

Yara Relay Server

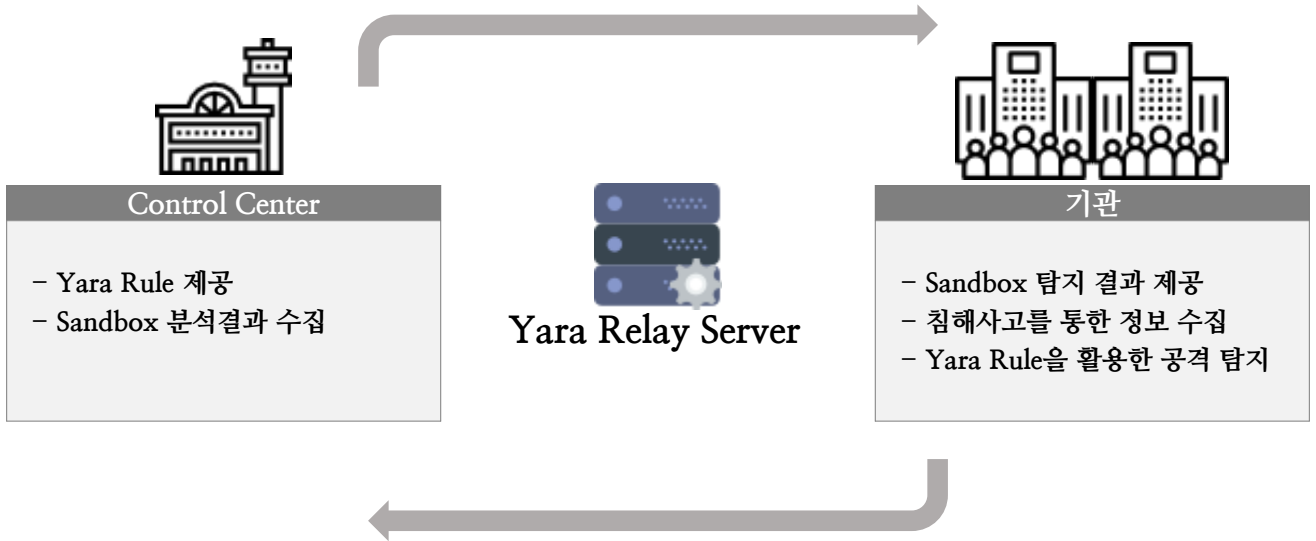
Control Center Yara Rule 연동 시스템



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

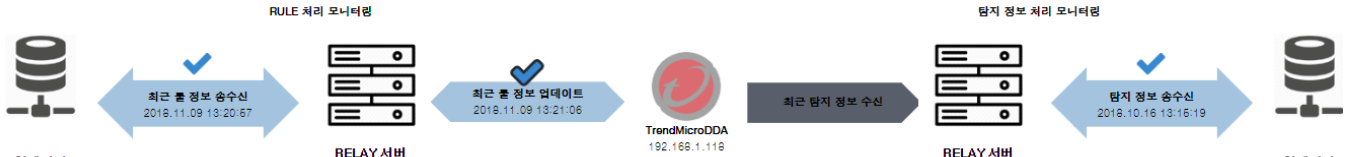
탐지 결과 송신

- 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)을 연계하여 악성파일 탐지 시 로그 전송



연계서버 RULE 송수신 처리 이력					연계서버 탐지 결과 송수신 처리 이력					
호출시간	응답결과	송수신정보	종파일보기		SANDBOX	탐지시간	탐지종정보	블랙리스트 여부	Virus Total Positive Rate	링크
2018.11.09 13:20:67	200 OK, 성공	1	종파일보기		Trend Micro Deep Discovery Analyzer 6.0.0.1212	2018.10.16 00:12:04	종파일: SandBox	0	24 / 40	진단결과
2018.11.09 13:16:67	200 OK, 성공	1	종파일보기		Trend Micro Deep Discovery Analyzer 6.0.0.1212	2018.10.12 10:11:20	종파일: SandBox	0	24 / 40	진단결과
2018.11.09 13:10:67	200 OK, 성공	1	종파일보기		Trend Micro Deep Discovery Analyzer 6.0.0.1212	2018.10.12 10:11:20	종파일: SandBox	0	24 / 40	진단결과
2018.11.09 13:06:67	200 OK, 성공	1	종파일보기		Trend Micro Deep Discovery Analyzer 6.0.0.1212	2018.10.12 10:11:20	종파일: SandBox	0	24 / 40	진단결과
2018.11.09 13:00:67	200 OK, 성공	1	종파일보기		Trend Micro Deep Discovery Analyzer 6.0.0.1212	2018.10.12 10:11:20	종파일: SandBox	0	24 / 40	진단결과
2018.11.09 12:56:67	200 OK, 성공	1	종파일보기		Trend Micro Deep Discovery Analyzer 6.0.0.1212	2018.10.12 10:11:20	종파일: SandBox	0	24 / 40	진단결과
2018.11.09 12:50:67	200 OK, 성공	1	종파일보기		Trend Micro Deep Discovery Analyzer 6.0.0.1212	2018.10.12 10:11:20	종파일: SandBox	0	24 / 40	진단결과

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