사이버침해대응의 완성

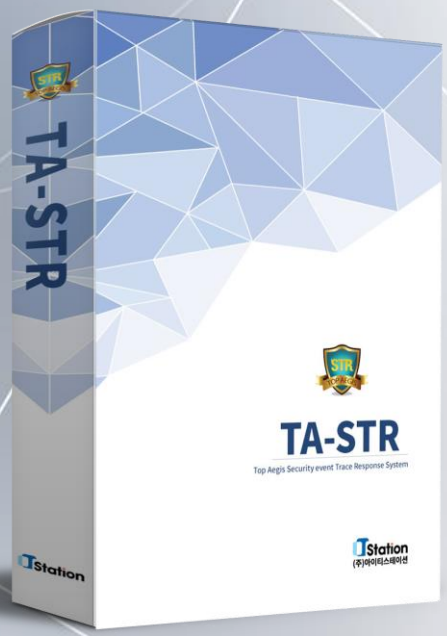
보안이벤트 추적·대응 자동화 시스템

TA-STR

핵심요약 제안서

Station

㈜아이티스테이션



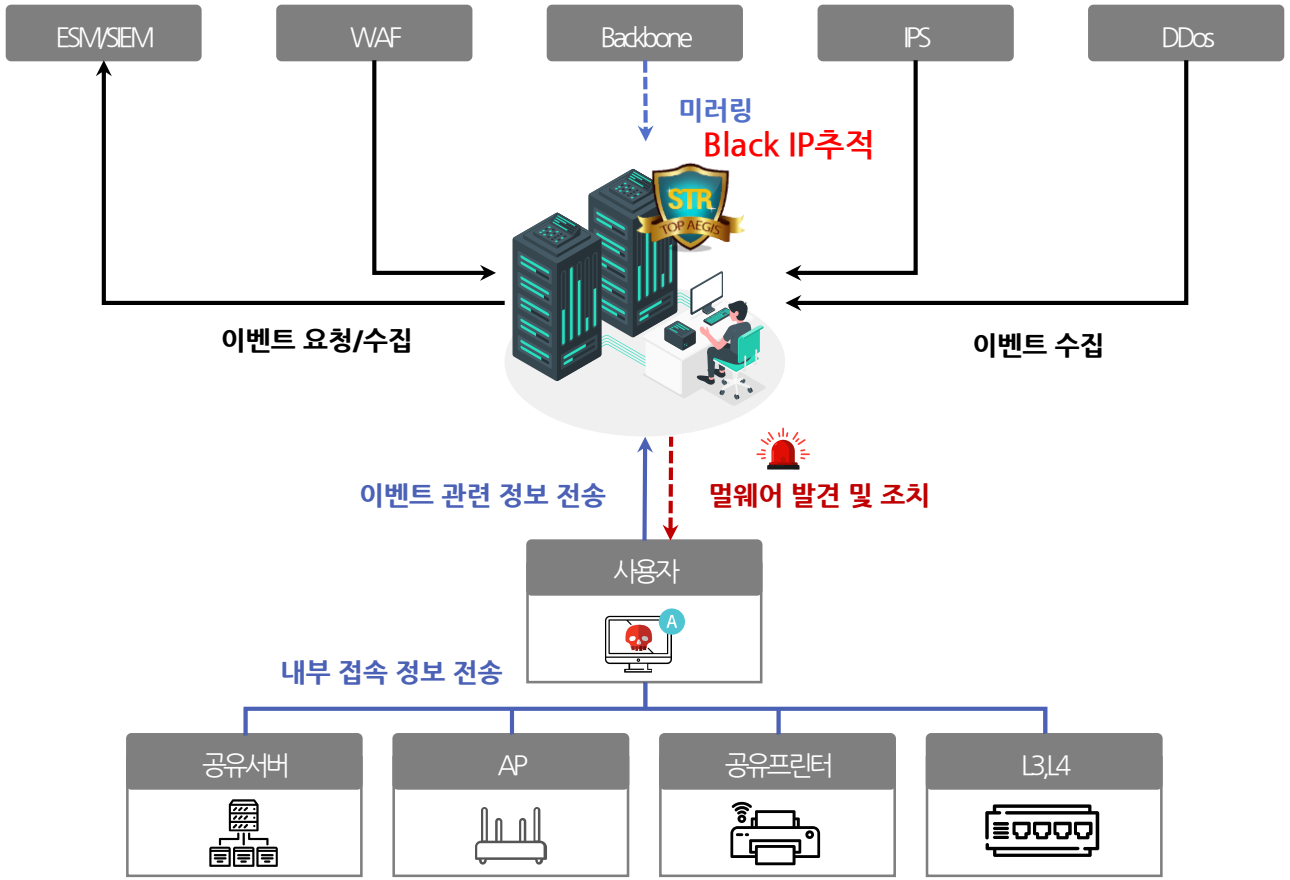
TA-STR

솔루션 주요특징

- 10년간 사이버 보안관제 용역사업을 수행하면서 축적된 노하우와 현업 보안담당자와의 협업을 통해 사이버침해대응 업무에 가장 필요한 대응업무를 2년간 분석하여 침해대응업무에 가장 필요로 하는 기능들을 시스템에 반영하여 보안대응업무에 혁신을 가져온다.
- 기 구축된 보안 시스템들에서 발생하는 모든 보안위협 경고 및 침해위협 정보를 연계 하여 **모든 보안이벤트**에 대해 **실시간 전수조사**를 하고 위협행위PC를 **자동 추적** 후 **즉각 조치** 할 수 있다.
- 보안이벤트와 연관된 프로세스와 파일을 특정하여 **증적파일을 자동으로 수집**하고 정적,동적분석을 실시하여 침해발생원인을 발생 즉시 처리할 수 있다.
- 주요 정보자산에 대한 접근을 관제하여 침입 장악된PC 또는 악성코드에 의한 침해 사고 발생을 추적하여 원인을 차단한다.
- **원인행위PC**의 네트워크 접속 정보에 관한 **네트워크 통신기록**과 **증적자료(dll/process file, comm log)정보를 확보** 및 **보관**하여 추후 **상위기관보안관제 또는 국가보안기관의 분석요구에 대응**할 수 있다
- 통합보안관제시스템(SIEM,ESM) 및 각종보안시스템(IPS, DDoS, FW, WAF, VPN, BlackIP)에서 발생되는 경보와 침해로그를 매칭 분석하여 **해당 원인행위 PC를 자동 추적하여 대응**함으로써 자동화된 하나의 프로세스로 **보안관제업무의 완성**을 가져온다.

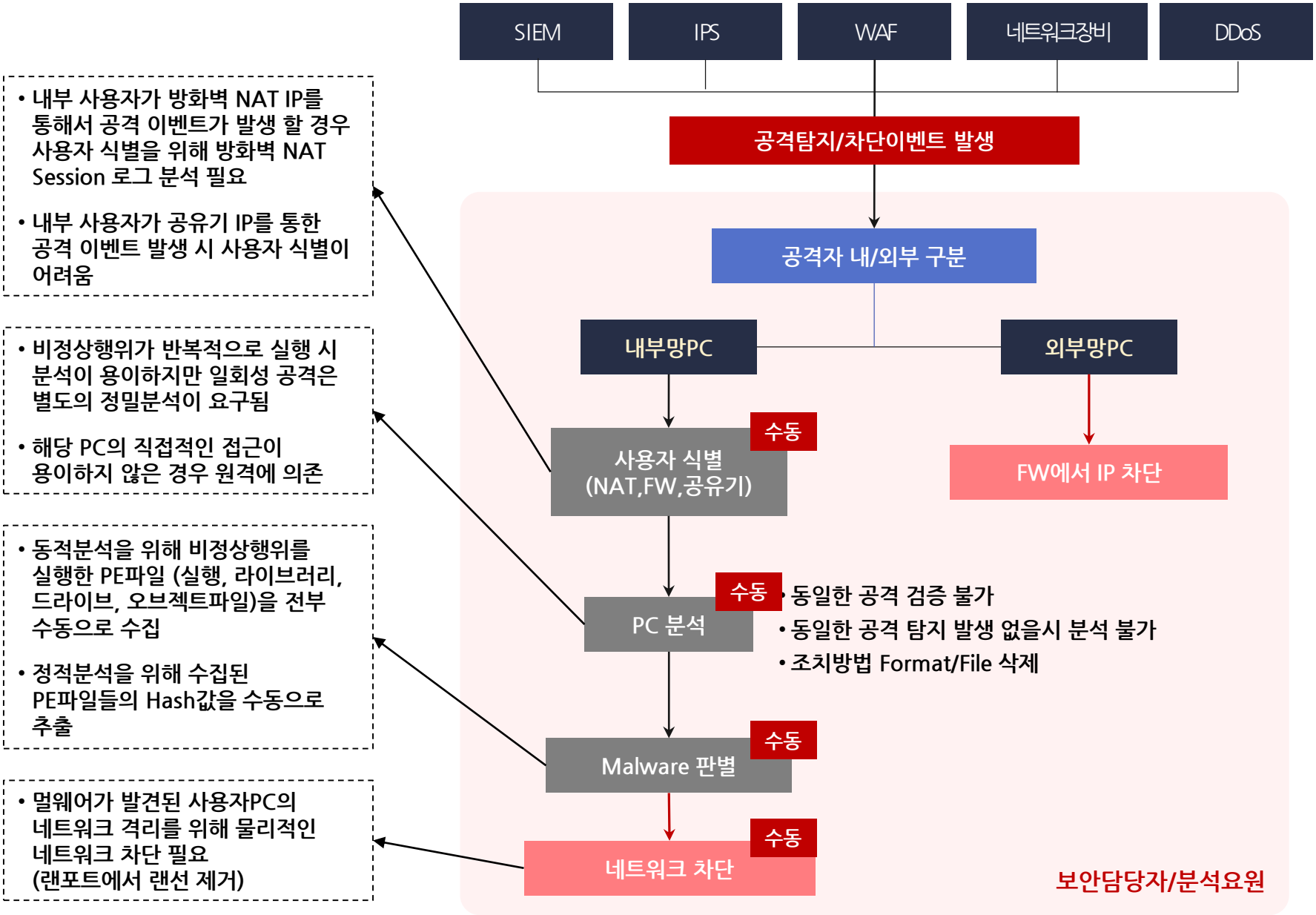
기 구축된 보안시스템 연계 및 보안이벤트 처리 흐름도

- TA-STR은 보안장비 보안이벤트 및 백본 미러링 데이터를 수집하고 분석하여 보안이벤트를 발생
- 모든 보안이벤트를 전수조사 후 보안이벤트에 해당하는 사용자 PC를 자동 추적
- 위협의심 행위 사용자 PC는 보안이벤트에 연관된 증적 파일인 PE파일(exe,dll 등 실행 가능한 파일) 확보
- TA-STR에 수집된 증적 파일을 정적/동적 자동분석 및 자동조치
- 기 보안장비와 연계하여 수집된 보안이벤트를 추적.분석 후 오탐 및 진탐 판별
- 분석 결과에 따라 해당 위협행위로 판별시 PC의 격리 자동 결정 및 대응조치



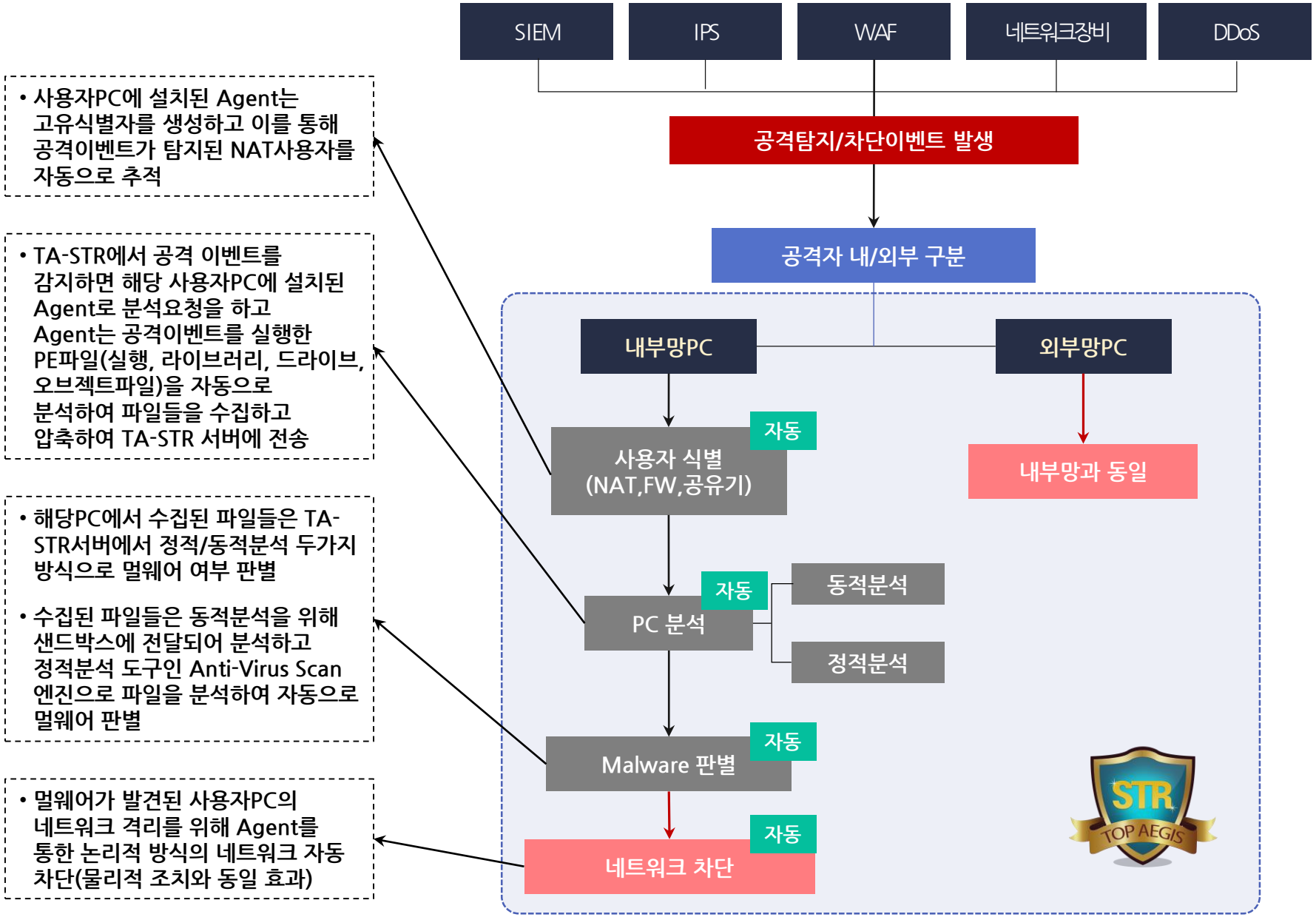
도입 전 보안침해대응 업무 프로세스

>> 하나의 보안이벤트 처리 예상시간 : 몇십분~몇일



도입 후 보안침해대응 업무 프로세스

>> 하나의 보안이벤트 처리 예상시간 : 3분 이내



- 사용자PC에 설치된 Agent는 고유식별자를 생성하고 이를 통해 공격이벤트가 탐지된 NAT사용자를 자동으로 추적

- TA-STR에서 공격 이벤트를 감지하면 해당 사용자PC에 설치된 Agent로 분석요청을 하고 Agent는 공격이벤트를 실행한 PE파일(실행, 라이브러리, 드라이브, 오브젝트파일)을 자동으로 분석하여 파일들을 수집하고 압축하여 TA-STR 서버에 전송

- 해당PC에서 수집된 파일들은 TA-STR서버에서 정적/동적분석 두가지 방식으로 멀웨어 여부 판별
- 수집된 파일들은 동적분석을 위해 샌드박스에 전달되어 분석하고 정적분석 도구인 Anti-Virus Scan 엔진으로 파일을 분석하여 자동으로 멀웨어 판별

- 멀웨어가 발견된 사용자PC의 네트워크 격리를 위해 Agent를 통한 논리적 방식의 네트워크 자동 차단(물리적 조치와 동일 효과)

보안장비 연동을 통한 이벤트 수집

Database Connection을 통한 이벤트 수집

- SIEM에서 발생한 경보 이벤트 감시

백본 미러링을 통한 이벤트 수집

- Black IP 접근 현황 감지
- 내부 사용자 중요서버 접근 현황 감지

SysLog 전송을 통한 이벤트 수집

- IPS 차단/탐지 로그 감시
- WAF 차단/탐지 로그 감시
- DDos 차단/탐지 로그 감시
- 사용자 PC에서 중요서버존 통신 현황 감시 (방화벽 차단 로그)

Agent 모니터링을 통한 이벤트 탐지

- 사용자 PC에서 접근성이 용이한 주변 IT기기와 장비들의 접근 시도 감시
- 외부에서의 접근 시도 감시

연동 보안 장비 로그 현황

장비별로 전송되는 이벤트 로그를 통합하여 저장

통합로그 > 로그정보 > 통합로그

☑ 분류 ☐ BlackIP ☑ ESM/SIEM ☑ IPS ☑ 중요서버 ☑ 네트워크장비

갱신주기 정지 통합검색 검색

NO	상태	분류	탐지번호	탐지명/서버명	출발지 정보	목적지 정보
1	관리범위	네트워크장비	357385	인터넷망_IPS_#01 비인가 접근 시도	109.0.55.62:24176	109.0.23.51:4000
2	관리범위	네트워크장비	357384	인터넷망_IPS_#02 비인가 접근 시도	109.0.55.62:24173	109.0.23.52:4000
3	관리범위	IPS	4160052	K_mal_Attack-PAT-HeartBleed(SSLv3).19042301@	109.0.27.70:443	109.50.25.3:3667
4	관리범위	IPS	4160051	JB Ransomware_2017051304	109.0.93.36:12399	192.168.32.2:445
5	관리범위	네트워크장비	357383	인터넷망_IPS_#01 비인가 접근 시도	109.0.55.62:24113	109.0.23.51:4000
6	관리범위	네트워크장비	357382	인터넷망_IPS_#01 비인가 접근 시도	109.0.55.60:5292	109.0.23.51:4000
7	관리범위	IPS	4160050	JB Ransomware_2017051303	109.0.41.37:1228	192.168.32.100:139
8	관리범위	네트워크장비	357381	인터넷망_IPS_#02 비인가 접근 시도	109.0.55.62:24097	109.0.23.52:4000
9	관리범위	IPS	4160049	JB Ransomware_2017051304	109.0.83.24:13894	192.168.32.2:445
10	관리범위	IPS	4160048	Jeus WAS "#" Source File Disclosure	109.50.1.38:2617	58.225.75.206:80
11	관리범위	네트워크장비	357380	도청내부_IPS_#02 비인가 접근 시도	109.0.55.62:24063	109.0.27.61:4000
12	관리범위	네트워크장비	357379	도청내부_IPS_#01 비인가 접근 시도	109.0.55.62:24059	109.0.27.62:4000
13	관리범위	네트워크장비	357378	인터넷망_IPS_#01 비인가 접근 시도	109.0.55.62:24040	109.0.23.51:4000
14	관리범위	IPS	4160047	JB Ransomware_2017051304	109.0.152.89:1136	192.168.32.100:445
15	관리범위	네트워크장비	357377	인터넷망_IPS_#02 비인가 접근 시도	109.0.55.62:24010	109.0.23.52:4000
16	관리범위	IPS	4160046	JB Ransomware_2017051304	109.0.76.11:13793	192.168.32.2:445
17	관리범위	네트워크장비	357376	인터넷망_IPS_#01 비인가 접근 시도	109.0.55.60:5083	109.0.23.51:4000

파일의 Hash DataBase 구축

- 내부 사용자 PC에 설치된 TA-STR Agent는 PC내 모든 PE파일을 전수 조사하여 TA-STR 서버에 전송되고 “관리자 정의”,”시스템 설정”, “OS별 설정” 별로 파일 분포도를 작성하여 DataBase 구축

☑ 분류 ☑ 관리자 정의 ☑ 시스템 설정 ☑ OS별 설정

검색하고자 하는 프로세스명 및 체크섬을 입력하세요 검색

분류	프로세스명	체크섬정보
OS별 설정	msls31.dll	3ED04E60EC1859086A633C98448306DEB95FE5DFB8DA511C91E3D2C1B1F38DFB
OS별 설정	profapi.dll	93276D45950109D8C676168DCFAA852FBABFCB98C63C5A7AB823DE195E75D19B
OS별 설정	eeprov.dll	EBE5C4D53E3069AF66C79321141EF30B4DF6B6ABAF8311C1B75C243813DDC5BB
OS별 설정	hrtfapo.dll	3F4110CC93DABBFEB13159BA033D017C8AFDFA55D317C94AC0257F6021B7CBED
OS별 설정	msimg32.dll	936B00CF39ED8146AAAE8DAB3239D81423808CB2560E7D6A43A79A356F6CA62F
OS별 설정	sensorsutilsv2.dll	EC13B446BE3797CFB3573720B4A99565A34711A3A03D02AE53E416A7253E02DB
OS별 설정	powrprof.dll	3F9674B385C0CFC4C93961620C6237499C1701CE76094DAB6F6E4E502E7881FC
OS별 설정	execmodelclient.dll	93CC27ABC0A7F8887A5DE16DC419E3E3A823310B61148E3564778ED572F880E7
OS별 설정	clbcatq.dll	EC3D61CB2C5D1511051882F3C0E2B8B6F74B011CFB972112179090F2C3F3F5FC
OS별 설정	energy.dll	3FBA66BB548EF084DAC3C4F4D1FCFAE3EB9B007669AEFC3A74298A739244D8CD
OS별 설정	ws2_32.dll	93DB7C9699594CAA19490280842FBEBEC3877278C92128B92E63D75FCD01397A
OS별 설정	dusmapi.dll	EC96AF4FC4B1302B75519FDC6DCBA023BC04883E5DE6F3A408F23D4D820847F1
OS별 설정	proximityservice.dll	3FD06BB9E1775C59C48FB8778FF0BEB0BAC7954406733F058E4F5FF31545F37B
OS별 설정	netprovfw.dll	941E5B59406CE904C9AF5E954EC6E76293224D2E85FB2005D3322C09D74505EC
OS별 설정	profext.dll	ED354ED6A85255C99654F0FFA055C60C46FC1B0426D87577F46E4793FD702F29
OS별 설정	dxp.dll	40A8394E422489DAFBE0121C6DC334A5BEA9362FC9F6749E607ACED9691ADBA2

멀웨어 사용자 현황

정적/동석 분석 엔진을 통해 판별된 멀웨어 현황

파일명	체크섬	분석결과	다운로	사용비율
newsfeed.exe	B76DEAFB0EEDFA03450E...	Cuckoo SandBox 분석결과 : [6.0]점으로 파일 감염 의심		0.07%
ceuuecouqpmm.exe	19BED4E54694133EFAFB...	[MD5:8eaf3014efacc8143e5f83e83f6a1ff9] ...		0.17%
kmsss.exe	FD7499214ABAA13BF56D...	Cuckoo SandBox 분석결과 : [6.6]점으로 파일 감염 의심		0.02%
wdetector.w	229313A5FF391EC049F5...	Cuckoo SandBox 분석결과 : [33.8]점으로 파일 감염 의심		0.15%
mbtipv32.exe	820BD8387DD1DEEB9076...	Cuckoo SandBox 분석결과 : [5.0]점으로 파일 감염 의심		0%
autopico.exe	4A714D98CE40F5F3577C...	Cuckoo SandBox 분석결과 : [4.2]점으로 파일 감염 의심		0.15%
dwcnmx.exe				
안카메라.exe				

Click

프로세스 사용자정보

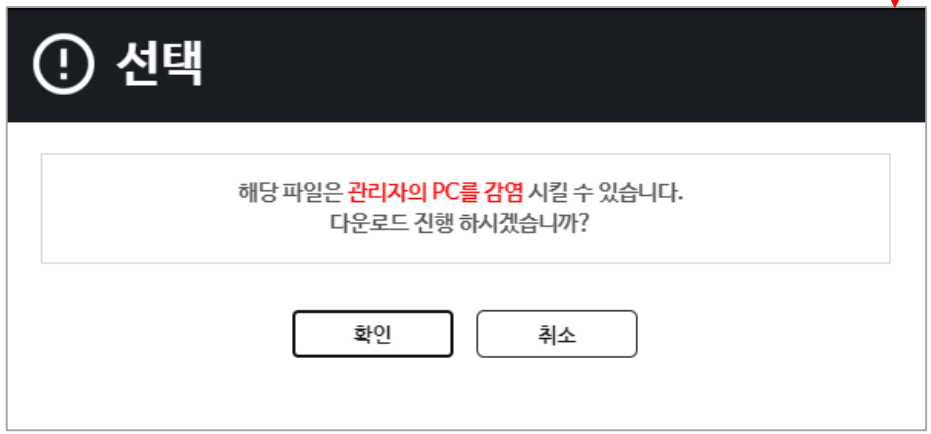
NO	부서위치	사용자 정보	기기OS	IP주소	백신설치	실시간감시
1	전체		Windows 10 Pro (1909)		Windows Defender	동작중
2	전체		Windows 10 Pro (1809)		AhnLab V3 Internet Security 9.0	동작중
3	전체		Windows 10 Pro (1903)		AhnLab V3 Internet Security 9.0	동작중

멀웨어 의심 파일 분석

- 멀웨어로 의심되는 파일을 다운로드하여 분석사이트(Virustotal, malwares 등)에 파일을 직접 업로드 후 멀웨어 판별

IPS장비 IP	사용자정보	접근정보	탐지명	프로세스명	사용비율	서명	다운로드
109.0.23.52			L_web_EmailAddress_Collector_UserAgent_20200207	zoneplayer.exe	0.15%	✓	
109.0.23.52			L_web_EmailAddress_Collector_UserAgent_20200207	zoneplayer.exe	0.15%	✓	
109.0.23.52			K_mal_Attack-IP-J2(SPAM).20011608@	decacopy.exe	0.02%	✓	
109.0.23.52			K_mal_Attack-IP-J2(SPAM).20011608@	decacopy.exe	0.02%	✓	
109.0.23.52			K_mal_Attack-IP-J2(SPAM).20011608@	decacopy.exe	0.02%	✓	
109.0.23.52			L_web_EmailAddress_Collector_UserAgent_20200207	zoneplayer.exe	0.15%	✓	
109.0.23.52			K_mal_Attack-IP-J2(SPAM).20011608@	iexplore.exe	84.91%	✓	
109.0.23.52			K_mal_Attack-IP-J2(SPAM).20011608@	iexplore.exe	84.91%	✓	

Click



멀웨어 판별 후 대응

파일명	체크섬	분석결과	다운로드	보고서	사용비율
gfx.dll	60B0969141F74A0F88FA...	Yanadoo		한	2.13%
urlmon.dll	04FDDB14198BE2DB721B...	9.6		한	19.15%
m.exe	364B6FDE43FB977C11E1...	Yara		한	2.13%
mdnsnsp.dll	043779B2C684699C89D6...	9.2		한	2.13%
안카메라.exe	E8B2AD3C801157CA219E...	he GenericRXFB-IW!567C534516DC trojan !!!		한	0%
clienth.exe	55475C36F4899B3A628D...	he GenericRXFQ-WC!584EE60499E5 trojan !!!		한	0%
relatedpop.exe	183CE4EBB2F5D7B5A10B...	he Generic Trojan.kk trojan !!!		한	0%

Click

1

프로세스 사용자정보

NO	네트워크 차단	부서위치	사용자 정보	기기OS	IP주소
1	OFF			Windows 10 Pro (2009)	

2

금지프로세스 정책

NO	정책명	프로세스명	등록일자	금지정책
1	sihclient.exe	sihclient.exe	2021-01-05 10:43:38	ON

- 윈도우사용자 > 금지프로세스
- 멀웨어로 판별 시 금지프로세스로 자동 등록

✸핵심 기 구축 보안장비 연계를 통한 보안이벤트 자동추적대응 시스템

주요 보안장비 SIEM/ ESM / IPS / 방화벽 / DDoS / 웹방화벽 / Black IP / 중요서버 접근 탐지 / PC간통신기록 등 연계를 통해 발생한 보안이벤트의 원인행위PC에 대해 **현재까지는 보안담당자가 수동분석을 통해 사용자PC 추적 후 분석해야 했지만**, TA-STR은 해당 보안이벤트를 실시간 **자동으로 추적하여 분석 후 대응하고 증적 PE파일 확보**를 통해 이벤트 발생 이후에도 포렌식을 진행할 수 있는 시스템으로 **보안관제(침해대응) 업무를 완성해주는 시스템**입니다.

주요 보안시스템과 연계, 이상행위PC 자동 추적대응

주요보안장비의 보안이벤트를 실시간 수집 후 전수 조사하여 원인행위를 한 PC를 실시간 추적하고 상관 분석하여 즉각적인 침해대응이 가능

보안위협 발생시 즉각 보고 및 조치

보안위협으로 판별될 경우 즉시 관리자에게 보고되며, 원인행위PC에 대해 자동으로 증적 PE파일 수집 및 분석하여 멀웨어 판별 시 차단(정책적용시) 실행

정적·동적분석을 통한 신뢰도 높은 위협 적발

수집된 증적 파일에 대해 2가지 세계적 악성코드 검사 엔진으로 정적분석 후, 샌드박스를 통해 동적분석을 거침으로 신뢰성 있는 위험도 판별 제공

PC 리소스 사용률 최소화/최적화

증적PE파일 수집 시 낮은 리소스율로 이상행위 프로세스 수집 후 의심파일을 서버에 분석의뢰 하여 PC성능에 전혀 영향 없음

보안(관제)담당자 보안업무 실효성의 극적인 효과

보안이벤트 추적 및 대응 현황을 쉽게 파악하고, 자동으로 분석하여 보안관리자의 업무프로세스를 획기적으로 줄여주며 보안업무대응에 극적인 실적을 가져옴

기대효과 : 보안침해대응을 완성할 수 있게 해주는 시스템

기존 구축된 보안장비의 도입효과 극대화

기 구축된 보안장비들의 보안이벤트를 연계하여
전수조사 분석 후 보안위협을 자동추적 및 조치하여
기 구축된 보안장비의 성능효율을 극대화하는 효과

보안업무의 극적인 간편화

보안이벤트 자동 전수조사를 통해
위협행위PC에 대한 실시간 추적 및 대응으로
보안업무의 극적인 간편화를 가져옴

보안(관제)업무의 실적상승

보안침해대응 및 해결시간을 극적으로
단축하고 실적화를 실현하여
보안관제업무의 실효성 있는 효과를 가져옴

TA-STR 제안 키워드

ESM/SIEM 경보 추적
IPS Attack로그 추적
Black IP접속PC추적조치
중요서버 비정상 접근탐지
내부 네트워크 추적
방화벽 차단로그 추적
PC간 통신 추적

정적분석
동적분석
상관분석
프로세스 중복카운트 판별
원인행위PC 자동추적 보안이벤트 연계
접근허가PORT 프로세스 분석

증적PE파일 확보
시나리오기반 경보
사용자PC 통신기록 저장
동일 의심행위 프로세스 보유자 색출
원인행위PC자동식별

보안(관제)업무의 극적인 변화
보안(관제)업무의 완성
PC부하 전혀 없음
선제적 Zeroday Attack 대응
조달등록

주요 기능 - 리소스의 최소화

리소스 최적화 기능

사용자 PC의 리소스(CPU, Memory, I/O)를 감지하여 TA-STR 에이전트 리소스 최소화 알고리즘 제공으로 TA-STR이 작동하는 PC에 전혀 부하가 없습니다.