Hewlett Packard
Enterprise

Intelligent SecOps

“실시간 상관분석과 빅데이터 분석을 하나로”

한국HPE 황원섭 차장 (bob.hwang@hpe.com)

2016년 전 세계인의 주목을 끌었던 뉴스

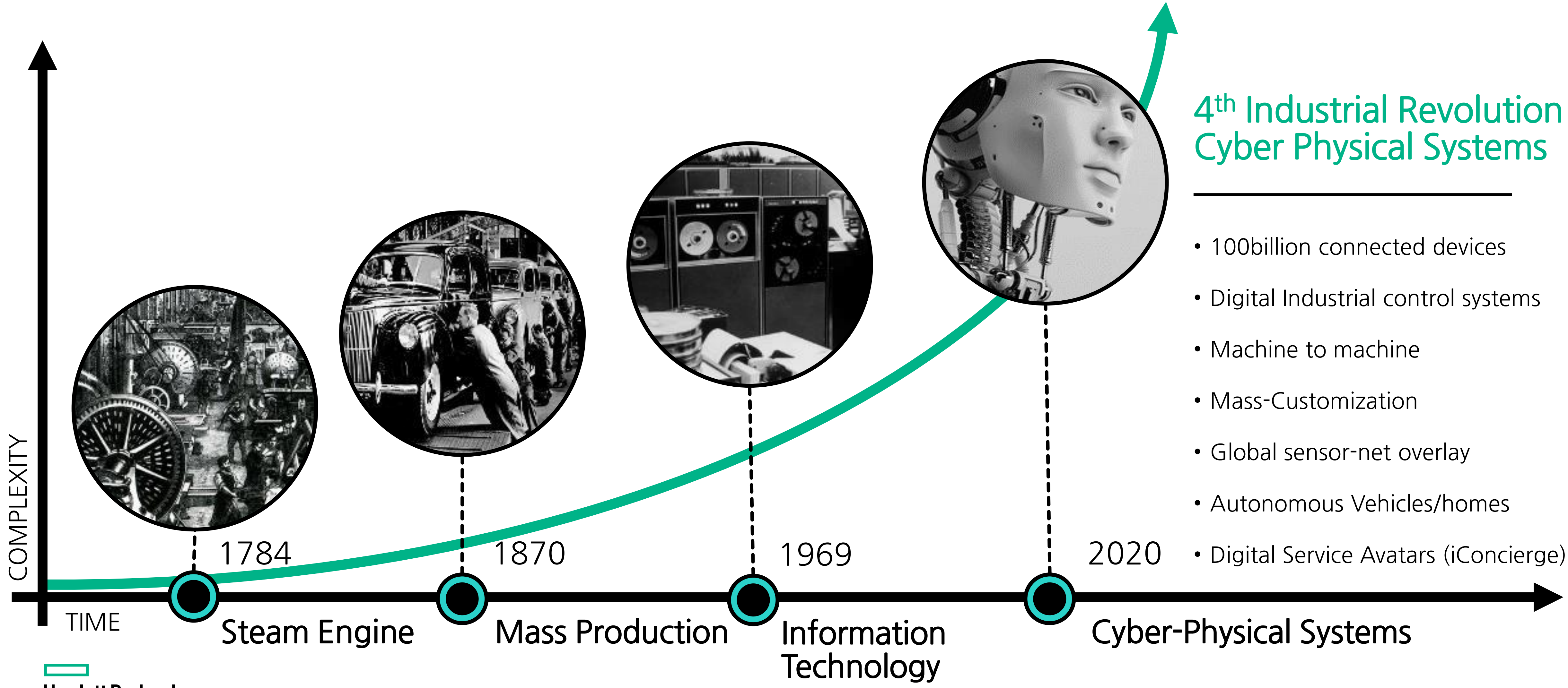
"AI 알파고가 이세돌 9단과의 대국에서 이겼다." -> 4주 동안 딥러닝으로 400만 번의 경기를 반복

"구글의 무인 자동차가 300만km 주행에 성공했다." -> 초당 1GB 규모로 발생하는 센서 데이터를 분석

"미국의 어떠한 언론도 트럼프의 대선 승리를 예측하지 못했다." -> 빅데이터만이 트럼프의 승리를 예측

Hewlett Packard
Enterprise

제4차 산업혁명은 이미 시작됐다! - Klaus Schwab



COMPLEXITY

TIME

1784

Steam Engine

1870

Mass Production

1969

Information Technology

2020

Cyber-Physical Systems

4th Industrial Revolution Cyber Physical Systems

- 100billion connected devices
- Digital Industrial control systems
- Machine to machine
- Mass-Customization
- Global sensor-net overlay
- Autonomous Vehicles/homes
- Digital Service Avatars (iConcierge)

사이버 위협에 대한 신속하고 효율적인 보호방안 필요

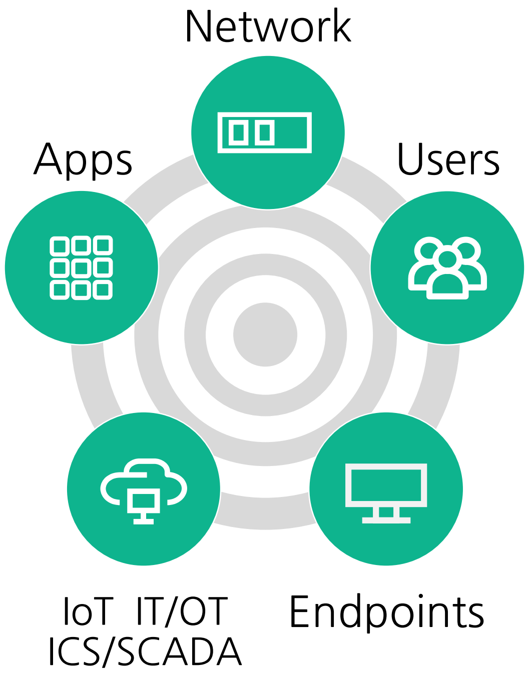
- 조직의 공격 빈도가 증가하고 있다[1] …

Malware
% of respondents
98%

Malicious insider
% of respondents
99%

Phishing attacks
% of respondents
62%

- 내부 네트워크와 클라우드 모두 공격 대상이 되고 있다 …



- 공격자는 알려진 취약점과 알려지지 않은 취약점을 악용하고 있다[2]

44% **of security breaches** occur after vulnerabilities have been identified

75% **Mobile apps** with critical vulnerabilities

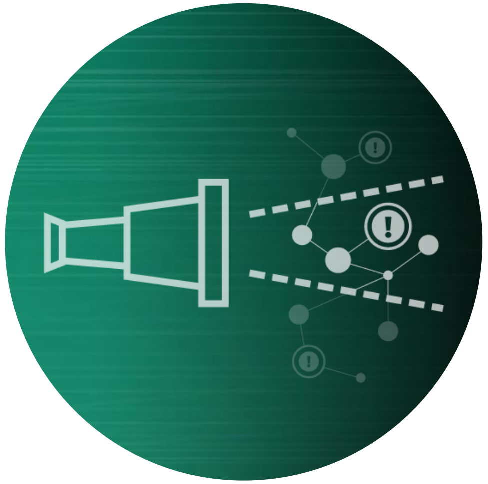
95% **of organizations** Have advanced malware infections in their web/e-mail & sharing infrastructures

Data Sources: HPE Security Research: [1]Cost of Cyber Crime [2]Cyber Risk Report 2015, & BMC

SOC(Security Operations Center)의 직면 과제

분석할 데이터의 증가

빠른 속도로 증가하는 이벤트를 수집 할 수 있수 있어야 하는데, 이것은 초당 수백 ~ 수백만건의 이벤트 수집 능력 필요



제한된 탐지 및 대응 기능

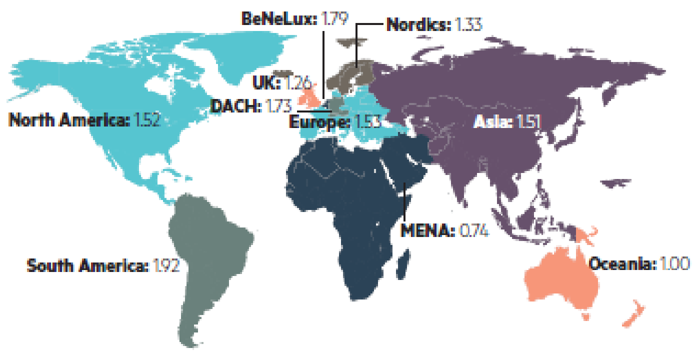
분석가들은 위협을 보다 효과적으로 발견하기 위해 연결된 모든 시스템에 대한 더 넓은 View(시야)를 제공하는 솔루션이 필요

복잡하고 느린 상세분석 기능

경보(Alert)의 우선 순위를 지정하고,
경보(Alert) 를 분석하고,
복잡한 검색을 수초내에 검색 필요

2016 State of Security Operations

154 assessments in 26 countries



Major findings

The **#1 concern** is access to **skilled resources**

24% not providing minimum security monitoring capabilities

85% not achieving recommended maturity levels

Trends

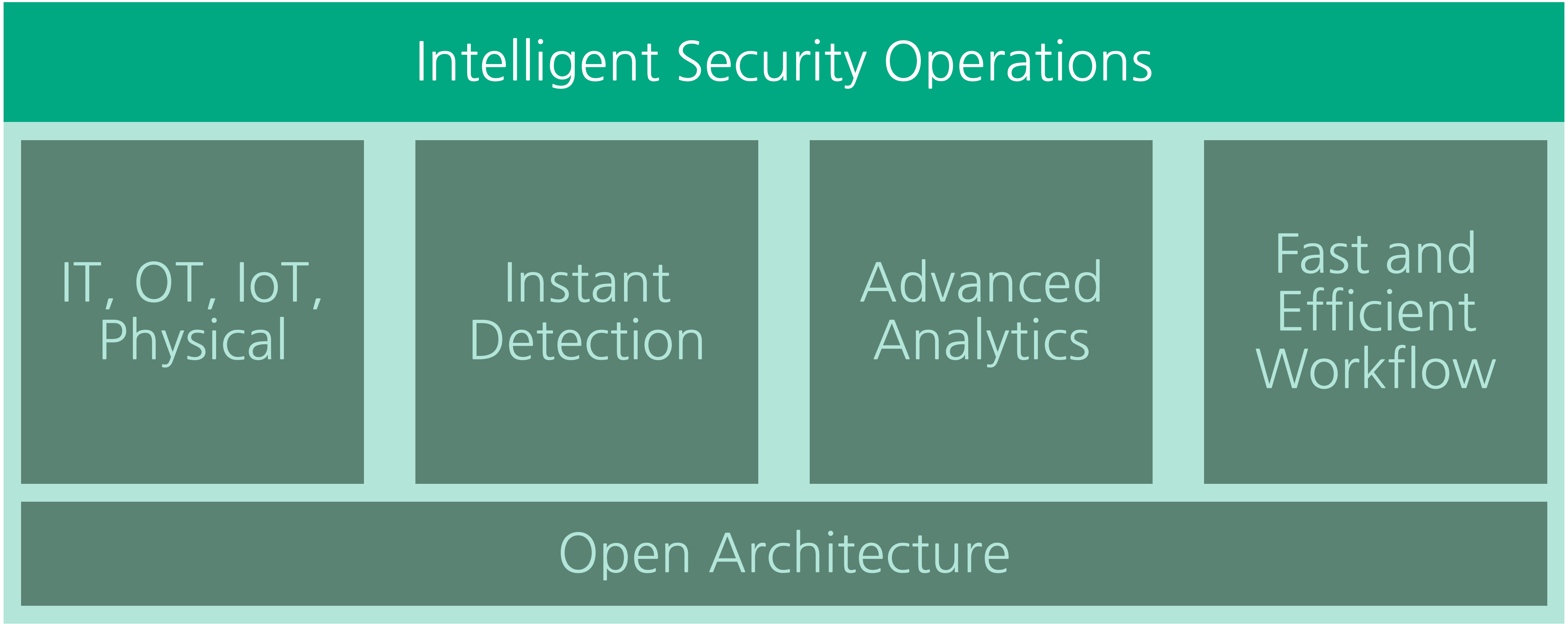
- Hunt teams and analytics
- Security orchestration and automation
- Hybrid staffing and infrastructure models
- Intelligence sharing

2015 SOMM Trend

Overall ↓	Energy ↓	Financial ↓	Government ↓	Healthcare ↓
Retail ↓	Services ↑	Telecom ↓	Technology ↓	Manufacturing —

Read the report at
hpe.com/software/StateOfSecOps

성숙한 SOC를 위한 핵심 요소



Intelligent Security Operations

IT, OT, IoT, Physical

Instant Detection

Advanced Analytics

Fast and Efficient Workflow

Open Architecture

Intelligent Security Operations

실시간 상관분석과 빅데이터 분석이 동시에 가능한 개방형 SIEM 플랫폼 필요

경계없는 가시성

실시간 경보 및 장기간 조사(분석), 모두를 지원할수 있는 방대한 로그 수집 능력을 가진 개방형 플랫폼

포괄적인 탐지 및 분석

제한없는 탐지와 대응을 위해, 실시간 탐지와 빅데이터 분석을 하나로 통합하는 구조로 확장

직관적인 조사 및 대응

우선순위, 조사, 엔터티 프로파일링 그리고 워크플로우를 이용한 신속한 대응 지원

ArcSight New Architecture

실시간 상관분석과 빅데이터 분석이 동시에 가능한 개방형 SIEM 플랫폼

Security Operations
(On-prem & Managed)

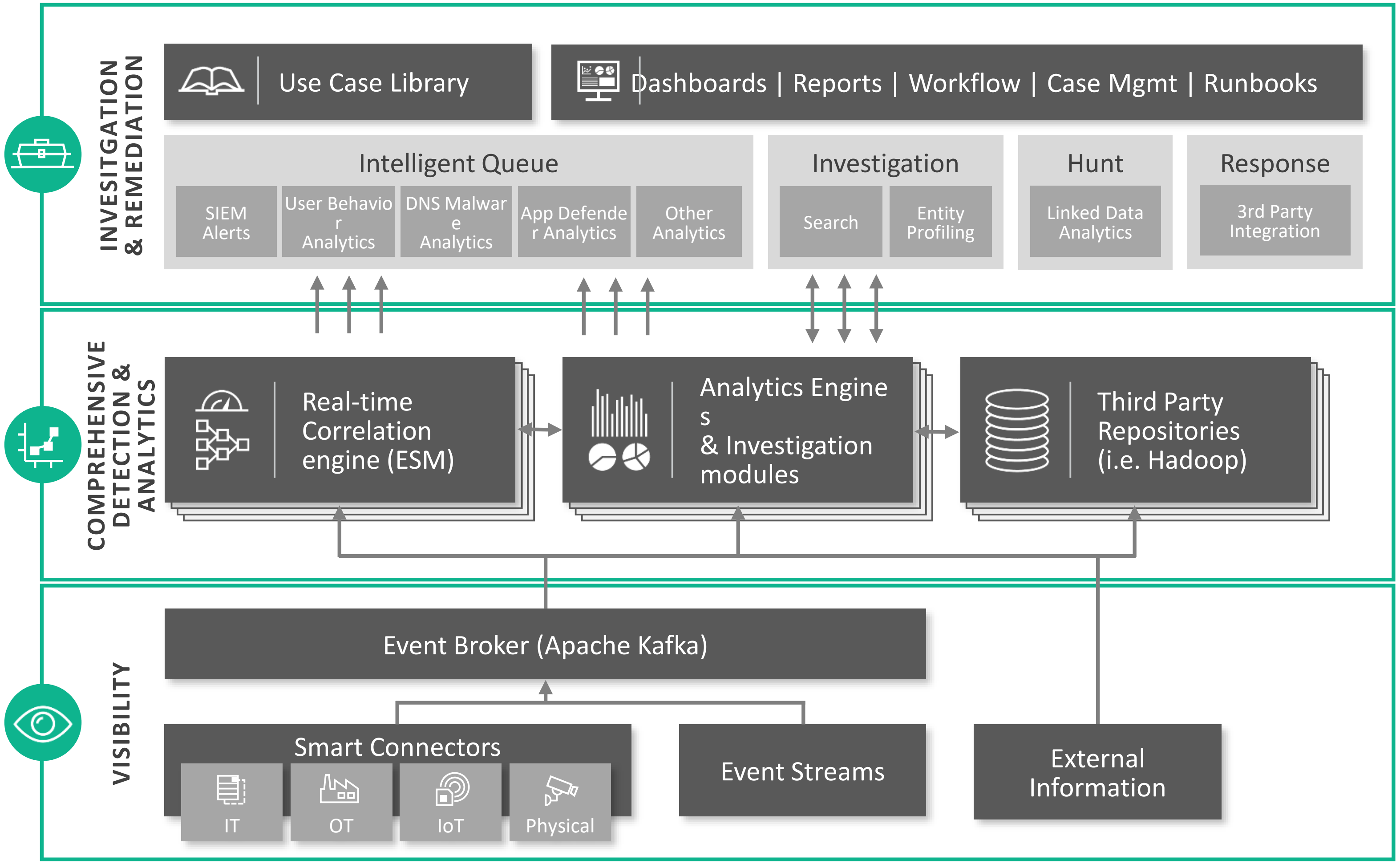
Security Analysts Level 1

Security Analysts Level 2

Hunt Team

Data Sources
(Structured & Unstructured)
+ Control points

- Users
- Cloud
- Apps
- Servers & Workload
- s
- Network
- Endpoints
- IoT



INVESITGATION & REMEDIATION

Use Case Library

Dashboards | Reports | Workflow | Case Mgmt | Runbooks

Intelligent Queue

SIEM Alerts

User Behavio r Analytics

DNS Malwar e Analytics

App Defende r Analytics

Other Analytics

Investigation

Search

Entity Profiling

Hunt

Linked Data Analytics

Response

3rd Party Integration

COMPREHENSIVE DETECTION & ANALYTICS

Real-time Correlation engine (ESM)

Analytics Engine s & Investigation modules

Third Party Repositories (i.e. Hadoop)

VISIBILITY

Event Broker (Apache Kafka)

Smart Connectors

IT

OT

IoT

Physical

Event Streams

External Information

Ticketing & Workflow

IT Operations & Management S ystems

Identity & Configuration

Active Directory

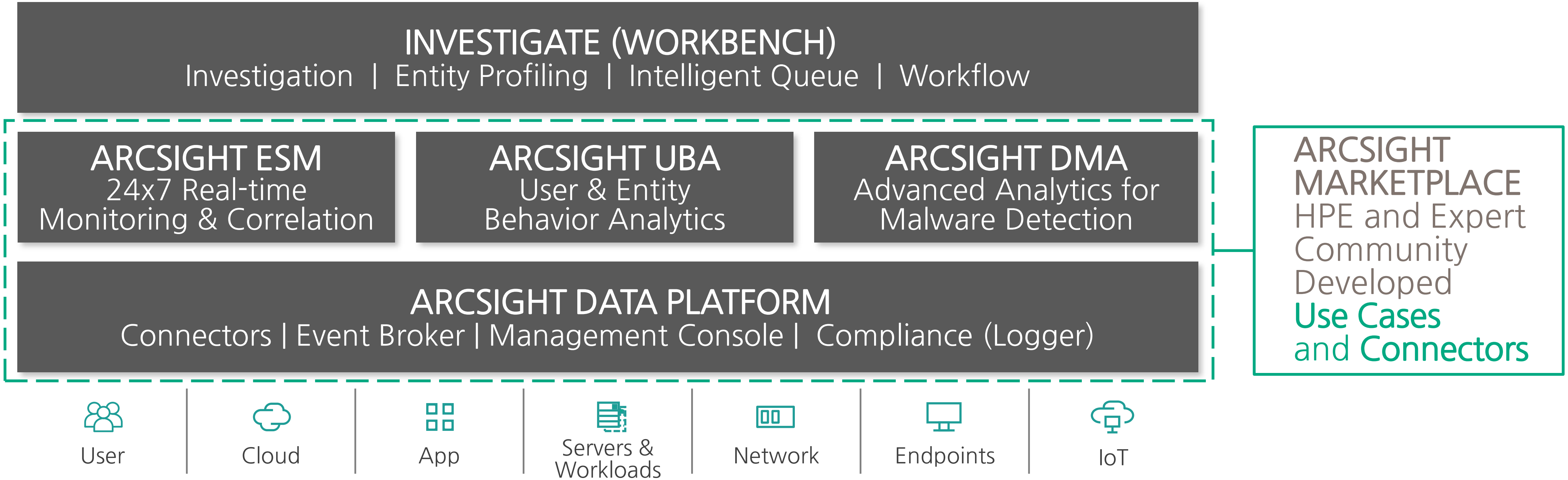
Config Mgmt DB

Intelligence Feeds

Threat Central

3rd Party Feeds

ArcSight product portfolio overview



INVESTIGATE (WORKBENCH)
Investigation | Entity Profiling | Intelligent Queue | Workflow

ARCSIGHT ESM
24x7 Real-time Monitoring & Correlation

ARCSIGHT UBA
User & Entity Behavior Analytics

ARCSIGHT DMA
Advanced Analytics for Malware Detection

ARCSIGHT DATA PLATFORM
Connectors | Event Broker | Management Console | Compliance (Logger)

ARCSIGHT MARKETPLACE
HPE and Expert Community Developed Use Cases and Connectors

User | Cloud | App | Servers & Workloads | Network | Endpoints | IoT

Hewlett Packard Enterprise

ArcSight Data Platform (ADP)

Open and scalable security data solution that can take data from any source and send it to any location, including third-party applications like Hadoop.

Capabilities/Benefits

– **Event Broker** - Extend visibility to third party applications with Kafka-based open architecture data hub

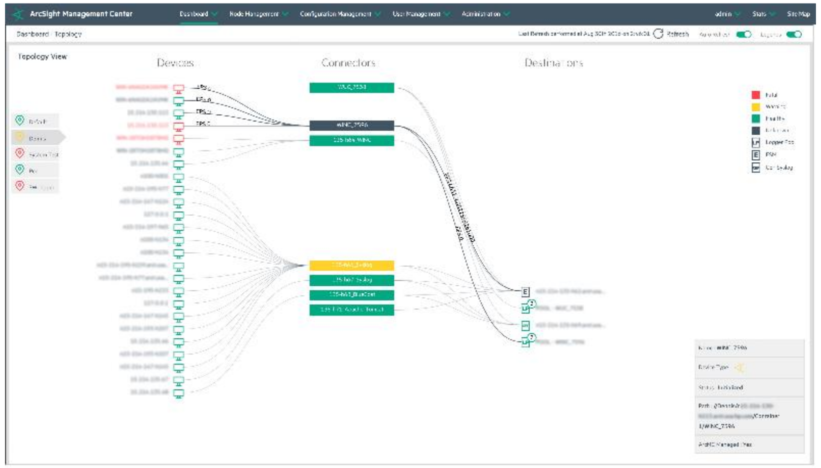
– **1M EPS ingestion rate** - Scale seamlessly to expand security posture

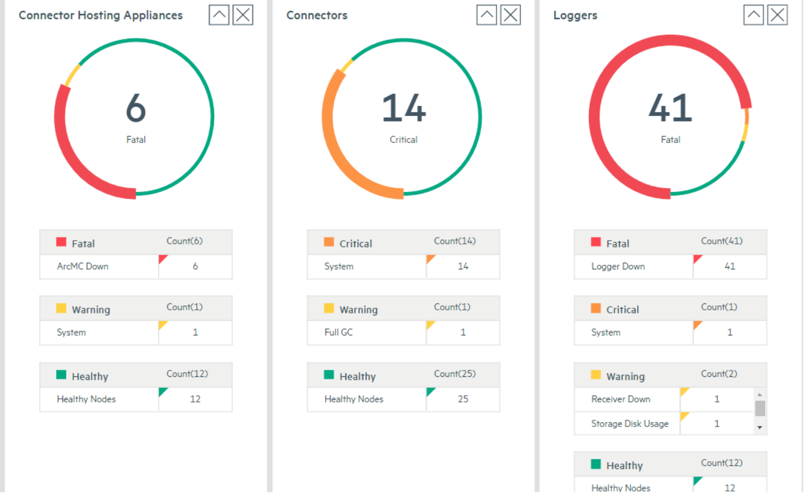
– **Centralized management console** - Simplify management with end-to-end environment monitoring and bulk operations with ArcMC

– **1:10 data compression ratio** - Reduce cost of data storage with compressed logs up to 1200 TB

– **Data enrichment** -Improve threat detection and analysis by security applications through data augmented with security context

– **350+ pre-built connectors** - Extend data collection sources without manual customization





Connector Hosting Appliances

6
Fatal

🟥 Fatal	Count(6)
ArcMC Down	6

🟨 Warning	Count(1)
System	1

🟩 Healthy	Count(12)
Healthy Nodes	12

Connectors

14
Critical

🟧 Critical	Count(14)
System	14

🟨 Warning	Count(1)
Full GC	1

🟩 Healthy	Count(25)
Healthy Nodes	25

Loggers

41
Fatal

🟥 Fatal	Count(41)
Logger Down	41

🟧 Critical	Count(1)
System	1

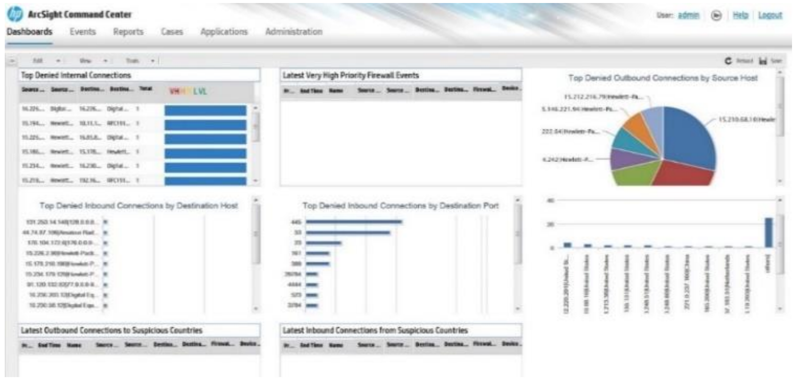
🟨 Warning	Count(2)
Receiver Down	1
Storage Disk Usage	1

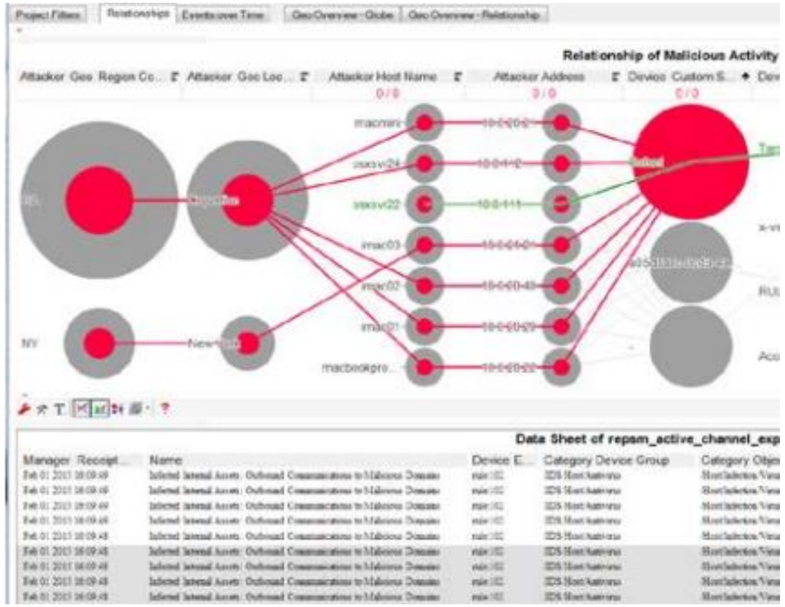
🟩 Healthy	Count(12)
Healthy Nodes	12

Hewlett Packard
Enterprise

ArcSight ESM (SIEM)

Comprehensive, scalable security management application that combines event correlation and security analytics to detect and prioritize threats in real-time to respond and remediate quickly.


ArcSight Command Center
User: admin
Help
Logout
Dashboards
Events
Reports
Cases
Applications
Administration
Top Denied Internal Connections
Latest Very High Priority Firewall Events
Top Denied Outbound Connections by Source Host
Top Denied Inbound Connections by Destination Host
Top Denied Inbound Connections by Destination Port
Latest Outbound Connections to Suspicious Countries
Latest Inbound Connections from Suspicious Countries

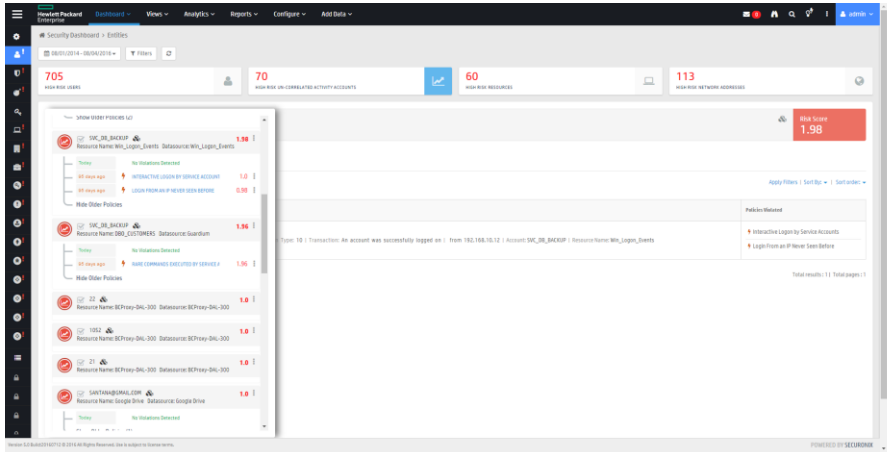


Capabilities/Benefits

- **Real-time correlation** - Improve incident response time from days to minutes with the most intelligent correlation engine in the industry. It filters out irrelevant noise while zeroing in on threats that matter most
- **Ultra-fast forensics -** Rapidly search terabytes of data using a simple search interface. Enables needle-in-the-haystack queries of both active and historical data with a simple search interface
- **Feature rich web active channel with integration command -** Enables faster threat investigation or the security analyst
- **New Express Appliance (search and web UI)** - Faster G9 appliances and feature parity with ESM for Express customers
- **Large hierarchical deployment best practices** - Supports multiple deployment scenarios with hierarchy models for Scalability, MSSP, and HQ/branch offices

ArcSight User and Entity Behavior Analytics (UBA)

Advanced analytics that minimize the risk and impact of cyberattacks by detecting anomalous user and entity behavior in real time.



Capabilities/Benefits

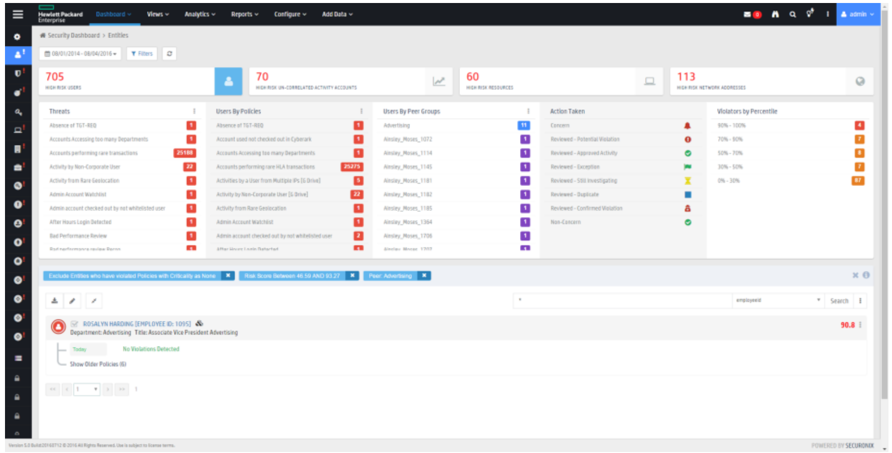
Real-time alerting - Quickly discover unknown threats and gain insight into the highest risk users and entities, even when credentials are legitimate

Entity and threat risks scoring - Prioritize the most suspicious and abnormal activities across users and entities

Threat Library with 500+ built in use cases - Respond to common threats and attacks more intelligently - without manual customization

Integrated with ADP and ESM - Leverage existing security investments

Streamlined investigations - More efficient hunting of advanced persistent threats and faster remediation



Hewlett Packard Enterprise

ArcSight DNS Malware Analytics (DMA)

An automated security analytics solution that detects malware-infected hosts and endpoints rapidly and with high fidelity, enabling remediation in real time.

Capabilities/Benefits

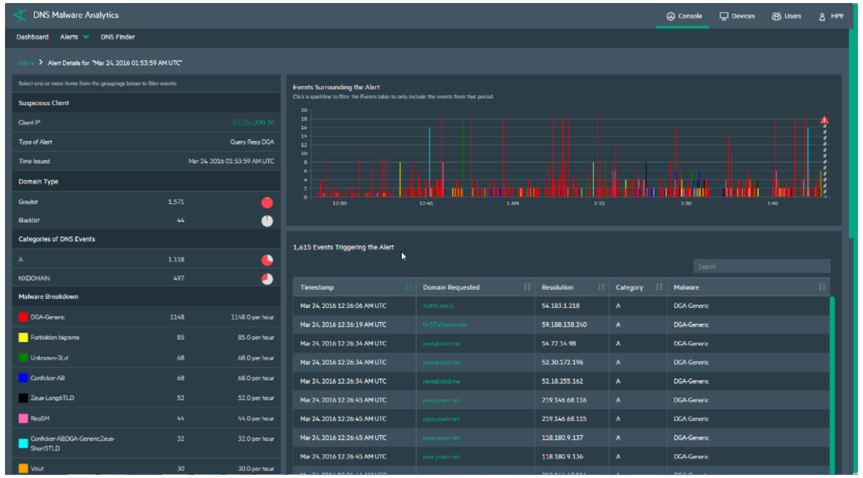
20 minutes to start detecting malware, easy installation - Achieve faster event resolution and contain threats quickly

Near zero false positives - Achieve investigation efficiency by reducing DNS signal noise and time to investigate and locate infections

Small footprint Data Capture Appliance - Capture and pre-filter DNS data, eliminating the need for costly hardware

Enhanced UI and reporting capabilities - A simple workflow for basic resolution as well as deep analytics and forensics

Encrypted communication - Protect data and management paths from unwanted intruders, snooping, hijacking, and man-in-the-middle attacks



Alert Details for "Mar 24, 2016 01:53:59 AM UTC"

Select one or more items from the groupings below to filter events.

Suspicious Client	
Client IP	[redacted]200.30
Type of Alert	Query Resp DGA
Time Issued	Mar 24, 2016 01:53:59 AM UTC

Domain Type	
Graylist	1,571
Blacklist	44

Categories of DNS Events	
A	1,118
NXDOMAIN	497

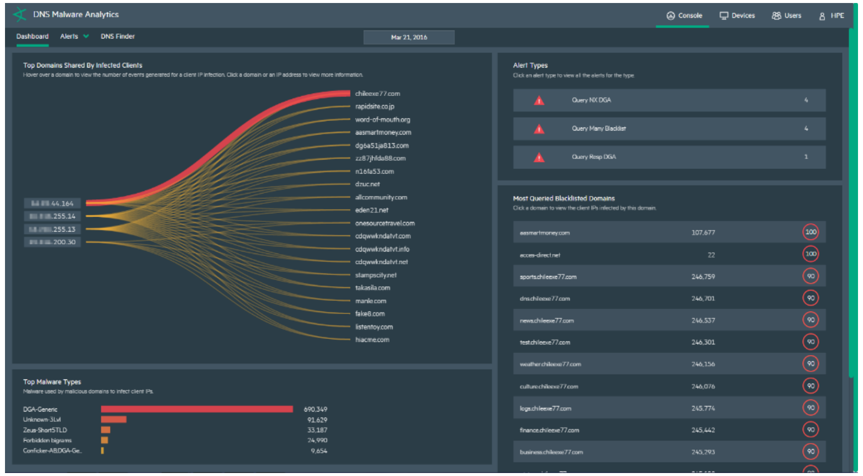
Malware Breakdown		
🟥 DGA-Generic	1148	1148.0 per hour
🟨 Forbidden bigrams	85	85.0 per hour
🟩 Unknown-3Lvl	68	68.0 per hour
🟦 Conficker-AB	68	68.0 per hour
⬛ Zeus-Long6TLD	52	52.0 per hour
RepSM	44	44.0 per hour
Conficker-AB,DGA-Generic,Zeus-Short5TLD	32	32.0 per hour
🟧 Virut	30	30.0 per hour

Events Surrounding the Alert

Click a sparkline to filter the Events table to only include the events from that period.

1,615 Events Triggering the Alert

Timestamp	Domain Requested	Resolution	Category	Malware
Mar 24, 2016 12:26:06 AM UTC	traffic.em.io	54.183.1.218	A	DGA-Generic
Mar 24, 2016 12:26:19 AM UTC	hk3740.xoxv.net	59.188.138.240	A	DGA-Generic
Mar 24, 2016 12:26:34 AM UTC	reveal.dsid.me	54.77.14.98	A	DGA-Generic
Mar 24, 2016 12:26:34 AM UTC	reveal.dsid.me	52.30.172.196	A	DGA-Generic
Mar 24, 2016 12:26:34 AM UTC	reveal.dsid.me	52.18.255.162	A	DGA-Generic
Mar 24, 2016 12:26:45 AM UTC	user.yswm.net	219.146.68.116	A	DGA-Generic
Mar 24, 2016 12:26:45 AM UTC	user.yswm.net	219.146.68.115	A	DGA-Generic
Mar 24, 2016 12:26:45 AM UTC	user.yswm.net	118.180.9.137	A	DGA-Generic
Mar 24, 2016 12:26:45 AM UTC	user.yswm.net	118.180.9.136	A	DGA-Generic



Top Domains Shared By Infected Clients

Hover over a domain to view the number of events generated for a client IP infection. Click a domain or an IP address to view more information.

Top Malware Types

Malware used by malicious domains to infect client IPs.

DGA-Generic	690,349
Unknown-3Lvl	91,629
Zeus-Short5TLD	33,187
Forbidden bigrams	24,990
Conficker-AB,DGA-Ge...	9,654

Alert Types

Click an alert type to view all the alerts for the type.

Query NX DGA	4
Query Many Blacklist	4
Query Resp DGA	1

Most Queried Blacklisted Domains

Click a domain to view the client IPs infected by this domain.

aasmartmoney.com	107,677	100
acces-direct.net	22	100
sports.chileexe77.com	246,759	90
dns.chileexe77.com	246,701	90
news.chileexe77.com	246,537	90
test.chileexe77.com	246,301	90
weather.chileexe77.com	246,156	90
culture.chileexe77.com	246,076	90
logs.chileexe77.com	245,774	90
finance.chileexe77.com	245,442	90
business.chileexe77.com	245,293	90

ArcSight Investigate (출시예정)

Threat investigation solution that provides refined alerts, guided investigation and intuitive search to increase speed and efficiency for intelligent security operations.

Capabilities/Benefits

Industry-leading search speed - Search up to 10 times faster than any other security tool available today

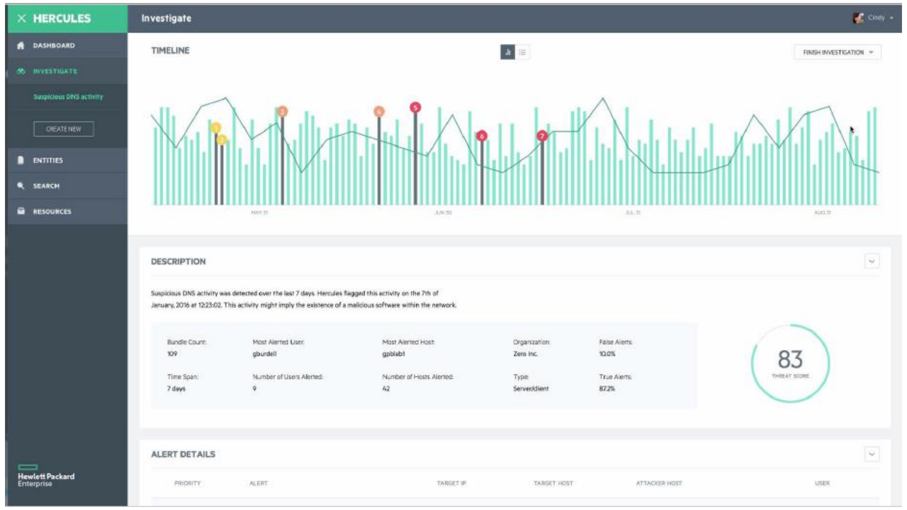
Natural language-like search - Ramp analysts quickly, without requiring any knowledge to build complicated query scripts

Predictive search builder- Expedite investigation with automatically generated search queries

Prioritized bundle of alerts - Increase efficiency with aggregated and prioritized alerts based on algorithm

Entity profiling - Investigate alerts more quickly and precisely by enriching context and getting anomalies versus baseline

Guided investigation - Shorten time to identify threat factors through analytics derived statistics, visualizations and global threat intelligence



DESCRIPTION

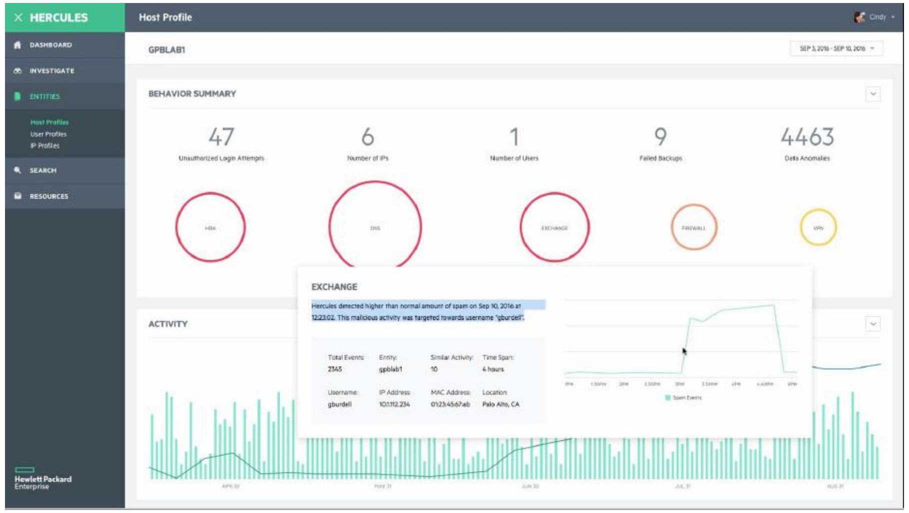
Suspicious DNS activity was detected over the last 7 days. Hercules flagged this activity on the 7th of January, 2016 at 12:23:02. This activity might imply the existence of a malicious software within the network.

Bundle Count: 109
Most Alerted User: gburdell
Most Alerted Host: gpblab1
Organization: Zero Inc.
False Alerts: 10.0%
Time Span: 7 days
Number of Users Alerted: 9
Number of Hosts Alerted: 42
Type: Server/client
True Alerts: 87.2%

83 THREAT SCORE

ALERT DETAILS

PRIORITY	ALERT	TARGET IP	TARGET HOST	ATTACKER HOST	USER



GPBLAB1

SEP 3, 2016 - SEP 10, 2016

BEHAVIOR SUMMARY

47	6	1	9	4463
Unauthorized Login Attempts	Number of IPs	Number of Users	Failed Backups	Data Anomalies

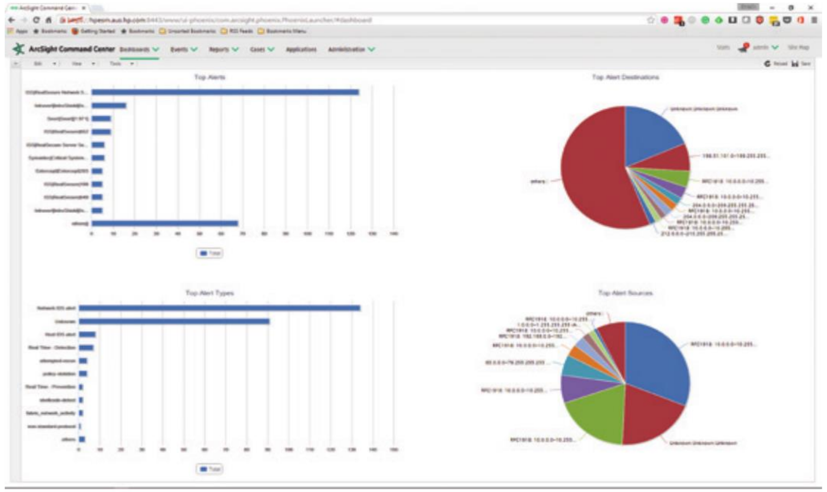
EXCHANGE

Hercules detected higher than normal amount of spam on Sep 10, 2016 at 12:23:02. This malicious activity was targeted towards username "gburdell".

Total Events: 2345
Entity: gpblab1
Similar Activity: 10
Time Span: 4 hours
Username: gburdell
IP Address: 10.1.112.234
MAC Address: 01:23:45:67:ab
Location: Palo Alto, CA

Hewlett Packard Enterprise

ArcSight SIEM과 ArcSight ADP가 2017년(2017년 2월 14일) RSA 컨퍼런스에서 SC Magazine Award 최고의 SIEM Solution으로 선정되었습니다. SC Award는 사이버 보안산업 전반에 걸쳐 인정받고 있으며, 70개 이상의 사이버 보안 업계의 유명 인사들이 심사합니다.



ArcSight ESM and ArcSight ADP

SC 2017 awards

Winner

Finalists 2017

- LogRhythm for Security Intelligence and Analytics Platform
- Rapid7 for InsightIDR- The SIEM You Always Wanted
- RSA for NetWitness Suite
- Splunk for Enterprise Security 4.5 (ES) with Adaptive Response

Trust Award

BEST SIEM SOLUTION

WINNER

Hewlett Packard Enterprise for ArcSight Enterprise Security Manager(SIEM) and ArcSight Data Platform(ADP)

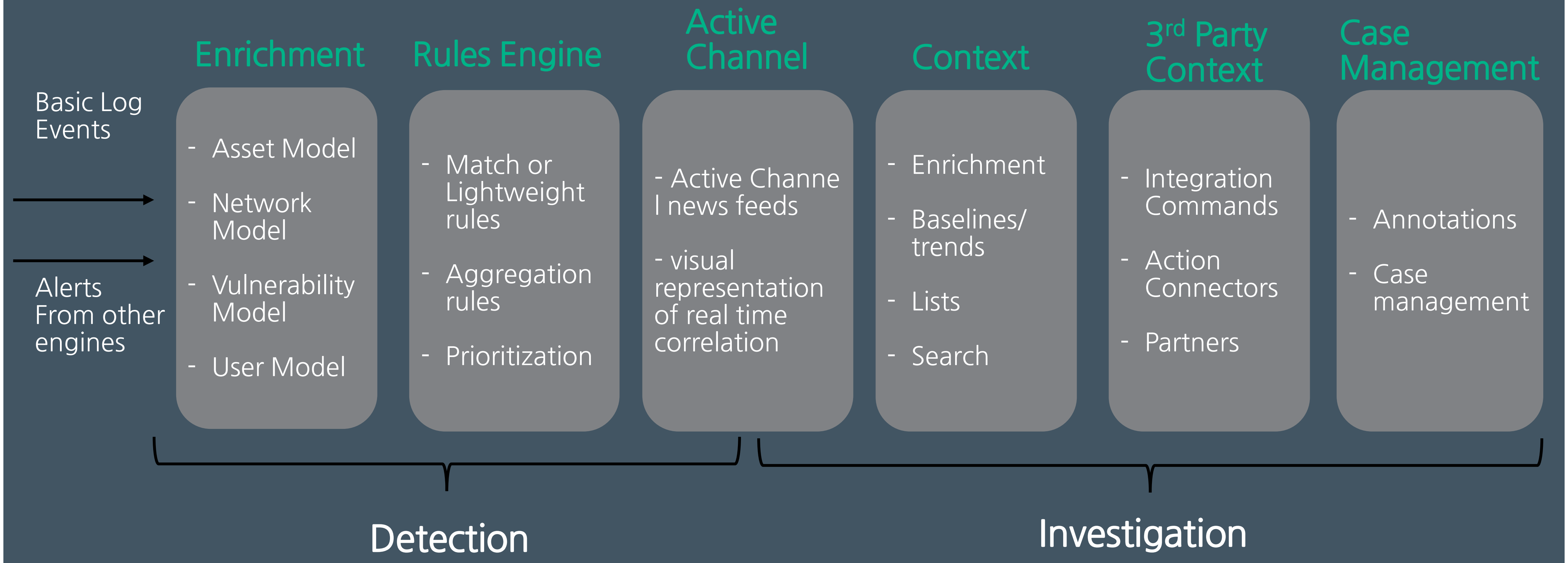
ArcSight has protected enterprises for over a decade, evolving over years as a SIEM market leader (Gartner MQ 2016 for SIEM).

As organizations scale, they rely on intelligent security operations to maintain the integrity of their security posture. ArcSight addresses sophisticated attacks, needs for quick resolution under shortage of security personnel, and data volume, variety and velocity needs due to expanding attack surface.

ArcSight Data Platform(ADP)'s open architecture supports the use of data by third-party applications such as Hadoop, data lakes and proprietary in-house applications. It collects data from any source and enriches it with security context, consolidates the information for maximum storage and retrieval efficiency. ArcSight Enterprise Security Manager (SIEM) is a powerful enterprise security management software for analyzing and correlating every event that occurs, enabling customers to get a quick and accurate picture of users, apps and data to predict, protect and respond to attacks in real-time.

Deployment cost is lower given ArcSight's reduced hardware footprint from efficient compression and high ingestion rates. ArcSight Event Broker acts as a data hub, collecting information at one million events/second. ArcSight Logger can support large SOC operations by allowing 100 concurrent searches. ArcSight is the only open architecture SIEM solution in the market and is better equipped for SOC use cases where multiple products from different vendors are used. By embedding Kafka-based Event Broker, ArcSight collects and sends data anywhere, empowering customers to leverage existing solutions/in-house applications.

ArcSight SIEM functionality in 2 mins



Basic Log Events

Alerts From other engines

Enrichment

- Asset Model
- Network Model
- Vulnerability Model
- User Model

Rules Engine

- Match or Lightweight rules
- Aggregation rules
- Prioritization

Active Channel

- Active Channe l news feeds
- visual representation of real time correlation

Context

- Enrichment
- Baselines/ trends
- Lists
- Search

3rd Party Context

- Integration Commands
- Action Connectors
- Partners

Case Management

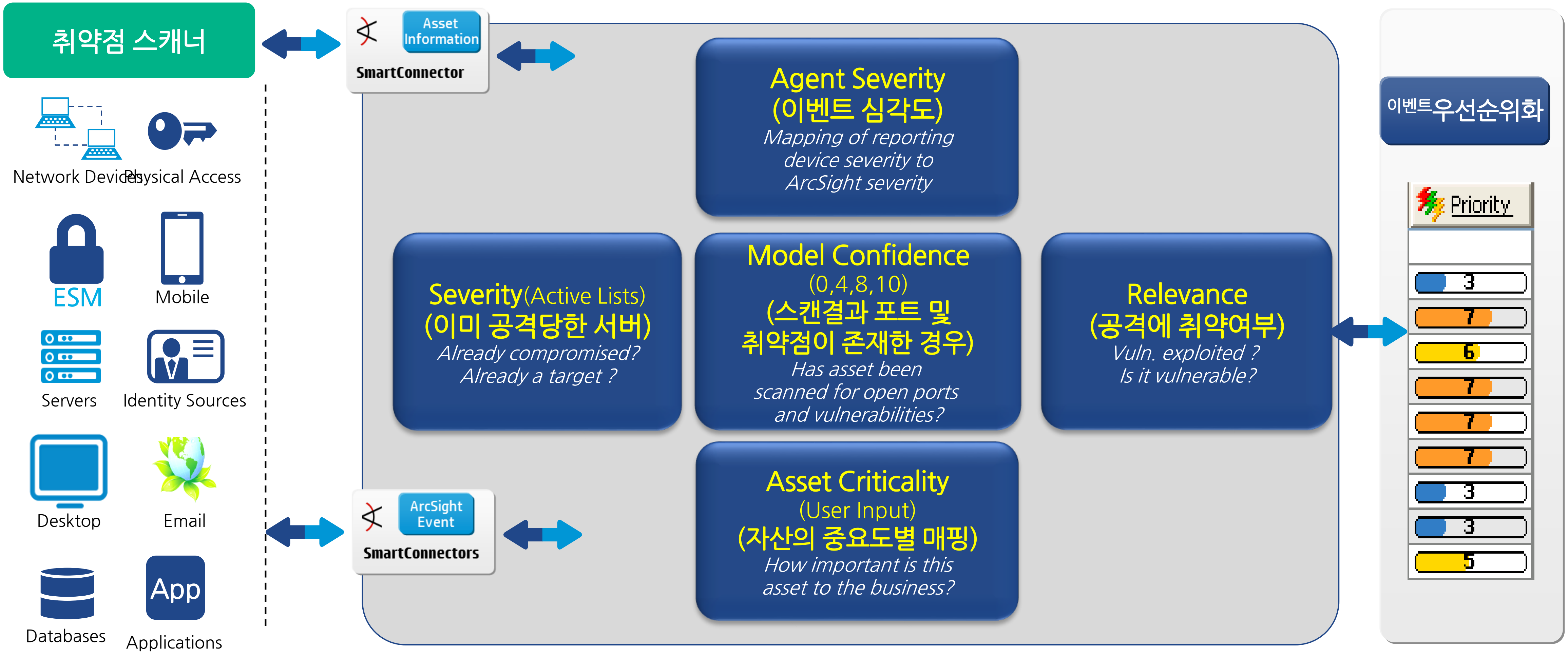
- Annotations
- Case management

Detection

Investigation

이벤트 필드의 풍부성과 우선 순위화

– 호스트 식별 및 취약점 스캐너 연동을 통하여 보안 이벤트 우선순위화



취약점 스캐너

Network Devices Physical Access

ESM Mobile

Servers Identity Sources

Desktop Email

Databases Applications

Asset Information

SmartConnector

ArcSight Event

SmartConnectors

Agent Severity (이벤트 심각도)
Mapping of reporting device severity to ArcSight severity

Severity(Active Lists)
(이미 공격당한 서버)
Already compromised?
Already a target ?

Model Confidence
(0,4,8,10)
(스캔결과 포트 및 취약점이 존재한 경우)
Has asset been scanned for open ports and vulnerabilities?

Relevance
(공격에 취약여부)
Vuln. exploited ?
Is it vulnerable?

Asset Criticality
(User Input)
(자산의 중요도별 매핑)
How important is this asset to the business?

이벤트우선순위화

Priority
3
7
6
7
7
7
3
3
5

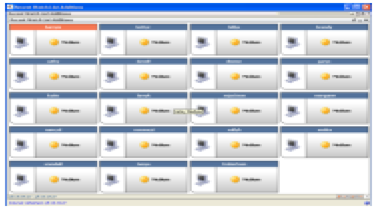
Hewlett Packard
Enterprise

유연한 상관분석 룰 구현

– 인메모리 기반 Active List 활용, 오탐 최소화하여 상관관계분석 및 단계별 공격 대응 가능

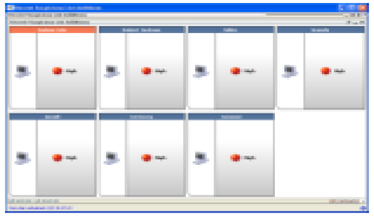
- 보이지 않는 위협분석

: ArcSight 분석 Rule에서 탐지한 위협마다 (공격자 IP) 별도 위협 지수 적용, 지속적인 정책 위반 또는 위협도가 높은 공격자를 탐지



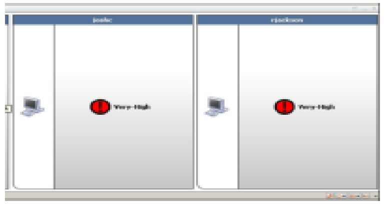
Watch List: (1000s)

- Correlation Rule에 의해 탐지된 이벤트
- Policy Violators



Monitored List: (100s)

- 지속적인 Suspicious Activity



Investigate List: (10)

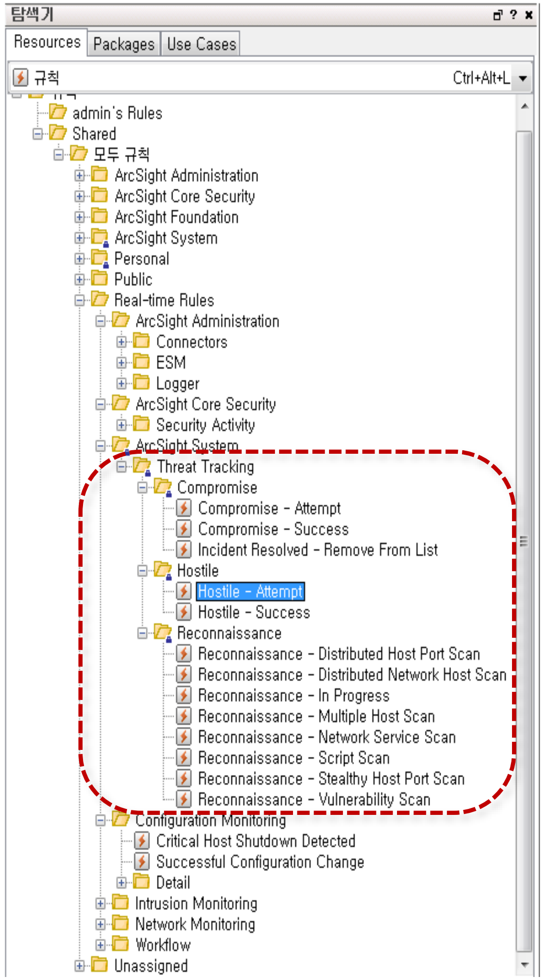
- 명백한 위협
(예: SQL Injection 중 Select * From 등)
- High Threat Score
- 다중의 위협 (공격)

확실한 위협(해킹공격)과 의심스러운 공격 파악

Hewlett Packard
Enterprise

유연한 상관분석 룰 구현

– 다단계 상관 관계 분석 (Active List 및 다단계 상관 분석 기법 활용)

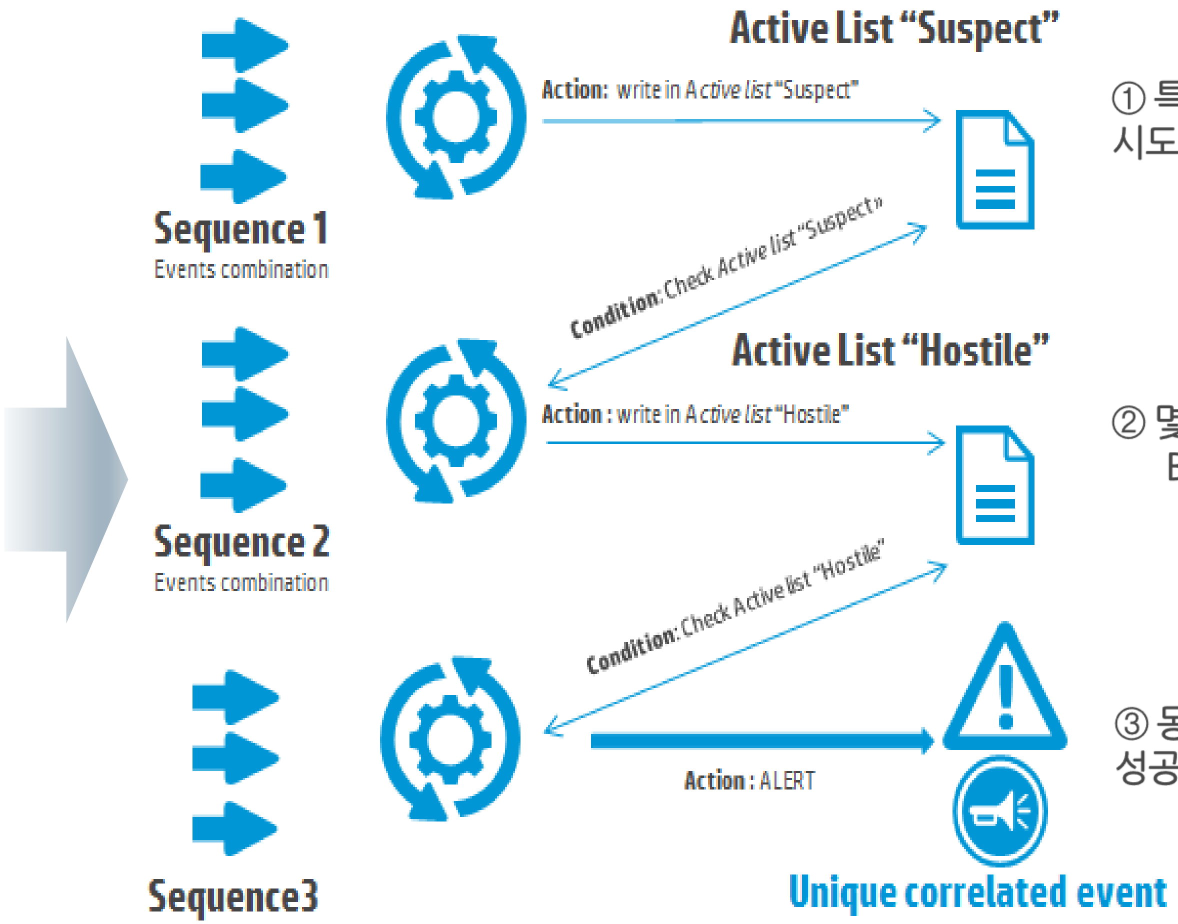


탐색기

Resources | Packages | Use Cases

규칙 Ctrl+Alt+L

- admin's Rules
- Shared
  - 모두 규칙
    - ArcSight Administration
    - ArcSight Core Security
    - ArcSight Foundation
    - ArcSight System
    - Personal
    - Public
    - Real-time Rules
      - ArcSight Administration
        - Connectors
        - ESM
        - Logger
      - ArcSight Core Security
        - Security Activity
      - ArcSight System
        - Threat Tracking
          - Compromise
            - Compromise - Attempt
            - Compromise - Success
            - Incident Resolved - Remove From List
          - Hostile
            - Hostile - Attempt
            - Hostile - Success
          - Reconnaissance
            - Reconnaissance - Distributed Host Port Scan
            - Reconnaissance - Distributed Network Host Scan
            - Reconnaissance - In Progress
            - Reconnaissance - Multiple Host Scan
            - Reconnaissance - Network Service Scan
            - Reconnaissance - Script Scan
            - Reconnaissance - Stealthy Host Port Scan
            - Reconnaissance - Vulnerability Scan
        - Configuration Monitoring
          - Critical Host Shutdown Detected
          - Successful Configuration Change
          - Detail
        - Intrusion Monitoring
        - Network Monitoring
        - Workflow
    - Unassigned



Active List "Suspect"
Action: write in Active list "Suspect"
Sequence 1
Events combination
Condition: Check Active list "Suspect"
Active List "Hostile"
Action : write in Active list "Hostile"
Sequence 2
Events combination
Condition: Check Active list "Hostile"
Action : ALERT
Sequence3
Unique correlated event

① 특정 공격자가 네트워크에 스캔을 시도함

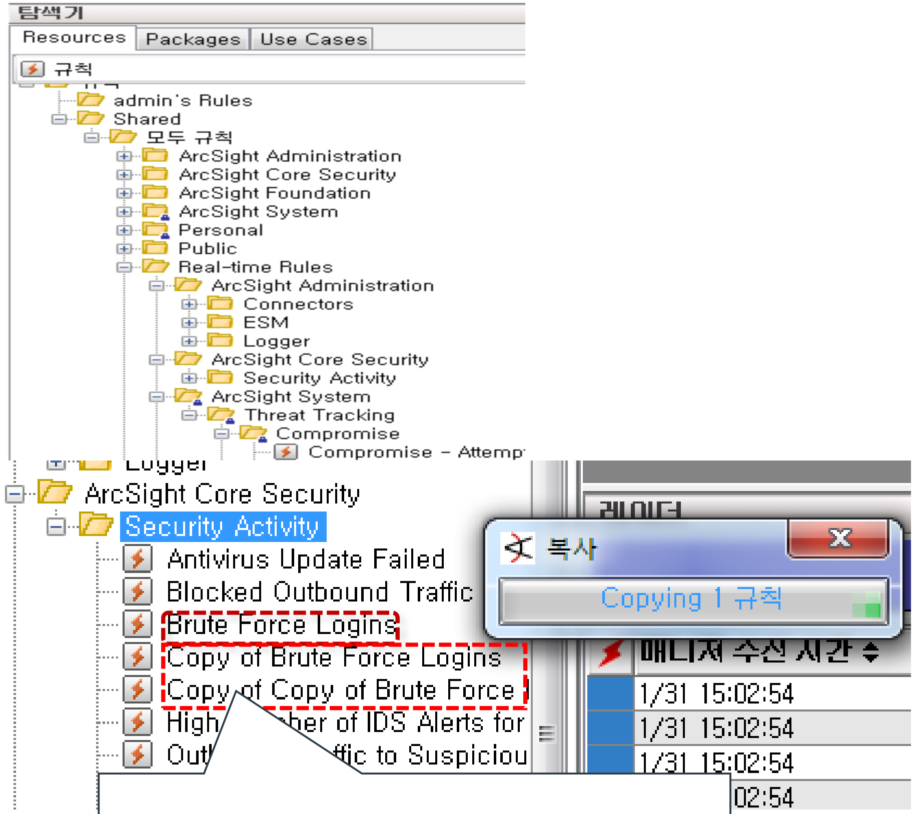
② 몇분 혹은 몇일 후에 동일 공격자가 Brute-Force공격시도

③ 동일 공격자가 결국에는 로그인 성공을 함

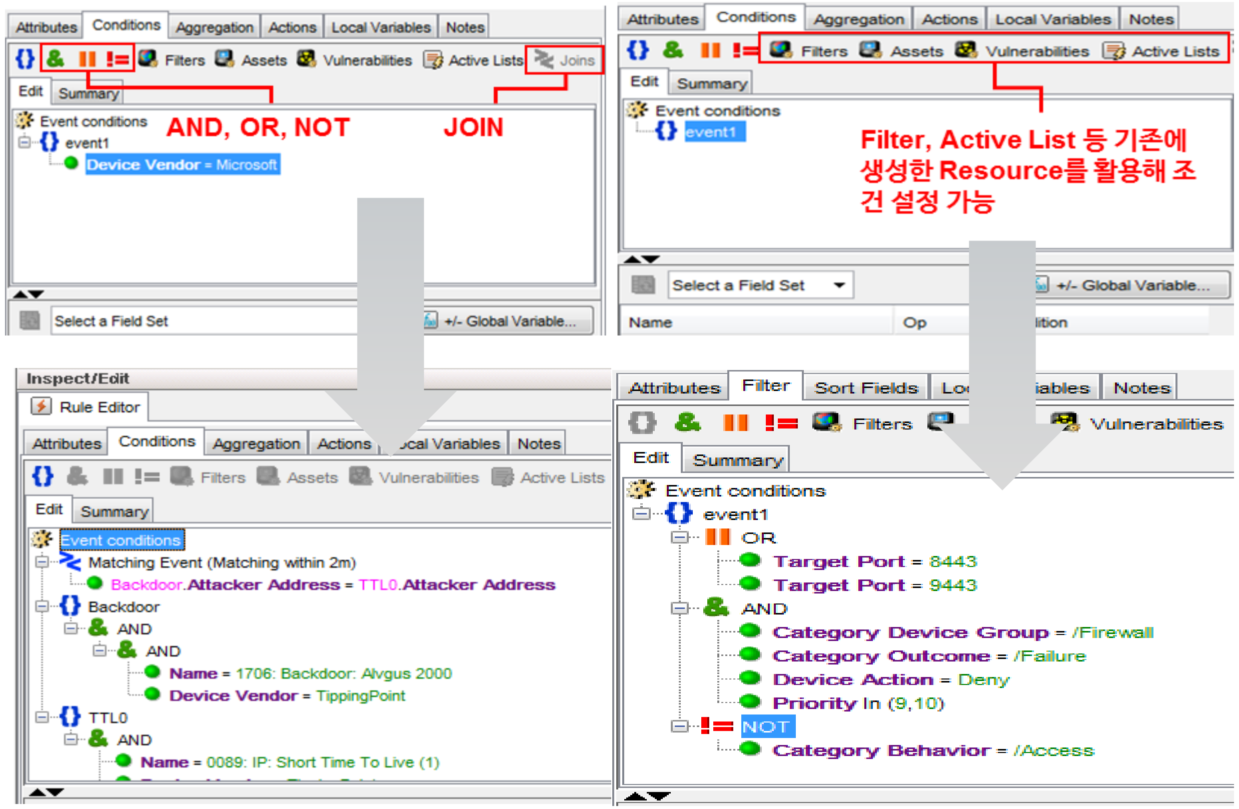
유연한 상관분석 룰 구현(Context기반 상관분석)

–복잡한 다단계 룰 생성 및 관리에 용이한 직관적인 단일 GUI 방식

- GUI화면에서 사용자가 직관적으로 이해할 수 있는 연산자와 이벤트 필드의 조합으로 룰셋을 쉽게 생성하며, 재사용 및 복사와 이동이 자유로운 구조로 사용 편리성 제공



기존 룰 Copy를 통한 재사용 용이



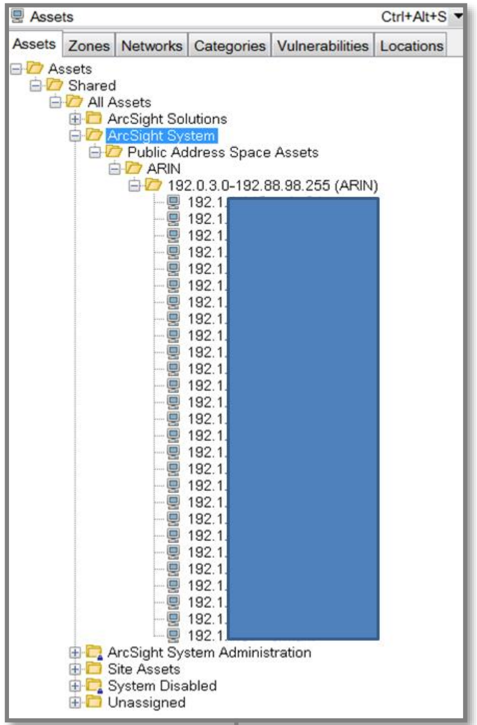
Event conditions
Matching Event (Matching within 2m)
Backdoor.Attacker Address = TTL0.Attacker Address
Backdoor
AND
AND
Name = 1706: Backdoor: Alvgus 2000
Device Vendor = TippingPoint
TTL0
AND
Name = 0089: IP: Short Time To Live (1)

Event conditions
event1
OR
Target Port = 8443
Target Port = 9443
AND
Category Device Group = /Firewall
Category Outcome = /Failure
Device Action = Deny
Priority In (9,10)
NOT
Category Behavior = /Access

Hewlett Packard
Enterprise

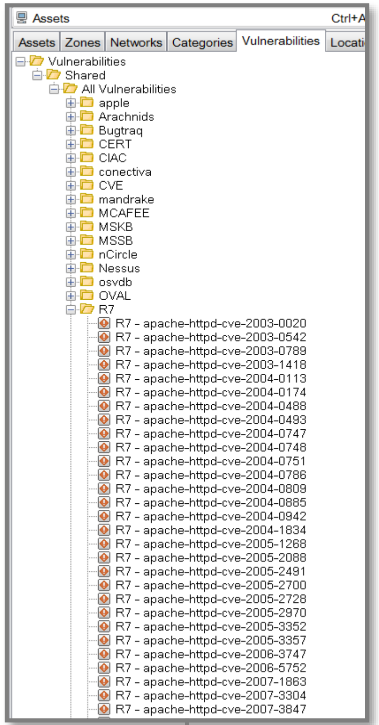
취약점 스캐너 연동 사례(3rd Party Context)

– 취약점 스캐너의 점검 결과를 자동으로 연동

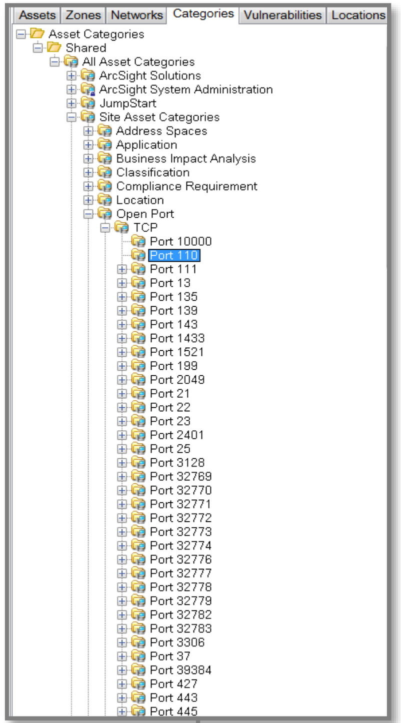


```
Assets                                        Ctrl+Alt+S
Assets | Zones | Networks | Categories | Vulnerabilities | Locations
⊟ Assets
  ⊟ Shared
    ⊟ All Assets
      ⊞ ArcSight Solutions
      ⊟ ArcSight System
        ⊟ Public Address Space Assets
          ⊟ ARIN
            ⊟ 192.0.3.0-192.88.98.255 (ARIN)
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
                192.1
      ⊞ ArcSight System Administration
      ⊞ Site Assets
      ⊞ System Disabled
      ⊞ Unassigned
```

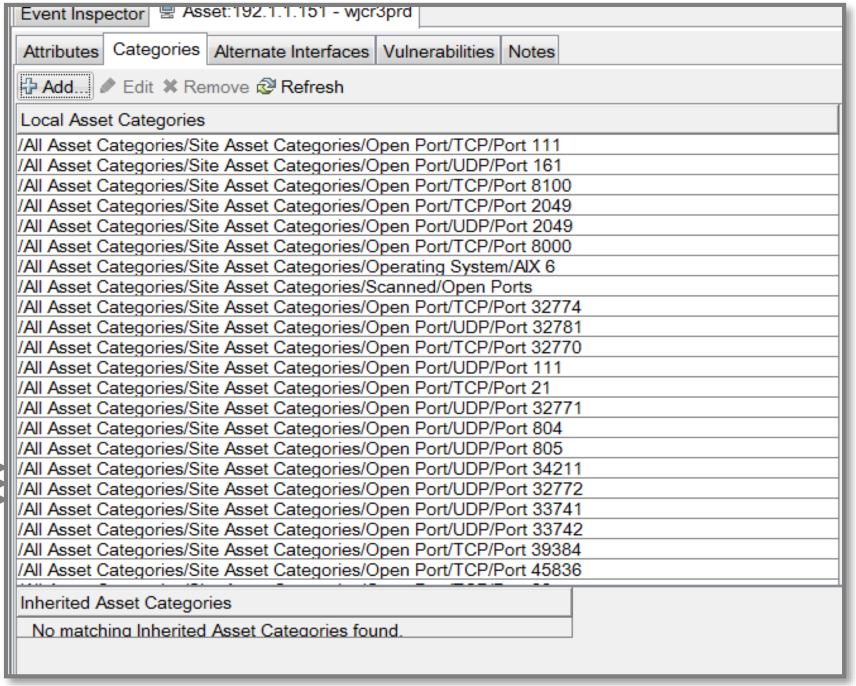
[redacted]



```
Assets                                        Ctrl+A
Assets | Zones | Networks | Categories | Vulnerabilities | Locati
⊟ Vulnerabilities
  ⊟ Shared
    ⊟ All Vulnerabilities
      ⊞ apple
      ⊞ Arachnids
      ⊞ Bugtraq
      ⊞ CERT
      ⊞ CIAC
      ⊞ conectiva
      ⊞ CVE
      ⊞ mandrake
      ⊞ MCAFEE
      ⊞ MSKB
      ⊞ MSSB
      ⊞ nCircle
      ⊞ Nessus
      ⊞ osvdb
      ⊞ OVAL
      ⊟ R7
          R7 - apache-httpd-cve-2003-0020
          R7 - apache-httpd-cve-2003-0542
          R7 - apache-httpd-cve-2003-0789
          R7 - apache-httpd-cve-2003-1418
          R7 - apache-httpd-cve-2004-0113
          R7 - apache-httpd-cve-2004-0174
          R7 - apache-httpd-cve-2004-0488
          R7 - apache-httpd-cve-2004-0493
          R7 - apache-httpd-cve-2004-0747
          R7 - apache-httpd-cve-2004-0748
          R7 - apache-httpd-cve-2004-0751
          R7 - apache-httpd-cve-2004-0786
          R7 - apache-httpd-cve-2004-0809
          R7 - apache-httpd-cve-2004-0885
          R7 - apache-httpd-cve-2004-0942
          R7 - apache-httpd-cve-2004-1834
          R7 - apache-httpd-cve-2005-1268
          R7 - apache-httpd-cve-2005-2088
          R7 - apache-httpd-cve-2005-2491
          R7 - apache-httpd-cve-2005-2700
          R7 - apache-httpd-cve-2005-2728
          R7 - apache-httpd-cve-2005-2970
          R7 - apache-httpd-cve-2005-3352
          R7 - apache-httpd-cve-2005-3357
          R7 - apache-httpd-cve-2006-3747
          R7 - apache-httpd-cve-2006-5752
          R7 - apache-httpd-cve-2007-1863
          R7 - apache-httpd-cve-2007-3304
          R7 - apache-httpd-cve-2007-3847
```



```
Assets | Zones | Networks | Categories | Vulnerabilities | Locations
⊟ Asset Categories
  ⊟ Shared
    ⊟ All Asset Categories
      ⊞ ArcSight Solutions
      ⊞ ArcSight System Administration
      ⊞ JumpStart
      ⊟ Site Asset Categories
        ⊞ Address Spaces
        ⊞ Application
        ⊞ Business Impact Analysis
        ⊞ Classification
        ⊞ Compliance Requirement
        ⊞ Location
        ⊟ Open Port
          ⊟ TCP
              Port 10000
              Port 110
            ⊞ Port 111
            ⊞ Port 13
            ⊞ Port 135
            ⊞ Port 139
            ⊞ Port 143
            ⊞ Port 1433
            ⊞ Port 1521
            ⊞ Port 199
            ⊞ Port 2049
            ⊞ Port 21
            ⊞ Port 22
            ⊞ Port 23
            ⊞ Port 2401
            ⊞ Port 25
            ⊞ Port 3128
            ⊞ Port 32769
            ⊞ Port 32770
            ⊞ Port 32771
            ⊞ Port 32772
            ⊞ Port 32773
            ⊞ Port 32774
            ⊞ Port 32776
            ⊞ Port 32777
            ⊞ Port 32778
            ⊞ Port 32779
            ⊞ Port 32782
            ⊞ Port 32783
            ⊞ Port 3306
            ⊞ Port 37
            ⊞ Port 39384
            ⊞ Port 427
            ⊞ Port 443
            ⊞ Port 445
```



Event Inspector | Asset:192.1.1.151 - wjcr3prd

Attributes | Categories | Alternate Interfaces | Vulnerabilities | Notes

Add... | Edit | Remove | Refresh

Local Asset Categories
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 111
/All Asset Categories/Site Asset Categories/Open Port/UDP/Port 161
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 8100
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 2049
/All Asset Categories/Site Asset Categories/Open Port/UDP/Port 2049
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 8000
/All Asset Categories/Site Asset Categories/Operating System/AIX 6
/All Asset Categories/Site Asset Categories/Scanned/Open Ports
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 32774
/All Asset Categories/Site Asset Categories/Open Port/UDP/Port 32781
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 32770
/All Asset Categories/Site Asset Categories/Open Port/UDP/Port 111
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 21
/All Asset Categories/Site Asset Categories/Open Port/UDP/Port 32771
/All Asset Categories/Site Asset Categories/Open Port/UDP/Port 804
/All Asset Categories/Site Asset Categories/Open Port/UDP/Port 805
/All Asset Categories/Site Asset Categories/Open Port/UDP/Port 34211
/All Asset Categories/Site Asset Categories/Open Port/UDP/Port 32772
/All Asset Categories/Site Asset Categories/Open Port/UDP/Port 33741
/All Asset Categories/Site Asset Categories/Open Port/UDP/Port 33742
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 39384
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 45836

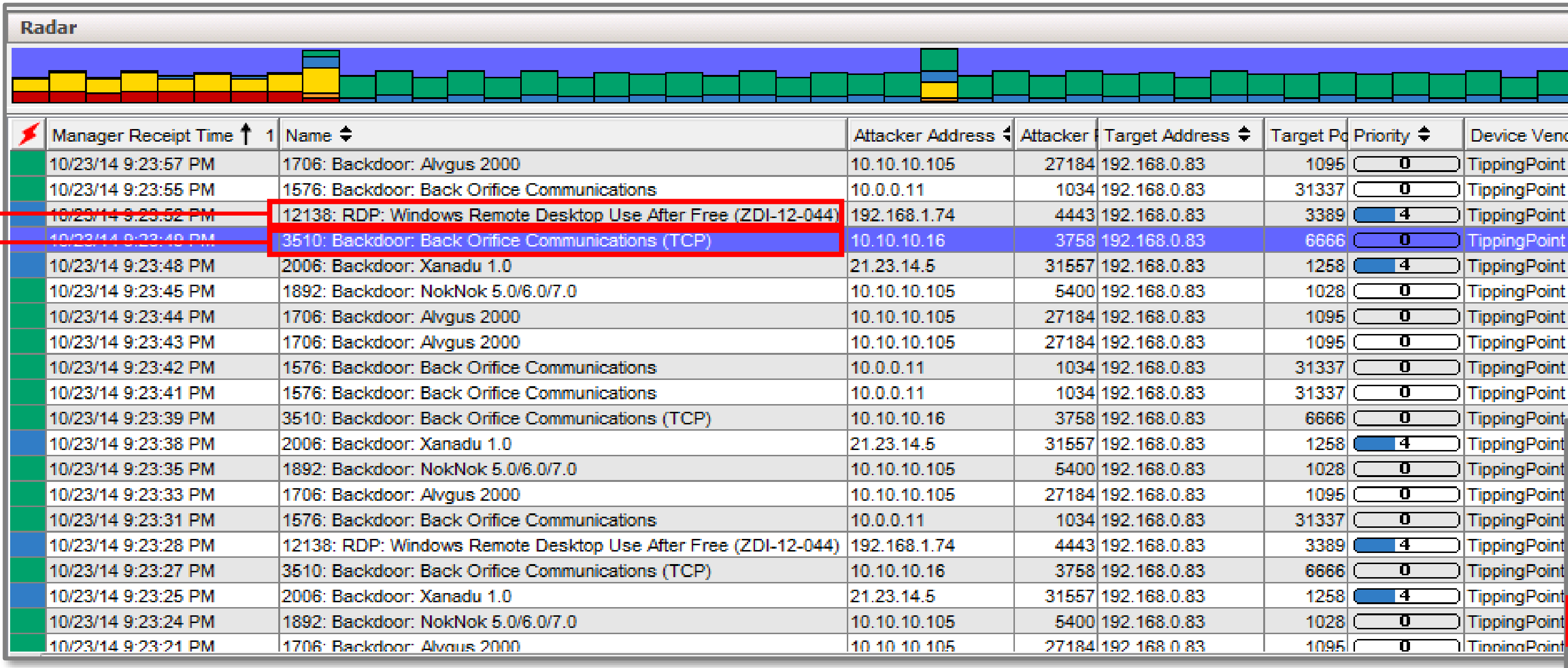
Inherited Asset Categories
No matching Inherited Asset Categories found.

취약점 진단 결과로 받은 Assets, open port
취약점 결과 등이 자동으로 ArcSight에 반영

Hewlett Packard
Enterprise

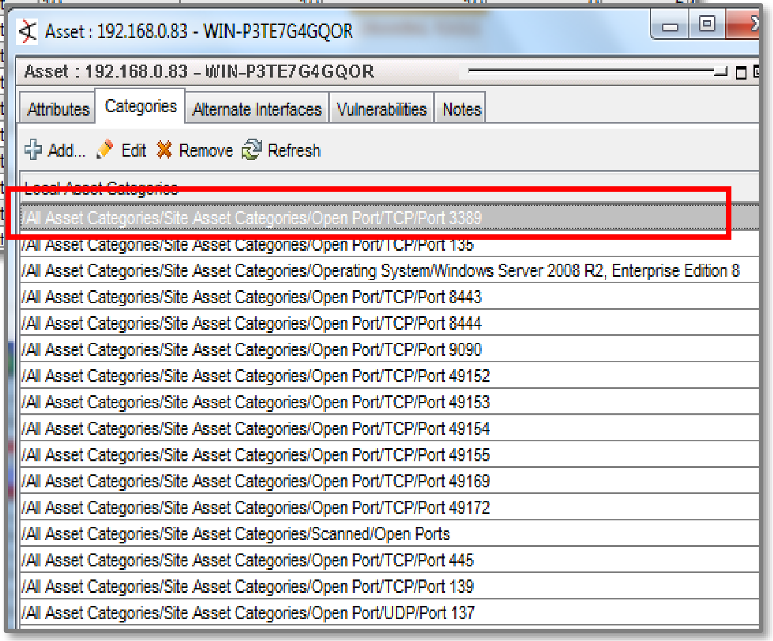
취약점 스캐너 연동 사례(3rd Party Context)

– 취약점 스캐너의 점검 결과를 바탕으로 이벤트에 대한 우선 순위 조정



Radar

⚡	Manager Receipt Time ↑ 1	Name ⬍	Attacker Address ⬍	Attacker	Target Address ⬍	Target Po	Priority ⬍	Device Vendor	Device Severity	Asset Criticality	Model Confidence	Relevance	Severity
🟩	10/23/14 9:23:57 PM	1706: Backdoor: Alvgus 2000	10.10.10.105	27184	192.168.0.83	1095	0	TippingPoint	4	10	10	0	5
🟩	10/23/14 9:23:55 PM	1576: Backdoor: Back Orifice Communications	10.0.0.11	1034	192.168.0.83	31337	0	TippingPoint	10	10	10	0	5
🟦	10/23/14 9:23:52 PM	12138: RDP: Windows Remote Desktop Use After Free (ZDI-12-044)	192.168.1.74	4443	192.168.0.83	3389	4	TippingPoint	1	10	10	10	0
	10/23/14 9:23:49 PM	3510: Backdoor: Back Orifice Communications (TCP)	10.10.10.16	3758	192.168.0.83	6666	0	TippingPoint	10	10	10	0	5
🟦	10/23/14 9:23:48 PM	2006: Backdoor: Xanadu 1.0	21.23.14.5	31557	192.168.0.83	1258	4	TippingPoint	4	10	10	5	5
🟩	10/23/14 9:23:45 PM	1892: Backdoor: NokNok 5.0/6.0/7.0	10.10.10.105	5400	192.168.0.83	1028	0	TippingPoint	4	10	10	0	5
🟩	10/23/14 9:23:44 PM	1706: Backdoor: Alvgus 2000	10.10.10.105	27184	192.168.0.83	1095	0	TippingPoint	4	10	10	0	5
🟩	10/23/14 9:23:43 PM	1706: Backdoor: Alvgus 2000	10.10.10.105	27184	192.168.0.83	1095	0	TippingPoint	4	10	10	0	5
🟩	10/23/14 9:23:42 PM	1576: Backdoor: Back Orifice Communications	10.0.0.11	1034	192.168.0.83	31337	0	TippingPoint	10	10	10	0	5
🟩	10/23/14 9:23:41 PM	1576: Backdoor: Back Orifice Communications	10.0.0.11	1034	192.168.0.83	31337	0	TippingPoint	10	10	10	0	5
🟩	10/23/14 9:23:39 PM	3510: Backdoor: Back Orifice Communications (TCP)	10.10.10.16	3758	192.168.0.83	6666	0	TippingPoint	10	10	10	0	5
🟦	10/23/14 9:23:38 PM	2006: Backdoor: Xanadu 1.0	21.23.14.5	31557	192.168.0.83	1258	4	TippingPoint					
🟩	10/23/14 9:23:35 PM	1892: Backdoor: NokNok 5.0/6.0/7.0	10.10.10.105	5400	192.168.0.83	1028	0	TippingPoint					
🟩	10/23/14 9:23:33 PM	1706: Backdoor: Alvgus 2000	10.10.10.105	27184	192.168.0.83	1095	0	TippingPoint					
🟩	10/23/14 9:23:31 PM	1576: Backdoor: Back Orifice Communications	10.0.0.11	1034	192.168.0.83	31337	0	TippingPoint					
🟦	10/23/14 9:23:28 PM	12138: RDP: Windows Remote Desktop Use After Free (ZDI-12-044)	192.168.1.74	4443	192.168.0.83	3389	4	TippingPoint					
🟩	10/23/14 9:23:27 PM	3510: Backdoor: Back Orifice Communications (TCP)	10.10.10.16	3758	192.168.0.83	6666	0	TippingPoint					
🟦	10/23/14 9:23:25 PM	2006: Backdoor: Xanadu 1.0	21.23.14.5	31557	192.168.0.83	1258	4	TippingPoint					
🟩	10/23/14 9:23:24 PM	1892: Backdoor: NokNok 5.0/6.0/7.0	10.10.10.105	5400	192.168.0.83	1028	0	TippingPoint					
🟩	10/23/14 9:23:21 PM	1706: Backdoor: Alvgus 2000	10.10.10.105	27184	192.168.0.83	1095	0	TippingPoint					



Asset : 192.168.0.83 - WIN-P3TE7G4GQOR

Asset : 192.168.0.83 – WIN-P3TE7G4GQOR

Local Asset Categories

/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 3389
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 135
/All Asset Categories/Site Asset Categories/Operating System/Windows Server 2008 R2, Enterprise Edition 8
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 8443
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 8444
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 9090
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 49152
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 49153
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 49154
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 49155
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 49169
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 49172
/All Asset Categories/Site Asset Categories/Scanned/Open Ports
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 445
/All Asset Categories/Site Asset Categories/Open Port/TCP/Port 139
/All Asset Categories/Site Asset Categories/Open Port/UDP/Port 137

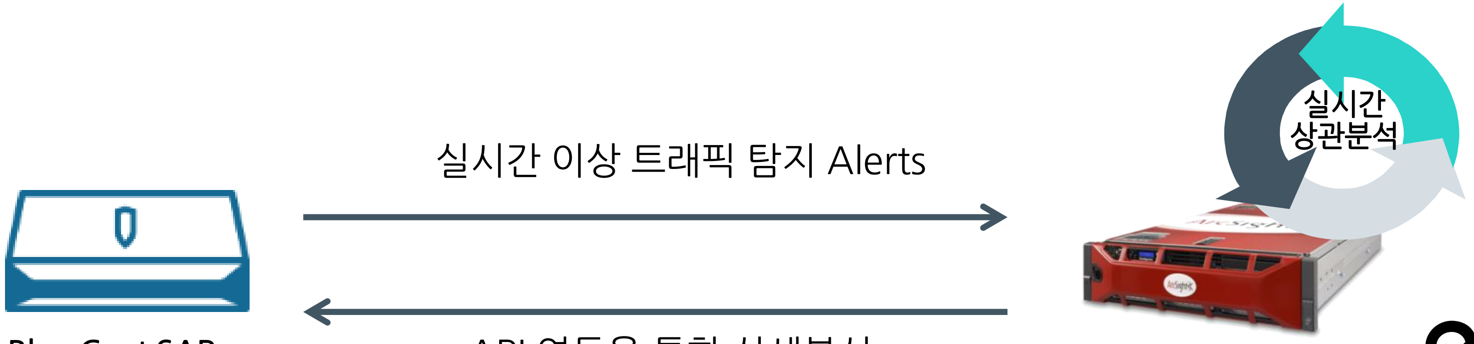
- 12138: RDP: Windows Remote Desktop Use After Free (ZDI-12-044) 는 Relevance가 10임. Scanner스캔 결과 RDP서비스인 TCP 3389번 포트에서 취약점이 발견되었기 때문에 Device Severity는 1이 었지만 전체적인 Priority는 4로 설정됨

- 3510: Backdoor: Back Orifice Communications (TCP)는 Relevance가 0임. Scanner 스캔 결과 열려진 포트가 없는데 공격이 시도 되었기 때문임 공격의 impact가 없다 판단.. 결과적으로 Priority가 0으로 떨어짐

Hewlett Packard
Enterprise

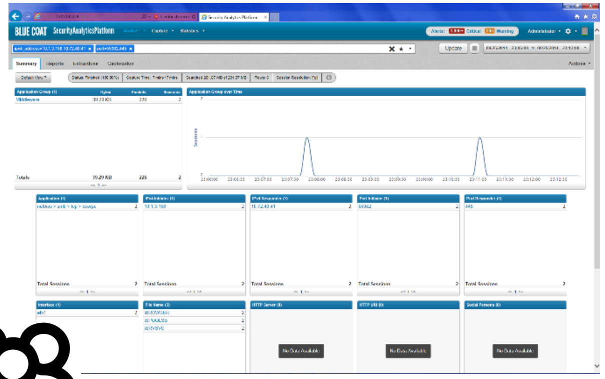
네트워크 포렌식 연동 사례(3rd Party Context)

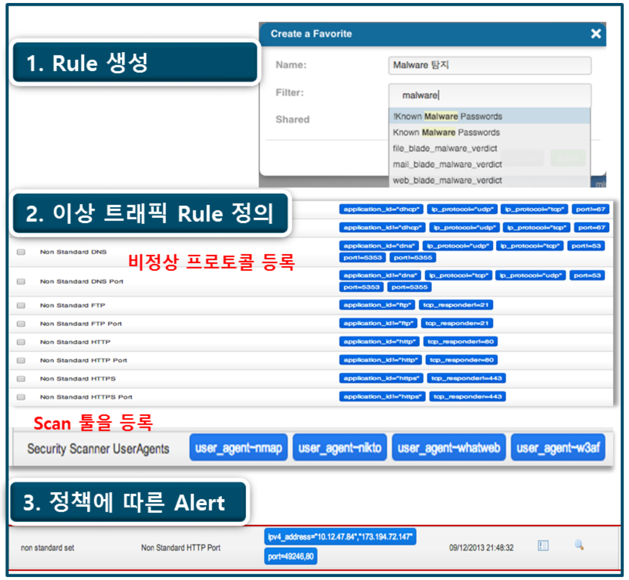
– 기존에 설치된 네트워크 포렌식 솔루션과 연동하여 보다 효과적인 관제 수행



Blue Coat SAP
(네트워크 패킷 및 세션
기반 분석/저장)

ArcSight SIEM





1. Rule 생성

Create a Favorite

Name: Malware 탐지

Filter: malware

Shared

- !Known Malware Passwords
- Known Malware Passwords
- file_blade_malware_verdict
- mail_blade_malware_verdict
- web_blade_malware_verdict

2. 이상 트래픽 Rule 정의

비정상 프로토콜 등록

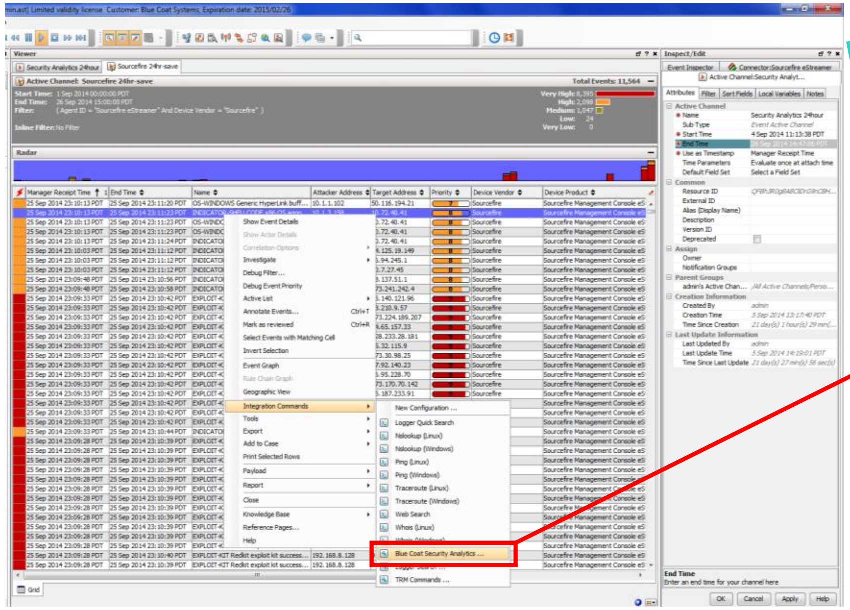
	application_id="dhcp" ip_protocol="udp" ip_protocol="tcp" port!=67
	application_id!="dhcp" ip_protocol="udp" ip_protocol="tcp" port=67
Non Standard DNS	application_id="dns" ip_protocol="udp" ip_protocol="tcp" port!=53 port!=5353 port!=5355
Non Standard DNS Port	application_id!="dns" ip_protocol="tcp" ip_protocol="udp" port=53 port=5353 port=5355
Non Standard FTP	application_id="ftp" tcp_responder!=21
Non Standard FTP Port	application_id!="ftp" tcp_responder=21
Non Standard HTTP	application_id="http" tcp_responder!=80
Non Standard HTTP Port	application_id!="http" tcp_responder=80
Non Standard HTTPS	application_id="https" tcp_responder!=443
Non Standard HTTPS Port	application_id!="https" tcp_responder=443

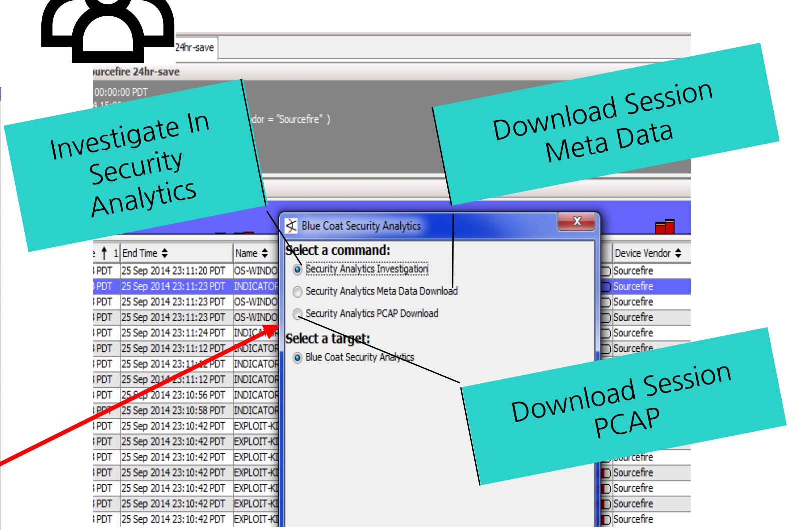
Scan 툴을 등록

Security Scanner UserAgents: user_agent=nmap user_agent=nikto user_agent=whatweb user_agent=w3af

3. 정책에 따른 Alert

non standard set	Non Standard HTTP Port	ipv4_address="10.12.47.84","173.194.72.147"
		port=49246,80
			09/12/2013 21:48:32





Blue Coat Security Analytics

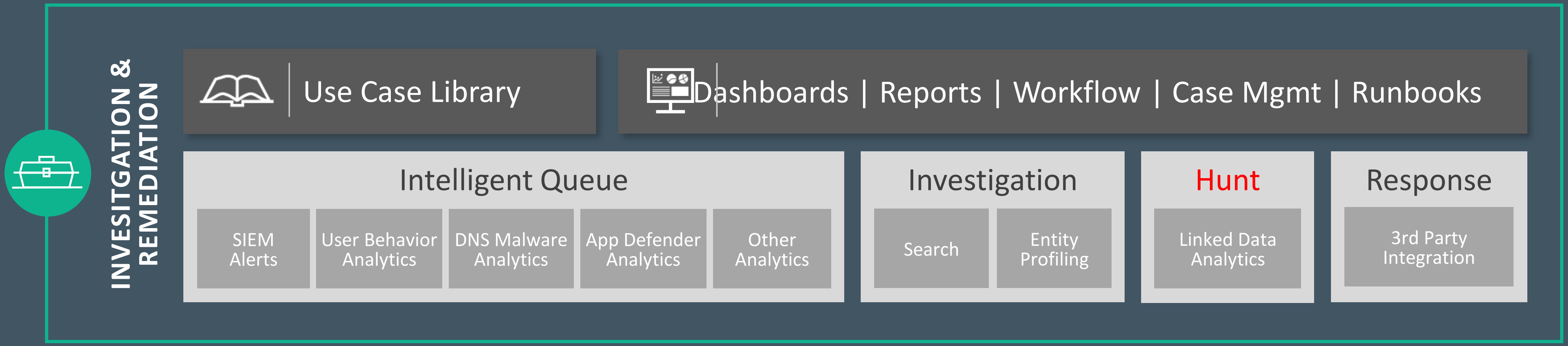
Select a command:
- ● Security Analytics Investigation
- ○ Security Analytics Meta Data Download
- ○ Security Analytics PCAP Download

Select a target:
- ● Blue Coat Security Analytics

End Time	Name	Device Vendor
25 Sep 2014 23:11:20 PDT	OS-WINDO	Sourcefire
25 Sep 2014 23:11:23 PDT	INDICATOR	Sourcefire
25 Sep 2014 23:11:23 PDT	OS-WINDO	Sourcefire
25 Sep 2014 23:11:23 PDT	OS-WINDO	Sourcefire
25 Sep 2014 23:11:24 PDT	INDICATOR	Sourcefire
25 Sep 2014 23:11:12 PDT	INDICATOR	Sourcefire
25 Sep 2014 23:11:12 PDT	INDICATOR	
25 Sep 2014 23:11:12 PDT	INDICATOR	
25 Sep 2014 23:10:56 PDT	INDICATOR	
25 Sep 2014 23:10:58 PDT	INDICATOR	
25 Sep 2014 23:10:42 PDT	EXPLOIT-KI	
25 Sep 2014 23:10:42 PDT	EXPLOIT-KI	
25 Sep 2014 23:10:42 PDT	EXPLOIT-KI	Sourcefire
25 Sep 2014 23:10:42 PDT	EXPLOIT-KI	Sourcefire
25 Sep 2014 23:10:42 PDT	EXPLOIT-KI	Sourcefire
25 Sep 2014 23:10:42 PDT	EXPLOIT-KI	Sourcefire
25 Sep 2014 23:10:42 PDT	EXPLOIT-KI	Sourcefire

Hewlett Packard
Enterprise

What is Hunt?



INVESITGATION & REMEDIATION

Use Case Library

Dashboards | Reports | Workflow | Case Mgmt | Runbooks

Intelligent Queue

SIEM Alerts

User Behavior Analytics

DNS Malware Analytics

App Defender Analytics

Other Analytics

Investigation

Search

Entity Profiling

Hunt

Linked Data Analytics

Response

3rd Party Integration

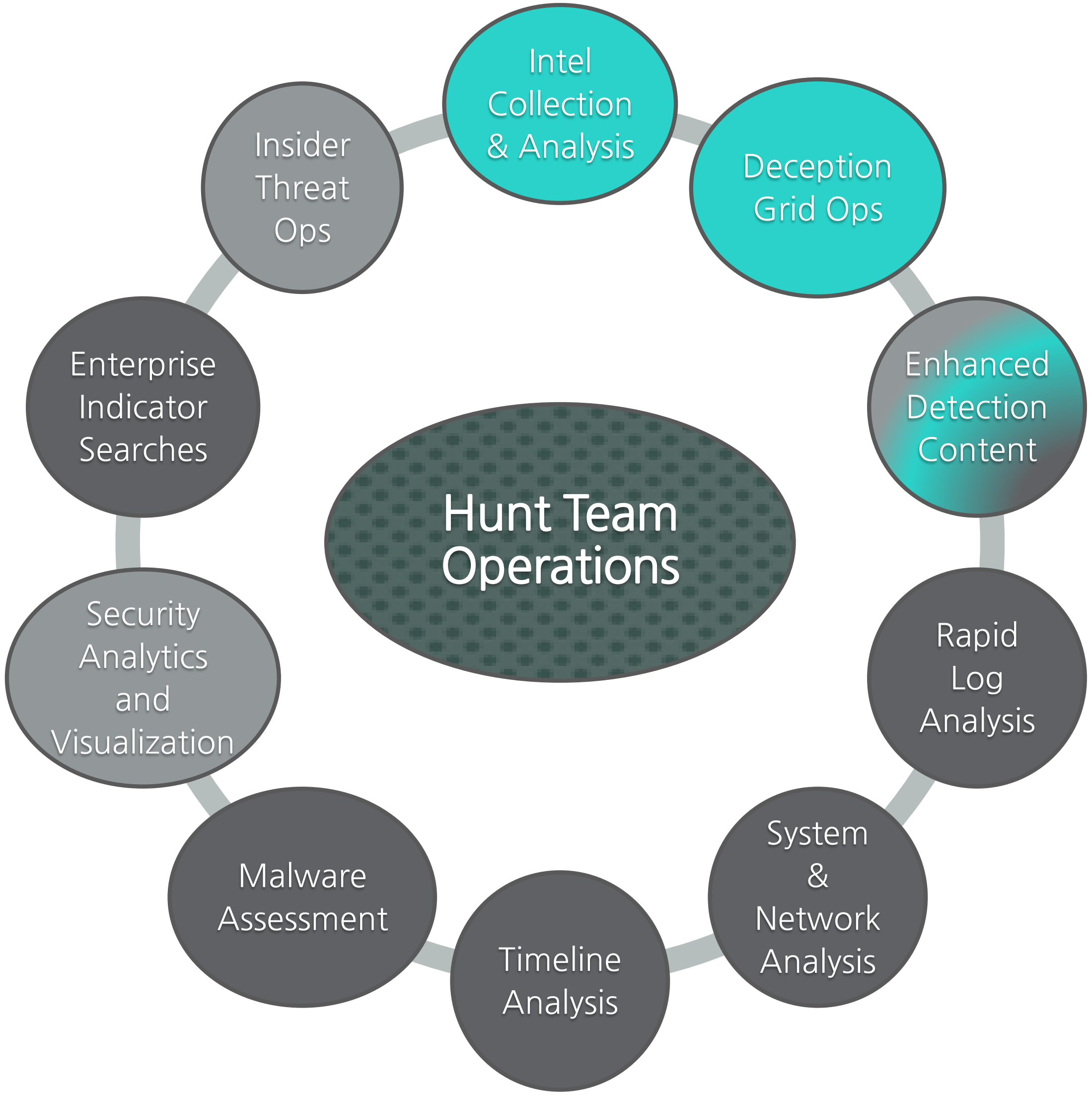
What is Hunt?

Hunt sits between the SOC, the intelligence team, analytics/data team, and Incident Response

Big Data & Analytics
Unknown unknowns

Finding needles in haystacks
Unknown knowns

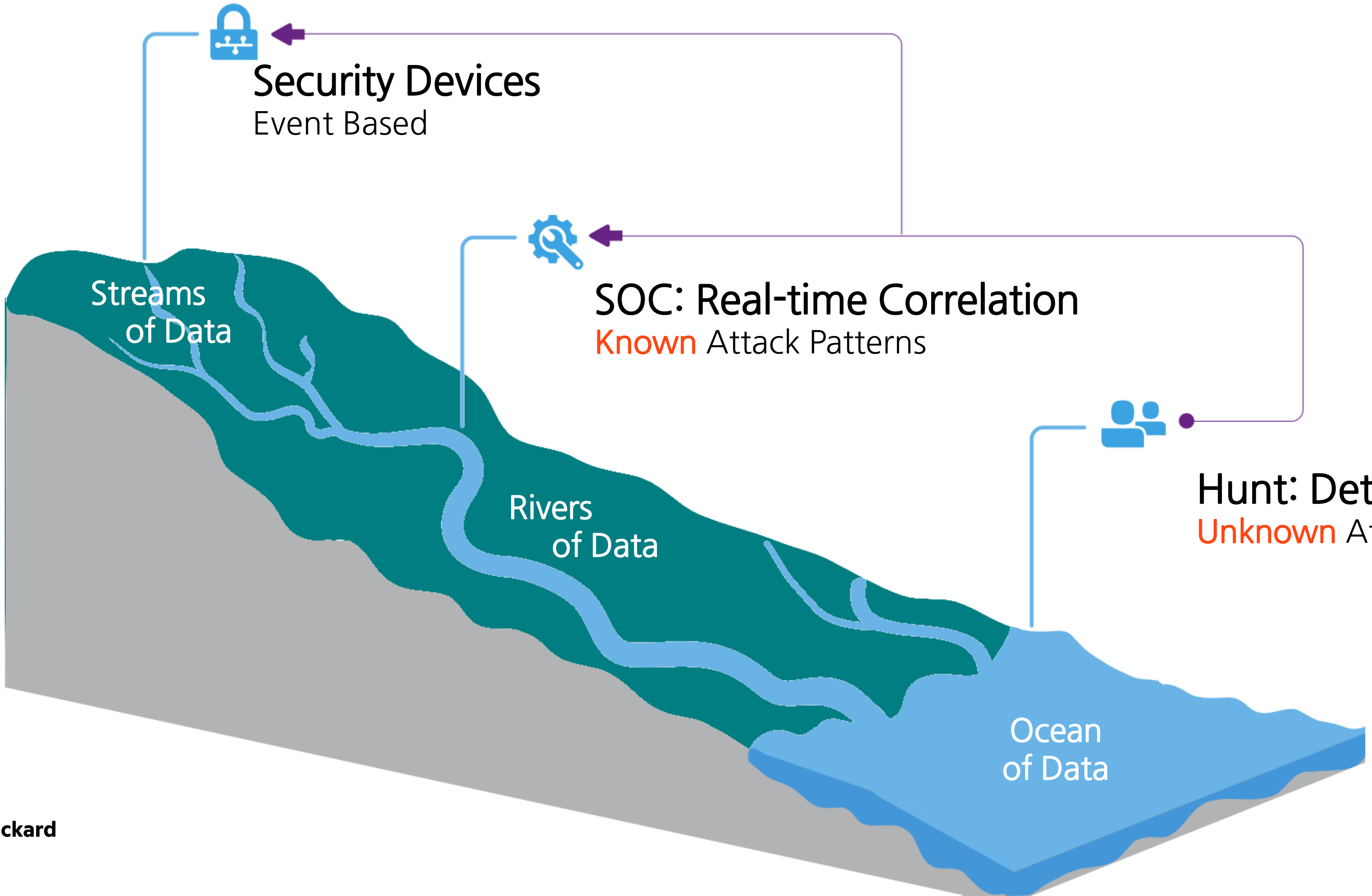
Incident Response
Understanding of business logic of apps and getting logs


Hunt Team Operations
Intel Collection & Analysis
Deception Grid Ops
Enhanced Detection Content
Rapid Log Analysis
System & Network Analysis
Timeline Analysis
Malware Assessment
Security Analytics and Visualization
Enterprise Indicator Searches
Insider Threat Ops

Hewlett Packard Enterprise

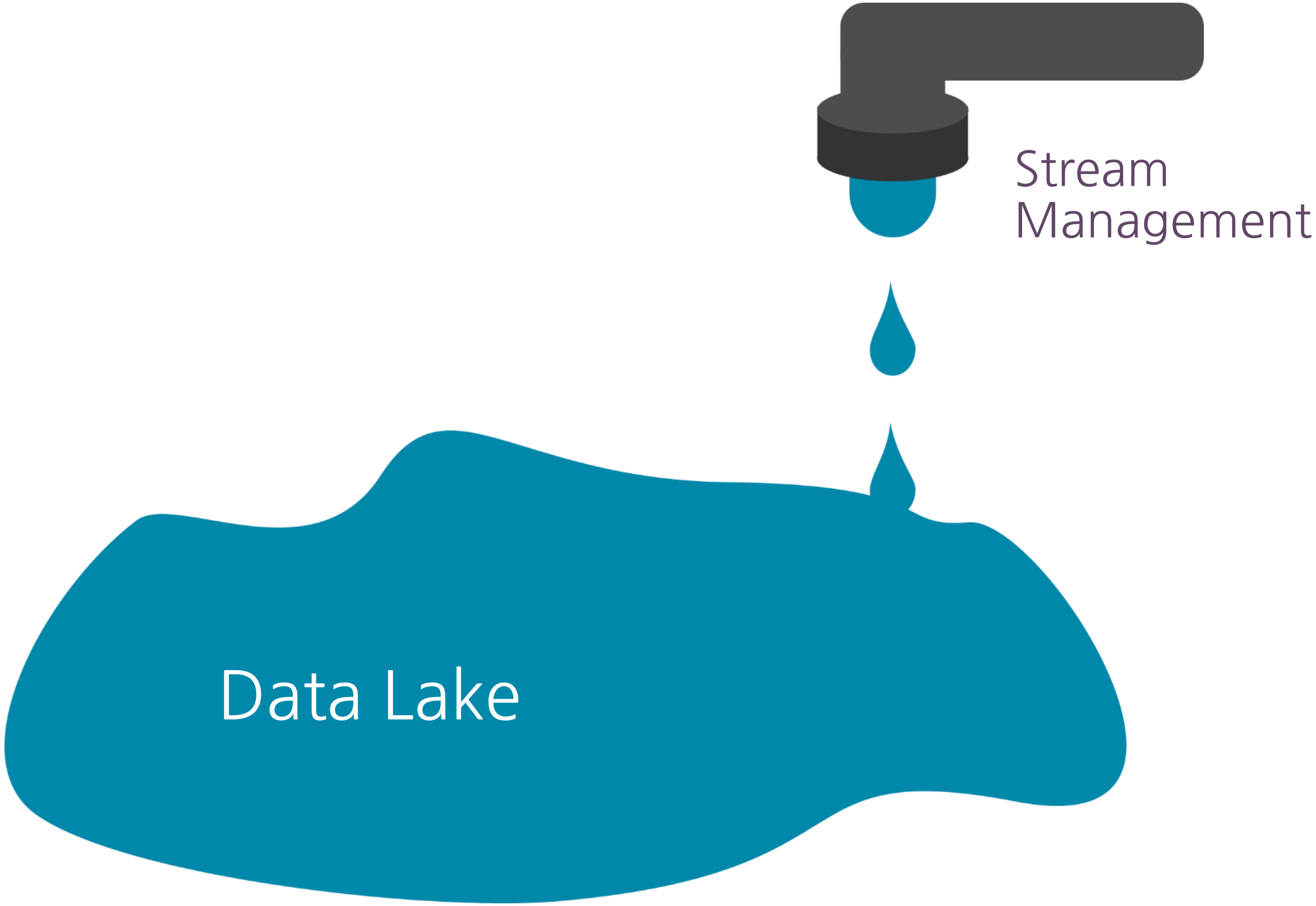
Hunt team이 필요한 이유

보안위협을 찾기위해 데이터 저장 및 처리 속도에 최신 기술을 활용



데이터 통합

Tooling and processes to ensure accurate data collection & persistence.



데이터 탐험(Exploration)

Tooling and processes on your data which provide flexible & capable:

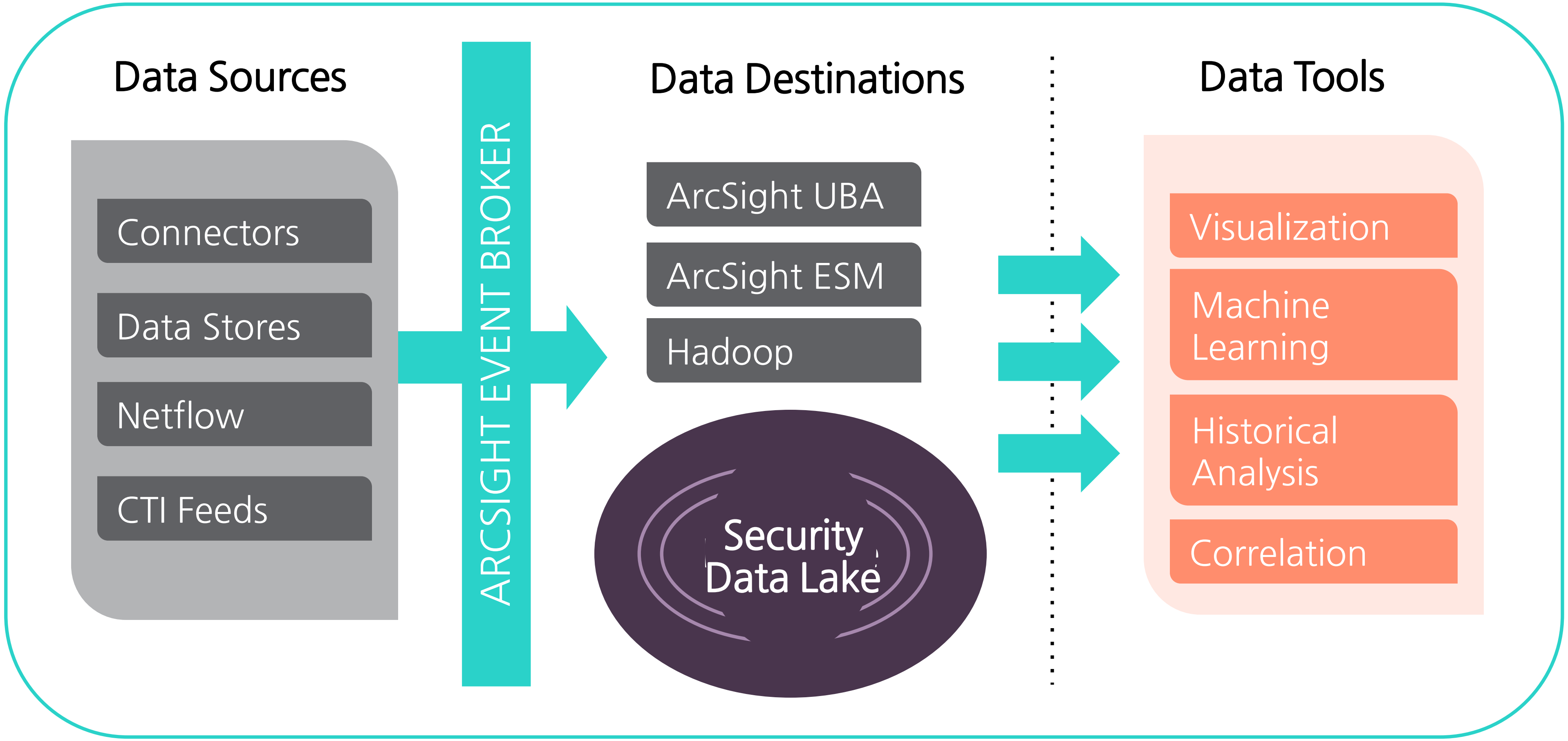
- access
- aggregation
- manipulation

Sometimes, you need a boat.
Sometimes, a bucket or funnel.

Hewlett Packard
Enterprise

ArcSight는 최적의 hunt 상태에서 데이터 확보를 지원

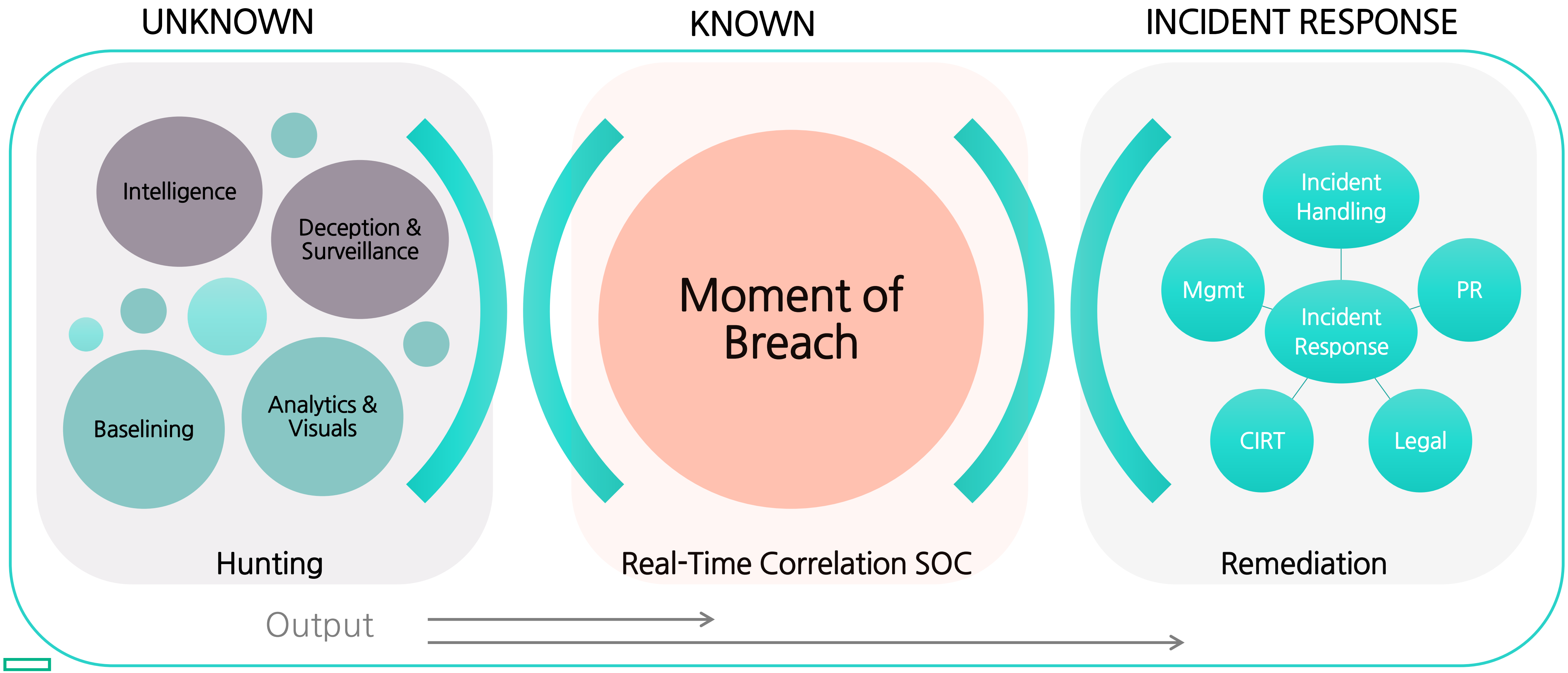
SOC 담당자(보안 분석가)는 여러 업무 단계에서 데이터 확보가 최우선으로 필요



Hewlett Packard
Enterprise

실시간 SOC 역량 강화를 위해 hunt program 필요

Hunting은 알려지지 않은 공격을 알려진 공격으로 바꾸어주며, 실시간 SOC시스템을 새로운 정보로 강화할 수 있는 방법을 제공



ArcSight New Architecture

실시간 상관분석과 빅데이터 분석이 동시에 가능한 개방형 SIEM 플랫폼

Security Operations
(On-prem & Managed)

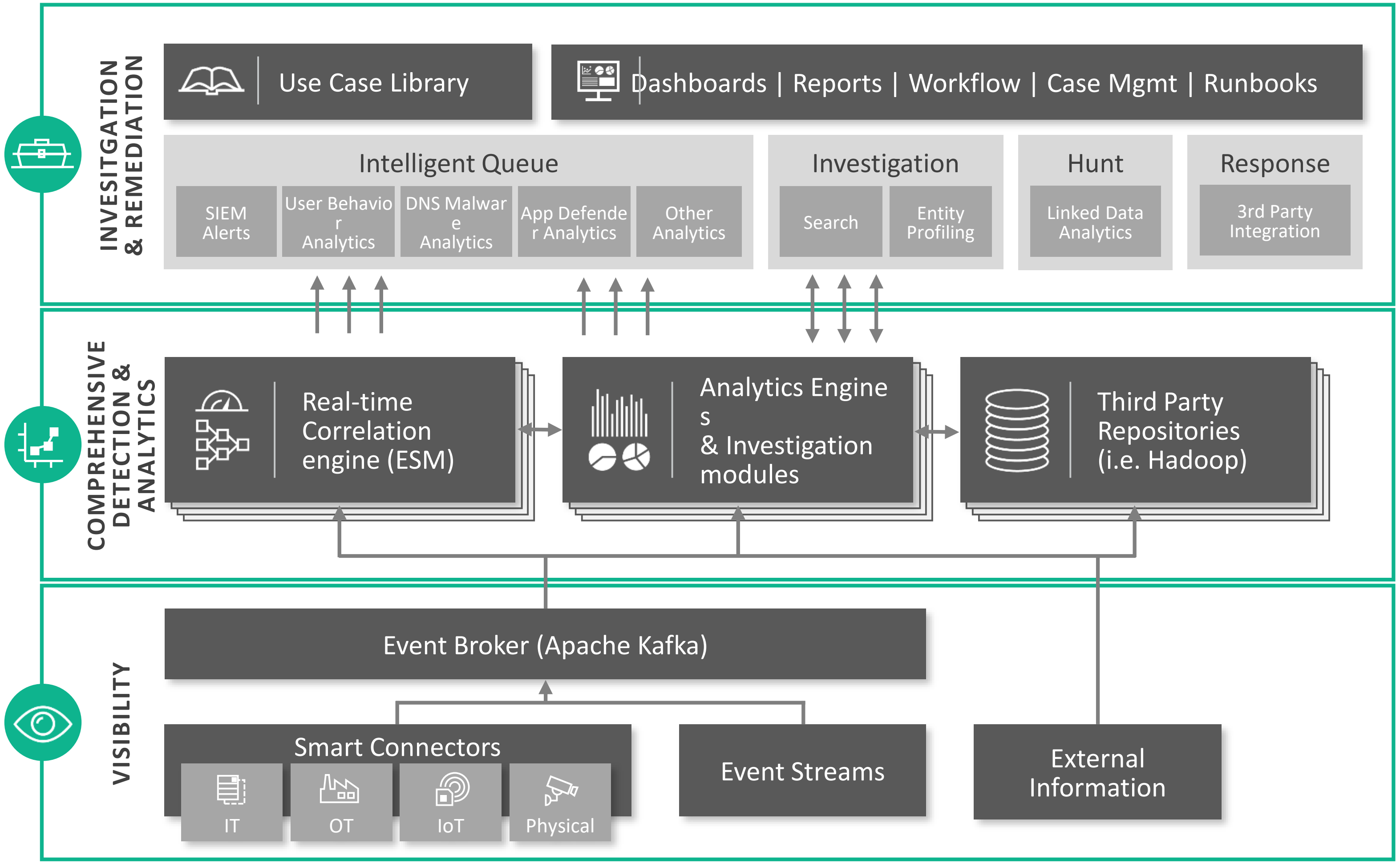
Security Analysts
Level 1

Security Analysts
Level 2

Hunt Team

Data Sources
(Structured & Unstructured)
+ Control points

- Users
- Cloud
- Apps
- Servers & Workload
- s
- Network
- Endpoints
- IoT



INVESITGATION & REMEDIATION

Use Case Library

Dashboards | Reports | Workflow | Case Mgmt | Runbooks

Intelligent Queue: SIEM Alerts; User Behavio r Analytics; DNS Malwar e Analytics; App Defende r Analytics; Other Analytics

Investigation: Search; Entity Profiling

Hunt: Linked Data Analytics

Response: 3rd Party Integration

COMPREHENSIVE DETECTION & ANALYTICS

Real-time Correlation engine (ESM)

Analytics Engine s & Investigation modules

Third Party Repositories (i.e. Hadoop)

VISIBILITY

Event Broker (Apache Kafka)

Smart Connectors: IT; OT; IoT; Physical

Event Streams

External Information

Ticketing & Workflow

IT Operations
& Management S
ystems

Identity & Configuration

Active Directory

Config Mgmt DB

Intelligence Feeds

Threat Central

3rd Party Feeds

감사합니다

ArcSight is not just a SIEM anymore…

It’s a Real Time, Modular, Open Source,
Comprehensive Threat and Compliance Management Tool