



# 브이엠레이 샌드박스 플랫폼 혁신

### 고객사 위협 탐지 플랫폼

<b>Email 연동</b> Office 365	<b>보안 제품 연동</b> SOAR, EDR, EPP, SWG, TI, SIEM
<b>레거시 연동</b> REST API	<b>수동 업로드</b> 
<b>File</b> 모든 파일 포맷	
<b>URL / IP</b> WWW	
<b>Email</b> 본문 링크 첨부 파일	

### VMRAY 샌드박스 플랫폼 (Hypervisor 기반 / Anti-Evasion)



**Reputation 체크**  
Static 분석  
Dynamic 파일 분석  
Dynamic 웹 분석

**[핵심 차별화 기술]**

- Built-in AV
- Yara Ruleset
- Macro De-Obfuscation
- Realtime 메모리 분석
- Auto Interaction
- Live User Interaction
- TLS Visibility
- VBA Stomping
- Browsing Simulation
- Link Detonation
- Golden 이미지
- Computer Vision
- 정확한 IOC 추출

### 분석 결과 유형 1 **Virdict** 악성 여부 판별

MALICIOUS

SUSPICIOUS

CLEAN

### 분석 결과 유형 2 **Report** 완벽한 상세 분석 보고서



### 고객사 보안 솔루션

**보안 운영팀**  
탐지 대응 팀  
CERT 팀  
IR 팀

**위협 대응 프로세스 자동화 연동**  
SOAR  
EDR  
SEG  
SWG  
TIP  
SIEM  
고객사 자체 대시보드

- 단순 분석 결과 연동 (악성 여부)
- 추출된 IOC 전송
- 다양한 연동 프로토콜 / API