configuration
4. 시계열 분석기능과 정확도 높은 스코어링
5. 네트워크 기반의 실시간 사이버공격 탐지
6. 직관적이고 간결한 관리자 화면
7. 기존 보안시스템과의 유연한 연동기능

머신런닝과 데이터사이언스 기반의 실시간 네트워크 Cyber Attack 탐지 및 모니터링

# CONTENTS

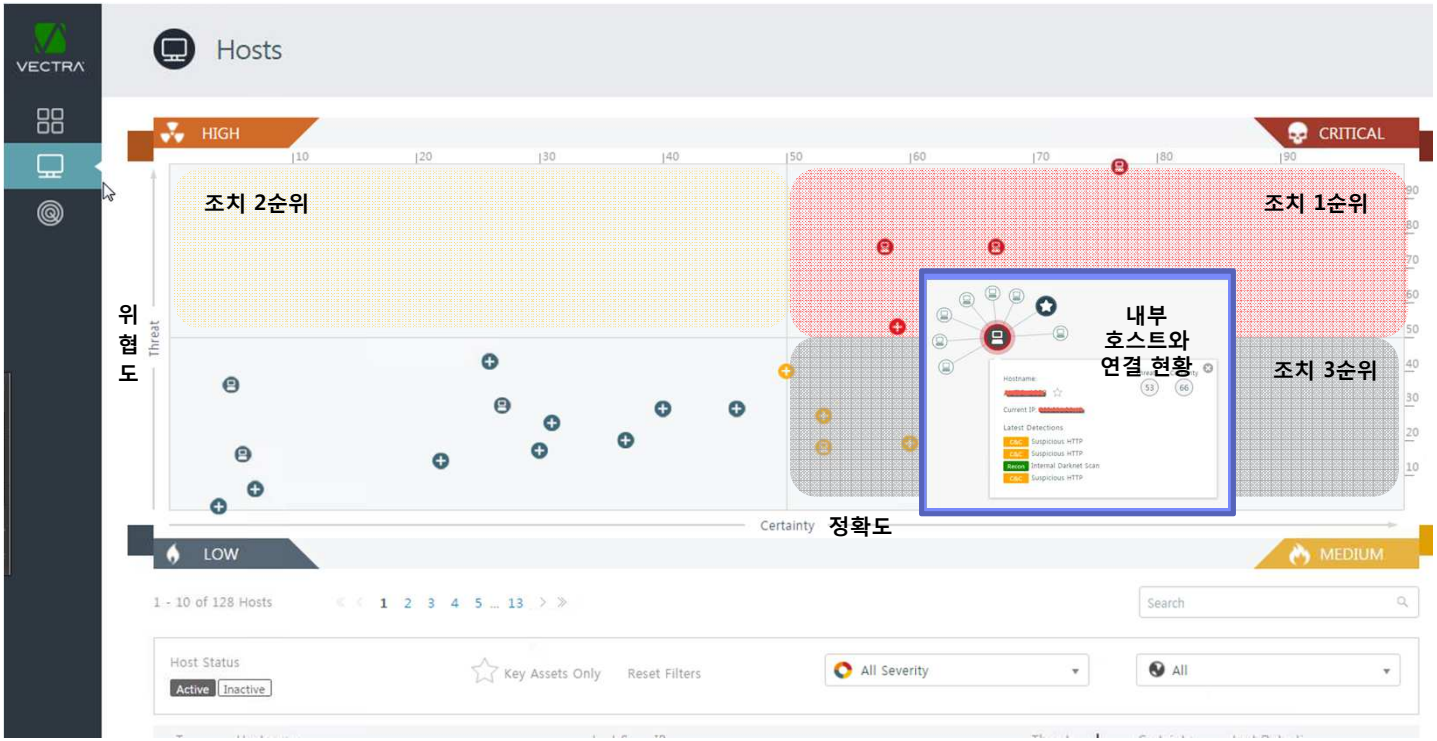
SINCE
2010

- 사이버공격 대응전략 전환의 필요성
- VECTRA의 진화된 사이버공격 대응전략
- **VECTRA가 제공하는 주요기능 및 화면**
- VECTRA 제품군과 CASE별 구성방안

주식회사 위키시큐리티
Information Security Solution Provider

# 1 Dashboard – 최근 1개월 탐지현황과 요약정보

대쉬보드는 실제로 내부 네트워크에서 진행되고 있는 공격 또는 악성행위를 일으키는 우선적으로 조치가 필요한 호스트를 직관적인 화면으로 제공하며 잠재적인 위협이 될 수 있는 의심스로운 호스트들을 모니터링

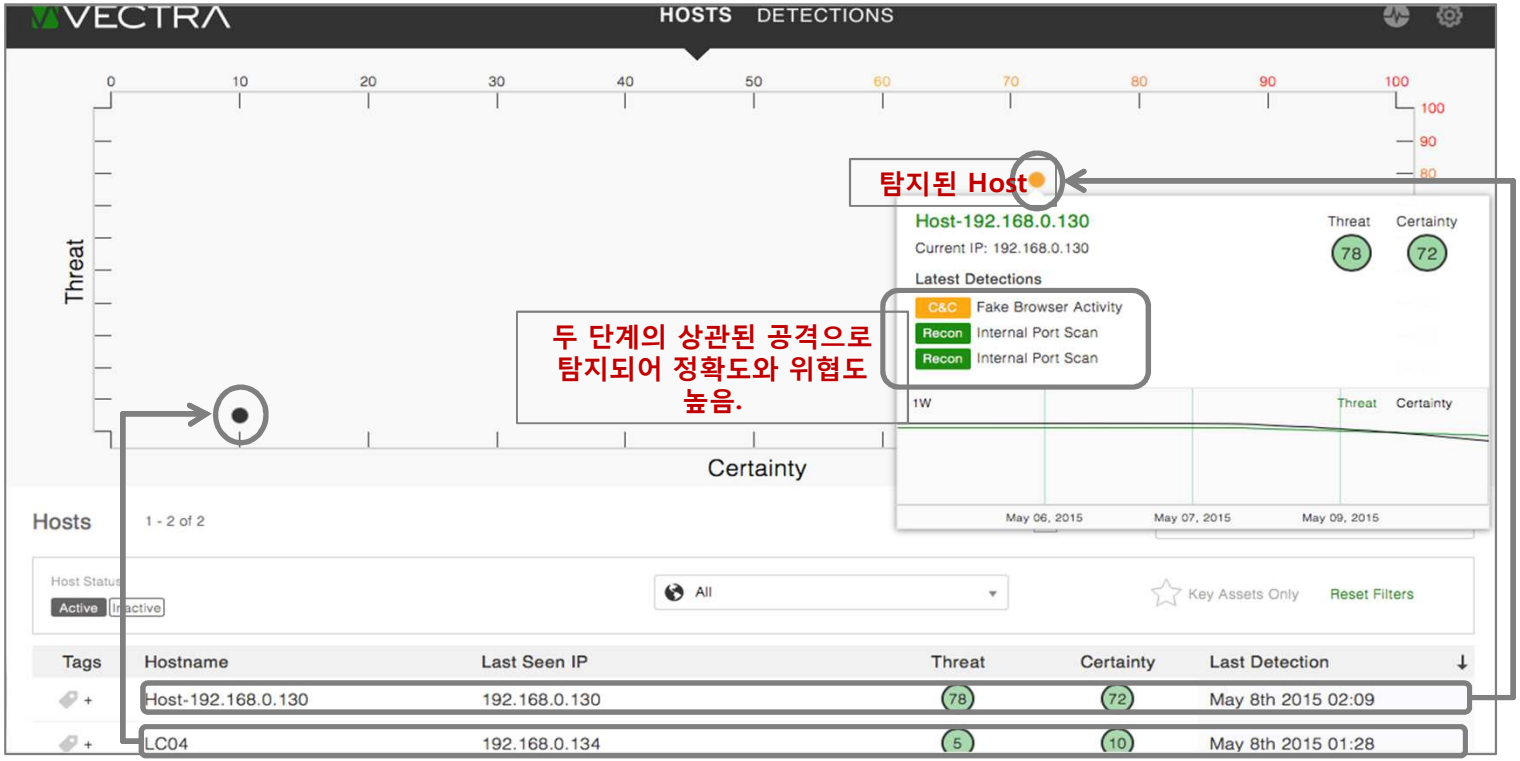


# 2 Dashboard – 24시간 현재 현황 요약

Vectra의 메인화면은 긴급조치해야 호스트별 현황(Host Serverity Summary), 핵심정보자산에 대한 요약정보(Key Assets) 등을 관리자의 관점에서 간략하게 요약한 화면을 제공함

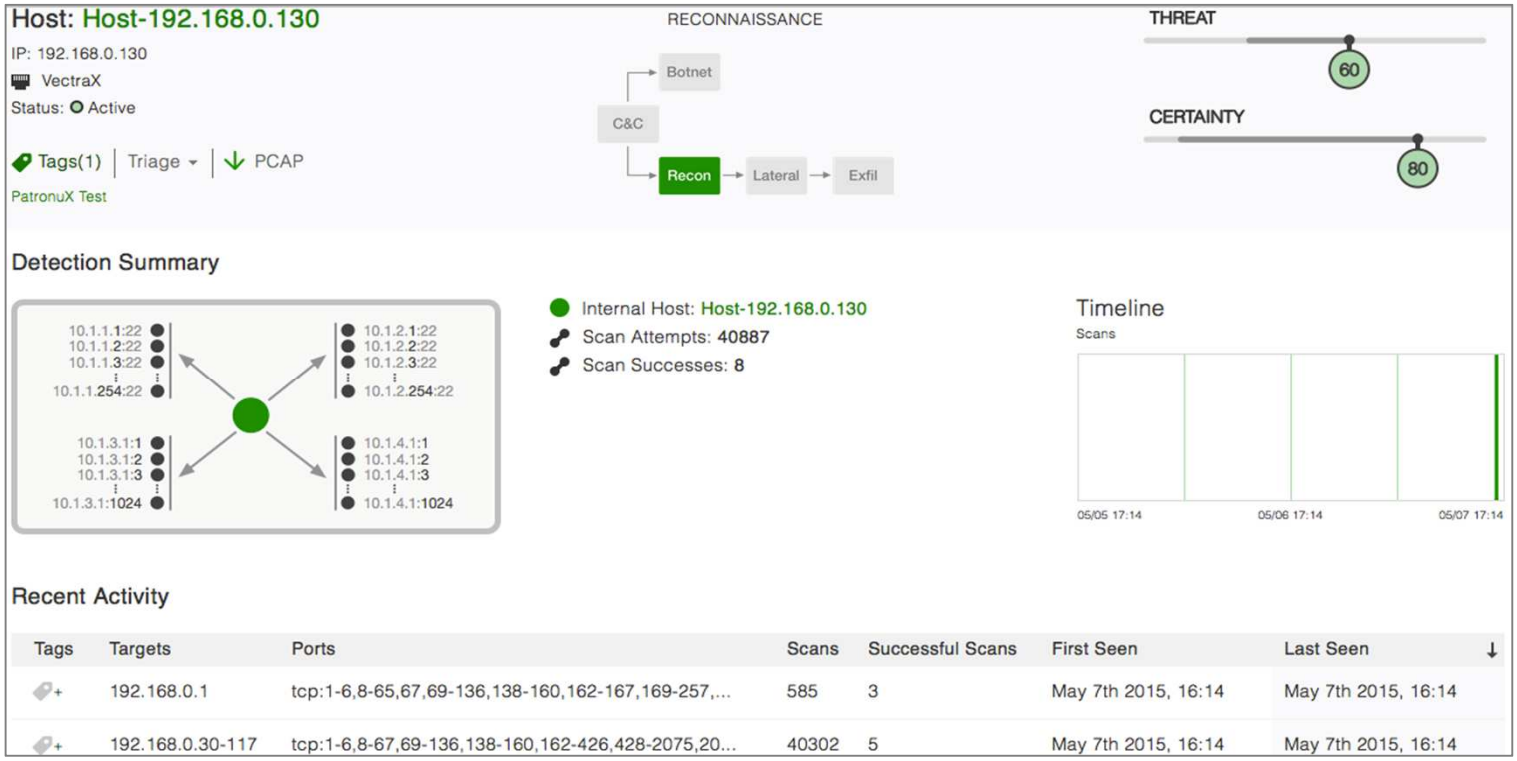
# 3 Cyber Attack이 탐지된 호스트와 내역

Cyber Attack이 탐지된 호스트의 세부 탐지내역을 제공함으로써 어떤 공격들이 언제 탐지되었고, 서로 어떤 관계가 있는지 직관적으로 인지할 수 있도록 위협과 정확도를 기준으로 그 상세내역을 제공함



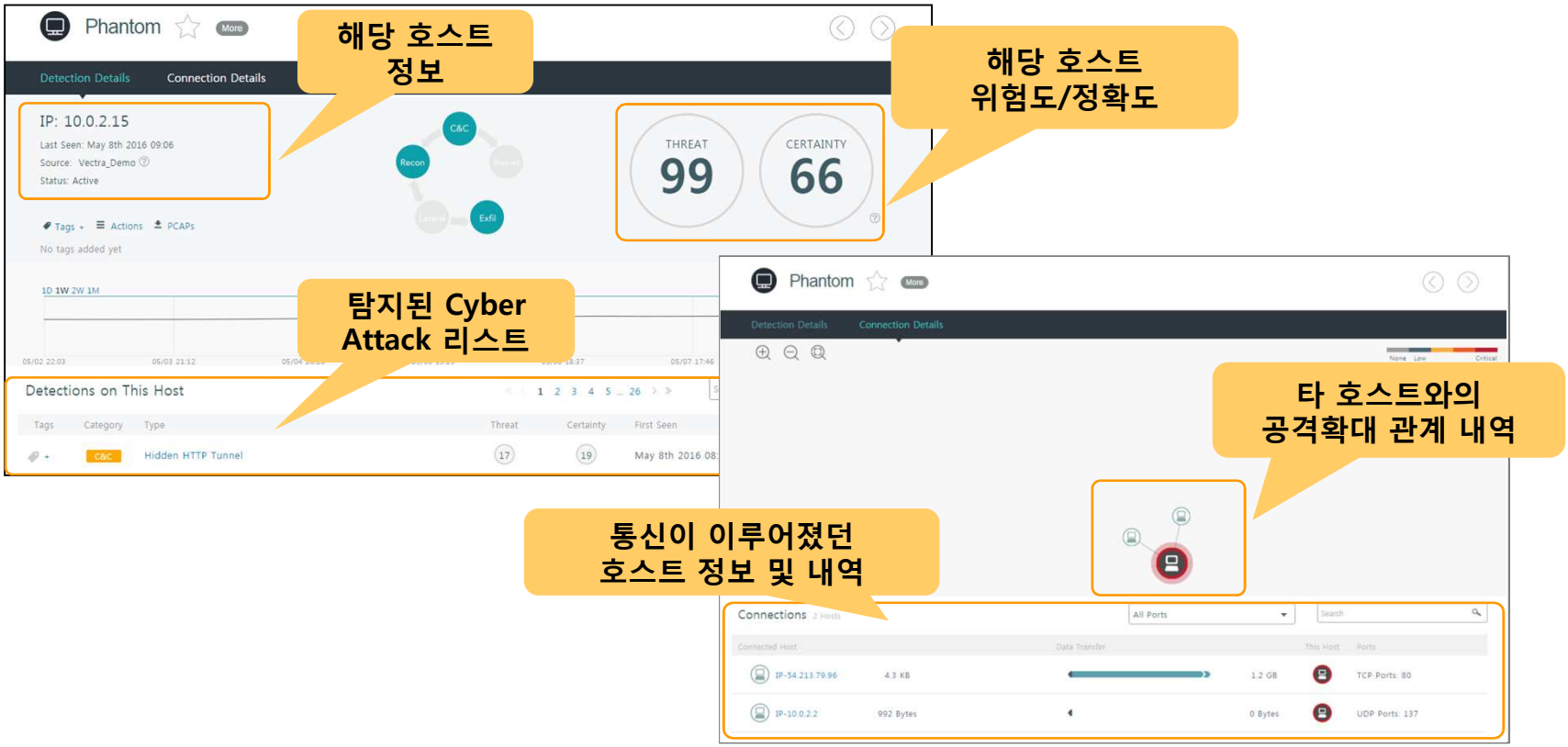
# 4 내부침투를 위해 스캔을 시도한 현황

Cyber Attack의 초기단계인 정찰단계(Reconaissance)를 탐지할 뿐만 아니라 내부공격의 전형적인 형태인 여러 호스트를 대상으로 내부 스캔 공격을 시도한 시간, 횟수, 패킷의 크기 등의 내역을 제공함



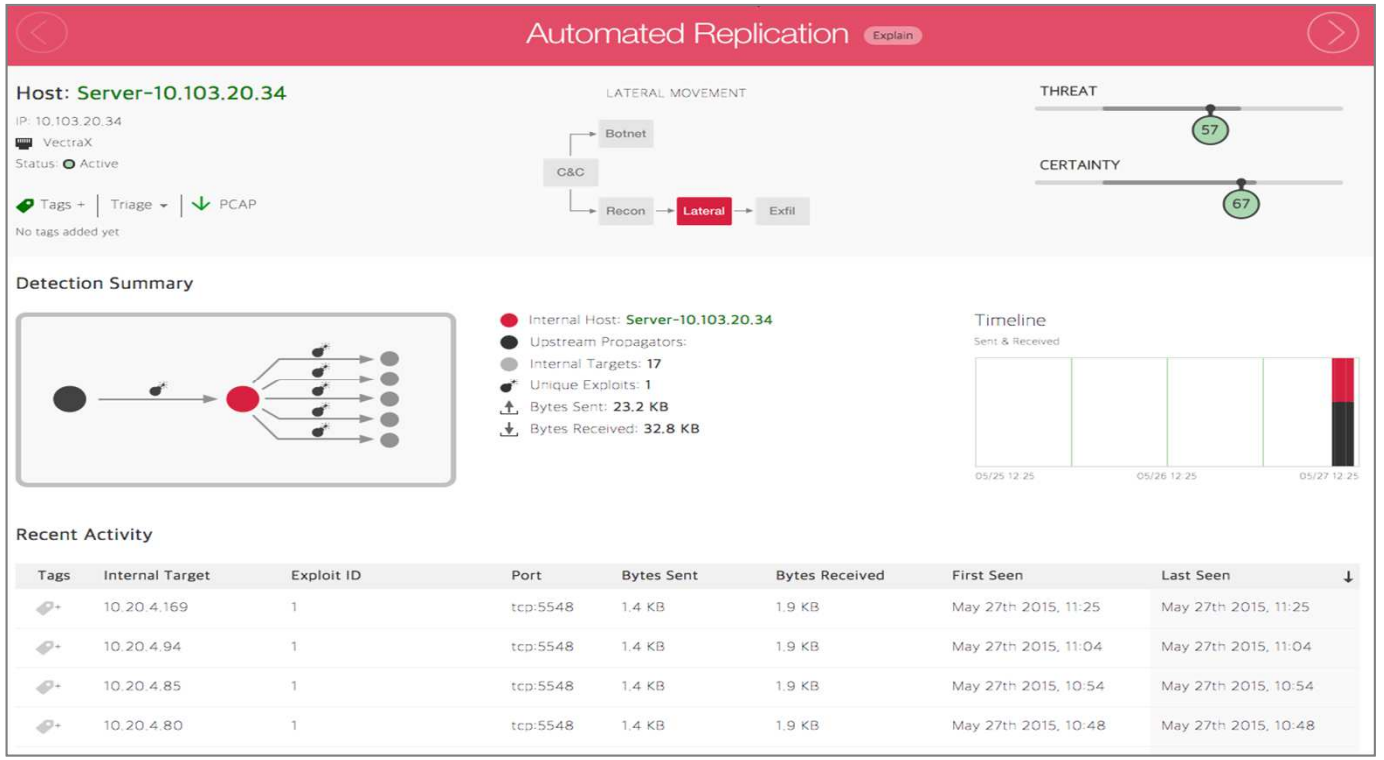
# 5 내부침투 성공 이후 타 호스트와 통신

Vectra는 Cyber Attack이 탐지된 호스트가 직접적인 공격 뿐만 아니라 권한이 빼앗긴 이후 다른 호스트로 공격을 내부로 확대 또는 전이하거나 C&C Server와의 통신내역을 모두 제공함



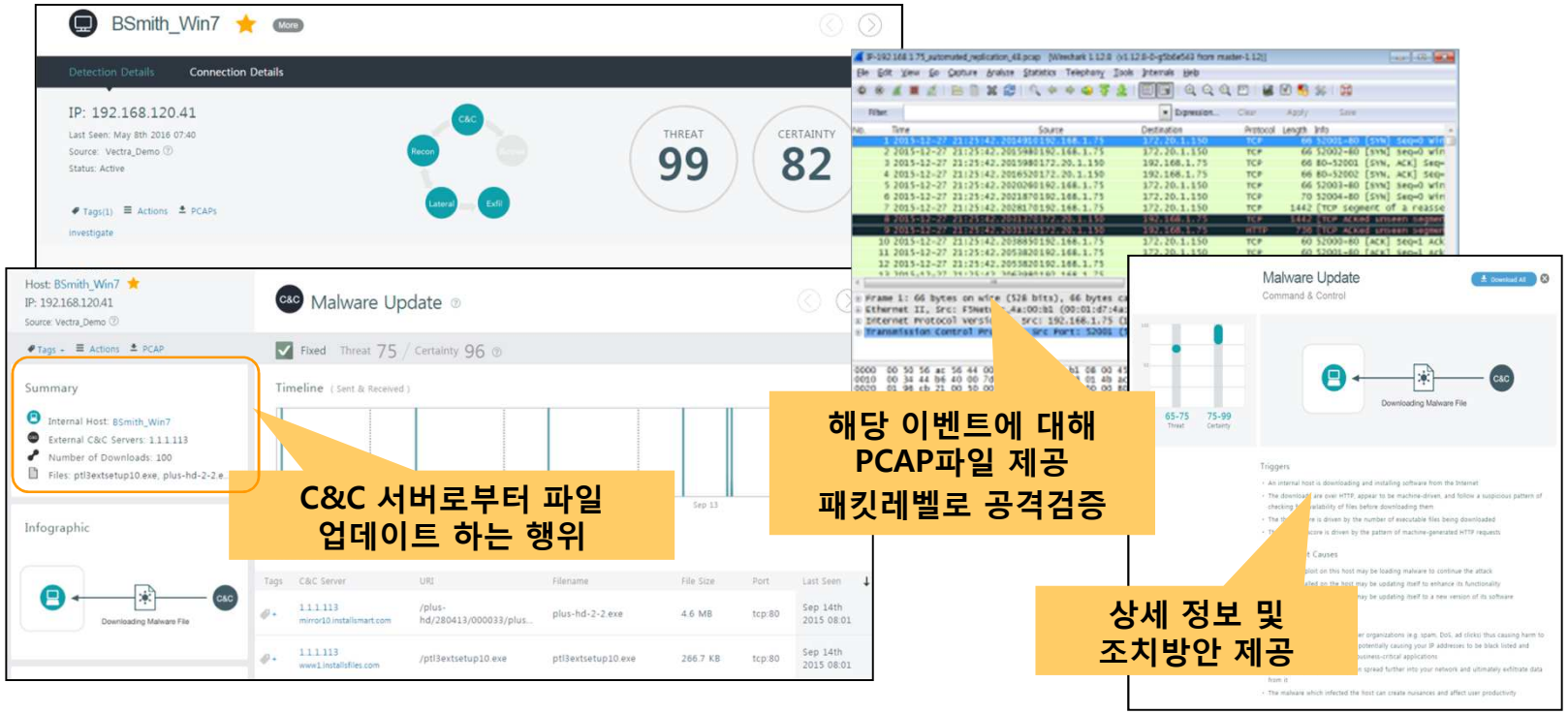
## 6 자신을 복제하는 자동화된 공격 탐지

내부침투에 성공한 이후, 공격확대 및 전이를 위해 내부의 여러 타 시스템들에게 자신의 복제를 시도한 내역들을 연관도와 시계열 분석, 파일사이즈, 사용된 서비스포트 등을 제공함



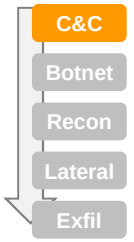
# 7 C&C서버 업데이트, 해당 위협의 PCAP 제공

내부침투에 성공한 이후, 공격확대 및 전이를 위해 내부의 여러 타 시스템들에게 자신의 복제를 시도한 내역들을 연관도와 시계열 분석, 파일사이즈, 사용된 서비스포트 등을 제공함



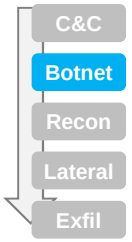
# Cyber Kill Chain별 탐지알고리즘(Command & Control)

| Cyber Kill Chain | 항 목 | 비 고 |
|---|---|---|
| Command & Control (악성 행위의 시발점인 다양한 C&C 공격 탐지) | External Remote Access | 외부에서의 원격접속으로 공격하는 행위 |
| | Hidden DNS Tunnel | 감염된 내부 호스트가 외부 호스트와 일반적인 프로토콜을 통해 은밀하게 위장하여 통신하는 행위<br>(HTTPS트래픽의 복호화 없이 데이타 사이언스 기법으로 통신 패턴을 분석( 딜레이,볼륨,순서,비정상 요청/응답등)하여 위협 행위 탐지) |
| | Hidden HTTP Tunnel | |
| | Hidden HTTPS Tunnel | |
| | Malware Update | 감염된 Malware의 업데이트 하는 행위<br>(외부로 부터 인스톨파일 다운로드, 다운로드 파일 체크 패턴등) |
| | Peer-To-Peer | 내부 호스트가 다수의 외부 IP와 P2P 통신을 하는 행위 |
| | Pulling Instructions | 외부 IP나 도메인과 통신하여 명령을 받는 행위<br>(통신 패턴과 송수신 데이타 양 분석) |
| | Stealth HTTP Post | 외부 호스트로 식별되지 않은 다수의 HTTP Post Request로 데이타를 보내는 행위 |
| | Suspect Domain Activity | 의심스러운 외부 도메인을 찾는 행위, 자동화된 도메인 이름 생성툴에 위한 도메인, 존재하지 않는 도메인 이름을 빠르게 찾는 행위등 |
| | Suspicious HTTP | 실제로 Browser가 아닌데 Browser형태로 기형의 User-agent string 정보를 송신하는 행위(바이너리파일 다운) |
| | Tor Activity | Tor(프락시를 통한 우회통신 등) 형태의 악성 통신. |



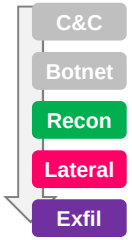
# Cyber Kill Chain별 탐지알고리즘(BotNet Activity)

| Cyber Kill Chain | 항 목 | 비 고 |
|---|---|---|
| Botnet Activity (감염된 Bot 들의 악성행위 탐지) | Abnormal Ad Activity | 감염된 내부 호스트가 일반적이지 않은 다수의 HTTP Redirection 등을 통해 악성 코드가 포함되어 있을 수 있는 배너 및 팝업 광고를 클릭하도록 유도하는 악성 행위 |
| | Abnormal Web Activity | 외부 웹 서버에 접속하여 악성 콘텐츠를 다운로드 하게 하는 악성 행위. |
| | Bitcoin Mining | 사이버 화폐(Bitcoin)를 수집하는 악성행위 |
| | Brute-Force Attack | 감염된 내부 호스트가 다양한 프로토콜로 내/외부 서버비정상적인 시도를 하거나 무차별 암호추측 공격을 하는 행위. |
| | Outbound DoS | 감염된 내부 호스트가 외부로 DoS 공격을 하는 행위<br>(SYN Flood, Slowloris) |
| | Outbound Scan | 감염된 내부 호스트가 외부 서비스에 연결하기 위해 Scan을 하는 행위 |
| | Outbound Spam | 외부로 일반적이지 않은 다량의 Spam 메일을 전송 하는 행위 |
| | Relay Communication | C&C 통신을 감추기 위한 연계 통신 행위. |



# Cyber Kill Chain별 탐지알고리즘(Reconnaissance, Lateral Movement, Exfiltration)

| Cyber Kill Chain | 항 목 | 비 고 |
|---|---|---|
| Reconnaissance (내부 탐색) | Internal Darknet Scan | 내부 확장을 하기 위해 감염된 호스트가 포함된 네트워크 및 더 넓은 확장을 위해 임의의 네트워크까지 Scan 하는 악성행위 |
| | Port Scan | |
| | Port Sweep | 내부 확장 행위 중 다수의 IP를 대상으로 소수의 Port 만을 스캔하는 행위 |
| Lateral Movement (공격전이 및 확대) | Automated Replication | 악성 코드를 내부 시스템에 확장을 시도하는 악성 행위<br>(같거나 유사한 payload를 다수의 내부서버에 전송) |
| | Brute-Force Attack | 내부 확장을 위해 다양한 프로토콜(RDP, VNC, SSH, HTTP/S, SSL/TLS)을 이용하여 계정을 탈취하기 위한 악성 행위(Heartbleed 공격(메모리 스크래핑등)) |
| | Kerberos Client Activity | Kerberos를 이용하여 계정을 탈취하기 위한 악성 행위<br>(Kerberos Client의 의심스로운 많은 인증 및 서비스 나 계정 요청 시도, Kerberos Server에 다수의 Client가 다수의 서비스로 많은 의심스러운 시도) |
| | Kerberos Server Activity | |
| | Kerberos Identity Activiry | |
| | Ransomware File Activity | SMB 프로토콜을 사용하여 공유중인 폴더에 하나 혹은 그 이상의 파일에 대해 같은 사이즈 또는 같은 파일 명으로 Read/Write 하는 행위 |
| | SQL Injection Activity | SQL Injection 공격 행위 |
| Exfiltration (데이터 유출) | Data Smuggler | 내부 호스트에서 데이터를 수집하여 외부 호스트로 유출하는 악성 행위 |
| | Hidden DNS Tunnel | DNS/HTTP/HTTPS 등의 통신 채널을 이용하여 눈에 띄지 않게 데이터를 유출하는 행위. |
| | Hidden HTTP Tunnel | |
| | Hidden HTTPS Tunnel | |
| | Staged Transfer-Hop1 | 내부호스트에서 수집된 데이타를 다른 내부 호스트로 보내고 수신한 호스트에서 외부로 송신하는 행우 |
| | Staged Transfer-Hop2 | |



# CONTENTS

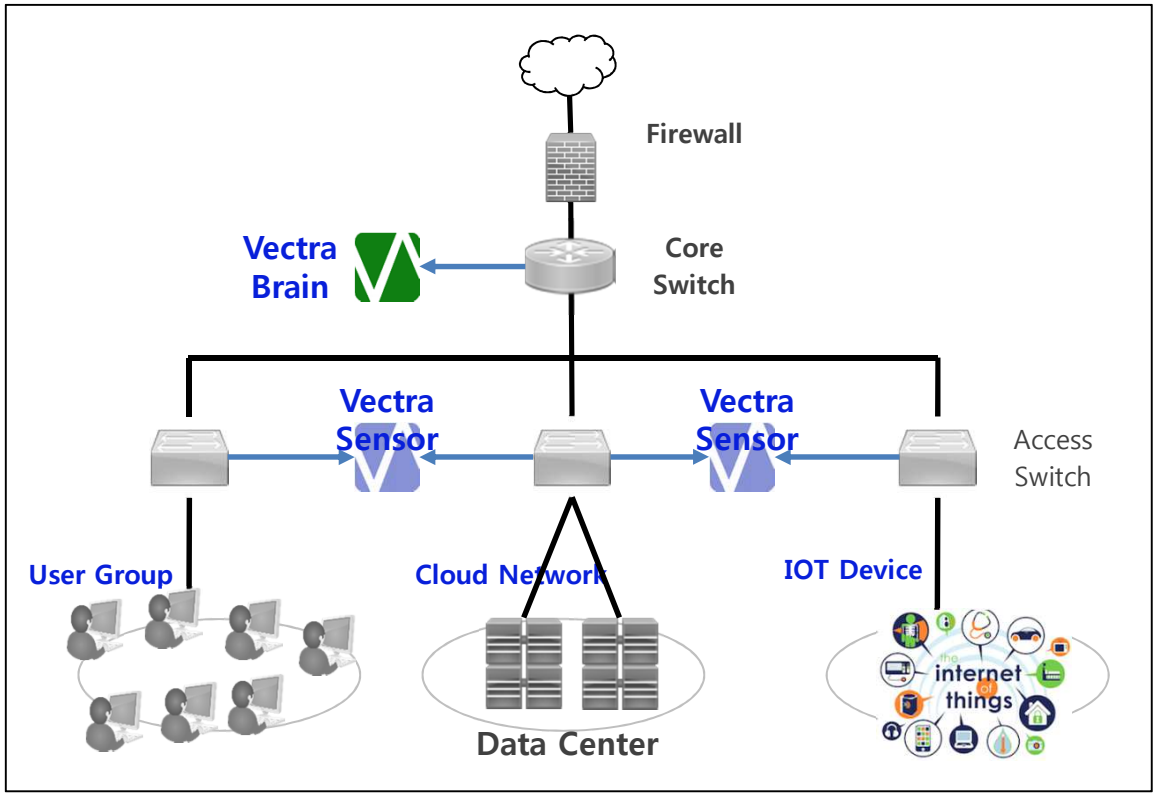
SINCE
2010

- 사이버공격 대응전략 전환의 필요성
- VECTRA의 진화된 사이버공격 대응전략
- VECTRA가 제공하는 주요기능 및 화면
- **CASE별 구성방안과 레퍼런스**

주식회사 위키시큐리티
Information Security Solution Provider

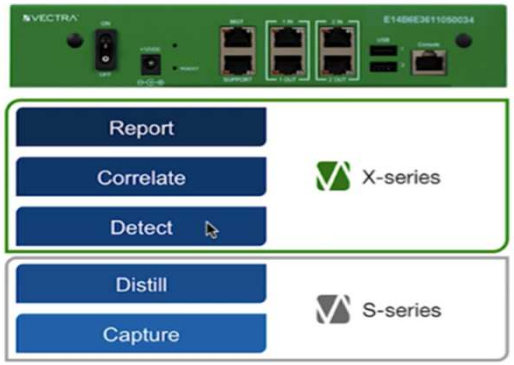
# 1 단일의 기업 모니터링 구조

기본 구성으로써, Core Switch에 X-Series(Brain)를 설치하고, 탐지 대상 서브네트워크에 S-Series (Sensor)를 설치하여 특정영역의 해킹 위협을 탐지 및 모니터링을 제공



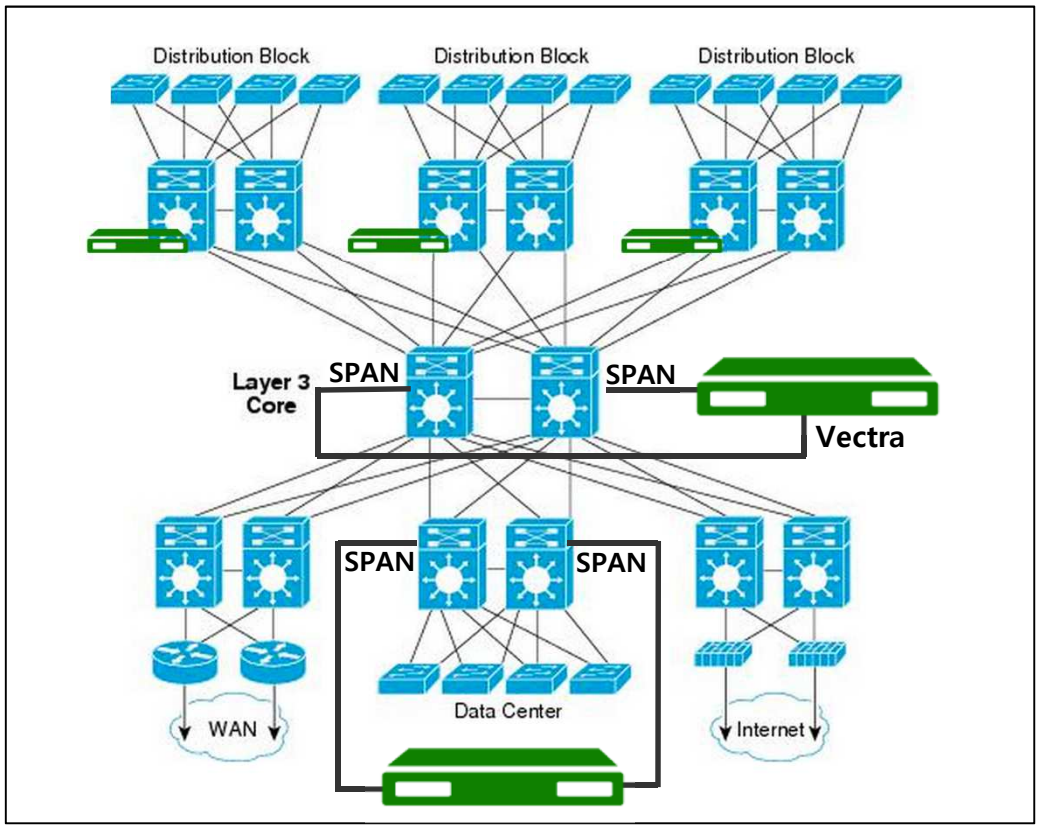

➢ **네트워크 Packet Mirroring으로 실시간 위협정보수집**

- **Vectra Brain**
  Core Switch를 통한 내외부 트래픽 캡춰 & 분석
- **Vectra Sensor**
  Access Switch를 통한 내부 트래픽 캡춰 & 분석

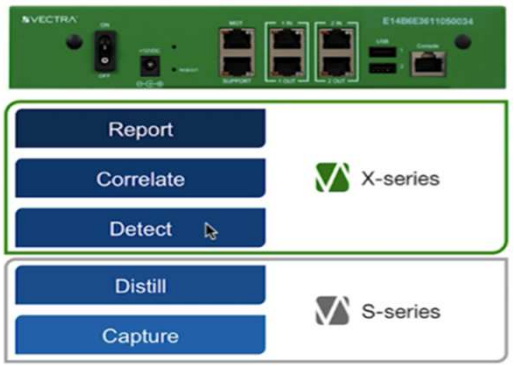


# 2 분산된 기업 통합 모니터링 구조

분산된 조직의 해킹위협을 탐지 모니터링하기 위한 구성으로써, 본사에 Core Switch에 X-Series(Brain)를 구성하고 지사 등의 원격 지에는 X-series(Mixed)또는 S-Series(Sensor)를 구성하여 통합 모니터링 제공

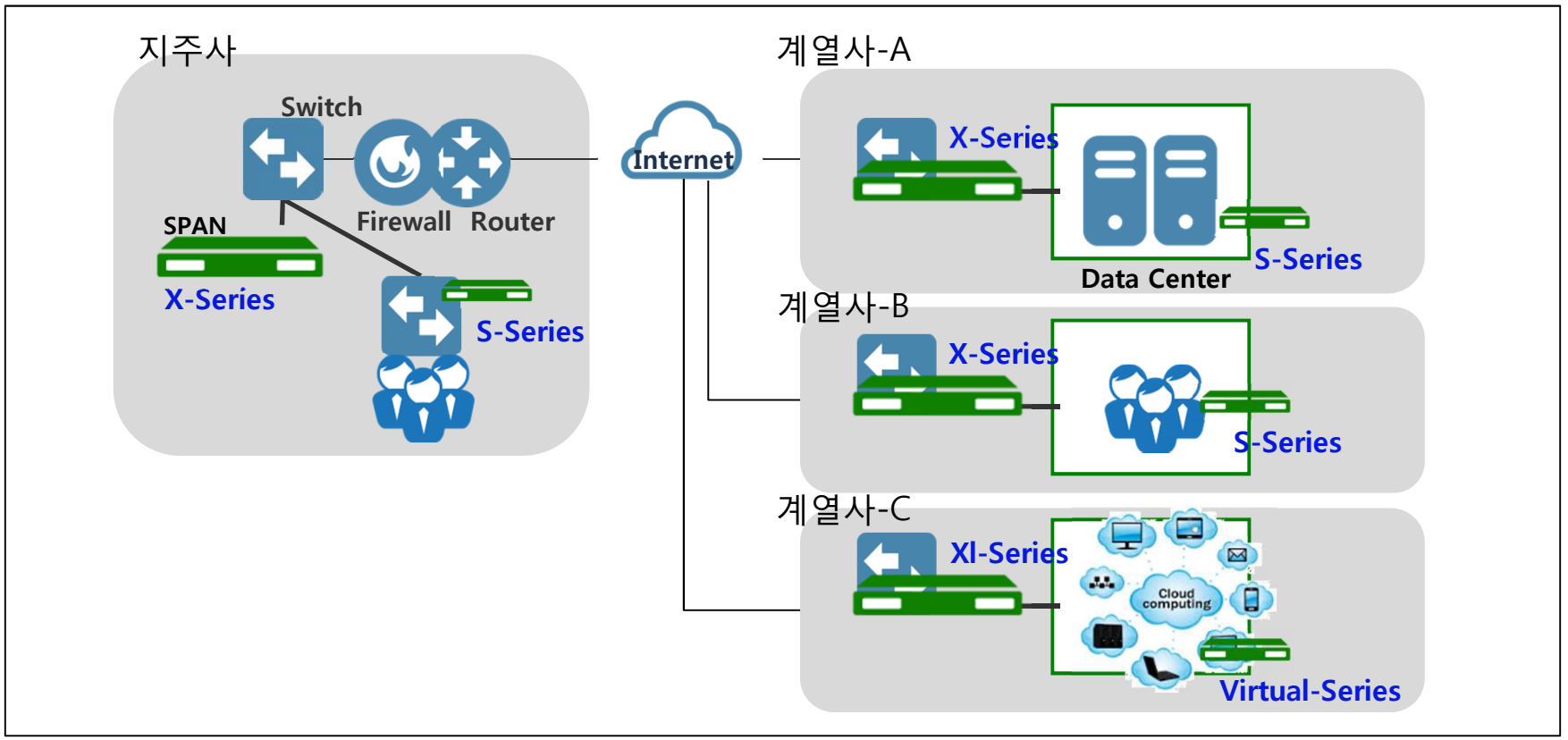



- **HQ에**
  자체 및 원격지 모니터링을 위한 X-Series와 S-Series구성
- **분산된 원격지 네트워크에**
  X-Series와 S-Series구성



# 3 여러 그룹계열사 모니터링 구조

그룹사차원에서 그룹지주사에서 그룹전체를 탐지 및 모니터링하고, 각 계열사는 자사만을 모니터링하는 구성으로 다수의 X-Series들과 S-Series, Virtual Machine으로 구성하여 그룹전체를 모니터링



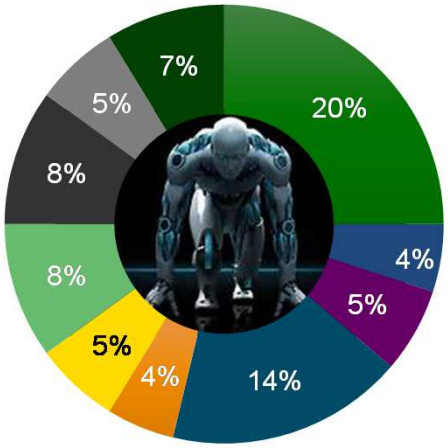
## Vectra Datasheet

### HARDWARE SPECIFICATIONS

| | S2 Sensor | X4 Platform | X20 Platform | X24 Platform | X80 Platform |
|---|---|---|---|---|---|
| **Capture Ports** | • Four 10/100/1000 BASE-T<br>• A total of two ports can be used in passive mode | • Four 10/100/1000 BASE-T | • Four 10/100/1000 BASE-T<br>• Two 10 Gigabit Ethernet SFP+ | • Four 10/100/1000 BASE-T<br>• Two 10 Gigabit Ethernet SFP+ | • Four 10 Gigabit Ethernet SFP+ |
| **Management Ports** | • One 10/100/1000 BASE-T out-of-band management port<br>• One 10/100/1000 BASE-T out-of-band support port<br>• One RJ-45 serial console port | • Two 10/100/1000 BASE-T ports<br>• One VGA video port<br>• Two USB 2.0 ports<br>• One DB-9 serial port | • Two 10/100/1000 BASE-T ports<br>• One VGA video port<br>• Two USB 2.0 ports<br>• One DB-9 serial port | • Two 10/100/1000 BASE-T ports<br>• One VGA video port<br>• Two USB 2.0 ports<br>• One DB-9 serial port | • One 1000 BASE-T port<br>• One 10 Gigabit Ethernet SFP+<br>• One VGA video port<br>• Two USB 2.0 ports<br>• One DB-9 serial port |
| **Storage Capacity** | • 1 TB hard disk drive | *Raw Storage:*<br>• 4 TB hard disk drive<br>*Configured Storage:*<br>• Two redundant 1 TB hard disk drives for operating system<br>• Two 1 TB hard disk drives as disk striping for data | *Raw Storage:*<br>• 6.8 TB hard disk drive<br>*Configured Storage:*<br>• Two redundant 1 TB hard disk drives for operating system<br>• Eight 600 GB hard disk drives as disk striping for data | *Raw Storage:*<br>• 4 TB hard disk drive<br>*Configured Storage:*<br>• Four redundant 1 TB hard disk drives for operating system and striping for data | *Raw Storage:*<br>• 12 TB hard disk drive<br>*Configured Storage:*<br>• Two redundant 1 TB SSD drives for operating system<br>• Eight 1 TB hard disk drives as disk striping for data |
| **Input Voltage** | • 100-240 VAC, 50-60 Hz | • Auto-sensing 100-240 VAC, 50-60 Hz | • Dual modular power supplies; auto-sensing 100-240 VAC, 50-60 Hz | • Auto-sensing 100-240 VAC, 50-60 Hz | • Dual modular power supplies; auto-sensing 100-240 VAC, 50-60 Hz |
| **Power** | • 60 watts | • 1800 watts | • 1800 watts | • 1800 watts | • 1800 watts |
| **Current** | • 5 A | • 7.5 A-18 A | • 7.5 A-18 A | • 7.5 A-18 A | • 7.5 A-18 A |
| **Dimensions** | • 1.74 in. (44.19 mm) H x 9.09 in. (230.88 mm) W x 7.74 in. (196.59 mm) D | • 1.7 in. (43.18 mm) H x 17.2 in. (436.88 mm) W x 31 in. (787.40 mm) D | • 3.5 in. (88.90 mm) H x 17.2 in. (436.88 mm) W x 31 in. (787.40 mm) D | • 1.7 in. (43 mm) H x 17.2 in. (437 mm) W x 27.82 in. (707 mm) D | • 1.7 in. (43 mm) H x 17.2 in. (437 mm) W x 27.82 in. (707 mm) D |
| **Weight** | • 5.18 lbs (2.3 kg) | • 26 lbs (11.8 kg) | • 54 lbs (24.5 kg) | • 26 lbs (11.8 kg) | • 26 lbs (11.8 kg) |
| **Environment** | *Operating Temperature:*<br>• 32° to 104° F (0° to 40° C)<br>*Non-Operating Temperature:*<br>• -4° to 158° F (-20° to 70° C) | *Operating Temperature:*<br>• 50° to 95° F (10° to 35° C)<br>*Non-Operating Temperature:*<br>• -4° to 158° F (-20° to 70° C) | *Operating Temperature:*<br>• 50° to 95° F (10° to 35° C)<br>*Non-Operating Temperature:*<br>• -4° to 158° F (-20° to 70° C) | *Operating Temperature:*<br>• 50° to 95° F (10° to 35° C)<br>*Non-Operating Temperature:*<br>• -4° to 158° F (-20° to 70° C) | *Operating Temperature:*<br>• 50° to 95° F (10° to 35° C)<br>*Non-Operating Temperature:*<br>• -4° to 158° F (-20° to 70° C) |

# Vectra References

[ 산업군별 레퍼런스 ]




- Education
- Energy & Trans
- Entertainment
- Finance
- Legal
- Health
- Gov't
- Mfg
- Prof Svcs
- Retail

[ 수상 경력 ]

Gartner 2015 CoolVendor
RSAC Innovation Sandbox FINALIST
The Golden Bridge Awards GOLD BEST 2015 BUSINESS WORLD
Info Security Products Guide 2015 GLOBAL EXCELLENCE GOLD
CRN EMERGING VENDORS 2015
CUTTING EDGE NETWORK SECURITY SOLUTION 2015 CDM
2015 SINET 16 INNOVATOR
COOL TOOL AWARD 2015 digest

[ 주요 고객사 레퍼런스 ]

UNDER ARMOUR
FHLBank San Francisco
Microsoft
Pinterest
Tribune Media
BOEING
PAUL HASTINGS
SANTA CLARA UNIVERSITY
Reed Elsevier
Virgin Pulse
Infoblox
riverbed
aruba NETWORKS
MONTICELLO ASSOCIATES
New Relic
shutterstock
TRI-STATE Generation and Transmission Association, Inc.
TY·LIN INTERNATIONAL
Good
Greenhill
SUNY
FORMFACTOR INC.
ISKANDAR MALAYSIA
(주)쌍방울

# End of Document

주식회사 위키시큐리티
Information Security Solution Provider

서울특별시 금천구 가산동 에이스테크노타워10차 601호
TEL : 02-322-4688 | Fax : 02-322-4646 | E-mail : info@wikisecurity.net