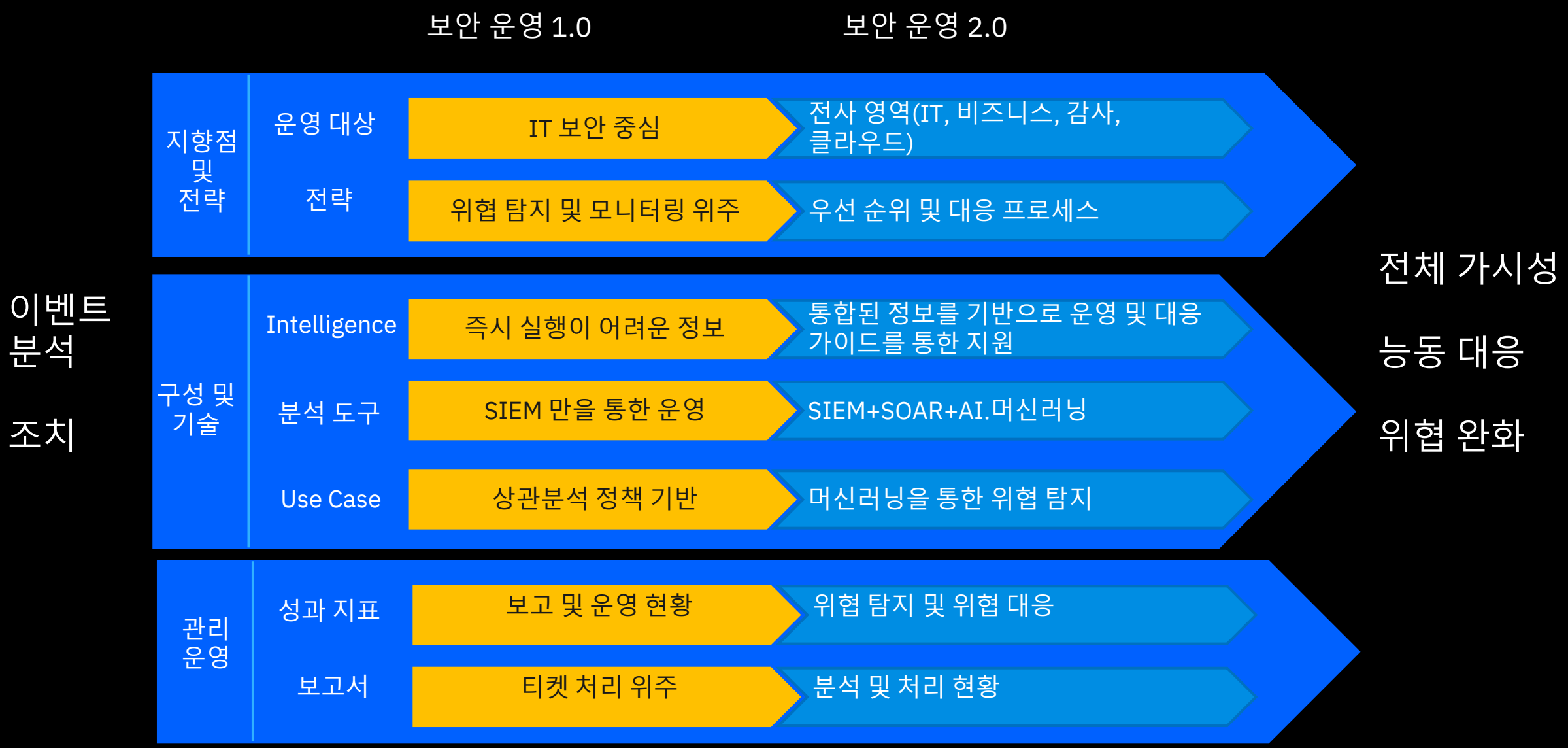
하이브리드 클라우드 환경의 차세대 보안관제 및 SOAR

나병준 실장/CISSP

한국IBM, 보안 사업부

보안 운영의 변화


보안 운영 1.0
보안 운영 2.0
지향점 및 전략
운영 대상
IT 보안 중심
전사 영역(IT, 비즈니스, 감사, 클라우드)
전략
위협 탐지 및 모니터링 위주
우선 순위 및 대응 프로세스
구성 및 기술
Intelligence
즉시 실행이 어려운 정보
통합된 정보를 기반으로 운영 및 대응 가이드를 통한 지원
분석 도구
SIEM 만을 통한 운영
SIEM+SOAR+AI.머신러닝
Use Case
상관분석 정책 기반
머신러닝을 통한 위협 탐지
관리 운영
성과 지표
보고 및 운영 현황
위협 탐지 및 위협 대응
보고서
티켓 처리 위주
분석 및 처리 현황
이벤트 분석
조치
전체 가시성
능동 대응
위협 완화

보안 운영에서 필요한 사항

보안 분석 효율 향상

분석을 위한 모든 데이터 연계 구성

위협 관리 프로세스 및 추가 분석 환경 구성

반복적이고 오랜 작업 자동화

- ✓ 빠른 위협 탐지, 지속적인 위협 조사와 빠른 대응을 통한 위험 완화
- ✓ 구현된 분석 프로세스 및 보고방안을 통해 지속적인 보안 모니터링 강화
- ✓ 보안 운영 팀의 기술, 효율 및 팀 분위기 향상

기존의 보안 방법이 디지털 혁신을 따라가기 힘든 이유

너무 많은 업무

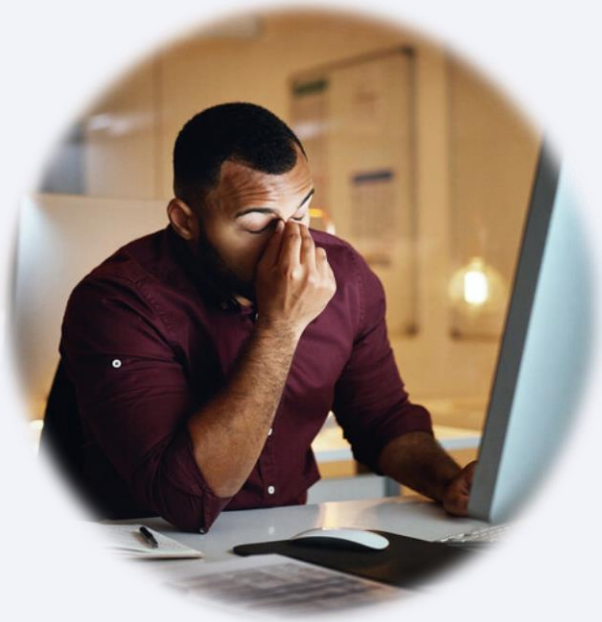
- Meet with CIO and stakeholders
- Nail down third-party risk
- Manage GDPR program with privacy office
- Respond to questions from state auditors
- Update CEO for board meeting
- Update budget projections
- Write security language for vendor's contract
- Make progress on the never-ending identity project
- Review and updated project list
- Edit communication calendar
- Update risk rankings on security roadmap
- Clarify policies governing external storage devices
- Provide testing and encryption tool direction
- Provide data handling best practices
- Help with new acquisition
- Meet with senior project manager
- Send new best practices to development teams
- Review logs for fraud ongoing investigation
- Help with insider threat discovery
- Determine location of sensitive data in the cloud
- Investigate possible infection on legacy system
- Continue pen testing of new business mobile app
- Help architects understand zero-trust
- Answer security policy emails
- Format security status report for executives
- Meet with recruiter to discuss staffing
- Write test plan requirements for new products
- Meet regarding improving security of facilities

너무 많은 공급 업체

너무 심한 복잡성

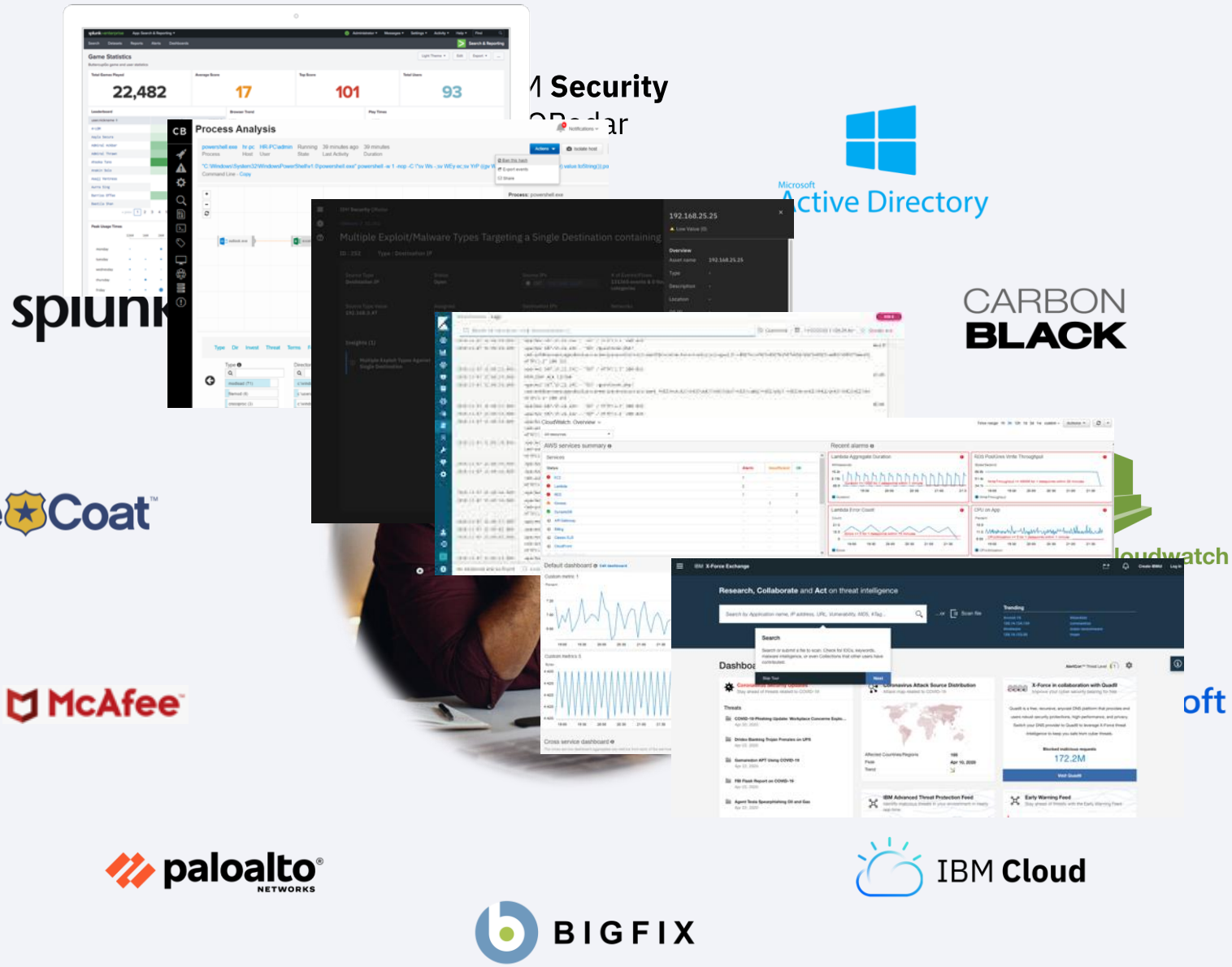
너무 많은 경고

완전한 보안 가시성을 얻으려면 보안 분석가가 여러 도구를 배워야합니다...



완전한 보안
가시성을 얻으려면
보안 분석가가
여러 도구를
배워야합니다...

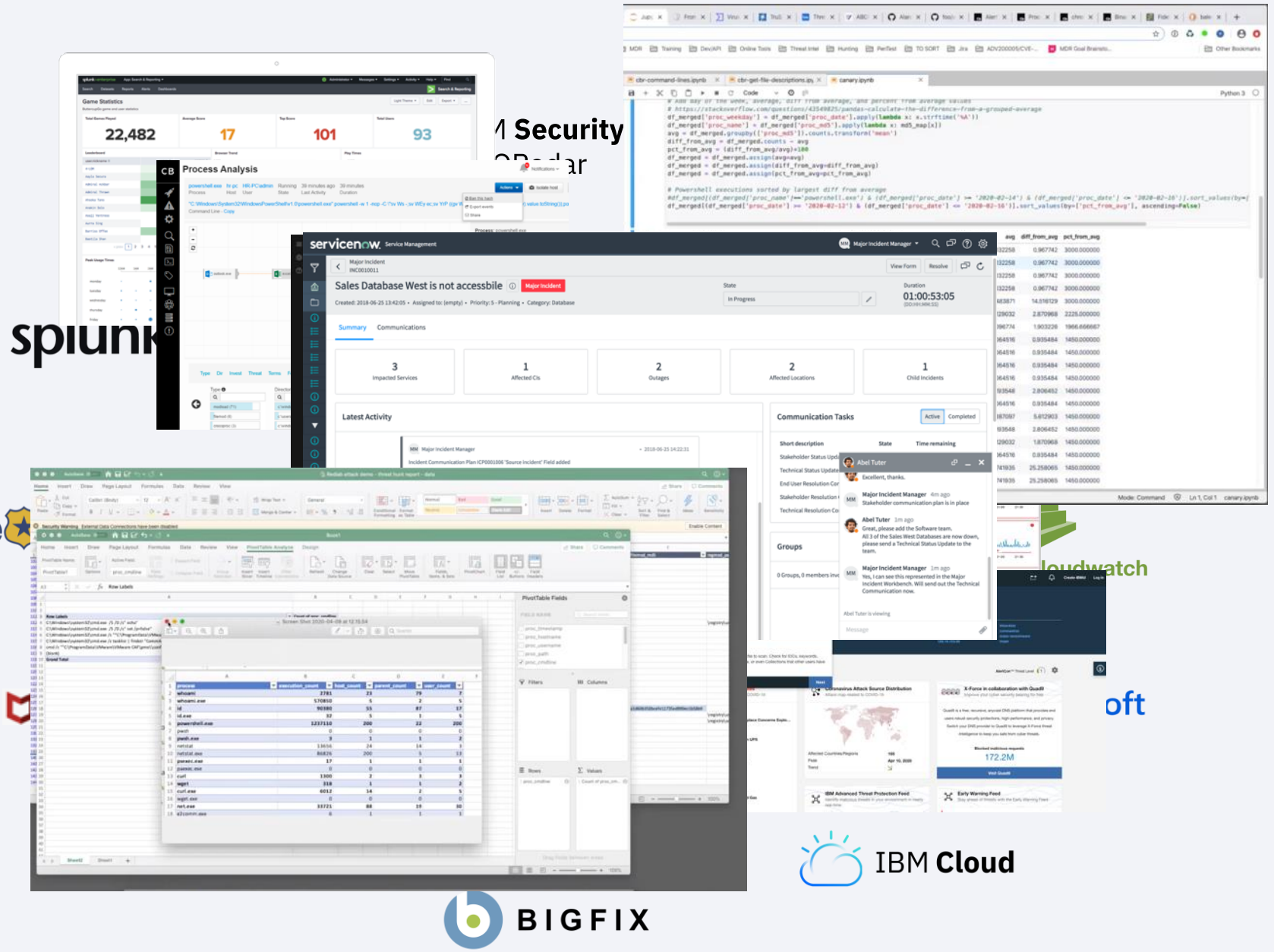
많은 화면을
열어 탐색을
해야 합니다.



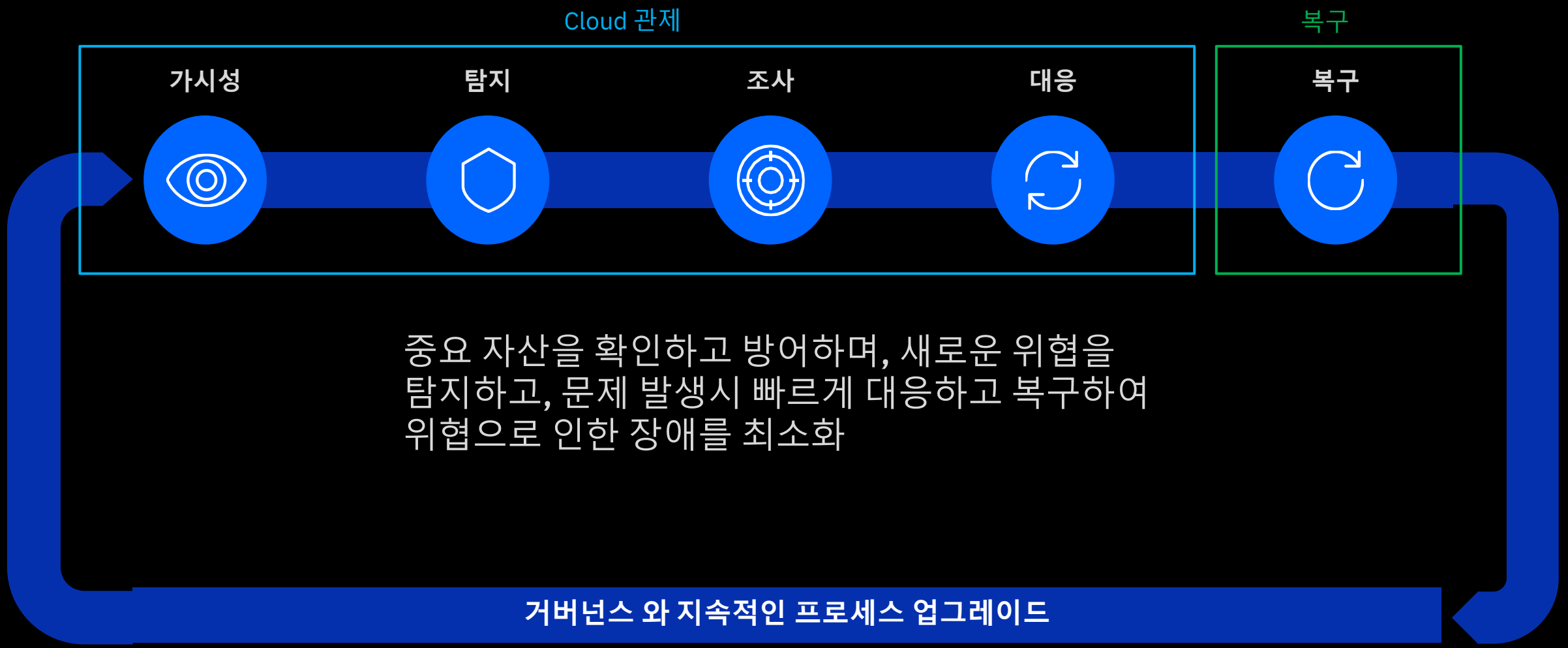
완전한 보안
가시성을 얻으려면
보안 분석가가
여러 도구를
배워야합니다...

많은 화면을
열어 탐색을
해야 합니다.

그리고 대응을 하기
위해서 격리된 툴과
팀을 통해 보안
인사이트를
공유해야 하는
비효율적인 절차에
의존합니다.



IBM 클라우드 SOC 운영 프로세스



SOAR의 정의

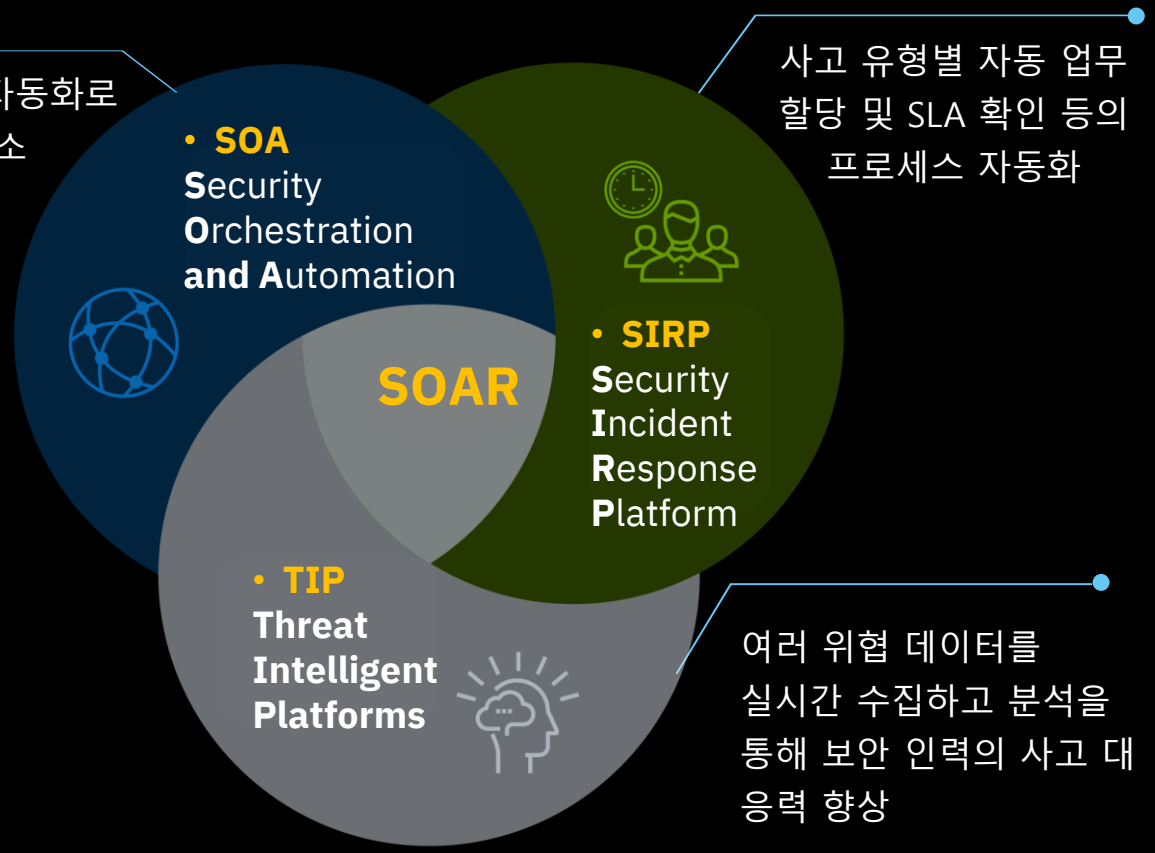
Gartner

"기술인력, 전문성 및 예산 부족과 더불어 적대적 위협발생이 증가하고 있는 어려움으로 인해 조직은 SOAR 기술을 검토하고 있습니다"

"The challenges from an increasingly hostile threat landscape, combined with a lack of people, expertise and budget are driving organizations toward SOAR technologies."

– Innovation Insight for Security Orchestration, Automation and Response
November 30, 2017

Growth of the Security Orchestration, Automation & Response market



SOAR의 주요역할

01 Orchestration

People (보안팀) / **Technology** (보안 솔루션)
/ **Process** (표준 대응 지침)을 하나로 조율

02 Automation

자동 프로세스 내 **관리자의 승인 절차** 삽입
자동 프로세스의 **모듈화**를 통한 재사용

03 Incident Management & Collaboration

타 부서 및 연계 기관과의 **협업환경**
인시던트별 보안 **컴플라이언스, 표준 대응 지침**
최신 위협 정보 피드 및 분석

04 Dashboards & Reporting

SLA 기반 대응 업무 현황 / 대응 **역할별** 데시보드 제공
자산 활용도에 대한 확인

SOAR의 보안사고 발생 시 동작방식

사고 예방 업무 지원 및 사고 발생 후 대응 자동화 환경 제공

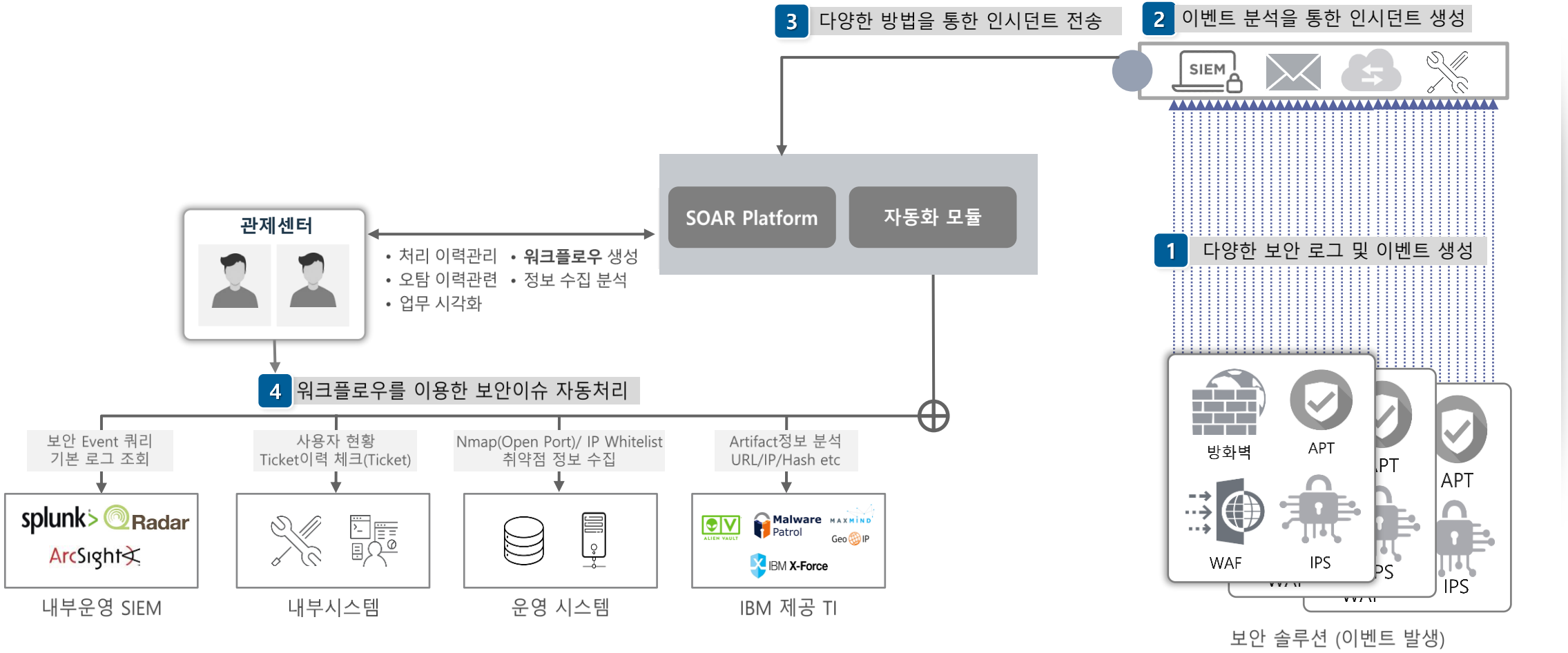
SOAR Platform

자동화 모듈

보안 솔루션 (이벤트 발생)

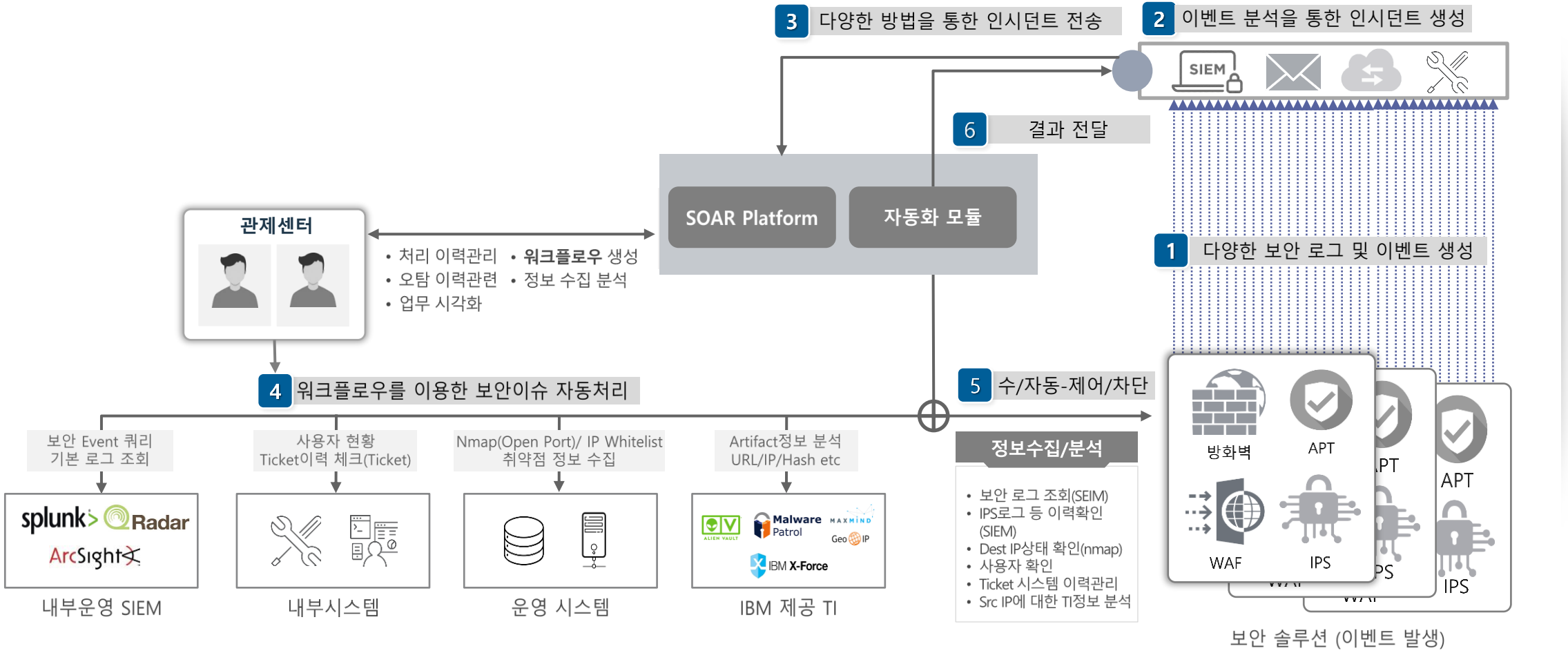
SOAR의 보안사고 발생 시 동작방식

사고 예방 업무 지원 및 사고 발생 후 대응 자동화 환경 제공



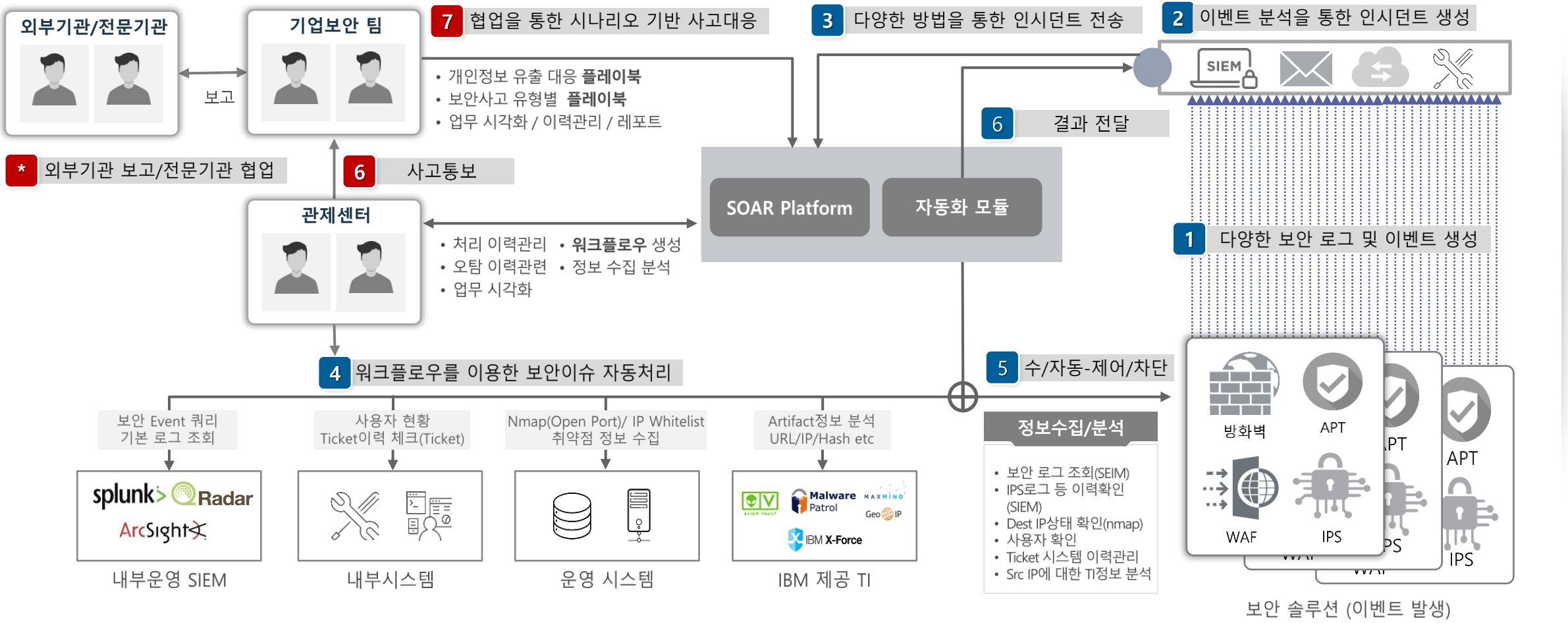
SOAR의 보안사고 발생 시 동작방식

사고 예방 업무 지원 및 사고 발생 후 대응 자동화 환경 제공

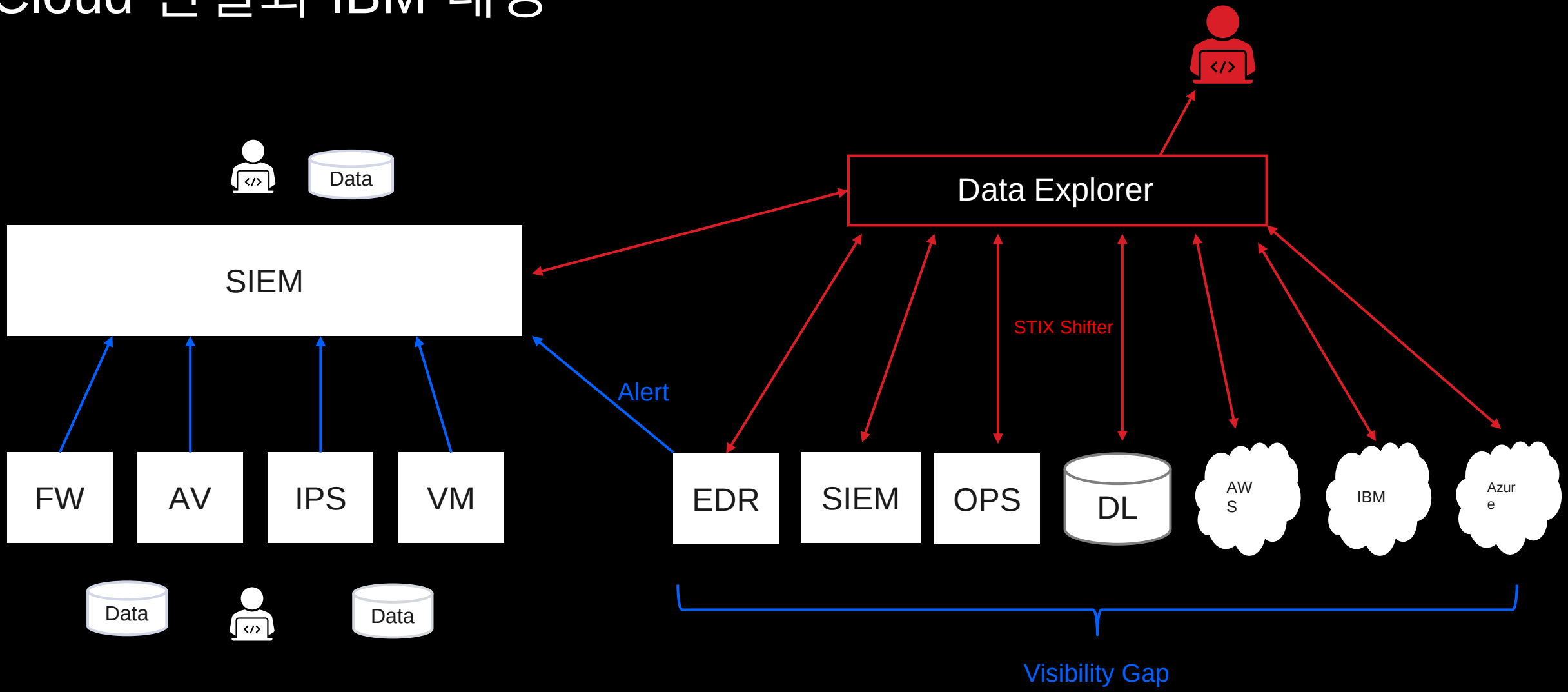


SOAR의 보안사고 발생 시 동작방식

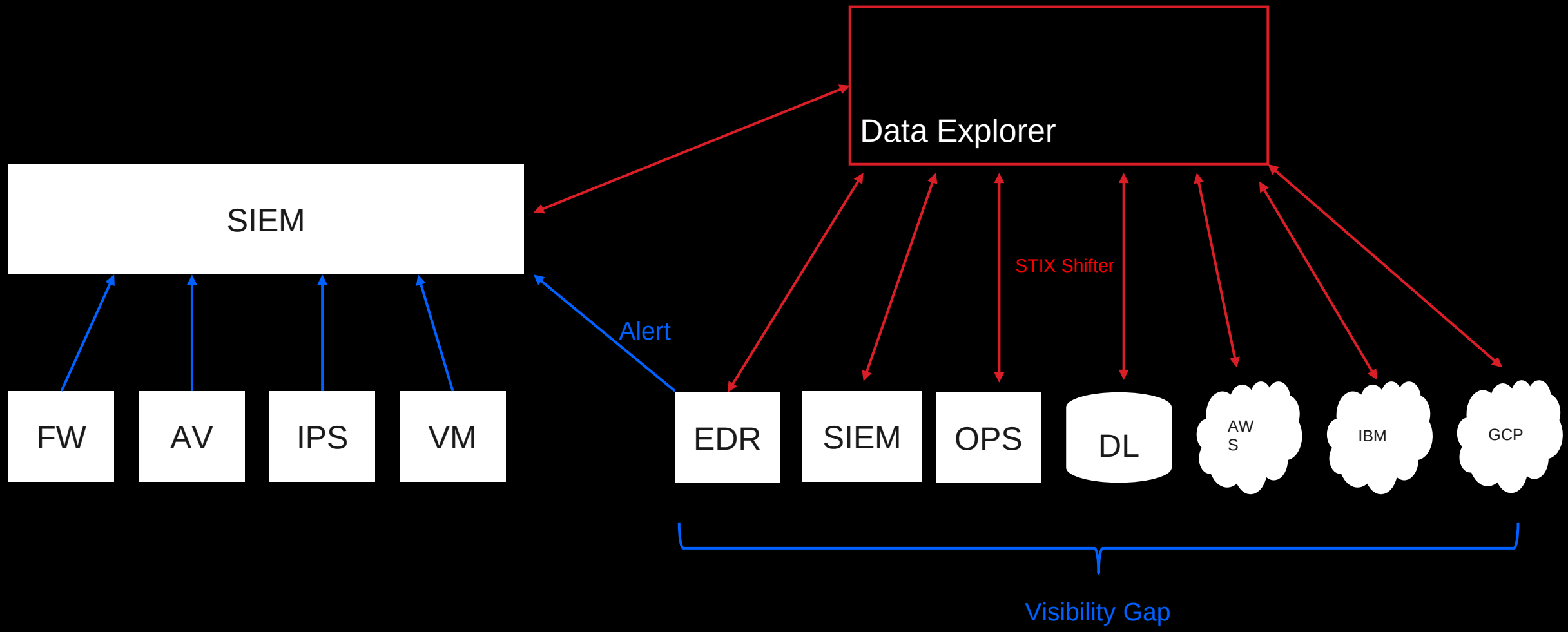
사고 예방 업무 지원 및 사고 발생 후 대응 자동화 환경 제공



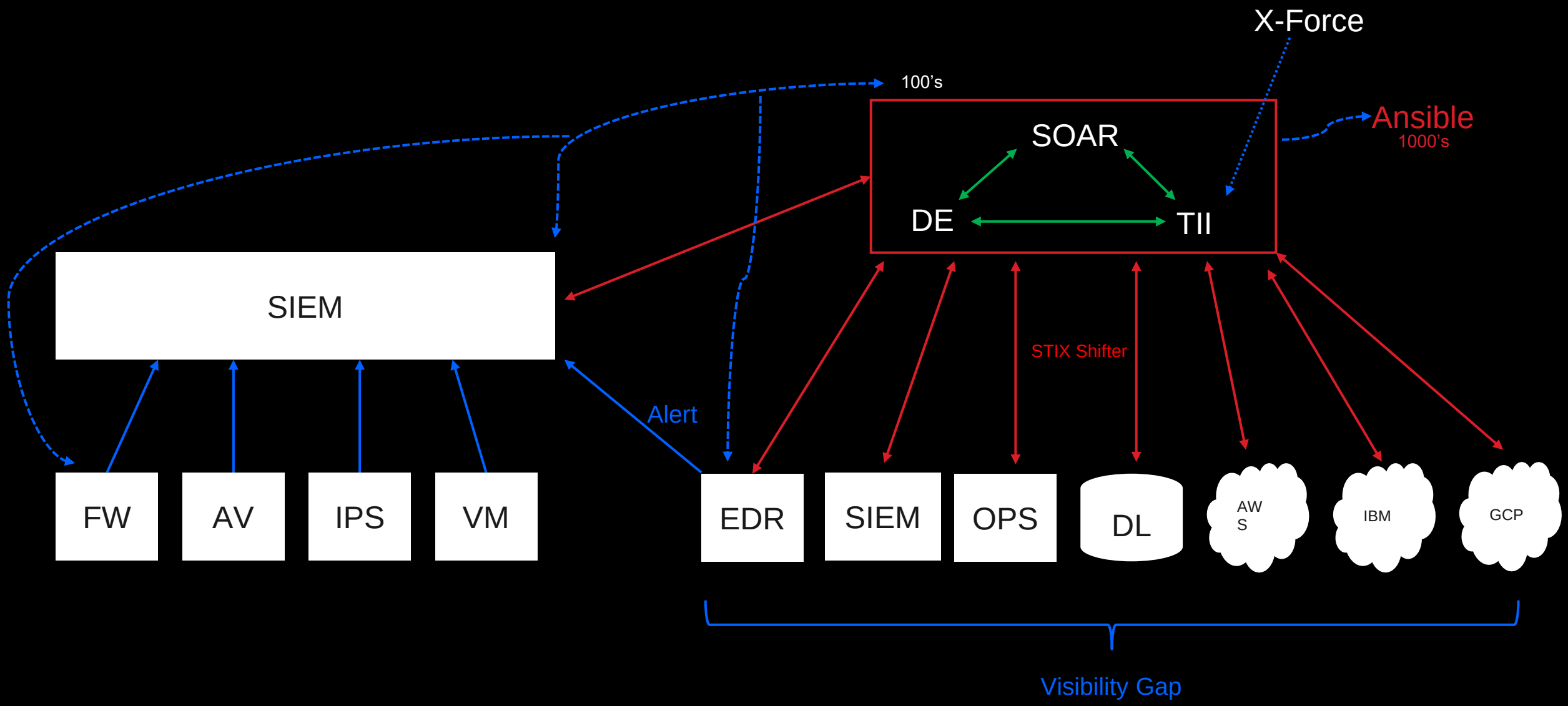
Cloud 현실과 IBM 대응



Cloud 현실과 IBM 대응



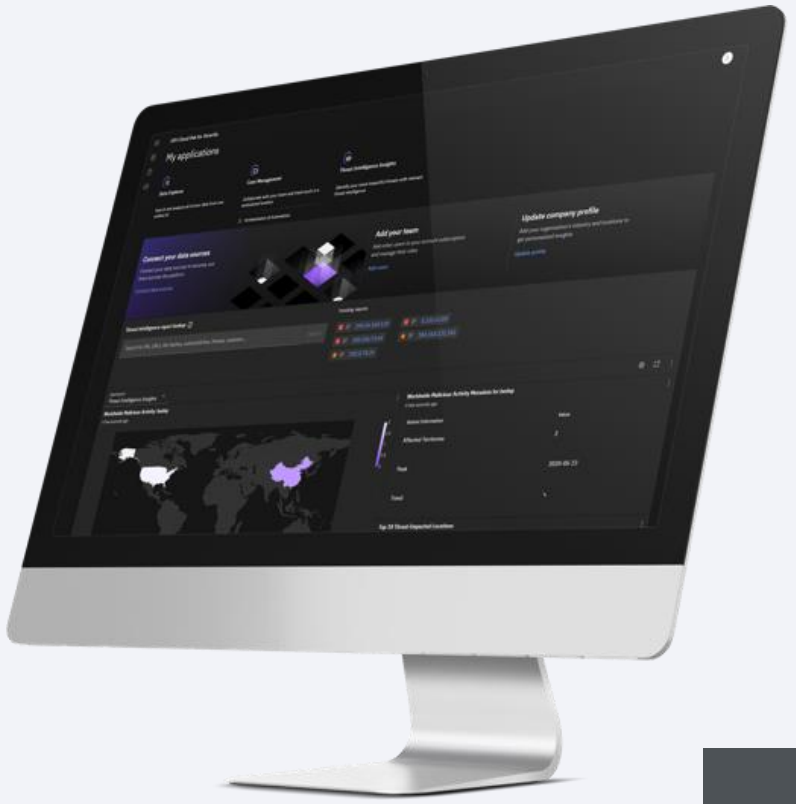
Cloud 현실과 IBM 대응



IBM Cloud Pak for Security

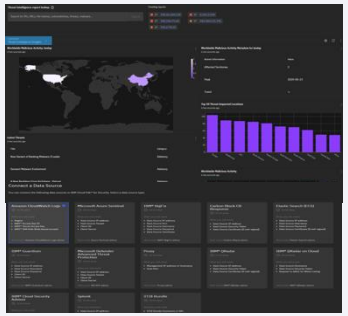
단순하고 통합된 UI로 **위협**을 조사하고 대응

위협 관리



통합된 보안 워크플로우

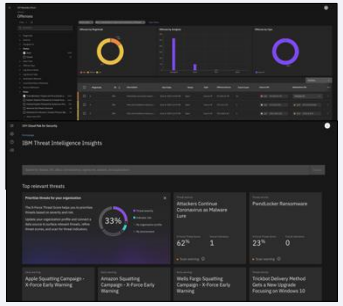
가시성



엔터프라이즈, 보안 도구 및 위협 인텔리전스에 대한 통합 가시성 확보

대시보드
보고 기능이 있는 통합 대시보드 및 시각화

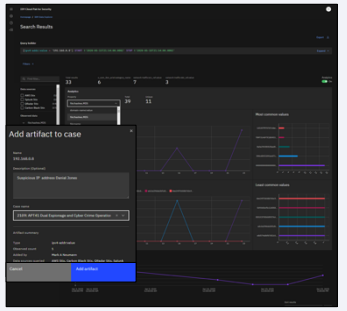
탐지



위협을 감지 및 통합하고 오탐 감소

Threat Intelligence Insights
X-Force 및 타사 소스의 위협 인텔리전스

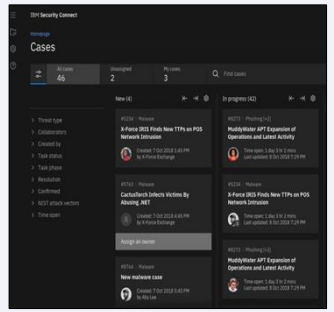
조사



AI 및 통합 검색으로 조사를 자동화. 통합 케이스 관리로 협업 수행

Data Explorer
보안 보안 시스템에 걸친 **검색과 조사**

대응



자동화, 플레이북 및 Ansible 통합으로 더 빠르게 대응

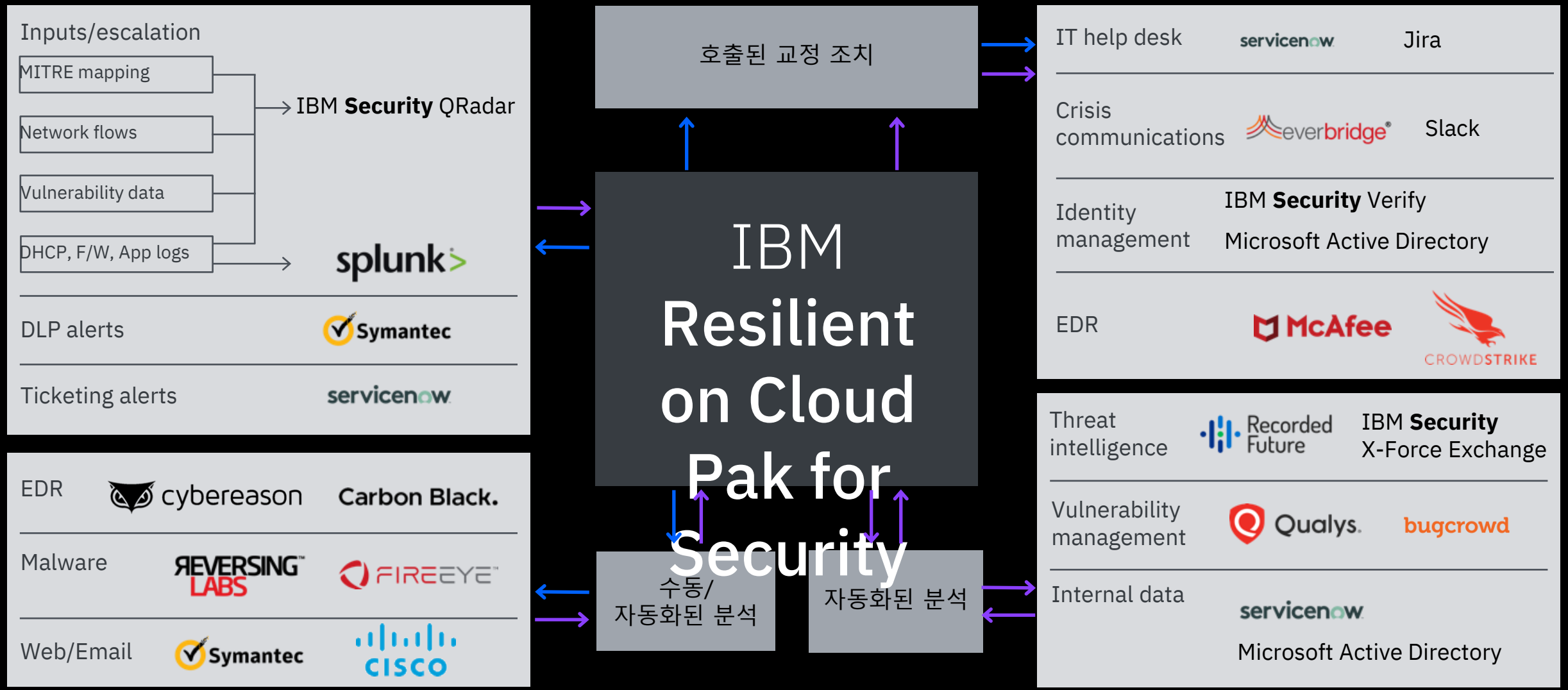
SOAR
오펜스와 통합된 케이스 관리

플랫폼 서비스

- 데이터 연결
- 자산 enrichment
- 케이스 관리
- 오케스트레이션
- 자동화
- 위험 관리

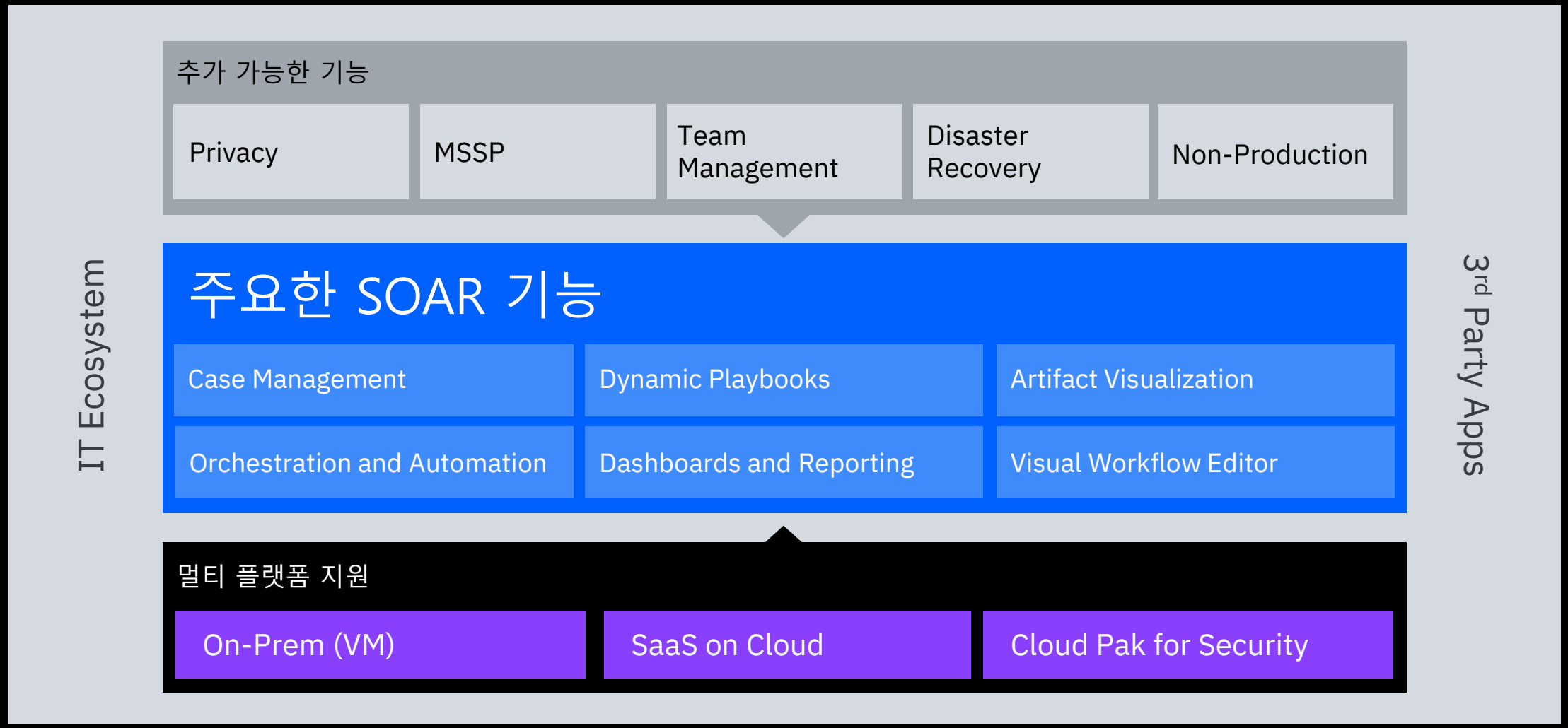
개방적이고 통합된 하이브리드 멀티클라우드 플랫폼

보안 사고 해결을 위한 중앙 허브



Manual Automatic

IBM Resilient의 아키텍처

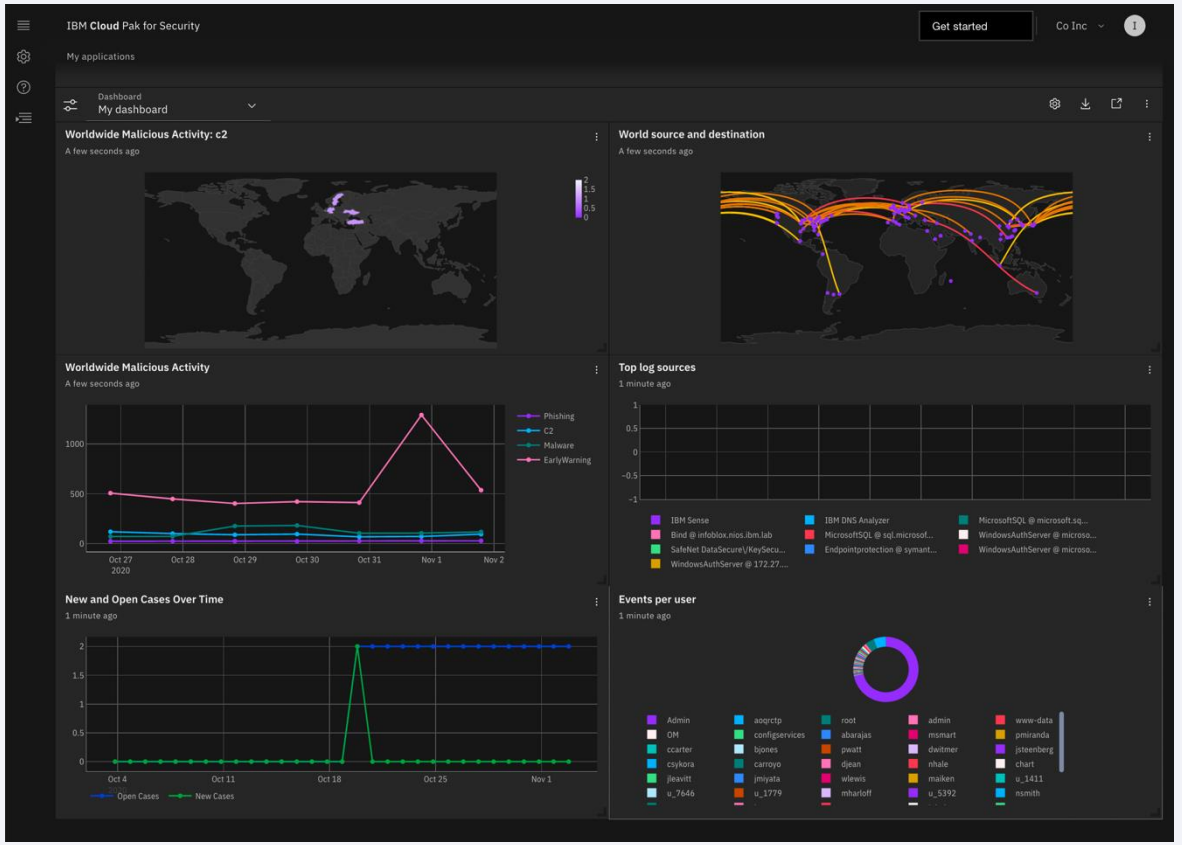


* 추가 기능에 대한 가격은 설정 옵션에 따라 다릅니다.

대시보드와 분석

위협 및 위험에 대한 맞춤형 메트릭

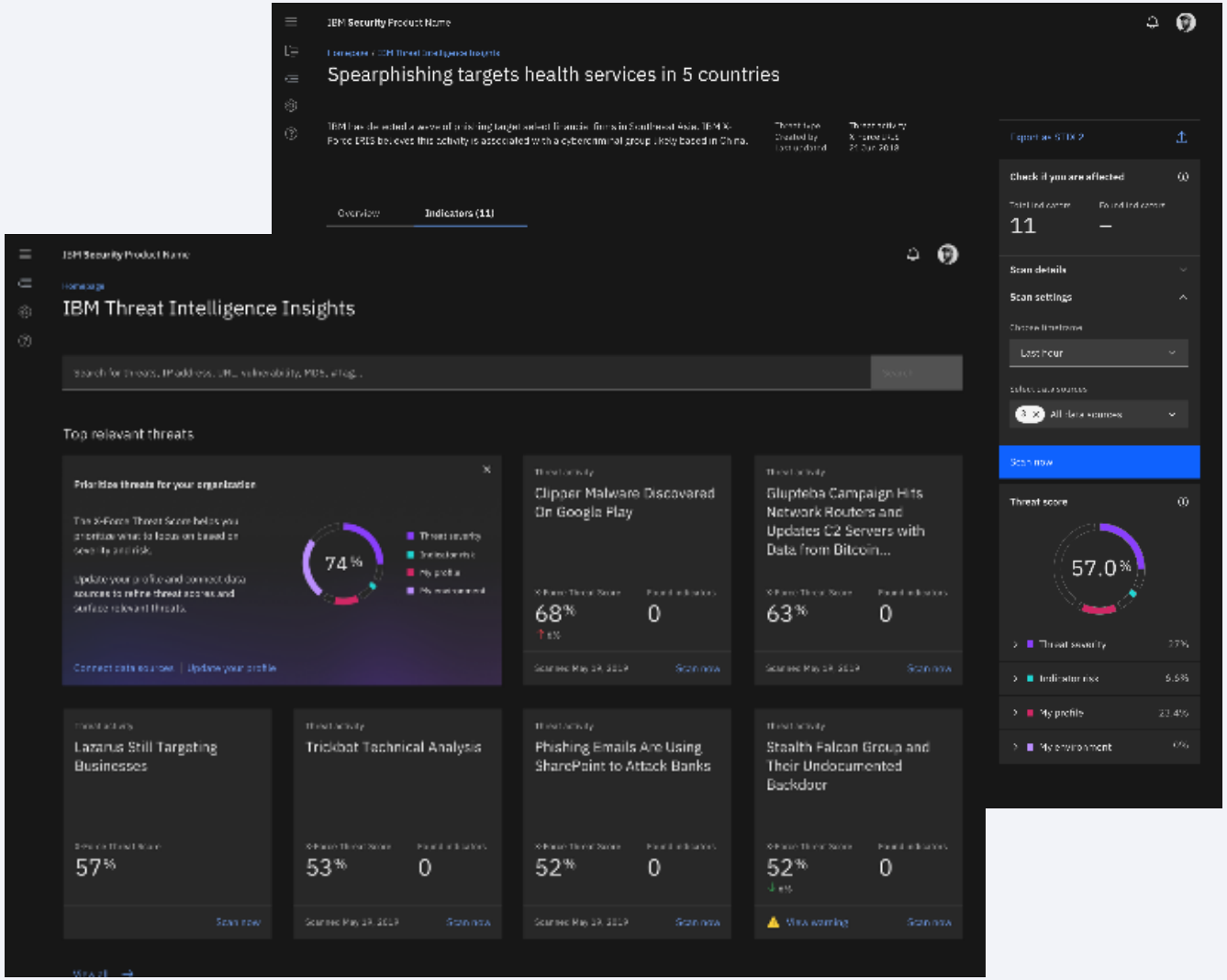
- Threat Intelligence, SIEM 및 SOAR 시스템의 운영 메트릭을 사용한 **통합 SOC 대시 보드를 통한 모니터링 및 커스터마이징**
- 관리를 위해 높은 수준의 보안 데이터를 시각화하고 자체 대시 보드를 구축하여 **분석가가 세부 정보를 드릴 다운하도록 함**
- 케이스 유형, 심각도 및 시간에 대한 SOAR 관련 메트릭을 통해 **케이스 관리 및 응답 효율성 이해**
- QRadar User Behavior Analytics**에 직접 액세스하여** 내부자 위협과 관련된 위험한 사용자를 신속하게 식별



Threat Intelligence Insights

우선 순위가 지정되고 실행 가능한 위협 인텔리전스

- IBM X-Force 팀에서 선별한 상황 별 정보가 포함 된 보고서를 통해 **글로벌 위협 인텔리전스를 확보**
- 관련성, 심각도, 침투, 영향 및 실제 환경 관찰을 기반으로 계산 된 적응형 점수인 X-Force 위협 점수로 조직에 대한 **위협의 우선 순위를 지정**
- 연결된 데이터 소스에서 지속적이고 자동화 된 검색을 실행하고 활성 위협에 대한 사례를 자동으로 생성하는 Am I Affected를 사용하여 **환경에서 활성 위협을 식별하고 조치를 취함**
- **타사 위협 인텔리전스 피드를 주입하여** 간단한 단일 구성 화면을 통해 추가 위협 인텔리전스에 대한 투자를 재사용하고 조사 또는 사고의 맥락에서 플랫폼 전체에 정보를 풍부하게 함

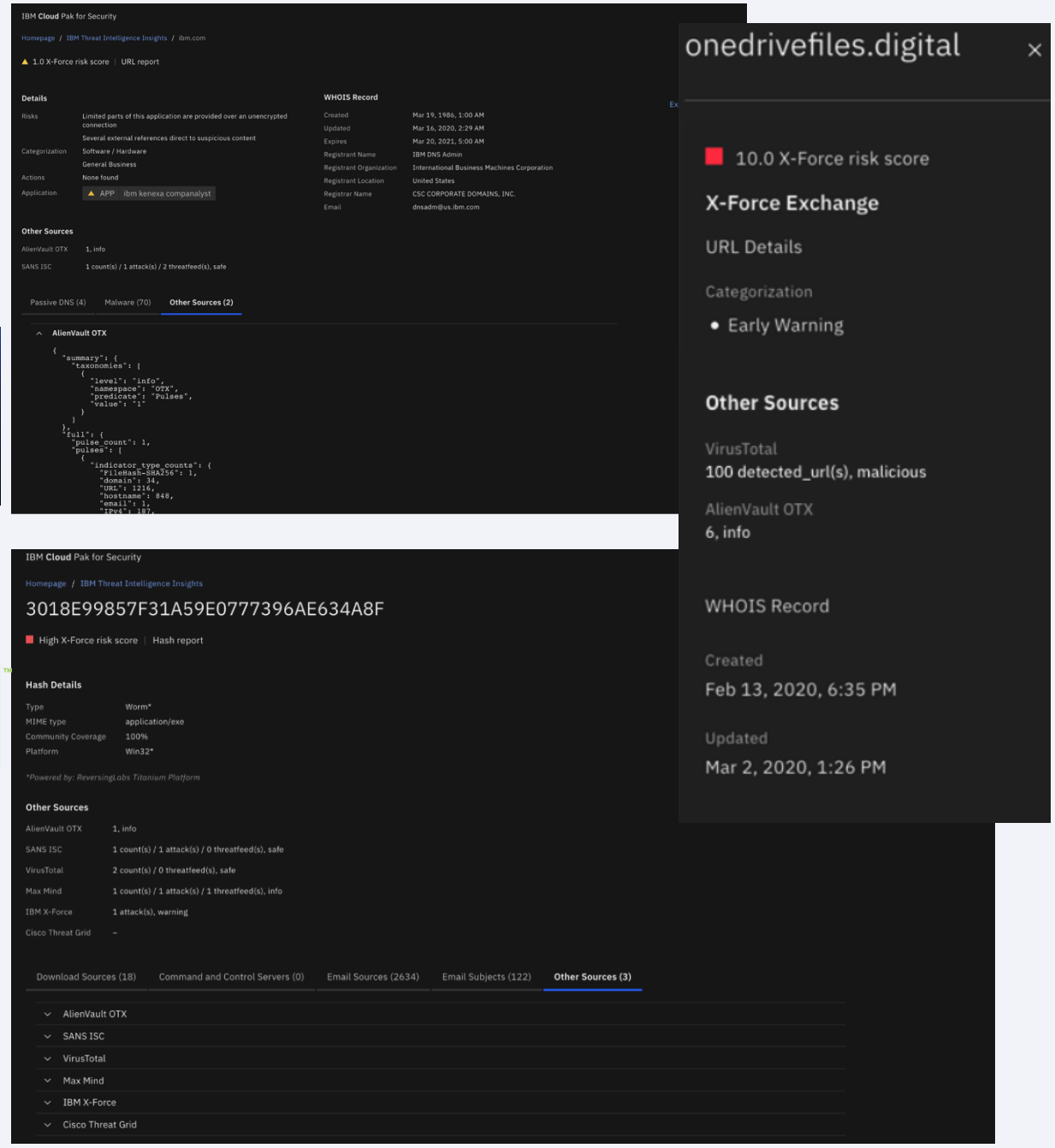


타사 위협 인텔리전스 소스로 확대

- 타사 위협 인텔리전스 피드를 주입하여 간단한 단일 구성 화면을 통해 추가 위협 인텔리전스에 대한 투자를 재사용하고 조사 또는 사고의 맥락에서 플랫폼 전체에 정보를 풍부하게 함

- 해당 기능은 위협 피드 라이선스 키와 자격 증명을 플랫폼에 추가하면 활성화 됨

- **IBM의 선도적인 X-Force 위협 인텔리전스 피드** 외에도이 플랫폼에는 AlienVault OTX, Cisco Threatgrid, MaxMind Geolocation, SANS Internet StormCenter 및 Virustotal과 같은 타사 소스의 5 가지 추가 위협 인텔리전스 피드에 통합이 사전 설정된 형태로 제공됨(단, 타사 피드 비용은 별도)

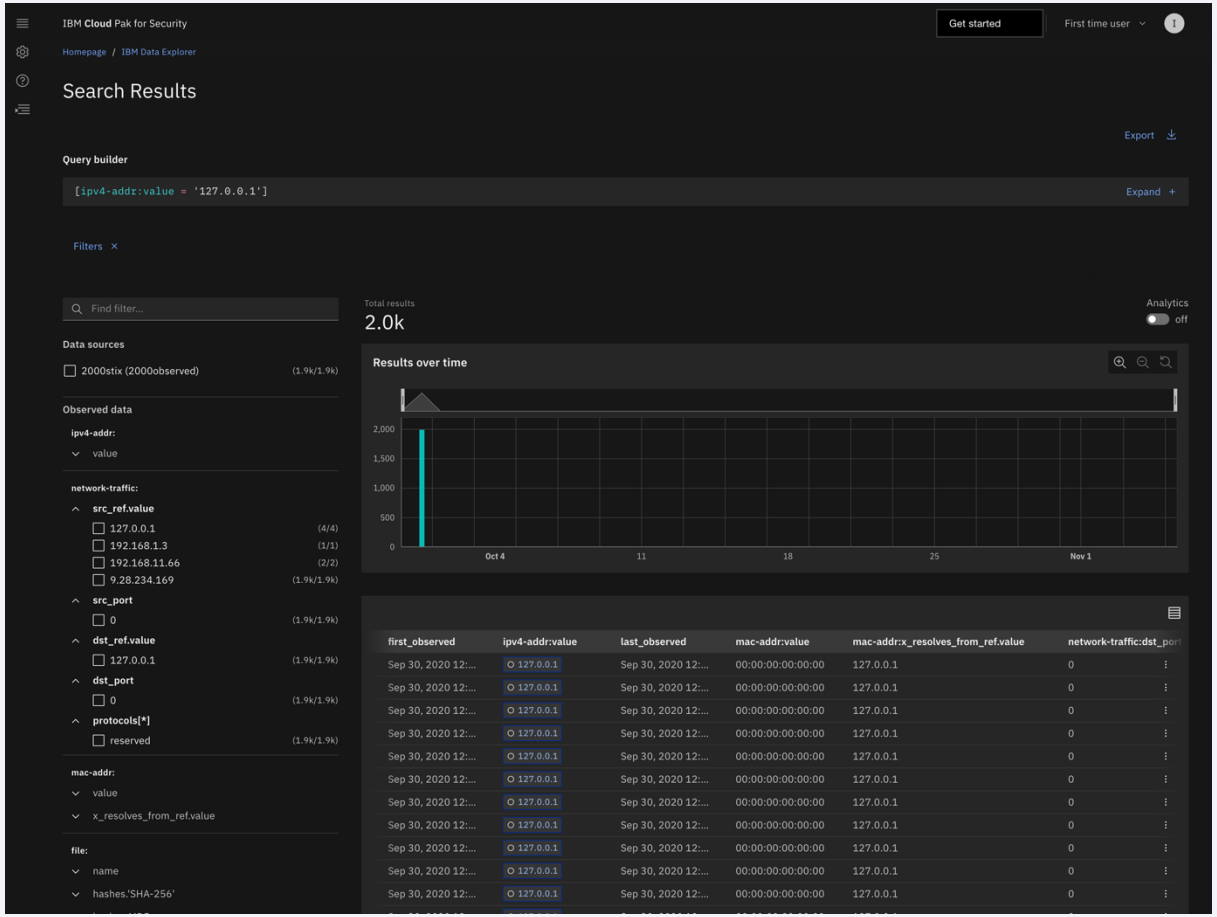


*Upcoming capabilities

Data Explorer

통합 검색 & 조사

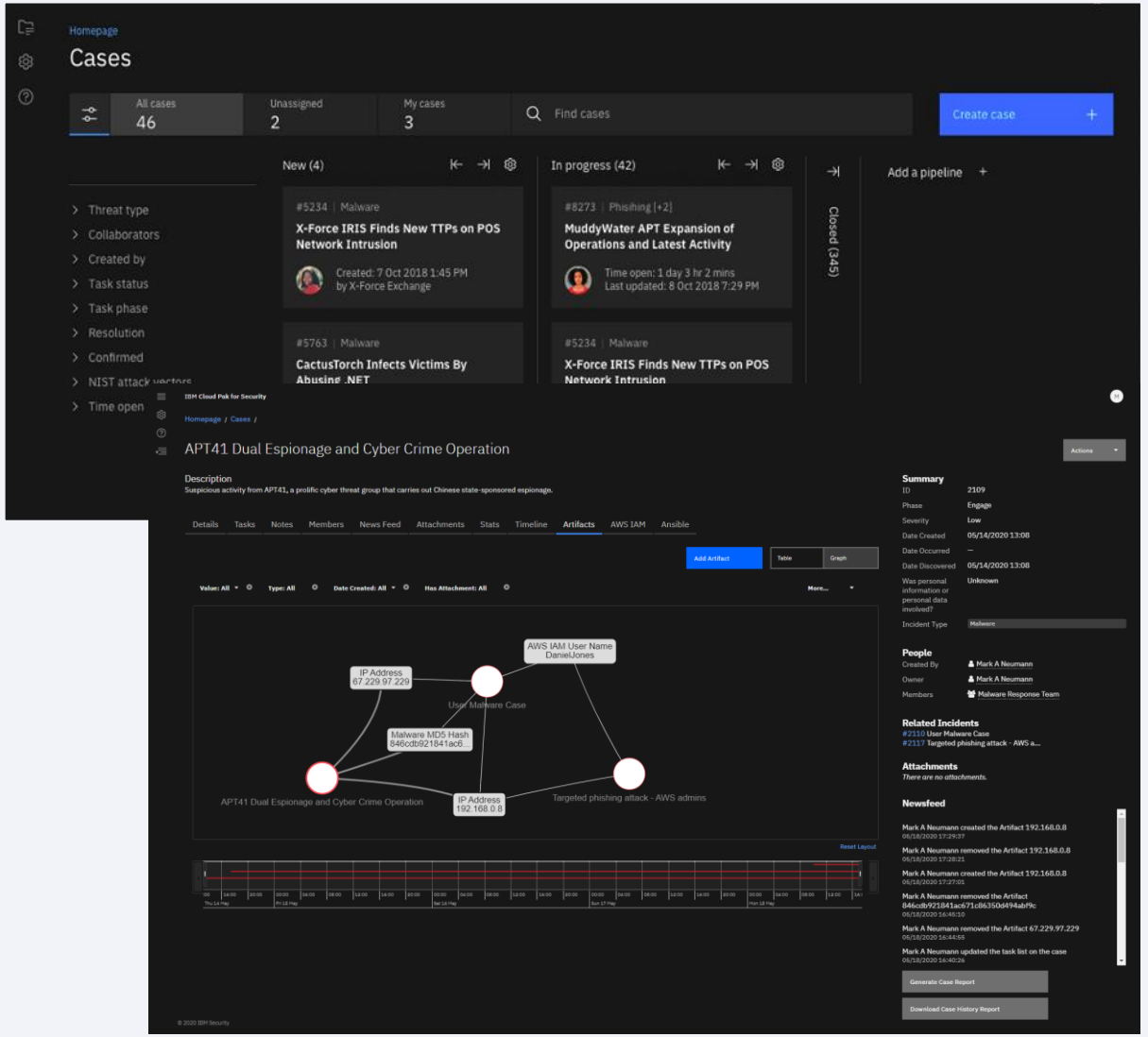
- 사전 구축된 커넥터를 사용하여 클라우드 및 보안 데이터 소스를 한 곳으로 저장, 이동하지 않고도 모든 **중요한 보안 데이터에 대한 가시성 확보**
- 모든 데이터 소스에서 위협, 패턴, IOC 등을 **조사하기위한 단일 쿼리 언어** (STIX)
- 위협 인텔리전스와 자산 및 위험 데이터베이스에 대한 연동을 통해 **데이터와 속성을 자동으로 보강**
- **쿼리가 필요 없는 통계적 통찰력**은 가장 일반적이지 않거나, 가장 일반적이거나, 잠재적인 이상값에 대한 즉각적인 분석을 제공
- 통찰력, 검색 및 결과를 공유하기 위해 SOAR**와** Seamless**하게 통합**
- SDK 또는 IBM 서비스로 **데이터 소스 및 기능을 확장**하여 새 커넥터를 만듦



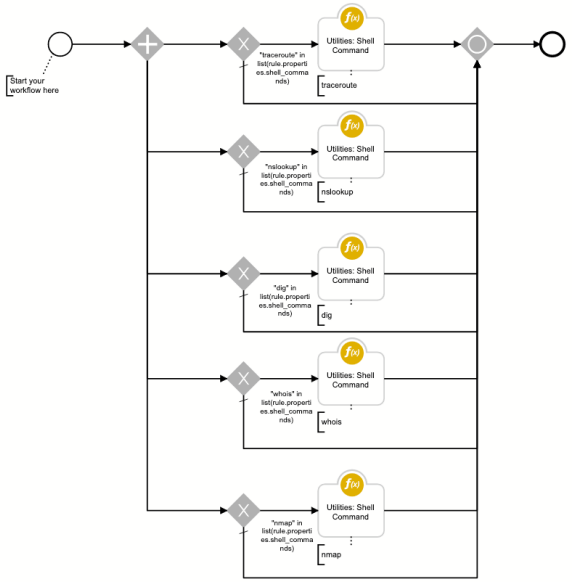
케이스 관리

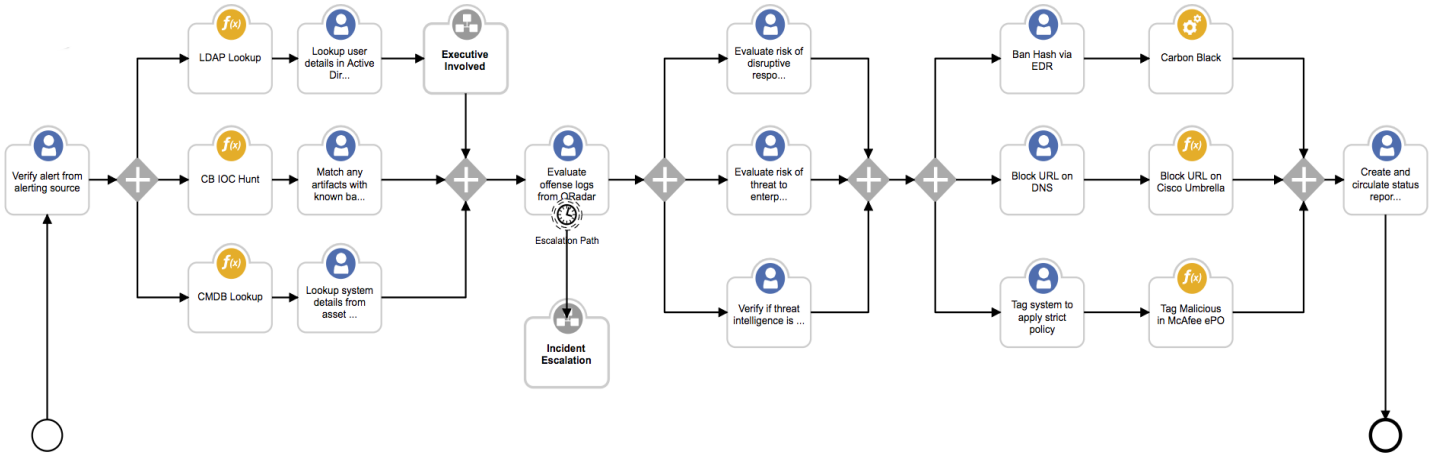
Orchestration, Automation, Response

- 사고 대응 프로세스를 자동화하여 복잡한 사이버 위협에 **대응하고 해결하는 시간을 단축**
- IOC 강화와 같은 수동 및 반복 작업을 **간소화 및 자동화**하고 공격자가 사용하는 레버리지 포인트를 쉽게 식별하고 시간 경과에 따라 IOC를 추적하고 속성을 분류
- 린 제조 기술을 활용한 강력한 케이스 관리 및 작업을 통해 **조사 및 대응 조치를 일관되게 안내**하고 실행하며 시각적 프로세스 기술을 활용
- 160 개 이상의 타사 통합에 대한 간단한 포인트 앤 클릭 배포를 통해 **조직 전체에서 조사 추진**
- 시각적 워크 플로우 편집기를 통해 **동적 플레이 북을 사용자 정의하고 확장**
- 프라이버시 애드온으로 **컴플라이언스 요구 사항 지원**



워크플로우를 활용한 보안이슈 대응 업무처리 자동화(SOA)





Functions

- 빠른 체인 방식의 **양방향 연계**
- IBM Security App Exchange를 통해 다운로드 하여 즉시 **사용 가능한 기능 통합기능 제공**

Dynamic Business Logic

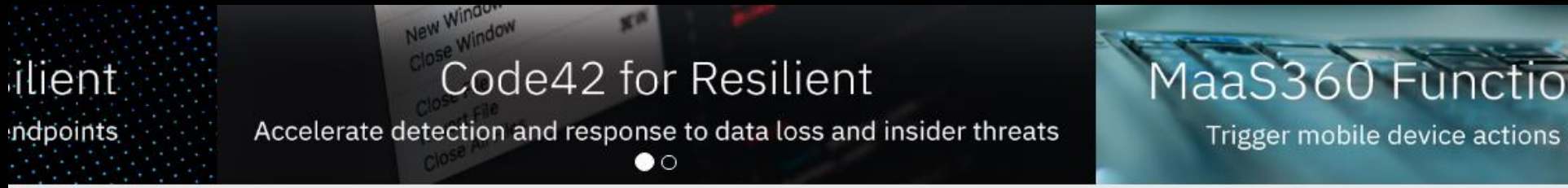
- 이해 관계자 참여, 즉 **승인 프로세스 통합**
- **재사용 가능**한 하위 프로세스

Human Decision Logic

- 주요 진행 사항에 대한 업무 조율
- 분석가가 정확하고 **신속한 의사 결정**을 내릴 수 있도록 안내 및 권한 부여

IBM Security App Exchange를 통해 SOAR 플랫폼 확장

- 165개의 검증 및 현재까지 게시 된 커뮤니티 앱
- Red Hat ™ Ansible ™을 통해 보안 자동화(700여개 앱)를 DevOps로 확장
- Resilient 플레이 북에 쉽게 추가되는 280개 이상의 사전 구성된 워크 플로우
- 주요 보안 공급 업체에서 다루는 강화, 봉쇄 및 수정 사용 사례



IBM and Business Partner Applications (71)

Items Per Page 8 Sort By Newest

NEW
Resilient
Amazon AWS IAM Integration for Resilient
The Amazon AWS IAM integration with the Resilient platform for querying and updating of AWS accounts.
By IBM Resilient
IBM Validated

UPDATED
Resilient
Utility Functions for Resilient
Useful workflow functions for common automation and integration activities in the Resilient platform
★★★★★ (3)
By IBM Resilient
IBM Validated

EARLY ACCESS
Resilient
Machine Learning for Resilient
The Resilient Machine Learning function enables users to predict incident field values based on historical data.
By IBM Resilient
Early Access

UPDATED
Resilient
Microsoft Security Graph Integration for Resilient
Integrates Resilient incidents and Microsoft Security Graph alerts.
By IBM Resilient
IBM Validated

EARLY ACCESS
Resilient
Proofpoint TRAP Integration for IBM

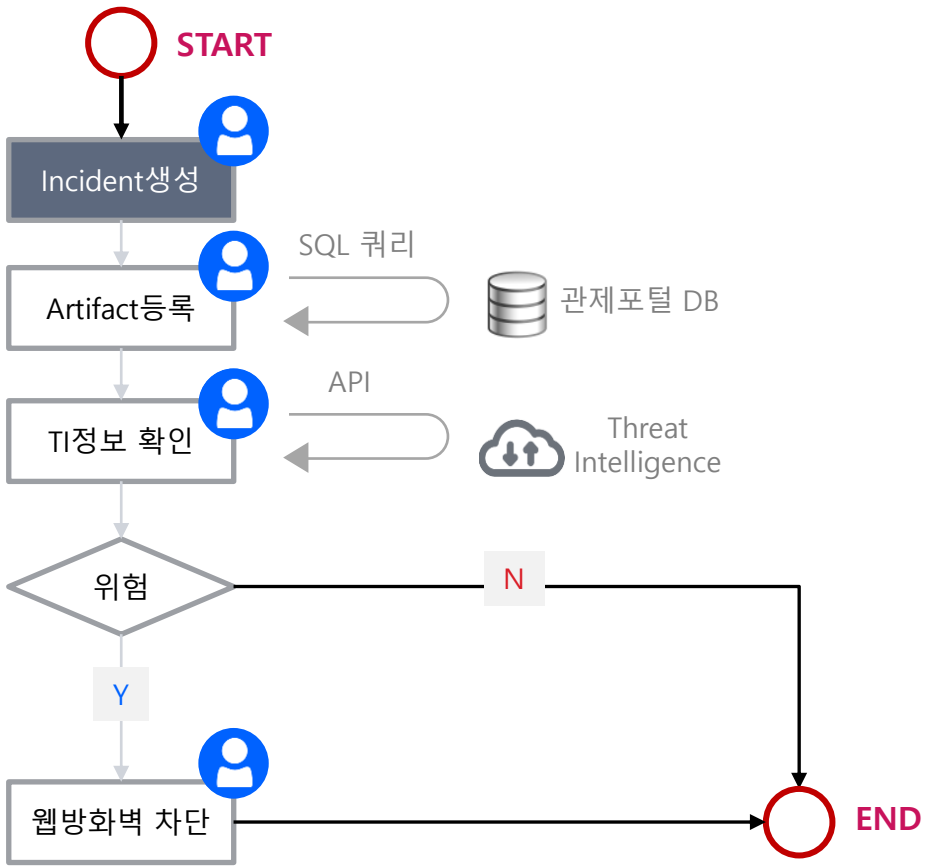
UPDATED
Resilient
Slack Integration for Resilient

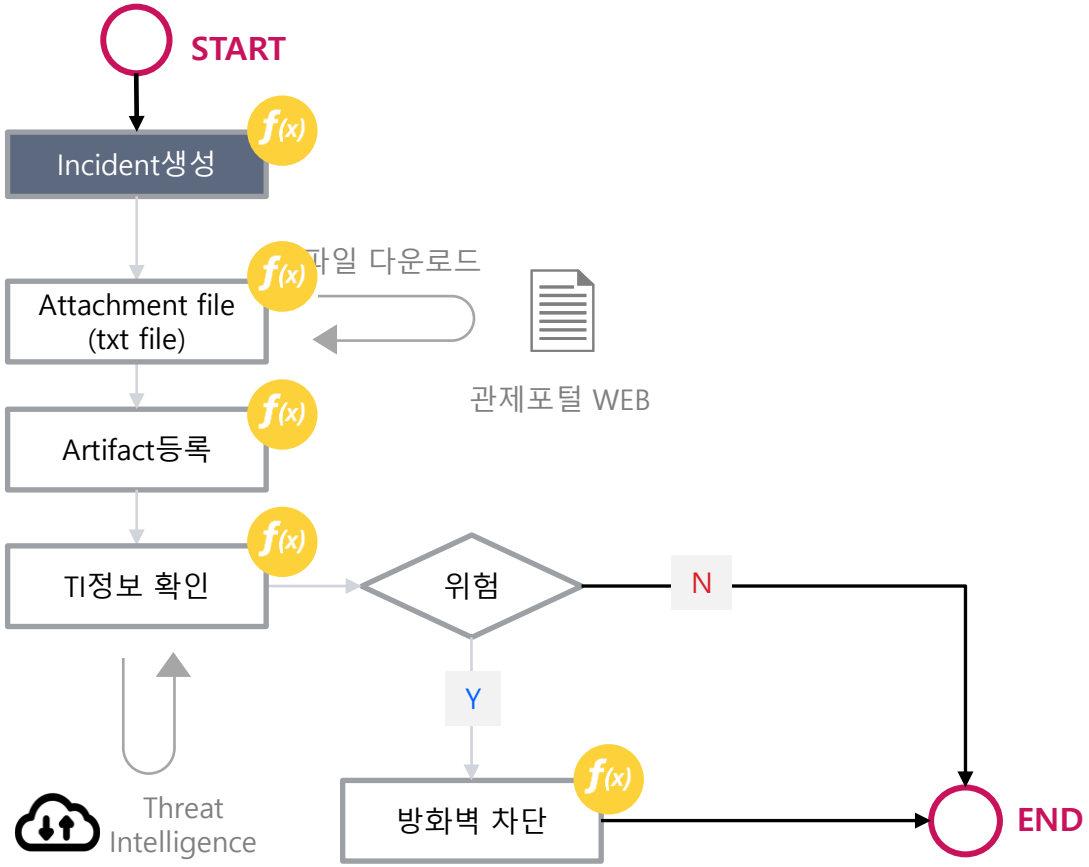
Resilient
QRadar Advisor with Watson Functions for

QRadar
IBM Resilient QRadar Integration

고객 Use Case 1

Scenario 01 (웹공격차단) & Scenario 02 (간단 악성코드 감염 대응)

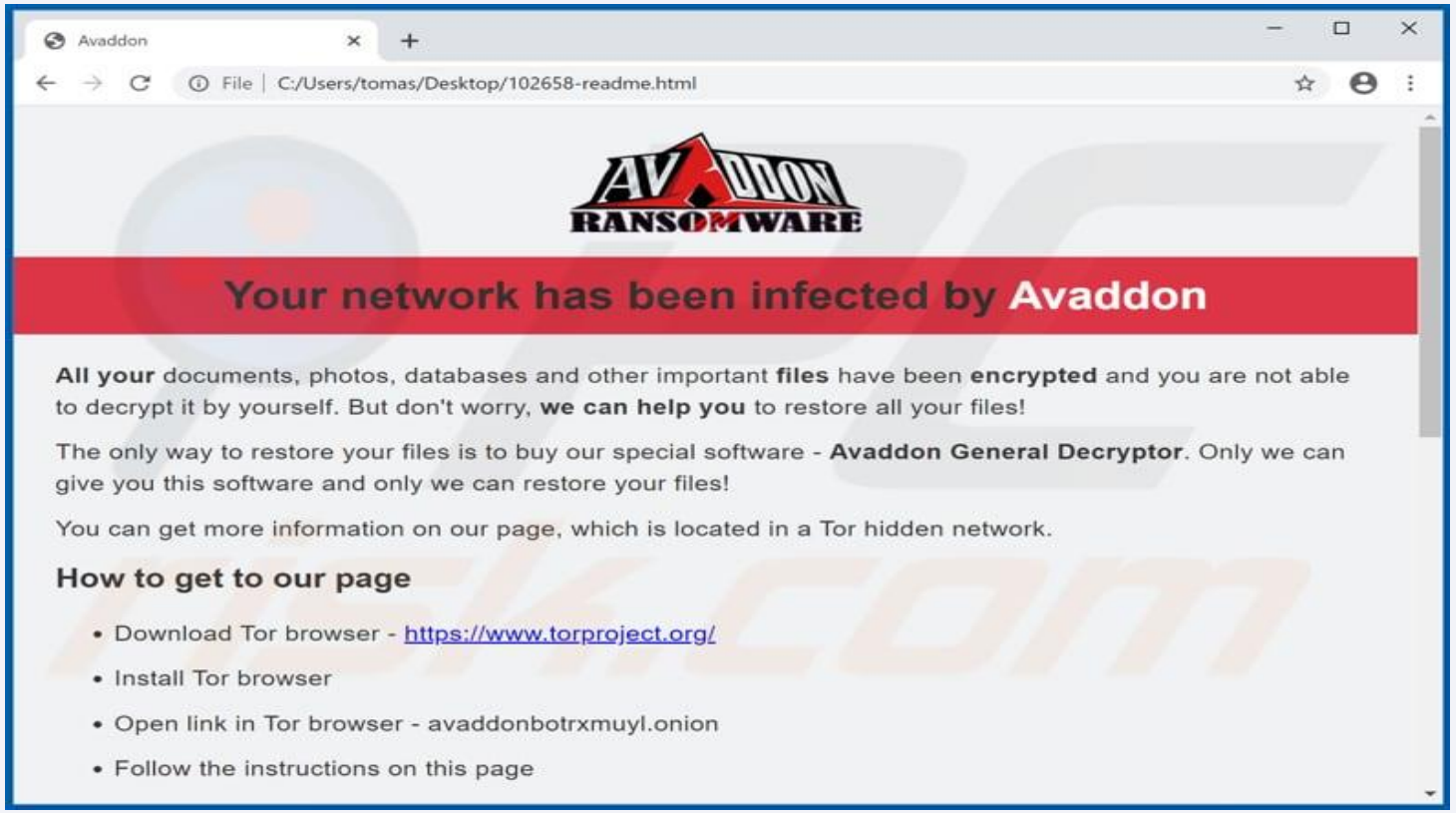




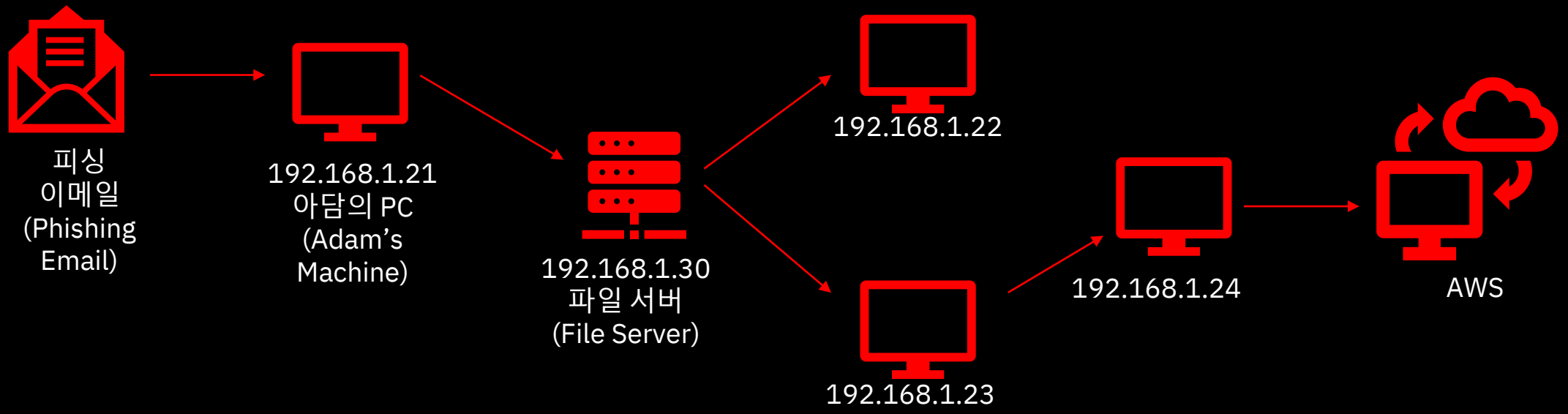
랜섬웨어 공격 탐지대응 시나리오

랜섬웨어 공격(Ransomware Attack)

랜섬웨어 공격 → 피싱 메일 → 직원 확인 → 해당 PC 감염 → 감염 확산 → 네트워크 감염

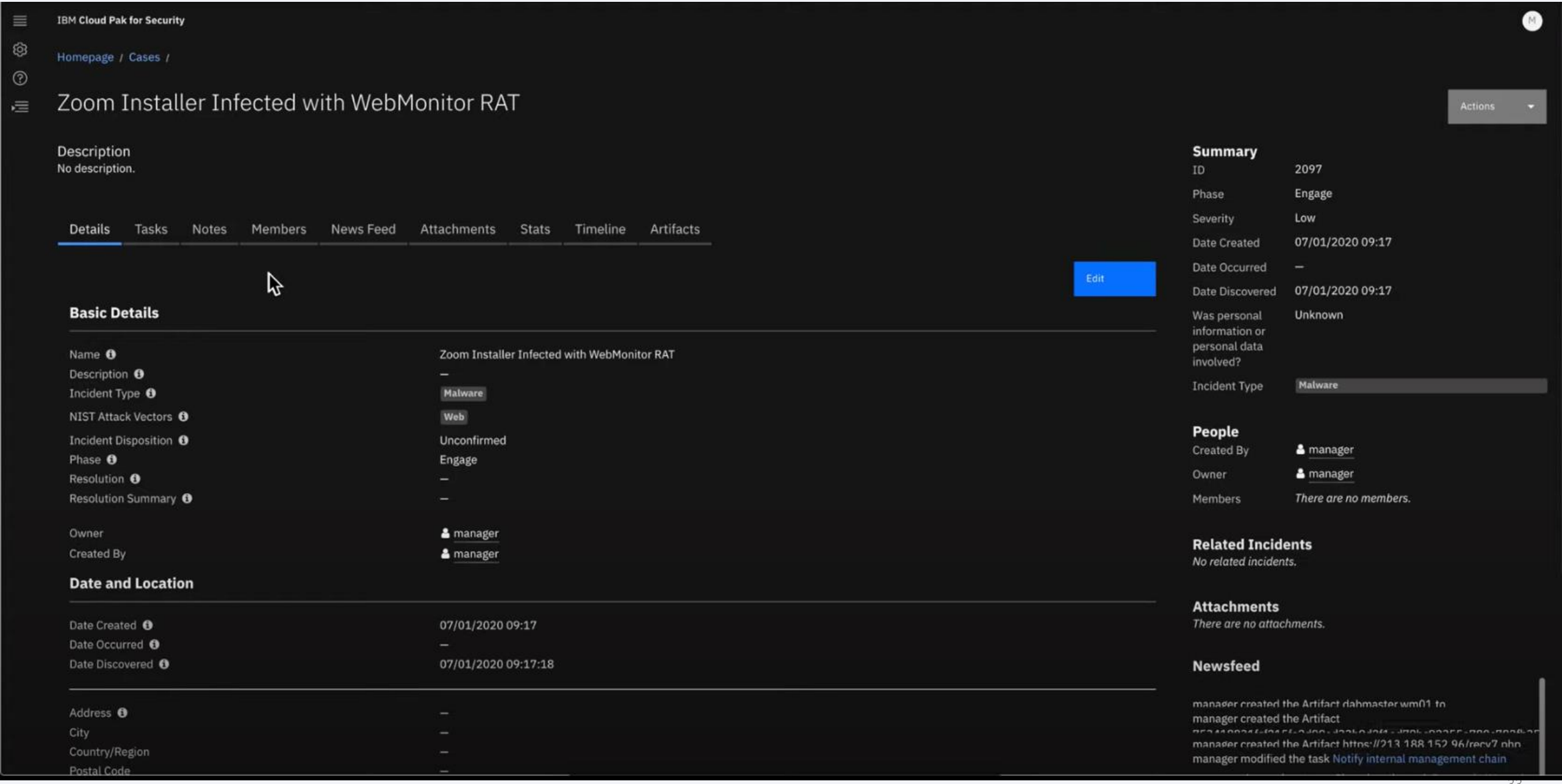


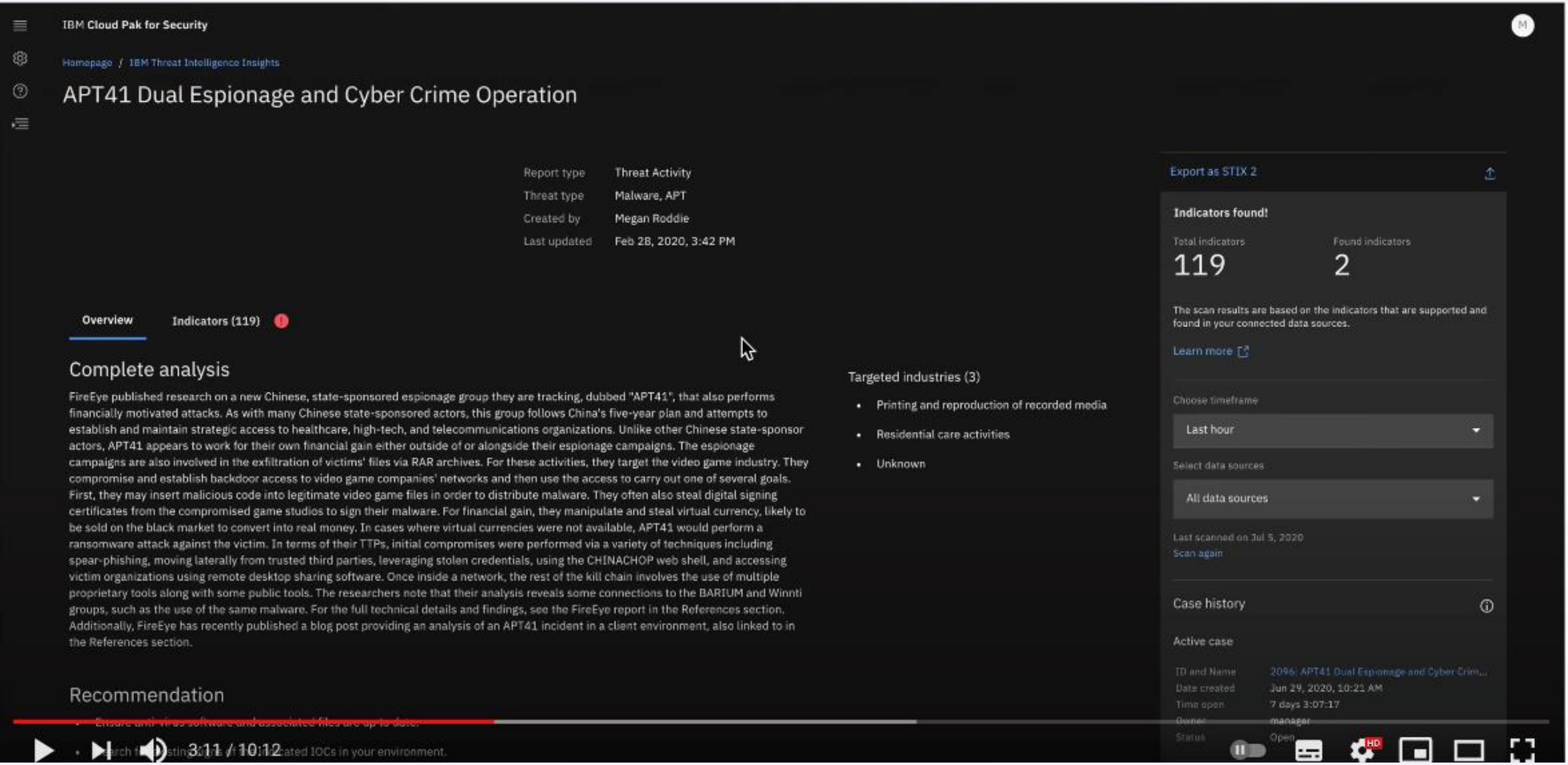
위협 헌팅 (Threat Hunting) 결과

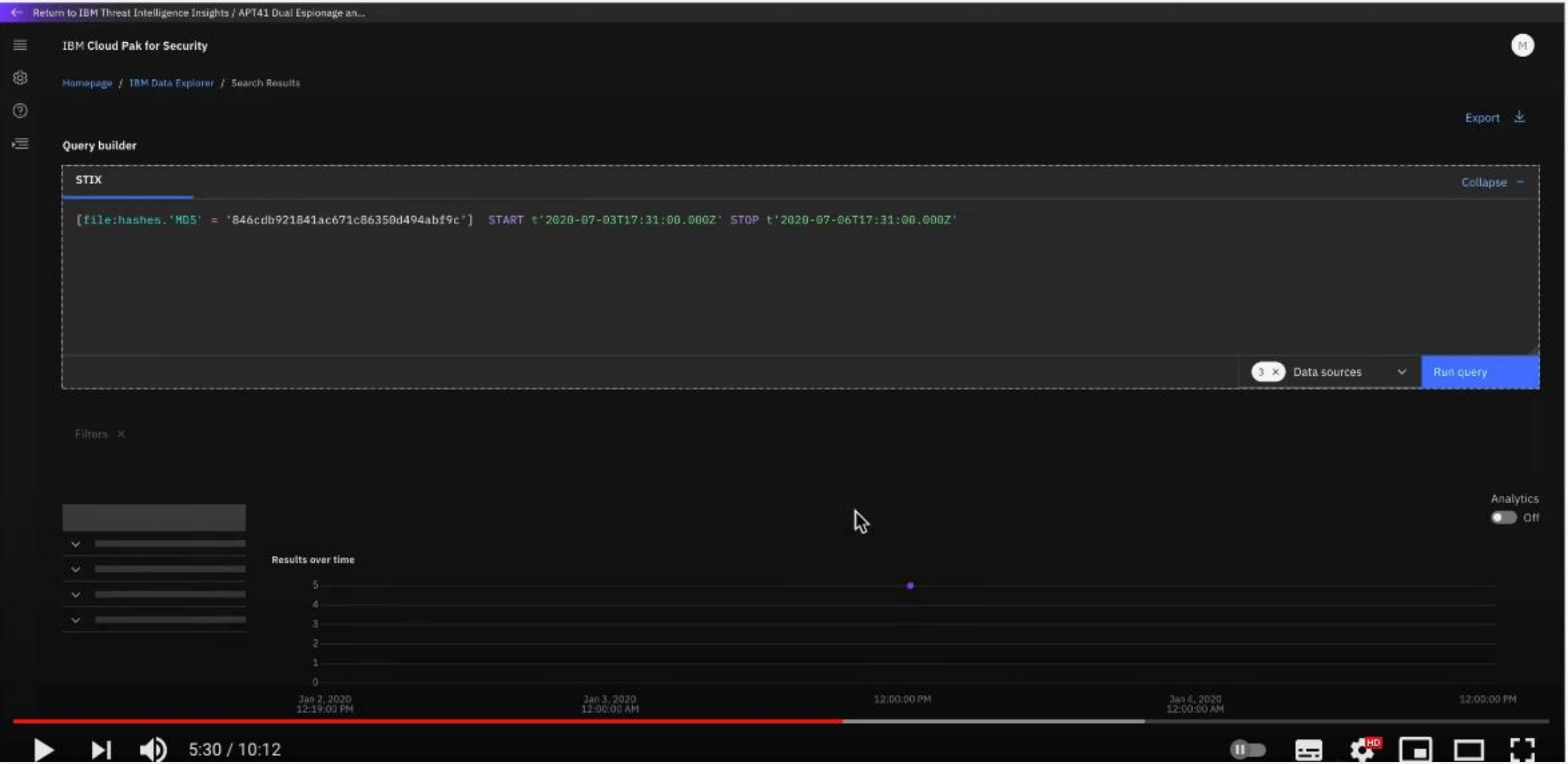


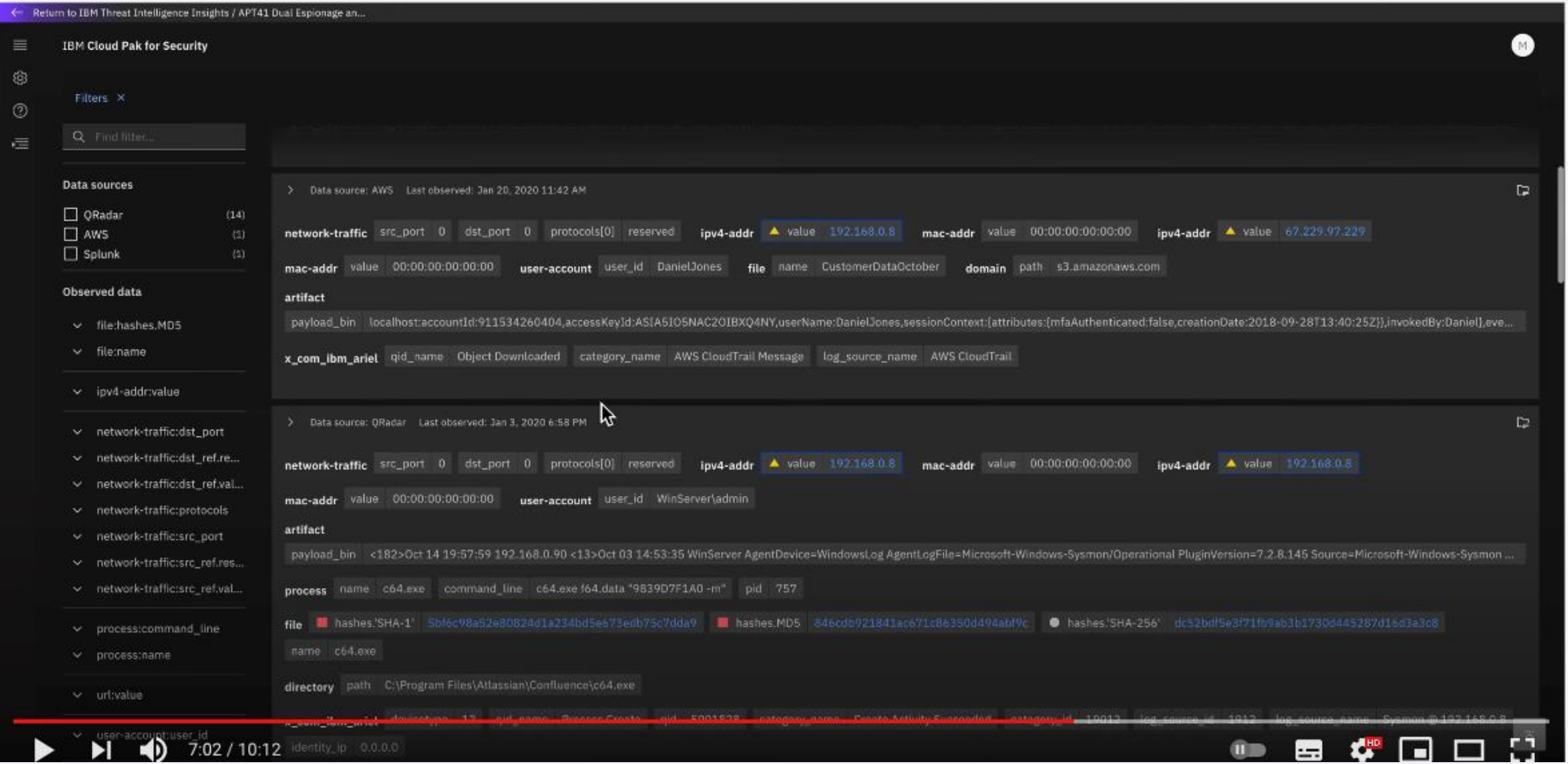
위협 조사와 대응의 복잡성

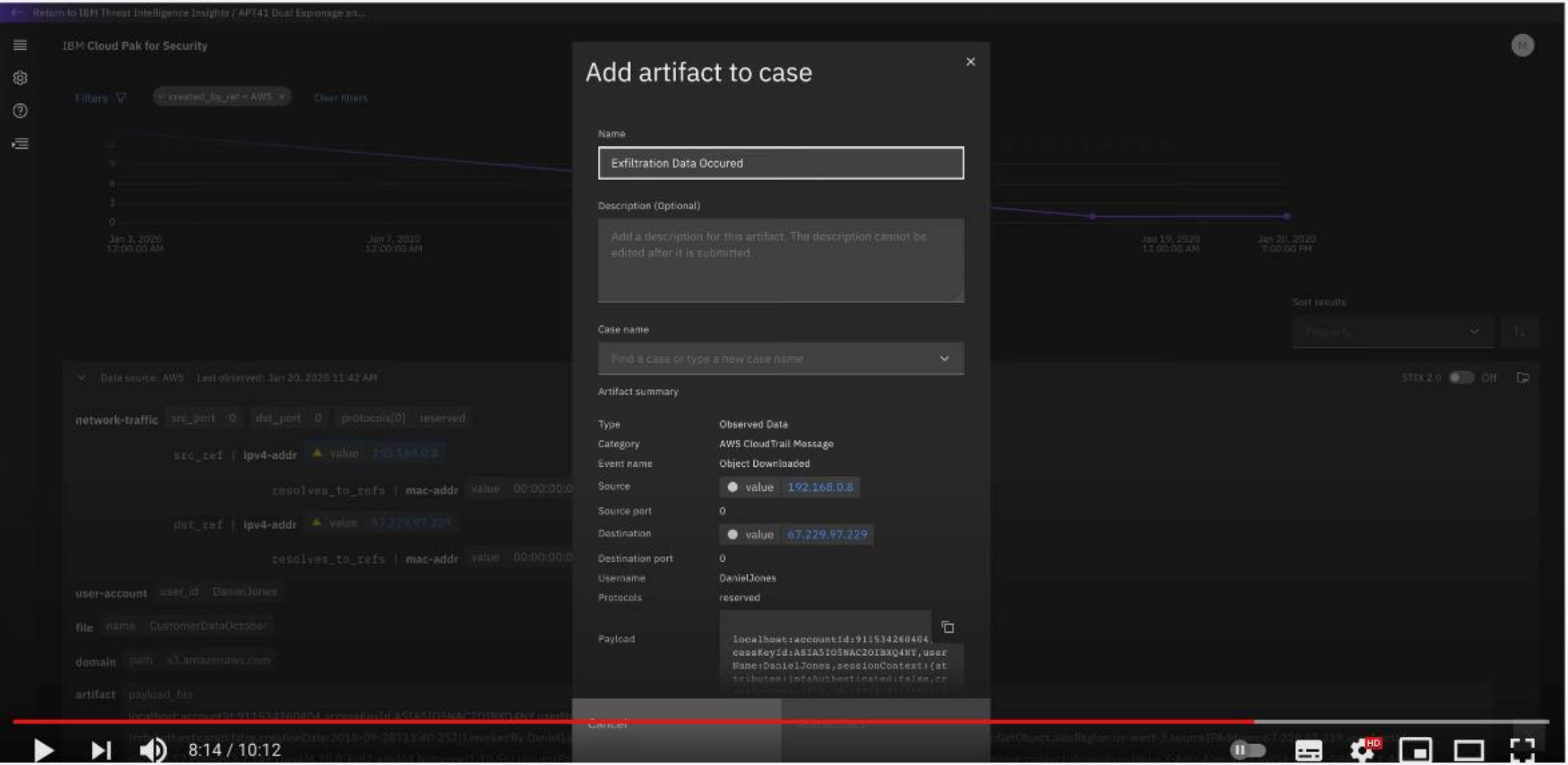
1. 로그소스에서 IoC 기반으로 사례를 조사하고, 첫번째 감염자를 찾습니다.**(2일)**
2. 위협정보로부터 모든 IOC를 스캔합니다. **(IoC 당 1분)**
3. QRadar 참조 셋에 모든 IOC를 추가합니다. **(IoC 당 1분)**
4. 모든 사용자의 메일박스에서 악성 이메일을 검색하여 대상 사용자를 찾습니다. **(1주일)**
5. 모든 대상 사용자의 모든 악성 이메일을 제거합니다. **(1주일)**
6. 모든 사용자의 노트북/ PC/서버에서 이 이메일과 함께 제공된 모든 악성 파일을 찾습니다.**(1주일)**
7. 감염된 모든 노트북 / PC / 서버에서 악성 파일을 제거합니다. **(1주일)**
8. 다른 서버를 감염시킬 수 있는 모든 감염된 서버를 격리합니다. **(24시간)**

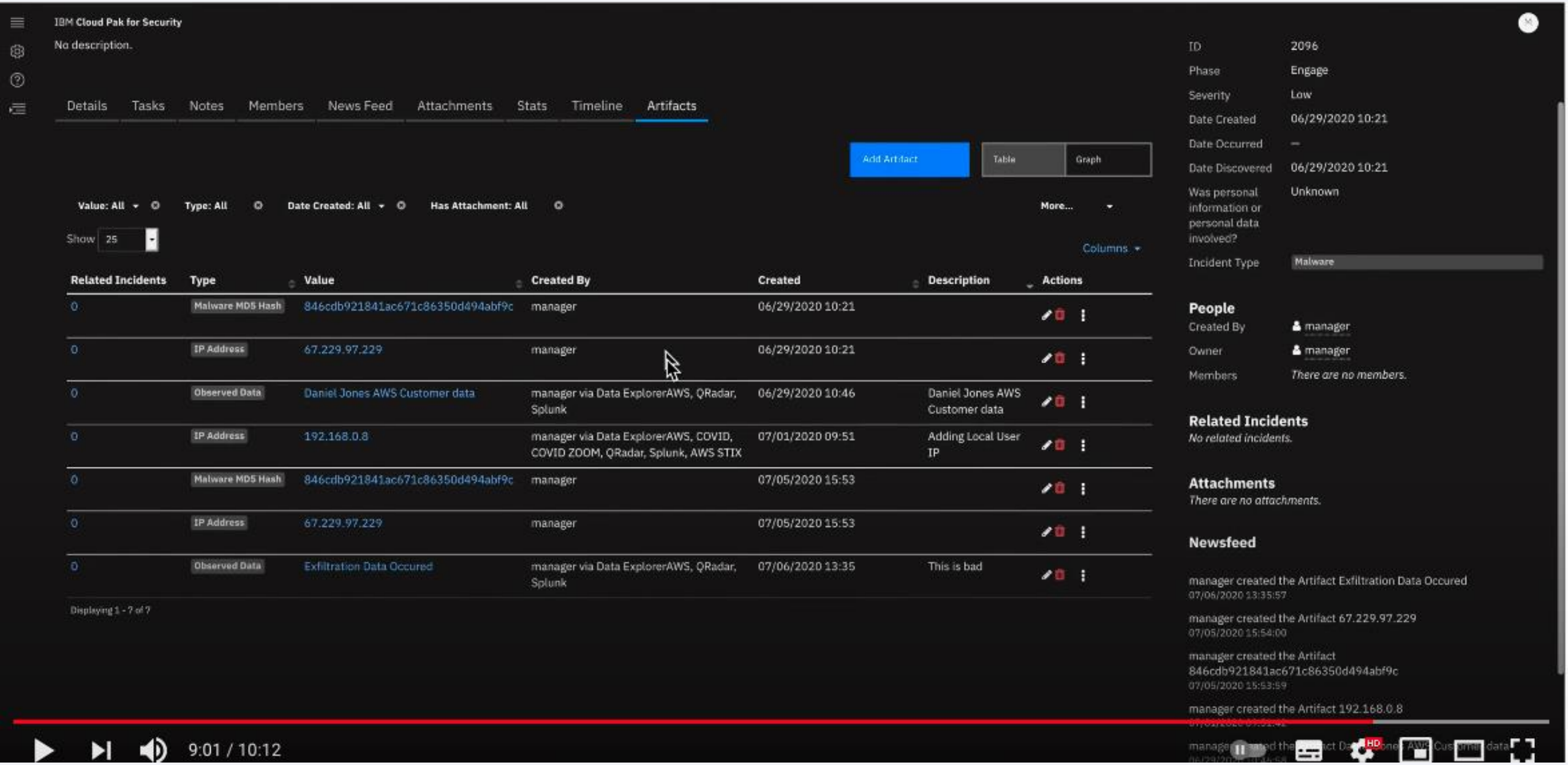

IBM Cloud Pak for Security
Homepage / Cases /
Zoom Installer Infected with WebMonitor RAT
Actions
Description
No description.
Details
Tasks
Notes
Members
News Feed
Attachments
Stats
Timeline
Artifacts
Edit
Basic Details
Name
Zoom Installer Infected with WebMonitor RAT
Description
–
Incident Type
Malware
NIST Attack Vectors
Web
Incident Disposition
Unconfirmed
Phase
Engage
Resolution
–
Resolution Summary
–
Owner
manager
Created By
manager
Date and Location
Date Created
07/01/2020 09:17
Date Occurred
–
Date Discovered
07/01/2020 09:17:18
Address
–
City
–
Country/Region
–
Postal Code
–
Summary
ID
2097
Phase
Engage
Severity
Low
Date Created
07/01/2020 09:17
Date Occurred
–
Date Discovered
07/01/2020 09:17
Was personal information or personal data involved?
Unknown
Incident Type
Malware
People
Created By
manager
Owner
manager
Members
There are no members.
Related Incidents
No related incidents.
Attachments
There are no attachments.
Newsfeed
manager created the Artifact dabmaster.wm01.to
manager created the Artifact
manager created the Artifact https://213.188.152.96/recv7.php
manager modified the task Notify internal management chain

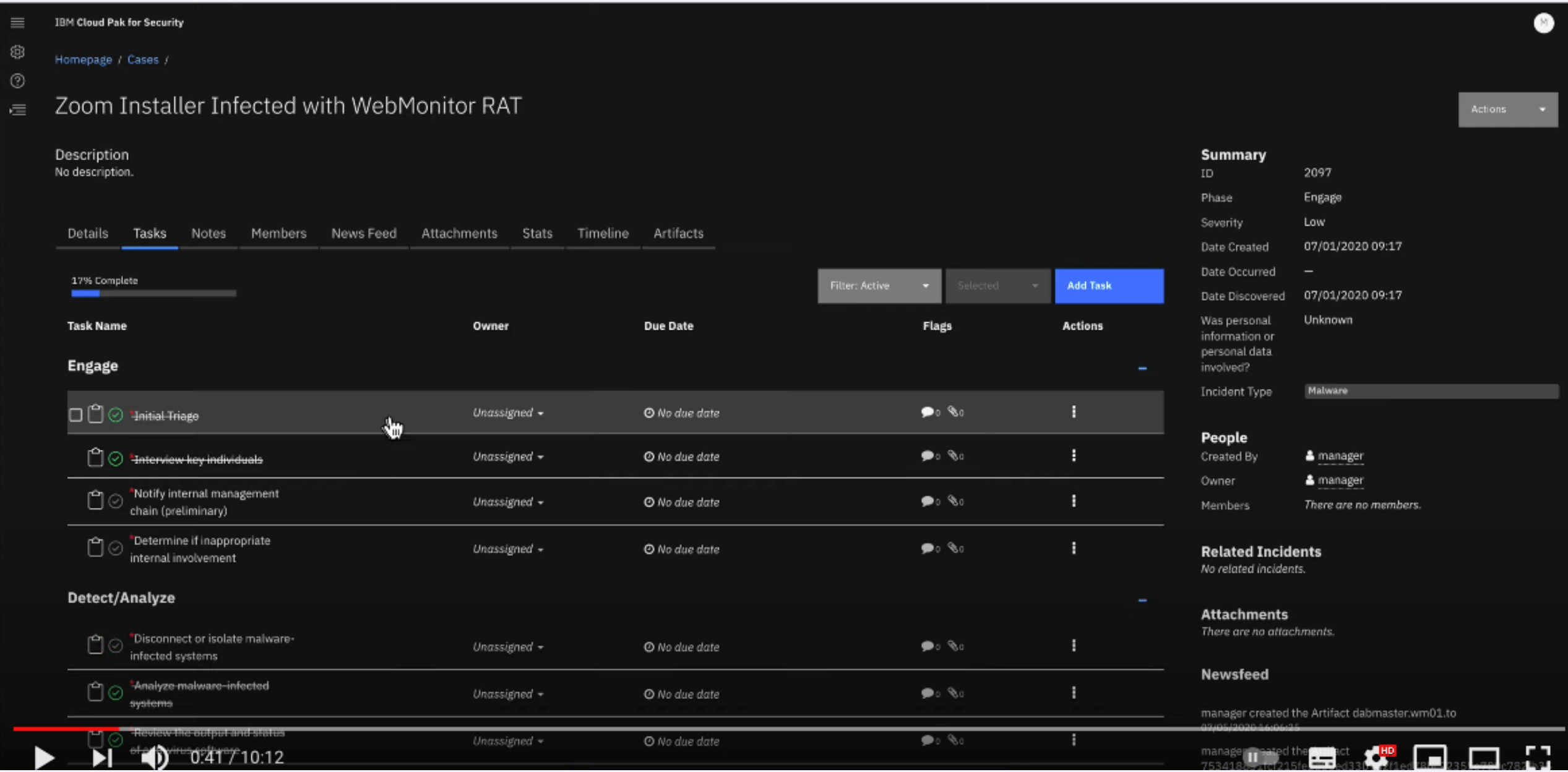

IBM Cloud Pak for Security
Homepage / IBM Threat Intelligence Insights
APT41 Dual Espionage and Cyber Crime Operation
Report type Threat Activity
Threat type Malware, APT
Created by Megan Roddie
Last updated Feb 28, 2020, 3:42 PM
Overview
Indicators (119)
Complete analysis
FireEye published research on a new Chinese, state-sponsored espionage group they are tracking, dubbed "APT41", that also performs financially motivated attacks. As with many Chinese state-sponsored actors, this group follows China's five-year plan and attempts to establish and maintain strategic access to healthcare, high-tech, and telecommunications organizations. Unlike other Chinese state-sponsor actors, APT41 appears to work for their own financial gain either outside of or alongside their espionage campaigns. The espionage campaigns are also involved in the exfiltration of victims' files via RAR archives. For these activities, they target the video game industry. They compromise and establish backdoor access to video game companies' networks and then use the access to carry out one of several goals. First, they may insert malicious code into legitimate video game files in order to distribute malware. They often also steal digital signing certificates from the compromised game studios to sign their malware. For financial gain, they manipulate and steal virtual currency, likely to be sold on the black market to convert into real money. In cases where virtual currencies were not available, APT41 would perform a ransomware attack against the victim. In terms of their TTPs, initial compromises were performed via a variety of techniques including spear-phishing, moving laterally from trusted third parties, leveraging stolen credentials, using the CHINACHOP web shell, and accessing victim organizations using remote desktop sharing software. Once inside a network, the rest of the kill chain involves the use of multiple proprietary tools along with some public tools. The researchers note that their analysis reveals some connections to the BARIUM and Winnti groups, such as the use of the same malware. For the full technical details and findings, see the FireEye report in the References section. Additionally, FireEye has recently published a blog post providing an analysis of an APT41 incident in a client environment, also linked to in the References section.
Recommendation
Targeted industries (3)
Printing and reproduction of recorded media
Residential care activities
Unknown
Export as STIX 2
Indicators found!
Total indicators 119
Found indicators 2
The scan results are based on the indicators that are supported and found in your connected data sources.
Learn more
Choose timeframe
Last hour
Select data sources
All data sources
Last scanned on Jul 5, 2020
Scan again
Case history
Active case
ID and Name 2096: APT41 Dual Espionage and Cyber Crim...
Date created Jun 29, 2020, 10:21 AM
Time open 7 days 3:07:17
Owner manager
Status Open
3:11 / 10:12
HD


Return to IBM Threat Intelligence Insights / APT41 Dual Espionage an...
IBM Cloud Pak for Security
Homepage / IBM Data Explorer / Search Results
Export
Query builder
STIX
Collapse
[file:hashes.'MD5' = '846cdb921841ac671c86350d494abf9c'] START t'2020-07-03T17:31:00.000Z' STOP t'2020-07-06T17:31:00.000Z'
3
Data sources
Run query
Filters
Analytics
Off
Results over time
5
4
3
2
1
0
Jan 2, 2020
12:19:00 PM
Jan 3, 2020
12:00:00 AM
12:00:00 PM
Jan 4, 2020
12:00:00 AM
12:00:00 PM
5:30 / 10:12
HD

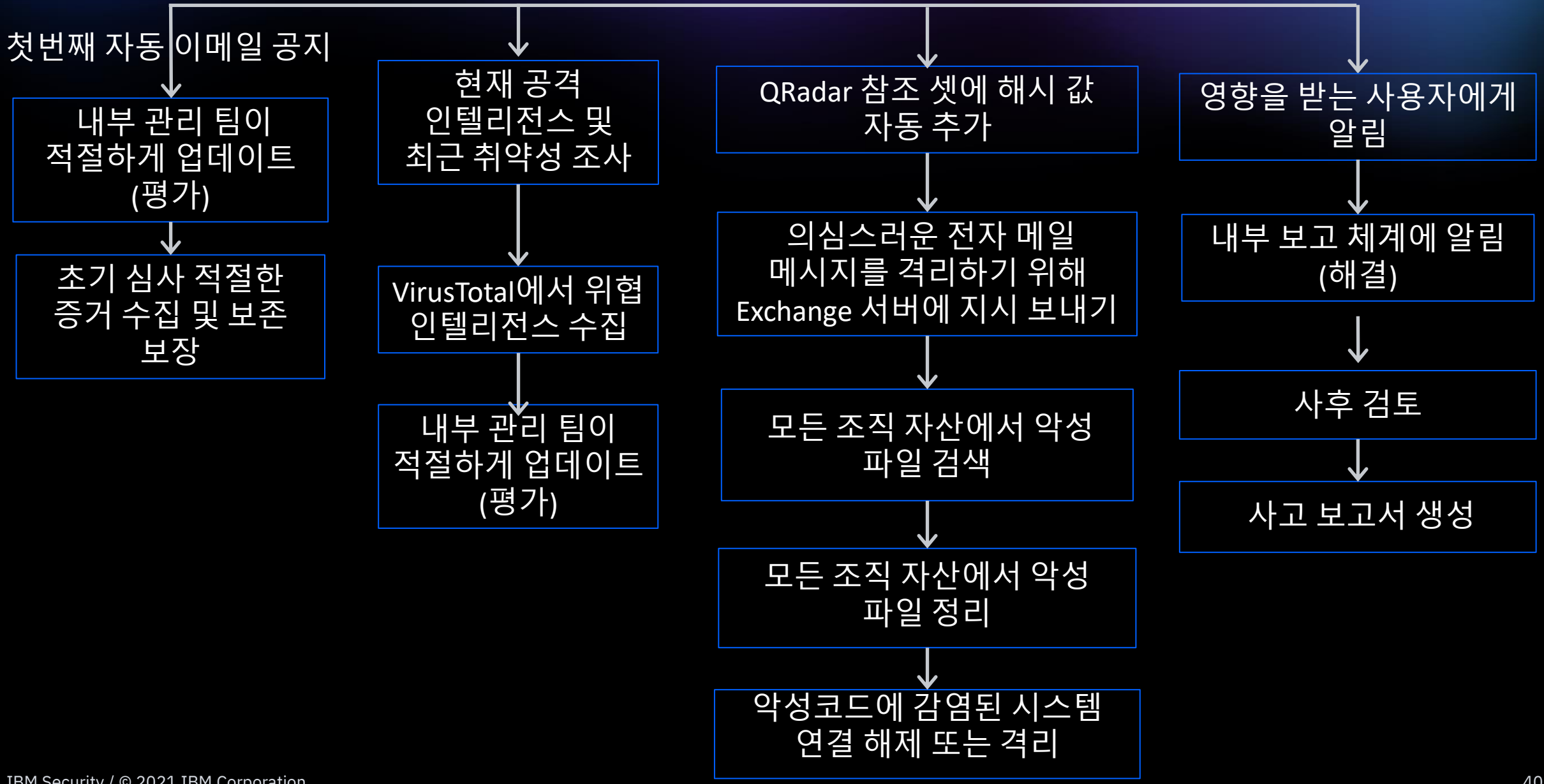

Return to IBM Threat Intelligence Insights / APT41 Dual Espionage an...
IBM Cloud Pak for Security
Filters
Find filter...
Data sources
QRadar (14)
AWS (1)
Splunk (1)
Observed data
file:hashes.MD5
file:name
ipv4-addr:value
network-traffic:dst_port
network-traffic:dst_ref.re...
network-traffic:dst_ref.val...
network-traffic:protocols
network-traffic:src_port
network-traffic:src_ref.res...
network-traffic:src_ref.val...
process:command_line
process:name
url:value
user-account:user_id
Data source: AWS Last observed: Jan 20, 2020 11:42 AM
network-traffic src_port 0 dst_port 0 protocols[0] reserved
ipv4-addr value 192.168.0.8
mac-addr value 00:00:00:00:00:00
ipv4-addr value 67.229.97.229
mac-addr value 00:00:00:00:00:00
user-account user_id DanielJones
file name CustomerDataOctober
domain path s3.amazonaws.com
artifact
payload_bin localhost:accountId:911534260404,accessKeyId:ASIA5IO5NAC2OIBXQ4NY,userName:DanielJones,sessionContext:{attributes:{mfaAuthenticated:false,creationDate:2018-09-28T13:40:25Z}},invokedBy:Daniel},eve...
x_com_ibm_ariel qid_name Object Downloaded category_name AWS CloudTrail Message log_source_name AWS CloudTrail
Data source: QRadar Last observed: Jan 3, 2020 6:58 PM
network-traffic src_port 0 dst_port 0 protocols[0] reserved
ipv4-addr value 192.168.0.8
mac-addr value 00:00:00:00:00:00
ipv4-addr value 192.168.0.8
mac-addr value 00:00:00:00:00:00
user-account user_id WinServer\admin
artifact
payload_bin <182>Oct 14 19:57:59 192.168.0.90 <13>Oct 03 14:53:35 WinServer AgentDevice=WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational PluginVersion=7.2.8.145 Source=Microsoft-Windows-Sysmon ...
process name c64.exe command_line c64.exe f64.data "9839D7F1A0 -m" pid 757
file hashes.'SHA-1' 5bf6c98a52e80824d1a234bd5e573edb75c7dda9 hashes.MD5 846cdb921841ac671c86350d494abf9c hashes.'SHA-256' dc52bdf5e3f71fb9ab3b1730d445287d16d3a3c8
name c64.exe
directory path C:\Program Files\Atlassian\Confluence\c64.exe
identity_ip 0.0.0.0
7:02 / 10:12
HD


Return to IBM Threat Intelligence Insights / APT41 Dual Espionage an...
IBM Cloud Pak for Security
Add artifact to case
Name
Exfiltration Data Occured
Description (Optional)
Add a description for this artifact. The description cannot be edited after it is submitted.
Case name
Find a case or type a new case name
Artifact summary
Type
Observed Data
Category
AWS CloudTrail Message
Event name
Object Downloaded
Source
value 192.168.0.8
Source port
0
Destination
value 67.229.97.229
Destination port
0
Username
DanielJones
Protocols
reserved
Payload
Cancel
8:14 / 10:12

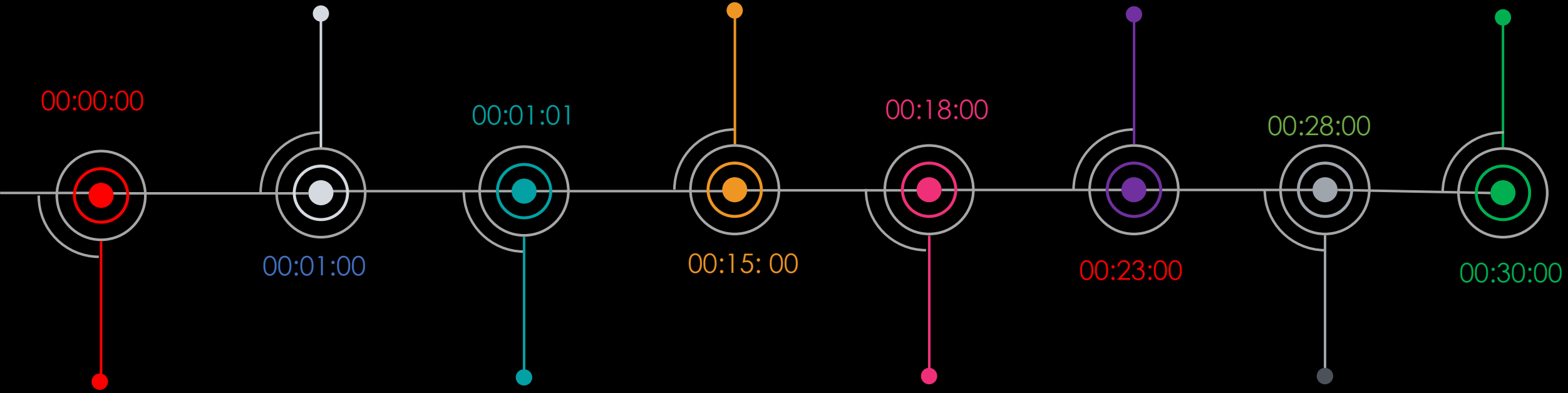

IBM Cloud Pak for Security
No description.
Details
Tasks
Notes
Members
News Feed
Attachments
Stats
Timeline
Artifacts
Add Artifact
Table
Graph
Value: All
Type: All
Date Created: All
Has Attachment: All
More...
Show 25
Columns
Related Incidents
Type
Value
Created By
Created
Description
Actions
0
Malware MD5 Hash
846cdb921841ac671c86350d494abf9c
manager
06/29/2020 10:21
0
IP Address
67.229.97.229
manager
06/29/2020 10:21
0
Observed Data
Daniel Jones AWS Customer data
manager via Data ExplorerAWS, QRadar, Splunk
06/29/2020 10:46
Daniel Jones AWS Customer data
0
IP Address
192.168.0.8
manager via Data ExplorerAWS, COVID, COVID ZOOM, QRadar, Splunk, AWS STIX
07/01/2020 09:51
Adding Local User IP
0
Malware MD5 Hash
846cdb921841ac671c86350d494abf9c
manager
07/05/2020 15:53
0
IP Address
67.229.97.229
manager
07/05/2020 15:53
0
Observed Data
Exfiltration Data Occured
manager via Data ExplorerAWS, QRadar, Splunk
07/06/2020 13:35
This is bad
Displaying 1 - 7 of 7
ID 2096
Phase Engage
Severity Low
Date Created 06/29/2020 10:21
Date Occurred —
Date Discovered 06/29/2020 10:21
Was personal information or personal data involved? Unknown
Incident Type Malware
People
Created By manager
Owner manager
Members There are no members.
Related Incidents
No related incidents.
Attachments
There are no attachments.
Newsfeed
manager created the Artifact Exfiltration Data Occured
07/06/2020 13:35:57
manager created the Artifact 67.229.97.229
07/05/2020 15:54:00
manager created the Artifact 846cdb921841ac671c86350d494abf9c
07/05/2020 15:53:59
manager created the Artifact 192.168.0.8
9:01 / 10:12
HD


IBM Cloud Pak for Security
Homepage / Cases /
Zoom Installer Infected with WebMonitor RAT
Actions
Description
No description.
Details
Tasks
Notes
Members
News Feed
Attachments
Stats
Timeline
Artifacts
17% Complete
Filter: Active
Selected
Add Task
Task Name
Owner
Due Date
Flags
Actions
Engage
*Initial Triage
Unassigned
No due date
*Interview key individuals
*Notify internal management chain (preliminary)
*Determine if inappropriate internal involvement
Detect/Analyze
*Disconnect or isolate malware-infected systems
*Analyze malware-infected systems
Summary
ID
2097
Phase
Engage
Severity
Low
Date Created
07/01/2020 09:17
Date Occurred
—
Date Discovered
07/01/2020 09:17
Was personal information or personal data involved?
Unknown
Incident Type
Malware
People
Created By
manager
Owner
manager
Members
There are no members.
Related Incidents
No related incidents.
Attachments
There are no attachments.
Newsfeed
manager created the Artifact dabmaster.wm01.to
0:41 / 10:12
HD

자동화 및 오케스트레이션 프로세스



사고대응 시간별 내역 (Running Against “TIME”)



분석가는 조직의 보안 상태에 영향을 미칠 수 있는 관련 위협을 발견했습니다.

CP4S Threat intel은 데이터 소스를 스캔하고 조직 네트워크에서 위협 지표의 존재를 찾습니다.

CP4S가 스캔 결과에서 케이스를 생성합니다.

분석가는 침해, 측면 이동(확산), 최초 희생자의 모든 지표들을 찾습니다.

1단계 CP4S SOAR – 아티팩트, 의심스러운 이메일 분석, IOC에 대한 QRadar 조회를 통해 모든 인텔리전스를 수집하고 사례에 추가합니다.

2단계 검역 - CP4S SOAR는 이메일을 수신하는 사용자와 사용자가 다운로드 한 모든 악성 파일을 이메일 상자에서 검색하라는 지침을 보냅니다.

3단계 대응 조치 – 악성코드를 삭제합니다. CP4S SOAR Playbook은 QRadar Notes를 업데이트하고 영향을 받은 사용자에게 해당 내용을 알립니다.

CP4S SOAR는 취해진 자동 대응 조치에 대해 SOC 및 내부 관리자에게 알리고 최종 검토를 수행하기 위해 작업을 남깁니다.

보안사고 응답 시간 98.8 % 감소
대규모 글로벌 제약 회사

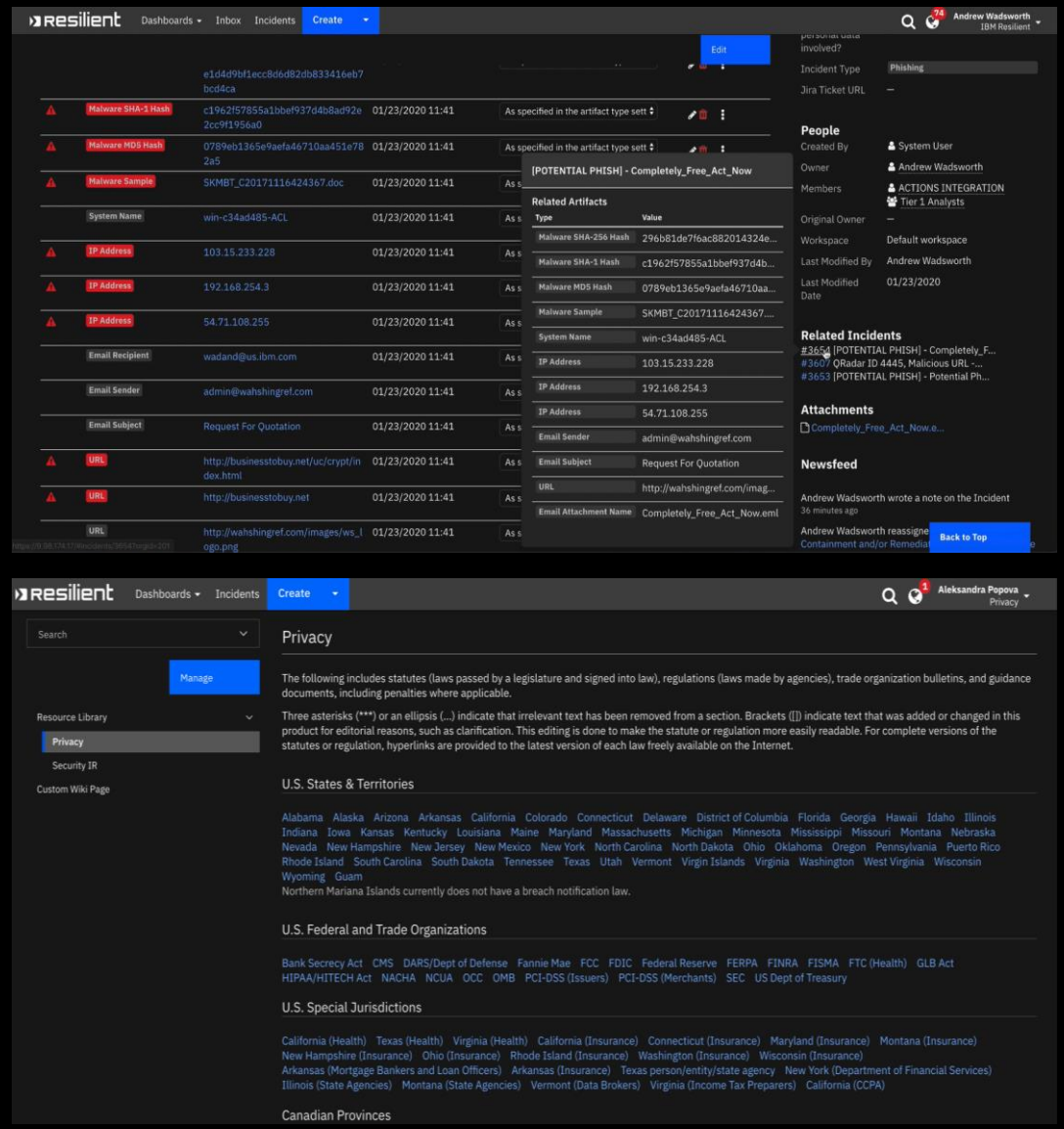
Action	Before Resilient	With Resilient	Example
SIEM, EDR 또는 NGFW를 통해 에스컬레이션	5 분	**10 초**	QRadar에서 의심스러운 엔드 포인트 활동 인시던트 에스컬레이션
영향을 받는 자산 식별 — CMDB / AD / IAM	5–10 분	**10 초**	랩톱에서 CMDB 조회 및 Active Directory 사용자 조회
위협 인텔리전스 피드에 대해 IOC 확인	5 분	**10 초**	인시던트에 알려진 악성코드 변형에 연결된 해시가 포함
과거 사건과 데이터의 상관 관계	10–20 분	**즉시**	지난 달에 발생한 다른 2건의 사건에서 동일한 해시 및 아웃바운드 트래픽이 더 큰 캠페인을 가리킴
수동 조사 — 엔드포인트, 외부 네트워크, VPN 로그, DNS 레코드, 네트워크 인프라 및 엔드 포인트 포렌식 작업 가져오기	30–55 분	**30 초**	카본 블랙을 사용하여 랩톱에서 프로세스 트리를 가져오고 웹 프록시에서 DNS를 가져와 C2 서버 확인
인시던트 추적 – 인시던트 라이프 사이클 전체에 걸쳐 자세한 메모와 작업을 유지	N/A	**즉시**	Resilient는 사고 대응의 일부로 완료된 작업 및 자동업무를 자동으로 추적하며 모든 분석가의 노트는 플랫폼에 저장
감사 추적 및 로깅 유지 – 법정에서 허용되는 사고 대응 감사 추적을 유지	N/A	**즉시**	Resilient에서 수행 된 모든 작업은 기록되며 수정할 수 없으며, 법원에서 소환장을 받으면 경영진은 로그만 출력 가능
경영진에게 사고 상태를 보고하고 가시성을 제공	N/A	**즉시**	경영진 대시 보드 및 외부 알림은 SOC의 추가 노력없이 경영진에게 실시간 통찰력을 제공
Total	**85 분**	**1 분**	

보안 사고 발생 시 자신 있게 대응

지식을 활용하여 보안 팀의 자율권 확보 및 역량 강화

특징 및 기능 :

- 인시던트 플레이북을 통해 산업 및 조직 관련 지식 수집 및 디지털화
- 기존 직원이 공격에 대응할 수 있도록 대응 프로세스 조정
- 글로벌 위반 보고 요구사항에 대한 최고의 지식 기반을 제공하여 컴플라이언스 요구사항 충족
- 아티팩트와 인시던트 간의 관계를 명확하게 파악하여 인시던트 대응의 우선 순위 지정

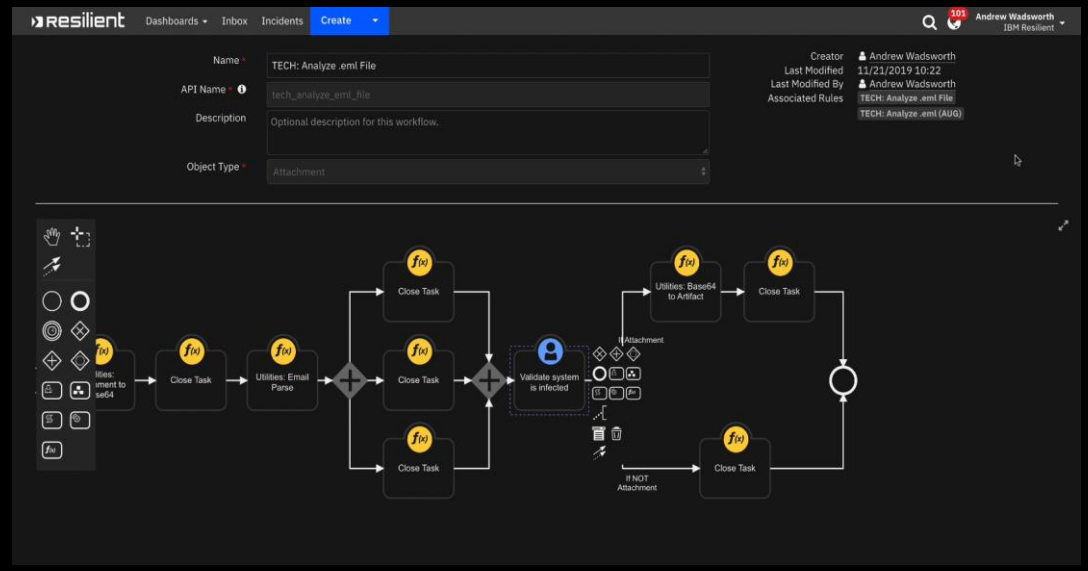


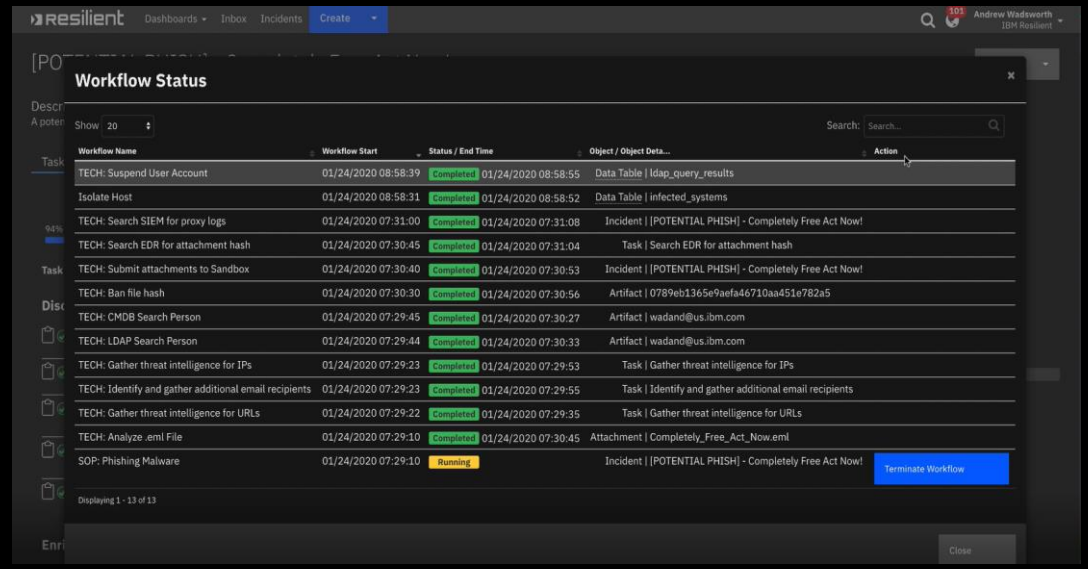
인텔리전스를 통한 업무 관련 작업 자동화

리스크를 완화하기 위해 대응 가속화 및 오케스트레이션

특징 및 기능 :

- 복잡한 사이버 위협을 찾고, 대응하고, 해결할 수 있어 시간 단축
- 수동 및 반복 작업 간소화 및 자동화
- 보안 에코시스템 및 외부 위협 인텔리전스 조정
- 높은 가치 조사 및 대응 활동에 대한 분석 워크로드 우선순위 지정



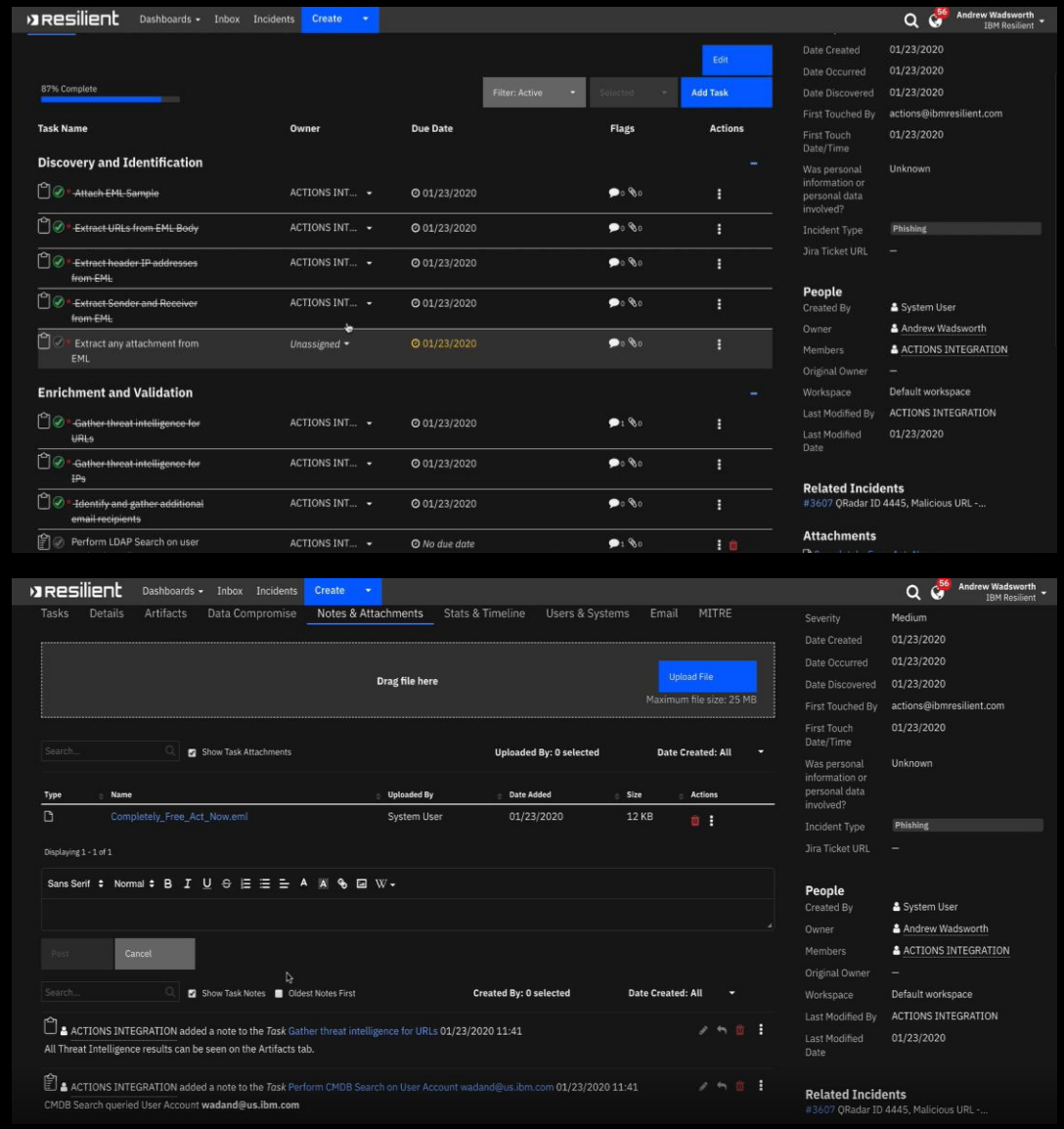


사고 발생 시 일관성 있는 팀 간 협업

보안 사고를 시각화하고 이해하여 우선 순위를 정하고 조치

특징 및 기능 :

- 강력한 케이스 관리 및 태스크와 일관되게 조사 및 대응 조치 안내 및 실행
- 공유 정보를 통해 조직 전체에서 보다 신속하게 대응, 보다 효율적으로 조율하여 보다 스마트하게 대응
- 보안 분석가가 자신의 역할과 책임을 확실히 알 수 있도록 작업 및 조치 우선순위 지정
- 가장 효율적인 커뮤니케이션 채널을 통해 팀으로서 효과적으로 업무에 활용



SOAR 기대효과

IBM Resilient 도입의 가장 큰 효과는 사람, 기술, 프로세스를 하나로 만드는 것입니다. 숙련된 보안 직원만 알고 있는 지식을 신입 직원도 따라 할 수 있도록 반복 가능한 프로세스로 정리, 체계화되며 대응 시간을 단축해 실무 처리에 대한 일관성과 집중도를 높일 수 있습니다.

1 전사적 효과

- 보안 사고 대응 훈련을 통해 책임감 향상
- 사고 대응 시간 기록 및 성능 관리
- 컴플라이언스, 감사 등을 위한 규정준수 증거 확보
- 보안 사고 대응 프로세스 내 보안 외 타 부서와의 협업 환경 구축

기업 내 지속 사용이 가능한 보안 표준 운영 프로세스 보유

2 실무적 효과

- SOC의 생산성 측정과 향상
- 공격 별 적합한 대응 프로세스 자동 적용
- SLA에 준한 업무 적용으로 MTTR (평균해결시간) 감소
- 부서별, 지역별 모의훈련을 통한 사고 대응 일관성 유지

반복적인 업무의 자동화로 보안 인력의 분석 및 대응 집중 시간 확보

3 관리적 효과

- 데시보드와 리포팅을 통해 담당자, 진행상황, 보안 사고 내역 등 신속한 보안 사고 대응 현황 파악
- 내부 보안 기술 상향 평준화로 추가 인력 비용 감소
- 보안 자원 활용 현황 수치화를 통해 업무 성과 측정 및 ROI 파악

기존 보안 투자의 비즈니스 가치 파악

Modernize your security with IBM Cloud Pak for Security

Silo

Manual

Integration

Federated Search

Automation

Prebuilt-Integration