CODENOMICON

CODENOMICON defensics™

CODENOMICON

Preemptive Security & Robustness Test Solutions

Ruediger Rey
Area Manager Central Europe
Mail: ruediger.rey@codenomicon.com

CODENOMICON

About Codenomicon

- Value proposition - accelerate preemptive security and quality assurance
  - Greater security and quality testing prior to release or deployment
  - Risk management: service outage, zero-day attack, compliance and brand liability
- DEFENSICS™ security and robustness test platform
  - Blackbox and broadest protocol test coverage; Internet, Wireless and Digital Media
  - Negative testing with immediate results: simple to use/integrate & negates app. expertise, test plan development
- Headquartered in Finland with offices in US & Asia
  - 10+ years research heritage - OUSPG (Oulu University Security Program Group)
  - 85+ top tier, global customers -carrier, networking equipment, software developers, financial services, defense

Cisco
Nortel
Alcatel
Ericsson
Siemens
Motorola
Microsoft
Adobe
Verizon
ATT
Sprint
T-Systems
Symbian
Qualcomm
Broadcom

2007 FROST & SULLIVAN Global Product Differentiation Innovation Award

TTL

RED HERRING 100 EUROPE WINNER

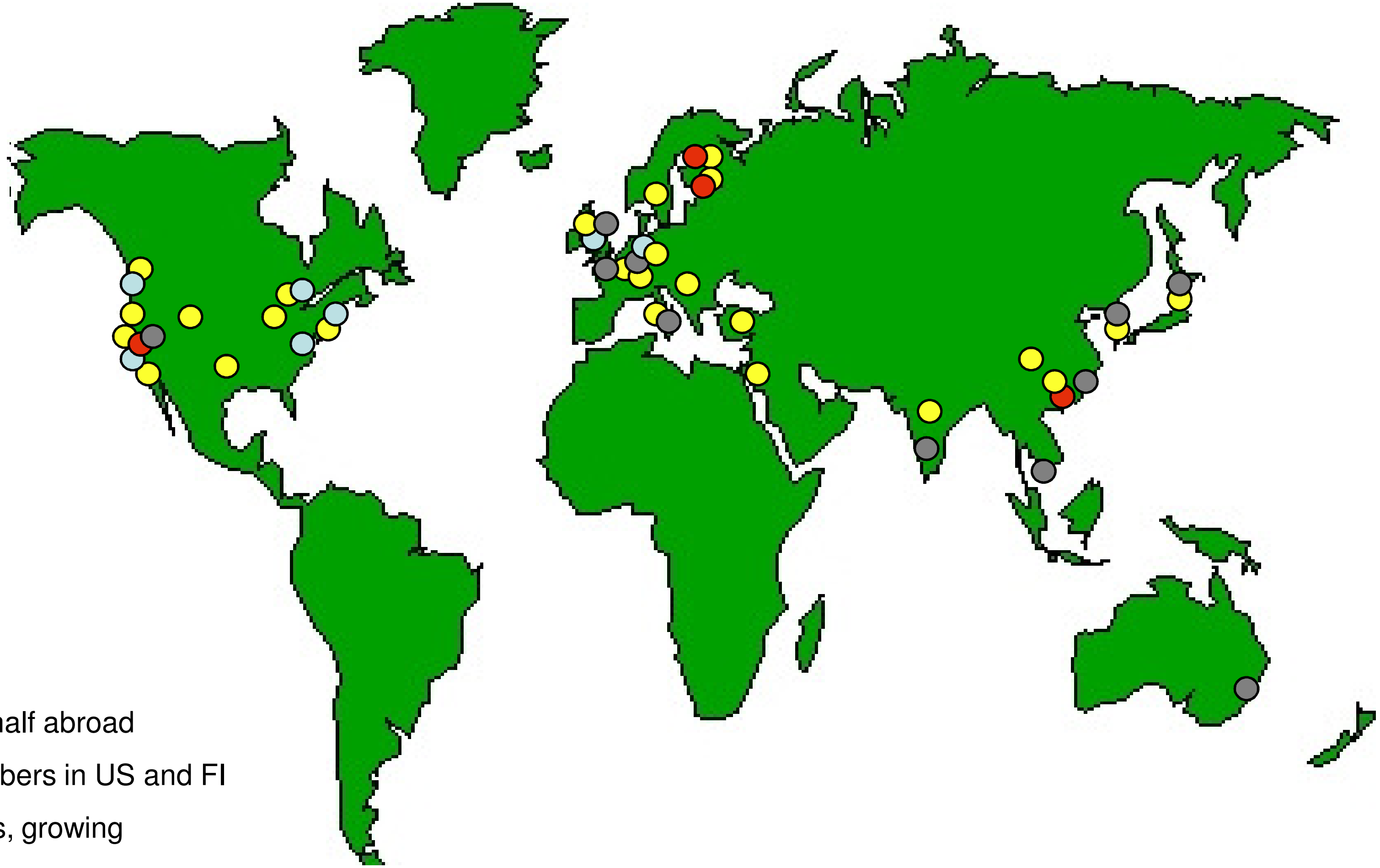
07 AO100 Winner

🟡 Customers

⚪ S&T Offices

🔴 Main Offices

⚫ Resellers



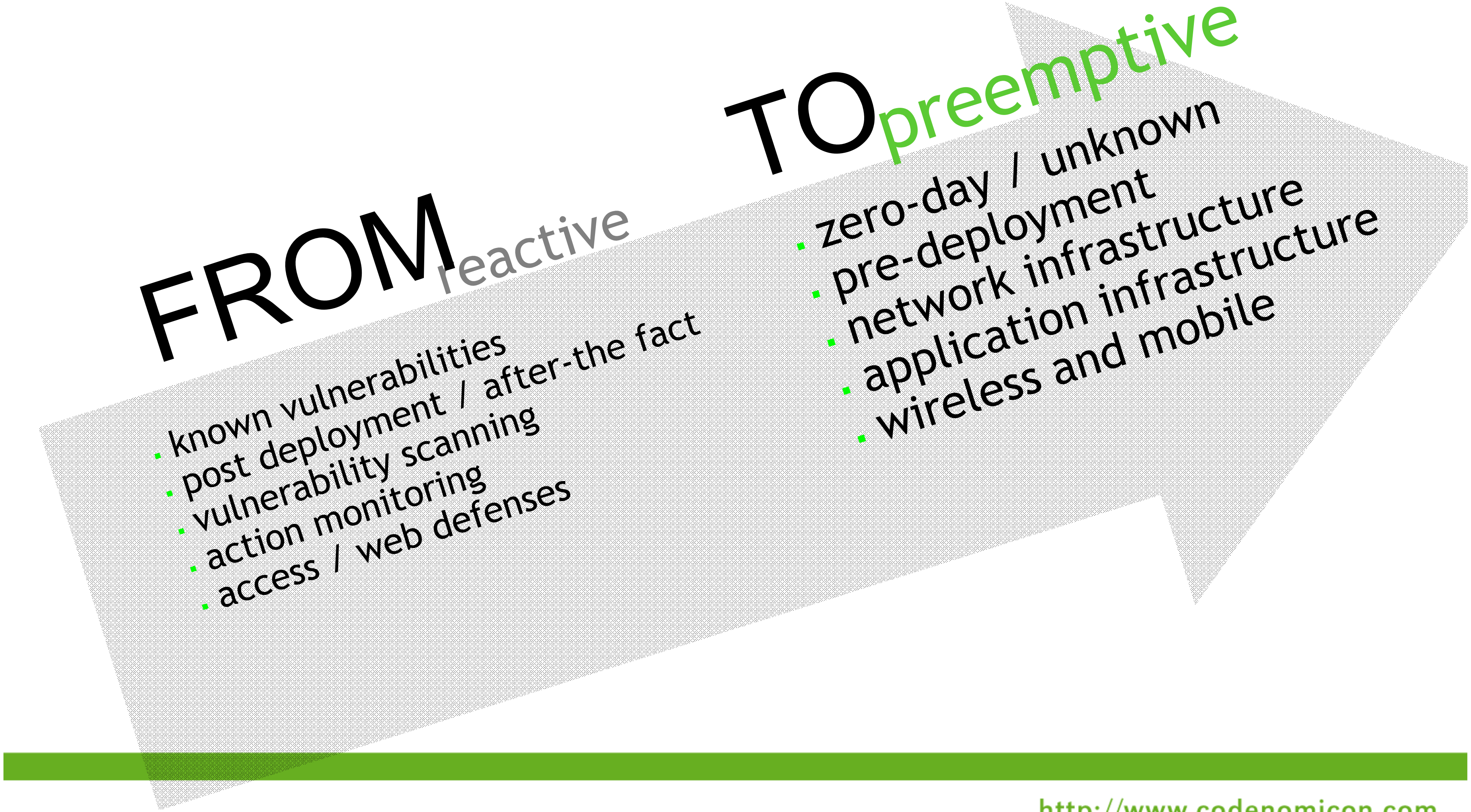
- Chairman of Board ,UK
- Board members half FI half abroad
- Management team members in US and FI

--more than 50 employees, growing

- Operations in Europe, US, Asia

CODENOMICON

THE SECURITY TREND



FROM reactive

- known vulnerabilities
- post deployment / after-the fact
- vulnerability scanning
- action monitoring
- access / web defenses

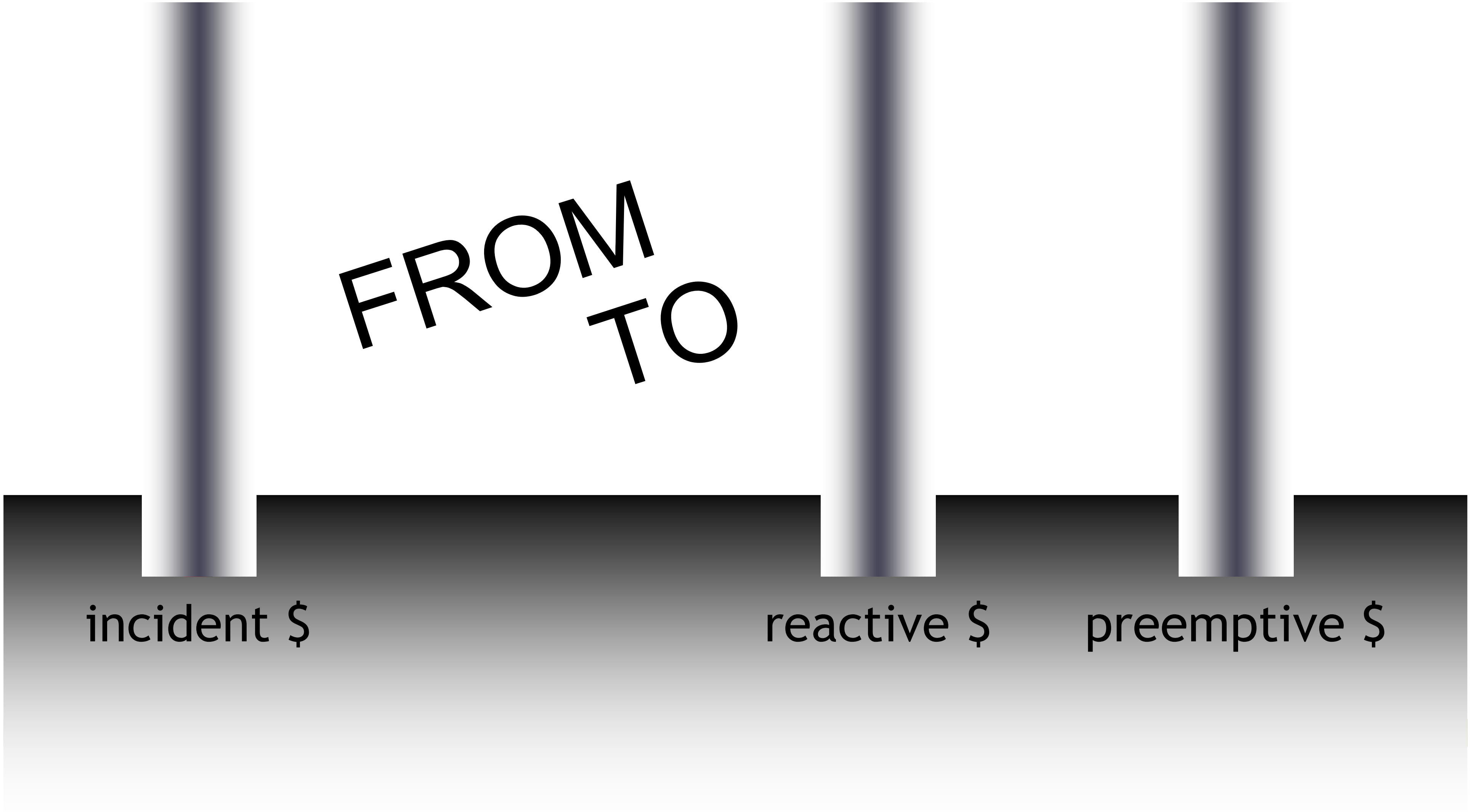
TO preemptive

- zero-day / unknown
- pre-deployment
- network infrastructure
- application infrastructure
- wireless and mobile

THREAT EVOLUTION

- hacker communities
- faster release cycles
- outsourcing
- greater attack surface

SECURITY INVESTMENTS AND RETURNS



FROM

TO

incident $

reactive $

preemptive $

“What measures can mitigate our quality and zero-day exposure?”

GENERAL MANAGER
NETWORK
DEVICE DEVELOPER

“Do our IT infrastructure defenses align with compliance and risk management best practices?”

CHIEF INFORMATION OFFICER
FINANCIAL SERVICES
ENTERPRISE

“Are flaws and patches impacting sales and damaging our brand?”

VICE PRESIDENT – IT
GLOBAL 1000
ENTERPRISE

“How resilient is our service? Will the next partner application or attack take us down?

CHIEF SECURITY OFFICER
CARRIER / SERVICE
PROVIDER

MY WORRIES?

DEFEND. THEN DEPLOY.

CODENOMICON defensics

Preemptively test software, services and devices for unknown and known security flaws - prior to release or deployment - before systems are exposed, outages occur or zero-day attacks strike.

DEFENSICS. THE PREEMPTIVE SECURITY TEST PLATFORM

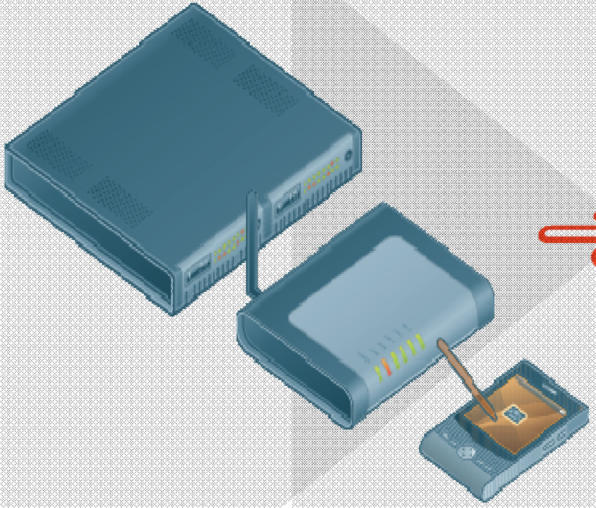
INPUT ANOMALIES

FIELD LEVEL
overflows
integer anomalies

STRUCTURAL
underflows
repetition of elements
unexpected elements

SEQUENCE
out of sequence
omissions
unexpected messages
repetition of messages

system / device under test

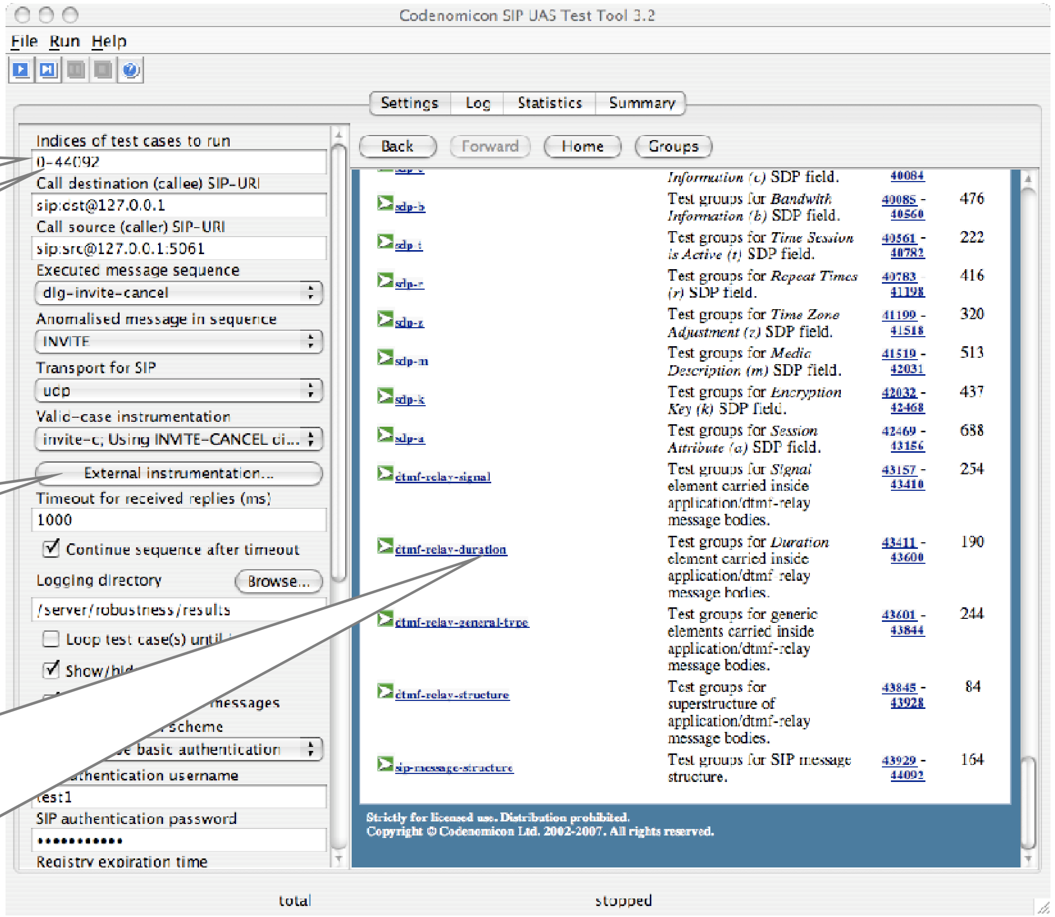


- SYSTEMATIC
- REPEATABLE
- INTELLIGENTLY TARGETED

EXPOSE VULNERABILITIES

- crashes
- denial of service
- security exposures
- degradation of service
- thrashing
- anomalous behavior

CODENOMICON



Indices of test cases to run
0-44092
Call destination (callee) SIP-URI
sip:dst@127.0.0.1
Call source (caller) SIP-URI
sip:src@127.0.0.1:5061
Executed message sequence
dlg-invite-cancel
Anomalised message in sequence
INVITE
Transport for SIP
udp
Valid-case instrumentation
invite-c; Using INVITE-CANCEL di...
Timeout for received replies (ms)
1000
☑ Continue sequence after timeout
Logging directory
/server/robustness/results
□ Loop test case(s) until
☑ Show/hid
messages
scheme
e basic authentication
uthentication username
test1
SIP authentication password
••••••••••••
Registry expiration time

	Information (c) SDP field.	40084	
sdp-b	Test groups for *Bandwith Information (b)* SDP field.	40085 - 40560	476
sdp-t	Test groups for *Time Session is Active (t)* SDP field.	40561 - 40782	222
sdp-r	Test groups for *Repeat Times (r)* SDP field.	40783 - 41198	416
sdp-z	Test groups for *Time Zone Adjustment (z)* SDP field.	41199 - 41518	320
sdp-m	Test groups for *Media Description (m)* SDP field.	41519 - 42031	513
sdp-k	Test groups for *Encryption Key (k)* SDP field.	42032 - 42468	437
sdp-a	Test groups for *Session Attribute (a)* SDP field.	42469 - 43156	688
dtmf-relay-signal	Test groups for *Signal* element carried inside application/dtmf-relay message bodies.	43157 - 43410	254
dtmf-relay-duration	Test groups for *Duration* element carried inside application/dtmf-relay message bodies.	43411 - 43600	190
dtmf-relay-general-type	Test groups for generic elements carried inside application/dtmf-relay message bodies.	43601 - 43844	244
dtmf-relay-structure	Test groups for superstructure of application/dtmf-relay message bodies.	43845 - 43928	84
sip-message-structure	Test groups for SIP message structure.	43929 - 44092	164

Strictly for licensed use. Distribution prohibited.
Copyright © Codenomicon Ltd. 2002-2007. All rights reserved.

Test platform allows full configuration

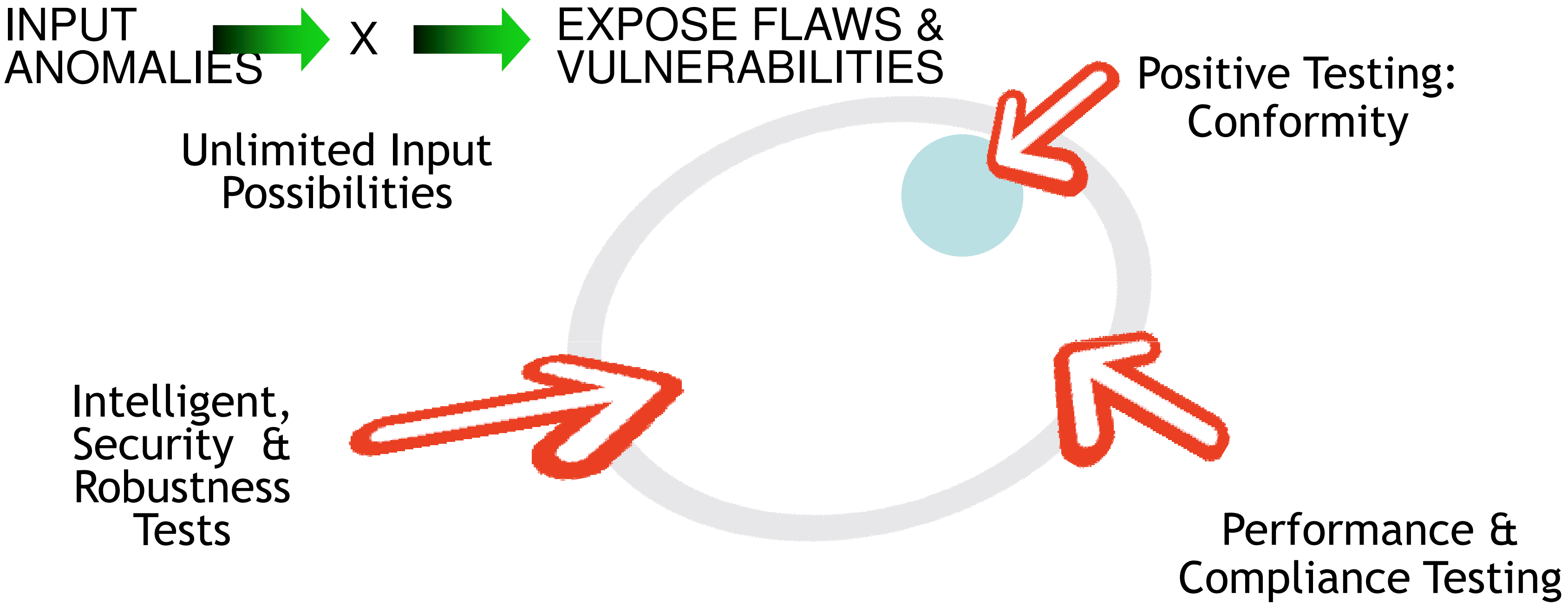
Our SIP Test Suite has over 44,000 unique test cases

Test platform

integrates with external test harness, monitors, and instrumentation

Complete test case documentation streamlines flaw identification, regression test and verified fix

NEGATIVE TESTING



INPUT ANOMALIES → X → EXPOSE FLAWS & VULNERABILITIES

Unlimited Input Possibilities

Positive Testing: Conformity

Intelligent, Security & Robustness Tests

Performance & Compliance Testing

White Box / Conformity

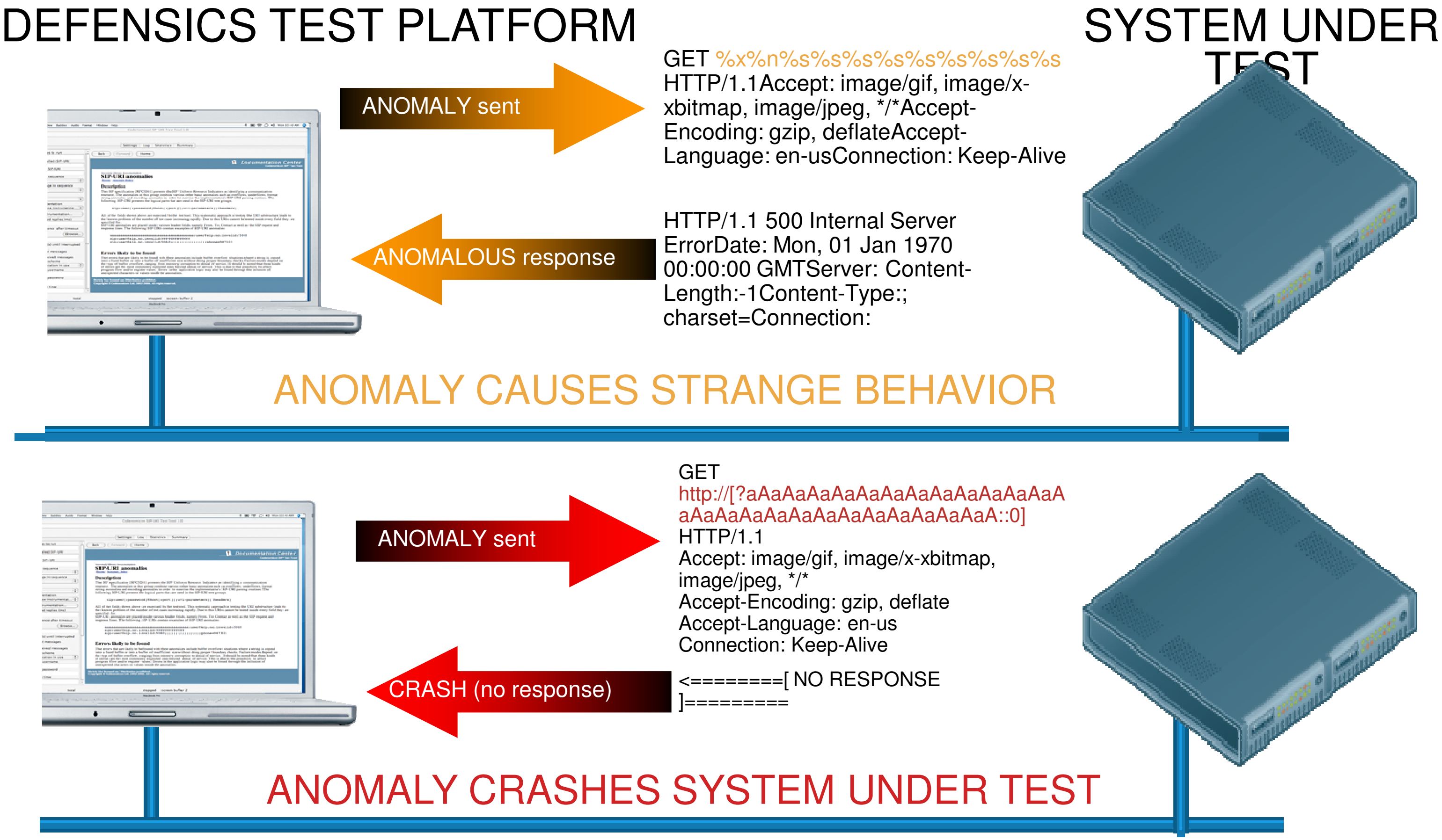
Preemptive Robustness Testing

Performance & Compliance

Web Application Test

Vulnerability Scanning

CODENOMICON DEFENSICS. HOW IT WORKS.



DEFENSICS TEST PLATFORM

SYSTEM UNDER TEST

ANOMALY sent

```
GET %x%n%s%s%s%s%s%s%s%s%s
HTTP/1.1Accept: image/gif, image/x-
xbitmap, image/jpeg, */*Accept-
Encoding: gzip, deflateAccept-
Language: en-usConnection: Keep-Alive
```

ANOMALOUS response

```
HTTP/1.1 500 Internal Server
ErrorDate: Mon, 01 Jan 1970
00:00:00 GMTServer: Content-
Length:-1Content-Type:;
charset=Connection:
```

ANOMALY CAUSES STRANGE BEHAVIOR

ANOMALY sent

```
GET
http://[?aAaAaAaAaAaAaAaAaAaAaAaAaA
aAaAaAaAaAaAaAaAaAaAaAaAaA::0]
HTTP/1.1
Accept: image/gif, image/x-xbitmap,
image/jpeg, */*
Accept-Encoding: gzip, deflate
Accept-Language: en-us
Connection: Keep-Alive
```

CRASH (no response)

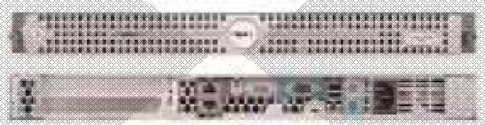
```
<========[ NO RESPONSE
]=========
```

ANOMALY CRASHES SYSTEM UNDER TEST

EXPOSING Zero-Day & Resiliency INFRASTRUCTURE FLAWS

publicly known vulnerabilities

- New family of routers deployed
- Various flaws could be exploited
- Publicly disclosed in detail at BlackHat
- Flaws resolved & in fix release process just prior to public disclosure



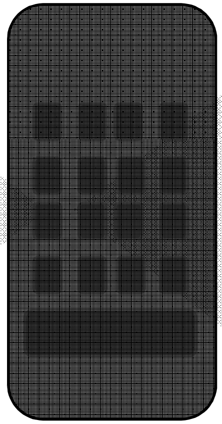
unknown vulnerabilities
that could be preempted

- IPv6
- SSL
- OSPF
- SIP

EXPOSING CORPORATE DATA IN A MODERN MOBILE DEVICE

publicly known vulnerabilities

- Phone released
- Hack-a-thon one week later
- Various flaws that expose user data
- Disclosed on the Internet

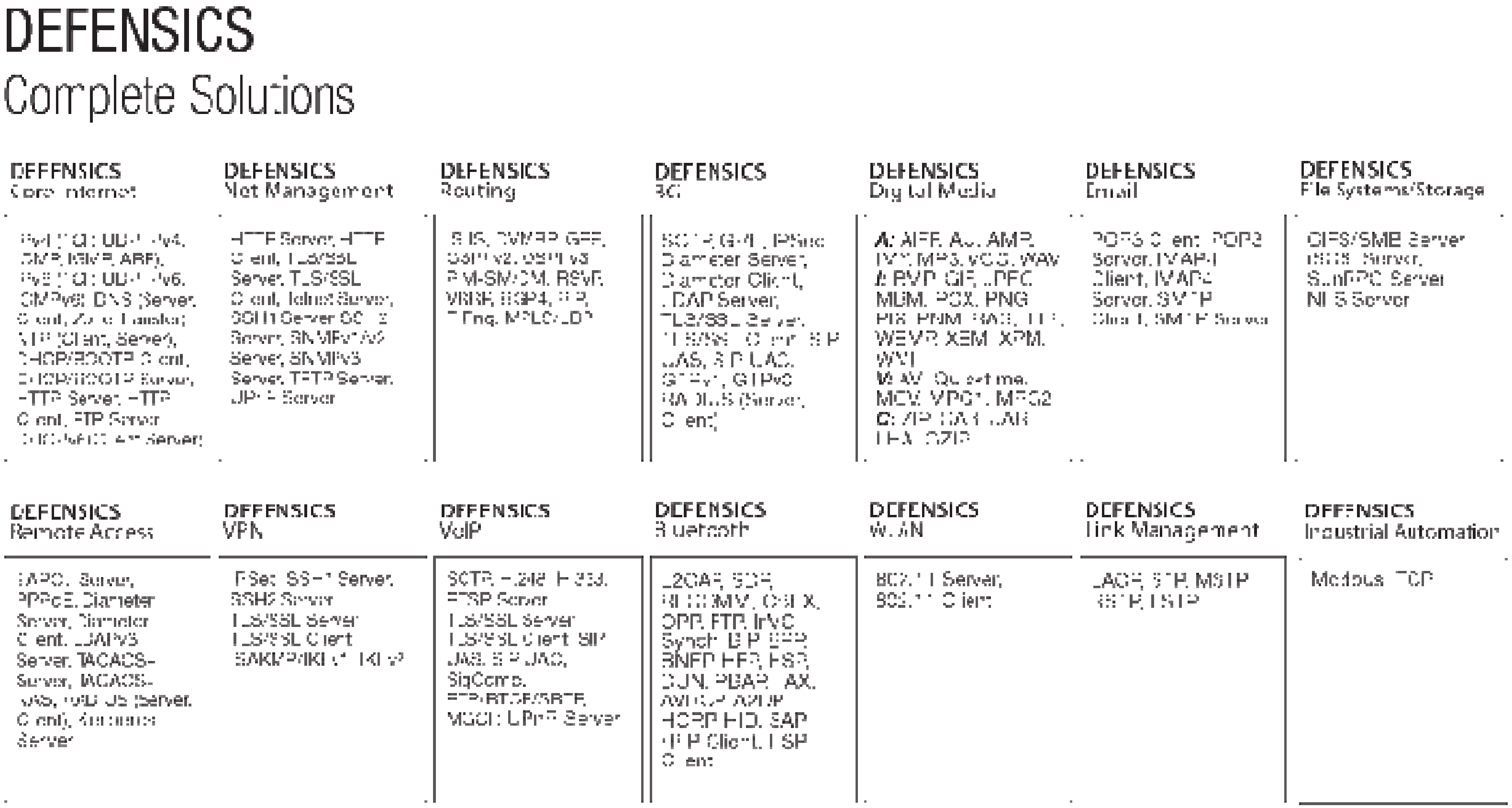


unknown vulnerabilities that could be preempted

- Bluetooth
- WiFi
- email
- VoIP

CODENOMICON

DEFENSICS TEST SUITES



DEFENSICS
Complete Solutions

DEFENSICS Core Internet

IPv4 (TCP, UDP, IPv4, ICMP, IGMP, ARP), IPv6 (TCP, UDP, IPv6, ICMPv6), DNS (Server, Client, Zone transfer), NTP (Client, Server), DHCP/BOOTP Client, DHCP/BOOTP Server, HTTP Server, HTTP Client, FTP Server, DHCPv6 (Client, Server)

DEFENSICS Net Management

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

DEFENSICS Routing

IS-IS, DVMRP, GRE, OSPFv2, OSPFv3, PIM-SM/DM, RSVP, VRRP, BGP4, RIP, TE Eng. MPLS/LDP

DEFENSICS 3G

SCTP, GTP, IPSec, Diameter Server, Diameter Client, LDAP Server, TLS/SSL Server, TLS/SSL Client, SIP UAS, SIP UAC, GTPv1, GTPv2, RADIUS (Server, Client)

DEFENSICS Digital Media

A: AIFF, AU, AMR, MIDI, MP3, VOC, WAV
I: BMP, GIF, JPEG, MBM, PCX, PNG, PIX, PNM, RAS, TIFF, WBMP, XBM, XPM, WMF
V: AVI, Quicktime, MOV, MPG1, MPG2
C: ZIP, CAB, JAR, LHA, GZIP

DEFENSICS Email

POP3 Client, POP3 Server, IMAP4 Client, IMAP4 Server, SMTP Client, SMTP Server

DEFENSICS File Systems/Storage

CIFS/SMB Server, iSCSI Server, SunRPC Server, NFS Server

DEFENSICS Remote Access

EAPOL Server, PPPoE, Diameter Server, Diameter Client, LDAPv3 Server, TACACS+ Server, TACACS+ NAS, RADIUS (Server, Client), Kerberos Server

DEFENSICS VPN

IPSec, SSH1 Server, SSH2 Server, TLS/SSL Server, TLS/SSL Client, ISAKMP/IKEv1, IKEv2

DEFENSICS VoIP

SCTP, H.248, H.323, RTSP Server, TLS/SSL Server, TLS/SSL Client, SIP UAS, SIP UAC, SigComp, RTP/RTCP/SRTP, MGCP, UPnP Server

DEFENSICS Bluetooth

L2CAP, SDP, RFCOMM, OBEX, OPP, FTP, IrMC Synch, BIP, BPP, BNEP, HFP, HSP, DUN, PBAP, FAX, AVRCP, A2DP, HCRP, HID, SAP, HFP Client, HSP Client

DEFENSICS WLAN

802.11 Server, 802.11 Client

DEFENSICS Link Management

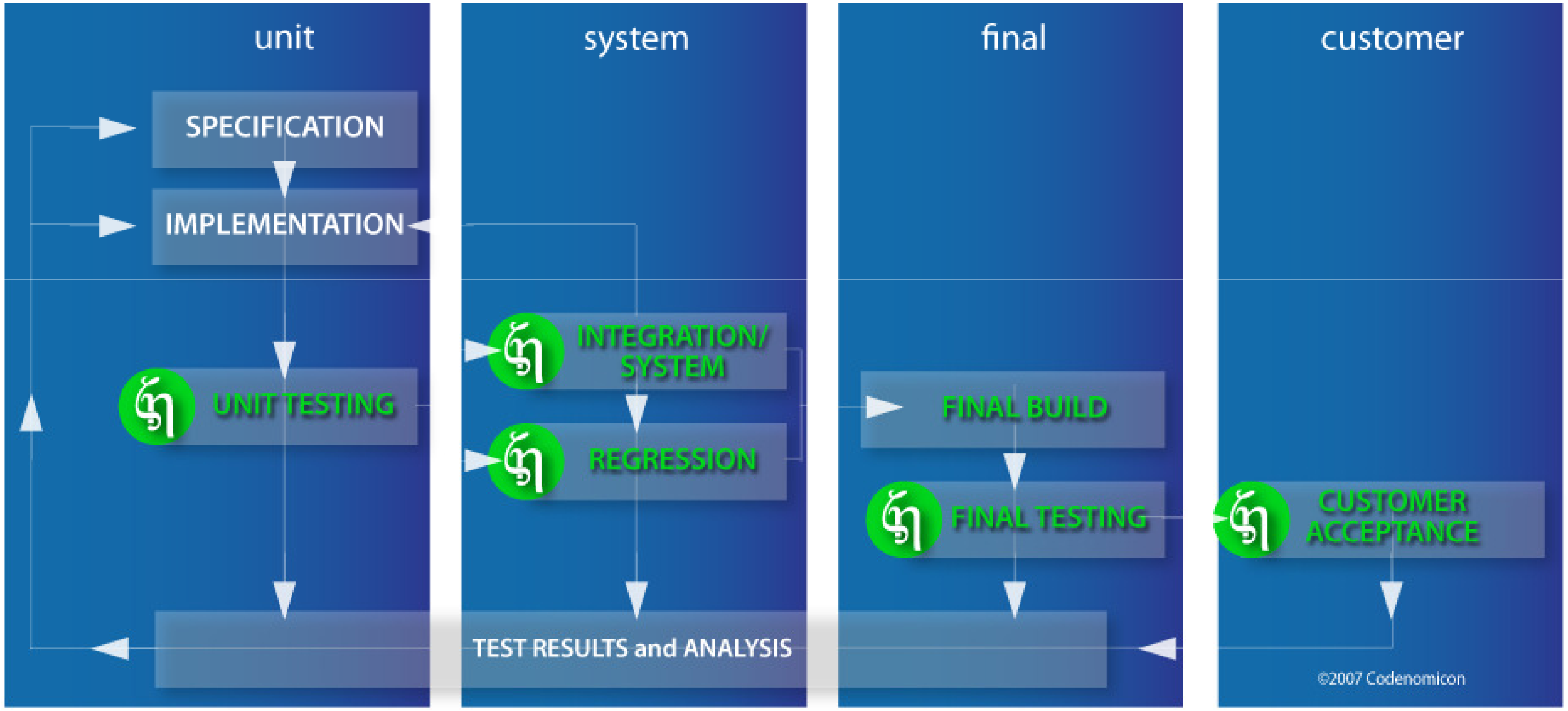
LACP, STP, MSTP, RSTP, LSTP

DEFENSICS Industrial Automation

Modbus TCP

DEFENSICS WHERE IT FITS

DEFENSICS in the Security Lifecycle



CODENOMICON SERVICES

- Expert professional test and implementation services
  - Accelerate time-to-value
  - Expedite product expertise and use
  - Enhance release and deployment security readiness
  - Advance quality and risk assurance; on-time & within budget
  - Extend partner and vendor test requirements
  - Increase system and service resiliency

CODENOMICON SERVICES

- Quick Start
  - Accelerate your adoption and proficiency of DEFENSICS and supplement quality testing resources
- Training
  - Understand DEFENSICS theory of operation, best practices and proficiency
- Monitoring Services
  - Supplement your quality testing resources when you need it
- Custom Test Support
  - Facilitate use of Codenomicon DEFENSICS platform for testing unsupported or custom protocols

PREEMPTIVE SECURITY ADVANTAGES

- greater release quality and resiliency
- published and zero-day attack mitigation
- reduced fix + patch costs
- lower brand damage risk
- lower compliance risks

CODENOMICON ADVANTAGE

- Best-in-Class security and robustness test platform
  - Broadest protocol coverage; Internet, wireless and digital media
  - World-proven blackbox, negative test methodology and technology
  - Complete test case documentation and full flaw regression testing
  - Software-flexible implementation and external test integration
- Accelerated time-to-value
  - Simple to use, simple to integrate, simply achieve immediate results
  - Maximum results with nominal resource and test process impact
  - No expert resources, source code access, or defining more test cases
- Superior Risk Reduction
  - Downtime exposures, post-fix costs, zero-day attacks, & tarnished brand

Network
Connected devices

VPN

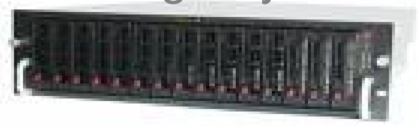
Firewalls + IPS
Security Infrastructure
Network Infrastructure

Wireless and Bluetooth

Portals and any kind of Software

Embedded and special systems

Storage Systems



And many things more.....

CODENOMICON

Some of the companies we service

Dialogic
Making Innovation Thrive

Nokia Siemens Networks

T · · Systems ·

symbian OS

verizon

· · T · · Mobile ·

NOKIA
Very Human Technology

· · T · · Com ·

CISCO

SIEMENS

Microsoft

NORTEL NETWORKS

Swedbank

Adobe

QUALCOMM

Nordea

BROADCOM

Sprint

Alcatel·Lucent

ERICSSON

at&t

SIEMENS
Gigaset

AVM

EUROPÄISCHES PARLAMENT

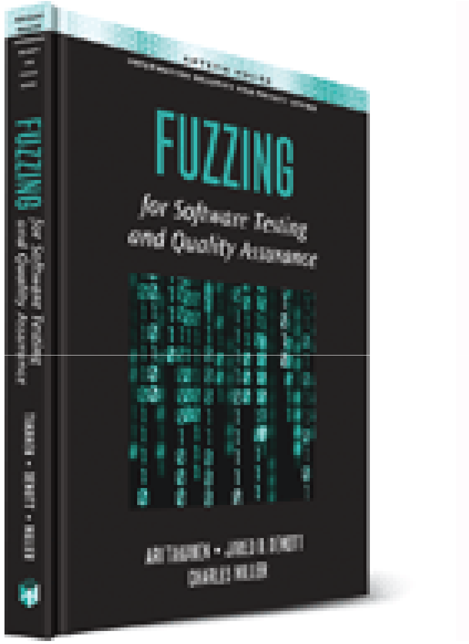
Win a new originally signed „Fuzzing“ book from famous Fuzzing specialist Ari Takanen!

Winners of the book will be informed soon after the fair!

CODENOMICON

Win a signed Fuzzing book from Ari Takanen!

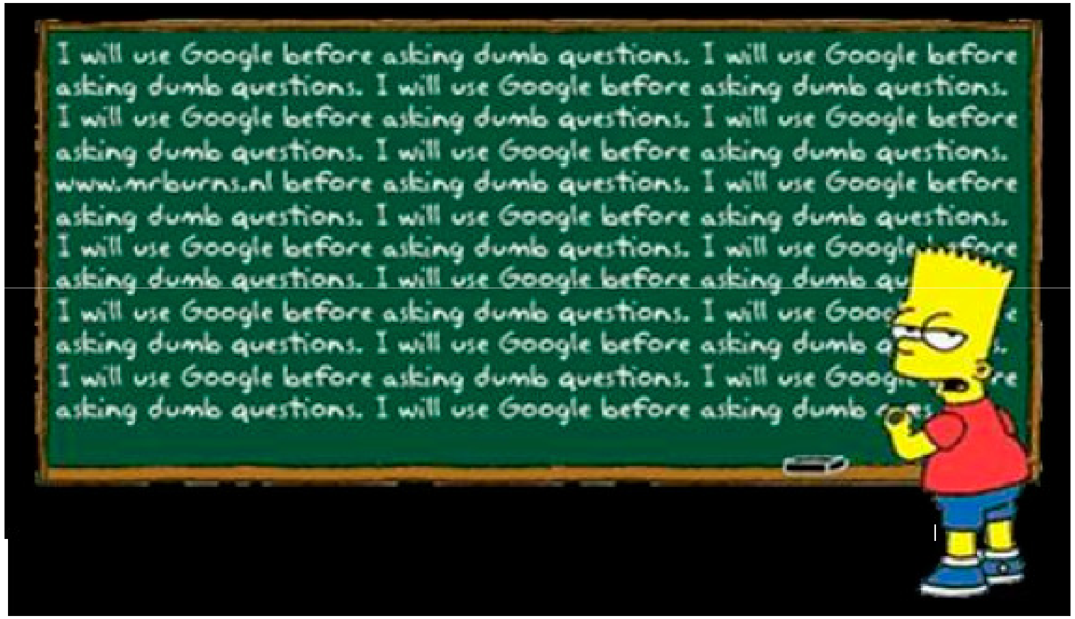
"A fascinating look at the new direction fuzzing technology is taking — useful for both QA engineers and bug hunters alike!"
—Dave Aitel, CTO, Immunity Inc.



Learn the code cracker's malicious mindset, so you can find worn-size holes in the software you are designing, testing, and building. Fuzzing for Software Security Testing and Quality Assurance takes a weapon from the black-hat arsenal to give you a powerful new tool to build secure, high-quality software. This practical resource helps you add extra protection without adding expense or time to already tight schedules and budgets. The book shows you how to make fuzzing a standard practice that integrates seamlessly with all development activities.

This comprehensive reference goes through each phase of software development and points out where testing and auditing can tighten security. It surveys all popular commercial fuzzing tools and explains how to select the right one for a software development project. The book also identifies those cases where commercial tools fall short and when there is a need for building your own fuzzing tools.

Questions????? – Just ask!


I will use Google before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
I will use Google before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
www.mrburns.nl before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
I will use Google before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb qu
I will use Google before asking dumb questions. I will use Goog
asking dumb questions. I will use Google before asking dumb q
I will use Google before asking dumb questions. I will use Goog
asking dumb questions. I will use Google before asking dumb

Thanks!

Codenomicon Oy/Ltd.
Ruediger Rey
Mail: ruediger.rey@codenomicon.com
www.codenomicon.com
or
www.gohackyourself.net