

**Hewlett Packard  
Enterprise**

# UBA(User Behavior Analytics)

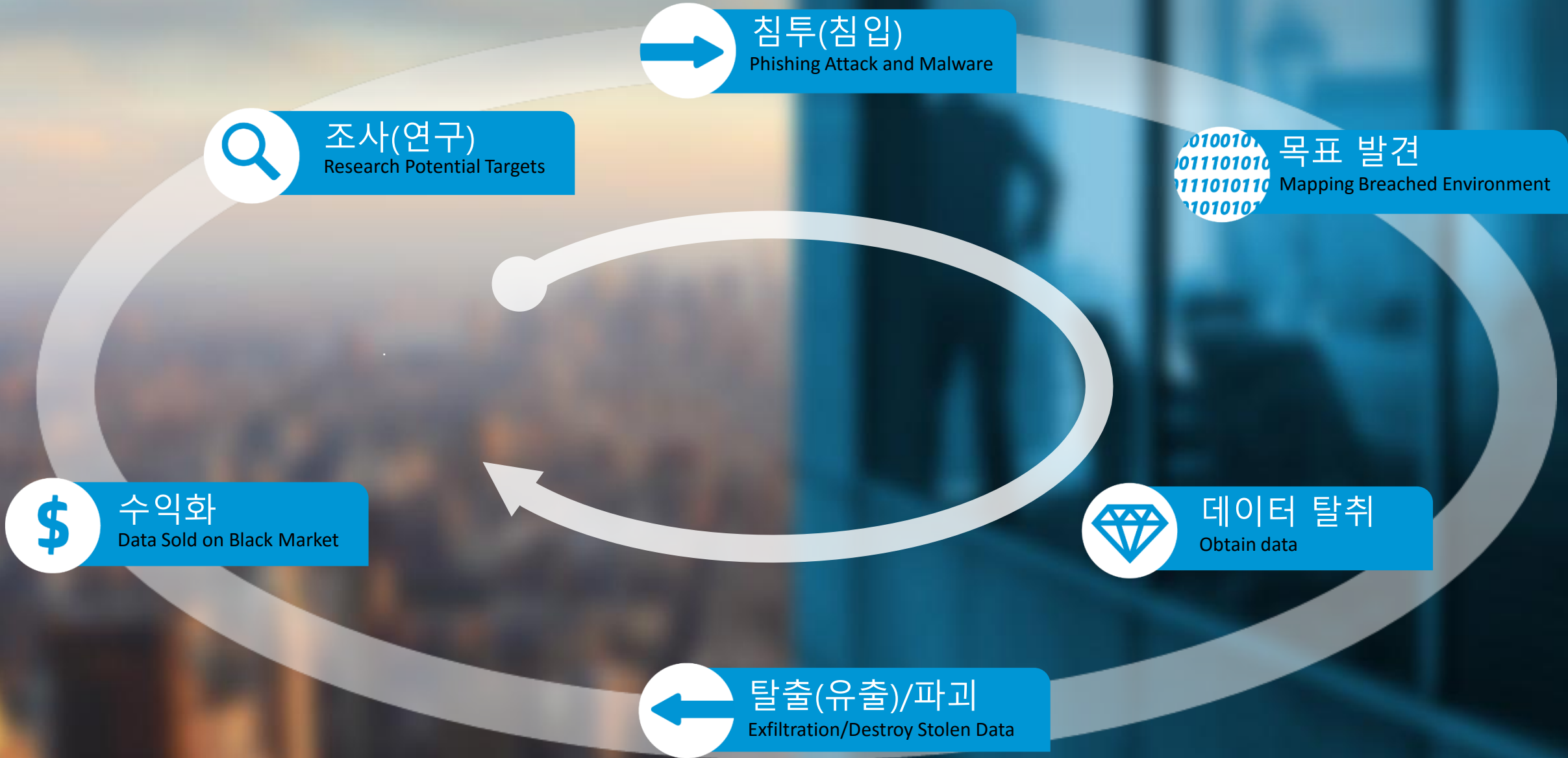
내부정보 유출을 방지하기 위한 프로파일링  
기반의 사용자 이상행위 분석 시스템

**HPE Security**

2016. 4. 21.



# Attack Life Cycle



---

# Current Security Solutions ...

## NETWORK SECURITY

HOW DO I CONNECT SAFETY TO THE WEB?

- ✓ Firewall, intrusion prevention and protection
- ✓ Remote SSL VPN
- ✓ Identify and access management

## CONTENT SECURITY

HOW DO I DEAL WITH THE SOCIAL MEDIA TREND?

- ✓ Email, web and data content security
- ✓ Secure web gateway
- ✓ Application security

## ENDPOINT SECURITY

HOW DO I DEAL WITH THE BYOD TREND?

- ✓ Mobile device security
- ✓ Data loss prevention and protection
- ✓ Data encryption
- ✓ Anti-malware / SPAM protection

# 주요 보안 사고 원인은 무엇일까? 왜 반복될까?

지능화된 해킹 공격, 내부 위협 요소, 보안 관리 미흡 그리고 보안 솔루션의 한계

## 국내/외 주요 보안 사고 사례



## 지속적으로 반복되는 보안 사고 주요 원인은

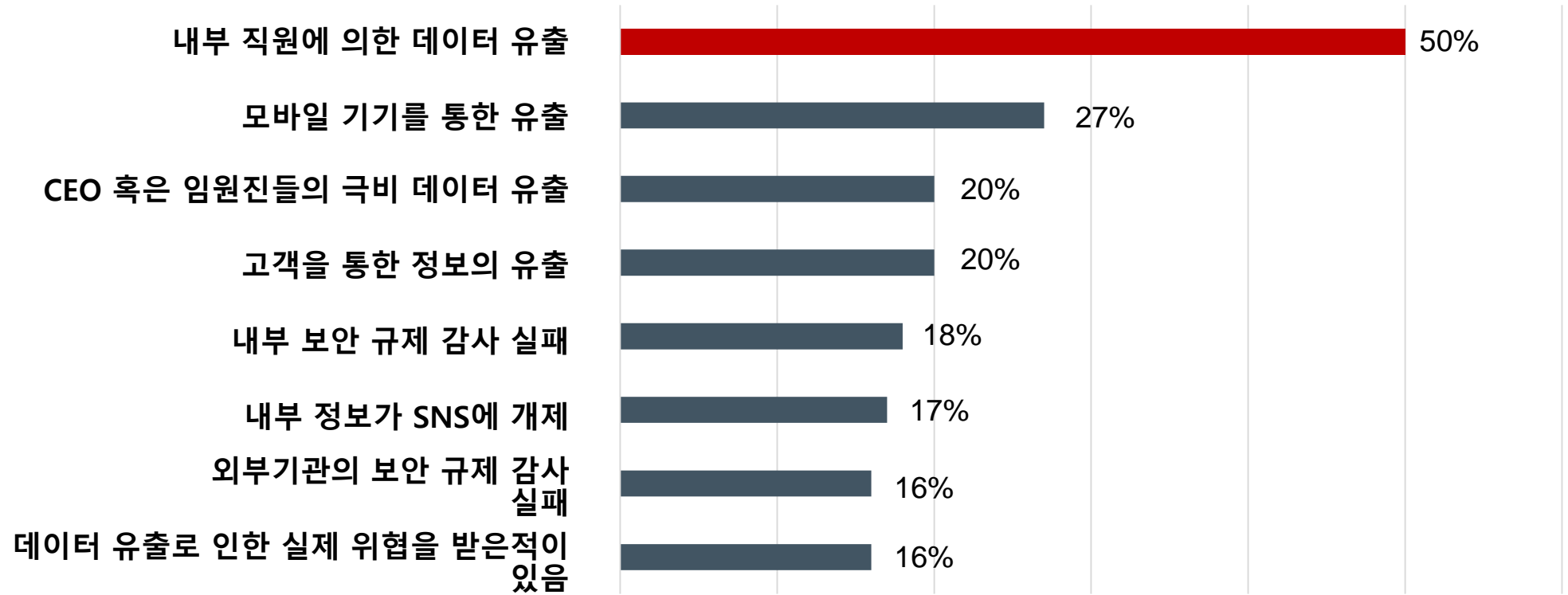
- 다양한 데이터 수집 요구에 대한 보안 대응 기술 부재
- 데이터 자산가치의 증가에 따른 내부자의 악의적인 목적에 의한 정보유출 보안 사고
- 중요정보 및 개인정보 유출에 대한 보안 기술 대책 부재 및 관리 체계 미흡
- 다양한 애플리케이션 구축/운영시 사용되는 데이터 원본 데이터 노출로 인한 유출

# The Challenge: How to Detect and React Quickly

## 대부분의 데이터 유출 사고는 인가된 사용자에게 의해서.....

정보 보호 업체인 “Websense Security Labs”이 미국, 영국, 캐나다, 호주의 IT관리자 1,000명 을 대상으로 조사한 결과 보고서 ‘보안 전문가 및 컨설턴드(Security Pros and Cons)’가 발표됐다. 이 보고서에 따르면, 데이터 유출 사고가 점점 더 확산되고 있으며 현업 임원들까지도 이에 관여하고 있는 것으로 나타났다.

- Network World



# The Challenge: How to Detect and React Quickly

데이터 유출의 83%는 정상적인 사용자를 통해서 이뤄진다

Source : Verizon Data Breach Report

## Attack vector



악의의 사용자  
Rogue Users

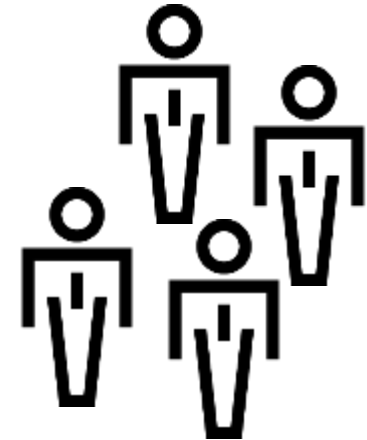


탈취된  
사용자 계정  
Compromised Accounts

## Security challenge



급증하는  
데이터 및 범위



개인별 다수의  
사용자 ID 보유

내부 사용자가 가장 약한 고리이다! 어떻게 탐지하고 대응할 것인가?

---

# The Solution : User Behavior Analytics

## Security Analytics 요구 조건

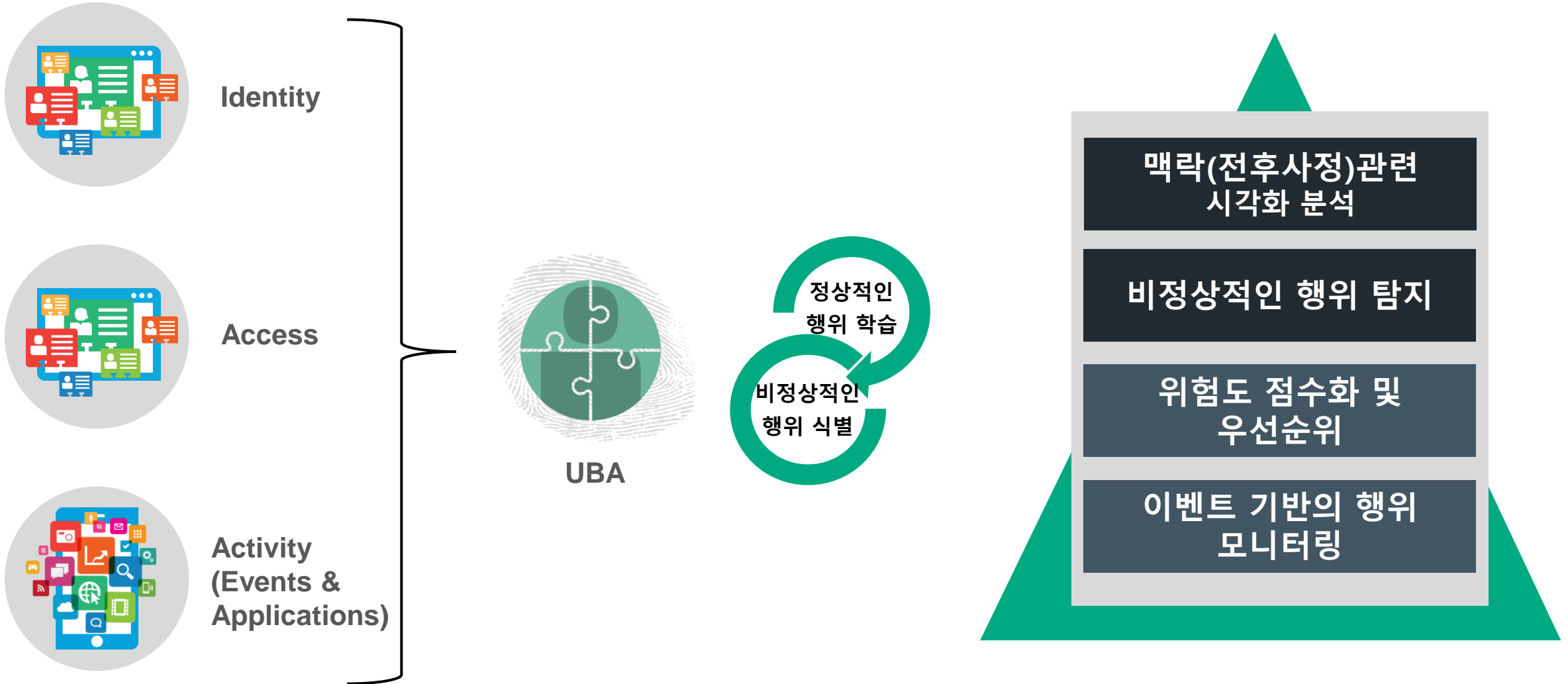


Unknown Threat

- 자동화 분석 | **NOT manual analysis**, Machine Based
- IP 기반 행위 뿐만 아니라 Entity 중심 분석
- 다른 Entity 간 이상행위를 상관관계 분석



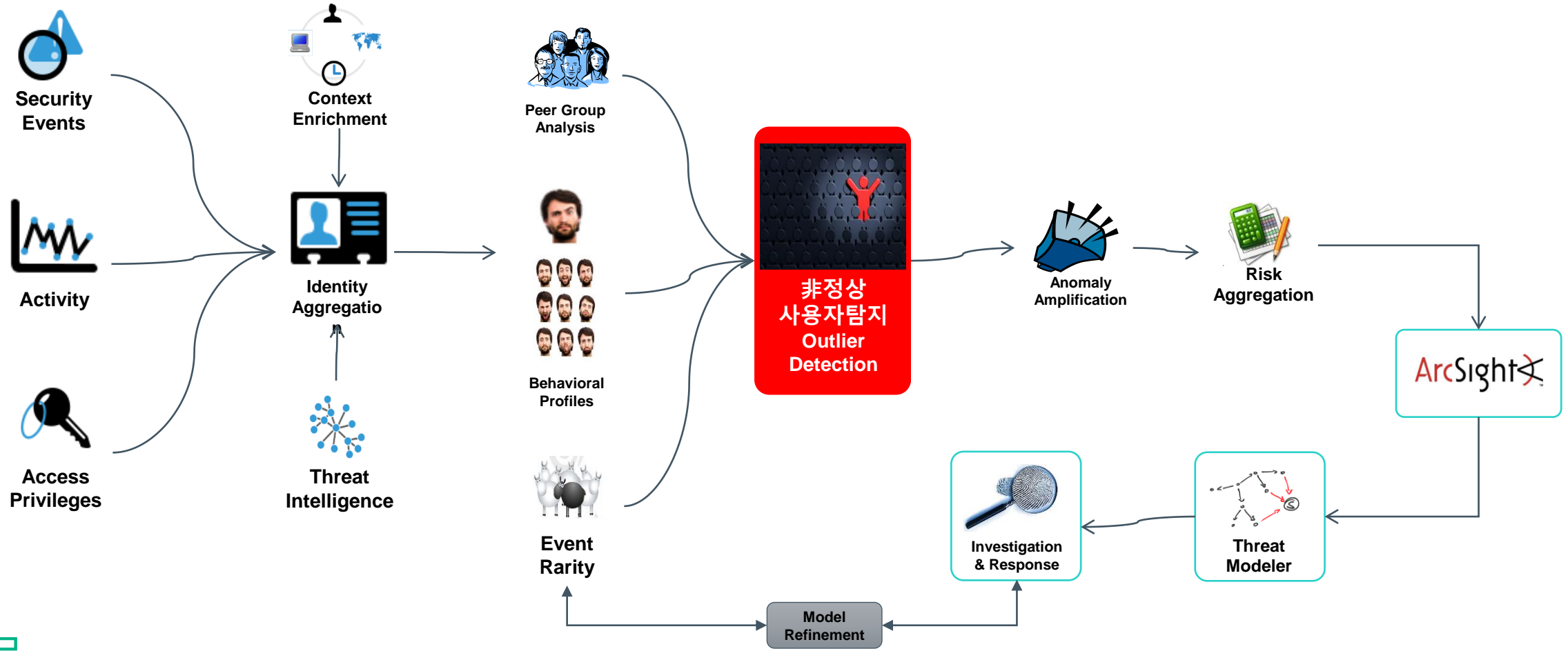
# HPE User Behavior Analytics Overview





# UBA User Behavior Analytics 동작 원리 및 분석 프로세스

## 프로파일링 기반 이상행위분석 기반 Insider Threat 보안 분석 프로세스



# UBA User Behavior Analytics 동작 원리 및 분석 프로세스

## Calling out the abnormal behavior based on identity & behavior context





# ArcSight UBA Security Intelligence

---

# Behavior Based Analysis

# Step 1: 신원(ID) 및 행위 context 기반의 비정상 행위 도출



Encrypted User Information

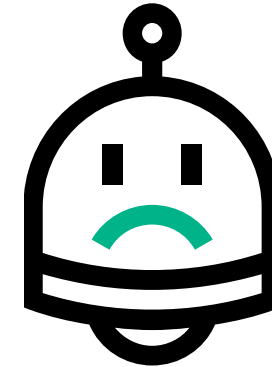
Identity context



Behavior context

Detecting the abnormal

- Peer outlier
- Event rarity
- Amount spike
- Frequency spike



Risk scoring & prioritization

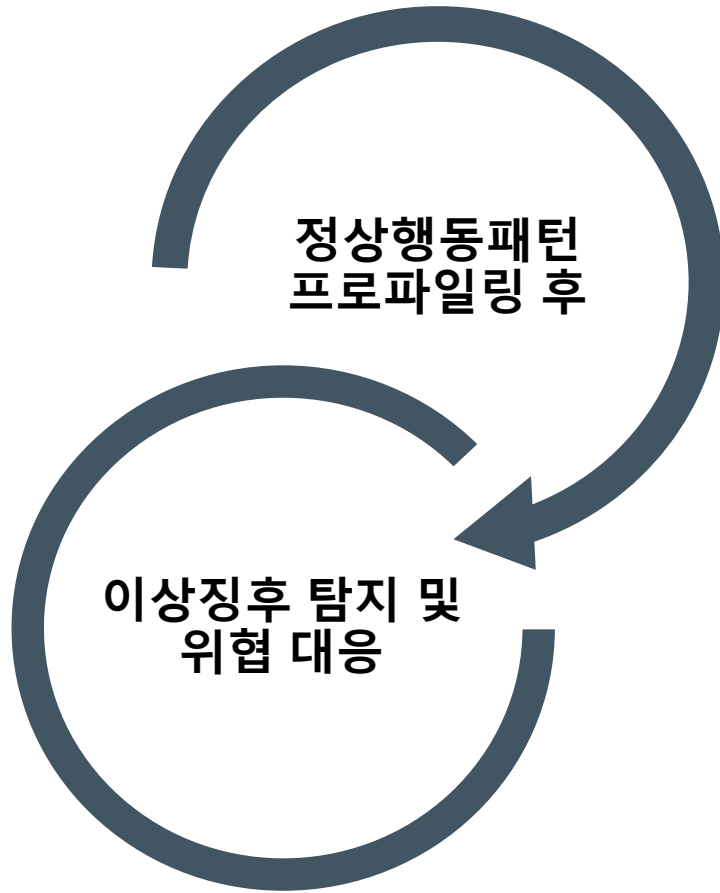


Visualization



Decrypted User Information

## Step 2: 사용자의 정상 행위 정의



### 사용자 행동패턴 프로파일링 데이터마이닝 알고리즘

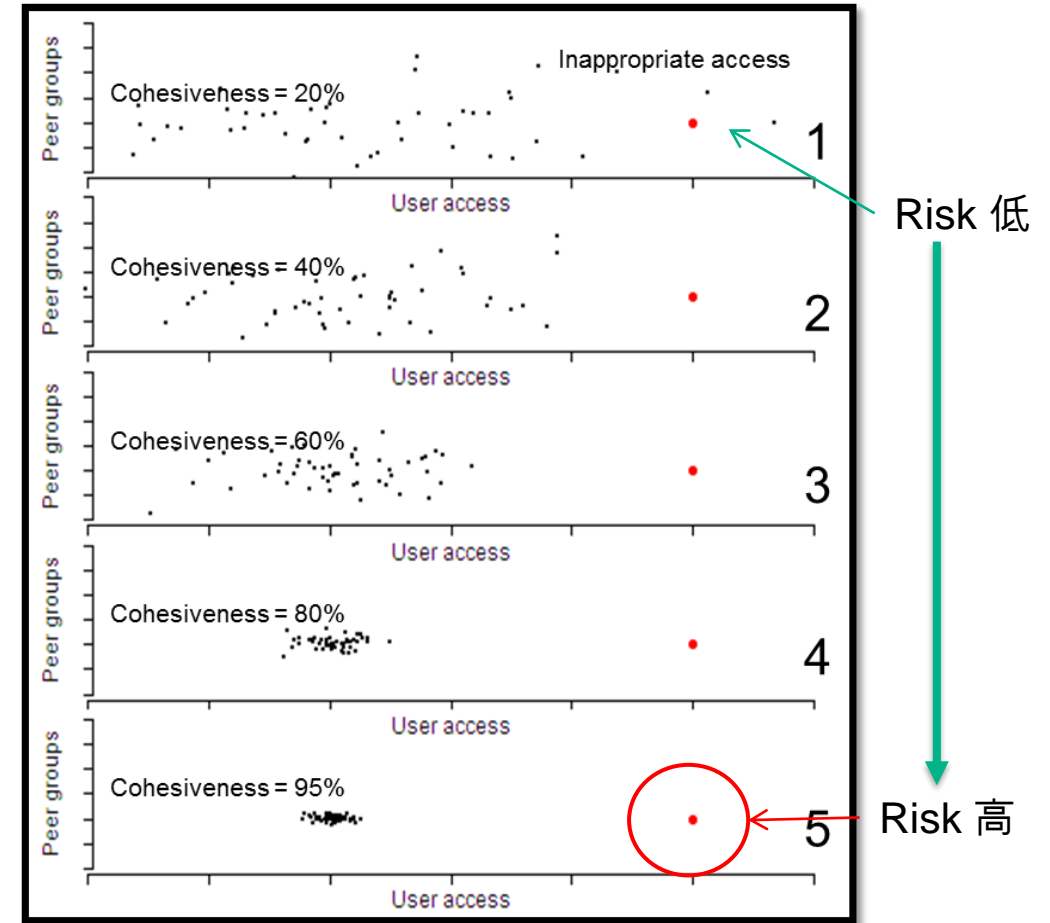
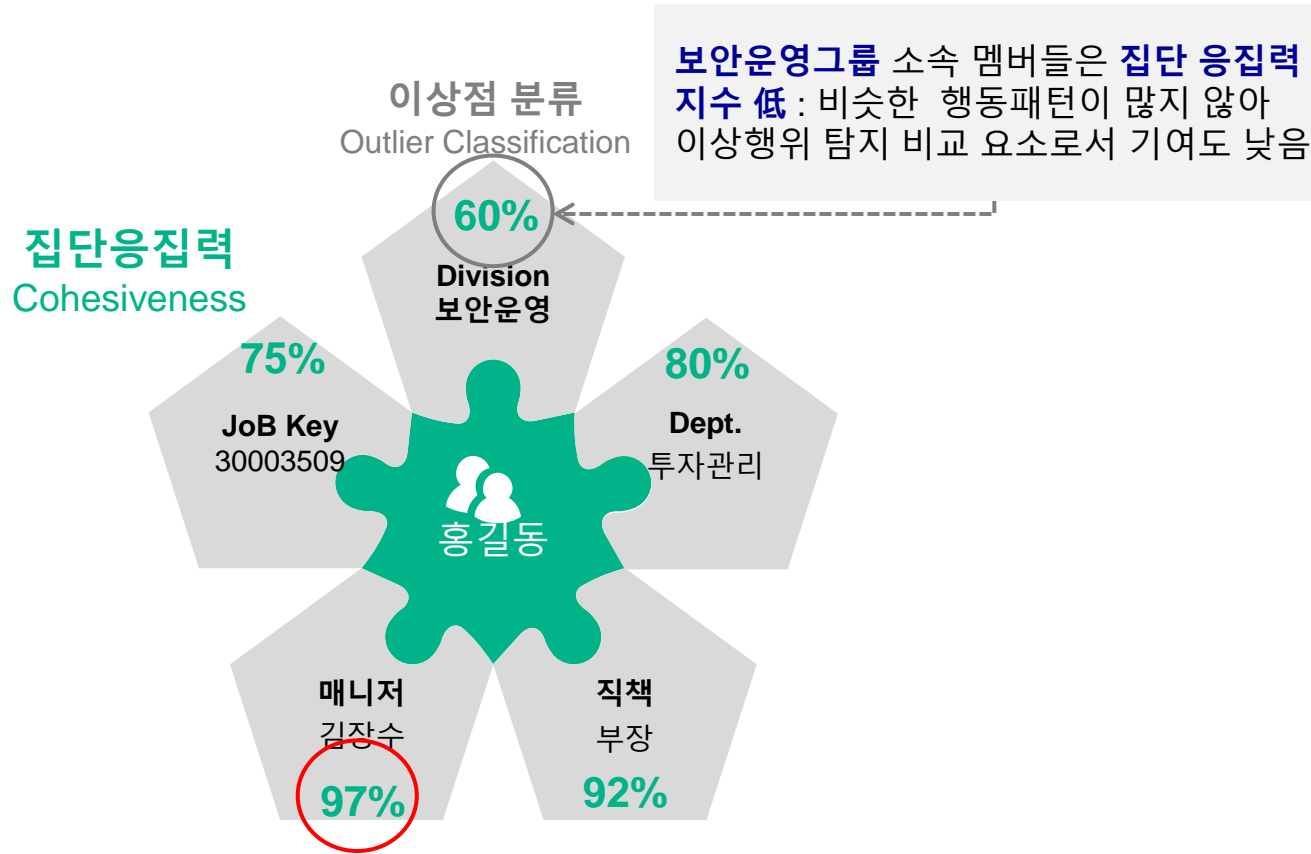
- 각각의 애플리케이션 및 수집 로그 이벤트 기준으로 정상 사용자의 행위패턴을 프로파일링, 이를 기반으로 정상행동패턴 기준 (Baseline) 설정
- 트랜잭션 양 / 빈도수(시간별, 일별, 주별, 월별) / 트랜잭션 타입, 프로세스,....
- 동료그룹 (Peer Group)의 행동패턴 학습하고 이를 기반으로 동료그룹 정상행동패턴 기준 (Baseline) 설정 (i.e. 관리자, 업무부서, 시스템 종류, 운영체제, 위치, ...)
- IP, 로그인 시도, 파일 접근, 트랜잭션, 소량의 자금 다수 이체시도, 퇴사자의 시스템 접근시도.. 다양한 활동 패턴 프로파일링 지원 - 과거 보지 못했던 잠재적인 보안 위협 식별 목적

# Step 3a: 비정상 사용자 탐지





# Step 3b: 동료들과 비교하여 비정상 사용자 탐지



## 동료그룹과의 비교 분석

- 그룹 : 동일 목적/역할의 사용자 집단
- 동료그룹과의 행동패턴 비교분석을 통한 이상 징후 탐지
- 집단응집력 지수(Cohesiveness) : 동료집단소속 멤버의 동일행동패턴 지수

# Step 4: 위험 점수화 및 우선순위를 통해 가장 위험한 사용자 식별

## 정적 리스크 (Criticality)

- 리스크 평가 기반 (자산 자체의 기본 보유 리스크): 메인프레임/리소스와 같은 중요한 자산 및 애플리케이션
- 고 위험도 자산 접근이 허용된 슈퍼사용자 및 그룹

## 동적 리스크 (Derived)

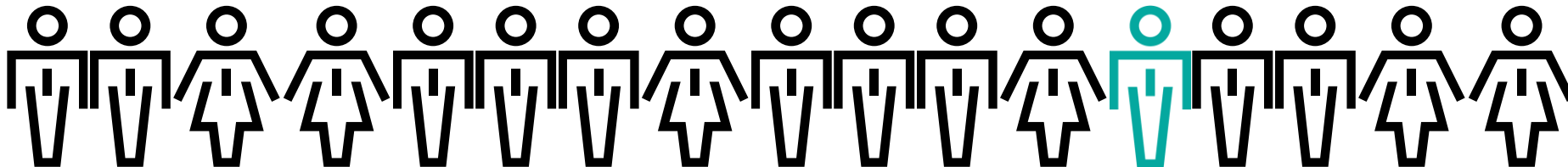
- 보안정책에 의해 탐지되는 리스크:
- 보안정책 위배
- 비이상적인 행위
- 동료그룹과의 비교 시 이상 징후

## 신원(Identity) risk (Risk boosters)

- "신원" 컨텍스트에 의해 발행하는 리스크(리스크 상승 촉진제)
- 인사 데이터 (계약직 혹은 협력업체 직원), 퇴사 위험, 최근 업무 평가 시 낮은 점수...



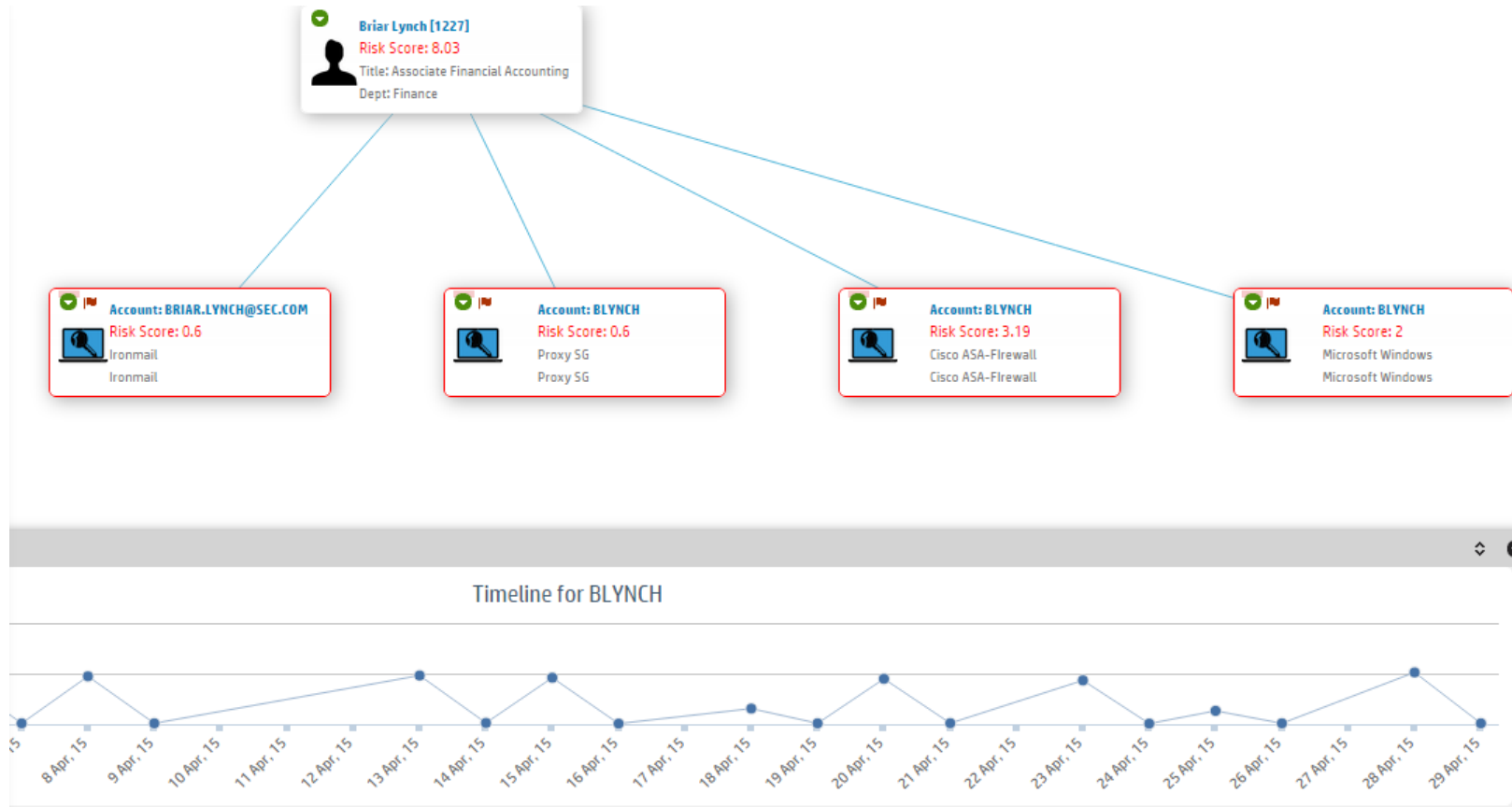
Highest risk users



Preserving privacy through encryption

# Step 5: Link Analysis를 통해 가장 위험한 사용자 조사

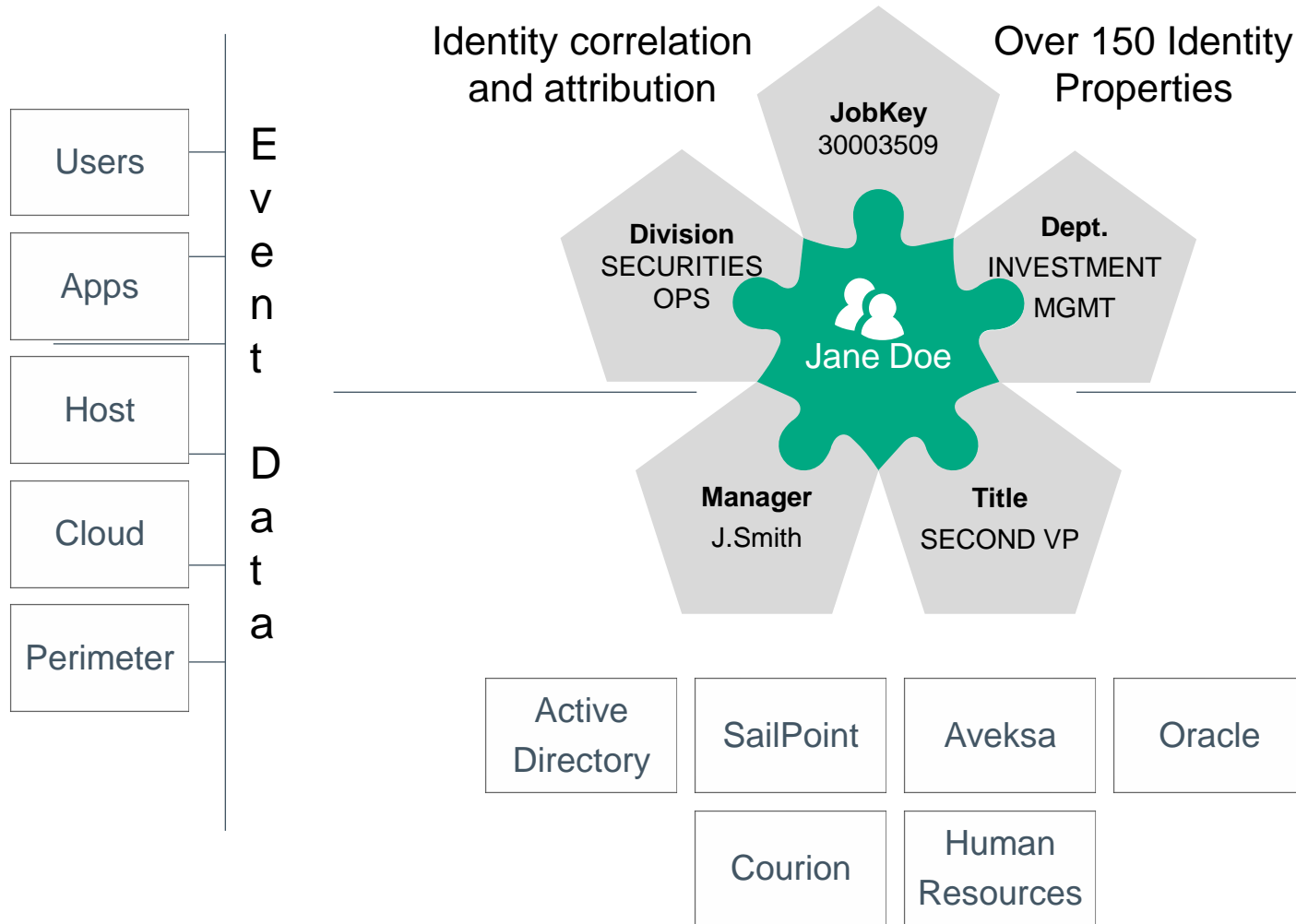
탐지된 이상징후에 대해 리스크 스코어링 기반 연계분석 GUI 제공  
드릴다운 (Drill Down) 메뉴를 통한 엔터티 간 연관관계 분석



---

# Rule Based Analysis

# Step 1: Understand the User



Employee Type	Full Time
	Contractor
	Part Time
Shared Properties	Division
	Department
	Manager
Employee Data	Hire Date
	Term Date
	Contract End
Lookup Data	IP metadata
	User Watchlist
	Asset Criticality
HR Data	Sentiment
	Phone/Address
	Last Review

# Microsoft Windows Rule-Based Policies

Rule-based policies		
Policy Name	Description	Criticality
Activity Conducted by Terminated Users	Detect activities done by users that have status=0 and Activity Date greater than User Termination Date	High
After hours login using privileged account	Accounts on Privileged Accounts watch list performing Security:528 and Microsoft-Windows-Security-Auditing:4624 event after 7pm and before 6 am.	High
Audit Log Tampering	Detect Windows Event id: 517 or 1102	Medium
Interactive Logon by Privileged Account	Detect interactive Successful Logons by Accounts tagged as service accounts. Account Type in ("high privileged","service","firecall") and Logon Type in (2,10,11) and Transaction is a successful Logon	Low
Password changed on privileged account	Detects password changes to Accounts in the Privileged account Watch list	High
Privileged Activities by Non Privileged User	Accounts performing privileged activities is not in approved Privileged Users list. Approved privileged users must be set with high criticality	High
Privileged Logon by Non Privileged User	This alert is triggered when a user account logs on with Privileged Access and the user account is not tagged as critical user.	High
Security Access Granted by Non Admin Accounts	Account Type is not in ("High Privileged" or "Service" or "Firecall") and Windows Event Id In (632,4728,636,650,4732,4746,660,4756)	Low
Security Configuration Changes by Non Admin Accounts	Account Type not in ("high privileged","service","firecall") and Windows Event ID IN (612,4715,4719,4739,643)	Medium

# Examples of Behavior and Peer Detection

## Unusual Activity

## Inappropriate Activity

## Unusual Transaction

### 1) Build Context

- Poor HR Review, Upcoming Termination
- Database username to identity correlation

- Multiple user names to identity correlation
- High privileged account to identity correlation

- User name to identity correlation
- IP address to user mapping
- User IP to threat intelligence feeds

### 2) Classify Normal

- User profile of frequency and time of DB access
- User/peer profile of common database commands
- User/peer profile of normal volume of database files accessed and removed

- User profile of normal privileged account activities
- Peer profile of normal privileged account activities

- User profile of normal IP addresses accessed
- User profile of normal VPN geo-locations and times

### 3) Detect the Anomaly

- **Behavior:** Monthly increase in DB access
- **Peer:** Anomalous DB command-clear logs, wire transfer, select \*, Anomalous DB access activity

- **Peer:** Anomalous high privileged account entitlement & commands

- **Behavior:** Never before seen IP address, VPN geo-location

### 4) Classify, Score & Visualize, Investigate

- Toxic combination, amplify risk score
- Trace user activity on separate systems and accounts

- Prioritize privileged account violations, Three Strike rules, Multiple Indicators
- Visualize user association with privileged accounts

- Investigate compromised account, IP associate with other users
- Identify activities associated with account after compromise





# Use Cases

# UBA User Behavior Analytics 분석 사례 - Use Case

## 프로파일링 기반 이상행위 보안 분석 - What HP UBA can do!

: A사 연구원 홍길동은 공격타겟이 되어 자신의 계정 및 비밀번호가 노출되었으며 공격자는 이를 이용해 A사의 중요 지적자산(IP)이 도난당한 사례

### 계정 도난 후 지적자산 유출사례



홍길동: A사 연구원

Target >>

IAM HR AD LDAP

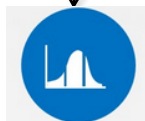


사용자에게 접근권한이 허가되었는가?

ArcSight

What >>

How >>



Behavior Anomaly



Peer Anomaly



Suspicious Activity

### What Was Seen

- ✓ 스피어 피싱 이메일
- ✓ 계정정보 외부 이메일 주소로 전송
- ✓ 적법한 사용자의 중요자산 시스템으로의 접근 시도
- ✓ 적법한 사용자의 중요자산 시스템으로의 접근 허가

### What was missed | HP UBA 커버리지

- 기존에 사용하지 않던 IP, 알려지지 않은 IP 로부터 높은 권한 보유 사용자 접근 시도(R+1)
- 평상시와 다른 접근시간 및 접근 빈도(R+1)
- 이전과 다른 사용자의 애플리케이션 접근 및 사용 명령어/수행 트랜잭션(R+1)
- 동료연구원들과 비교 시 평상시와 다른, 과다한 다수의 파일 접근 시도(R+1)
- 민감한 데이터의 대용량 다운로드 시도(R+1)

# UBA User Behavior Analytics 분석 사례 - Use Case

## Event Spikes 기준 사용자 행위 분석

Stuart Bowden은 2일 동안의 normal baseline 결과는 18번 Sharepoint 파일에 접근함

Behavior Anomaly in Sharepoint Document Access Policy Details														
Case ID	Threat Indicator	Datasource	Resource Name	Hostname	Employee Id	First Name	Last Name	Account	Transaction	Event Date/Time	Raw Score	Source IP		
	High Volume of Document Access	SECSHAREPOINT03	SECSHAREPOINT03		2866	Stuart	Bowden	2866	EVENT: View OBJECT TYPE:	07/27/2014 02:00:00	0.09			
Check Name		Frequency	Baseline	Raw Score	Generated Date									
Check for Daily Usage Threshold		18	2	0.09	2014-07-31 17:14:26.0		View Violations		Details					

Watchlist User Uploading Files Symantec DLP Endpoint Policy Details										
Violation Date	Event Date/Time	Resource Name	Account	POLICY CONDITION NAME	EVENT TYPE ID	ENDPOINT CONTENT ID	ENDPOINT INCIDENT ID	AGENT RESPONSE		
Mon Aug 04 18:55:32 CDT 2014	Mon Jul 14 19:46:16 CDT 2014	Symantec DLP Endpoint	NT\SBOWDEN	US Social Security Numbers	HTTP/SSL	15720	1468	Action Blocked		
Mon Aug 04 18:55:32 CDT 2014	Tue Jul 15 00:20:17 CDT 2014	Symantec DLP Endpoint	NT\SBOWDEN	C Source Code	HTTP/SSL	16070	1477	Action Blocked		

이 내용을 기준으로 분석 및 조사 후, 이 파일들은 confidential 파일였고, DLT 솔루션 탐지 이벤트 확인 결과 특정 웹사이트에 업로드 된 내용을 확인됨

# UBA User Behavior Analytics 분석 사례 - Use Case

## Rick Scoring | Prioritizing the Results in Business Terms

Employee Id	First Name	Last Name	Manager	Department	Division	Title	Job Code	Risk Score <sup>✓</sup>	Grade	GPA
2866	Stuart	Bowden	ROBERT WELLINGTON [1013]	Data Services	Global Technology	Associate-Database Administrator	M1	20.96	Critical	0.0

Threats [8]

Watch List [1]

# of Cases	Detected Date	Threat Name	Policy Name	Account Name	Risk Score
0	2014-08-04 12:54:38.0	Suspicious Process Detected	Behavior Anomaly	CS-SBOWDEN\$ [SecDCDAL01]	1.0
0	2014-07-31 17:14:26.0	High Volume of Document Access	Behavior Anomaly in Sharepoint Document Access	2866 [SECSHAREPOINT03]	0.09
0	2014-07-31 18:18:29.0	Anomalous DLP Violations	Behavior Anomaly in DLP Violations	SBOWDEN@SEC.COM [Symantec DLP Network]	0.07
0	2014-07-31 17:09:57.0	Suspicious Document Access	Peer Based Anomaly	2866 [SECSHAREPOINT03]	17.0
1	2014-08-04 16:55:32.0	Possible Data Exfiltration Attempt	Watchlist User Uploading Files Symantec DLP Endpoint	NT\SBOWDEN [Symantec DLP Endpoint]	1.0
0	2014-07-31 18:57:45.0	Possible Data Exfiltration Attempt	Watchlist Users Sending Attachments to Personal Emails Symantec DLP Network	SBOWDEN@SEC.COM [Symantec DLP Network]	0.6
0	2014-07-31 20:03:30.0	DLP Violation Pattern Observed	Frequent Violations Detected	SBOWDEN@SEC.COM [Symantec DLP Network]	0.6
0	2014-07-31 21:35:14.0	Possible Data Exfiltration Attempt	Files Uploaded	NT\SBOWDEN [Symantec DLP Endpoint]	0.6

# UBA User Behavior Analytics 분석 사례 - Use Case

## Visualization 기반 Workbench | Data Driven Discovery

**Stuart Bowden [2866]**

EmployeeId: 2866  
 Firstname: Stuart  
 Lastname: Bowden  
 Title: Associate-Database Administrator  
 Department: Data Services  
 Division: Global Technology  
 RiskScore: 20.96

**Associated Objects**

- Activity Accounts [Total: objectsList]
- Organizations [Total: 1]
- Policies Violated [Total: 8]

Policy: Behavior Anomaly  
 # of Cases: 0  
 Detection Date: Mon Aug 04 2014 14:54:38 GMT-0500 (CDT)  
 Threat: Suspicious Process Detected  
 Resource: SecDCDAL01  
 Account: CS-SBOWDENS  
 Risk Score: 1

Policy: Behavior Anomaly in Sharepoint Document Access  
 # of Cases: 0  
 Detection Date: Thu Jul 31 2014 15:14:26 GMT-0500 (CDT)

Performed Date/Time	Account Name	Network Address	EVENT TYPE ID	ENDPOINT CONTENT ID	POLICY NAME	CONDITION VIOLATION COUNT	FILE NAME
Tue Jul 15 00:20:17 CDT 2014	NT\SBOWDEN		HTTP/SSL	16070	Source Code	87.0	sockets.c TextBufferComponent:1 TextBuffer
Mon Jul 14 19:46:16 CDT 2014	NT\SBOWDEN		HTTP/SSL	15720	Americas PII (DCM) Credit Card Data HIPAA and HITECH (including PHI)	380.0	CustomersForProcessing_West.xls

Enter a search criteria to search for transactions. Select transaction and click on Apply to include it in the filter.

---

# User Behavior Analytics Use Case 예제

## Key Use Case Areas

### Insider Threat Intelligence

- Data theft detection and prevention
- Fraud detection and prevention
- VIP Snooping
- Sabotage detection and prevention

### Fraud Intelligence

- Enterprise fraud detection
- Web fraud detection
- Customer Service Rep fraud detection

### Cyber Event Intelligence

- Targeted attack detection
- Low and slow attacks
- Advanced malware detection
- Investigation & response

### Data Exfiltration Analytics

- Data theft detection and prevention
- Signature less and correlation analysis of Network DLP and Host DLP data
- Risk ranking of incidents and case management

### Identity & Access Intelligence

- Access risk monitoring & cleanup
- Risk-based access requests
- Risk-based access certifications

### Application Security Intelligence

- Privilege account misuse
- Unusual view/download of sensitive information
- Account takeover
- Off the shelf and custom apps

### Big Data Analytics

- Data mining for security intelligence
- Purpose built security analytics on Hadoop, Cloudera other data big data stores
- Visualization of linkages in large datasets

### Continuous Risk Monitoring

- Continuous risk monitoring
- Organization risk scorecard
- User risk scorecard
- System risk scorecard

# Investigate Highest Risk Users through UBA Dashboards

The screenshot displays the HP UBA dashboard interface. The top navigation bar includes 'Dashboard', 'Manage', 'Run', 'Respond', 'Reports', and 'Configure'. The main content area is titled 'High Risk' and features a table of users. The table columns are: # of Cases, Employee ID, First Name, Last Name, Manager, Department, Division, Title, Job Code, Risk Score, and Actions. The Risk Score column is sorted in descending order, with values ranging from 0.84 to 0.0. The left sidebar contains various navigation options like 'Users', 'Threats', 'Peer Based Activities', 'Resources', 'Organizations', 'ACCOUNT MISUSE', and 'Policies'. The top right corner shows 'admin' and 'Task Assistant' buttons.

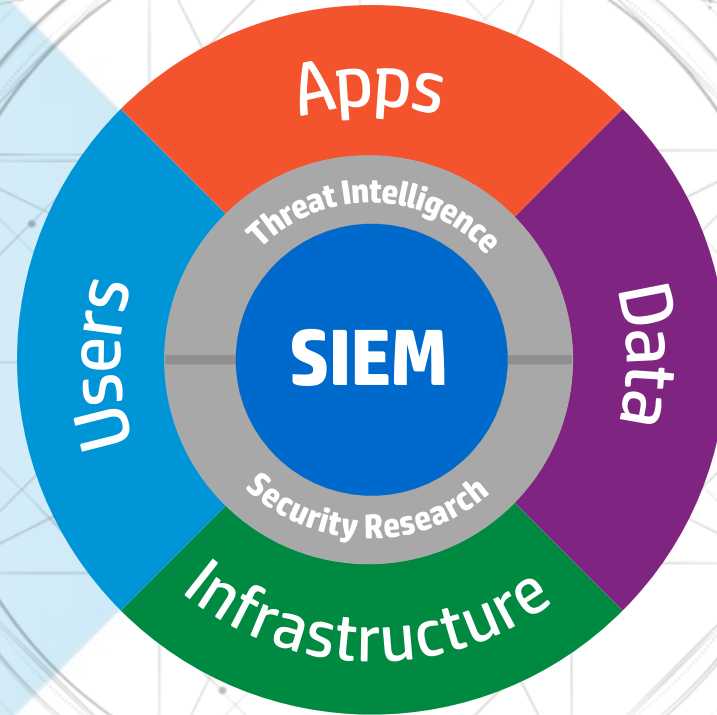
# of Cases	Employee ID	First Name	Last Name	Manager	Department	Division	Title	Job Code	Risk Score	Actions
	2256	Sinead	Snodgrass	2235	Information Risk	Corporate Risk	Associate Information Risk Services	R1	0.84	
	3210	Holmes	Lancaster	1160	Processing and Fulfillment	Business Banking	Associate Business Services	R1	0.61	
	2549	Louise	Mumaghan	2287	Credit	Global Markets	Associate Vice President Credit Market	R1	0.5	
	2616	Elaine	Noroney	2589	Debt Planning and Management	Corporate Strategy and Planning	Associate Debt Management		0.44	
	1940	Elizabeth	Waite	1853	Enterprise Loans	Global Banking	Associate Enterprise Loans	M1	0.39	
	1784	Aidan	Gilchrist	1084	Tech Support	Global Technology	Associate Technology Support Group	R1	0.22	
	1478	Erwin	Thomson	1365	Deposits and Debit Card Sales	Deposit and Card Products	Associate Deposits and Debit Cards	R1	0.01	
	1187	Maryam	Norris	1084	Tech Support	Global Technology	Associate Technology Support Group	R1	0.01	
	1020	HUAN	berringer	1013	Data Services	Global Technology	Associate Data Services	R1	0.01	
	1691	Mara	Rooney	1083	Payroll Processing	Corporate Human Resources	Associate Payroll Processing Admin	R6	0.01	
	2601	Maile	larry	2589	Debt Planning and Management	Corporate Strategy and Planning	Associate Debt Management		0.0	
	2281	Thomas	Maltony	2235	Information Risk	Corporate Risk	Associate Information Risk Services	R1	0.0	
	1401	Pardhan	Gunn	1402	Software Engineering Services	Global Technology	Associate Software Engineer	M3	0.0	
	2253	Sinead	Cotter	2235	Information Risk	Corporate Risk	Associate Information Risk Services	R1	0.0	
	2443	Orla	Morris	2442	Distressed	Global Markets	Vice President Distressed Assets	R1	0.0	
	2332	Darragh	Dyball	2287	Credit	Global Markets	Associate Vice President Credit Market	R1	0.0	
	1692	Harmony	Skiba	1083	Payroll Processing	Corporate Human Resources	Associate Payroll Processing Admin	R6	0.0	
	1948	Edward	Fusil	1944	Retail Banking	Global Banking	Associate Bank Teller	R1	0.0	
	1686	Rene	O'Byrne	1083	Payroll Processing	Corporate Human Resources	Vice President Payroll Processing Admin	R6	0.0	



# Summary

알려진·알려지지 않은 보안위협 대응 및 내부 통제 강화 필요

- Monitor** user behavior
- Analyze** anomalies
- Enforce** by activating forensics and investigation



“상황정보기반 /공격시나리오기반/과거데이터 기반/ 내·외부 보안위협 인텔리전스 연계/ 실시간 프로파일링 기반 이상행위 실시간 상관분석”을 통한 대응 전략 플랫폼 구축 필수

**보안위협 탐지, 예측, 예방을 위한 필수요소**





---

**Hewlett Packard**  
Enterprise

**Thank you**

**HPE Security**  
[danny.chang@hpe.com](mailto:danny.chang@hpe.com)