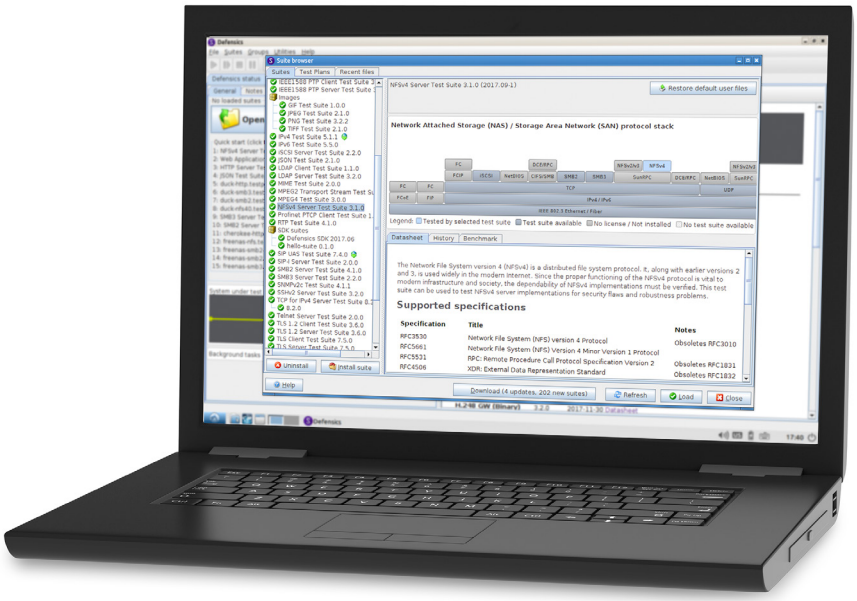
SYNOPSYS®

Defensics
퍼징 테스팅 도구

신규 도입 또는 구축하는
소프트웨어에서
보안성 향상,
시스템 상호운용성 보장,
보안 취약점 검출

제품 개요

Defensics® 퍼징 테스팅은 포괄적이고 자동화된 블랙박스 솔루션입니다. 조직은 이를 통해 소프트웨어의 보안 취약점을 찾아내고 문제를 해결할 수 있습니다. Defensics는 체계적이고 지능적인 네거티브 테스트를 진행하기 때문에 조직에서는 출시를 늦추거나 운영비를 늘리지 않고 소프트웨어 보안을 확보할 수 있습니다.

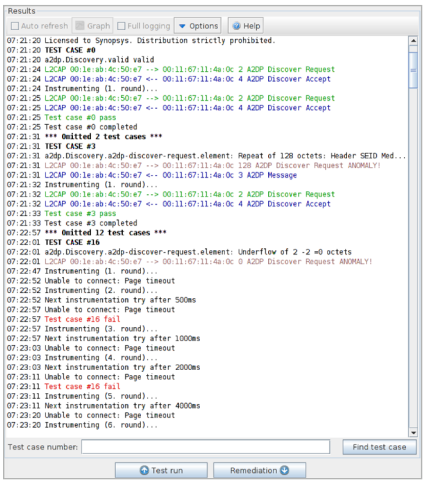


Defensics의 합리적인 유저 인터페이스는 프로세스의 각 단계를 하나씩 안내하며 진행하기 때문에 고급 퍼징 테스팅을 매우 쉽게 할 수 있도록 만들어 줍니다.

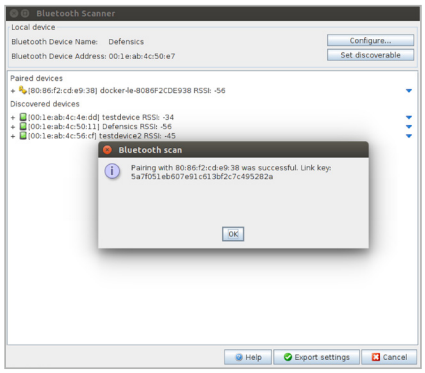
주요 기능

지능형 퍼징 엔진

Defensics 엔진은 인터페이스, 프로토콜, 파일 포맷 등 입력 형식에 대한 지식을 기반으로 프로그램됩니다. 입력 형식 내에서 통신을 관장하는 규칙을 엔진이 잘 알고 있기 때문에 그 입력 형식만의 보안 취약점을 악용하는 테스트 케이스를 제공합니다. 이처럼 퍼징 테스팅은 지능적이고 체계적이기 때문에 비용 증가와 보안성 저해 없이 테스팅 시간을 단축할 수 있습니다.



Defensics 보고서에는 사용자가 이상 반응의 근본 원인을 찾아내기 위해 참고할 수 있는 메시지 시퀀스 로그가 들어 있습니다.



Defensics에는 Device Explorer와 같은 자동 기능이 있어 사용자가 테스팅 중에 수동으로 구성을 할 필요가 없습니다.

포괄적인 퍼징 솔루션

300개 이상의 생성된 Test suite가 준비되어 있어 퍼즈 시간이 짧고 수동 테스트의 부담이 적습니다. Test suite는 새 입력 형식과 사양, RFC가 나올 때마다 업데이트합니다.

- Test suite는 어느 것이든 메시지 시퀀스를 미세 조정하여 커스터마이징할 수 있습니다. 데이터 시퀀스 편집기를 통해 Defensics의 지정 범위에 속하지 않는 케이스에도 대응할 수 있습니다.
- 확장을 더 해야 한다면 템플릿 퍼저(fuzzer)를 이용하면 됩니다. Universal Data Fuzzer는 파일 포맷 템플릿 퍼저이며, SDK Express는 사용자가 제공한 샘플 파일을 리버스 엔지니어링하여 테스트 케이스를 생성할 수 있는 솔루션입니다.
- 독자적인 입력 형식이나 커스텀 입력이 있다면 Defensics SDK로 자체 Test suite를 작성해도 됩니다. 이 솔루션은 Java와 일부 트랜스포트 레이어를 지원하며 인스트루먼테이션 기능을 탑재하고 있습니다.
- FuzzBox 지원으로 테스팅 속도를 올릴 수도 있습니다. 커스텀 하드웨어에서 테스트를 바로 시행하므로 무선 LAN과 IoT 프로토콜을 퍼징하기가 쉽습니다.

개발 라이프사이클에 대부분 적합

Defensics은 그 워크플로가 기술과 프로세스 측면에서 사실상 모든 환경에 적합합니다. Defensics는 기존 SDL을 채용하든, CI 개발 라이프사이클을 채용하든 개발 초기에 퍼징 테스팅을 적용하므로 비용 대비 높은 효율로 취약점을 찾아내 해결할 수 있습니다. 독특한 형태의 개발 라이프사이클이 아니라면 Synopsys의 노련한 전문 서비스팀이 퍼징 테스팅 체크포인트를 찾아내 퍼징 테스팅 지표를 정의하고 퍼징 테스팅 성숙도 프로그램을 만들어 드립니다.

단순히 개발 프로세스에 맞춰 넣는 것이 아니라 주변 기술과 협업하는 것입니다. Defensics는 API와 데이터 내보내기 기능을 통해 데이터를 공유하여 추가 보고 및 분석을 할 수 있으므로 진정한 플러그 앤 플레이 퍼저라고 할 만합니다.

데이터가 풍부한 상세 보고서로 효율적인 문제 해결

- **컨텍스트화 로그.** 문제 해결 로그는 Defensics와 테스트 대상 시스템(SUT) 간의 프로토콜 경로와 메시지 시퀀스를 자세히 담고 있어 각 취약점의 발생원인과 기술적 영향을 찾을 때 유용합니다.
- **취약점 매핑.** Defensics는 취약점을 CWE, 주입 형식과 같은 산업 표준과 매핑하므로 정보 탐색을 강화하고 시정을 촉진하는 역할을 합니다.
- **문제 재현.** Defensics는 취약점 발생원인을 한 테스트 케이스로 줄이므로 이를 통해 문제를 재현하고 수정 사항을 확인할 수 있습니다.
- **문제 해결 패키지.** 소프트웨어 공급업자를 대신해 암호화된 문제 해결 패키지를 생성하여 공급망에서 안전한 협업과 문제 해결을 촉진할 수 있습니다.

자동화를 통한 퍼징 테스팅 규모 확대

Defensics는 테스트 대상 스캐닝부터 연결할 계층 개수 결정까지 API가 다채로워 자동화가 유연하고 확장성이 좋습니다. 이를 통해, 다음과 같은 요구를 충족합니다.

- 단일 장치 테스트
- 반복 가능한 자동화 설정으로 테스트 계획 상시 준수
- 최신 스케일러블 가상화를 통한 테스팅 시간 단축

Defensics 퍼징 테스팅 | Test Suite 카탈로그

인증, 허가, 계정 (AAA)
- Diameter 클라이언트/서버
- EAPOL 서버
- Kerberos 서버
- LDAPv3 클라이언트/서버
- RADIUS 클라이언트/서버
- TACACS+ 클라이언트/서버
- MACsec 서버

애플리케이션
- FIX
- JSON Format
- 웹 애플리케이션
- WebSocket 클라이언트/서버
- XML SOAP 클라이언트/서버
- XML File
- XMPP 서버
- AMQP 서버
- WAMP 서버
- OWAMP 서버
- TWAMP 서버

오토모티브
- CAN Bus
- CAN FD
- DoIP 서버
- gPTP 서버
- SOME/IP
- SRP 서버

무선 통신 코어
- BICC/M3UA
- GRE
- GTP Prime
- GTPv0
- PMIPv6 클라이언트/서버
- SCTP 클라이언트/서버
- SMPP
- SMS (SMPP Injection)
- SMS (파일 Injection)
- MAP
- BSSAP
- BSSAP+
- CAP
- INAP
- ISUP
- MTP3 / M2UA|M2PA
- TCAP / SCCP / M3UA
- SBI 클라이언트/서버

IP
- DHCP/BOOTP 클라이언트/서버
- DHCPv6 클라이언트/서버
- DNS 클라이언트/서버
- FTP 클라이언트/서버
- HTTP 클라이언트/서버
- HTTP/2 클라이언트/서버
- ICAP 서버
- IPv4 패키지
  - ARP 클라이언트/서버
  - ICMP
  - IGMP
  - IPv4
  - TCP for IPv4 클라이언트/서버
- IPv6 패키지
  - ICMPv6
  - IPv6
  - TCP for IPv6 클라이언트/서버
- SOCKS 클라이언트/서버
- Multicast DNS
- PPP over L2TP 클라이언트
- PPPoE

이메일
- IMAP4 클라이언트/서버
- MIME
- POP3 서버
- SMTP 클라이언트/서버

커스텀
- SDK Express
- Universal ASN.1 BER
- Universal Fuzzer

ICS
- 60870-5-104 (iec104) 클라이언트/서버
- 61850/Goose/SV
- 61850/MMS 클라이언트/서버
- BACNET
- CIP 서버
- COAP 서버
- DNP3 클라이언트/서버
- MQTT 클라이언트/서버
- Modbus Master
- Modbus PLC
- OPC UA 서버
- Profinet DCP
- Profinet PTCP 클라이언트/서버
- DLMS/COSEM 클라이언트/서버
- ISASecure Testing Solution

Link 관리
- LACP (802.3ad)
- STP/RSTP/MSTP/ESTP

미디어
- 아카이브 패키지
  - GZIP
  - JAR
  - ZIP
- 오디오 패키지
  - MP3
  - MPEG4 (M4A/MP4)
  - OGG
  - WAV
  - Windows Media (WMA/WMV)
- 이미지 패키지
  - GIF
  - JPEG
  - PNG
  - TIFF
- 비디오 패키지
  - H.264 File Suite
  - H.264 RTP Format
  - MPEG2-TS
  - MPEG4 (M4A/MP4)
  - OGG
  - Windows Media (WMA/WMV)

메디컬
- DICOM 서버
- HL7v2 서버

메트로 이더넷
- BFD
- CFM (802.1ag, Y.1731)
- E-LMI (MEF-16)
- Ethernet (802.3, 802.1Q)
- GARP (802.1D)
- LLDP (802.1AB)
- OAM (802.3ah)
- PBB-TE 서버
- 동기화 이더넷(ESMC)

공용 키 인프라(PKI)
- CMPv2 클라이언트/서버
- CSR

원격 관리
- CWMP (TR-69) ACS
- CWMP (TR-69) CPE
- IPMI 서버
- NETCONF
- PCP 서버
- SNMP trap
- SNMPv2c 서버
- SNMPv3 서버
- SSHv1 서버
- SSHv2 서버
- Syslog
- TFTP 서버
- Telnet 서버

라우팅
- BGP4+ 클라이언트/서버
- IS-IS
- LDP
- MPLS 서버
- MSDP
- OSPFv2
- OSPFv3
- Openflow 컨트롤러
- Openflow 스위치
- PIM-SM/DM
- RIP
- RIPng
- RSVP
- TRILL 서버
- VRRP
- COPS 클라이언트/서버

저장장치
- CIFS/SMB 서버
- DCE/RPC 서버
- NFSv3 서버
- NFSv4.0 / 4.1 서버
- Netbios 서버
- DNNG
- SMBv2 클라이언트/ServerMP
- SMBv3 클라이언트/서버
- SunRPC 서버
- iSCSI 클라이언트/서버

시간 동기화
- IEEE1588 PTP 클라이언트/서버
- NTP 클라이언트/서버

Universal Plug and Play
- UPnP Package
  - UPnP Multicast Eventing
  - UPnP SOAP
  - UPnP SSDP Control Point
  - UPnP SSDP Device

VoIP
- H.323 클라이언트/서버
- H.284 GW Binary/Text
- H.284 MGC Binary/Text
- MGCP 서버
- MSRP 서버
- RTP/RTCP/SRTP
- RTSP 클라이언트/서버
- SIP UAC
- SIP UAS (+TT)
- SIP-I 서버
- STUN 클라이언트/서버
- TURN 클라이언트/서버
- SigComp 서버

VPN
- DTLS 클라이언트/서버
- IKEv2 클라이언트/서버
- IPSec
- ISAKMP/IKEv1 클라이언트/서버
- L2TPv2/v3 클라이언트/서버
- OCSP 클라이언트/서버
- SCEP
- SSTPT
- TLS/SSL 클라이언트/서버
- X.509v3 인증
- VXLAN

무선
- Zigbee 패키지
  - FuzzBox Zigbee APS
  - FuzzBox Zigbee MAC
  - FuzzBox Zigbee NWK
- Thread 패키지
  - FuzzBox Thread 6LoWPAN
  - FuzzBox Thread MAC
- Bluetooth LE 패키지
  - ATT 클라이언트/서버
  - Advertisement
  - HOGP Host
  - Health
  - L2CAP 서버
  - LL Peripheral
  - Profiles
  - SMP 클라이언트/서버
- Bluetooth 패키지
  - A2DP
  - AVRCP
  - BNEP
  - HFP AG/Unit
  - HSP AG/Unit
  - L2CAP
  - MAP 클라이언트
  - OBEX-서버
  - PBAP 클라이언트
  - RFCOMM
  - SDP
- Wi-Fi AP 패키지
  - 802.11 WLAN AP
  - 802.11 WPA AP
  - 802.11 WPA3 AP
- Wi-Fi 클라이언트 패키지
  - 802.11 WLAN 클라이언트
  - 802.11 WPA 클라이언트
  - 802.11 WPA3 클라이언트

5G
- GTPv2-C 클라이언트/서버
- S1AP/NAS 클라이언트/서버
- GTPv1 클라이언트/서버
- E1AP 클라이언트/서버
- NGAP/NAS 클라이언트/서버
- X2AP 클라이언트/서버
- XnAP 클라이언트/서버
- PFCP 클라이언트/서버
- F1AP 클라이언트/서버

모니터링과 엔진 기능

Instrumentation
- 유효 테스트 케이스
- Syslog
- 에이전트
- SNMP
- 테스팅 시 사용자 지정 스크립팅

SafeGuard 체커
- 증폭
- 우회 인증
- 블라인드 LDAP Injection
- 블라인드 SQL Injection
- 인증서 확인
- 서명인의 이름을 RRSIG 기록으로 압축
- 크로스 사이트 요청 위조
- 크로스 사이트 스크립팅
- ECDH 공용 키 검증
- 유효 케이스 대비 추가 쿠키
- Heartbleed
- 정보 유출
- 불충분한 랜덤값
- 회신에 LDAP Injection
- 비정상적 형태의 HTTP
- 원격 실행
- 회신에 SQL Injection
- SMP 불안정 페어링 매개변수
- 예상치 못한 데이터
- 비보호 자격증명
- 안전하지 않은 암호화

이상 데이터 카테고리
- ASN.1/BER 이상
- 자격증명 이상
- 심도 있는 패킷 검사
- EICAR 안티바이러스 테스트 파일
- GTUBE (Generic Test for Unsolicited Bulk Email)
- Control Plane Injection 이상
- 정수 이상
- 네트워크 주소 이상
- 오버플로 이상
- 언더플로 이상

주: Test Suite은 사전 예고없이 변경될수 있습니다. 최신 목록은 문의 바랍니다.

SYNOPSYS®

Synopsys의 차별성

Synopsys는 위험을 최소화하고 속도와 생산성은 극대화하여 개발팀이 안전한 고품질 소프트웨어를 개발할 수 있도록 지원합니다. 애플리케이션 보안 분야의 리더로서 Synopsys는 정적 분석, 소프트웨어 구성 분석, 동적 분석 솔루션을 제공합니다. 개발팀은 이를 활용하여 자사코드, 오픈소스 컴포넌트, 애플리케이션 동작의 취약점과 결함을 빠르게 발견하고 보완할 수 있습니다. 업계 최고 수준의 도구, 서비스, 전문성을 겸비한 Synopsys와 함께라면 DevSecOps 및 소프트웨어 개발 주기 전체에서 보안과 품질을 최적할 수 있습니다.

자세한 정보는 www.synopsys.com/software에서 확인할 수 있습니다.

Synopsys, Inc.
경기도 성남시 분당구 판교역로 235
에이치 스퀘어 N동 5층
(우)13494
시높시스코리아

Contact us:
대표 번호: (82) 2-3404-2700
Email: sig-info@synopsys.com