VMRAY

Detecting the Undetectable

PAGO NETWORKS

VMRay Sales & Technical Distributor

VMRay 미션

VMRAY

DETECT THE
UNDETECTABLE

Trusted By Elite Security Teams Across The Globe

VMRay 비젼

VMRAY

A world liberated from undetectable cyber security threats.

탐지할 수 없는 사이버 보안 위협으로부터 자유로운 세상.

VMRay 기업 개요

Innovation is in our DNA

VMRAY

샌드박스 전문가 기업

2013년 설립

자동화된 멀웨어 분석 및 탐지 전문가의 주도적인 창업

CEO - Carsten Willems

CTO - Ralf Hund

샌드박스 기술 혁신 리딩

20+ 혁신 기술 적용

업계 대비, 우월한 혁신 기술 적용
멀웨어 유형 상관없이 정확한 분석

글로벌 운영

- 독일 (본사 / 연구소)
- 영국
- 미국
- APAC

100+

- R&D 연구 개발 본부
- 리서치 본부

혁신 기술

- 보편적인 샌드박스 기술 대비, 혁신적인 기술 보유
- 진화하는 위협 대비, 정확한 식별, 탐지, 대응 고도화

다양한 산업 분야의 선택

VMRAY

글로벌 최대 기업들이 VMRay 를 신뢰하고 있습니다.
Again and again.

100 +
다양한 산업 분야의
글로벌 리더 기업

4 of 5
글로벌 최고
테크 자이언트 기업

34
시장을 리딩하는
글로벌 금융 기업

3 of 4
Big 6
글로벌 컨설팅기업

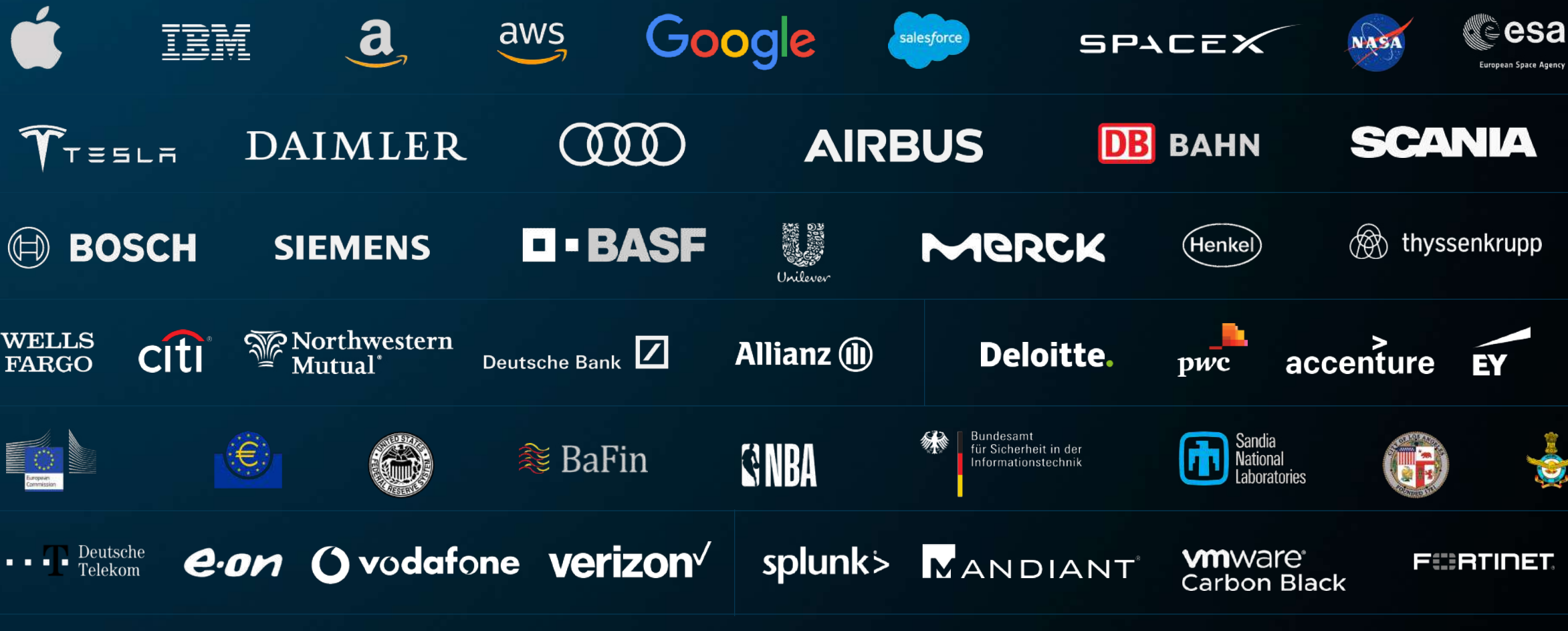
58
글로벌
공공기업 / 정부기관

107%
지속적인 재계약 비율
50%
지속적인 연간 성장률

주요 고객사

VMRay는 글로벌 주요 기업들과 긴밀하게 협업하고 있습니다

VMRAY



VMRay 고객들이 직접 공유하는 성공 스토리

VMRAY

	기존 이슈	업무 비효율성 초래	VMRay 도입 효과
1	• 위협의 보안솔루션 회피기술과 고도화된 표적공격 대응 실패 • 결정하기 어려운 보안분석 결과 • EDR 솔루션의 행위기반 분석 결과에 대한 판단력 부족	• 정확한 위협 분류 어려움 • 즉각적인 대응액션 미비 • 많은 보안 솔루션 Alert 분석 효율성 감소	• 피싱 메일의 빠른 탐지 • EDR Alert 빠른 검증 • Near-Realtime 분석 결과 • API 기반 다양한 보안솔루션 연동 및 협업 자동화 구현
2	• 전문 분석팀 구성의 어려움 • 수동 분석 프로세스 • 자동화 구현의 절실함	• 시간 소모적인 프로세스 • 실질적인 보안 경고 지연 • 전략적인 보안업무 활동 시간 없음	• 자동화된 분석 프로세스 • 위협 분석을 위한 시간 소모 사라짐 • 실질적인 대응 활동에 전념
3	• 보안팀 인원 잦은 교체 • 빠른 성장에 따른, 많은 보안솔루션 급증 • 사고 대응을 위한 고급 보안인력 부족 • 자동화 SOAR 있지만, 수동 분석 프로세스	• 부정확하고, Noise 많은 분석 보고서 • SOAR 플랫폼은 프로세스를 자동화 할 뿐, 실제 분석활동은 수동 처리 • 수많은 위협 Input 소스 통일화 필요	• 보안팀 구성 상관없이, 빠르고 정확한, 보안 분석 결과 획득 • 규모에 상관없이 자동화 및 확장성 보유 • 실질적인 위협 인텔리전스와 SOAR 연계

산업계 전반적인 당면 이슈 (리서치 참고)

VMRAY

충분한 보안 컨트롤 및 솔루션,
충분한 보안 이벤트,
하지만 …

45% 보안 경고 (Alert) "오탐"

(참고) IDC "The Voice of the Analyst : Improving Security Operations Center Processes through Adapted Technologies", 2021

<48% 보안 경고 (Alert) "재분석 필요"

(참고) Cisco "CISO Benchmark Study", 2020

58% 보안 분석가 "위협 우선순위 지정, 또는 대응에 자신이 없음"

(참고) Trend Micro "Security Operations on The Backfoot", 2021

고객들의 현실적인 이슈

VMRAY

보안팀
전문 인력 부족

Understaffed Security Teams

알려지지 않은
멀웨어 / 위협

Unknown Malware / Threat

시간이
많이 걸리는 분석

Time-Consuming Analysis

느린
응답 시간

Lagging Response Time

고객 이슈 해결을 위한 VMRay 제안

VMRAY

실현 가능한 기술 고도화
ENABLING TECHNOLOGY

진화하는 위협 대비

- 혁신적인 탐지 및 분석 플랫폼
- 샌드박스 기술 고도화 플랫폼

혁신을 주도하는 다양한 기술

: 독보적인 샌드박스 (Sandbox) 기술 리딩
: 인텔리전트 모니터링 (Intelligent Monitoring)
: 분석 회피기법 탐지 (Anti-Evasion)
: 난독화 기능 분석 기법 (De-Obfuscation)
: 머신러닝 (Machine Learning)

역량 강화
CAPABILITY

다른 분석 솔루션이 놓치는 Unknown 위협 탐지

- 모든 보안 영역에서 블라인드 스팟 (Blind Spot) 제거
- 고객 보안 스택 위에 Unknown 위협 탐지/분석 역량 강화

지능화되는 위협 행위 전반 강력한 분석 기술

- 정확한 분석
- 깊이 있는 in-depth 분석
- Noise-Free 분석 결과
- 대응 가능한 Actionable IOC 제공 / 연동

도입 효과 증명
SOLUTION

1

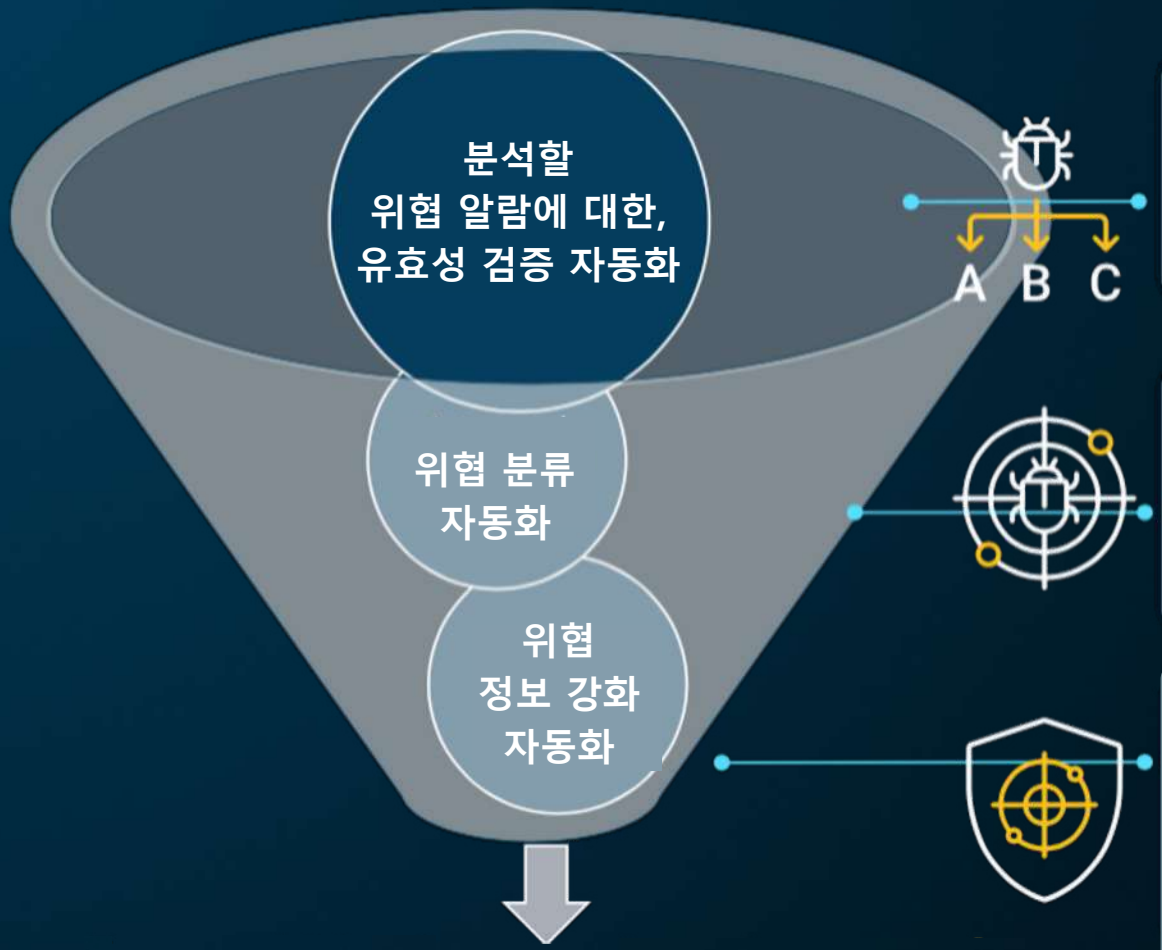
- **고객 보안 고도화 완성**
- **플랫폼 도입 ROI 증대**

2

- **현실적인 자동화 실현**
- **효율적인 보안팀 운영**

VMRay 기술 방향성 – 정확한 자동화 분석

VMRAY



ALERT VALIDATION (위협 유효성 검증)

- 오탐 (False Positive) 자동 제거
- 보안팀이 유효한 위협 알람에만 집중하도록 함

ALERT TRIAGE (위협 분류)

- 심각도 / 우선순위에 따라, 최적의 위협 알람 분류
- 에스컬레이션 할 위협 알람 신속히 식별

ALERT ENRICHMENT (위협 정보 강화)

- 위협 자동화 분류 (Classification)
- 멀웨어 패밀리 자동 식별 위한, Config 자동 추출
- 보안팀의 멀웨어 연결된 행위이벤트 이해력 도움

위협 조사, 분석, 대응
최고의 스피드 제공

VMRay 프레임워크 개요

VMRAY

고객 인프라스트럭쳐

Email Integration
Office 365

Security Automation
SOAR, EDR, SEG,
SWG, TIP, SIEM, ...

Custom Integration
REST API

Manual Usage

Files
- 모든 파일 포맷

URLs

Emails
- 본문 링크
- 첨부 파일

VMRay 플랫폼 (Hypervision 기반 / Anti-Evasion)

VMRAY

- Reputation 체크
- Static 분석
- Dynamic File 분석
- Dynamic Web 분석

- Embeded AV
- Yara Rulesets
- Macro De-Obfucation
- Realtime 메모리 덤프
- Auto Interaction
- Live User Interaction
- TLS Visibility
- VBA Stoming
- Browsing Simulation
- Link Detonation
- Golden 이미지

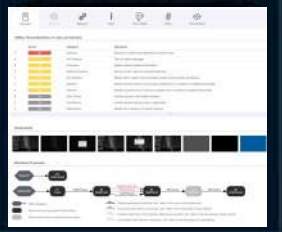
분석결과 유형 1

Verdict
악성 여부

MALICIOUS
SUSPICIOUS
CLEAN

분석결과 유형 2

Report
상세 분석 보고서



고객 인프라스트럭쳐

Security Automation
SOAR, EDR, SEG,
SWG, TIP, SIEM, ...

- 단순 분석 결과 (악성 여부)
- 추출된 IOC
- 상세 분석 레포트

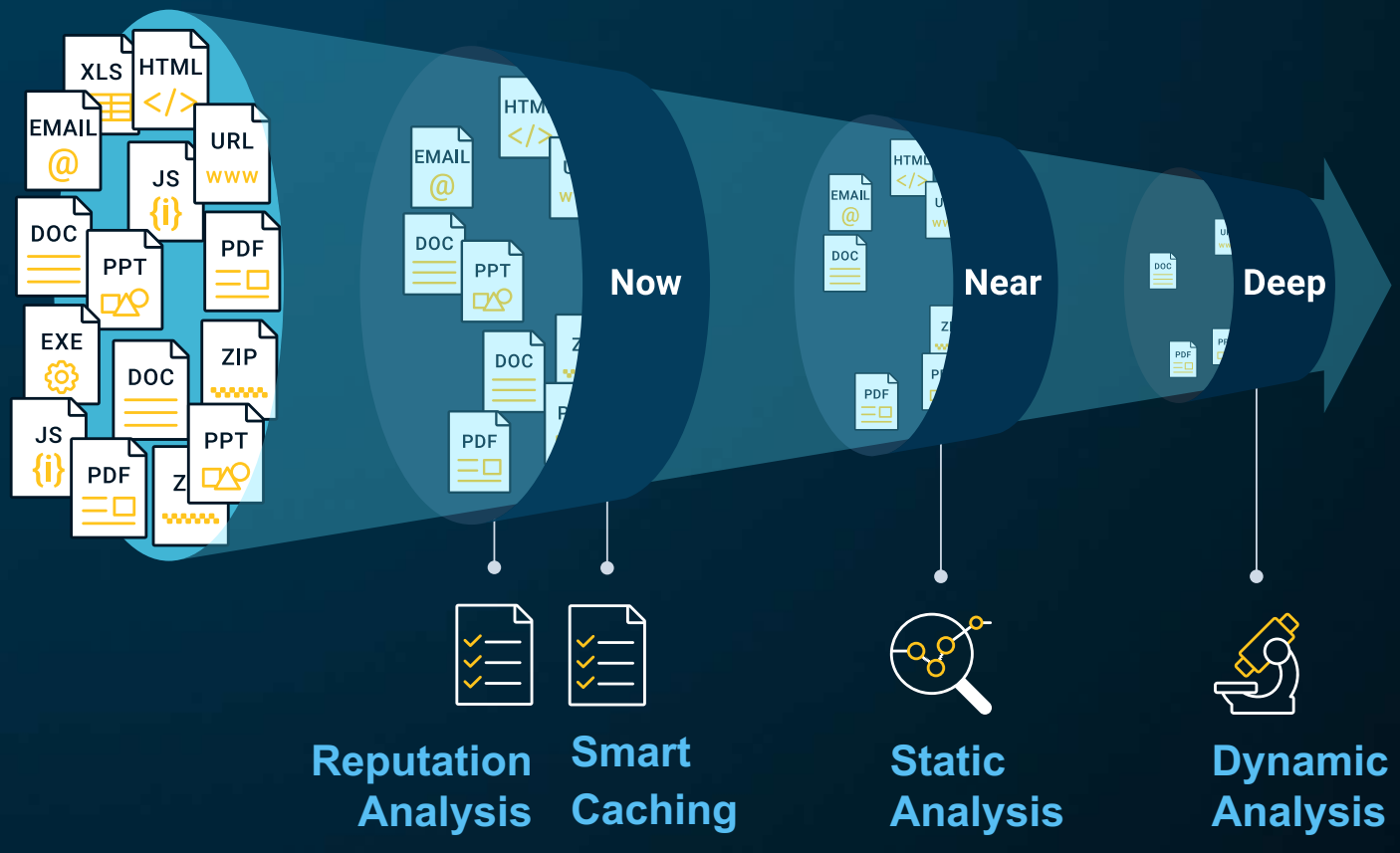
VMRay 분석 샘플 타입 (50+)

VMRAY

- [ ] Apple Script
- [ ] Archive
- [ ] CFB File
- [ ] Custom
- [ ] Email (EML)
- [ ] Email (MSG)
- [ ] Excel Document
- [ ] Executable and Linkable Format (ELF 32bit)
- [ ] Executable and Linkable Format (ELF 64bit)
- [ ] Hanword Document
- [ ] HTML Application
- [ ] HTML Application (Shell Link)
- [ ] HTML Document
- [ ] Java Archive
- [ ] Java Class
- [ ] JScript
- [ ] macOS App
- [ ] macOS DMG
- [ ] macOS Executable
- [ ] macOS PKG
- [ ] Macromedia Flash
- [ ] MHTML Document
- [ ] Microsoft Access Database
- [ ] Microsoft Project Document
- [ ] Microsoft Publisher Document
- [ ] Microsoft Visio Document
- [ ] MSI Setup
- [ ] PDF Document
- [ ] Powerpoint Document
- [ ] PowerShell Script
- [ ] PowerShell Script (Shell Link)
- [ ] Python Script
- [ ] RTF Document
- [ ] Shell Script
- [ ] Unknown
- [ ] URL
- [ ] VBScript
- [ ] Windows ActiveX Control (x86-32)
- [ ] Windows ActiveX Control (x86-64)
- [ ] Windows Batch File
- [ ] Windows Batch File (Shell Link)
- [ ] Windows DLL (x86-32)
- [ ] Windows DLL (x86-64)
- [ ] Windows Driver (x86-32)
- [ ] Windows Driver (x86-64)
- [ ] Windows Exe (Shell Link)
- [ ] Windows Exe (x86-32)
- [ ] Windows Exe (x86-64)
- [ ] Windows Help File
- [ ] Windows Installer Patch
- [ ] Windows Script File
- [ ] Word Document

VMRay 분석 프로세스

VMRAY



분석결과 유형 1

Verdict

악성 여부

- MALICIOUS
- SUSPICIOUS
- CLEAN

분석결과 유형 2

Report

상세 분석 보고서

Post-processing

VMRay 분석 단계별, 주요 코어 모듈

VMRAY

Reputation Analysis

Smart Caching

Static Analysis

Parse
- File Type Recognition
- Deep Content Extraction
- Password-Protected File Analysis
- Macro De-Obfuscation
- Computer Vision

Detect
- VBA Stomping Detection
- YARA Rulesets
- Built-In AV

Filter
- Sample Triage
- Smart Link Detonation
- Digital Signature Verification

Dynamic Analysis

Dynamic Web Analysis
- Adaptive Browsing Simulation
- Machine Learning

Dynamic File Analysis
- Intelligent Monitoring™
- Non-Intrusive TLS Visibility
- Smart Memory Dumping
- Auto Reboot
- Automatic User Interaction
- Live Interaction
- Golden Images

Post-processing

- VMRay Threat Identifiers (VTI)
- MITRE ATT&CK Mapping
- Automatic IOCs Classification

코어 모듈 요약 - 1

VMRAY

- VMRay Reputation Service 이용
- Built-in Reputation 엔진
- 대상
  - ✓ File, URL, Domain, IP
  - ✓ DB 내용 ➔ Hash for Known Malicious / Known Clean
- 지속적인 업데이트
- Cloud / On-Prem 아키텍쳐 모두 지원
- Reputation Lookup 기능 ➔ in Several Milliseconds
- Reputation 모드
  - ✓ Triage Mode : Lookup 결과가 Unknown 일때만, 다음 분석 과정 진행
  - ✓ Auxiliary Mode : Lookup 결과에 상관없이, 무조건 다음 분석 과정 진행
  - ✓ Exclusive Mode : Lookup 만 진행

코어 모듈 요약 - 2

VMRAY

Smart Caching

- VMRay 글로벌 캐싱 메타니즘
- 동일한 샘플을 "다시 재분석" 할 때, 업데이트 된 내용의 정확성 유지 및 추적 가능
- 새로운 탐지룰, 시그니쳐 업데이트, Yara Ruleset 적용하여 신규 C2 등이 추가로 탐지되면, 기존 Report 연계하여 추가 내용 업데이트 (동일한 샘플에, 업데이트된 Report 추가)

한개의 분석 샘플에 대해서,
기존 Suspicious 상태가 Malicious 상태로 업데이트 되었으며,
2개의 Dynamic Report 생성됨 (비교 가능)

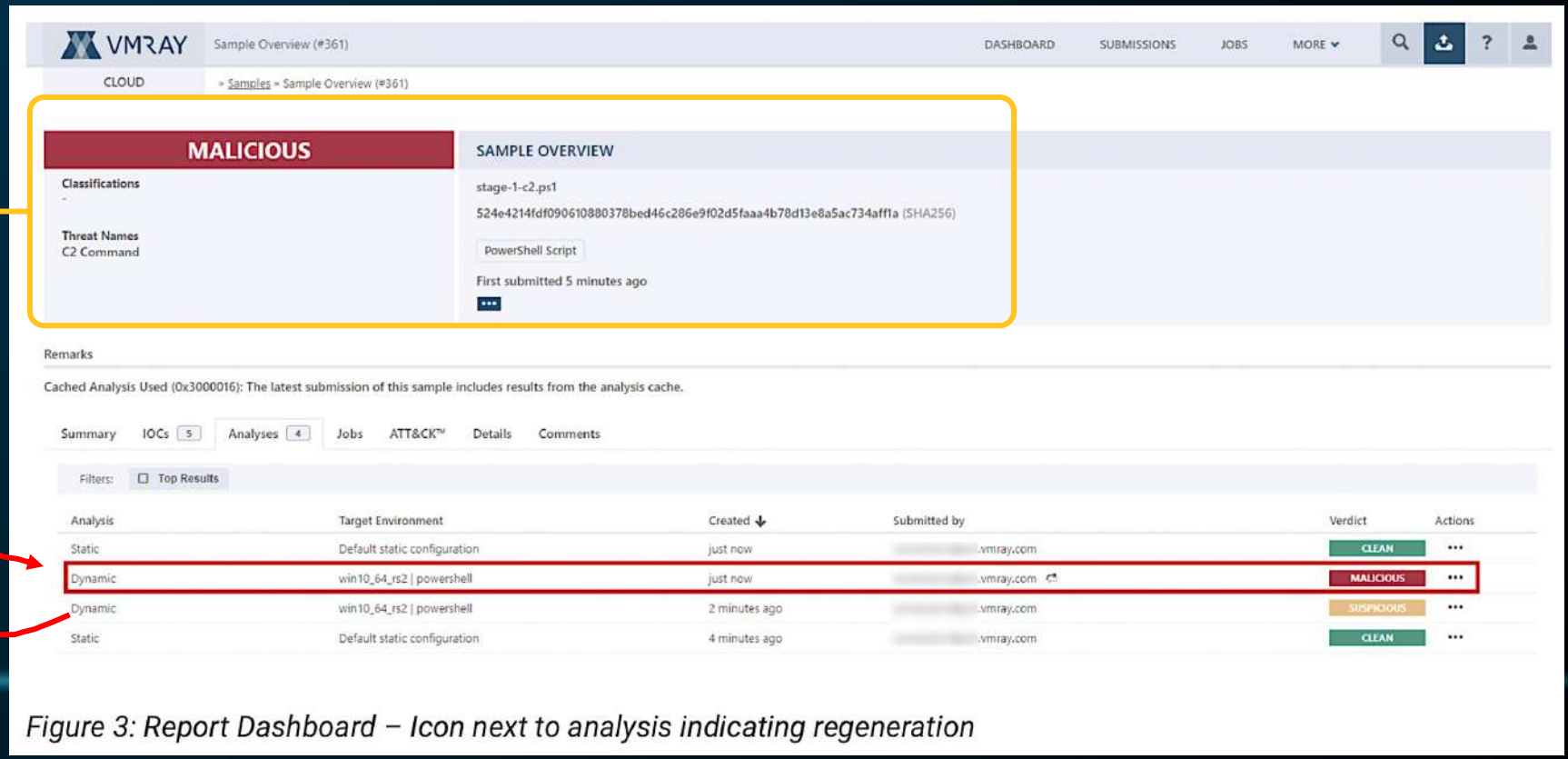


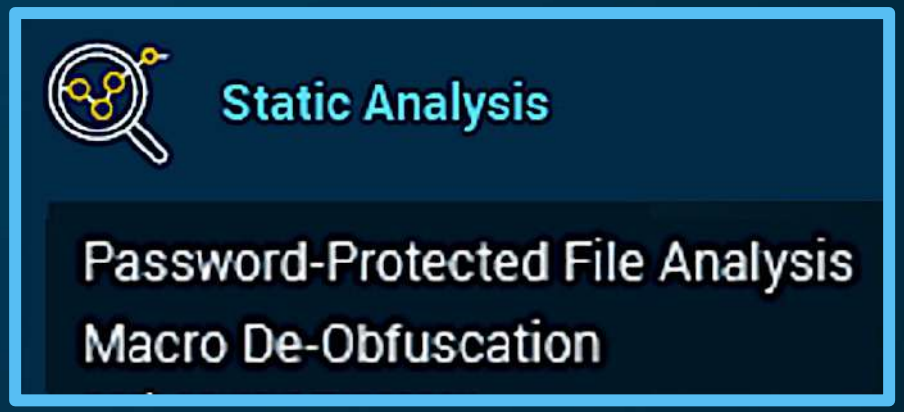
Figure 3: Report Dashboard – Icon next to analysis indicating regeneration

코어 모듈 요약 - 3

VMRAY

- **File Type Recognition**
  - 파일 스트럭쳐 기반, "정확한 파일 타입 " 식별
  - 동적 분석 중, 부분적 깨져서 " 실행 불가한 파일 타입" 정보도 식별
- **Deep Content Extraction**
  - 샘플에서 "모든 Embedded 오브젝트" 추출
  - 추출을 위한 "Depth-Level" 제한 없음
  - 추출된 모든 오브젝트 → 추가 분석 진행(*****)
  - 추출되는 오브젝트 종류
    - ✓ 문서 파일 → Embedded 오브젝트, 링크 (URL 등)
    - ✓ 이메일 → 본문 링크 (URL 등), 첨부파일
    - ✓ 압축 파일 → 패스워드 기반 압축파일 자동 해제
      → 압축 Depth-Level 제한 없음
  - 특징 – 링크 또는 파일에서 추출되는 추가적인 오브젝트 모두 분석

코어 모듈 요약 - 4

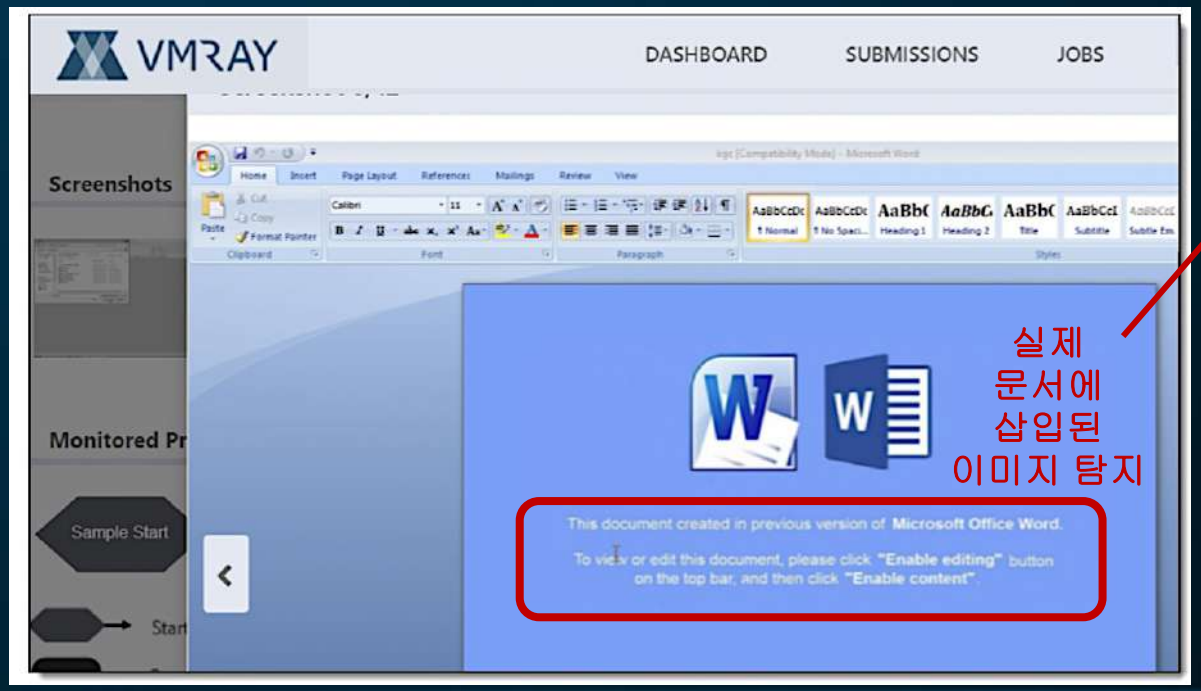


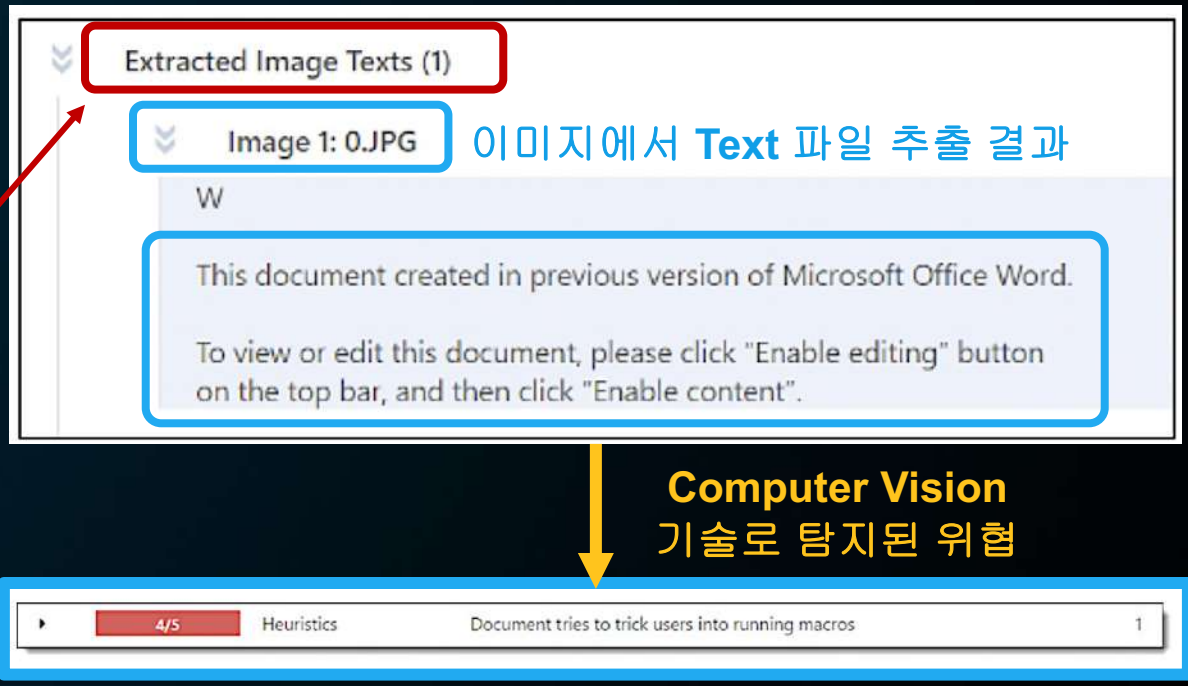
- **Password-Protected File Analysis**
  - 이메일 첨부파일이 "암호 보호된 문서" 인 경우
  - 이메일 본문/제목에서 패스워드 존재여부 자동검색
  - 단, 패스워드 Brute Force 기능은 아님
- **Macro De-Obfuscation (난독화된 매크로, 복호화 기능)**
  - 분석시간 지연 위해서 사용된 난독화된 매크로의 복호화
  - Office 파일 난독화된 매크로 복호화
  - 매크로 내부 "Dead Code" 제거
  - Malicious 매크로 탐지

코어 모듈 요약 - 5

VMRAY

- **Computer Vision**
  - 이미지에서 "Text 파일 추출" 기술
  - OCT 이용 (Optical Character Recognition)
  - 메일 피싱 캠페인 – 이미지 이용한 악의적인 소셜 엔지니어링 탐지 목적





코어 모듈 요약 - 6

VMRAY

- **VBA Stompting Detection**
  - VBA Stompting 공격 기술 탐지
  - 컴파일된 매크로 코드 (P-Code) vs. 소스코드 (VBA) 비교

VBA Macros (2)

Macro #1: Auth (source code)

Possible VBA Stomping evasion: The p-code of this macro does not match its source code. It might have been tampered with to evade detection.

```
Private Function Fennec(Noxious As String, Fox As String) As String
    Dim Sahara As Long
    Dim Desert As String
    Dim SleepyFennec As Integer, NoxiousFox As Integer
    For Sahara = 0 To Len(Fox) - 1
        SleepyFennec = Asc(Mid$(Fox, Sahara + 1, 1))
```

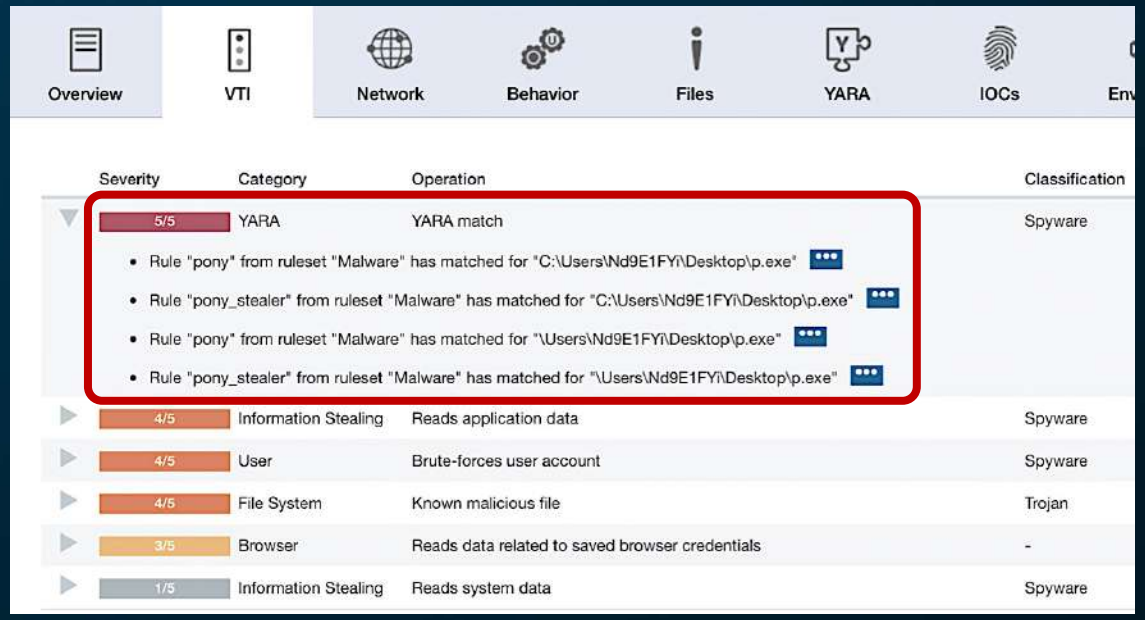
Score	Category	Operation	Count	Cla
4/5	Obfuscation	Document contains a macro whose p-code does not match its source code	1	-

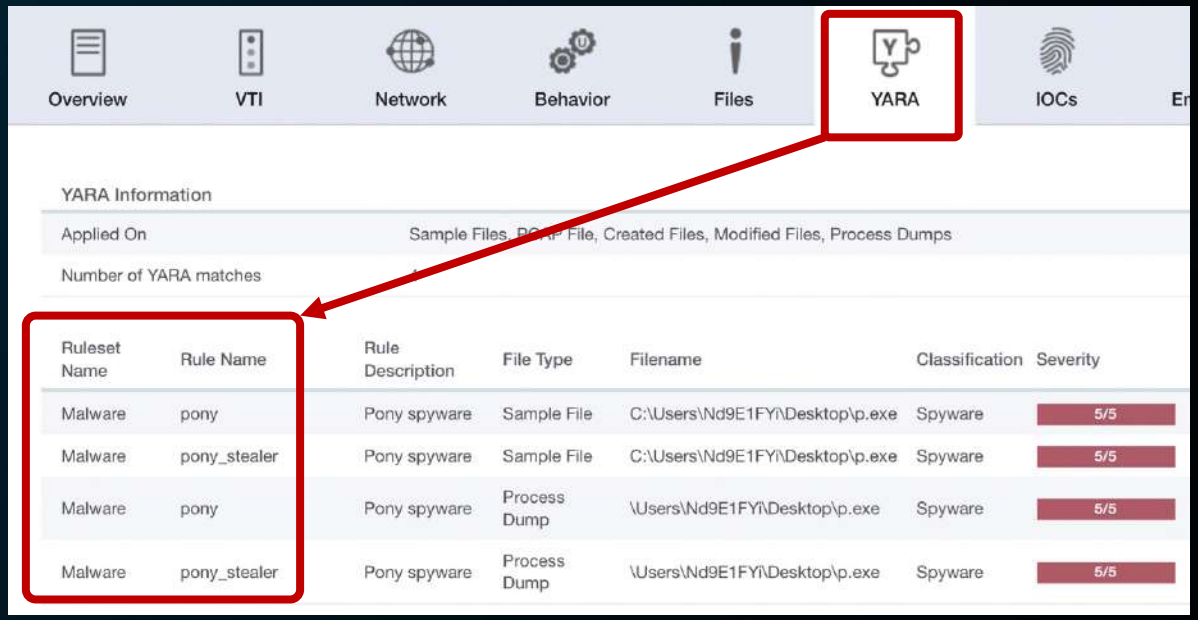
- Office document e514ebdd9ae5b5092c7eab9e334627b87f1124a5982a92b00611493987070187.doc contains a macro with p-code that does not match its source code

코어 모듈 요약 - 7

VMRAY

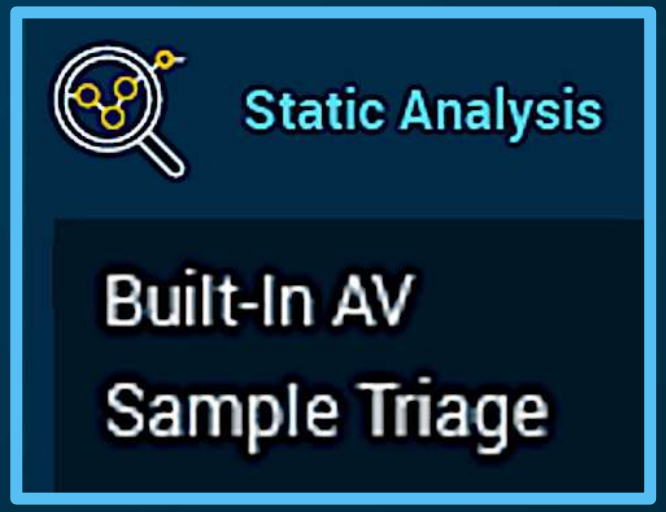
- **YARA Rulesets**
  - 파일에 특정 Characteristics 포함 여부 탐지
  - Static / Dynamic 분석중에 추출된, 모든 오브젝트 스캔할 때 사용됨





코어 모듈 요약 - 8

VMRAY



- **Built-In AV (빌트인 안티바이러스)**
  - AVCore + BitDefender 듀얼 엔진
  - Static / Dynamic 분석중에 추출된 모든 오브젝트 스캔할 때 사용
  - Content-based AV 엔진
    - ✓ Signaturer
    - ✓ Behavior 기반 휴리스틱. (Dynamic File / Dynamic Web 분석)

- **Sample Triage (샘플 필터링 기능)**
  - 분석 성능 최적화 위해, 사전 샘플 필터링 기능
    - ✓ Known Clear (Benign) 파일
    - ✓ No Active Content 파일
    - ✓ PDF with non-standard 구조 파일
    - ✓ Clear (Benign) 매크로 포함된 문서 파일

코어 모듈 요약 - 9

- **Smart Link Detonation**
  - VMRay Web Analysis 기술 이용해서, "이메일 / 문서" 에 삽입된 링크를 추가 분석할 것인지 결정하는 Attribute-Based Rule
  - 어떤 유형의 Link 가 분석 대상인가 ?
    - ✓ "File" 에서 추출된 Link
    - ✓ "Email 본문" 에서 추출된 Link
    - ✓ "Email 첨부 파일" 에서 추출된 Link
  - Link 의 어떤 부분을 분석하는가 ?
    - ✓ Domain Age
    - ✓ Reputation Score
    - ✓ Abnormal URL 등 ...

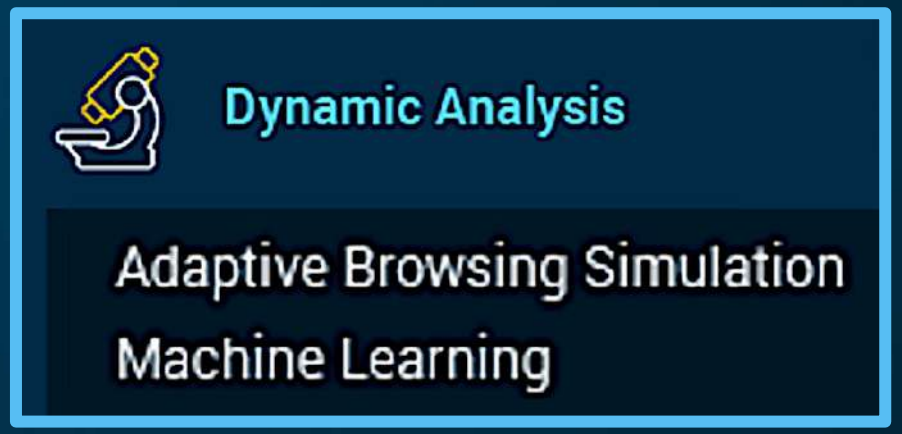
코어 모듈 요약 -10

VMRAY

- **Digital Signature Verification (인증서 싸이닝 유효성 검증)**
  - PE 샘플 Digital Signature 유효성 검증
  - Revoked Certificate 여부 체크
  - Static Analysis 기법에 포함
  - CRL (Certificate Revoke List) 체크
  - 만약, Revoked Certificate 로 싸이닝 한 샘플인 경우, VTI (VMray Threat Indicator) Rule 작동함

코어 모듈 요약 -11

VMRAY

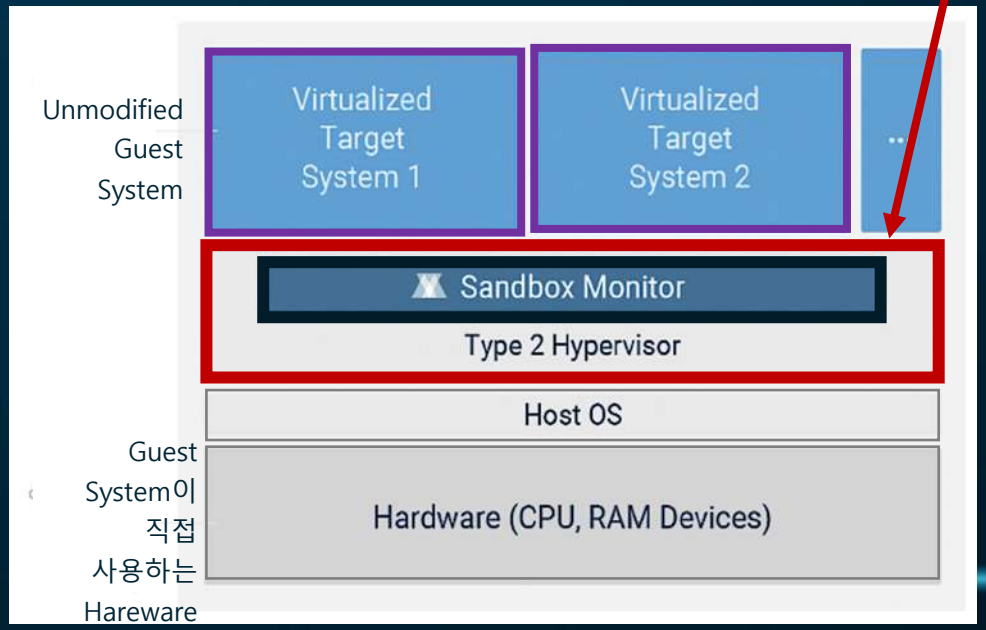


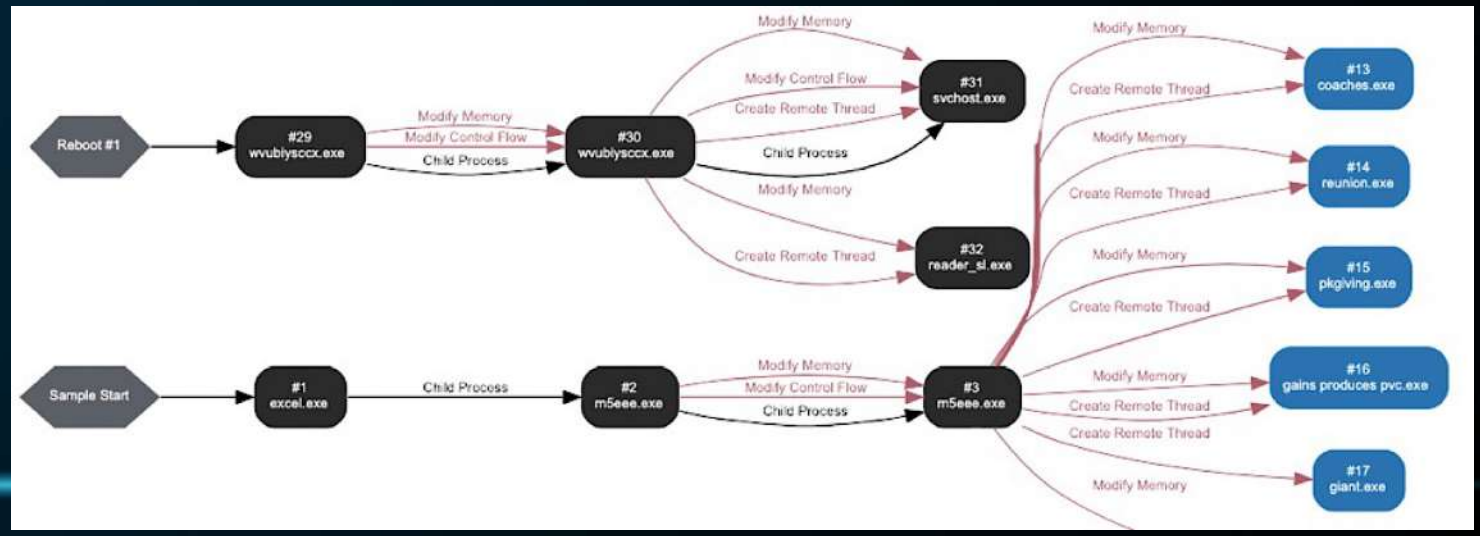
- **Adaptive Browsiing Simulation**
  - 특정 웹기반 피싱 공격은 사용자가 실제로 "버튼 클릭" 할때만 다음 프로세스가 트리거 되도록 설계됨
  - 이런 경우, " 자동 버튼 탐지 / 클릭 수행 " 하여 다음 단계의 "Payload Delivery 를 트리거" 하도록 유도
- **Machine Learning**
  - 웹기반 피싱 위협 식별 목적으로 작동
  - Dynamic Web Analysis 결과에 대해서, 머신러닝 분석 기술 적용

코어 모듈 요약 - 12

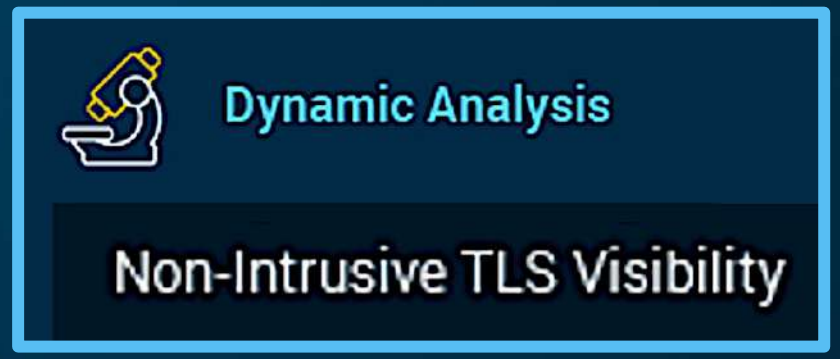
VMRAY

- **Intelligent Monitoring**
  - VMRay Dynamic File Analysis 핵심 기능
  - Hypervisor Layer 에서, 독립적으로 실행 / 모든 인터랙션 모니터링
    - ✓ 샌드박스 회피 기능의 멀웨어가 인지하지 못함
  - Noise-Free 분석 레포트 생성
  - ITM 기술 적용 (Intermodular Transition Monitoring)
    - ✓ 멀웨어 실제 행위 vs. 시스템의 정상적인 이벤트 정확히 분류



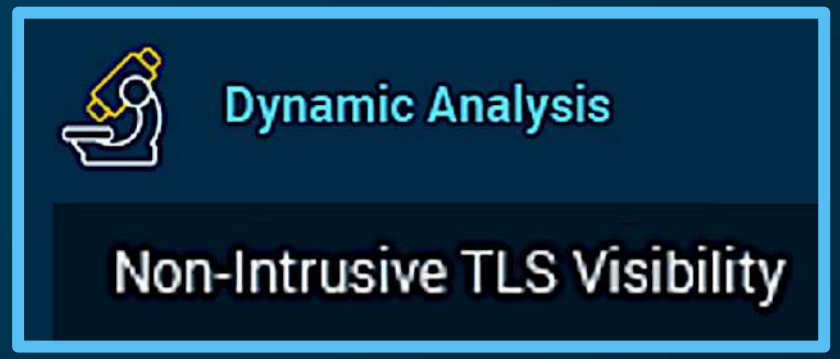


코어 모듈 요약 – 13 (1)



- **Non-Intrusive TLS Visibility**
  - VM 내부에서 "TLS / SSL" 트래픽 복호화 기능
  - 멀웨어의 외부 C2 서버와의 "TLS/SSL" 트래픽 분석
  - Hypervisor Layer 에서 실행 → 멀웨어가 인지하지 못함
  - 참고
    - ✓ 타 샌드박스 처럼, MITM 기반 복호화 / API 후킹 사용 안함
    - ✓ VM 내부 환경변화 없이, 투명하게 복호화 수행
    - ✓ 암호화된 트래픽 자체 저장 → Hypervisor 메모리 분석 후, "키 추출" → 멀웨어 실행 완료이후, 저장된 트래픽 대상으로 추출된 키로 복호화 수행
  - 정확한 URL 정보 획득
  - 다운로드 된, "Payload 정보" 확인 및 2차 Static / Dynamic 분석

코어 모듈 요약 – 13 (2)

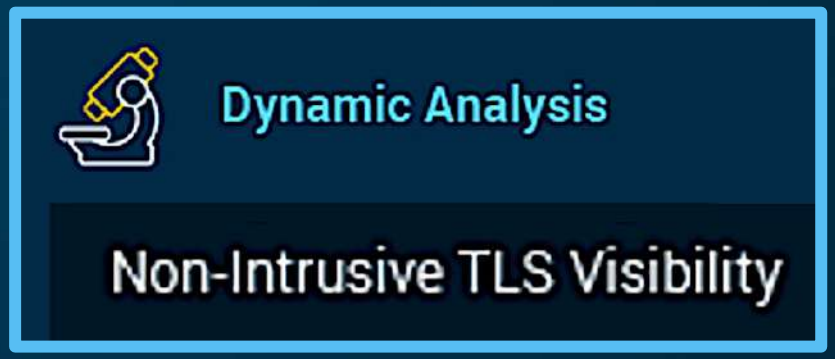


- **Non-Intrusive TLS Visibility**
  - PCAP 파일 다운로드 기능
    - ✓ TLS 복호화 중, 추출된 "Key Material" 이용해서
    - ✓ "Shared Secret" 을 포함함 "Key Log File" 생성 후, PCAP 파일에 자동으로 Embed 시킴
  - 위 PCAP 파일을 "WireShark 연계" 분석 시 장점은?
    - ✓ "Key Log File" 이용한 TLS 복호화 기능지원
    - ✓ 복호화 이후, 상세 트래픽 분석가능

코어 모듈 요약 – 13 (3)

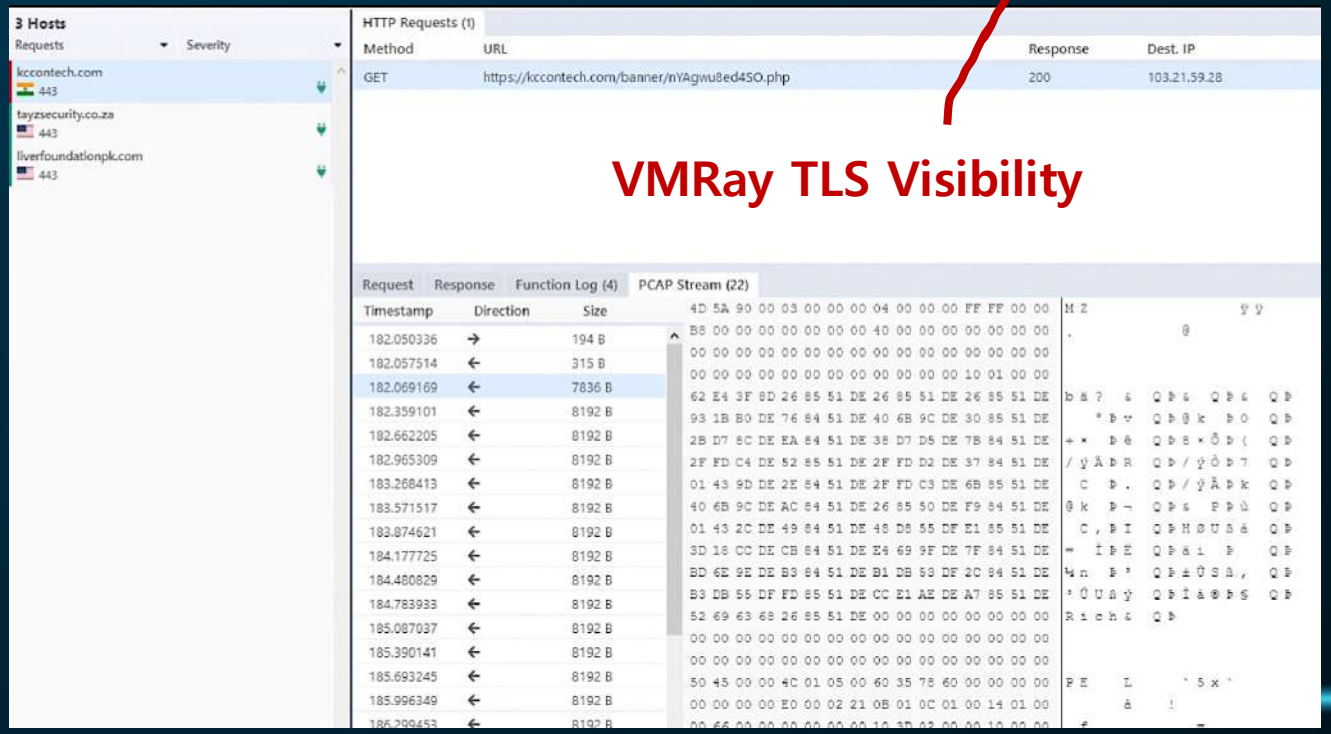
VMRAY

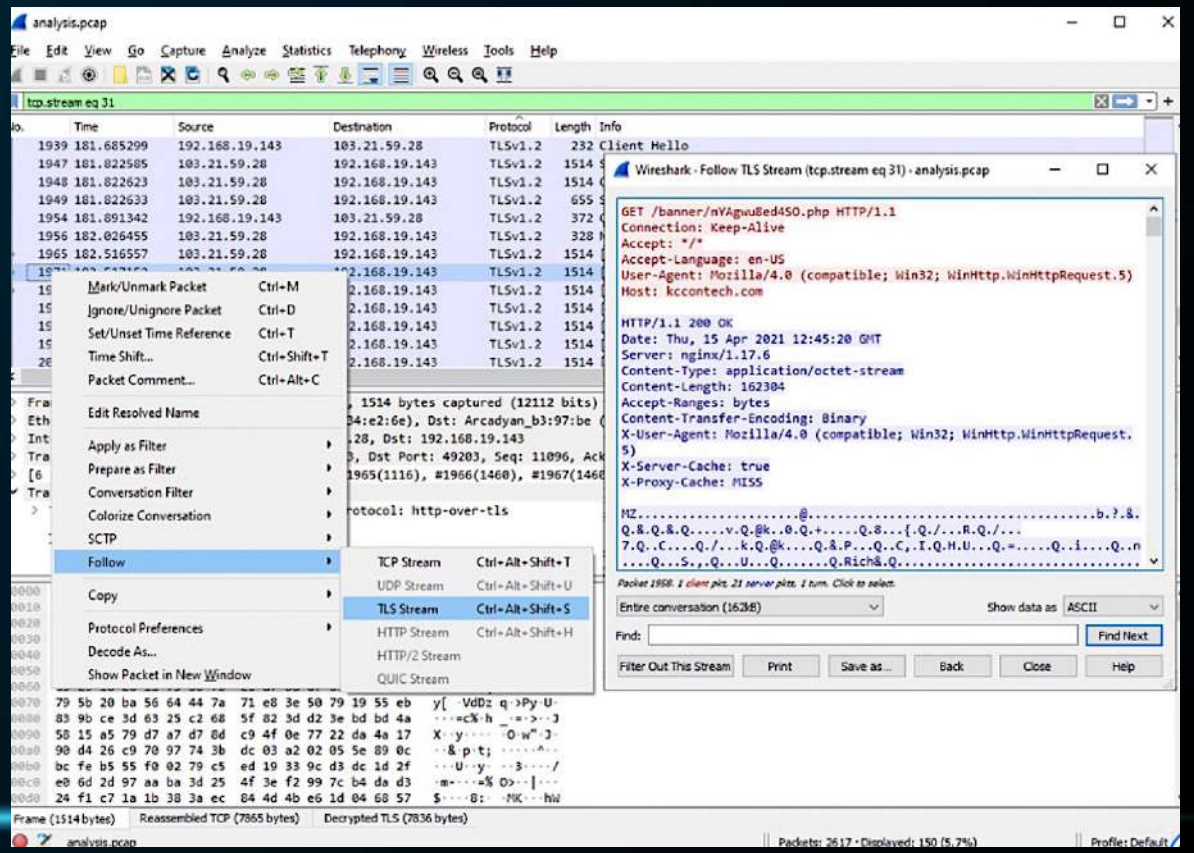
- Non-Intrusive TLS Visibility



VMRay 에서
Key Log File 연계한 PCAP 추출 파일로
WireShark
TLS Stream 분석

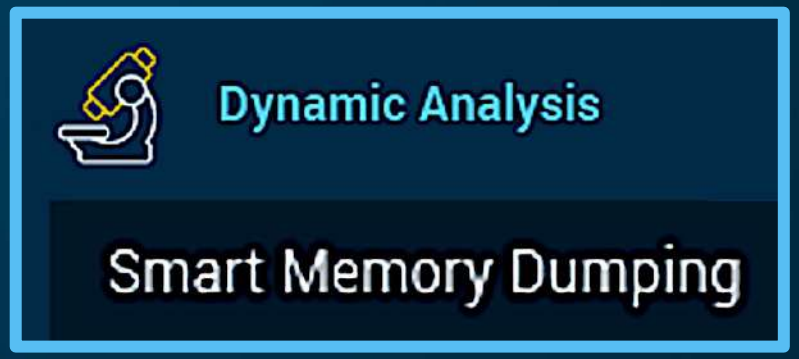
VMRay TLS Visibility





코어 모듈 요약 - 14

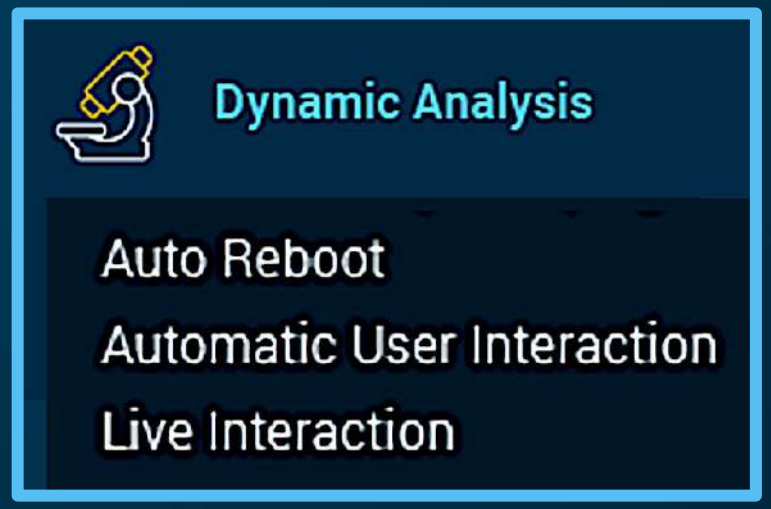
VMRAY



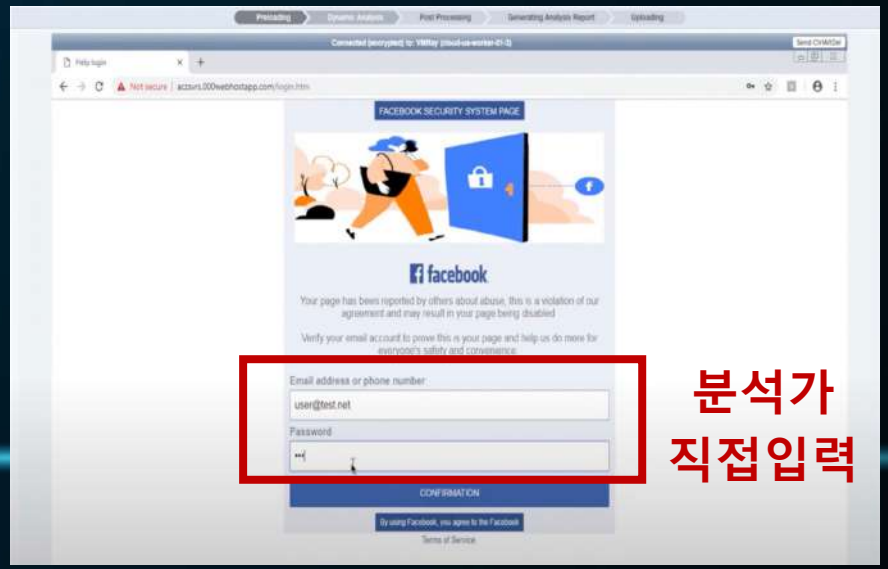
- **Smart Memory Dumping**
  - 실시간 모든 멀웨어 행위, 메모리 덤프 및 저장
  - IDA Plugin 이용 → 추가 분석 지원
  - 참고 – 멀웨어가 사용하는 Evasion (회피) 일반 기술
    - ✓ Compress (압축), Encrypt (암호화), Obfuscation (난독화)
    - ✓ 하지만, 위 모든 기술들도 메모리 상에서는 모두 복호화 및 정상 작동함
  - VMRay Smart Memory Dumping 은 실시간 메모리 모니터링 및 Rule Trigger 수행
    - ✓ Private Memory Region / Buffer → 실행파일 마킹될 때
    - ✓ Memory Region 에서, Code 실행될 때
    - ✓ Memory Region 에, Write (쓰기) 될 때

코어 모듈 요약 - 15

VMRAY



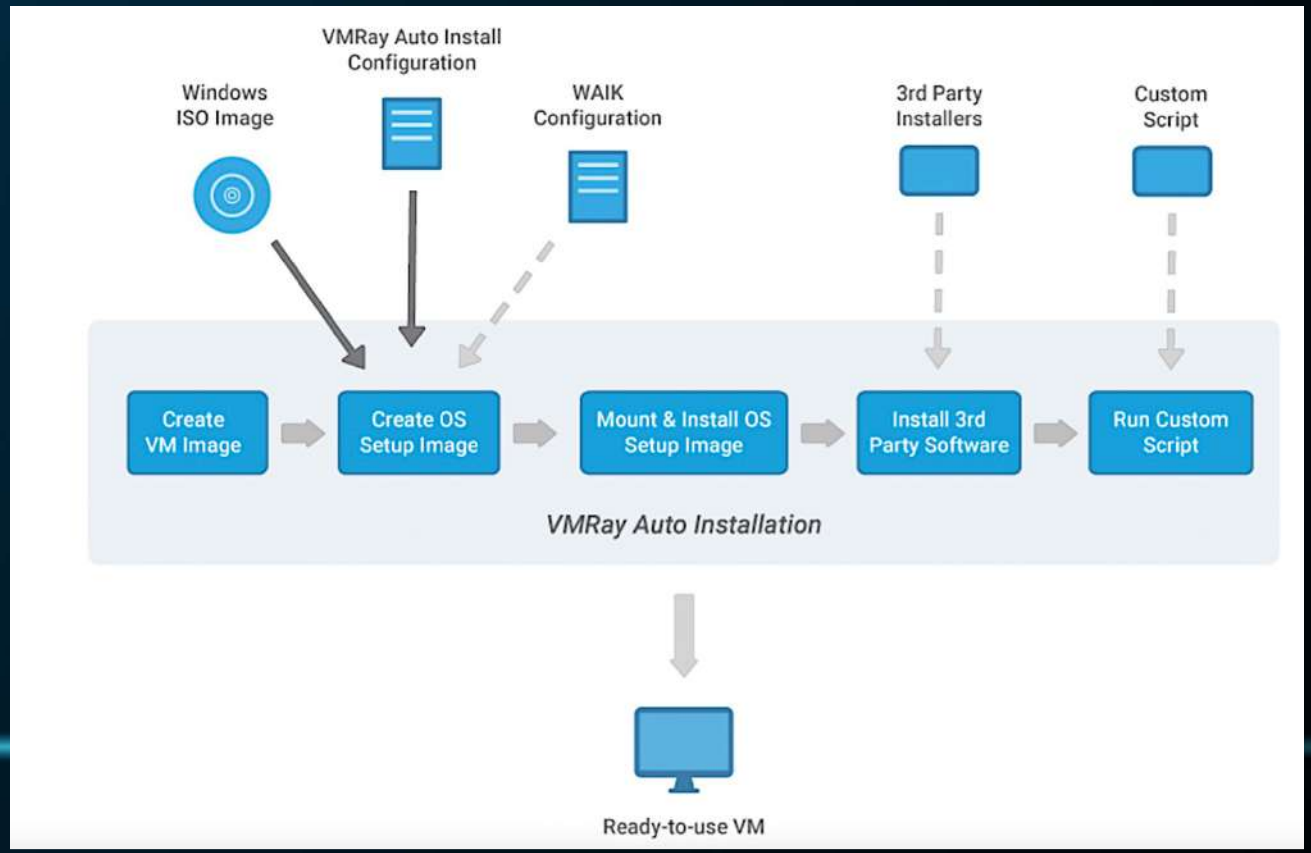
- **Auto Reboot**
  - 분석 중, "Auto Start" 기능 탐지 시, 다음 분석 위해서 자동 리부팅
- **Automatic User Interaction**
  - 멀웨어가 실제 사용자 개입을 요청하는 단계를 포함하는 경우, 자동으로 사용자 행위 Simulation 수행
    - ✓ 자동 마우스 컨트롤, 자동 클릭, 자동 대화형박스 클릭
- **Live Interaction**
  - 분석가가 직접 수동으로 개입하면서, 멀웨어 분석



코어 모듈 요약 - 16

VMRAY

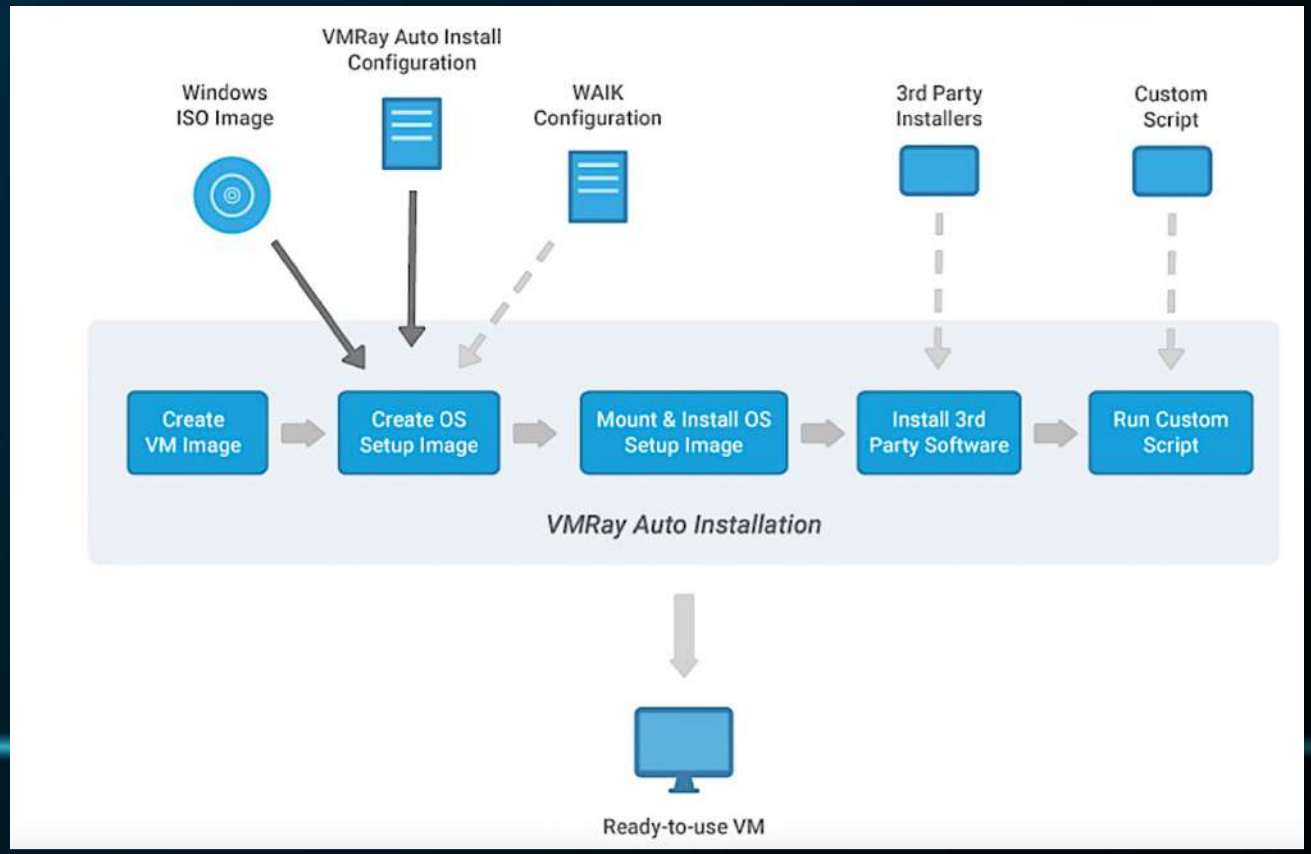
- **Golden Images**
  - 실제 사용자 환경 OS 이미지 배포 기능
  - On-Prem 아키텍쳐에서만 지원
  - 주로, 사고 분석.대응 목적으로 악성코드 분석할 때, 활용



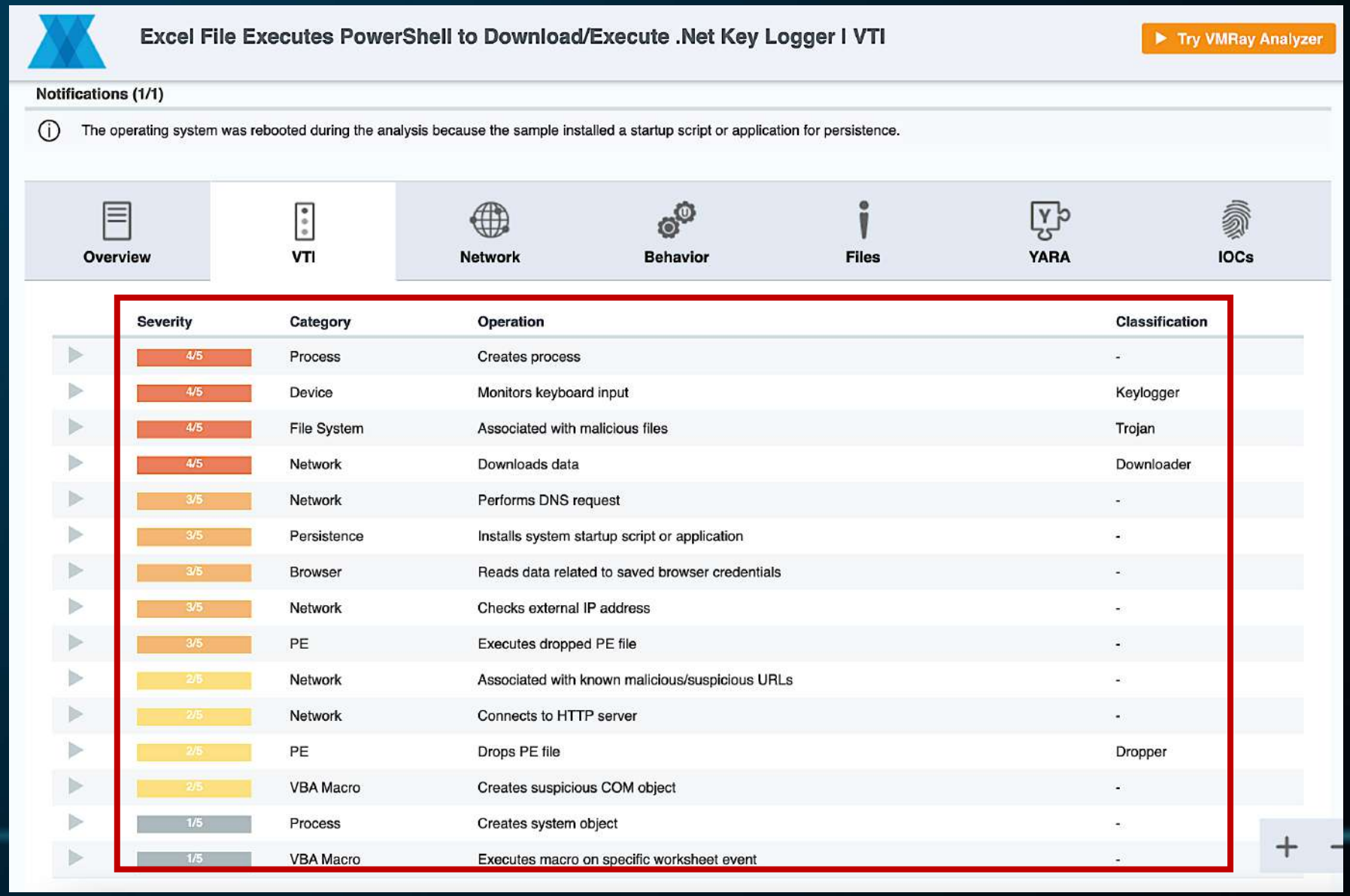
코어 모듈 요약 - 17

VMRAY

- **Golden Images**
  - 실제 사용자 환경 OS 이미지 배포 기능
  - On-Prem 아키텍쳐에서만 지원
  - 주로, 사고 분석.대응 목적으로 악성코드 분석할 때, 활용



기능 스크린샷 – 엑셀 → 파워쉘 → 키로거 드롭

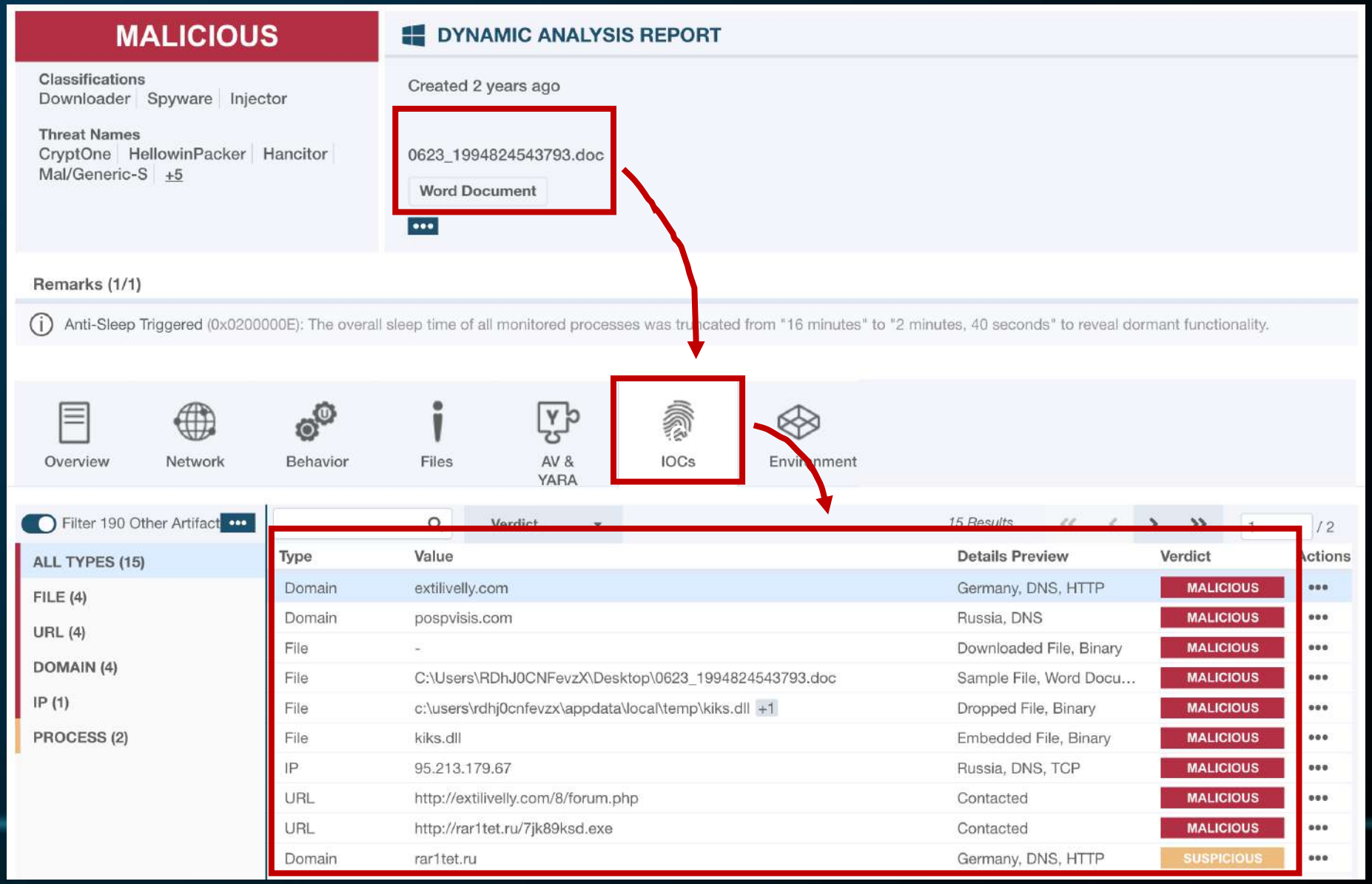


Severity	Category	Operation	Classification
4/5	Process	Creates process	-
4/5	Device	Monitors keyboard input	Keylogger
4/5	File System	Associated with malicious files	Trojan
4/5	Network	Downloads data	Downloader
3/5	Network	Performs DNS request	-
3/5	Persistence	Installs system startup script or application	-
3/5	Browser	Reads data related to saved browser credentials	-
3/5	Network	Checks external IP address	-
3/5	PE	Executes dropped PE file	-
2/5	Network	Associated with known malicious/suspicious URLs	-
2/5	Network	Connects to HTTP server	-
2/5	PE	Drops PE file	Dropper
2/5	VBA Macro	Creates suspicious COM object	-
1/5	Process	Creates system object	-
1/5	VBA Macro	Executes macro on specific worksheet event	-

기능 스크린샷 – Non-PE 문서파일 분석

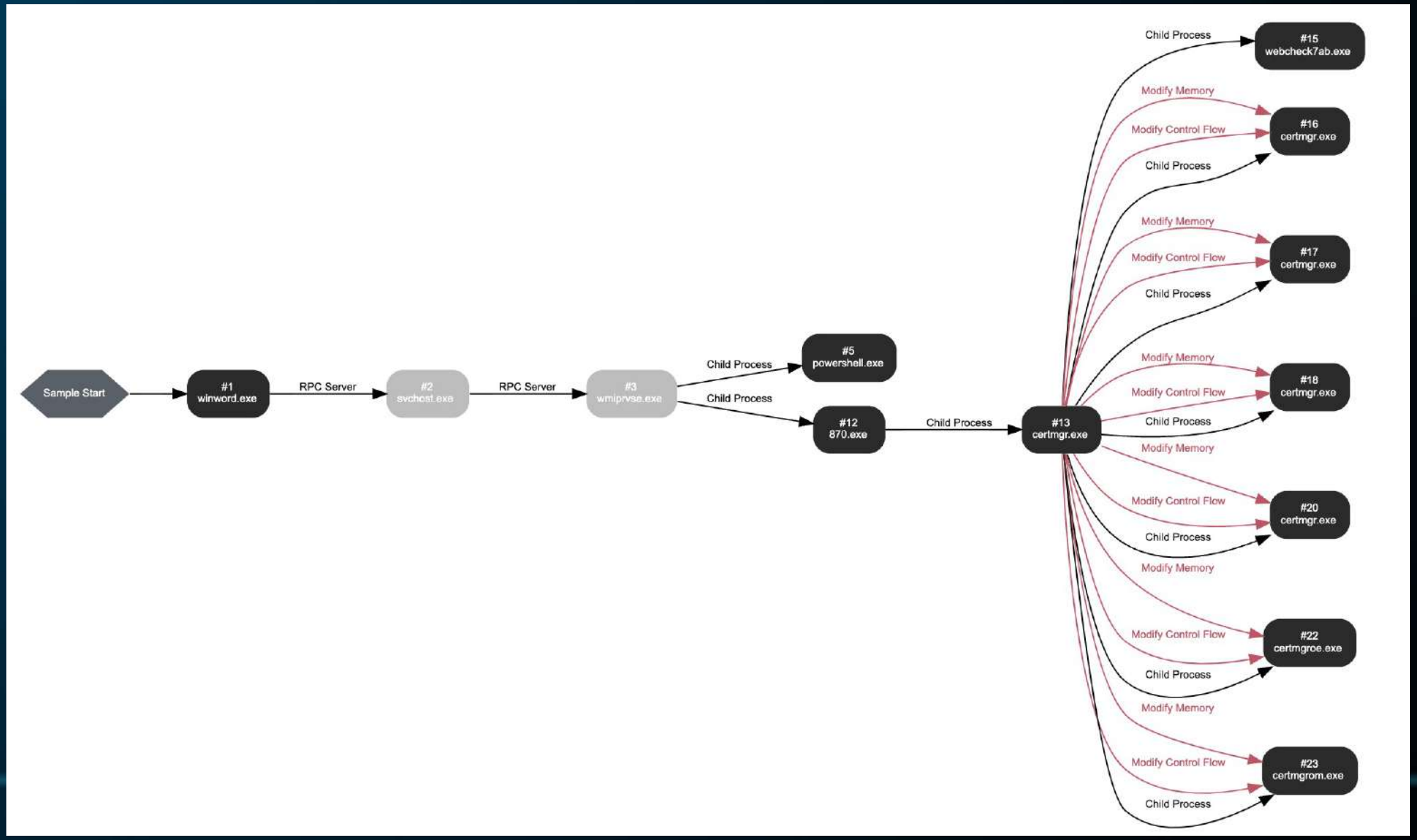
VMRAY

- **Word 파일**
- **추출된 IOC**
  - ✓ Domain
  - ✓ File
  - ✓ IP
  - ✓ URL



기능 스크린샷 – 이모텟 (프로세스 행위 탐지)

VMRAY



기능 스크린샷 – Readable Threat Identifiers

VMRAY

VMRay Threat Identifiers (36 rules, 98 matches)

Severity	Category	Operation	Count	Classification
5/5	Defense Evasion	Obscures a file's origin	1	-
5/5	Antivirus	Malicious content was detected by heuristic scan	10	-
5/5	Injection	Writes into the memory of a process running from a created or modified executable	3	-

- "c:\users\aetadzjz\appdata\local\msvcr100\certmgr.exe" modifies memory of "c:\users\aetadzjz\appdata\local\msvcr100\certmgr.exe". •••
- "c:\users\aetadzjz\appdata\local\msvcr100\certmgr.exe" modifies memory of "c:\users\aetadzjz\appdata\local\msvcr100\certmgroe.exe". •••
- "c:\users\aetadzjz\appdata\local\msvcr100\certmgr.exe" modifies memory of "c:\users\aetadzjz\appdata\local\msvcr100\certmgrom.exe". •••

5/5	Injection	Modifies control flow of a process running from a created or modified executable	3	-
5/5	YARA	Malicious content matched by YARA rules	4	Spyware

- Rule "MailPassview" from ruleset "PUAs" has matched on a memory dump for process "certmgr.exe". •••
- Rule "EmotetMAPI" from ruleset "Malware" has matched on a memory dump for process "certmgr.exe". •••
- Rule "EmotetMAPI" from ruleset "Malware" has matched on a memory dump for process "certmgroe.exe". •••
- Rule "EmotetMAPI" from ruleset "Malware" has matched on a memory dump for process "certmgrom.exe". •••

5/5	Data Collection	Exhibits Spyware behavior	1	Spyware

- Tries to read sensitive data of: Google Talk, SeaMonkey, Vivaldi, Google Chrome, Mozilla Firefox, Google Desktop, Internet Explorer, IncrediMail, Internet Explorer / Edge, Windows Mail, Yandex Browser, Safari, Microsoft Outlook, Opera.

기능 스크린샷 – 행위 기반 증거, MITRE ATT&CK

VMRAY

Screenshots

Monitored Processes

Start of Analysis

Process with activity relevant to the analysis

Process with activity not relevant to the analysis

abc Relationship between processes. 'abc' refers to the nature of the relationship

abc Successful code injection into process. 'abc' refers to the nature/type of code injection

abc Unable to determine if code injection attempt was succesful. 'abc' refers to the nature/type of code injection

abc Unsuccessful code injection into process. 'abc' refers to the nature/type of code injection

MITRE ATT&CK™ Matrix - Windows

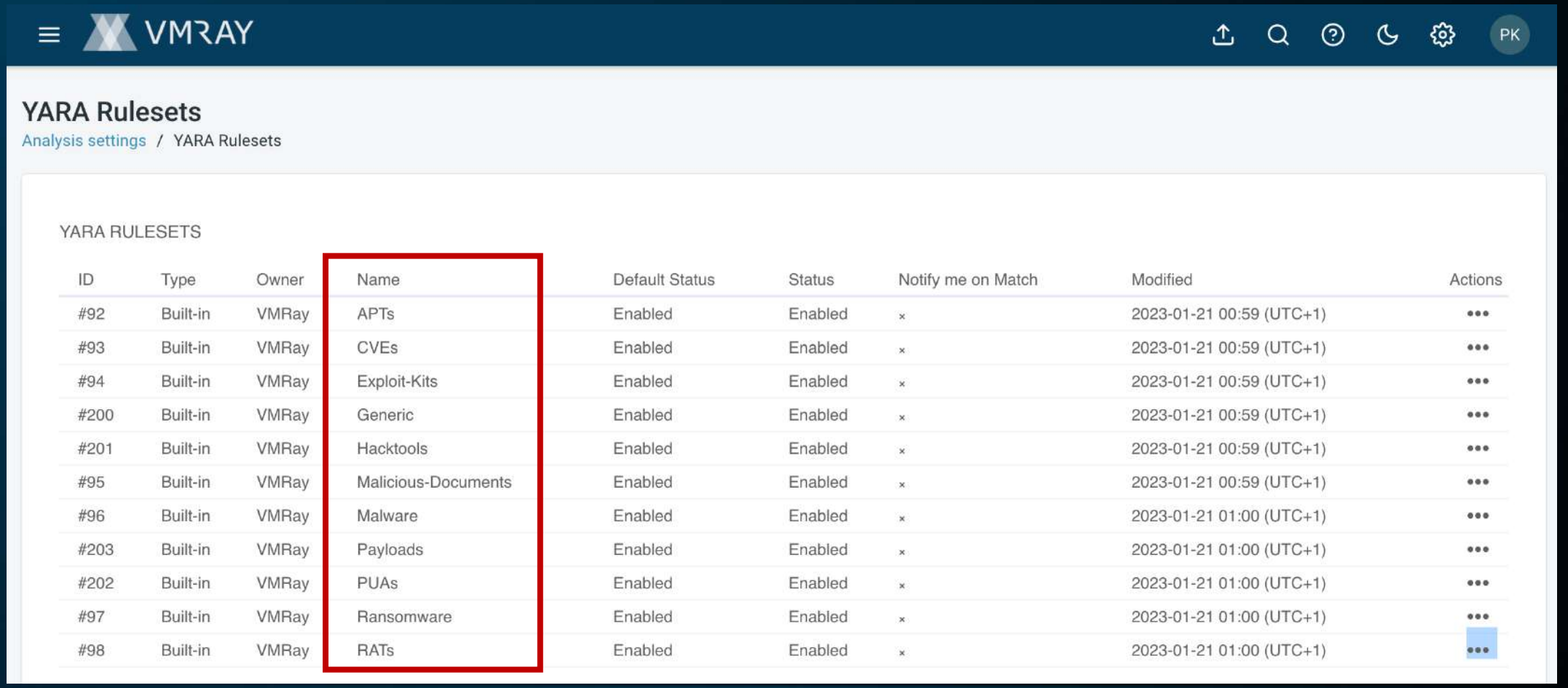
ACTIVE ALL

Version: 2019-04-25 20:53:07.719000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	Exploitation for Client Execution			Obfuscated Files or Information	Credentials in Registry	System Information Discovery	Remote File Copy	Automated Collection	Remote File Copy		
	Windows Management Instrumentation				Credentials in Files	File and Directory Discovery		Data from Local System	Standard Application Layer Protocol		
					Credential Dumping	System Network Configuration Discovery			Standard Cryptographic Protocol		

기능 스크린샷 – YARA Rulesets

- 카테고리 : 11개
- YARA Rule 적용 대상 파일 : 최초 Sample, Created, Modified, PCAP, Process Dump

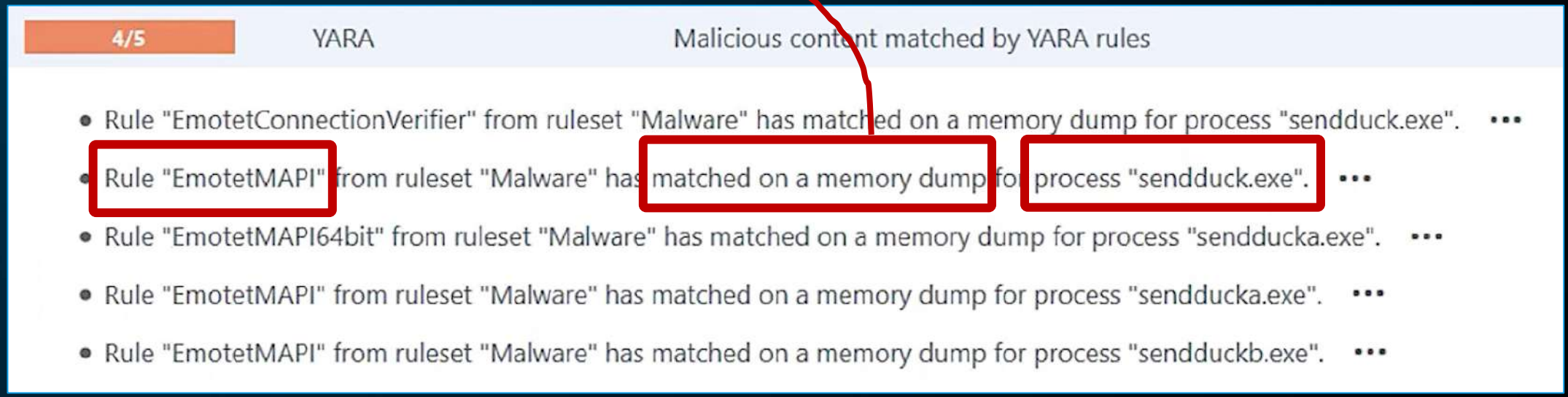


ID	Type	Owner	Name	Default Status	Status	Notify me on Match	Modified	Actions
#92	Built-in	VMRay	APTs	Enabled	Enabled	×	2023-01-21 00:59 (UTC+1)	•••
#93	Built-in	VMRay	CVEs	Enabled	Enabled	×	2023-01-21 00:59 (UTC+1)	•••
#94	Built-in	VMRay	Exploit-Kits	Enabled	Enabled	×	2023-01-21 00:59 (UTC+1)	•••
#200	Built-in	VMRay	Generic	Enabled	Enabled	×	2023-01-21 00:59 (UTC+1)	•••
#201	Built-in	VMRay	Hacktools	Enabled	Enabled	×	2023-01-21 00:59 (UTC+1)	•••
#95	Built-in	VMRay	Malicious-Documents	Enabled	Enabled	×	2023-01-21 00:59 (UTC+1)	•••
#96	Built-in	VMRay	Malware	Enabled	Enabled	×	2023-01-21 01:00 (UTC+1)	•••
#203	Built-in	VMRay	Payloads	Enabled	Enabled	×	2023-01-21 01:00 (UTC+1)	•••
#202	Built-in	VMRay	PUAs	Enabled	Enabled	×	2023-01-21 01:00 (UTC+1)	•••
#97	Built-in	VMRay	Ransomware	Enabled	Enabled	×	2023-01-21 01:00 (UTC+1)	•••
#98	Built-in	VMRay	RATs	Enabled	Enabled	×	2023-01-21 01:00 (UTC+1)	•••

기능 스크린샷 – 메모리 덤프에서 적용된 YARA

VMRAY

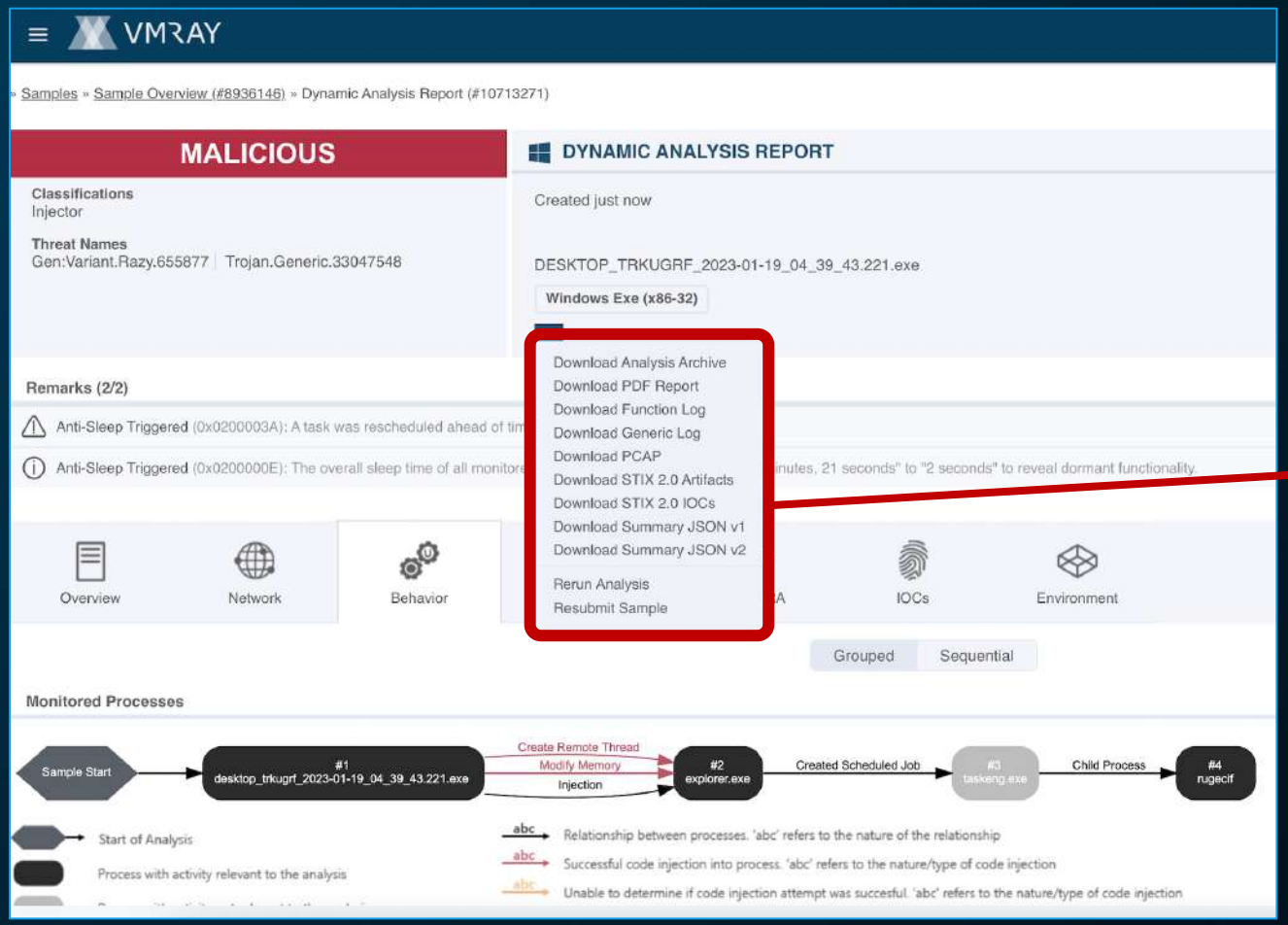
- Dynamic Analysis 수행 중,
  메모리에서 실행되는 모든 내용 저장,
  실시간 검사 및 위협 탐지 (****)



기능 스크린샷 – 상세 분석 레포트 Export

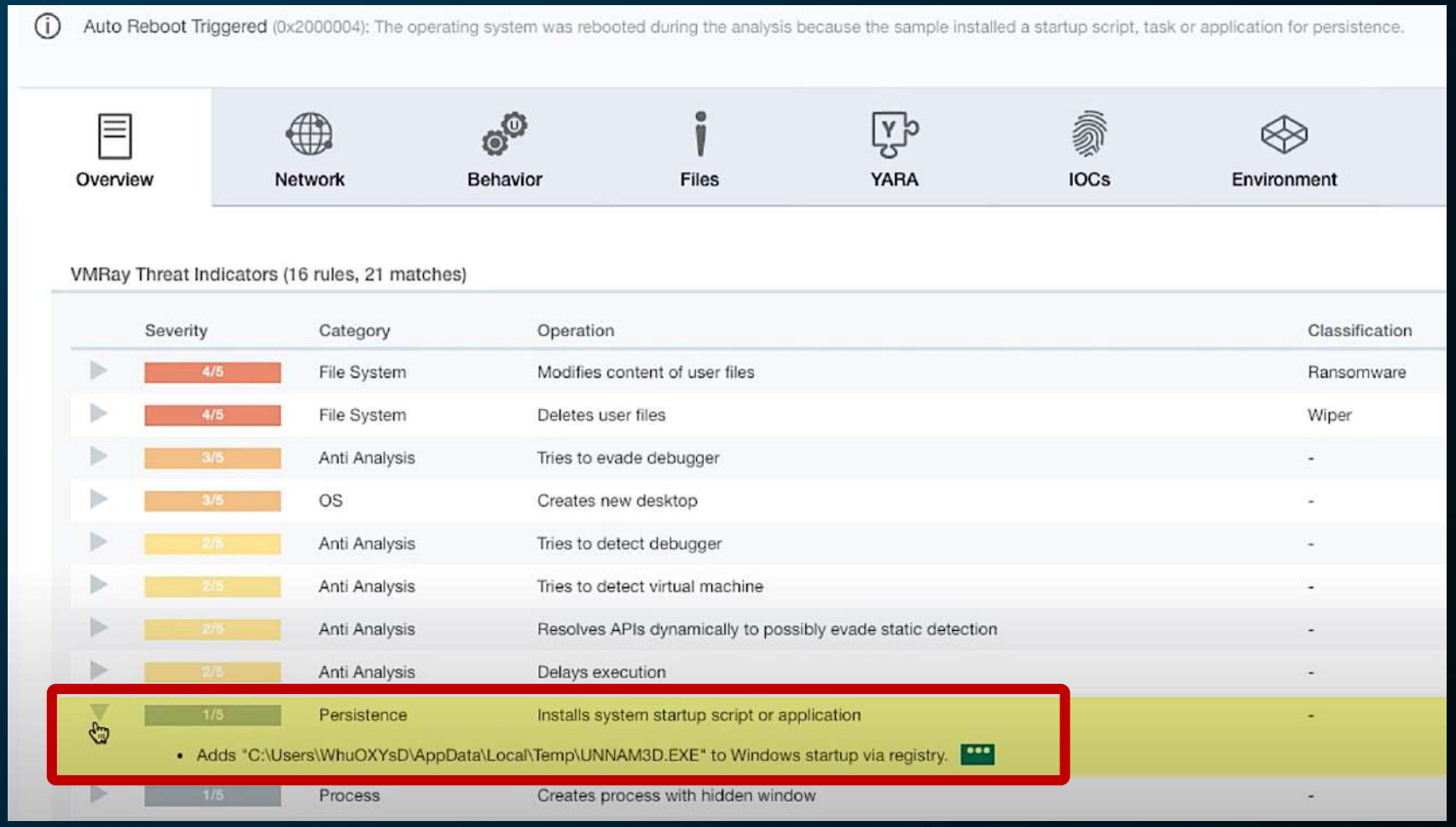
VMRAY

- 다양한 포맷 Export



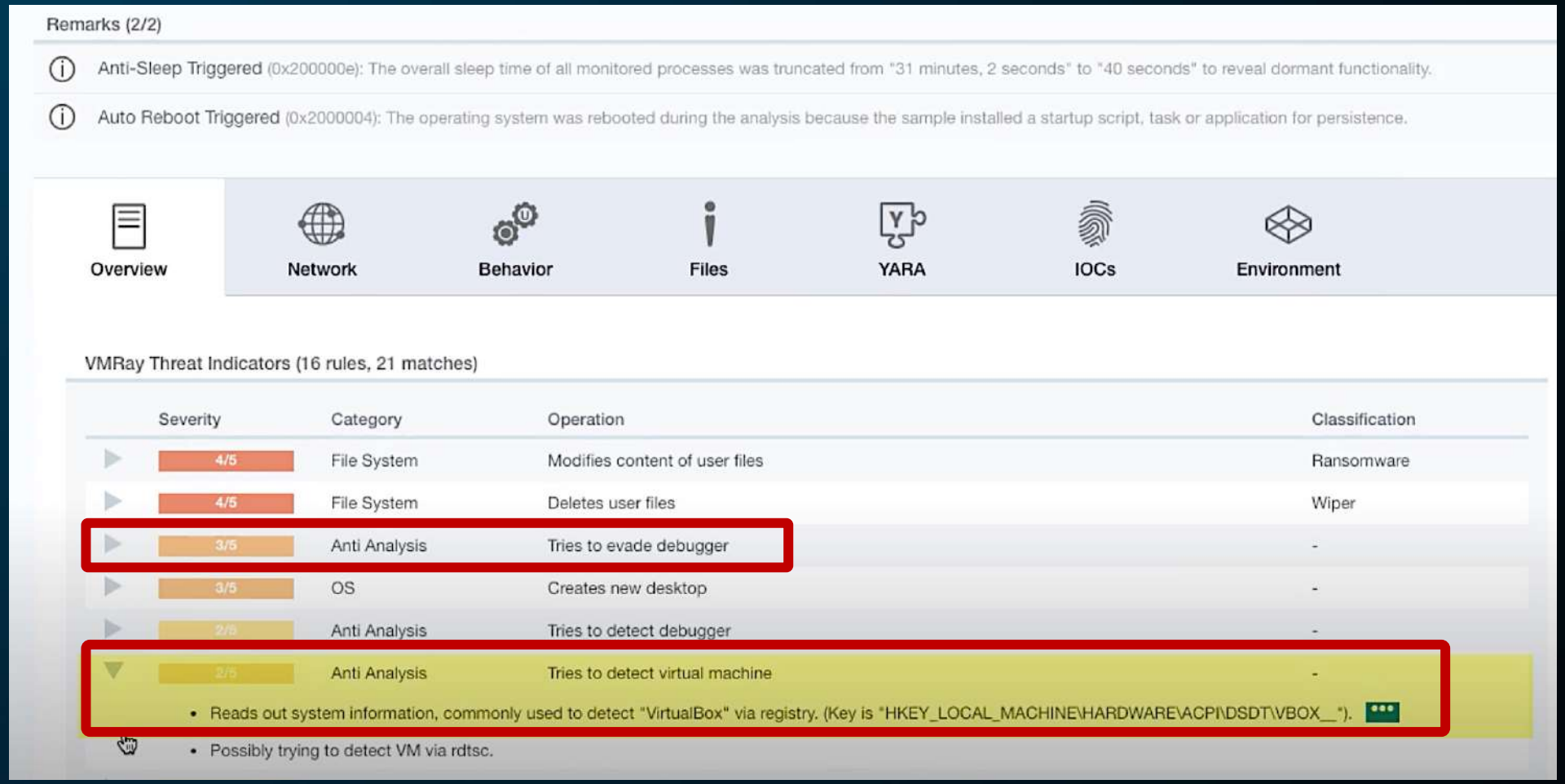
기능 스크린샷 – Persistence 인지, AutoReboot

- Persistenxe 카텍고리 "자동시작 레지스트리 " 추가 탐지 (Auto Reboot 후, 추가분석)



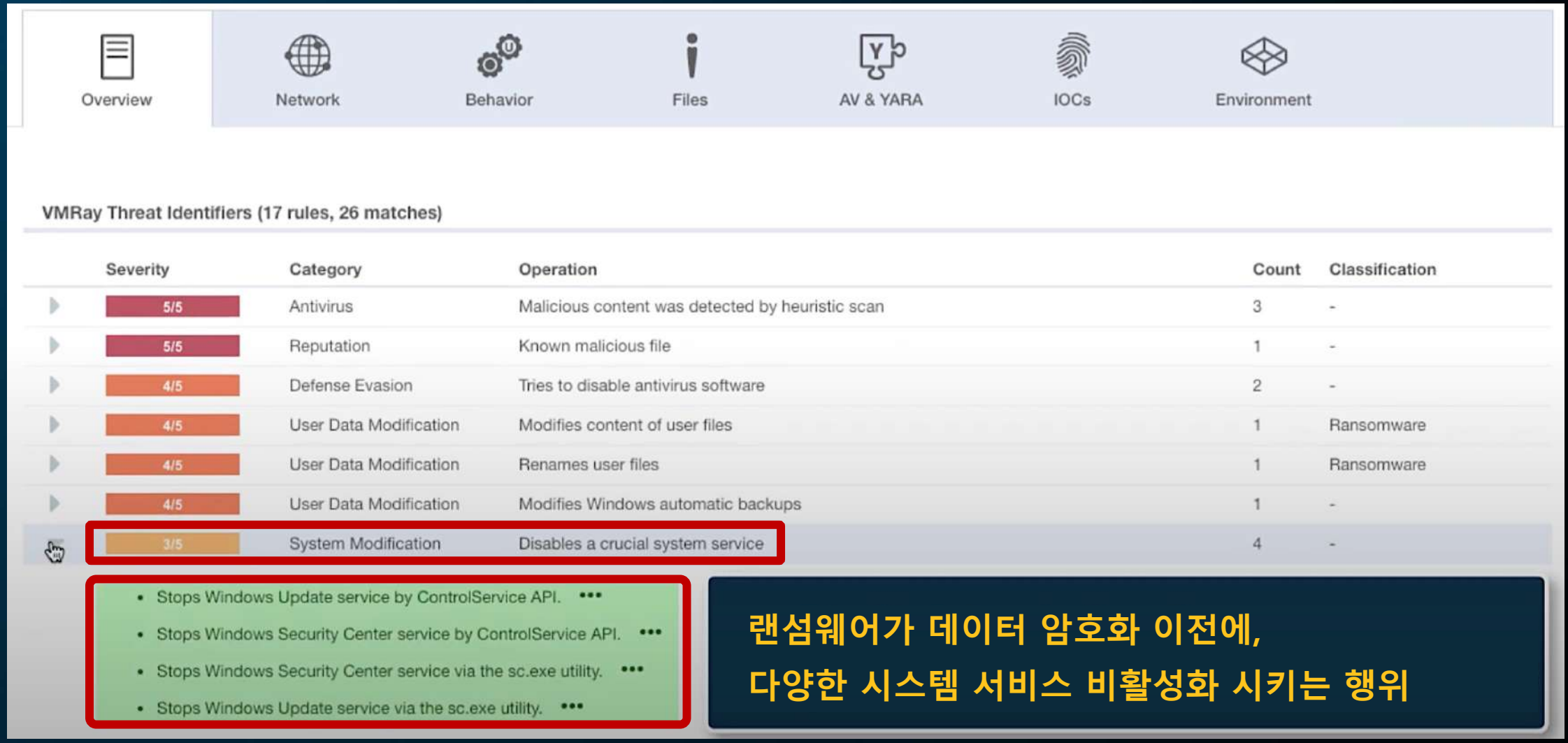
기능 스크린샷 – 다양한 회피(Evasion) 기술 탐지

- Anti-Analysis 기능 트리거 (멀웨어의 Debugger 회피 기능, Virtual Box 탐지 기능)



기능 스크린샷 – 랜섬웨어 분석 (1)

VMRAY



기능 스크린샷 – 랜섬웨어 분석 (2)

VMRAY

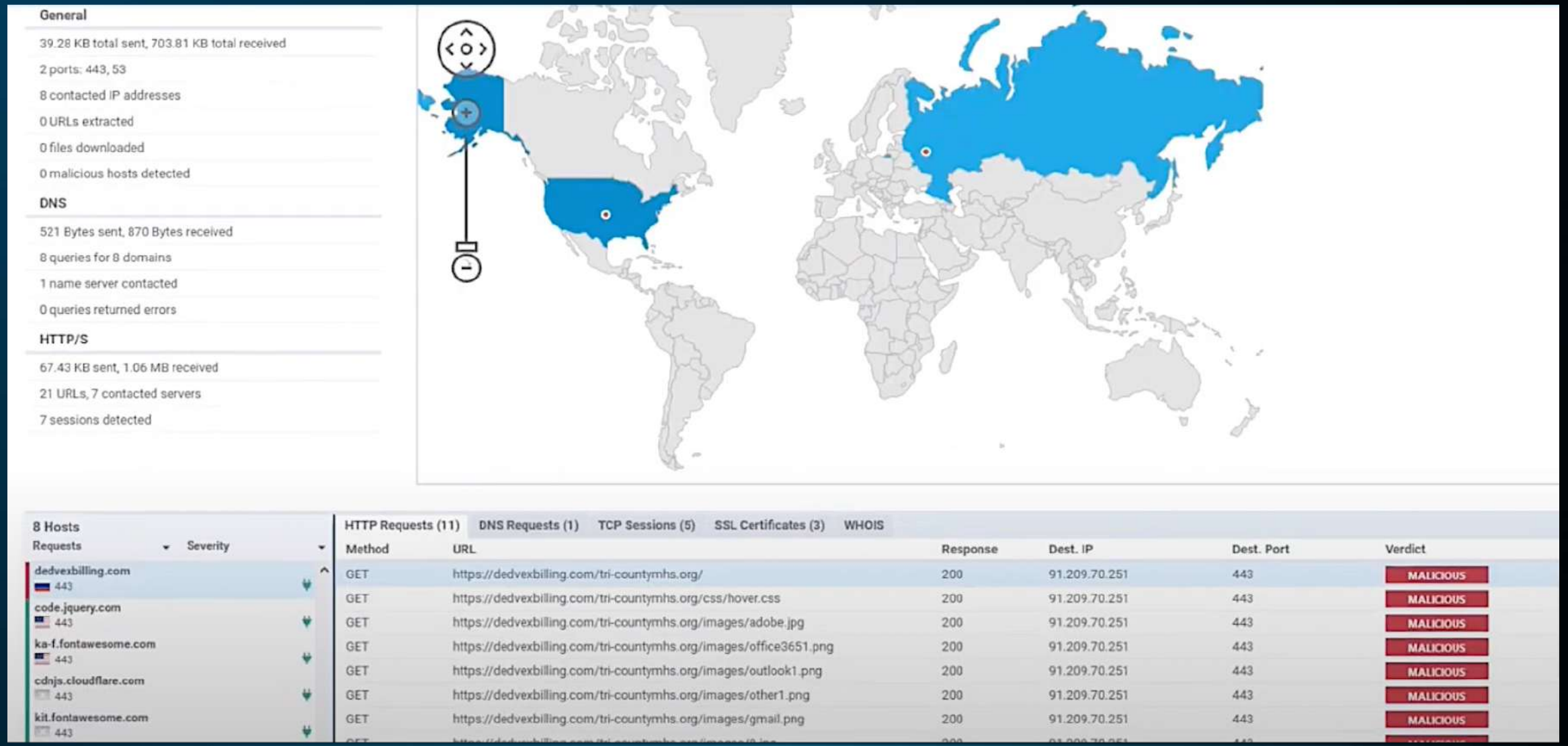
Create	sc	cmd_line = sc stop WerSvc, os_pid = 0x7c4, creation_flags = CREATE_NO_WINDOW, startup_flags = STARTF_USESHOWWINDOW, show_window = SW_HIDE	✓	1	FN
Create	cmd.exe	cmd_line = cmd.exe /c bcdedit /set {default} recoveryenabled No, os_pid = 0x7d0, creation_flags = CREATE_NO_WINDOW, startup_flags = STARTF_USESHOWWINDOW, show_window = SW_HIDE	✓	1	FN
Create	cmd.exe	cmd_line = cmd.exe /c bcdedit /set {default} bootstatuspolicy ignoreallfailures, os_pid = 0x64, creation_flags = CREATE_NO_WINDOW, startup_flags = STARTF_USESHOWWINDOW, show_window = SW_HIDE	✓	1	FN
Create	cmd.exe	cmd_line = cmd.exe /c vssadmin delete shadows /all /quiet, os_pid = 0x6c0, creation_flags = CREATE_NO_WINDOW, startup_flags = STARTF_USESHOWWINDOW, show_window = SW_HIDE	✓	1	FN
Create	cmd.exe	cmd_line = cmd.exe /c wmic shadowcopy delete, os_pid = 0x7f4, creation_flags = CREATE_NO_WINDOW, startup_flags = STARTF_USESHOWWINDOW, show_window = SW_HIDE	✓	1	FN
Create	cmd.exe	cmd_line = cmd.exe /c wbadmin delete catalog -quiet, os_pid = 0x814, creation_flags = CREATE_NO_WINDOW, startup_flags = STARTF_USESHOWWINDOW, show_window = SW_HIDE	✓	1	FN
Create	taskkill	cmd_line = taskkill /f /im MSExchange*, os_pid = 0x8d4, creation_flags = CREATE_NO_WINDOW, startup_flags = STARTF_USESHOWWINDOW, show_window = SW_HIDE	✓	1	FN
Create	C:\Users\5p5NrGJn0jS	os_pid = 0xac4, creation_flags = CREATE_NO_WINDOW, startup_flags =	✓	1	FN

랜섬웨어 추가 행위 모니터링

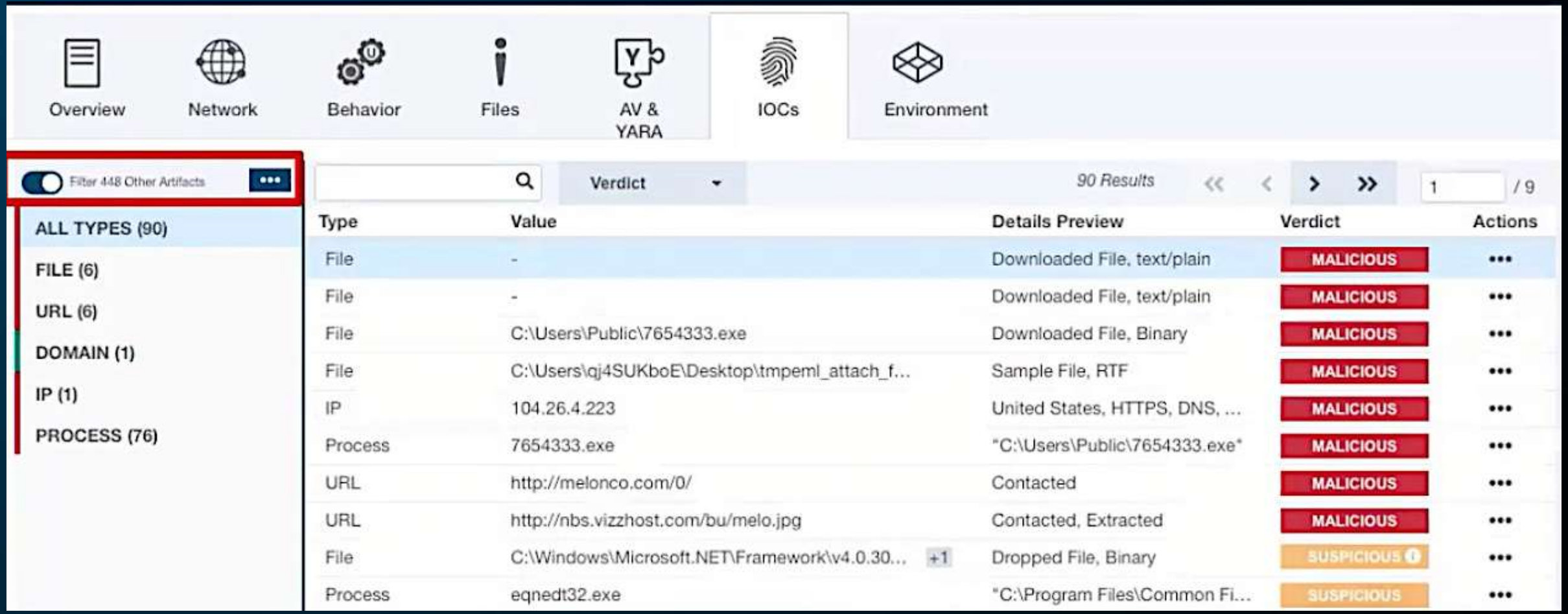
- **Shadow Copy / Backup Catalog 삭제**
- **“bcedit” 이용 및 “Windows. Recovery Mode” 비활성화**

기능 스크린샷 – 네트워크 위협 부문

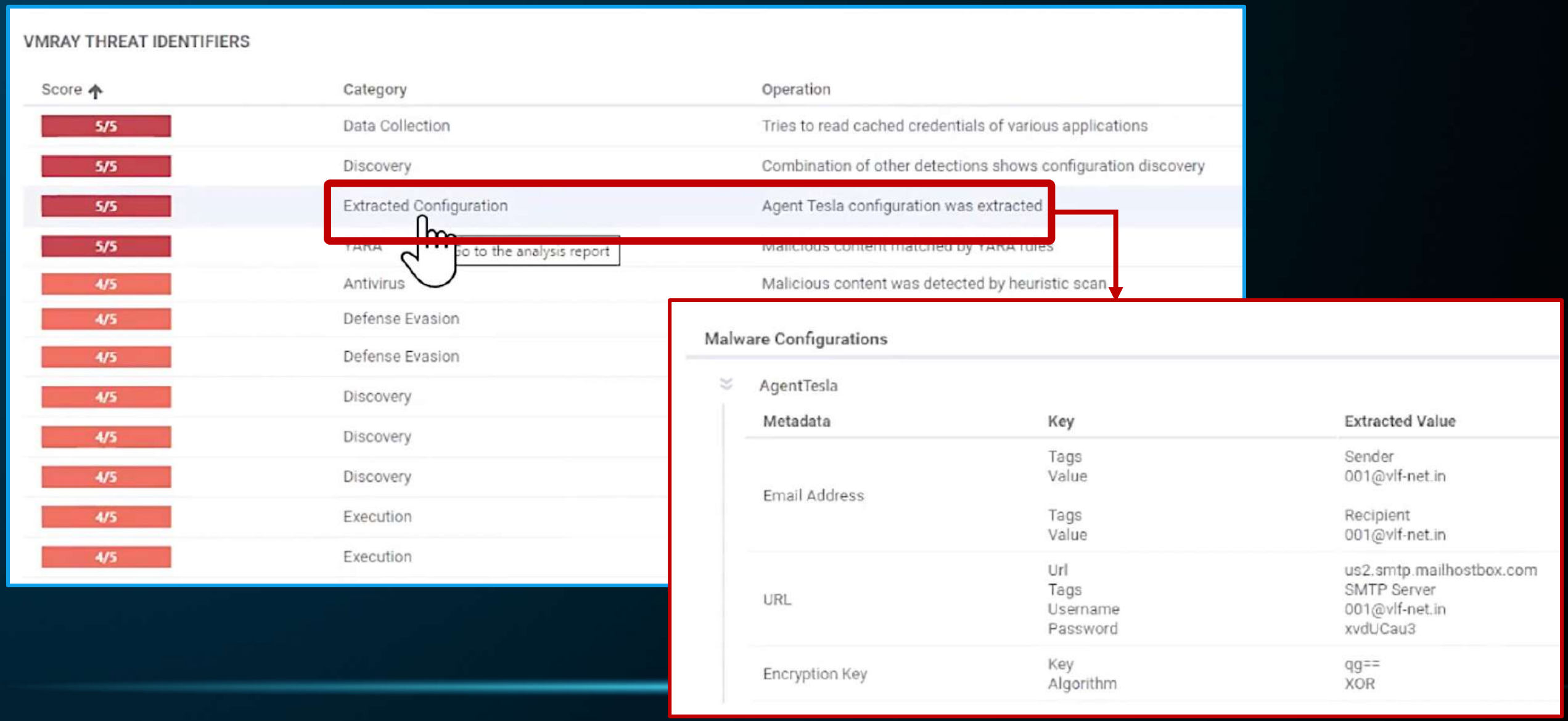
VMRAY



기능 스크린샷 – IOC 추출 (Artifact 명확히 구분)



기능 스크린샷 – 멀웨어 패밀리 (Config 자동추출)VMRAY



기능 스크린샷 – 멀웨어 패밀리 (Config 자동추출)

- **VMRay Malware Configuration Extraction 기능으로,**
  자동으로 구분되는 멀웨어 패밀리 (지속적인 업데이트 지원 **)**

- AgentTesla
- AsyncRAT
- CobaltStrike
- Emotet
- Formbook / XLoader
- Hancitor
- HawkEye
- Lokibot
- NanoCore
- njRAT
- PredatorPain
- Qbot
- Racoon
- Smoke Loader
- Racoon
- Smoke Loader
- Snake Keylogger
- Warzone
- XMRig
- IcedID
- BumbleBee
- QuasarRAT
- DanaBot

기능 스크린샷 – Hybervisor 기반 모든 Call 탐지

VMRAY

- **(X) API Hooking 기반 샌드박스**
  - 오직 후킹된 함수만 모니터링 가능 // Caller 에 의해 호출된 API 자체가 후킹되기도 함 (부정확)
- **(X) Emulator 기반 샌드박스**
  - 모든 Call 모니터링 하는 것은, 엄청난 성능 이슈 유발
- **(O) Hypervisor 기반 샌드박스**
  - 모든 Call, 성능 이슈 없이, 정확하게 모니터링 및 모든 위협 탐지 룰 적용

```
[0160.873] StrToIntExA (in: pszString="1000", dwFlags=0x0, piRet=0x1d1ab8f958 | out: pi
[0160.873] StrToIntExA (in: pszString="12", dwFlags=0x0, piRet=0x1d1ab8f958 | out: piRe
[0160.873] StrToIntExA (in: pszString="60", dwFlags=0x0, piRet=0x1d1ab8f958 | out: piRe
[0160.873] lstrlenA (lpString="WIdtM3YCfxhwrbV1") returned 16
[0160.873] lstrlenA (lpString="http://ey7kuuklgieop2pq.onion\n http://news-deck.at http
[0160.873] GetProcAddress (hModule=0x7ffaab030000, lpProcName="StrChrA") returned 0x7ff
[0160.873] StrChrA (lpStart="http://ey7kuuklgieop2pq.onion\n http://news-deck.at http:/
[0160.873] StrChrA (lpStart="http://news-deck.at http://taslks.at http://living-start.a
[0160.873] StrChrA (lpStart="http://taslks.at http://living-start.at http://ali-express
[0160.873] StrChrA (lpStart="http://living-start.at http://ali-express1.at", wMatch=0x2
[0160.873] StrChrA (lpStart="http://ali-express1.at", wMatch=0x20) returned 0x0
```

VMRay 연동 에코 시스템

고객사 기 보유중인 보안솔루션 연계 지원

VMRAY

Email Security

Member of Microsoft Intelligent Security Association
Microsoft

SIEM

splunk>
IBM Security QRadar
Microsoft Sentinel
INQUEST LABS
exabeam

Endpoint Protection EDR / XDR

vmware Carbon Black
SentinelOne
cybereason
MINERVA
Microsoft Defender for Endpoints
Cynet

SOAR

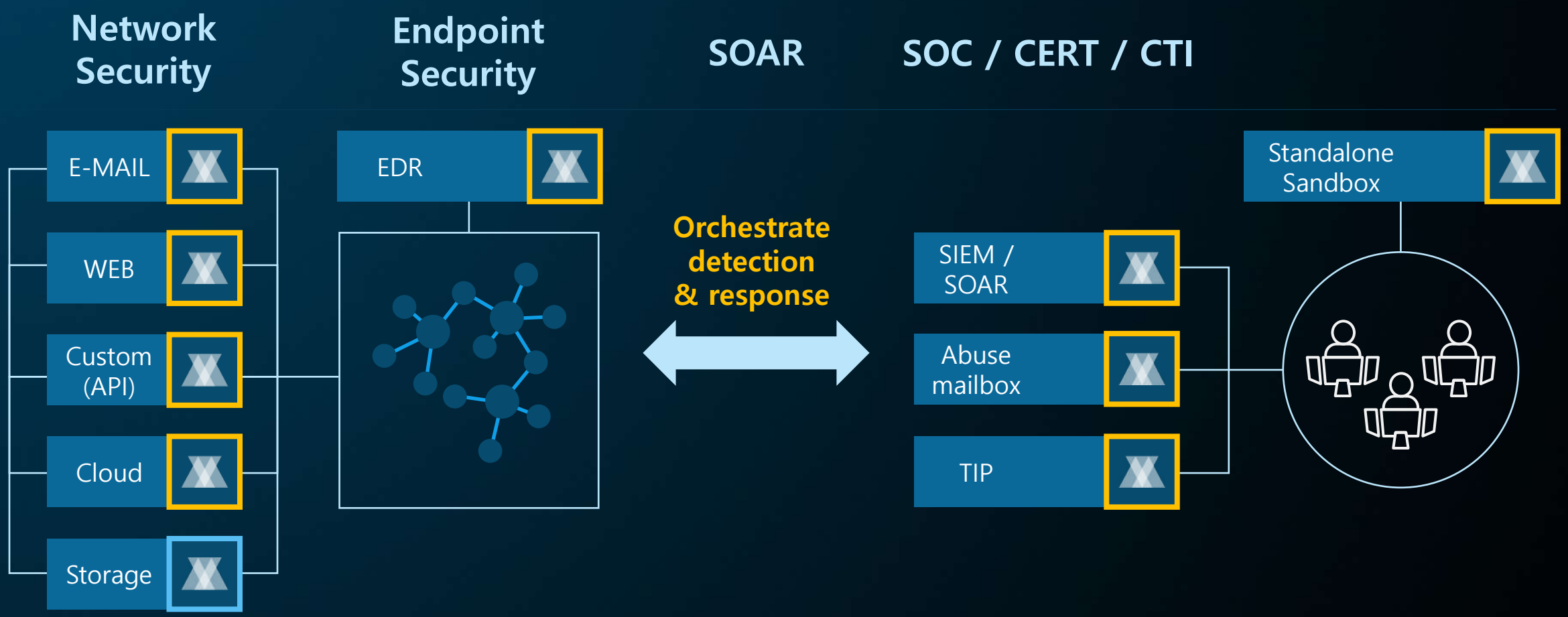
RAPID7 InsightConnect
CORTEX XSOAR BY PALO ALTO NETWORKS
IBM Security SOAR
splunk> SOAR
LogicHub
ayehu
Tines
SWIMLANE
Siemplify
Cortex
FORTINET FortiSOAR

Threat Intelligence TIP

ThreatConnect
MISP Threat Sharing
ANOMALI THREATSTREAM
EclecticIQ
McAfee TIE
THREATQ

보유하고 계신 모든 보안솔루션에 연동하십시오

VMRAY

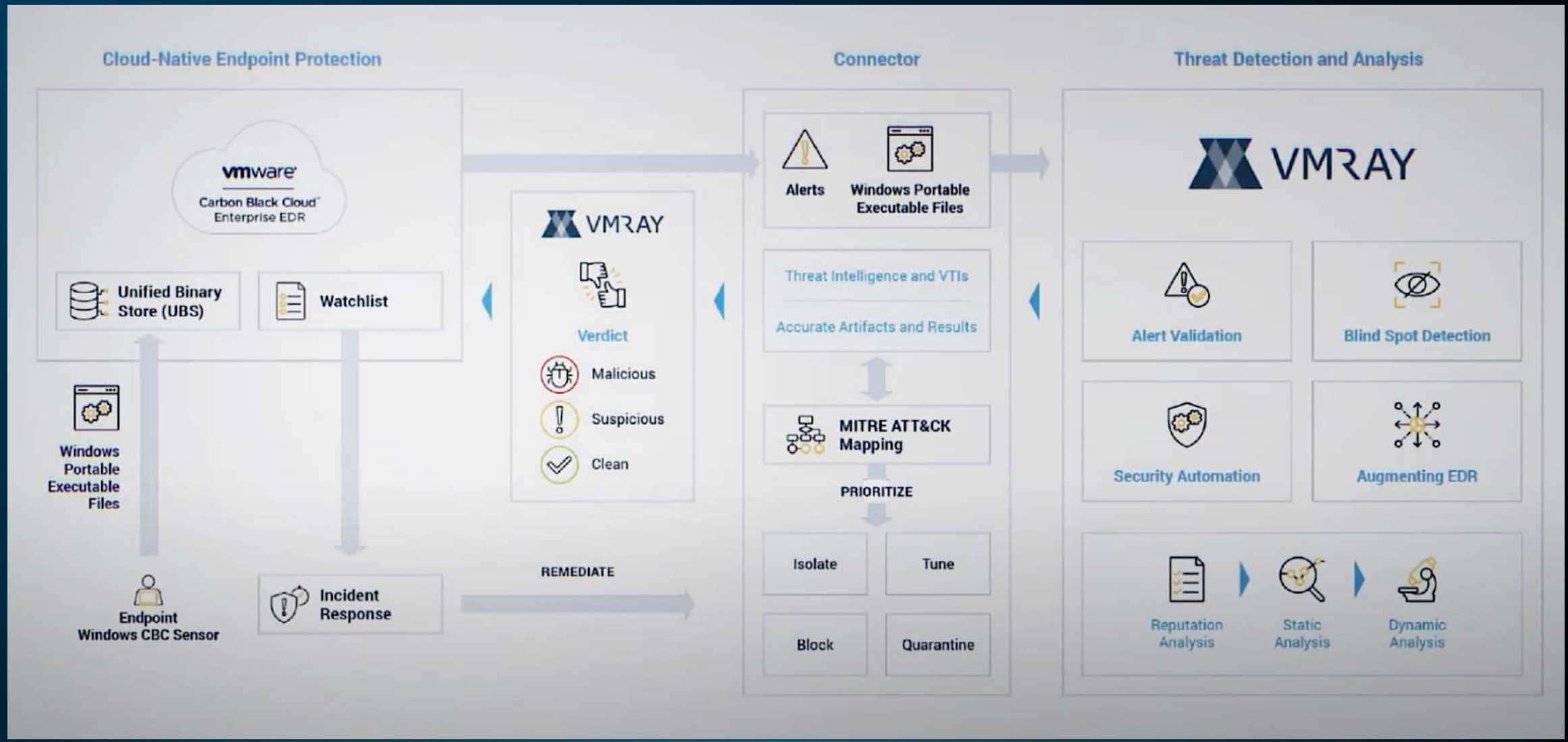


연동 샘플 – SentinelONE (센티넬원)

VMRAY

연동 샘플 – Carbon Black (카본블랙)

VMRAY

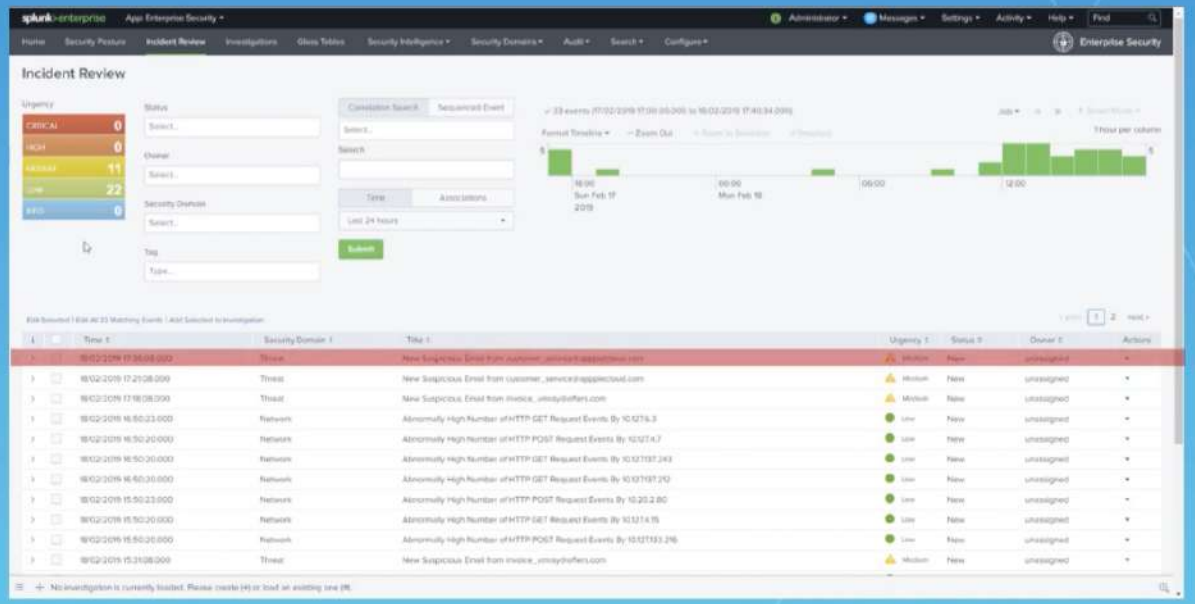


연동 샘플 – Splunk (스플렁크)

VMRAY

Centralizing Incident Response Operations

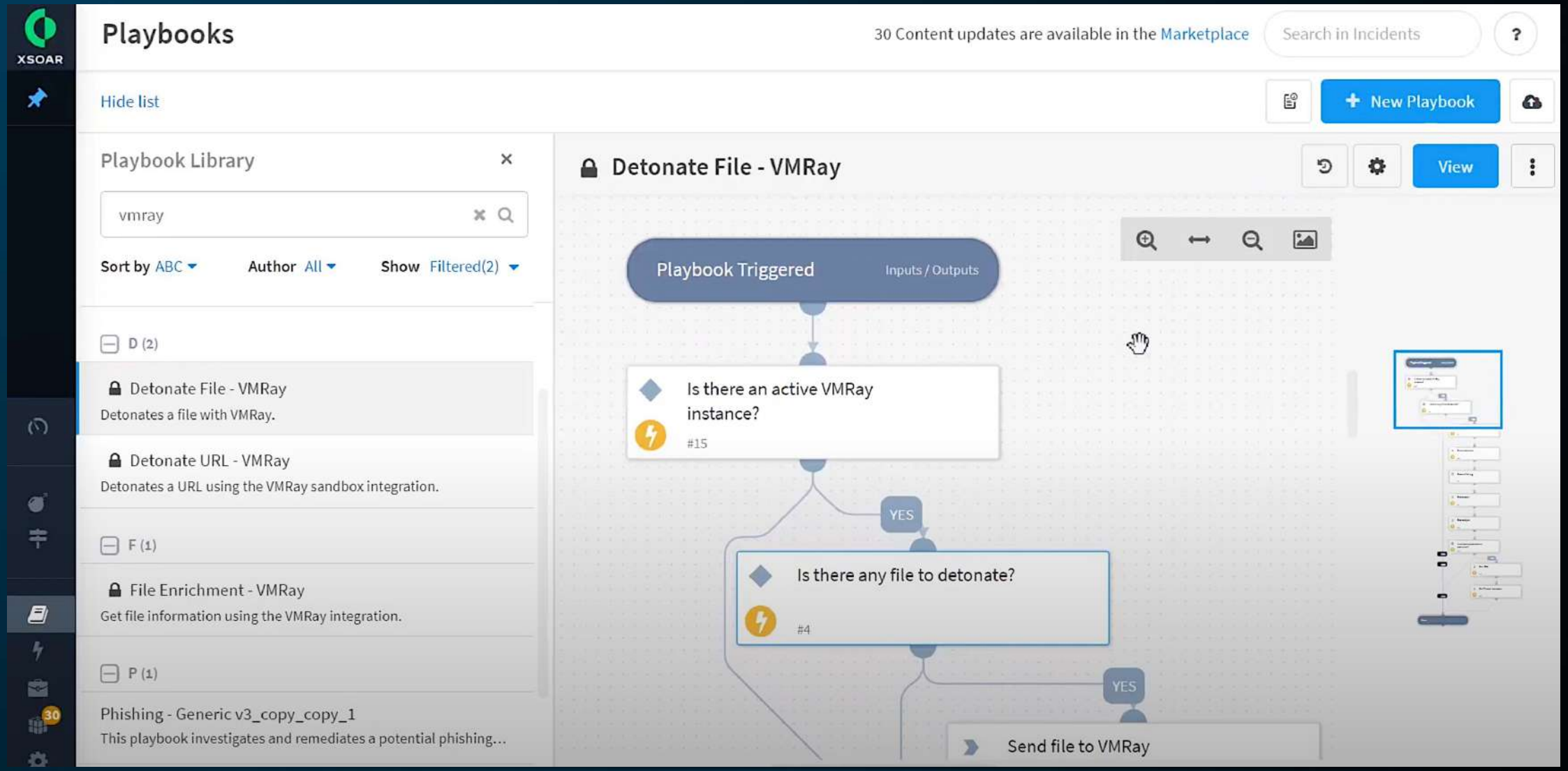
Endpoint Security Product



Splunk Enterprise Security

연동 샘플 – PaloAlto XSOAR (팔로알토)

VMRAY

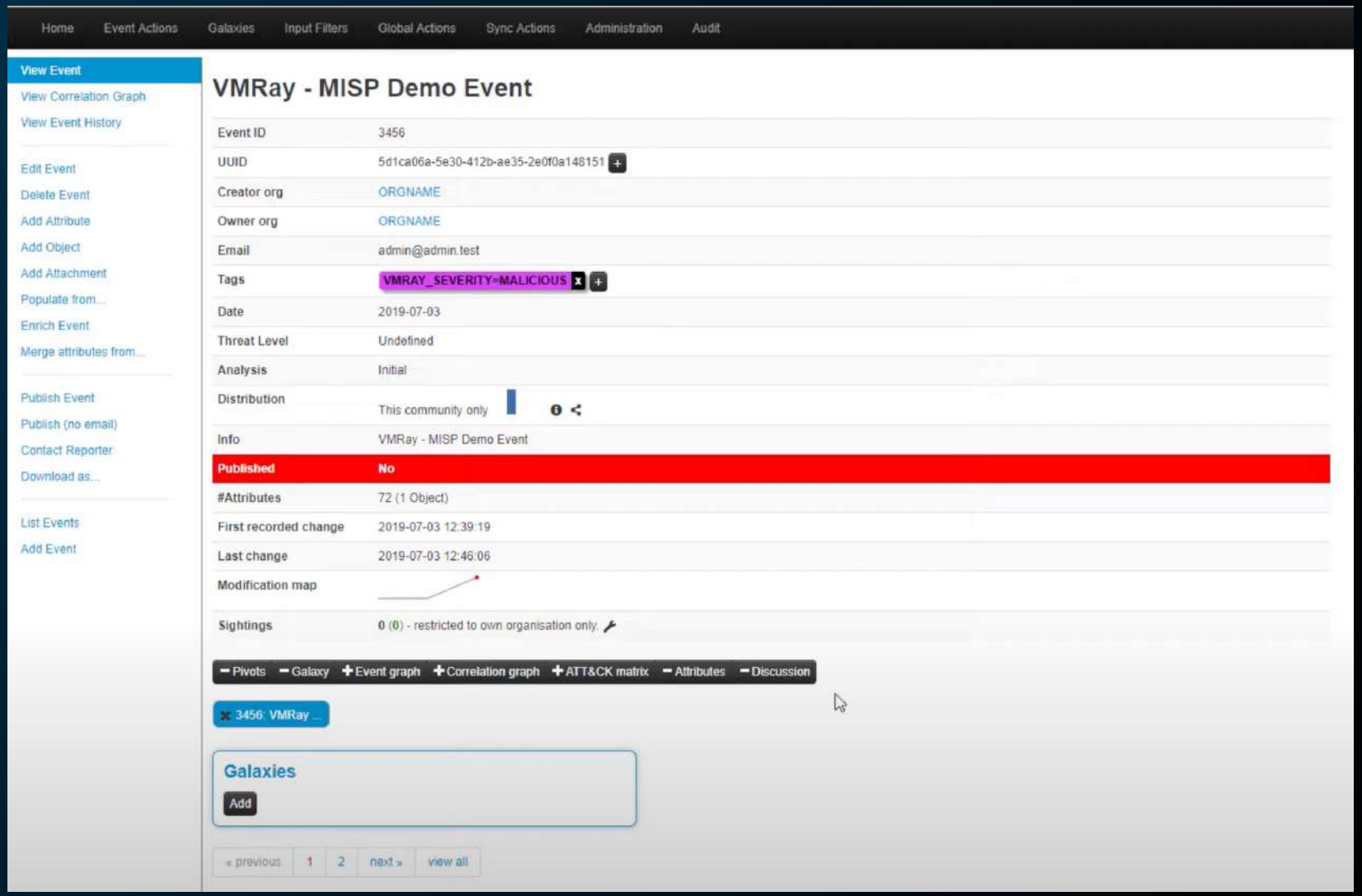


연동 샘플 – MISP (오픈소스 위협공유 플랫폼)

VMRAY

Using
VMRay & MISP

MISP
Threat Sharing



VMRay – 활용 방안 정리. (Use Cases)

VMRAY

Thank you.

VMRAY

Q&A