

IBM Security

The Last Piece of Puzzle in Cyber Security

IBM's 차세대 지능형 오케스트레이션

SOAR 플랫폼 리질리언트 소개

Resilient@IBM Security

Nov 2019

보안사업부 김승준 실장

(sjkim@kr.ibm.com)



IBM

THREAT PREVENTION
LEFT OF BOOM

BOOM

CRISIS RESPONSE
RIGHT OF BOOM

Malware Deployed

Additional Compromises

Press Conference

Notify Third Parties

SEC Investigation

Remote Access of Network

First Public Indicator

Stocks Fall

Forensic Research

Board Meeting

Phishing Email

Database Stolen

FBI Calls CEO

Social Media Sentiment Falls

Insider Victim

Response Website

Legal Deposition

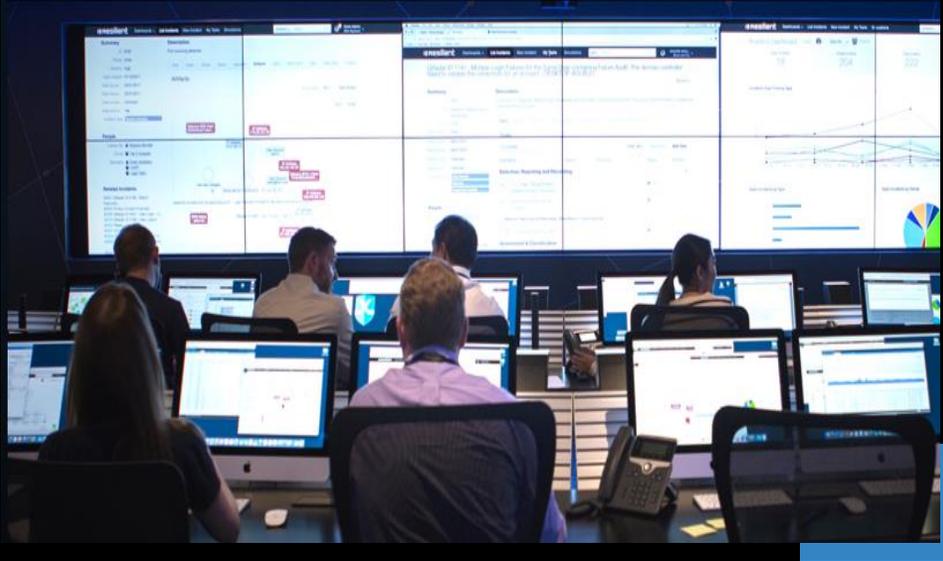
Credentials Stolen

Encrypted Communication

Update Executives

Validate Altered Financial Reports

기업 보안의 현황



Cyber Threat Increased

200억개

이상의 정보보호 대상

50억건

개인정보 유출

6000조원

피해 예상 (향후 2년간)

Advanced Threat

5000건

국내 기업의 60%가
매일 탐지하는 이벤트

83%

탐지 이벤트의
조치 / 대응

Skill Shortage

180만

사이버 보안 인력 부족
(향후 2022년)

Too Many tools & Complex Process

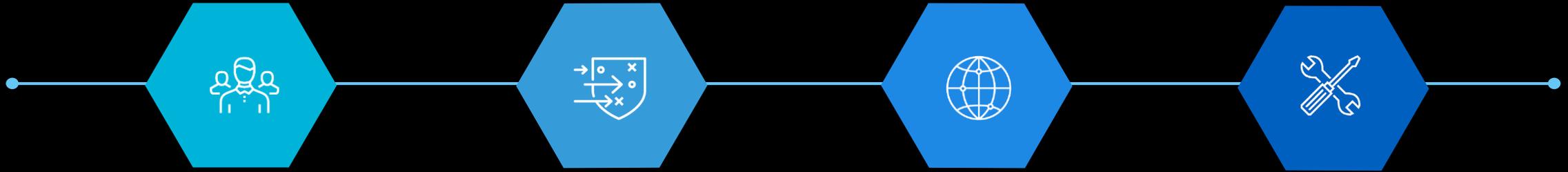
80종

기업 평균 보안솔루션

90%

협업/조율에 어려움을
호소하는 국내 보안 담당자

기업 보안 운영의 어려움



지속적인 기술 인력 부족

- 숙련된 보안 인력 고용 부족
- 보안 인력의 잦은 이직
- 보안 업무 이해도의 격차

공격의 빈도와 위험도 증가

- False Positive 발생 증가
- 수동 분석에 의한 실수 발생
- 데이터 수집 시간 · 업무 증가

점점 증가하는 각종 규제

- 복잡한 컴플라이언스 대응 필요
- GDPR 등 글로벌 정보보호 규정
- 침해 사고 대응의 표준화

복잡해지는 보안 업무 환경

- 보안 사고에 대한 전사적 대응 필요
- 사고 대응 이해 관계자 협업 환경 요구
- 보안 사고에 대한 타 부서 업무 이해 필요

SOAR의 정의

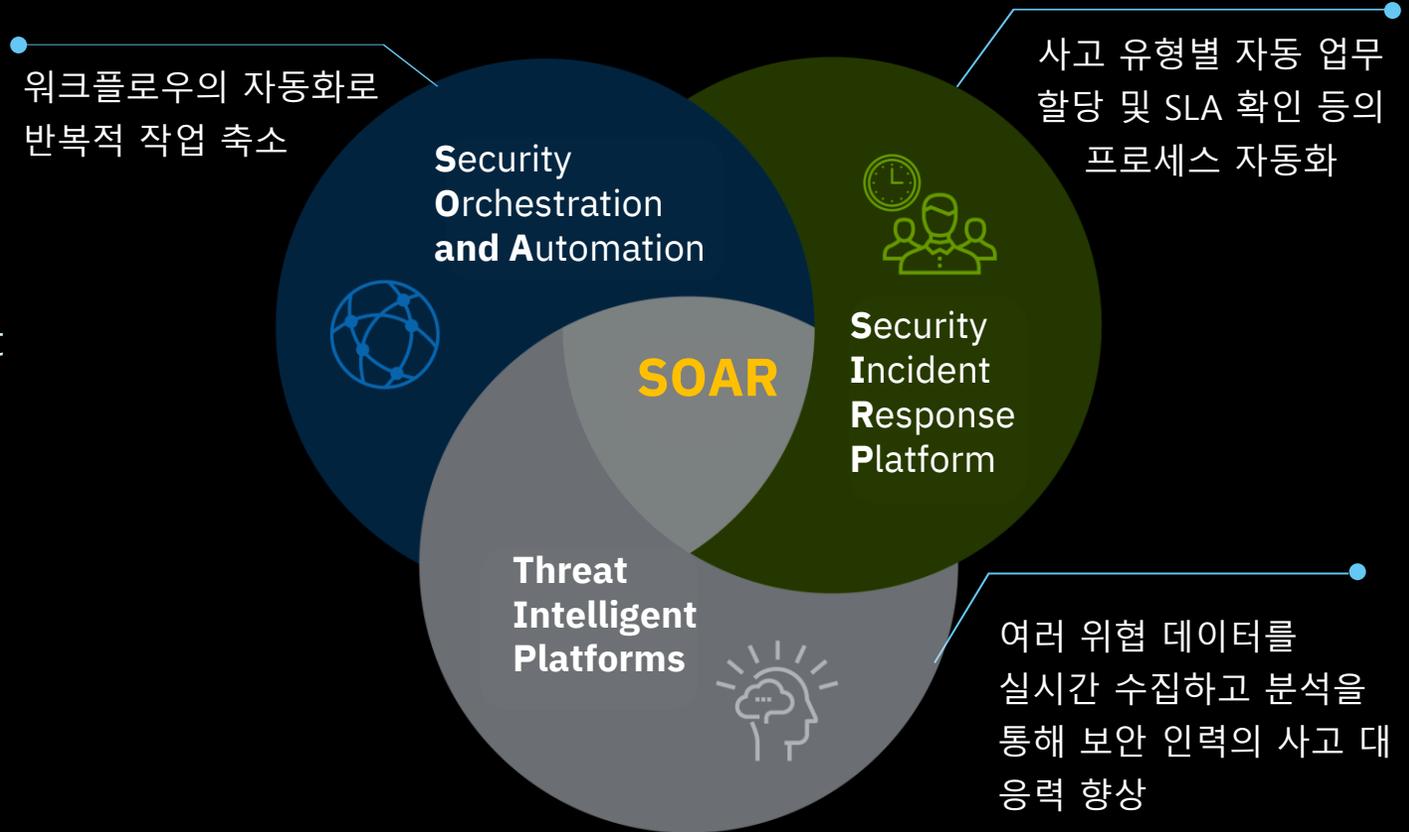
Gartner®

“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 모듈화를 통한 재사용

03 Incident Management & Collaboration

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

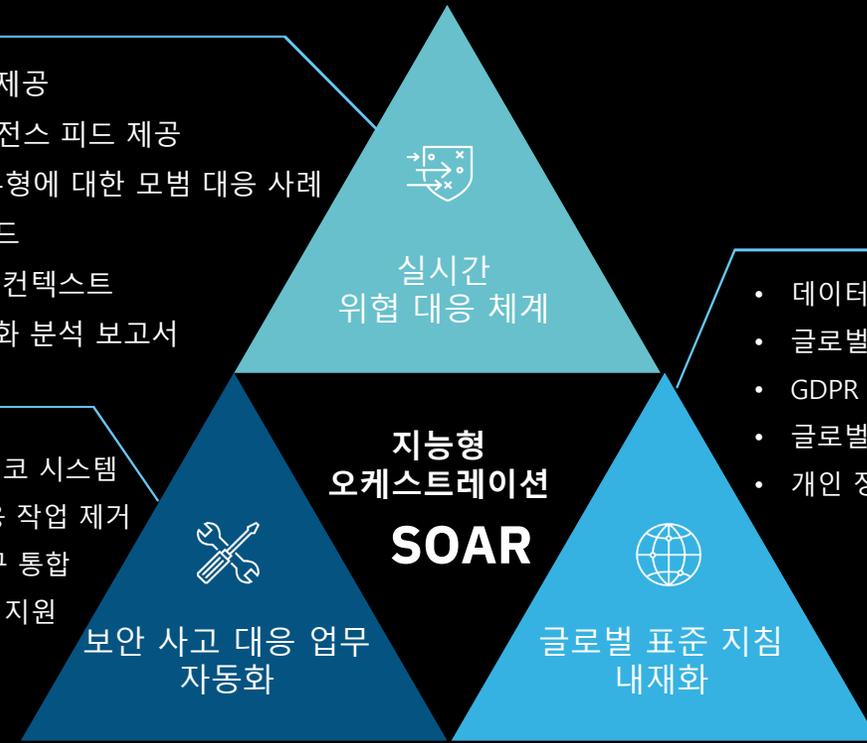
04 Dashboards & Reporting

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

IBM's SOAR PLATFORM - RESILIENT



- Dynamic Playbook 제공
- 10개 이상의 인텔리전스 피드 제공
- 18개 이상의 사고 유형에 대한 모범 대응 사례
- 사용자 정의 데시보드
- 실제 대응이 가능한 컨텍스트
- 경영진을 위한 시각화 분석 보고서
- APP Exchange를 통한 에코 시스템
- 반복적, 수동적 사고 대응 작업 제거
- 100가지 이상의 보안도구 통합
- REST-API를 이용한 통합 지원

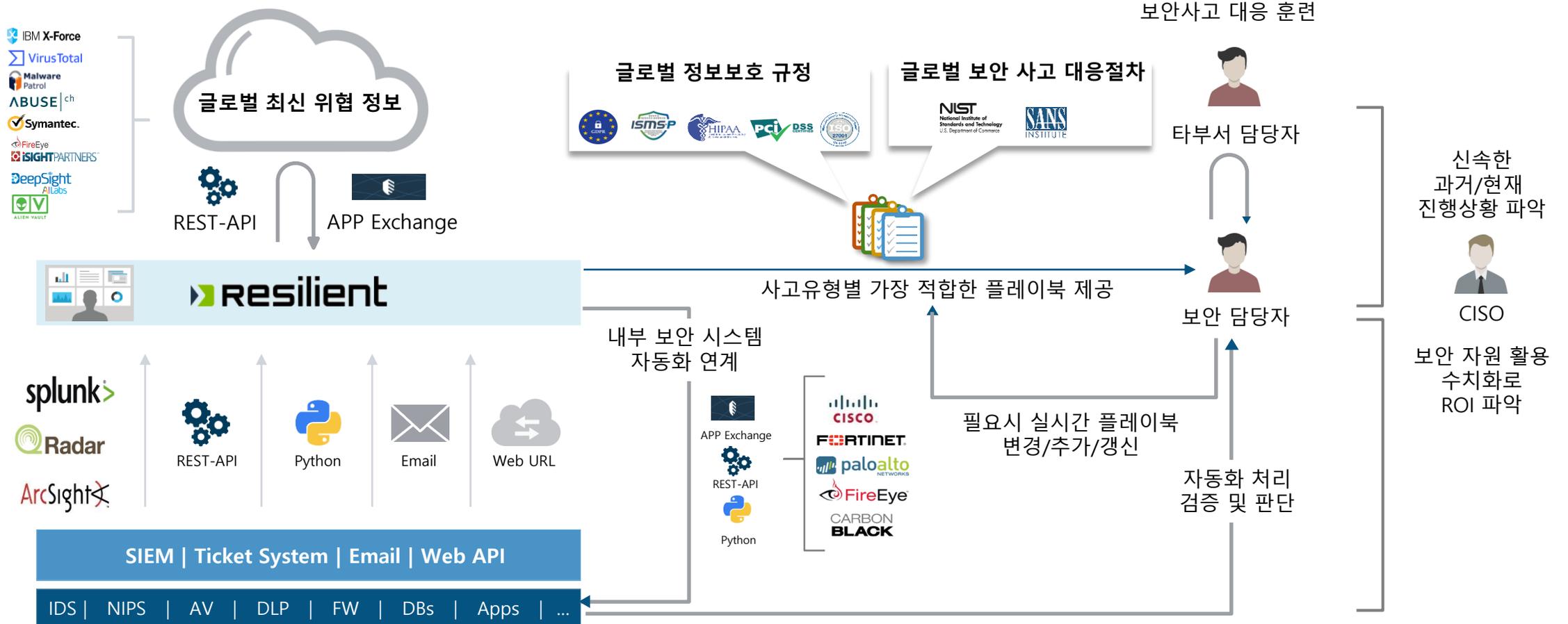


- 데이터 유출 알림 평가, 대응
- 글로벌 규정 데이터베이스 업데이트
- GDPR 등 글로벌 개인정보 준수
- 글로벌 산업 규제 준수
- 개인 정보 평가 도구 및 시뮬레이션

< IBM Resilient 특징 >

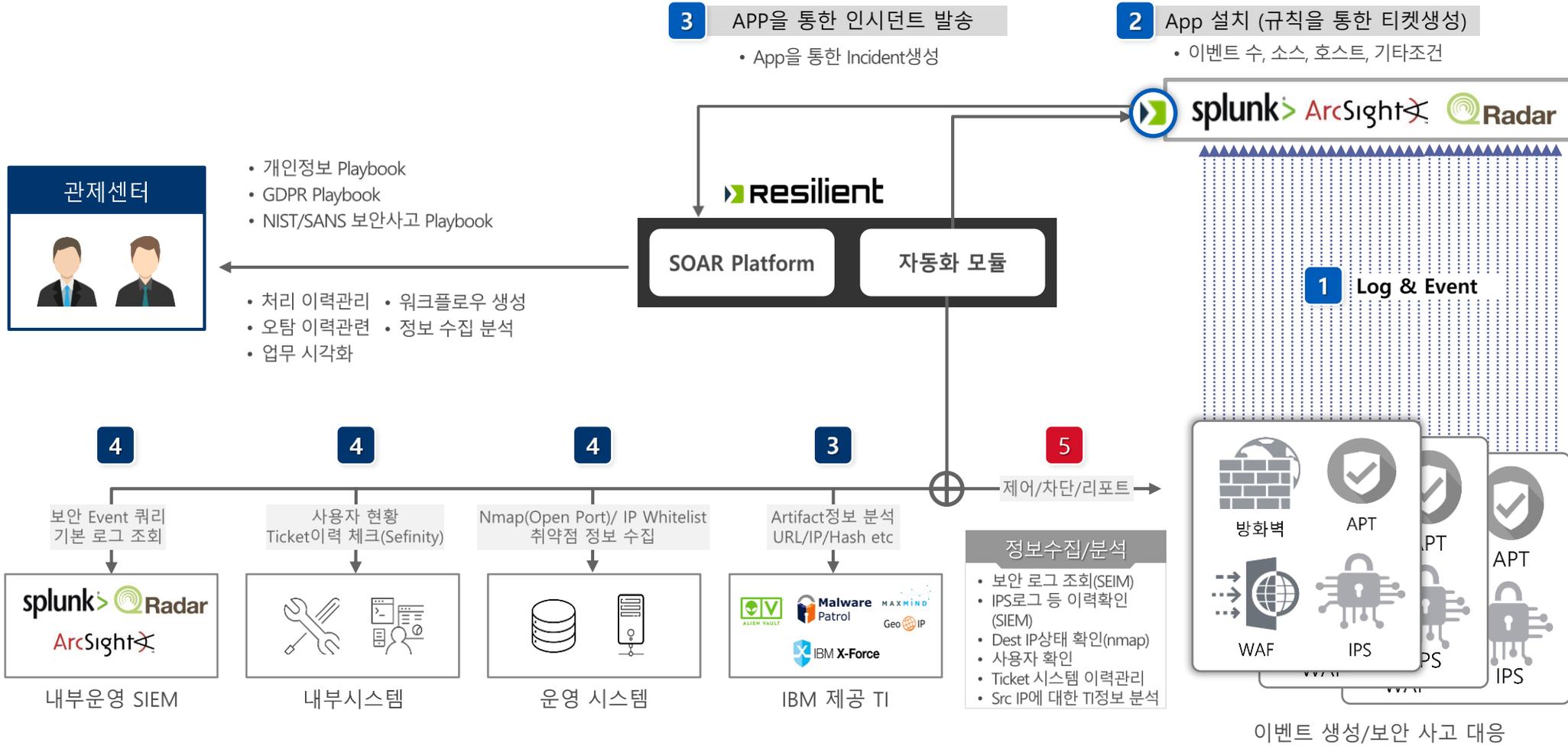
RESILIENT 동작방식

보안티켓 및 악성코드 탐지 시 해킹 IP 및 URL 자동 차단 방안

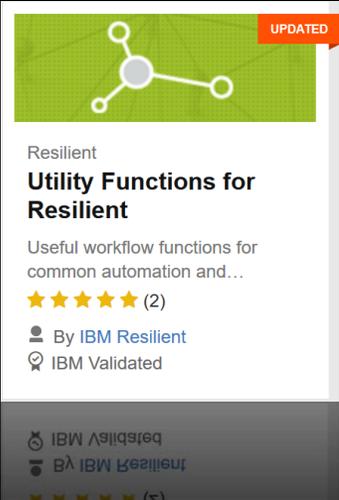


관제업무 자동화(사고예방 업무 자동화)

보안티켓 및 악성코드 탐지 시 해킹 IP 및 URL 자동 차단 방안



보안관제 업무 자동화를 위한 위한 앱 제공(AppExchange)



Resilient Utility Functions for Resilient

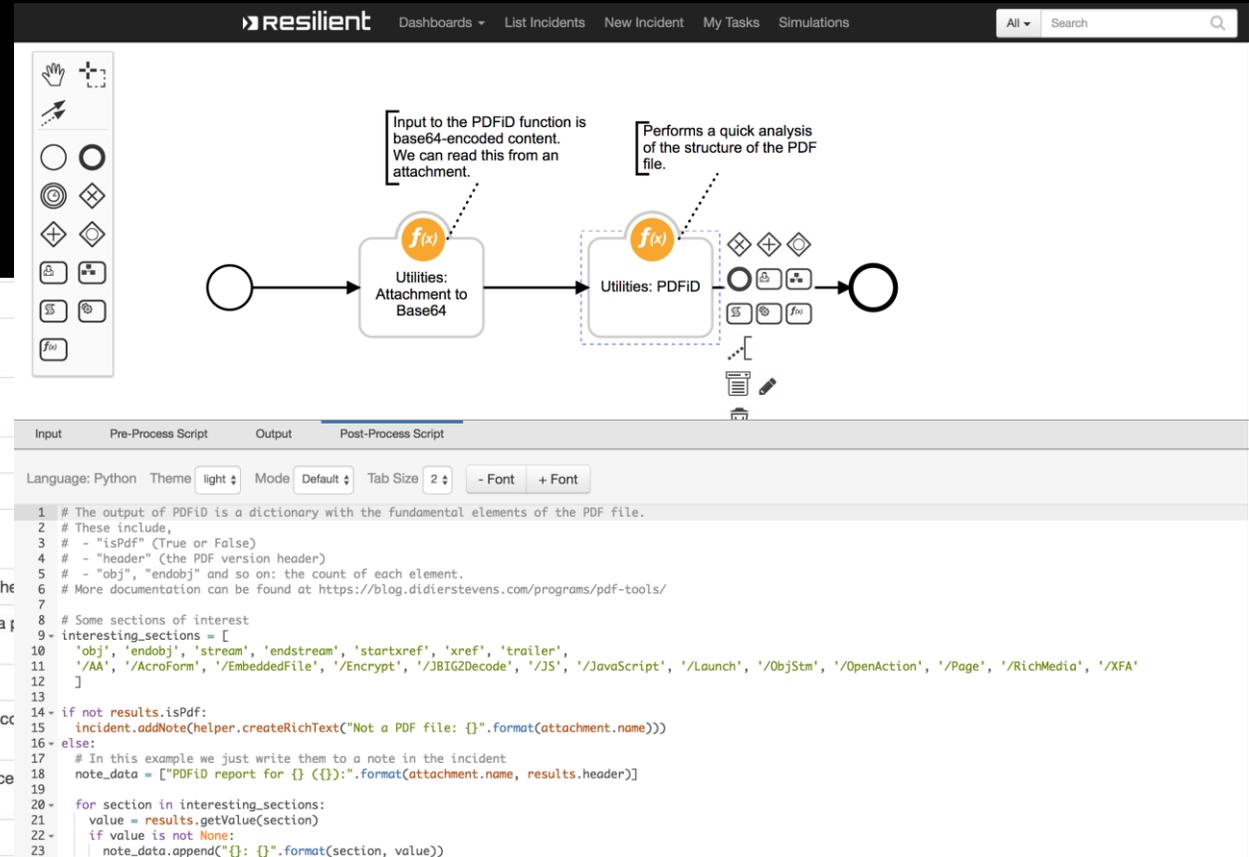
Useful workflow functions for common automation and...

★★★★★ (2)

By IBM Resilient
IBM Validated

- Function to call generic REST/JSON web service APIs,
- Function to run arbitrary shell scripts (bash and PowerShell),
- Functions to fetch SSL certificates from a server and parse them,
- Functions to work with Excel, HTML, XML, JSON and EML files,
- Functions to work with Resilient attachments: calculate hashes, list and extract ZIP archives, convert to and from base64
- Function to parse .eml and .msg email files
- Function to pause a workflow for a specified amount of time.

Utilities: Attachment Hash	Calculate hashes for a file attachment.
Utilities: Attachment to Base64	Read a file attachment as a Base64 string.
Utilities: Attachment Zip Extract	Extract a file from a zipfile attachment, producing a base64 string.
Utilities: Attachment Zip List	For a zipfile attachment, return a list of its contents.
Utilities: Base64 to Artifact	Create a new artifact from a Base64 string
Utilities: Base64 to Attachment	Create a new attachment from a base64 string.
Utilities: Call REST API	Call a REST web service. The function parameters determine the type of call (GET, POST, etc), the URL, and optionally the headers.
Utilities: Domain Distance	Identifies similarity between a suspicious domain name and a list of valid domain names. Low distance result indicates a high likelihood of a match.
Utilities: Email Parse	Extract message headers and body parts from an email message artifact.
Utilities: PDFID	Produces summary information about the structure of a PDF file, using Didier Stevens' pdfid (https://blog.didierstevens.com/tools/pdfid/)
Utilities: Resilient Search	Searches Resilient for incident data. NOTE: The results may include data from incidents that the current user cannot access due to permissions.
Utilities: Shell Command	Runs a shell command.



The screenshot shows a workflow in the Resilient console. The workflow consists of two utility functions: "Utilities: Attachment to Base64" and "Utilities: PDFID".

Annotations for the workflow:

- Input to the PDFID function is base64-encoded content. We can read this from an attachment.
- Performs a quick analysis of the structure of the PDF file.

The Python script for the PDFID utility function is as follows:

```

1 # The output of PDFID is a dictionary with the fundamental elements of the PDF file.
2 # These include,
3 # - "isPdf" (True or False)
4 # - "header" (the PDF version header)
5 # - "obj", "endobj" and so on: the count of each element.
6 # More documentation can be found at https://blog.didierstevens.com/programs/pdf-tools/
7
8 # Some sections of interest
9 - interesting_sections = [
10   'obj', 'endobj', 'stream', 'endstream', 'startxref', 'xref', 'trailer',
11   '/AA', '/AcroForm', '/EmbeddedFile', '/Encrypt', '/JBIG2Decode', '/JS', '/JavaScript', '/Launch', '/ObjStm', '/OpenAction', '/Page', '/RichMedia', '/XFA'
12 ]
13
14 - if not results.isPdf:
15   incident.addNote(helper.createRichText("Not a PDF file: {}".format(attachment.name)))
16 - else:
17   # In this example we just write them to a note in the incident
18   note_data = ["PDFID report for {} ({}):".format(attachment.name, results.header)]
19
20 - for section in interesting_sections:
21   value = results.getValue(section)
22   if value is not None:
23     note_data.append("{}: {}".format(section, value))
  
```

보안관제 업무 자동화를 위한 위한 기본적인 앱 제공(Community)

Edit Activity Field

What type of field is this?

What is the label for this field? * Requirement

API Access Name * Tooltip

Placeholder

Add/Edit Values

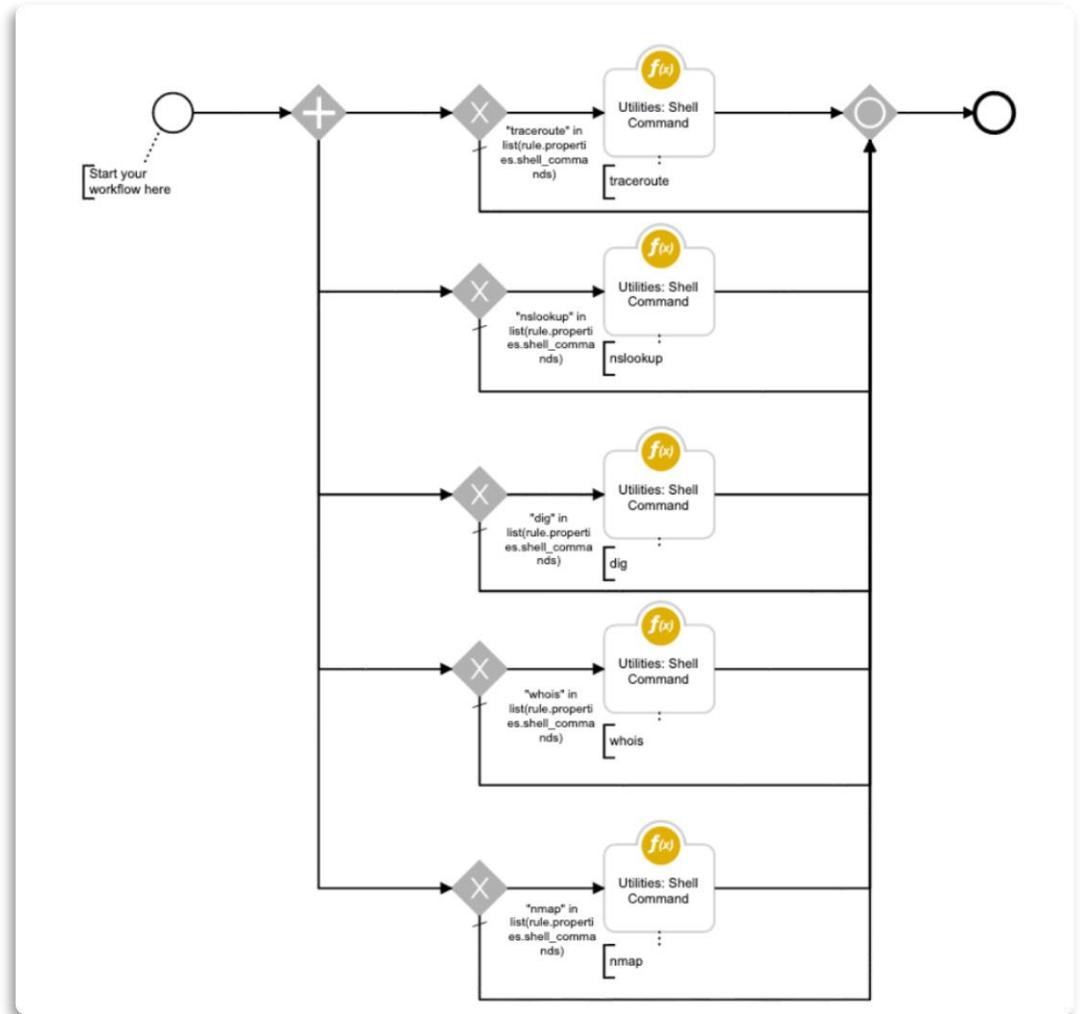
- nslookup default x
- dig default x
- traceroute default x
- whois
- nmap default x

Select one or more options as default when creating new incidents.

78.46.222.235

Details

Created	08/26/2019 12:30
Created By	Benoit Rostagni
Value	78.46.222.235
Type	IP Address
Description	Command succeeded: nslookup "78.46.222.235". See Note for output results Command succeeded: dig "78.46.222.235". See Note for output results Command succeeded: traceroute -m 15 "78.46.222.235". See Note for output results Command succeeded: whois "78.46.222.235". See Note for output results Command succeeded: nmap "78.46.222.235". See Note for output results
Relate?	As specified in the artifact type settings (currently Relate)



자동화를 위한 APP연동 지원 (App Exchange & Community)

업데이트됨



Resilient MITRE ATT&CK Integration

Contains sample functions to retrieve MITRE technique information.

작성자: IBM
IBM이 유효성 검증함

신규



Resilient Cisco WebPulse (Snort) for Resilient

Function provides data on DNS Names and available from Symantec...

작성자: Resilient Labs
커뮤니티가 제공됨

업데이트됨



Resilient Symantec WebPulse (Snort) for Resilient

Function provides data on DNS Names and available from Symantec...

작성자: Resilient Labs
커뮤니티가 제공됨



Resilient Splunk Integration for Resilient

Contains sample functions to demonstrate bi-directional...

★★★★★ (1)

작성자: IBM Resilient
IBM이 유효성 검증함



Resilient ElasticSearch Functions for Resilient

Workflow functions to search and query...

작성자: Resilient
커뮤니티가 제공됨



Resilient QRadar Functions for Resilient

Contains functions to search QRadar offenses and work with QRadar reference sets from...

By IBM Resilient
IBM Validated

Resilient Microsoft Exchange for IBM Resilient

This package provides an interface to Microsoft Exchange email and...

★★★★★ (1)

작성자: IBM Resilient
IBM이 유효성 검증함

Resilient ODBC Functions for Resilient

Workflow functions to query and update ODBC data sources.

작성자: IBM Resilient
IBM이 유효성 검증함

Release Report: v35 of Resilient

Dec 3, 11:00 AM - 11:30 AM (ET)

Resilient User Group: Paris

Dec 4, 9:30 AM - 12:00 PM (CET)
Paris, France

Community Members

578 Members

Show All 24 per page

 Wendy Batten group admin	 Connor Costello group admin	 Will Machin group admin	 Andrew McCarl group admin	 Beth Carroll McCawley group admin	 Scott Puls group admin
 Jennifer Tullman-Botzer group admin	 Cindy Wotus group admin	 Afflospark.com	 Hodor 7Rob	 Thirumurugan A	 Kelly Abbott
 Ashraf Abdelazim	 Ashraf Abdelazim	 Zaid Abrahams	 ahmed abushanab	 Pablo Acevedo	 Bruce Adams

Latest Articles

What you need to know about the transition to the IBM support portal

one month ago

New MSP functionality for the Resilient SOAR platform –

2 months ago

Accelerating Incident Response with the Code42 for Resilient App

3 months ago

Group Home
Discussion 1.1K
Library 80
Blogs 24
Events 2
Members 578

Welcome to the **IBM Resilient online community!** Join us to learn more from a community of collaborative experts, who will help you take full advantage of the most advanced, battle-tested incident response platform.

The Resilient SOAR Platform is the leading platform for orchestrating and automating incident response processes. Collaborate, communicate, and contribute solutions with like-minded Resilient users right here.

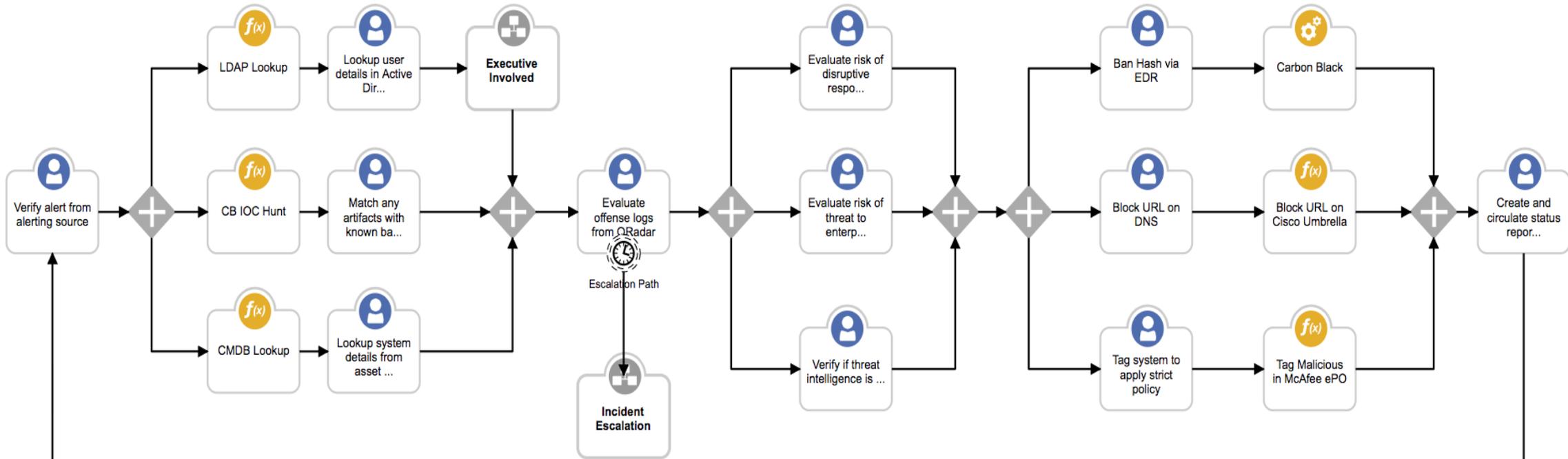
For any questions related to this user group, please contact Community Manager [Connor Costello](#).

Resilient Resources

- [IBM Security App Exchange - Resilient](#)
- [IBM Security Learning Academy - Resilient](#)
- [IBM Resilient SuccessHub](#)
- [IBM Knowledge Center - Resilient](#)
- [IBM Resilient Ideas \(RFE's\)](#)
- [IBM Resilient Homepage](#)

Search Group

다이나믹 플레이북을 통한 기술과 사람의 유기적 자동화



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 가능한** 하위 프로세스

Human Decision Logic

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

보안 위협정보 자동분석 - 외부 위협정보 자동연계 분석

위협 소스

abuse.ch Zeus IP Blocklist 커짐
IP 주소로 알려진 Zeus 서버를 추적하는 www.abuse.ch의 블랙리스트.

abuse.ch Zeus Domain Blocklist 커짐
DNS 도메인 이름으로 알려진 Zeus 서버를 추적하는 www.abuse.ch의 블랙리스트.

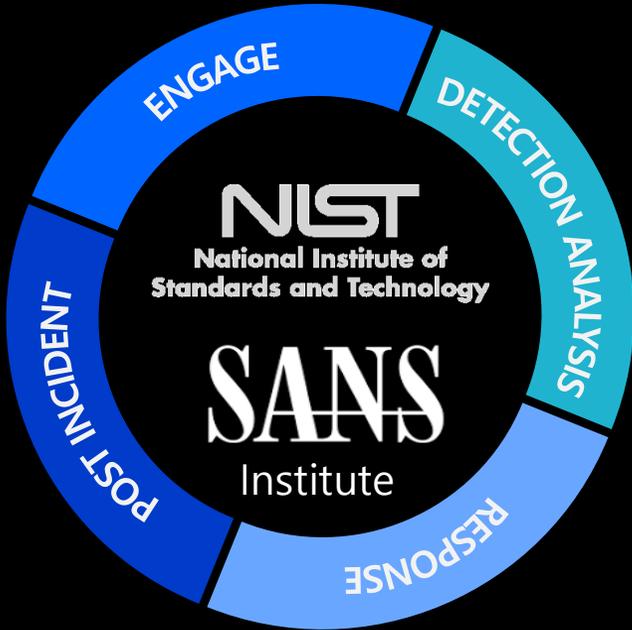
AlienVault IP Reputation Feed 커짐
AlienVault 랩의 의심스러운 IP 주소 목록.

iSIGHT Partners 꺼짐
iSIGHT 파트너의 위협 인텔리전스.

SANS Internet Storm Center 커짐
SANS ISC(Internet Storm Center) 데이터베이스.



글로벌 산업 표준 개인정보 및 사고대응 매뉴얼(플레이북) 제공



• 글로벌 산업표준 사고 대응 업무 가이드 – 침해 사고에 대한 글로벌 표준 대응 프로세스

- 리눅스용 침입감지 체크리스트
- 윈도우용 침입감지 체크리스트
- 인시던트 핸들러

- 보안 인시던트 처리 안내서
- 포렌식 기술 통합 안내서
- 멀웨어 인시던트 방지 및 처리 안내서



멀웨어	랜섬웨어	통신오류	익스플로잇
서비스 거부	시스템 침해	노트북분실	SQL injection
이메일 피싱	개인정보 유출	이상행위 탐지	인증오류
PDA분실	감사이슈	시스템접근이슈	솔루션 오류
기밀 데이터 및 개인정보 유출			

• 글로벌 보안 규정 가이드 – 글로벌 보안 사고 발생 후 위기 대응

- 글로벌 개인정보보호 규정
- ISMS-P
- GDPR
- PCI-DSS
- HIPPA
- FISMA



FERPA /FINRA /FISMA HITECH Act /PCI-DSS (Issuers) PCI-DSS (Merchants) / SEC US Dept of Treasury 등 지원

보안사고 자동대응 프로세스 - 글로벌 정보보호 규정 및 보안 사고 대응 프로세스

데이터 유형별

Data Types

Contact Information

- First name
- First initial
- Middle name
- Last name
- Address
- Phone number
- Email address

Personal Information

- Birth Certificate
- Date of birth
- Driver's license number
- Marital status
- Marriage Certificate
- Occupation
- Passport number
- SSN or SIN

Identification Data

- State ID number
- Tax ID number
- Personal identification
- Tribal ID number
- Employee ID number
- Military ID number
- Student ID Number

Financial Information

- Account password / access code (financial)
- Bank account number
- Bank routing number
- Brokerage account data
- Financial account number
- Income Tax Withheld
- Online username (financial)
- Payment card mag strip data
- Personal ID for financial accounts
- Tax information
- Third-party account information
- Other personal financial information

Credit Card Data

- Credit card CVV code
- Credit card expiration date
- Credit card number
- Credit card password / security code

Debit Card Data

- Debit card CVV code

Medical Information

- Medical history
- Medical treatment
- Diagnostic information
- Mental condition
- Organ donor information

Health-Related Information

- Personal Health Record (electronic)
- Health insurance policy number
- Health insurer ID
- Healthcare payment, eligibility or entitlement information
- Substitute decision maker
- Medicare number
- Medical registration information
- Healthcare provider

Other Data

- Account password / access code (non-financial)
- Biometric data
- CPNI/Communications Data
- Digitized / electronic signature
- Educational records
- Fingerprint
- Genetic information
- Insurance policy number (non-health)
- License information and status
- License plate information
- Online username (non-financial)
- Parent's legal surname prior to marriage
- Security question and answer
- Work-related evaluations

Special Categories

- Criminal activities
- Graphic, photographic or acoustic
- Other information relating to an identified or identifiable person
- Political opinions
- Racial/ethnic origin
- Religious or philosophical beliefs
- Sex life/orientation
- Trade union membership

규제 기관별

Regulators

Organizational Rules

- Data Breach Best Practices ⓘ

U. S. Federal and Trade Organizations

조직을 규제하는 규제자 또는 규정만 선택하십시오.

- Bank Secrecy Act ⓘ
- CMS ⓘ
- DARS/Dept of Defense ⓘ
- Fannie Mae ⓘ
- FCC ⓘ
- FDIC ⓘ
- Federal Reserve ⓘ
- FERPA ⓘ
- FINRA ⓘ
- FISMA ⓘ
- FTC (Health) ⓘ
- GLB Act ⓘ
- HIPAA/HITECH Act ⓘ
- NACHA ⓘ
- NCUA ⓘ
- OCC ⓘ
- OMB ⓘ
- PCI-DSS (Issuers) ⓘ
- PCI-DSS (Merchants) ⓘ
- SEC ⓘ
- US Dept of Treasury ⓘ

U. S. Special Jurisdictions

업종에 따라 조직에 적용되는 관할권만 선택하십시오. 추가 세부사항은 각각의 도구 팁을 참조하십시오.

- California (Health) ⓘ
- Texas (Health) ⓘ
- Virginia (Health) ⓘ
- California (Insurance) ⓘ
- Connecticut (Insurance) ⓘ
- New Hampshire (Insurance) ⓘ
- Montana (Insurance) ⓘ
- Ohio (Insurance) ⓘ
- Rhode Island (Insurance) ⓘ
- Washington (Insurance) ⓘ
- Wisconsin (Insurance) ⓘ
- Arkansas (Mortgage Bankers and Loan Officers) ⓘ
- Arkansas (Insurance) ⓘ
- Texas person/entity/state agency ⓘ
- New York (Department of Financial Services) ⓘ
- Illinois (State Agencies) ⓘ

Canada

회사 설립이나 데이터 처리가 이 특정 인시던트에 중요한 해당 국가만 선택하십시오.

국가별

Asia/Pacific

회사 설립이나 데이터 처리가 이 특정 인시던트에 중요한 해당 국가만 선택하십시오.

- Australia ⓘ
- China ⓘ
- Hong Kong ⓘ
- Indonesia (electronic service providers) ⓘ
- Japan ⓘ
- New Zealand ⓘ
- Philippines ⓘ
- Singapore ⓘ
- South Korea ⓘ
- Taiwan ⓘ

Latin America

회사 설립이나 데이터 처리가 이 특정 인시던트에 중요한 해당 국가만 선택하십시오.

- Argentina ⓘ
- Bahamas ⓘ
- Colombia ⓘ
- Costa Rica ⓘ
- Mexico ⓘ
- Mexico (Payment Card Networks) ⓘ
- Peru ⓘ
- Uruguay ⓘ

다이나믹 플레이북을 통한 보안 사고대응 자동화

대시보드 > 인시던트 > 작성

1247 Level 2 Analyst
ACH

31% 완료

대응 진행 현황

1개의 태스크가 선택됨
필터: 활성
선택됨
태스크 추가

단계별 대응 업무 자동 생성

- 랜섬웨어에 감염된 자산 확인 (Identify assets affected by ransomware-attack)
- 중요개인 인터뷰(Interview key individuals)
- 랜섬웨어 변종 확인 (Identify ransomware-variant)
- 초기분류(Initial-Triage)
- 내부 관리 체인에 알림(사전) Notify internal management chain (preliminary)

Detect/Analyze

- 적절한 제거 또는 복구 전략 결정 (Determine an appropriate eradication or recovery strategy)
- 현재 공격 인텔리전스 및 취약성 조사 (Research current attack intelligence and recover vulnerabilities)

중요개인 인터뷰(Interview key individuals)

세부사항 참고 멤버 첨부 파일

상세한 업무 사항 명시

지시사항

소유자 Level 1 Analyst 작성자 Admin Staff

만기 날짜 2019.06.14 09:47 시작된 날짜 2019.06.13 09:47

일반 사용자, 시스템 관리자 및 감염된 시스템/애플리케이션 소유자 등의 중요 개인과 인터뷰하십시오. 판별:

- 최신의 비정상적 활동이 기록되어 있습니까?
- 포함된 감염 시스템에 대한 관리자 액세스 권한은 누구에게 있습니까?
- 최신 구성 변경사항 또는 패치가 적용되었습니까?
- 최근에 의심스러운 이메일이나 문서의 수신 및/또는 열기를 수행했습니까?
- 최근에 의심스러운 웹 찾아보기 활동이 있었습니까?
- 감염된 시스템/애플리케이션에서 제공하는 로깅은 무엇입니까?
- 민감한 개인 또는 기밀 정보가 감염된 시스템에 포함되어 있습니까?

모든 활동과 찾은 결과를 캡처하여 이 태스크에 참고를 추가하거나 인터뷰 참고를 첨부하십시오.

Interview key individuals such as end users, system administrators and affected system/application owners. Determine:

완료 및 닫기

유형별 대응업무자동추가

Incident Type 공인데이터

대응 담당자 현황

People

Created By Admin Staff

Owner Admin Staff

Members

- Level 1 Analyst
- Level 2 Analyst
- Level 3 Analyst
- Incident Manager

관련된 과거 인시던트

Related Incidents

- #2310 Incident generated from email ...
- #2301 QRadar ID 2333 , Anomaly: Access...
- #2299 QRadar ID 1908 , Policy: Chat or...
- #2206 Incident generated from email "R..."
- #2205 QRadar ID 774 , REXEC: Account L...
- #2202 Incident generated from email ...

첨부된 관련 파일

Attachments

ransomware-wannacry.jpg

Newsfeed

Level 2 Analyst이(가) 태스크에서 닫힘(으)로 상태를 변경함 초기 분류(Initial Triage) 1분 전

태스크 이름

담당자 자동할당

SLA기반 완료기한지정

의견 및 파일 첨부

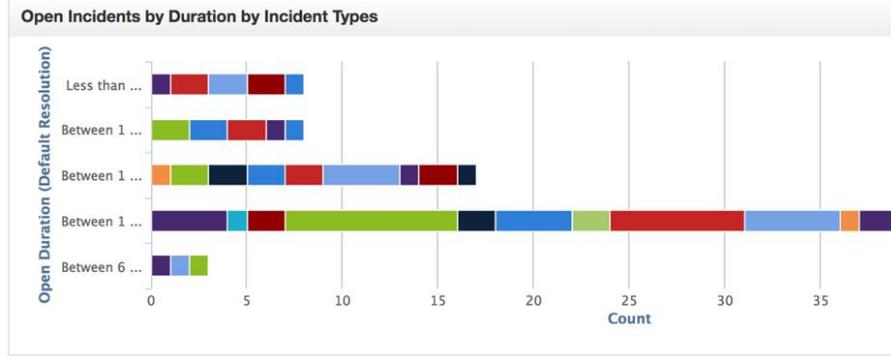
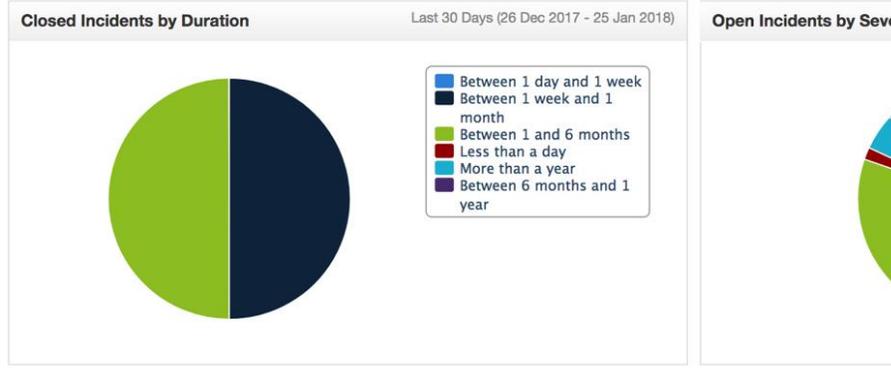
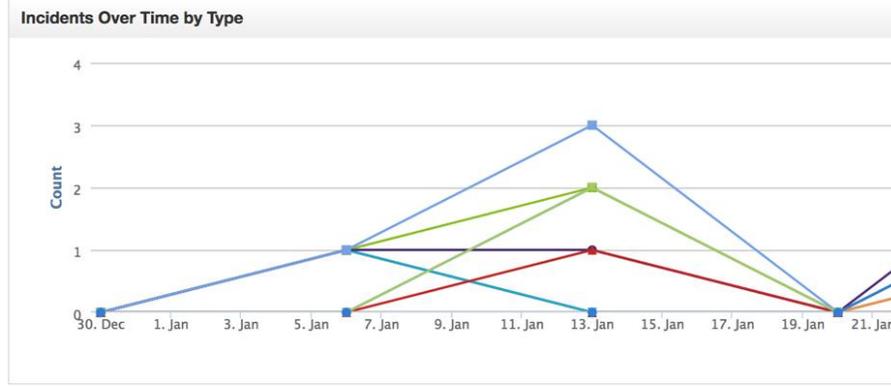
조치 필요시 업무 추가

세부사항

Level 2 Analyst

2019.06.15

레포트와 권한 별 대시보드



Summary

ID 4786
 Severity 1
 Impact 1
 Risk 1
 Phase Respond

Date Created 12/07/2017
 Date Occurr... 12/07/2017
 Incident Type **System Intrusion**

People

Created By Jessica Cholerton
 Owner Jessica Cholerton
 Members L1 Team
 Data Privacy Team
 Andrew Yeates

Related Incidents

#4782 Stolen Laptop Report - USERHH

Attachments

pcap.pdf

Newsfeed

Jessica Cholerton wrote a note on the task [Analyze application data for signs of intrusion](#) 6 months ago

Select a Template ✕

- ✓ Major Incident Report Print
- Executive Summary - Breach
- Executive Summary
- Security Incident Details
- Breach Incident Details
- Incident History

Cancel

44% Complete Filter: All ▾ Selected ▾ **Add Task**

Task Name	Owner	Due Date	Flags	Actions
Initial				
Initial - (Data Breach - Organizational)				
Identify the risk of harm that the data breach poses	Unassigned ▾	No due date	0 0	⋮
Engage				
*Initial Triage-01	Andrew Yeates ▾	No due date	1 1	⋮
*Interview key individuals	Andrew Yeates ▾	No due date	0 0	⋮
*Determine Systems Involved	Jessica Chole... ▾	No due date	0 0	⋮
Notify internal management chain (preliminary)	Jessica Chole... ▾	No due date	0 0	⋮
*Determine if illegal activity is involved	Jessica Chole... ▾	No due date	0 0	⋮
*Determine if inappropriate internal involvement	Andrew Yeates ▾	No due date	0 0	⋮
Detect/Analyze				

Resilient 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





Thank you so much!

고맙습니다.