



TongRo Images Inc. is a content company who is responsible for creating digital images and distributing those. Vulnerability Automatic Detection & Analysis system

지란지교에스앤씨의 시스템 취약점 진단 솔루션 바다

1. VADA 사용자 교육

I. 자산관리

- ▶ VADA에서 진단을 수행하기 위하여 진단 대상 자산을 등록
- ▶ “자산관리” 메뉴에서 진단을 수행할 자산을 등록, 수정, 삭제가 가능
- ▶ EXCEL을 이용하여 일괄 자산 등록 및 수정이 가능

The screenshot displays the VADA Asset Management interface. On the left is a sidebar with navigation icons for '내업무' (My Work), '자산관리' (Asset Management), '보안규정' (Security Policy), '진단 수행' (Perform Diagnosis), '조치관리' (Action Management), and '보고서' (Report). The main area shows the '[자산분류그룹] 보안 현황' (Security Status by Asset Classification Group) page. It includes a '보안점수' (Security Score) of 79, a bar chart for '분류별 보안 점수' (Security Score by Classification), and a table of assets. A red box highlights the '자산등록' (Asset Registration), '자산수정' (Asset Modification), '자산삭제' (Asset Deletion), and 'EXCEL' buttons. A callout points to the 'EXCEL' button with the text: '자산 등록/수정/삭제, Excel을 이용한 일괄등록' (Asset registration/modification/deletion, bulk registration using Excel). Another callout points to the 'Linux_Test' tag in the asset list with the text: 'Agent 자동 등록 혹은 수동 등록 한 리스트' (List of assets registered automatically by Agent or manually).

보안점수	그룹	Tag	자산명	IP	HostName	자산분류	검검대상	버전
71	JIRANSNC	Win_Test	VMWIN2019	20.20.20.9	VMWIN2019	OS	WINDOWS_SERVER	2019
98	VADA	VD_HOST	VADA	20.20.20.103	VADA	OS	LINUX	Ubuntu 16.04.7 LT
	VADA	VD_HOST	VADA	20.20.20.103	VADA	WEB	TOMCAT	Apache Tomcat/8.
100	VADA	VD_HOST	VADA	20.20.20.103	VADA	DB	MARIA	10.1.45-MariaDB-
74	JIRANSNC	Linux_Test	CentOS7	20.20.20.10	CentOS7	OS	LINUX	CentOS Linux rele
44	JIRANSNC	Linux_Test	CentOS7	20.20.20.10	CentOS7	WEB	APACHE	Apache/2.4.6 (Ce
85	JIRANSNC	Linux_Test	CentOS7	20.20.20.10	CentOS7	DB	MYSQL	5.7.32 for Linux o

1. VADA 사용자 교육

I. 자산관리

- ▶ “자산관리” 메뉴를 통한 수동으로 자산을 등록 시 해당 자산에 대한 정보를 입력
- ▶ 시스템 정보, 자산 정보로 나뉘며 작성 완료 후 등록 (* 정보의 경우 필수 항목)

자산등록 정보	설 명
IP	• IP 설명 -> 확인 버튼으로 중복 체크
Platform Type	• 시스템 종류 (Ex : 운영체제 및 network 등)
진단방식	• 기본 방식은 Agent 방식으로 제공하며, 관리자가 환경에 맞게 방식을 선정하여 진단 가능 • 진단 방식 종류 - Agent, Interview, Manual, SSH
리소스 절약	• 취약점 진단 수행 시, 자산에서 사용되는 CPU사용률 조절
자산명	• VADA에서 관리상의 자산명
자산그룹	• 해당 자산의 그룹지정
운영담당자	• 자산의 담당자 지정 (정, 부 지정 가능)
자산분류	• OS, DB, WEB 중 선택
점검대상	자산, 분류 목록에 따른 점검대상 선택 (Ex : DB -> oracle, mysql)

1. VADA 사용자 교육

II. 보안규정

- ▶ 기본적인 보안규정(주요통신기반, 금융기반)을 제공하며, 고객사에 따라 맞춤형으로 사용 가능
- ▶ 기존 보안규정을 편집하여 새로운 보안규정을 생성 및 관리 가능

Ver. 3.0.0(R210303.001)
Copyright © JiranSNC

최고관리자(admin) 로그인 로그아웃 AGENT

규정

공통규정(1813)
Common Compliance(1292)
Extend Compliance(13)
금융기반(2020)(245)
주요기반(2018)(263)
Custom 규정(0)

사용자정의규정

사용자정의규정(0)
보안규정_테스트(20)

규정 목록

키워드 정의 사전조회 목록


공통 규정을 기반으로 사용자가 규정을 편집하여 별도로 관리

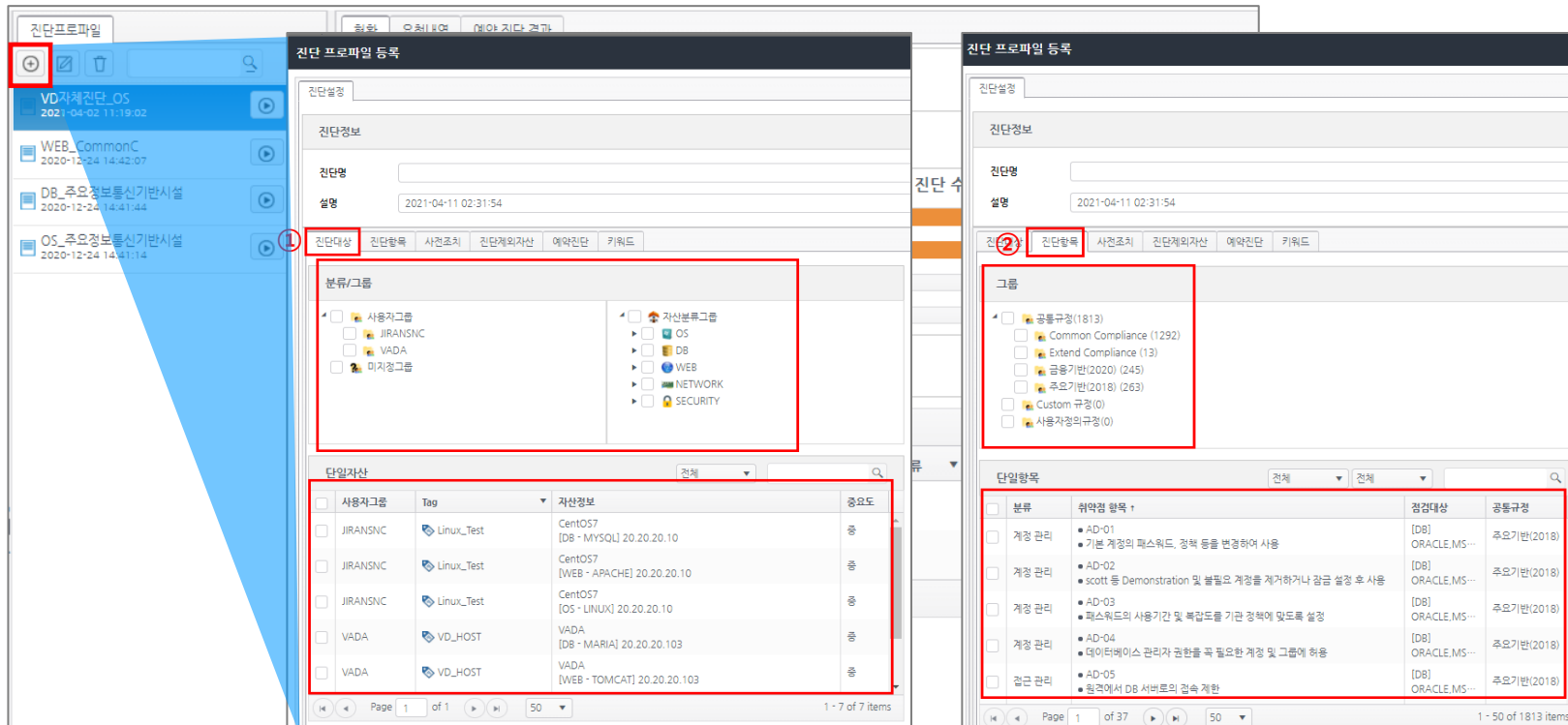
그룹	코드	분류	위약점 항목	자산분류	점검대상	중요도	상태	참조 규정	상세
보안규정_테스트	APC-01	계정 관리	패스워드의 주기적 변경	OS	WINDOWS_PC	상	DEFAULT	주요기반(2018)	
보안규정_테스트	APC-02	계정 관리	패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정	OS	WINDOWS_PC	상	DEFAULT	주요기반(2018)	
보안규정_테스트	APC-03	서비스 관리	공유 폴더 제거	OS	WINDOWS_PC	상	DEFAULT	주요기반(2018)	
보안규정_테스트	APC-04	서비스 관리	불필요한 서비스 제거	OS	WINDOWS_PC	상	DEFAULT	주요기반(2018)	
보안규정_테스트	APC-05	서비스 관리	Windows Messenger(MSN, NET 메신저 등)와 같은 상용 메신저의 사용 금지	OS	WINDOWS_PC	상	DEFAULT	주요기반(2018)	
보안규정_테스트	APC-06	패치 관리	HOT FIX 등 최신 보안패치 적용	OS	WINDOWS_PC	상	DEFAULT	주요기반(2018)	
보안규정_테스트	APC-07	패치 관리	최신 서비스팩 적용	OS	WINDOWS_PC	상	DEFAULT	주요기반(2018)	
보안규정_테스트	APC-08	패치 관리	MS-Office, 한글, 어도비 아크로벳 등의 응용 프로그램에 대한 최신 보안패치 및 번드 팩트업 적용	OS	WINDOWS_PC	상	DEFAULT	주요기반(2018)	
보안규정_테스트	APC-09	보안 관리	바이러스 백신 프로그램 설치 및 주기적 업데이트	OS	WINDOWS_PC	상	DEFAULT	주요기반(2018)	
보안규정_테스트	APC-10	보안 관리	바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화	OS	WINDOWS_PC	상	DEFAULT	주요기반(2018)	
보안규정_테스트	APC-11	보안 관리	OS에서 제공하는 침입차단 기능 활성화	OS	WINDOWS_PC	상	DEFAULT	주요기반(2018)	
보안규정_테스트	APC-12	보안 관리	화면보호기 대기 시간을 5~10분으로 설정 및 재시작 시 암호로 보호하도록 설정	OS	WINDOWS_PC	상	DEFAULT	주요기반(2018)	
보안규정_테스트	APC-13	보안 관리	CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방지 등 이동식 미디어에 대한 보안대책 수립	OS	WINDOWS_PC	상	DEFAULT	주요기반(2018)	
보안규정_테스트	APC-14	보안 관리	PC 내부의 미사용(3개월) ActiveX 제거	OS	WINDOWS_PC	상	DEFAULT	주요기반(2018)	
보안규정_테스트	APC-15	계정 관리	복구 콘솔에서 자동 로그인을 금지하도록 설정하여 사용하고 있는가?	OS	WINDOWS_PC	중	DEFAULT	주요기반(2018)	
보안규정_테스트	APC-16	서비스 관리	파일 시스템이 NTFS 포맷으로 되어 있는가?	OS	WINDOWS_PC	중	DEFAULT	주요기반(2018)	
보안규정_테스트	APC-17	서비스 관리	대상 시스템이 Windows 서버를 제외한 다른 OS로 릴리부팅이 가능하지 않도록 설정하여 사용하는가?	OS	WINDOWS_PC	중	DEFAULT	주요기반(2018)	
보안규정_테스트	APC-18	서비스 관리	브라우저 종료 시 임시 인터넷 파일 폴더의 내용을 삭제하도록 설정하여 사용하는가?	OS	WINDOWS_PC	하	DEFAULT	주요기반(2018)	

Page 1 of 1 200 items per page 1 - 20 of 20 items

1. VADA 사용자 교육

III. 진단수행

- ▶ 진단 수행은 진단 프로파일(진단대상 + 진단항목) 기준으로 수행
- ▶ 진단 프로파일  버튼을 클릭하여 등록
- ▶ 진단 대상 탭에서 진단 수행할 자산을 단일로 선택하거나, 자산이 속해 있는 그룹을 선택 가능
- ▶ 진단 항목 탭에서 진단 수행할 보안 항목 선택



진단프로파일 등록

진단대상

진단정보

진단명

설명

2021-04-11 02:31:54

진단대상 진단항목 사전조치 진단제외자산 예약진단 키워드

분류/그룹

사용자그룹

JIRANSNC

VADA

미지정그룹

자산분류그룹

OS

DB

WEB

NETWORK

SECURITY

단일자산

사용자그룹	Tag	자산정보	중요도
<input type="checkbox"/>	JIRANSNC	Linux_Test	CentOS7 [DB - MYSQL] 20.20.20.10
<input type="checkbox"/>	JIRANSNC	Linux_Test	CentOS7 [WEB - APACHE] 20.20.20.10
<input type="checkbox"/>	JIRANSNC	Linux_Test	CentOS7 [OS - LINUX] 20.20.20.10
<input type="checkbox"/>	VADA	VD_HOST	VADA [DB - MARIA] 20.20.20.103
<input type="checkbox"/>	VADA	VD_HOST	VADA [WEB - TOMCAT] 20.20.20.103

1 - 7 of 7 items

진단항목

진단정보

진단명

설명

2021-04-11 02:31:54

진단대상 진단항목 사전조치 진단제외자산 예약진단 키워드

그룹

공통규정(1813)

Common Compliance (1292)

Extend Compliance (13)

금융기반(2020) (245)

주요기반(2018) (263)

Custom 규정(0)

사용자정의규정(0)


단일항목

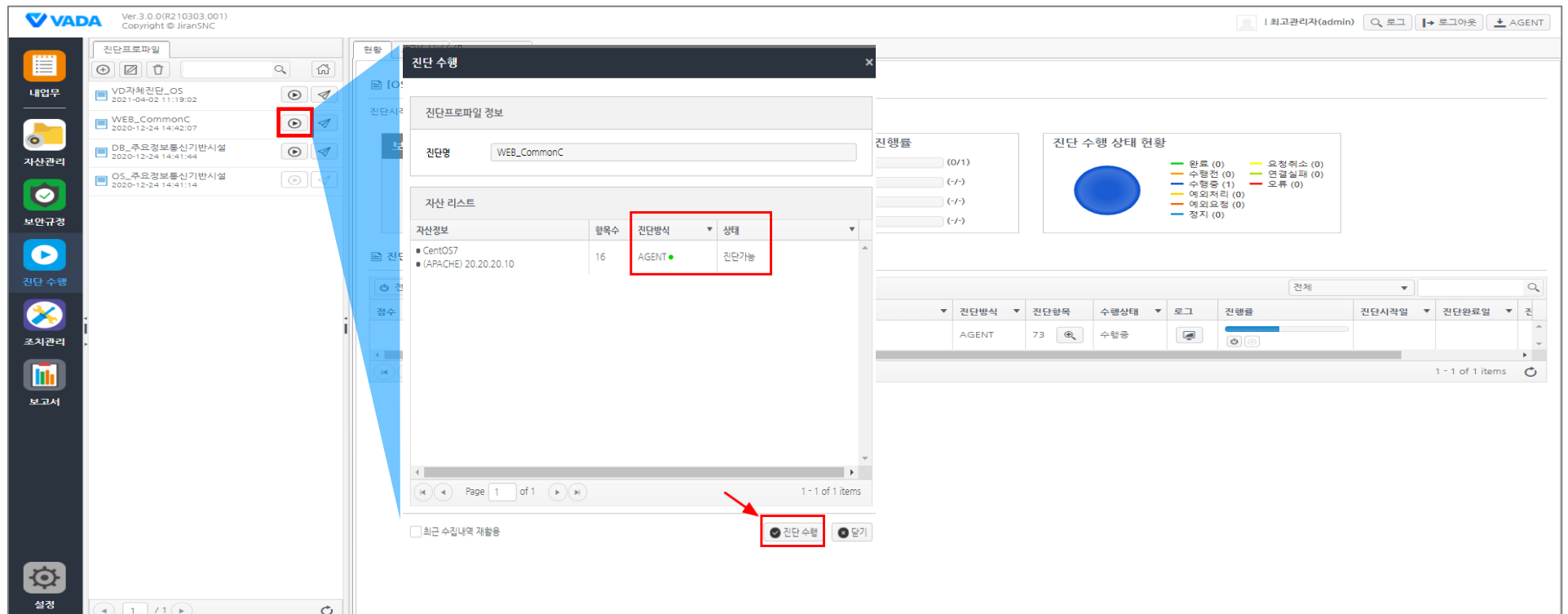
분류	위협점 항목	검증대상	공통규정
<input type="checkbox"/>	계정 관리	AD-01	[DB] 주요기반(2018)
<input type="checkbox"/>	계정 관리	AD-02	[DB] 주요기반(2018)
<input type="checkbox"/>	계정 관리	AD-03	[DB] 주요기반(2018)
<input type="checkbox"/>	계정 관리	AD-04	[DB] 주요기반(2018)
<input type="checkbox"/>	계정 관리	AD-05	[DB] 주요기반(2018)

1 - 50 of 1813 items

1. VADA 사용자 교육

III. 진단수행

- ▶ 생성 한 진단프로파일의  클릭하여 직접 진단 수행
- ▶ 진단 수행 시 자산 상태에 대해서 확인 후 진단 수행을 진행
- ▶ 수행 상태 및 진행률로 수행 완료 확인



The screenshot displays the VADA web interface. On the left sidebar, the '진단수행' (Diagnostic Execution) button is highlighted. A blue arrow points from this button to the '진단수행' button in the '진단프로파일' (Diagnostic Profile) list. Another red arrow points from the '진단수행' button in the '진단프로파일' list to the '진단수행' button in the '진단수행' modal window.

The '진단수행' modal window shows the following information:


- 진단프로파일 정보**: 진단명: WEB_CommonC
- 자산 리스트**:

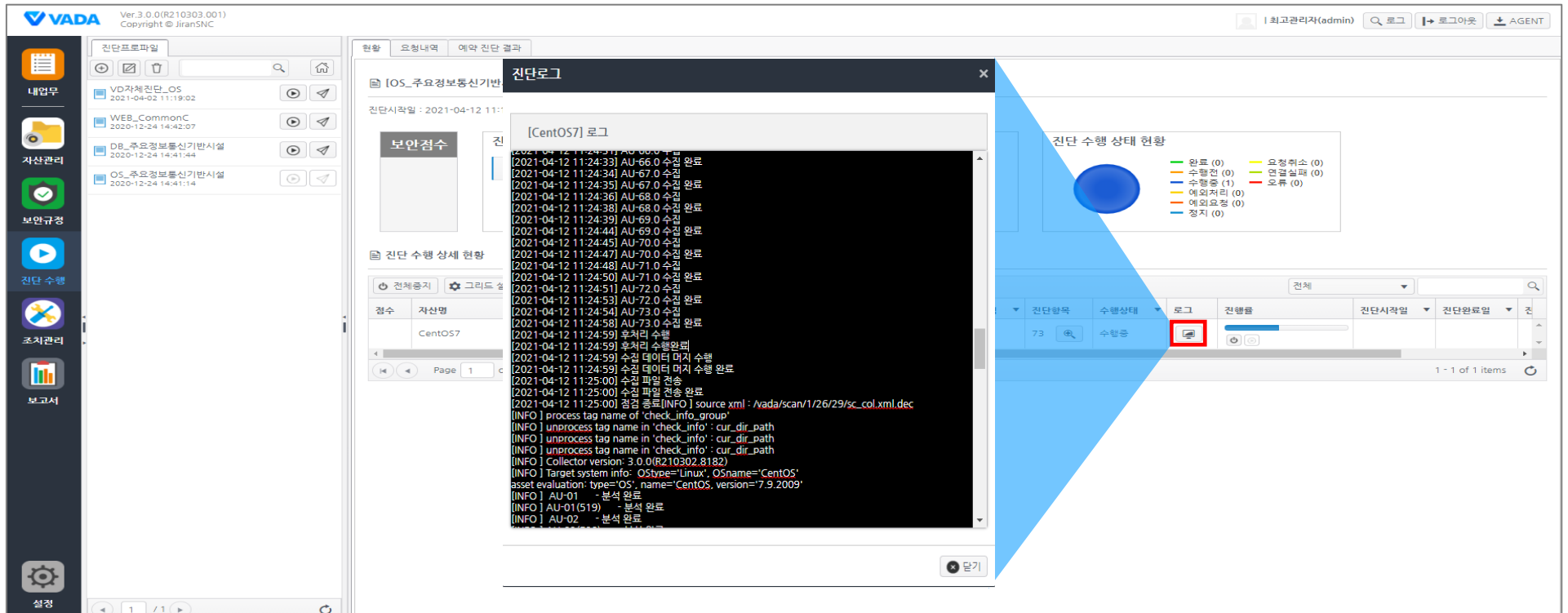
자산정보	월목수	진단방식	상태
CentOS7	16	AGENT	진단가능
(APACHE) 20.20.20.10			
- 진행률**: 0/1
- 진단수행 상태 현황**:
 - 완료 (0)
 - 수행중 (0)
 - 수행중 (1)
 - 예외처리 (0)
 - 예외요청 (0)
 - 정지 (0)
 - 요청취소 (0)
 - 연결실패 (0)
 - 오류 (0)
- 진행률**: 0/1
- 진행률**: 0/1

The '진단수행' button in the modal window is highlighted with a red box and a red arrow.

1. VADA 사용자 교육

III. 진단수행

- ▶ 진단로그 () 를 통해 실시간으로 수집 상황 및 진단 로그를 확인
- ▶ 진단 수행 중인 자산에 대해서 "상세 진단 수행 현황" 및 "진단 시 오류 내역" 정보에 대해서 체크 가능
- ▶ 각 자산별 진단 시 "재수행 / 중지" 버튼을 제공



The screenshot displays the VADA web application interface. On the left is a sidebar with navigation icons for '내업무' (My Work), '자산관리' (Asset Management), '보안규정' (Security Policy), '진단수행' (Diagnostic Execution), '초지관리' (Initial Management), and '보고서' (Report). The main area is divided into several sections. At the top, there's a header with the VADA logo, version information (Ver. 3.0.0(R210303.001)), and user information (최고관리자(admin)). Below the header, there's a '진단프로파일' (Diagnostic Profile) section on the left, listing various profiles like 'VD 자체진단_OS' and 'WEB_CommonC'. The central part of the interface shows the '진단수행 상태 현황' (Diagnostic Execution Status Overview) section, which includes a '진단로그' (Diagnostic Log) window. This window displays a list of diagnostic logs for 'CentOS7', showing timestamps, asset names, and completion status. A large blue arrow points from the '진단로그' window to the '진단수행 상태 현황' section, highlighting the '진단수행' (Diagnostic Execution) button. The '진단수행 상태 현황' section also includes a legend for diagnostic status (완료, 수행중, 예외처리, 중지) and a table of diagnostic results. The bottom of the interface shows a '진단결과' (Diagnostic Result) section with a table of results, including columns for '진단항목' (Diagnostic Item), '수행상태' (Execution Status), and '진행률' (Progress).

1. VADA 사용자 교육

IV. 조치관리

- ▶ [진단프로파일] - [진단리스트] - [전체 혹은 특정 자산] 을 선택하여 기본적인 진단 결과를 확인 가능
- ▶ 조치관리 메뉴는 최고관리자 및 보안관리자만 접근이 가능

① 조치관리를 하고자 하는 "프로파일 리스트" 중 하나를 선택

② 진단리스트 중 원하는 진단 이력을 선택

③ 전체 자산 혹은 특정 자산을 선택하여 우측 화면에서 진단결과를 확인 가능

진단결과	요청내역	진단프로파일	코드	분류	진단항목명	중요도	조치계획	결과	상태	기준수정내역	조치담당(장)
CentOS7 (LINUX) 20.20.20.10	OS_주요정보통신기반시설	AU-01	계정 관리	root 계정 원격 접속 제한	상		위약				lott1(lot)
CentOS7 (LINUX) 20.20.20.10	OS_주요정보통신기반시설	AU-02	계정 관리	패스워드 복잡성 설정	상		위약				lott1(lot)
CentOS7 (LINUX) 20.20.20.10	OS_주요정보통신기반시설	AU-03	계정 관리	계정 잠금 임계값 설정	상		위약				lott1(lot)
CentOS7 (LINUX) 20.20.20.10	OS_주요정보통신기반시설	AU-04	계정 관리	패스워드 파일 보호	상		알호				lott1(lot)
CentOS7 (LINUX) 20.20.20.10	OS_주요정보통신기반시설	AU-05	파일 및 디렉토리 관리	root 홈, 패스 디렉토리 권한 및 패스 설정	상		알호				lott1(lot)
CentOS7 (LINUX) 20.20.20.10	OS_주요정보통신기반시설	AU-06	파일 및 디렉토리 관리	파일 및 디렉토리 소유자 설정	상		알호				lott1(lot)
CentOS7 (LINUX) 20.20.20.10	OS_주요정보통신기반시설	AU-07	파일 및 디렉토리 관리	/etc/passwd 파일 소유자 및 권한 설정	상		알호				lott1(lot)
CentOS7 (LINUX) 20.20.20.10	OS_주요정보통신기반시설	AU-08	파일 및 디렉토리 관리	/etc/shadow 파일 소유자 및 권한 설정	상		알호				lott1(lot)
CentOS7 (LINUX) 20.20.20.10	OS_주요정보통신기반시설	AU-09	파일 및 디렉토리 관리	/etc/hosts 파일 소유자 및 권한 설정	상		알호				lott1(lot)
CentOS7 (LINUX) 20.20.20.10	OS_주요정보통신기반시설	AU-10	파일 및 디렉토리 관리	/etc/xxinetd.conf 파일 소유자 및 권한 설정	상		위약				lott1(lot)
CentOS7 (LINUX) 20.20.20.10	OS_주요정보통신기반시설	AU-11	파일 및 디렉토리 관리	/etc/syslog.conf 파일 소유자 및 권한 설정	상		알호				lott1(lot)
CentOS7 (LINUX) 20.20.20.10	OS_주요정보통신기반시설	AU-12	파일 및 디렉토리 관리	/etc/services 파일 소유자 및 권한 설정	상		알호				lott1(lot)
CentOS7 (LINUX) 20.20.20.10	OS_주요정보통신기반시설	AU-13	파일 및 디렉토리 관리	SUID, SGID, Sticky bit 설정 및 권한 설정	상		위약				lott1(lot)
CentOS7 (LINUX) 20.20.20.10	OS_주요정보통신기반시설	AU-14	파일 및 디렉토리 관리	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상		알호				lott1(lot)
CentOS7 (LINUX) 20.20.20.10	OS_주요정보통신기반시설	AU-15	파일 및 디렉토리 관리	world writable 파일 점검	상		알호				lott1(lot)
CentOS7 (LINUX) 20.20.20.10	OS_주요정보통신기반시설	AU-16	파일 및 디렉토리 관리	/dev에 존재하지 않는 device 파일 점검	상		알호				lott1(lot)
CentOS7 (LINUX) 20.20.20.10	OS_주요정보통신기반시설	AU-17	파일 및 디렉토리 관리	\$HOME/.rhosts, hosts.equiv 사용 금지	상		알호				lott1(lot)
CentOS7 (LINUX) 20.20.20.10	OS_주요정보통신기반시설	AU-18	파일 및 디렉토리 관리	접속 IP 및 포트 제한	상		위약				lott1(lot)

1. VADA 사용자 교육

IV. 조치관리

- ▶ "결과수정" 버튼을 통해 진단 결과와 상관없이 결과수정 및 수정 사유에 대해서 처리 가능
- ▶ 결과수정 및 수정사유에 대한 선택지는 아래 그림을 참조
- ▶ 추가적으로 증빙자료를 업로드하여 관리 용이 (단, 10MB 이하의 1개의 파일만 허용)

진단 결과 수정

결과수정: 알고

수정사유: 기타

증빙자료 관리

결과수정 및 수정사유에 대한 선택지는 아래 그림을 참조

진단항목명	코드	분류	진단항목명	중요도	조치계획	결과	상태	기준수정내역	조치담당자
AU-01	계정 관리	root 계정 원격 접속 제한	상		취약				lott1(lot)
AU-02	계정 관리	패스워드 복잡성 설정	상		취약				lott1(lot)
AU-03	계정 관리	계정 잠금 임계값 설정	상		취약				lott1(lot)
AU-04	계정 관리	패스워드 파일 보호	상		알고				lott1(lot)
AU-05	파일 및 디렉토리 관리	root 홈, 패스 디렉토리 권한 및 패스 설정	상		알고				lott1(lot)
AU-06	파일 및 디렉토리 관리	파일 및 디렉토리 소유자 설정	상		알고				lott1(lot)
AU-07	파일 및 디렉토리 관리	/etc/passwd 파일 소유자 및 권한 설정	상		알고				lott1(lot)
AU-08	파일 및 디렉토리 관리	/etc/shadow 파일 소유자 및 권한 설정	상		알고				lott1(lot)
AU-09	파일 및 디렉토리 관리	/etc/hosts 파일 소유자 및 권한 설정	상		알고				lott1(lot)
AU-10	파일 및 디렉토리 관리	/etc/xxinetd.conf 파일 소유자 및 권한 설정	상		리뷰				lott1(lot)
AU-11	파일 및 디렉토리 관리	/etc/syslog.conf 파일 소유자 및 권한 설정	상		알고				lott1(lot)
AU-12	파일 및 디렉토리 관리	/etc/services 파일 소유자 및 권한 설정	상		알고				lott1(lot)
AU-13	파일 및 디렉토리 관리	SUID, SGID, Sticky bit 설정 및 권한 설정	상		취약				lott1(lot)
AU-14	파일 및 디렉토리 관리	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상		알고				lott1(lot)
AU-15	파일 및 디렉토리 관리	world writable 파일 점검	상		알고				lott1(lot)
AU-16	파일 및 디렉토리 관리	/dev에 존재하지 않는 device 파일 점검	상		알고				lott1(lot)
AU-17	파일 및 디렉토리 관리	\$HOME/.rhosts, hosts.equiv 사용 금지	상		알고				lott1(lot)
AU-18	파일 및 디렉토리 관리	접속 IP 및 포트 제한	상		취약				lott1(lot)

1. VADA 사용자 교육

IV. 조치관리

- ▶ 진단 결과에 대해 서버 담당자에게 조치요청 및 조치계획을 설정하여 취약점 결과를 관리
- ▶ 조치요청의 경우 **"가장 최근 진단 항목"**에서만 요청이 가능
- ▶ 조치기한 및 요청하고자 하는 메시지를 기재하여 서버 담당자에게 요청 가능
- ▶ "결과수정" 과 동일하게 증빙파일을 첨부하여 관리가 가능

Ver. 3.0.0 (R210303.001)
Copyright © JiranSNC

최고관리자(admin) | 로그 | 로그아웃 | AGENT

공통

- 자산분류그룹 (7)
- OS (3)
- DB (2)
- WEB (2)

자산관리

자산그룹 Tag

- 사용자그룹 (7)
- JIRANSNC (4)
- VADA (3)
- 미지정그룹 (0)

보안규정

진단 수행

조치관리

보고서

진단프로파일

진단결과

조치요청

조치계획

결과수정

기존 수정내역 적용

기존 수정 내역 초기화

그리드 설정

코드	분류	진단항목명	중요도	조치계획	결과	상태	기존수정내역	조치담당자(정)
AU-01	계정 관리	root 계정 원격 접속 제한	상		취약			lott1(lot)
AU-02	계정 관리	패스워드 복잡성 설정	상		취약			lott1(lot)
AU-03	계정 관리	계정 잠금 임계값 설정	상		취약			lott1(lot)
AU-04	계정 관리	패스워드 파일 보호	상		알호			lott1(lot)

조치기한

2021-04-12 15:20

☐ 기한없음

내용

증빙자료 관리

파일업로드 (총용량은 10MB 이하의 1개의 파일만 업로드 할 수 있습니다.)

첨부 파일 목록

1 / 155 of 155 items

