Yara Relay Server

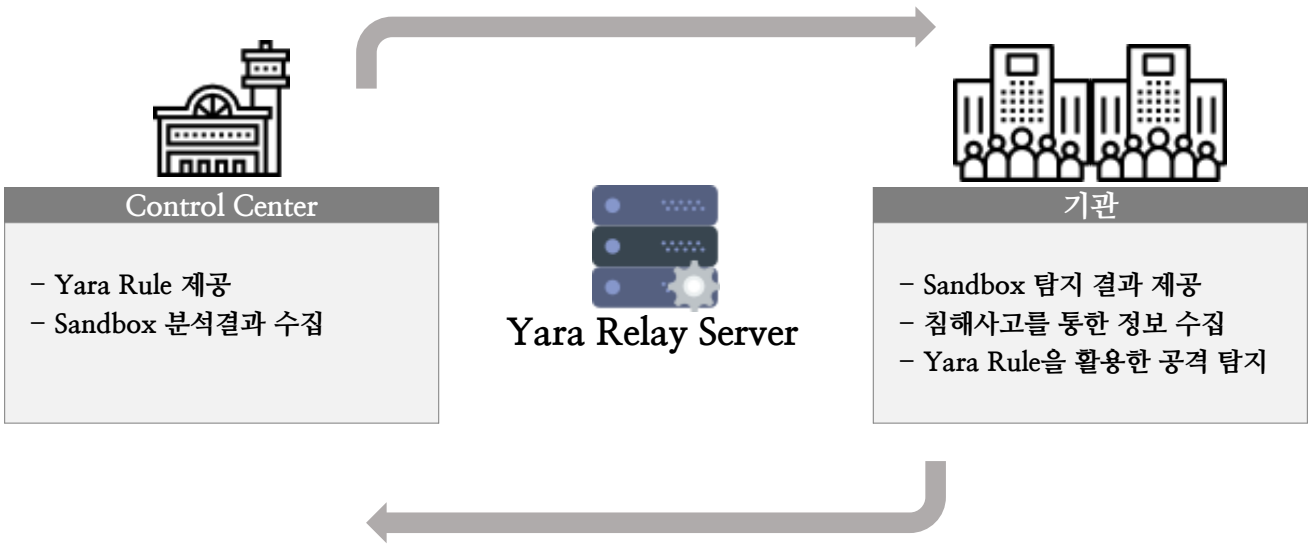
Control Center Yara Rule 연동 시스템

GuardianNET
Guard Your Business
(주)가디언넷

Yara Relay Server

Control Center Yara Rule 연동 시스템

위협정보 공유 체계



주요 기능

Control Center과 연동 제공
- Control Center에서 제공하는 API v2.0 지원

탐지결과 모니터링
- 배포 기관 전송 탐지 결과 조회
- 탐지 결과 응답(VirusTotal, MD5 등) 조회

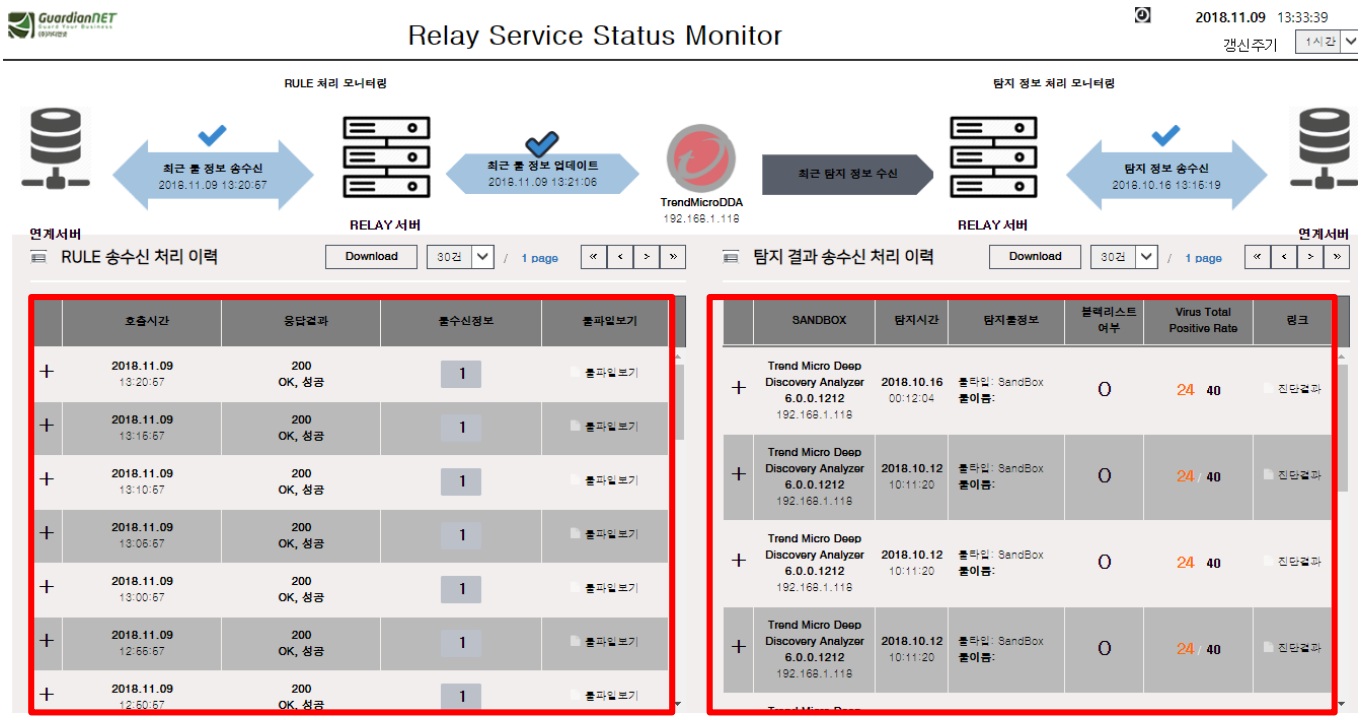
탐지 규칙 수신
- 탐지 규칙을 Sandbox에 적용
- 탐지 결과 수집

탐지 결과 송신
- 주기적으로 YARA에 의한 탐지 결과 전송
- 탐지 결과 응답(VirusTotal, MD5 등) 결과 수신

Yara Relay Server

Control Center Yara Rule 연동 시스템

Control Center과의 탐지룰(YARA)를 연계하여 악성파일 탐지 시 로그 전송



APT 장비로의 YARA 배포 성공 이벤트 로그

APT 장비에서 YARA에 의해 탐지된 결과 값을 Control Center으로 전송한 로그

- 정상적으로 APT 장비로의 탐지룰 배포 상태를 시간 별 로그로 확인 가능

- APT 장비에서 YARA에 의한 탐지 시 해당 결과 값을 전송하고, Virus Total에서 해당 결과 값에
  대한 정보 및 블랙 리스트 여부를 확인 가능

서울특별시 마포구 마포대로 33, 312
Tel. 02 - 6334 - 1113 Fax. 02 - 6334 - 1112