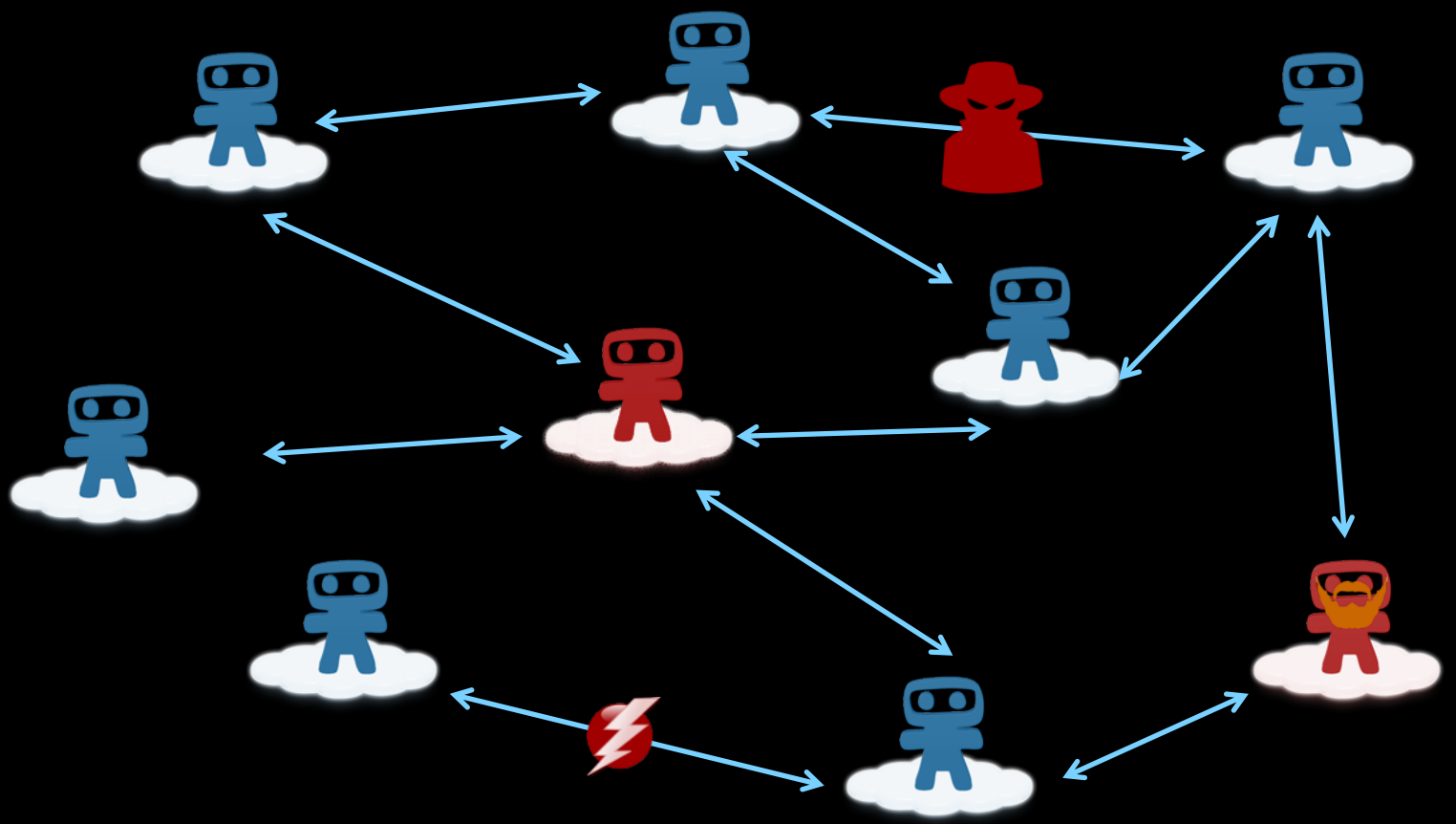
SYNOPSYS®
Silicon to Software™

IoT: Attack of the Clone Army?

Dr Ralf Huuck

London, December 2016

Some IoT Threat Vectors



Man-In-The-Middle between machines

Faulty Device

Faulty Connection

Outdated Software/ Default Passwords

SYNOPSYS®

Hack One – Control All

Billions of IoT devices in the near future.

Each IoT Product million times the same.

One Breach = One Clone Army.


BreakingNews

~~Breaking~~ Old News

145,607 hacked digital video recorders and IP cameras.

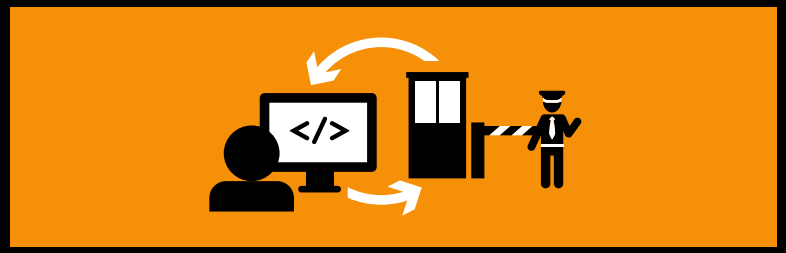
SYNOPSYS®

Where to Go From Here?

Prevention from the Ground Up

Manufacturer

Each component needs security



Each integration needs security

Consumer

ISO

UL

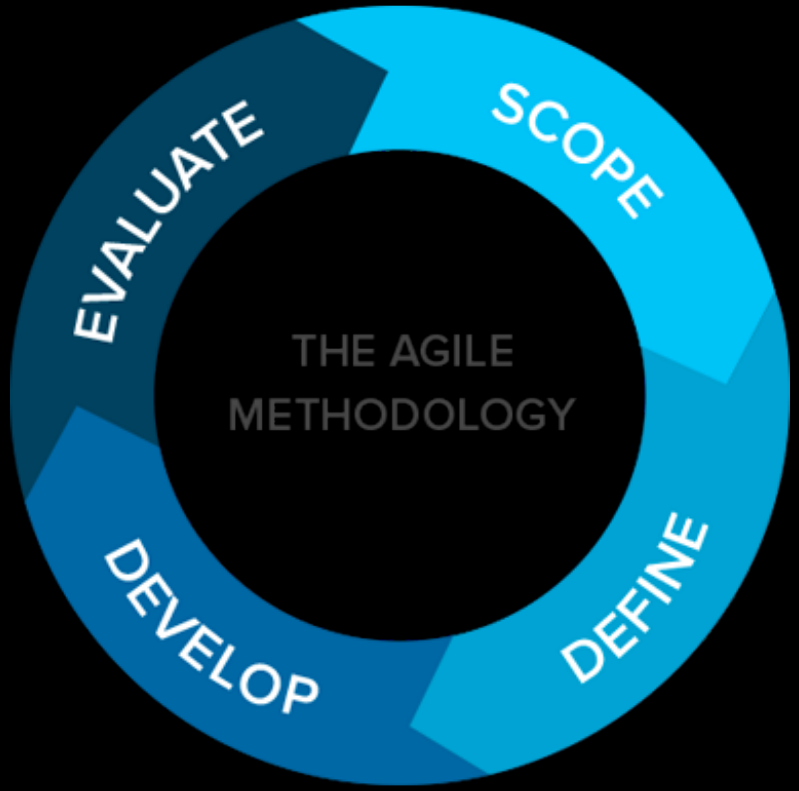
TÜV SÜD

SYNOPSYS®

Securing Software Lifecycle: Automation

Smart Protocol Testing

Source Code Security Analysis



Security Test Plan Optimization

SYNOPSYS®

Example: Protocol Fuzzing

Protocols

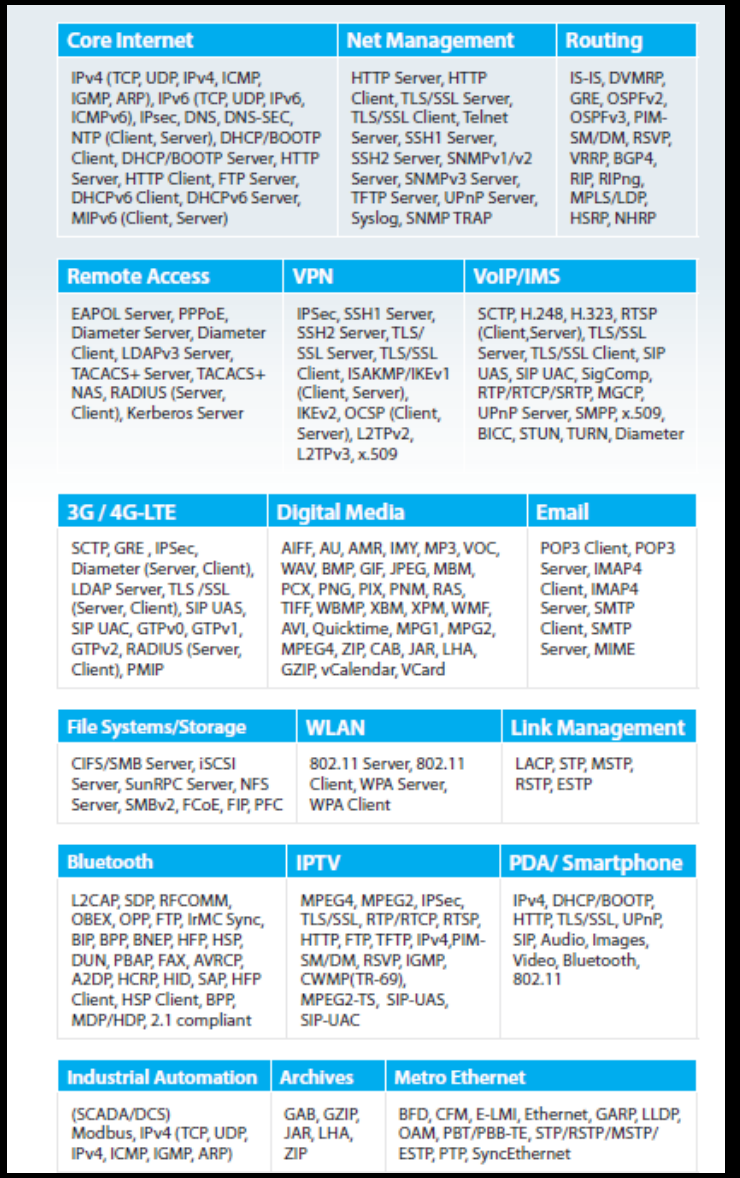
Software systems and components communicate

Automated Malformed Input Testing

Finding unknown, exploitable vulnerabilities

Hacking Preventions

Patch holes before exploitation



Core Internet	Net Management	Routing
IPv4 (TCP, UDP, IPv4, ICMP, IGMP, ARP), IPv6 (TCP, UDP, IPv6, ICMPv6), IPsec, DNS, DNS-SEC, NTP (Client, Server), DHCP/BOOTP Client, DHCP/BOOTP Server, HTTP Server, HTTP Client, FTP Server, DHCPv6 Client, DHCPv6 Server, MIPv6 (Client, Server)	HTTP Server, HTTP Client, TLS/SSL Server, TLS/SSL Client, Telnet Server, SSH1 Server, SSH2 Server, SNMPv1/v2 Server, SNMPv3 Server, TFTP Server, UPnP Server, Syslog, SNMP TRAP	IS-IS, DVMRP, GRE, OSPFv2, OSPFv3, PIM-SM/DM, RSVP, VRRP, BGP4, RIP, RIPng, MPLS/LDP, HSRP, NHRP

Remote Access	VPN	VoIP/IMS
EAPOL Server, PPPoE, Diameter Server, Diameter Client, LDAPv3 Server, TACACS+ Server, TACACS+ NAS, RADIUS (Server, Client), Kerberos Server	IPSec, SSH1 Server, SSH2 Server, TLS/SSL Server, TLS/SSL Client, ISAKMP/IKEv1 (Client, Server), IKEv2, OCSP (Client, Server), L2TPv2, L2TPv3, x.509	SCTP, H.248, H.323, RTSP (Client,Server), TLS/SSL Server, TLS/SSL Client, SIP UAS, SIP UAC, SigComp, RTP/RTCP/SRTP, MGCP, UPnP Server, SMPP, x.509, BICC, STUN, TURN, Diameter

3G / 4G-LTE	Digital Media	Email
SCTP, GRE , IPSec, Diameter (Server, Client), LDAP Server, TLS /SSL (Server, Client), SIP UAS, SIP UAC, GTPv0, GTPv1, GTPv2, RADIUS (Server, Client), PMIP	AIFF, AU, AMR, IMY, MP3, VOC, WAV, BMP, GIF, JPEG, MBM, PCX, PNG, PIX, PNM, RAS, TIFF, WBMP, XBM, XPM, WMF, AVI, Quicktime, MPG1, MPG2, MPEG4, ZIP, CAB, JAR, LHA, GZIP, vCalendar, VCard	POP3 Client, POP3 Server, IMAP4 Client, IMAP4 Server, SMTP Client, SMTP Server, MIME

File Systems/Storage	WLAN	Link Management
CIFS/SMB Server, iSCSI Server, SunRPC Server, NFS Server, SMBv2, FCoE, FIP, PFC	802.11 Server, 802.11 Client, WPA Server, WPA Client	LACP, STP, MSTP, RSTP, ESTP

Bluetooth	IPTV	PDA/ Smartphone
L2CAP, SDP, RFCOMM, OBEX, OPP, FTP, IrMC Sync, BIP, BPP, BNEP, HFP, HSP, DUN, PBAP, FAX, AVRCP, A2DP, HCRP, HID, SAP, HFP Client, HSP Client, BPP, MDP/HDP, 2.1 compliant	MPEG4, MPEG2, IPSec, TLS/SSL, RTP/RTCP, RTSP, HTTP, FTP, TFTP, IPv4,PIM-SM/DM, RSVP, IGMP, CWMP(TR-69), MPEG2-TS, SIP-UAS, SIP-UAC	IPv4, DHCP/BOOTP, HTTP, TLS/SSL, UPnP, SIP, Audio, Images, Video, Bluetooth, 802.11

Industrial Automation	Archives	Metro Ethernet
(SCADA/DCS) Modbus, IPv4 (TCP, UDP, IPv4, ICMP, IGMP, ARP)	GAB, GZIP, JAR, LHA, ZIP	BFD, CFM, E-LMI, Ethernet, GARP, LLDP, OAM, PBT/PBB-TE, STP/RSTP/MSTP/ ESTP, PTP, SyncEthernet

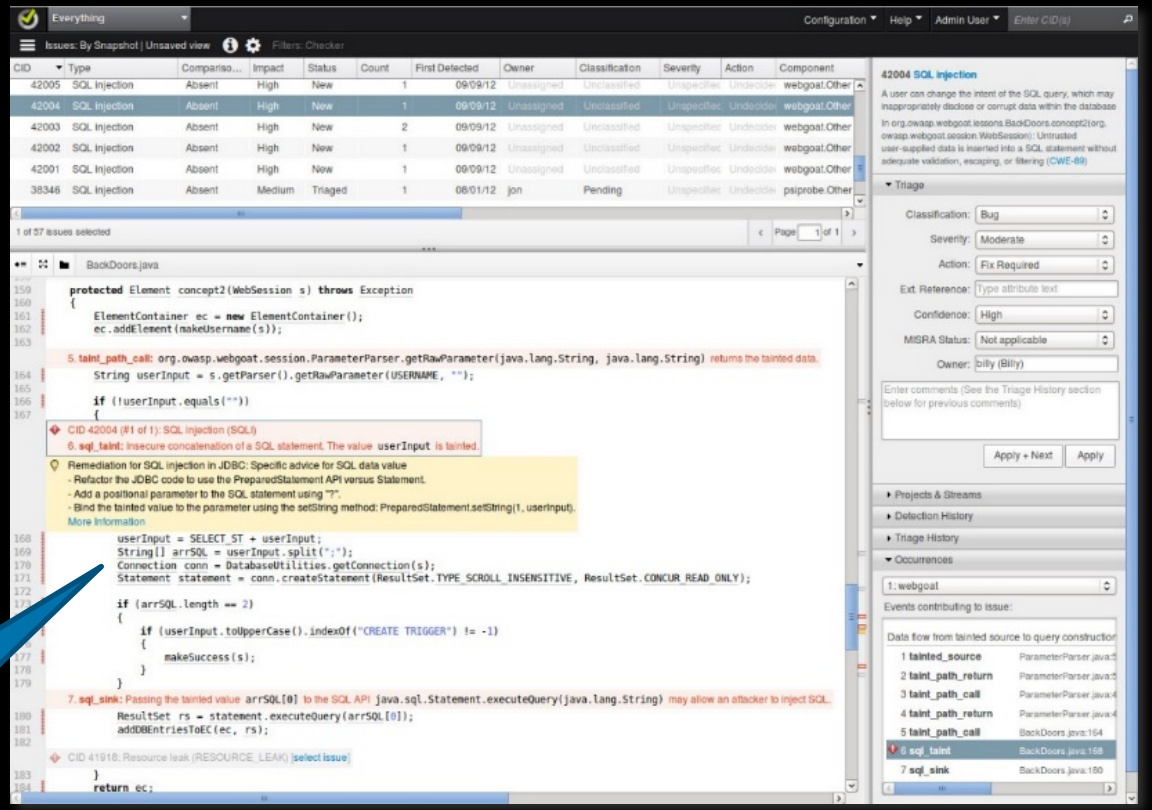
SYNOPSYS®

Example: Static Code Analysis

XSS, Injections, CSRF,
Security vulnerabilities

Memory violations,
Logic errors, Defects

Race conditions, Memory corruption,
Concurrency errors, Deadlocks



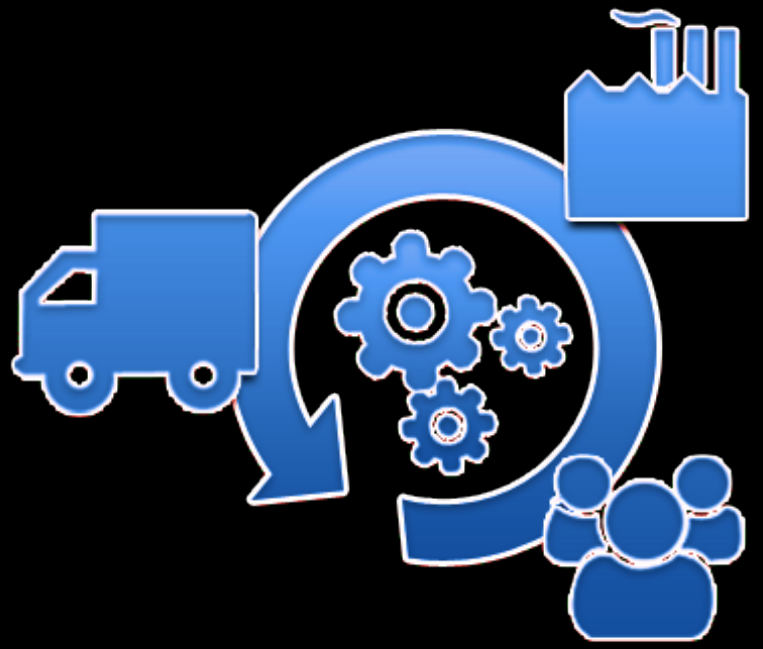
automated scan during coding

SYNOPSYS®

Securing Software Supply Chain: Automation

Smart Protocol Testing

Software Compostion Analysis



Runtime Security Analysis

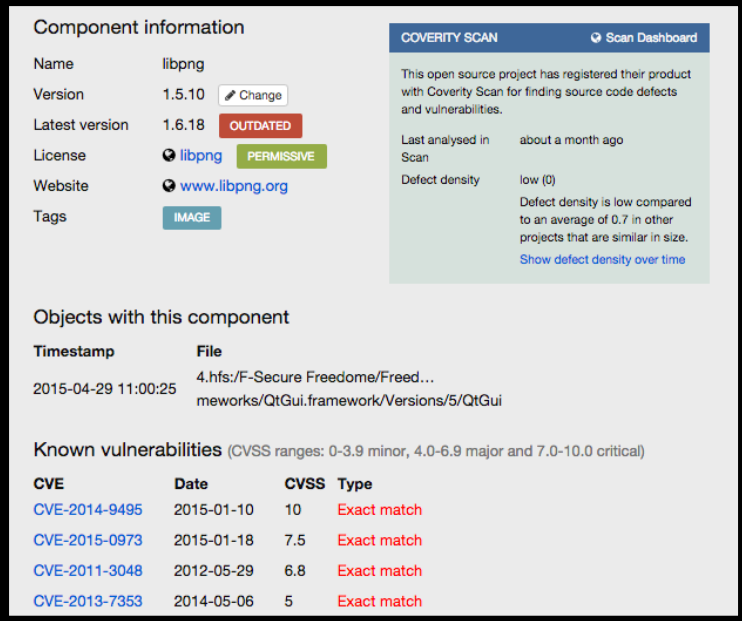
SYNOPSYS®

Example: 3rd Party Component Scanning

Daily updates from National Vulnerability Database (NVD)

THOUSANDS
of binary component signatures

HUNDREDS of THOUSANDS
of open source projects data base



Component information

Name	libpng
Version	1.5.10 Change
Latest version	1.6.18 OUTDATED
License	libpng PERMISSIVE
Website	www.libpng.org
Tags	IMAGE

COVERITY SCAN — Scan Dashboard

This open source project has registered their product with Coverity Scan for finding source code defects and vulnerabilities.

Last analysed in Scan	about a month ago
Defect density	low (0)

Defect density is low compared to an average of 0.7 in other projects that are similar in size.

Show defect density over time

Objects with this component

Timestamp	File
2015-04-29 11:00:25	4.hfs:/F-Secure Freedome/Freed…meworks/QtGui.framework/Versions/5/QtGui

Known vulnerabilities (CVSS ranges: 0-3.9 minor, 4.0-6.9 major and 7.0-10.0 critical)

CVE	Date	CVSS	Type
CVE-2014-9495	2015-01-10	10	Exact match
CVE-2015-0973	2015-01-18	7.5	Exact match
CVE-2011-3048	2012-05-29	6.8	Exact match
CVE-2013-7353	2014-05-06	5	Exact match

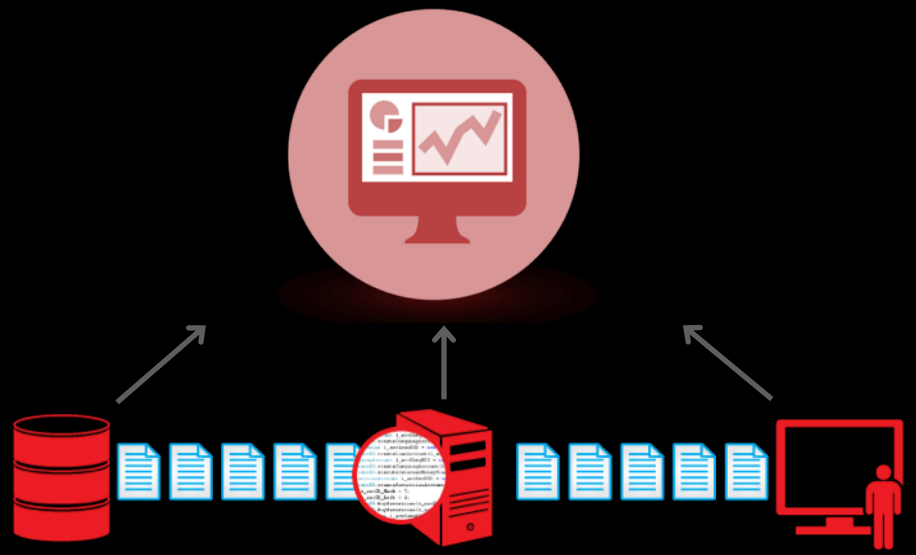
SYNOPSYS®

Example: Runtime Monitoring

Live tracking of data.

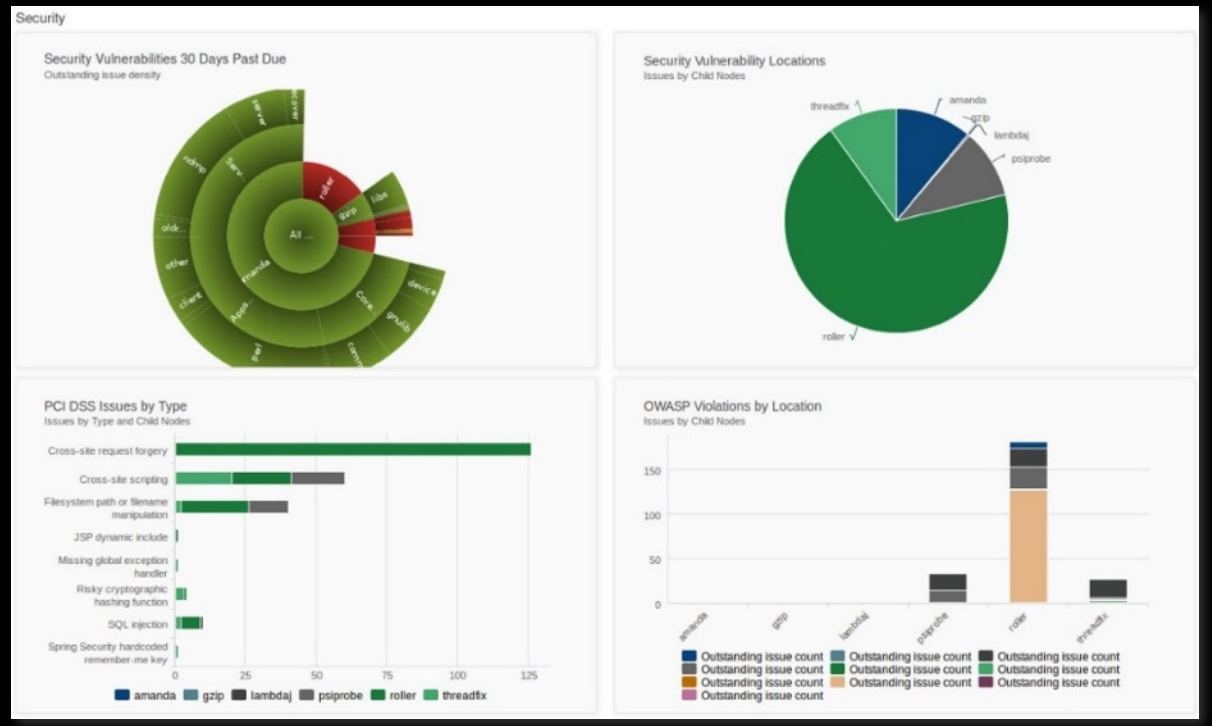
Analyzes code **as it runs, line by line**
Tracks **data** throughout the application
Maps **business processes** in the application
Simulates **attacks** (exploits)

Integrate with test systems.



SYNOPSYS®

Automated DevOps Security: Real-time View

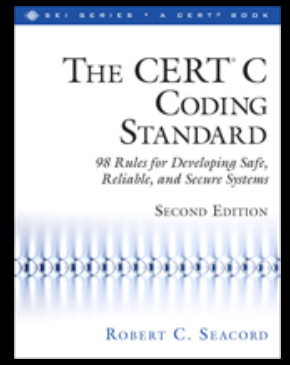


SYNOPSYS®

Independent Security Authorities

IoT Cyber Security Assurance

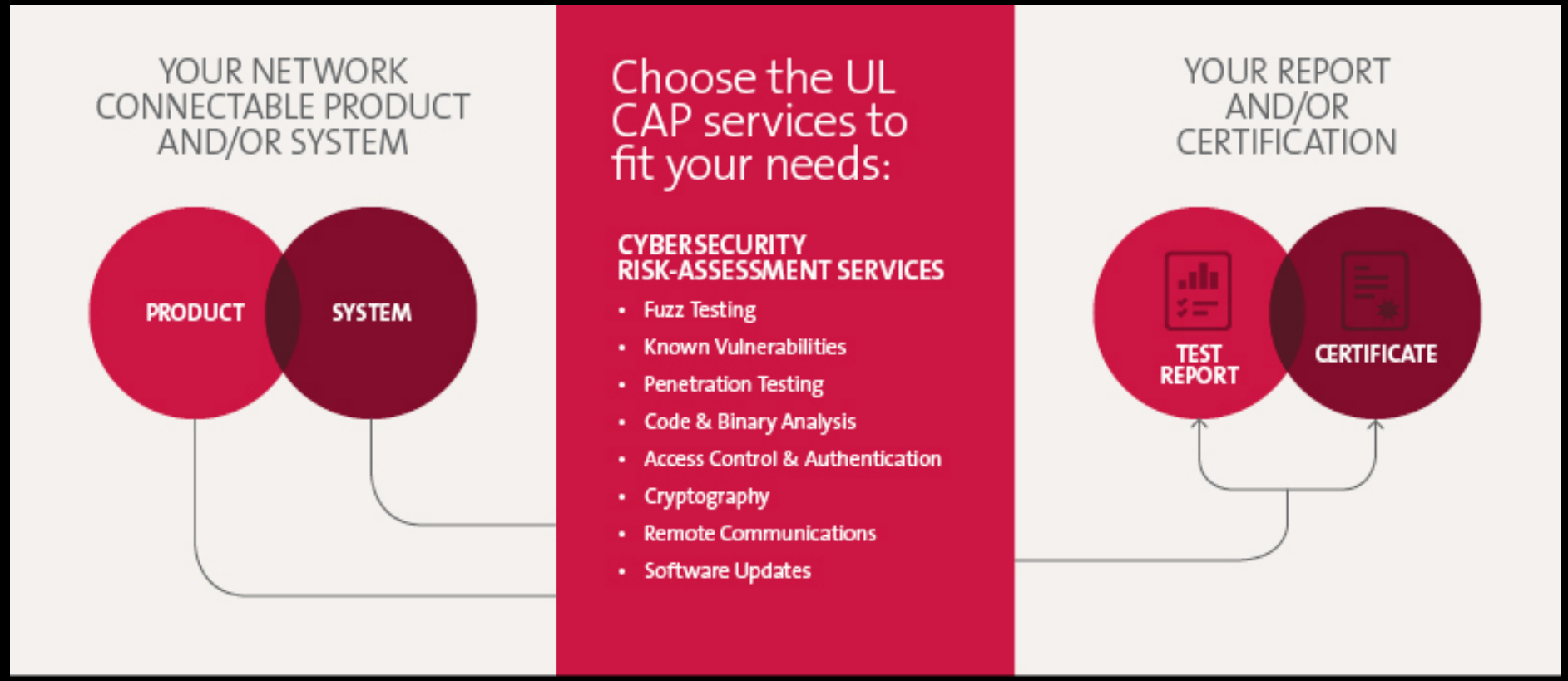
Secure Software Dev



Cyber Secuirty Insurance

SYNOPSYS®

Example: UL 2900 Cybersecurity Assurance Program



Assessment with time-bounded certification horizon.

SYNOPSYS®

Summary

Challenges Are Not Getting Smaller.

75-300 billion networked devices by 2022

– David Bray, CIO FCC

Cybercrime costs $3 trillion to economy

– World Economy Forum

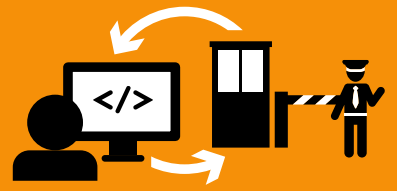
Security pros think over 50% of IoT products are insecure

– IOActive

SYNOPSYS®

No Single Responsibility

Signoff for Software Development



Signoff for Supply Chain

Signoff for Consumer Confidence

SYNOPSYS®

Future Challenges

How to Stop Breaches from Spreading?

Legal & Technical Constraints?

Shutting Down Rogues IoT Systems?

Geopolitical Implication?

SYNOPSYS®

Contact

Dr Ralf Huuck
Synopsys
ralf.huuck@synopsys.com

Q&A