Smalltalk Security Landscape

Jerry Kott, OSCP

image-ware.com/static/esug2018.pdf

image-ware.com

Context

Key Security concepts

Survey Overview

Dialect Assessment

Frameworks

Tools & Techniques
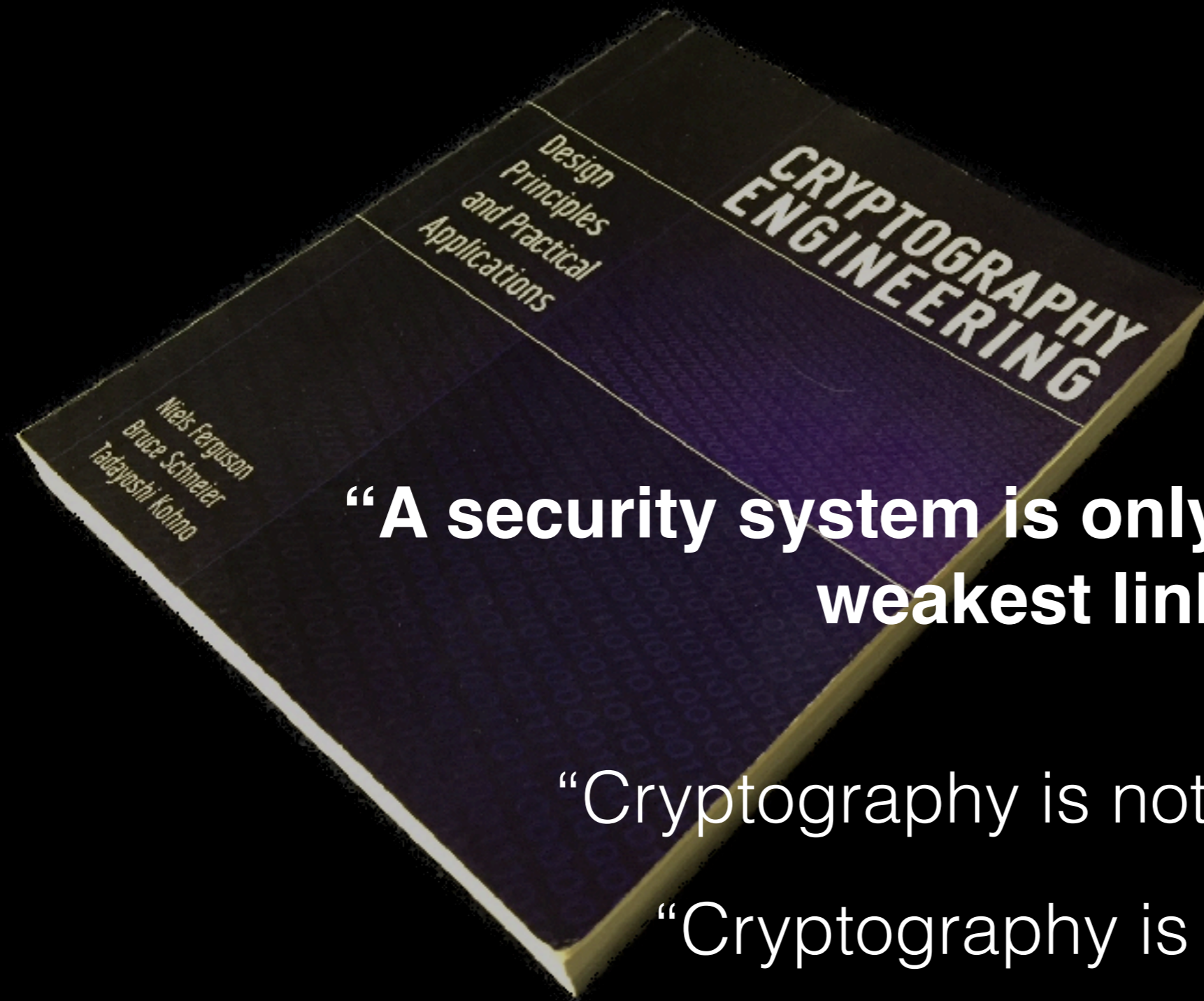
What's next?

The Context

Security is an Infinite Game

Who is this guy?

- Physics & Engineering Education

- Introduced to Smalltalk in 1988

- Using Smalltalk professionally since 1992

- Formerly *"Cincom Smalltalk Security Guy"*

- Web tools, protocols, algorithms… CRYPTO!

"A security system is only as strong as its weakest link."

"Cryptography is not the solution."

"Cryptography is very difficult."

"Cryptography is the easy part."

2013

image-ware.com

A lesson

- What I don't know can hurt me

- Security is 90% behaviour, 10% technology

- Understanding cryptography is not enough

- I must learn how attackers think, what they are after, and how they do it

Since 2014

- Focus on Privacy and Security

- Victoria Cybersecurity Hackers (not what you may think)

- Offensive Security

  ★ Vulnerability Assessment

  ★ Penetration Testing

  ★ OSCP

Offensive Security Certified Professional

- **Course**: Penetration Testing with Kali (PWK)

  About 50 vulnerable machines in a virtual lab environment

  Reconnaissance, fuzzing, SQLi, XSS, server misconfiguration, RCE, lateral movement, privilege escalation, …

- **Exam**: 24 hour simulated penetration test.

  5 machines of varying difficulty

  Another 24 hours to deliver a professional report

Key Security Concepts

The CIA triad

Confidentiality

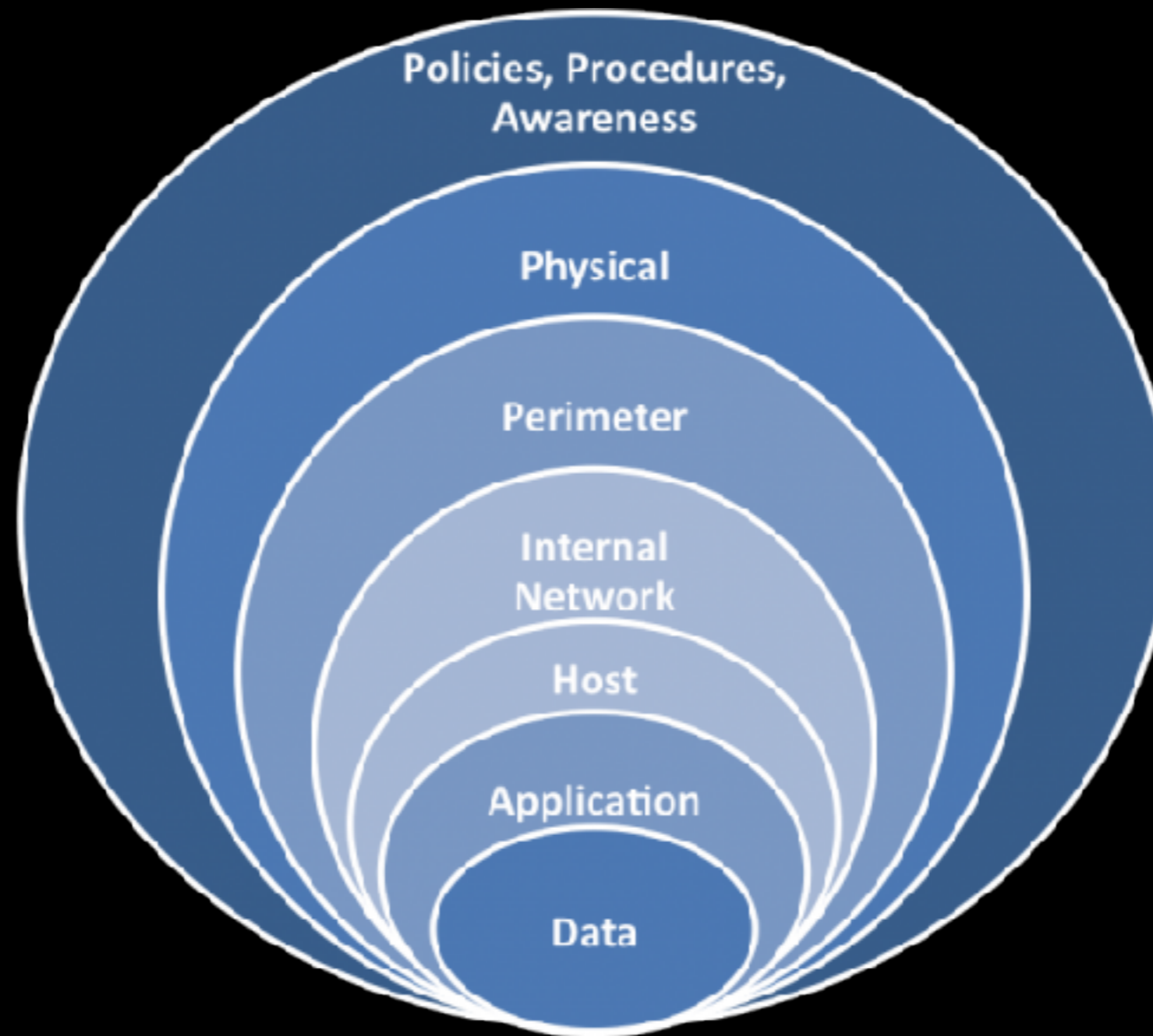**Integrity**

Availability

image-ware.com

Attack Surface

- Possible points of entry by an attacker

- Software (OS, services, applications)

- Data (from plain files to databases)

- Security is a **Team Sport**

image-ware.com

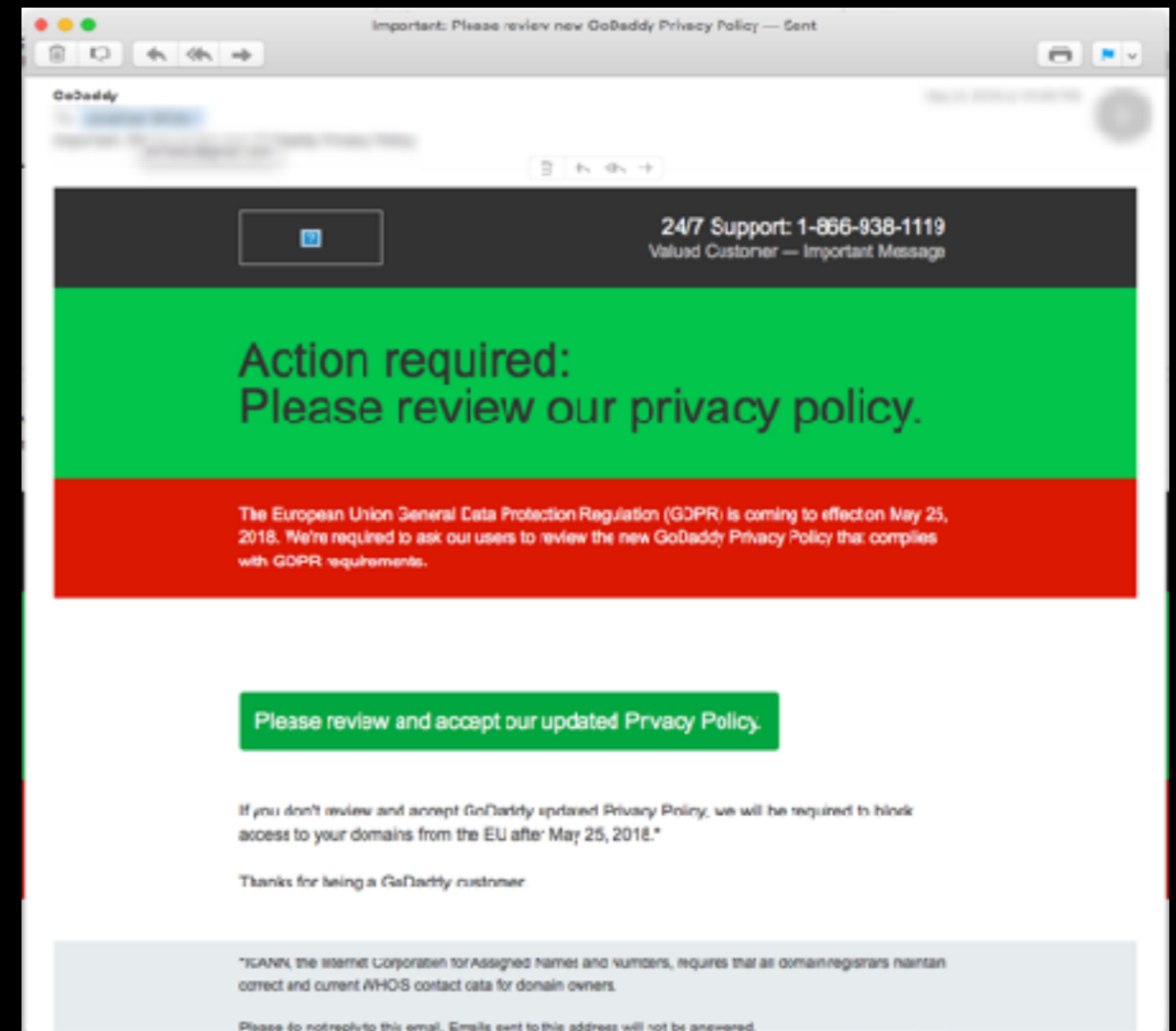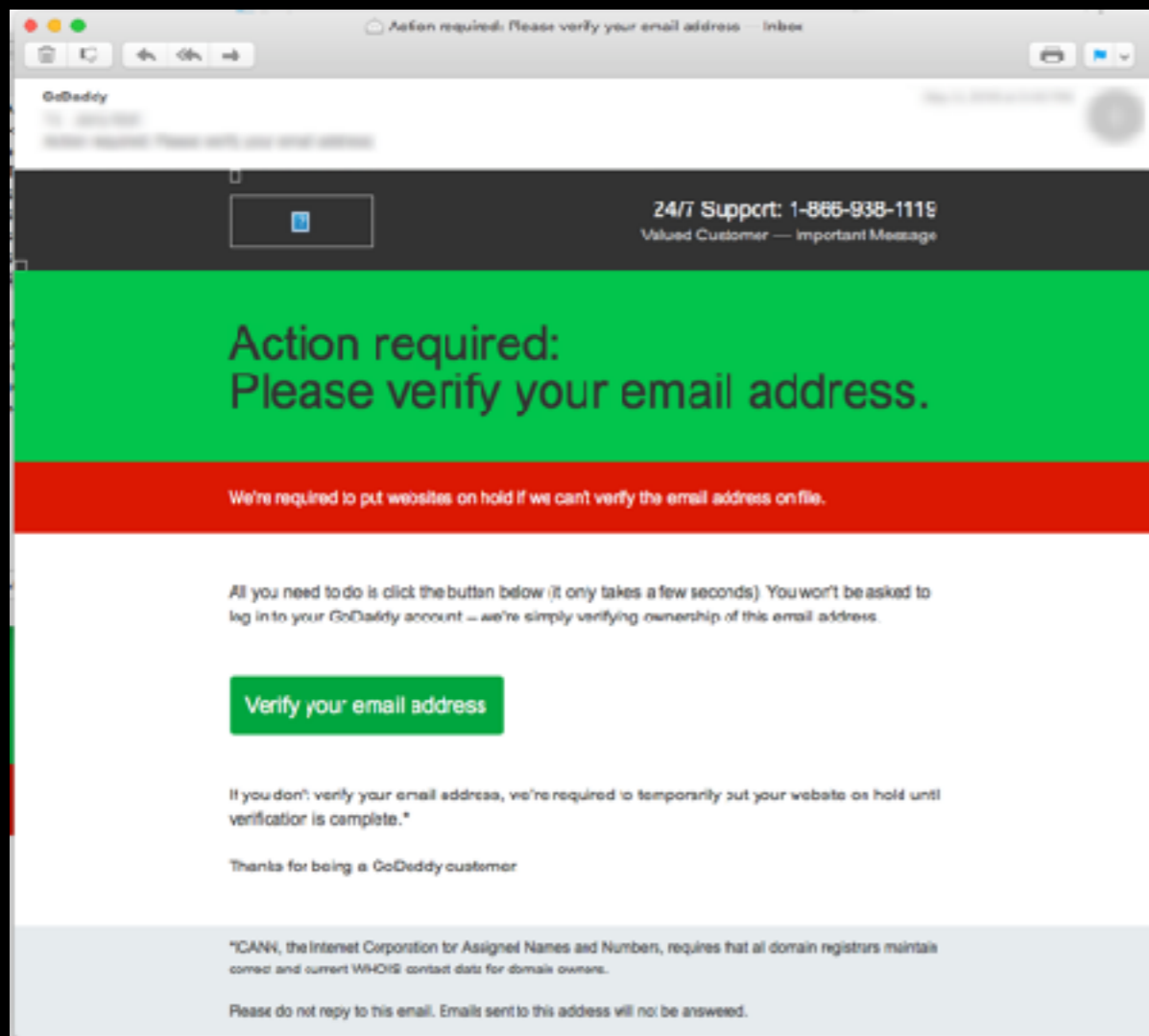# Defense In Depth

image-ware.com

Kill Chain

Cyber Attack Lifecycle

Reconnaissance → Weaponization and Delivery → Exploitation → Installation → Command-and-Control → Actions on the Objective

Unauthorized Access | **Unauthorized Use**

There is no predictable path for the advanced adversary.

Social Engineering

Which one is real?

Defensible Security

world-class

risk-based security

defensible

compliance

hygiene
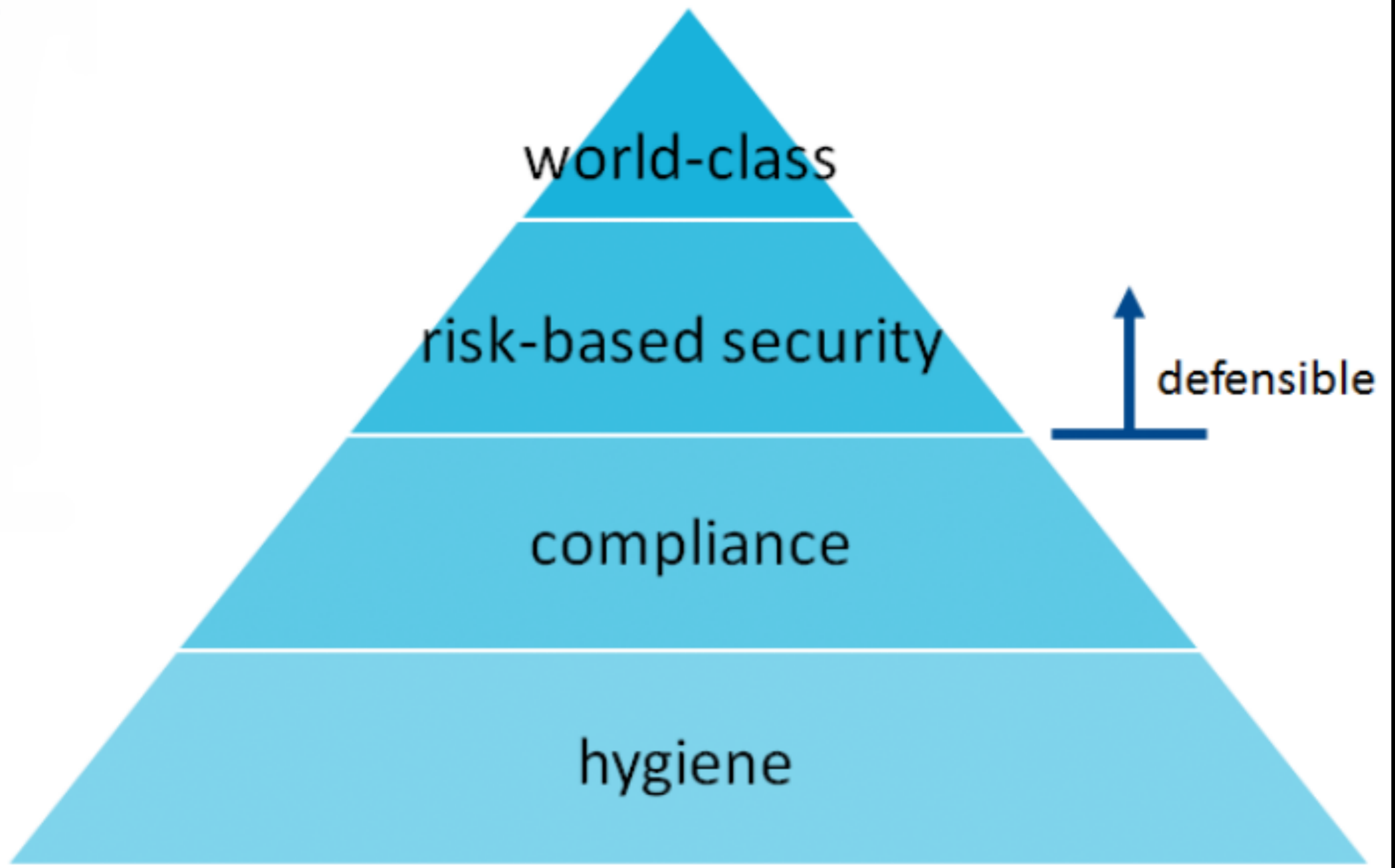
Security Prerequisites

* **Executive Support**

* Identify the **crown jewels** of the organization

* Identify and assign roles and responsibilities

* Know and regularly review organization's risk appetite

* Regular risk assessments for new systems and material changes to existing ones

* Conduct security assessments against an established security standard

image-ware.com

Responsible Disclosure

- Formal process for vulnerability reporting

- No specific vulnerability disclosure here

- Broad-brush security landscape painting

- Barely scratched the surface

- Direct work with vendors is needed

Smalltalk Security Landscape

What's the story?

image-ware.com

The story is mostly:

- NOT about algorithms

- About the weakest links

- Comedy? Tragedy? Farce?

image-ware.com

People are the worst!

Smalltalk Security Survey

- Anonymous survey at
  www.surveymonkey.com/r/esug2018

- Ran for about 3 weeks in August 2018

- A lot of interesting data

image-ware.com

Smalltalk Security Survey

Goals

- High level: Where are we as a community?

- How well do we understand the issues?

- How secure are our systems?

- What are our values and attitudes?

- How can we (and do we need to) do better?

Smalltalk Security Survey

Areas

- Use of Smalltalk (mostly demographics)

- Cybersecurity at respondents' organization (self-assessment)

- Privacy and Ethics

- Smalltalk and Security

image-ware.com

My own assessment

- High-level reconnaissance

- Based on OWASP Top 10
  (https://www.owasp.org/index.php/Top_10-2017_Top_10)

- Areas of analysis:

  - ★ Vendors' web site security configuration

  - ★ Privacy & Security of Download and Installation

  - ★ IDE / team environment configuration

  - ★ Vulnerability to memory based attacks (e.g., buffer overflow)

image-ware.com

OWASP Top 10 (2017)

1. **Injection** flaws such as SQL, NoSQL, OS

2. **Broken Authentication**

3. **Sensitive Data Exposure**

4. XML External Entities

5. **Broken Access Control**

6. **Security Misconfiguration**

7. **Cross-Site Scripting**

8. Insecure Deserialization

9. Using Components with Known Vulnerabilities

10. Insufficient Logging and Monitoring

26

Privacy Analysis

- Personal info leakage expands the attack surface (e.g., potential spear phishing)

- Personal Information collection and sharing with 3rd parties presents unknown risks (the weakest link may be outside of your organization)

- GDPR (non)compliance can have bottom line implications (fines, loss of customers)

image-ware.com

SMALLTALK SECURITY LANDSCAPE

THE GOOD
THE BAD
THE UGLY

The Good

- Smalltalk is awesome

- Growing security awareness

- Some security discussion on mailing lists

- Healthy respect for Privacy & Ethics

- Some VMs are compiled with ASLR and DEP

image-ware.com

The Good

- The language and the IDEs make it easy to prevent stupid mistakes, e.g.:

  - automatic GC

  - no messing with pointers

  - automatic bound checking (strings, byte arrays, etc…)

  - easy unit testing (if you have the discipline)

- Bugs can be fixed quickly (it's Smalltalk!)

- Smalltalk based systems benefit from relative *'security by obscurity'* (Controversial)

image-ware.com

The Bad

- Formal cybersecurity programs lacking or poorly defined / understood

- Misconfigured or insecure web sites

- Downloads & IDEs vulnerable to MITM attacks

- Too much reliance on *security by obscurity*

image-ware.com

The Bad

- Pervasive use of plaintext protocols

- Default settings too permissive (world-readable)

- Plaintext passwords stored in poorly protected configuration files

- Image files (i.e., executable code) contain sensitive information

image-ware.com

The Bad

- Legacy code from 1990s still in active use

- Lack of security training and skilled professionals

- Absence of Red Teams dedicated to find vulnerabilities

- Testing limited to Unit and Functional, little penetration testing. Correct me if I am wrong.

image-ware.com

The Ugly

- Passwords sent across the wire in plaintext

- Internal directory and file structure information leakage

- Code injection allowing arbitrary Remote Code Execution (e.g., the infamous reverse shell)

image-ware.com

Assume **BREACH**

image-ware.com
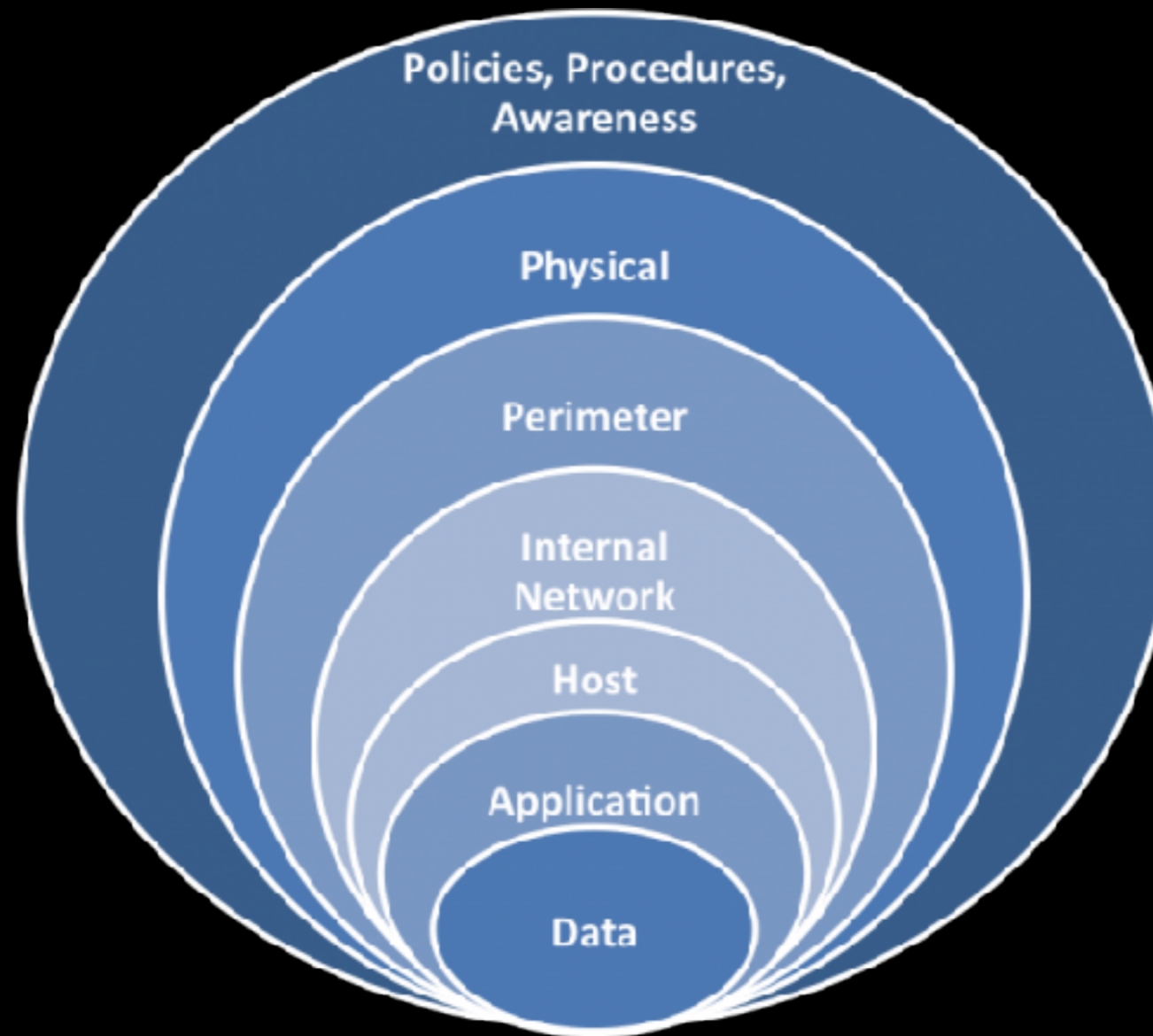
Assume **BREACH**

- Most companies discover hacks late

- Intrusion Detection System is imperative

- Incident Response Plan must be part of a Cybersecurity Program

"There are two kinds of big companies in the United States. There are those who've been hacked by the Chinese, and those who don't know they've been hacked by the Chinese."

–Former FBI Director James Comey (2014)

"There are two kinds of companies. There are those who've been hacked, and those who don't know they've been hacked."

–Anonymous (2018)

Smalltalk Security Survey

Quiz(?) Scores

image-ware.com
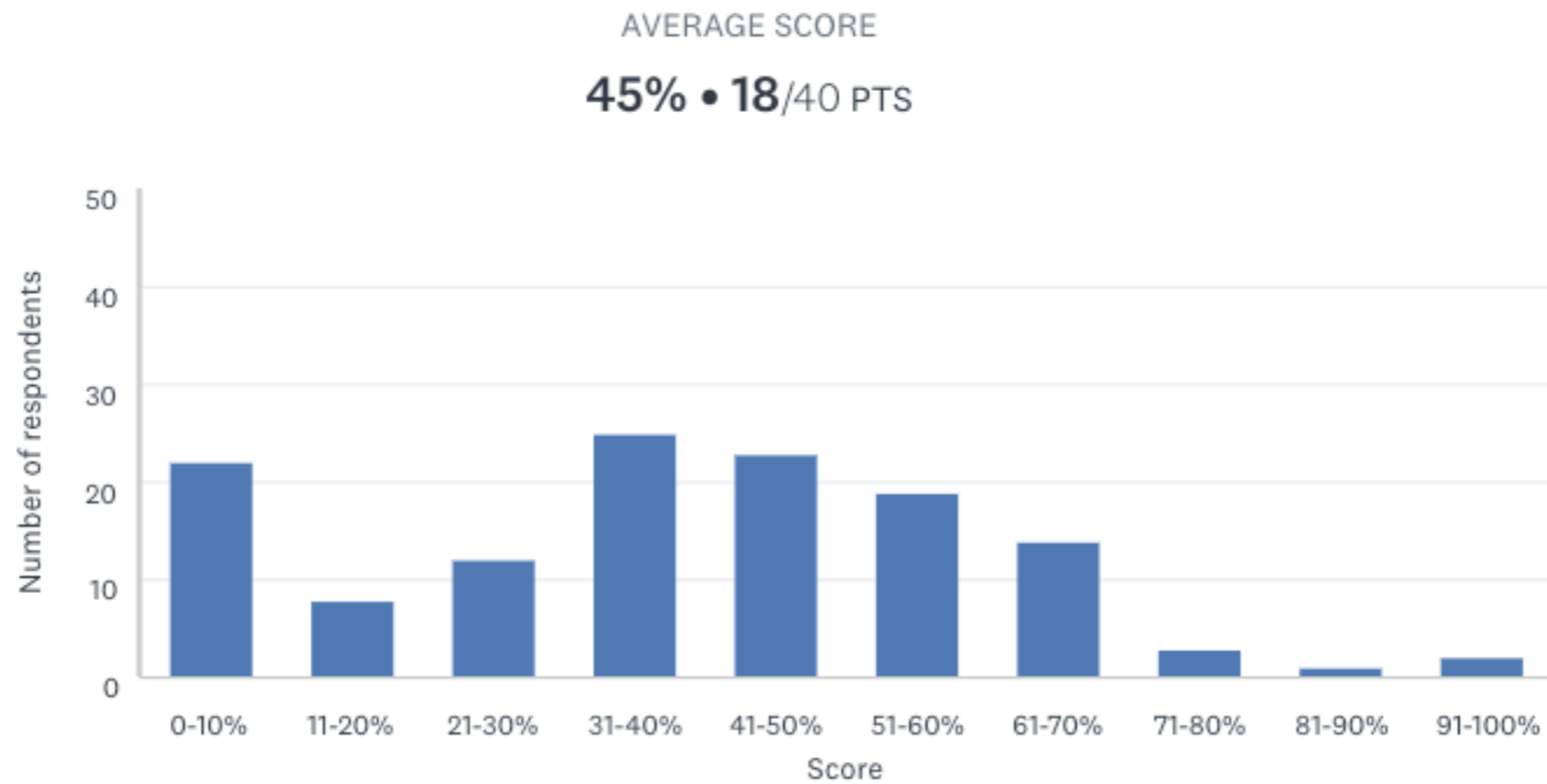
Quiz(?) Scores

Bug Bounty Program	5%
Familiar with Crypto in Smalltalk	13%
Smalltalk app uses encryption	23%
Awareness Program	28%
Regular Pentesting	32%
Formal Cybersec Program	37%

image-ware.com

Awareness

Q29 I think that overall, cybersecurity awareness within the Smalltalk community is:

image-ware.com
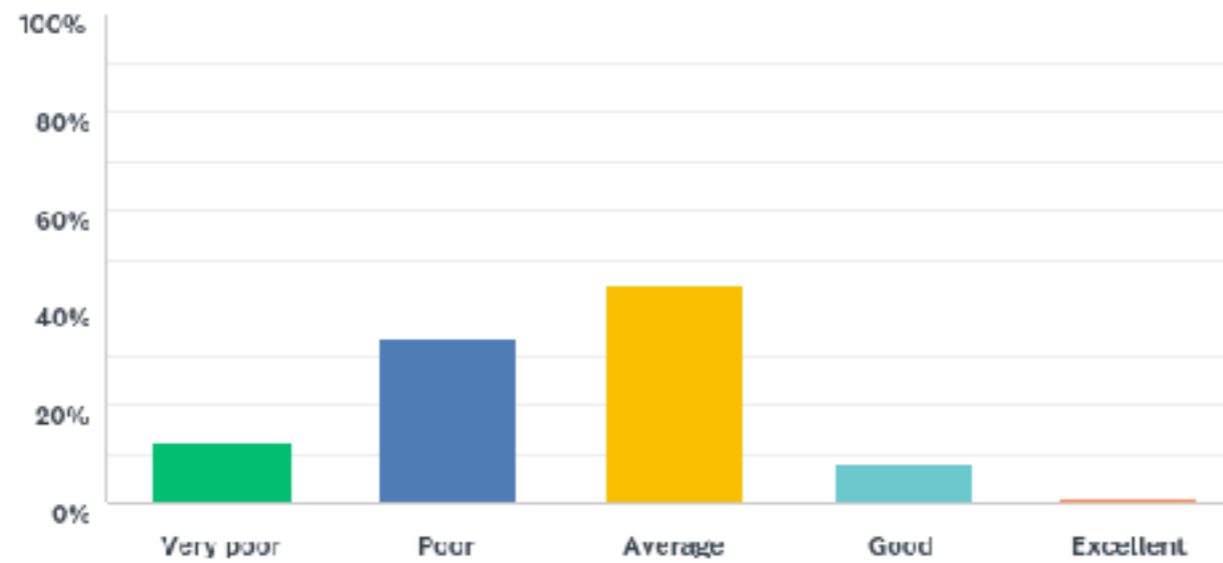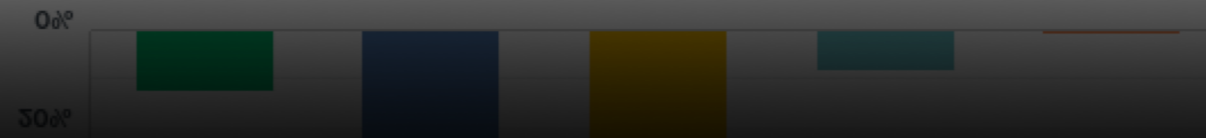
Awareness

Q48 Rank the strength of the links in the security chain at your organization, from Weakest to Strongest. Check 'N/A' if you think it's not a factor or not being used at your organization.
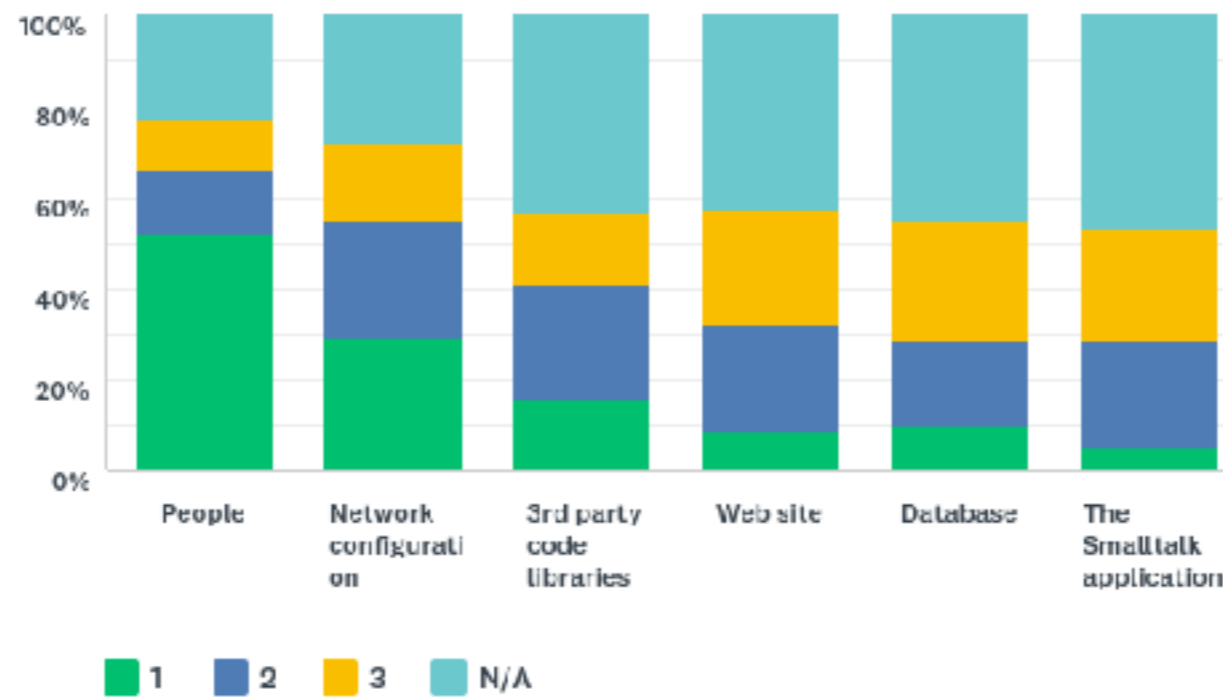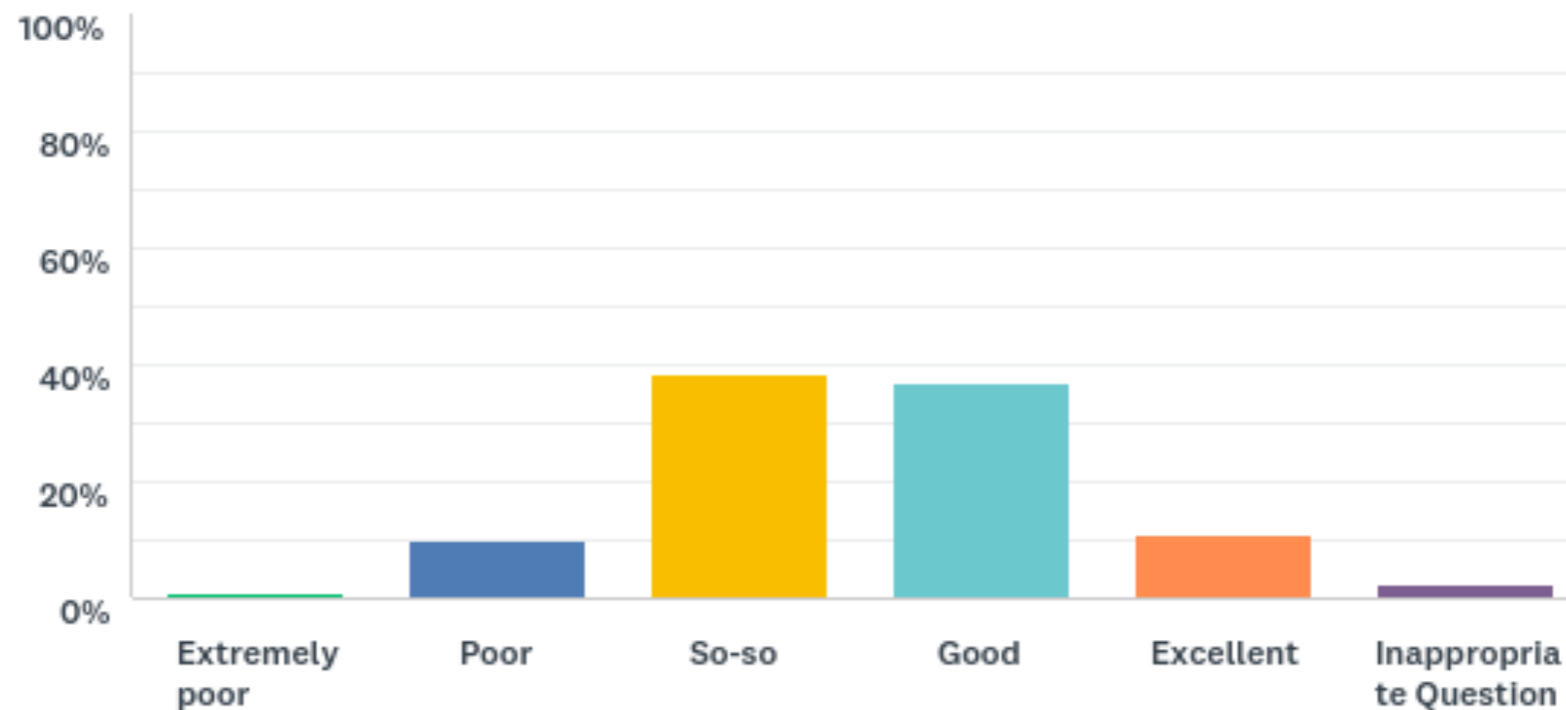
Security Posture

Q9 I would rate my organization's security posture as

Good or **Excellent** Security Posture

AVERAGE SCORE

50% • **20**/40 PTS
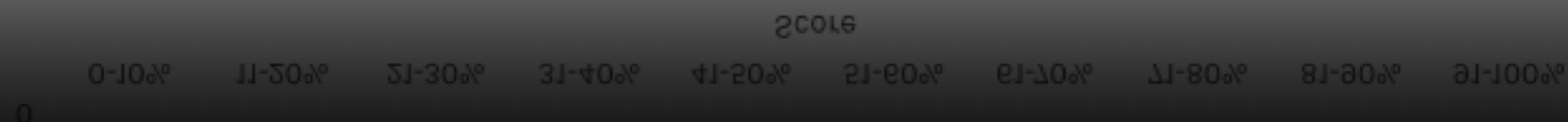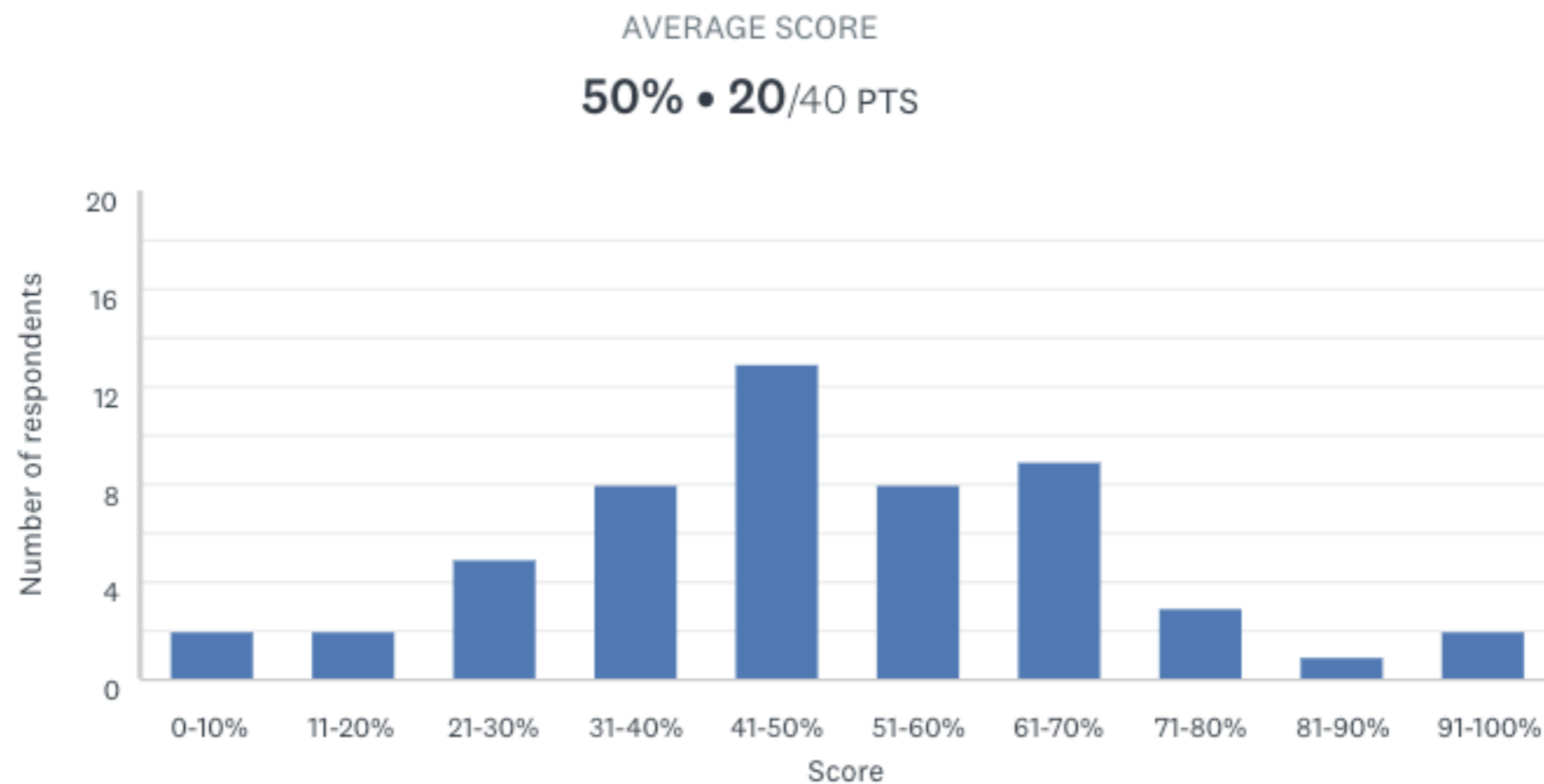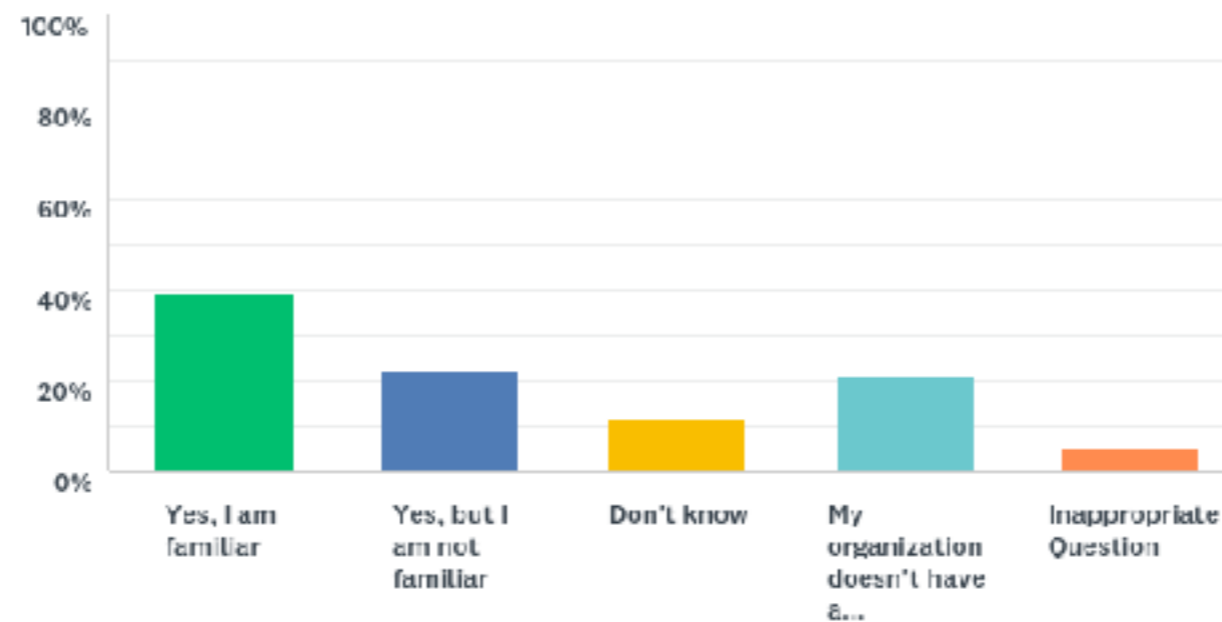
Good or **Excellent** Security Posture

Q10 My organization has a formal cybersecurity program (e.g., security policies, vulnerability assessments, penetration testing, incident response plan), and I am familiar with it.
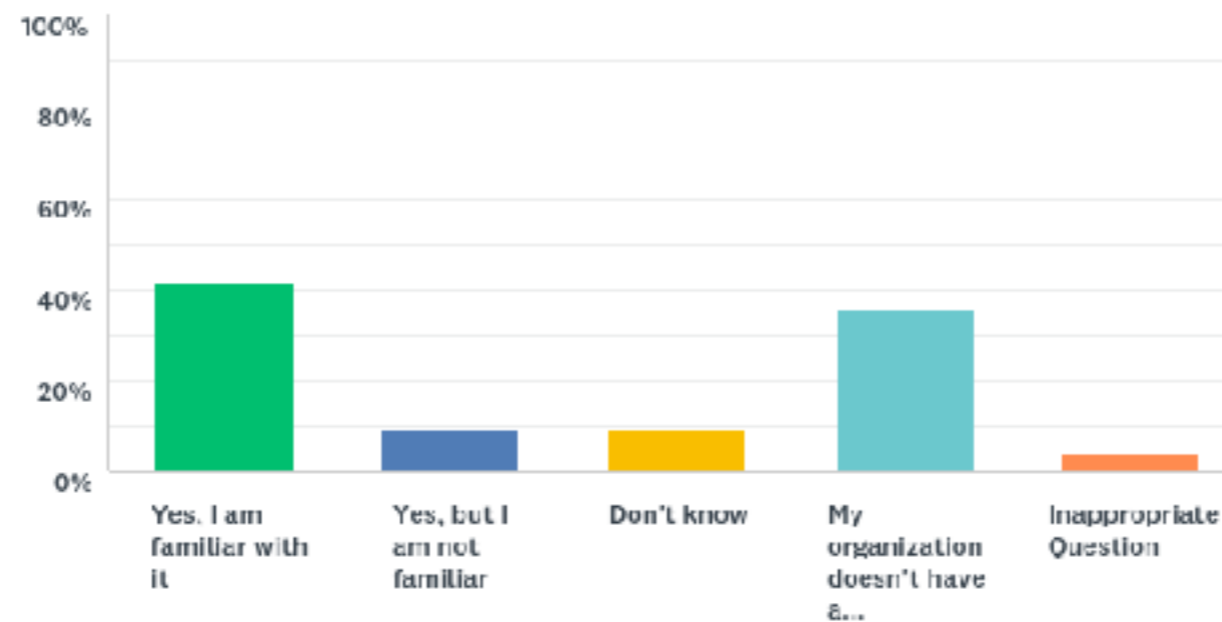
Good or **Excellent** Security Posture

Q11 My organization has a cybersecurity AWARENESS program for its employees (e.g., courses, workshops)

Good or **Excellent** Security Posture

Q15 My organization's network and systems are tested for security vulnerabilities (penetration testing)

Selected Quotes

Very complex question

****** has password within the image

No one has ever fixed any other vulnerabilities I have reported in open source Smalltalk software, so I stopped reporting them.

It's bad. I discreetly notified ****** more than once, but after two years it was still broken. So, I stopped using their system.
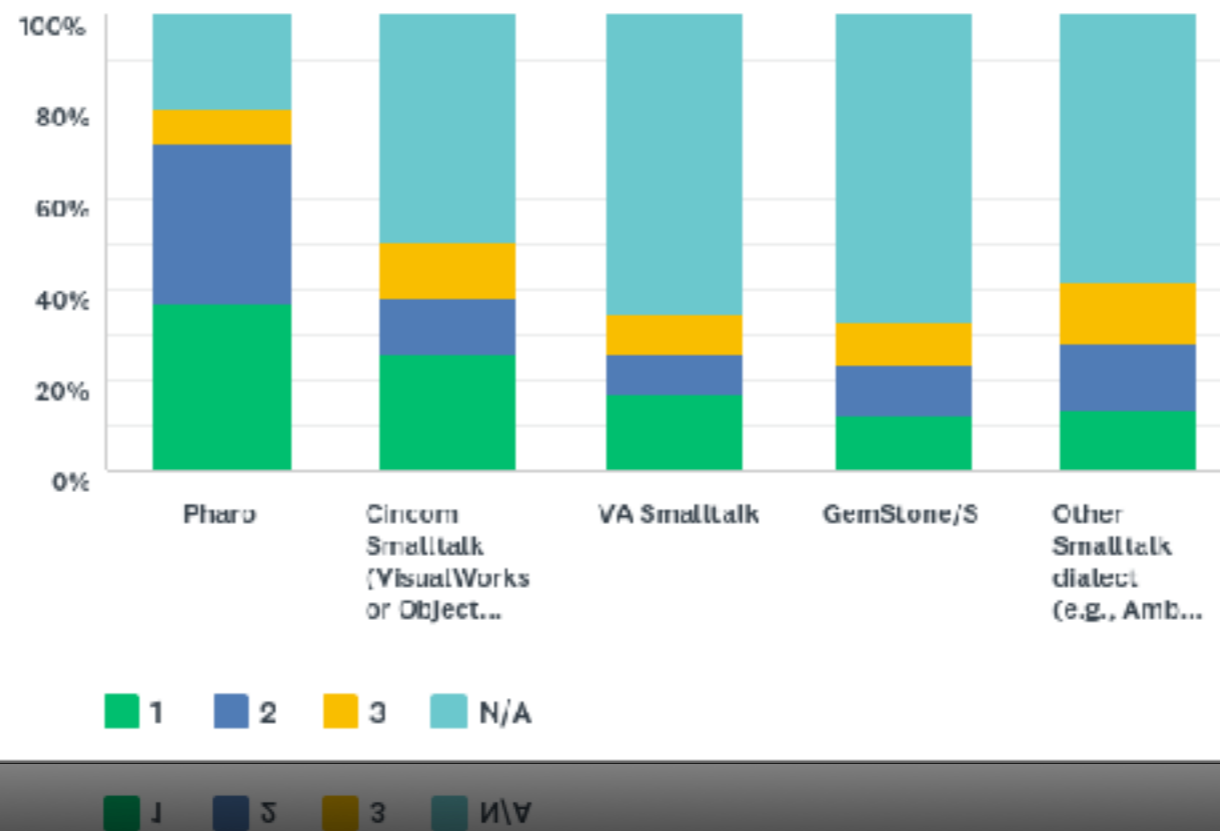
****** is the only one who does that !!!!

Password for a database server on a LAN.

image-ware.com

Dialect Assessment

Q8 Rank Smalltalk dialect(s) you use from the most to the least often used. If you don't use a dialect, please check 'N/A'.

Dialect Assessment

- Limited Scope - four major dialects / vendors

- WWW, FTP, … basic 'open source' reconnaissance

- Installed IDEs are fair game (I own the system)

- A somewhat reliable proxy for product security

image-ware.com

Dialect Assessment

- Six security categories, two privacy categories

- Higher score ~ higher risk

  ★ Vulnerability found and exploited: +2 + N points assigned based on severity, N = 0 (minor), 1 (serious), 2 (critical)

  ★ Potential vulnerability found: +1

  ★ Untested, unknown, or N/A: 0

  ★ Tested, no vulnerability found: -1

- Aggregate scores only

Dialect Assessment

	Cincom Smalltalk	GemStone/S	Pharo	VA Smalltalk
Security	9	3	7	7
Privacy	3	2	0	0
Total	**12**	**5**	**7**	**7**

image-ware.com

```
0F149Z0   00 D0 ED 0A 01 C1 ED 0A D0 C1 ED 0A 01 00 00 00   ................
0F14930   0F 00 00 00 0F 00 00 00 0F 00 00 00 03 00 00 00   ................
0F14940   03 00 00 00 03 00 00 00 03 00 00 00 0B 00 00 00   ................
0F14950   4C E8 AD 0A 18 D0 ED 0A 24 D0 ED 0A EC 76 B5 0A   L.......$....v..
0F14960   AC 17 EE 0A FC E0 C2 0A A0 17 EE 0A 0B 00 00 00   ................
0F14970   4C E8 AD 0A 3C D0 ED 0A 48 D0 ED 0A EC 76 B5 0A   L...<...H....v..
0F14980   C4 17 EE 0A FC E0 C2 0A B8 17 EE 0A 5C 75 40 5C   ............\u@\
0F14990   68 3A 5C 57 3E 00 00 00 0B 00 00 00 4C E8 AD 0A   h:\W>.......L...
0F149A0   78 D0 ED 0A 84 D0 ED 0A EC 76 B5 0A DC 17 EE 0A   x........v......
0F149B0   FC E0 C2 0A D0 17 EE 0A 0B 00 00 00 4C E8 AD 0A   ............L...
0F149C0   9C D0 ED 0A A8 D0 ED 0A EC 76 B5 0A F4 17 EE 0A   .........v......
0F149D0   FC E0 C2 0A E8 17 ..                               
0F149E0                                                      
0F149F0                                                      
0F14A00                         00 00 00 0B 00 00 00         
0F14A10   4C E8 AD 0A D8 D0 ED 0A E4 D0 ED 0A EC 76 B5 0A   L............v..
0F14A20   0C 18 EE 0A FC E0 C2 0A 00 18 EE 0A 0B 00 00 00   ................
0F14A30   4C E8 AD 0A FC D0 ED 0A 08 D1 ED 0A EC 76 B5 0A   L............v..
0F14A40   24 18 EE 0A FC E0 C2 0A 18 18 EE 0A 48 18 EE 0A   $...........H...
0F14A50   54 18 EE 0A 30 18 EE 0A 3C 18 EE 0A 17 00 00 00   T...0...<.......
0F14A60   07 00 00 00 FF FF FF FF 03 00 00 00 03 00 00 00   ................
0F14A70   50 41 54 48 04 57 B7 0A E8 C6 ED 0A 4C E8 AD 0A   PATH.W......L...
0F14A80   4C E8 AD 0A 4C E8 AD 0A 4C E8 AD 0A 4C E8 AD 0A   L...L...L...L...
0F14A90   4C E8 AD 0A 4C E8 AD 0A 4C E8 AD 0A 4C E8 AD 0A   L...L...L...L...
0F14AA0   4C E8 AD 0A 4C E8 AD 0A 4C E8 AD 0A 4C E8 AD 0A   L...L...L...L...
0F14AB0   4C E8 AD 0A 4C E8 AD 0A 4C E8 AD 0A 4C E8 AD 0A   L...L...L...L...
0F14AC0   4C E8 AD 0A 4C E8 AD 0A 4C E8 AD 0A 4C E8 AD 0A   L...L...L...L...
```

```
0629580   D8 57 3E 0A 00 00 00 00 C0 94 3E 0A 00 00 00 00   .W>........>.....
0629590   A0 29 03 0B 00 00 00 00 48 0B 6A 0B 00 00 00 00   .)......H.j.....
06295A0   B0 24 92 09 00 00 00 00 00 00 00 80 30 00 00 00   .$..........0...
06295B0   F0 35 23 0B 00 00 00 00 F0 35 23 0B 00 00 00 00   .5#......5#.....
06295C0   99 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00   ................
06295D0   0E 00 00 00 00 00 00 00 91 31 83 02 00 00 00 00   .........1......
06295E0   50 59 92 09 00 00 00 00 03 00 0C 50 06 00 00 00   PY.........P....
06295F0   ..    ..    ..    ..  ..    00 50 59 92 09 00 00 00 00   ........PY......
0629600   03 00 A2 50 0A 00 00 00 4A 65 72 72 79 20 4B 6F   ...P....Jerry Ko
0629610   74 74 00 00 00 00 00 00 B0 24 92 09 00 00 00 00   tt.......$......
0629620   00 00 00 80 30 00 00 00 A0 32 23 0B 00 00 00 00   ....0....2#.....
0629630   A0 32 23 0B 00 00 00 00 87 00 00 00 00 00 00 00   .2#.............
0629640   03 00 00 01 00 00 00 00 0E 00 00 00 00 00 00 00   ................
0629650   B1 17 83 02 00 00 00 00 B0 24 92 09 00 00 00 00   .........$......
0629660   00 00 00 80 30 00 00 00 A0 31 23 0B 00 00 00 00   ....0....1#.....
0629670   A0 31 23 0B 00 00 00 00 4D 01 00 00 00 00 00 00   .1#.....M.......
0629680   03 00 00 00 00 00 00 00 0E 00 00 00 00 00 00 00   ................
0629690   91 31 83 02 00 00 00 00 50 59 92 09 00 00 00 00   .1......PY......
06296A0   03 00 58 29 00 00 00 00 50 59 92 09 00 00 00 00   ..X)....PY......
06296B0   03 00 CC 29 42 00 00 00 43 3A 5C 55 73 65 72 73   ...)B...C:\Users
06296C0   5C 4A 65 72 72                                     \Jerry Kott
06296D0
06296E0
06296                                     00 00 00 00 00
0629700   B0 24 92 09 00 00 00 00 00 00 00 80 30 00 00 00   .$..........0...
0629710   A0 32 23 0B 00 00 00 00 A0 32 23 0B 00 00 00 00   .2#......2#.....
0629720   79 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00   y...............
0629730   0E 00 00 00 00 00 00 00 B1 17 83 02 00 00 00 00
```

55

```
00000078   00 00 00 25 00 00 00 00   00 00 00 0c 00 00 00 00    ...%.... ........
00000088   0b 5c b1 10 00 00 00 00                              .\......
    00000219   00 00 00 00 00 00 00 00   00 00 00 3a 21 00 00 00    ........ ...:!...
    00000229   00 00 00 00 34 33 32 31   58 00 00 00 3a 00 00 00    ....4321 X...:...
    00000239   3a 00 00 00 3a 1d 00 00   3a 1d 00 00 0a 53 75 70    :...:.. :....Sup
    00000249   65 72 76 69 73 6f 72 17   cb b5 00 17 cb b5 00 06    ervisor. ........
    00000259
00000090   00 00 00 25 00 00 00 00   00 00 00 0c 00 00 00 00    ...%.... ........
000000A0   0b 5c b1 70 00 00 00 00                              .\.p....
    0000025F   00 00 00 00 00 00 00 00   00 00 00 60 11 20 00 00    ........ ...`. ..
    0000026F   00 00 00 00 34 33 32 31   60 00 00 00 60 00 00 00    ....4321 `...`...
    0000027F   60 00 00 00 34 00 3e 00   00 00 00 00 00 00 00 00    `...4.>. ........
    0000028F   0c cb b5 00 0c cb b5 00   00 00 00 00 00 00 00 00    ........ ........
    0000029F   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00    ........ ........
    000002AF   00 00 00 00 00 00 00 00   4a 65 72 72 79 20 4b 6f    ........ Jerry Ko
    000002BF   74 74 6a 65 72 72 79 20   6b 6f 74 74               ttjerry  kott
000000A8   00 00 00 1d 00 00 00 00   00 00 00 00                ........ ....
    000002CB   00 00 00 00 00 00 00 00   00 00 00 04 00 00 00 02    ........ ........
000000B4   00 00 00 0b 00 00 00 00   00 00 00 14                ........ ....
000000C0   6a 65 72 72 79 20 6b 6f   74 74 00                   jerry ko tt.
000000C
    000002DB   00 00 00 00 00 00 00 00   00 00 00 00                ........ ....
```

Packet 16, 11 *client pkts*, 9 *server pkts*, 17 *turns*. Click to select.

Frameworks

- Seaside

- Magritte

- AppeX (CST)

- Opentalk (CST)

- Server Smalltalk (VA St)

etc…

Frameworks

- CSRF

- XSS

- Injection

- Broken Authentication

- Misconfiguration

- RCE

more detailed assessment needed

image-ware.com

Tools

- Kali Linux (https://www.kali.org/downloads/)

- nmap (https://nmap.org/)

- Wireshark (https://www.wireshark.org/download.html)

- Burp Suite (https://portswigger.net/burp/communitydownload)

image-ware.com

More Tools

- Net Cat (nc)

- tcpdump

- Dir Buster (dirb)

- nikto

- curl

- hex editor

…etc

image-ware.com

What's next?

- New Google Group: smalltalk-security (https://groups.google.com/forum/#!forum/smalltalk-security)

- Ask difficult and honest questions (assume breach)

- Work with vendors to address known issues

- Vulnerability reporting - CVEs etc…

- New framework versions (e.g., Seaside 4?) need to put more focus on security

image-ware.com

Conclusion

- People are the weakest link

- Improve Security Posture

- Awareness needs to get better

- Ethical responsibility to deliver software that works **and** has world class security

image-ware.com

Final Thought

Which would you rather build?

image-ware.com

Many Thanks!

My family

Victoria Cybersecurity Hackers

Offensive Security

Smalltalk Community

YOURSELVES

image-ware.com

Questions?

esug2018@image-ware.com

image-ware.com/static/esug2018.pdf

image-ware.com