내부망에서의 가시성 확보

CEO
DongBum Lee

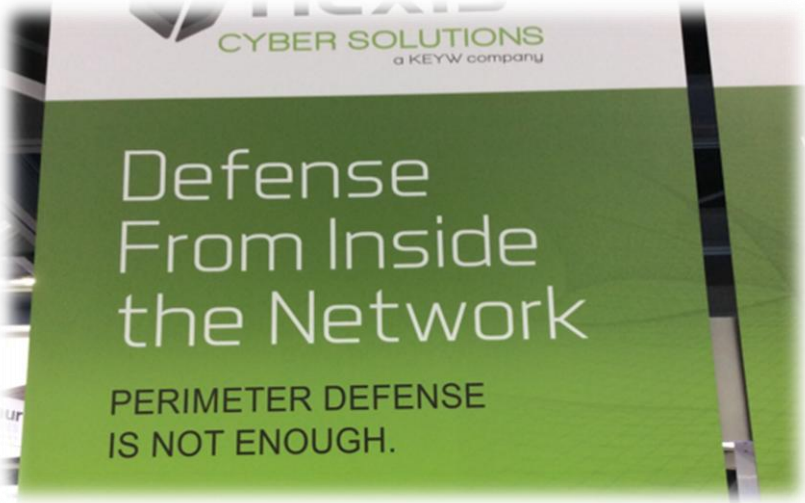
Thursday, April 24, 2014

GeniNetworks Inc.

Share.
Learn.
Secure.

Capitalizing on Collective Intelligence

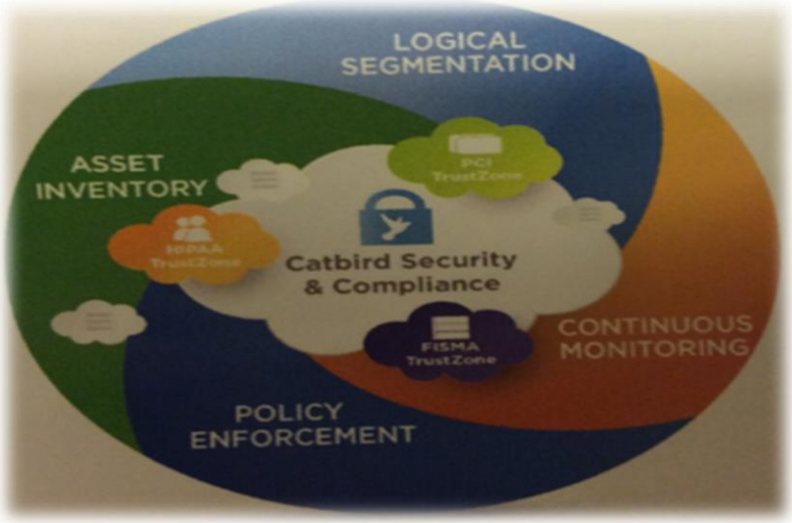
Insider Threat



Life style


onapsis
ontinuous Auditing and Secu
ERP CYBER SECURITY
nitoring of Your Business-Critical Systems
IDENTIFY
Automatically discover and map all SAP instances and their components.
AUDIT
Detect insecure configurations, missing SAP security patches, risky user authorizations, and dangerous interfaces.
SAP® Certified
Integration with SAP NetWeaver®
MITIGATE
Access detailed mitigation procedures that increase the overall security of your SAP platform.
COMPLY
Generate a variety of reports for effective risk communication and efficient remediation.


Fortify & Operationalize
Incident Resolution
Ongoing Operations
GLOBAL INTELLIGENCE NETWORK
Retrospective Escalation
Unknown Event Escalation
Incident Containment


LOGICAL SEGMENTATION
ASSET INVENTORY
Catbird Security & Compliance
CONTINUOUS MONITORING
POLICY ENFORCEMENT

Continuous


he New Security Mode
BEFORE, DURING AND AFTER AN ATTACK
A new model of security means accounting for the entire attack continuum
BEFORE
POLICY & CONTROL
DURING
IDENTIFICATION & BLOCK
AFTER
ANALYSIS & REMEDIATION
DISCOVER ENVIRONMENT
IMPLEMENT ACCESS POLICY
HARDEN ASSETS
DETECT
PREVENT
DETERMINE SCOPE
CONTAIN
REMEDIATE
A CONTINUOUS SECURITY PROCESS
TO RESPOND TO CONTINUOUS CHANGE
sourcefire.com


The Objective: "Continuous Threat Protection"
Time to Detect
Time to Fix
DETECT
CONTAIN
RESOLVE
PREVENT
Prevent
THEFT OF ASSETS & IP
COST OF RESPONSE
DISRUPTION TO BUSINESS
REPUTATION RISK

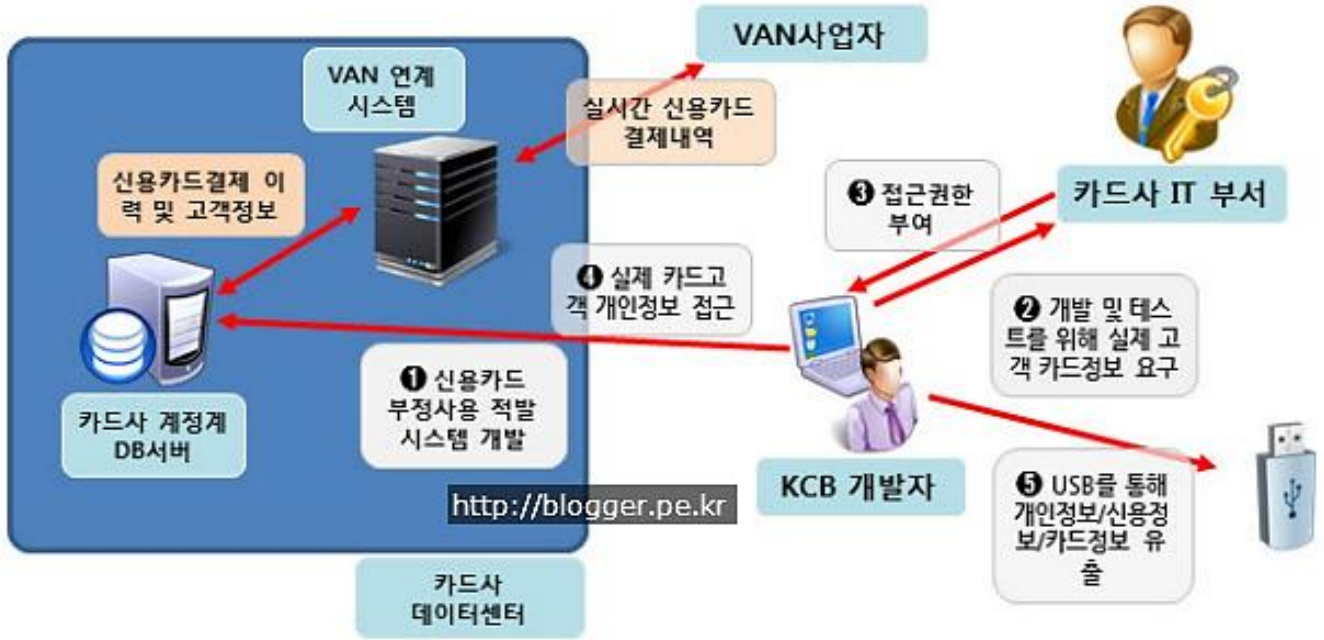
Intelligent

Visibility


Complete
Visibility
Security Architecture Simplified


VISIBILITY
is protection.
WatchGuard Dimension™
Real-time threat monitoring.

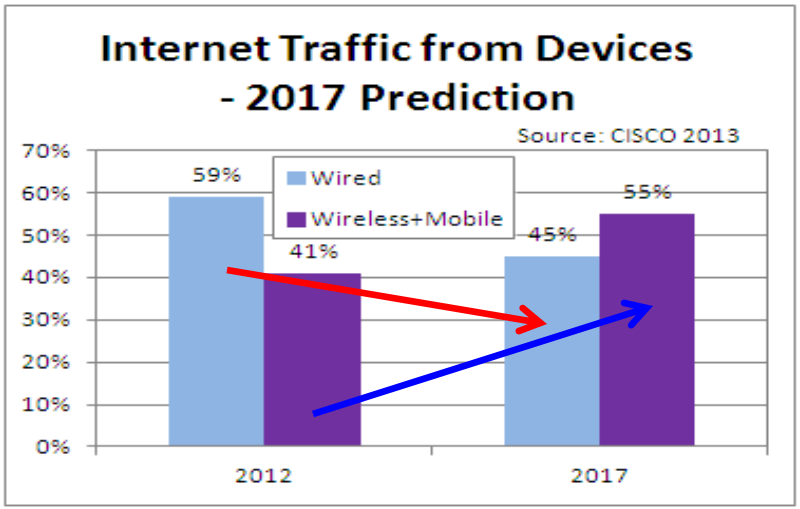

Network Infrastructure Security Management
If you can't
SEE
it, you can't secure it.



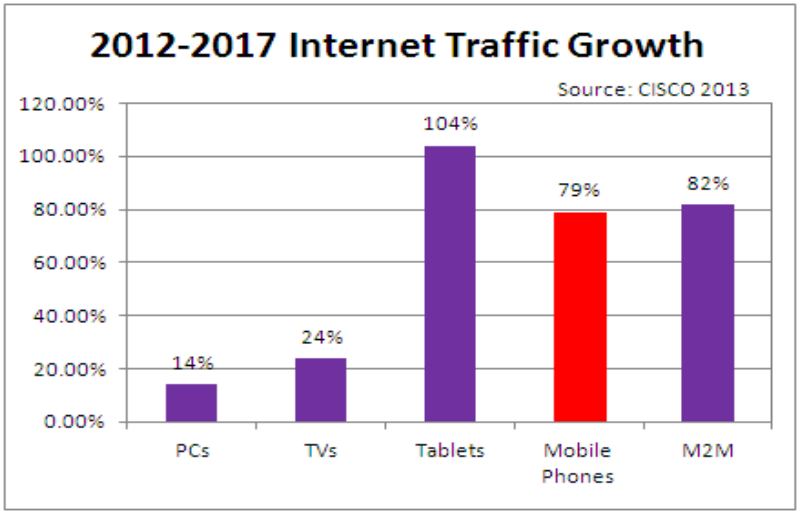
- **USB 통제 프로그램을 설치하지 않았을까?**
- **보안 관리자가 개발자망의 존재를 알았을까?**

점점 더 복잡해지는 인프라

➢ **Wired, Wireless BYOD, Cloud, IOT**



➢ **PC, Smart phone, Tablet, Cloud, IOT**



확인할 수 없는 것들

- **TCP 80 = Web? (Facebook, Dropbox, etc…)**
- **암호화된 traffic**
  - ✓ 전체 traffic의 25%가 암호화된 traffic
  - ✓ 공격 traffic의 80%가 암호화

확인할 수 없는 것들

SIEM

Security Information and Event Mgmt.

Find / Make 'Value'

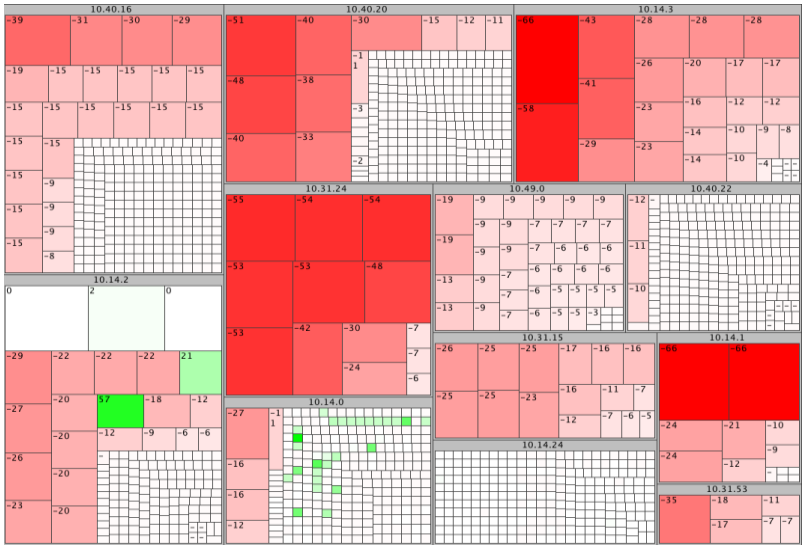
- 쓰레기 더미에서 폭발물 찾아 내기
- How?
  - ✓ Try
  - ✓ Practice
  - ✓ 보안 조직의 능력 배양

확인할 수 없는 것들

Data collection

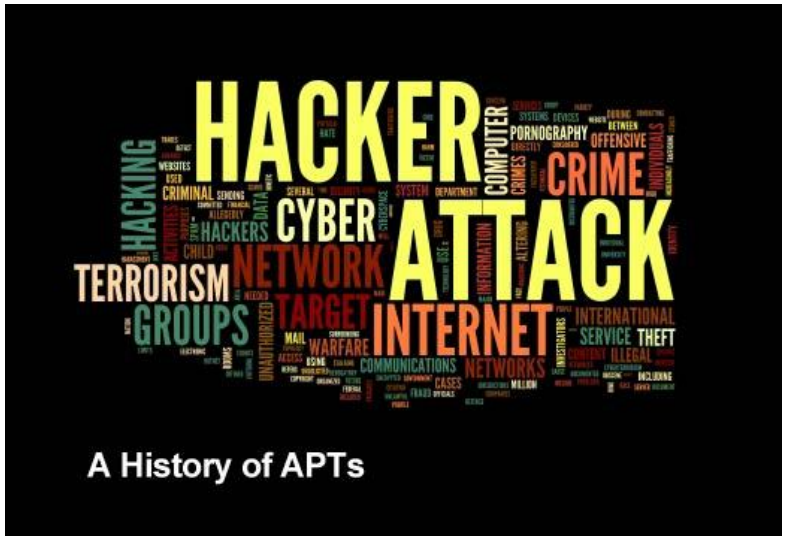
Data analysis

Visualization



APT와 Big data

APT



어떤 특정 공격이 아님
Unknown attack

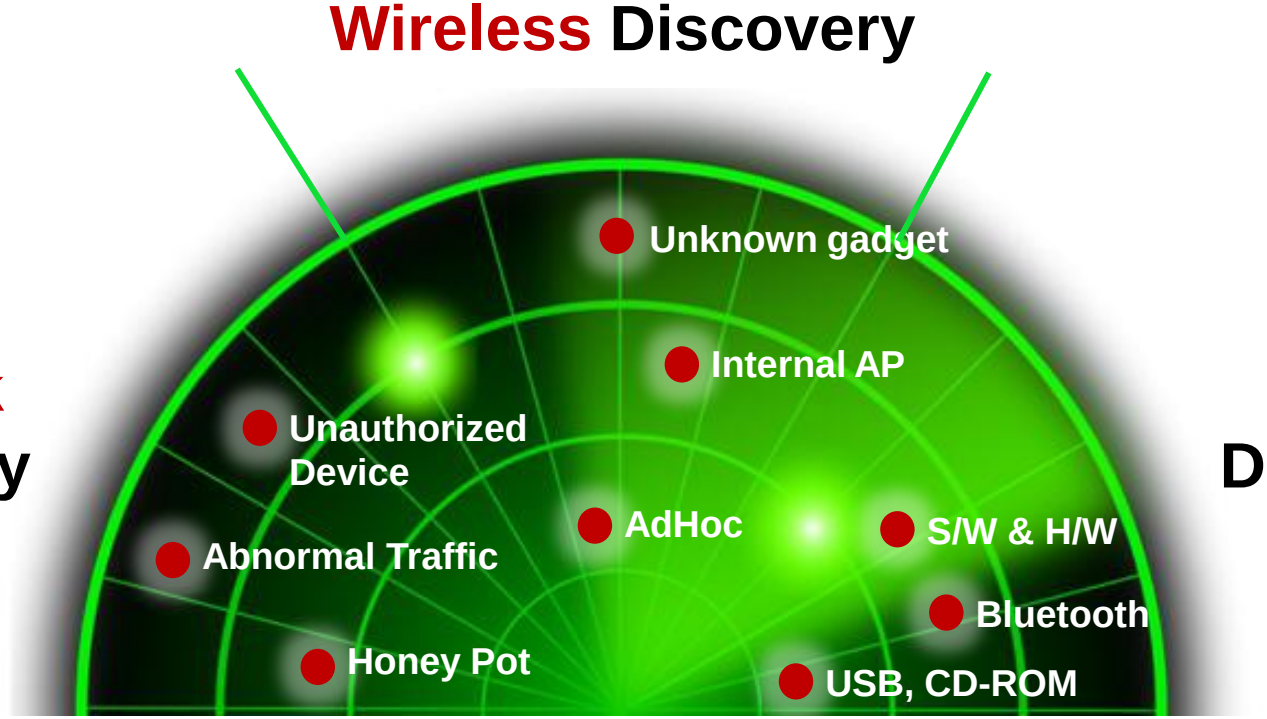
Big data

Data를 최대한 수집하여 저장
미래에 발생될 기회/위기를
포착하기 위한 도구

'불확실성'

NAC(Network Access Control) of New Era

Internal Visibility



NAC(Network Access Control) of New Era

Tracking Changes

How can you find
spot the differences?

NAC(Network Access Control) of New Era

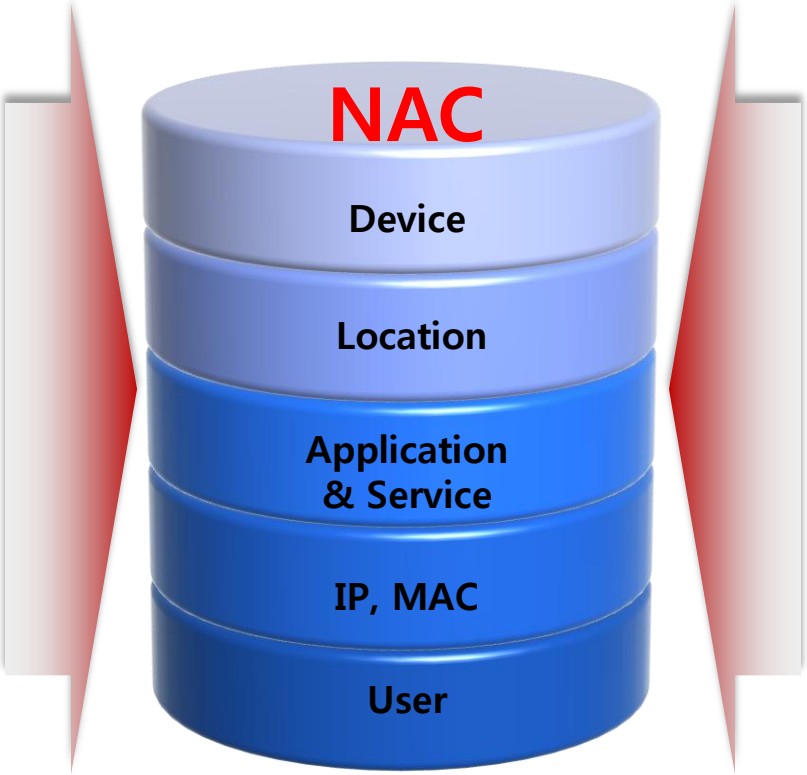
Full Visibility

Wired & Wireless Management

NAC(Network Access Control) of New Era

Internal Data Center

- 장비 탐지 정보
- 사용자 정보
- 설치 S/W 정보
- 사용자 위치 정보
- IP, MAC 정보
- AP정보, 위치 정보
- 운영 서비스 정보
- Patch 정보



- 사용시간 정보
- Up/down 이력
- IP 사용 이력
- 스위치 port 정보
- traffic 정보
- etc

Rich Interoperability

Makes 'Know the Unknown'

NAC

사용자 인증
+PC 자산관리
+네트워크 접근제어
+네트워크 보안관리
+어플리케이션 관리
+모바일 관리
+IP 관리
+etc...

Big data

Next Generation "NAC"

info@geninetworks.com