Operational Security

3 and RAV's

Operational Security

by

Cor Rosielle

ISACA – Netherlands Local Chapter
June 2nd, 2014

I am

- … Cor Rosielle (cor@osstmm.nl)
- … professionally involved in IT since 1983
- … specialized in operational security
- … a pentester for a governmental organization
- … a member of the ISECOM team
- … a contributor to the OSSTMM
- … certified in many area's CISSP, ISSAP, OPST, OPSA, OPSE, OWSE, CTA, CEH, ECSA
- … originally a civil engineer

This presentation

- The talk today is about an often neglected area of security:

Operational Security

Short introduction

- A security professional often spends his time on:
  - Compliancy
  - Risk Management

It does help

- Both Compliancy and Risk Management do help to increase security
- But neither of them is a complete solution
- Even if we do both, there remain a lot of practical questions:

What we don't know is ...

- What should be protected first?
- Which solutions helps best to protect?
- How to spend money wise on security controls?
- How much improvement is gained on security when using the intended solutions ?
- How do we measure the improvements?
- How do we know if we are reducing our exposure to threats instead of increasing them?
- How well can we resists attacks?

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

Characteristics

- Characteristics of Compliancy:
  - Checks to what extent an environment matches a reference model
  - Recommendations are based on mismatches between the environment and the reference model
  - Recommendations are prioritized according to qualitative standards

Characteristics

- Characteristics of Risk Management :
  - Determines the (sum of) risk(s) when an object is hit by certain threat(s)
  - Simplified risk formula:
    Risk = Chance x Impact
  - More advanced formula's also include chance
  - If the threat does not exist yet, we can't determine chance. This means the threat must be known before the risk calculation can start
  - Risks are often expressed in a qualitative manner

Other characteristics

- Other characteristics are (somewhat exaggerated)
  - Compliancy:
    describes a general set of rules and controls that worked for other organizations under different circumstances at another time
  - Risk Management:
    is always a step behind, because you can't determine the risk for unknown threats

Side effect examples

- Compliancy
  - Anti virus helps protecting the integrity of a system
  - But it is a system in itself that needs to be protected
  - To decide what is good for you, the vendor makes the choices mor often than you
- Risk Management
  - You can't do a proper risk assessment for 0-day vulnerabilities
  - If you focus on OWASP top 10, you're ignoring threats, responsible for about 75% of incidents

operational security

- Operational Security Audits are often missing
- Such an audit determines the resistance to unspecified threats of an object or environment
  - It doesn't focus on specific threats
  - It doesn't recommend to follow best/good practices
- Operational Security is not about threats or risks. It is about protection!

Tell me more ...

- There is a simple way to prevent shoplifting
- It has a little disadvantage

… go on ...

- To be in business, the shop has to be accessible for customers
- So it has to be open:

- Well, not necessarily 24/7

… proceed ...

- But letting the customers in the shop exposes the shopkeeper to threats:
  - Articles might get stolen by customers
  - Articles might get damaged by customers
  - Prices might get changed by customers
- The solution is not to find a way to resist each individual threat …
- … the solution is to control possible interactions.

Clever thinking

But how?

We'll use the ...

Open

Source

Security

Test

Methodology

Manual

OSSTMM

- The OSSTMM is:
  - Created in 2000 by Pete Herzog
  - Maintained by security professionals all over the globe
  - Current public version is OSSTMM 3
    - Which btw is a candidate for an ISO standard
  - OSSTMM 4 first draft is under review of contributors
  - Public availability for OSSTMM 4 is expected in 2014

OSSTMM Basics

- The basics are simple:
  1. To be in business, you have to be accessible
  2. Access creates opportunity to interact
  3. Interactions have to be sufficiently controlled
  4. Controls have to be well implemented

RAV's

- We're going to use RAV's to support our decissions
- RAV is an acronym for Risk Assessment Value

RAV's (continued)

- RAV is a security metric that shows how well protected a system or environment is to threats
- RAV's are not really about risk (but tells about protection).
- It is a quantitative, numeric value.
- 100 RAV is considered as perfect security. This means there is an optimal balance between possible interactions and controls

RAV's (continued)

- When a RAV is below 100, the calculation shows which controls are insufficient or even completely absent.
- When a RAV is 100 and more controls are added, the RAV exceeds 100
  - It means you're wasting money, because you spend money on something that is perfectly secure already

3 main elements

- OPSEC (operational security)
- Controls
- Limitations

OPSEC

- OPSEC is the necessary lowering of defenses to be in business
- There are 3 elements in OPSEC
- The elements of operational security are

visibility

access

trust

Geef deze stempas alleen mee aan een ander nadat de pas door
en uw gemachtigde is ingevuld en ondertekend.

VOLMACHTBEWIJS

Mijn verklaring:

Ik stem niet zelf. Ik laat mijn stem uitbrengen door:

Oproep voor de verkiezing van de Nederlandse leden van het Europees Parlement op donderdag 22 mei 2014

Controls

- **Loss controls** are counter measures that increase the amount of resistance and robustness

interactive controls

process controls

Limitations

- **Limitations** are imperfections in OPSEC and controls

Opsec - Visibility

- Suppose you’re a treasure hunter, where would you start digging? In the hard rock or the soft sand?
- If you are prey, wouldn't it be nice if you had camouflage colors or patterns?
- Visibility creates opportunity
- All accessible targets are counted once

Opsec - Access

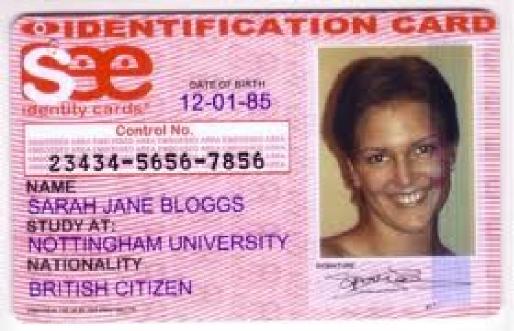
- Opportunity to interact with a target
- All individual ways to interact with a target are counted
- Examples
  - doors and windows
  - gates
  - network ports
  - fields in HTML form or query string

Opsec - Trust

- Trust is where target can interact freely with another target in the scope
- Example
  - A web service can connect to a database without the need the user authenticates to the database server
  - To count trust, the direction of trust is not important.
  - The rav for the lady involves a trust

Interactive Controls – Authentication

- Identification is claiming an identity
- Authentication is proving you are entitled to the claimed identity
- Authorization are the permissions you have after your identity has been proven
- Examples
  - password (something you know)
  - ID card, token, certificate (something you have)
  - Fingerprint, Iris pattern, DNA pattern (something you are)
  - White list (firewall), black list (AV)



IDENTIFICATION CARD

see identity cards

DATE OF BIRTH 12-01-85

Control No. 23434-5656-7856

NAME SARAH JANE BLOGGS

STUDY AT: NOTTINGHAM UNIVERSITY

NATIONALITY BRITISH CITIZEN

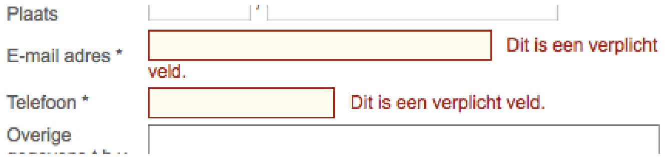
SIGNATURE

Interactive Controls – Indemnification

- All kind of paperwork and rules, mostly to cover your ass
- Examples
  - contracts
  - terms and condition
  - insurance
  - accept conditions

Interactive Controls – Subjugation

- Forcing something is done the way you want it to
- It removes the freedom from the user to act different
- Examples
  - HTTPS – forces using a secure protocol
  - Not proceeding to the next step until required phases from the previous step have not been completed



Plaats

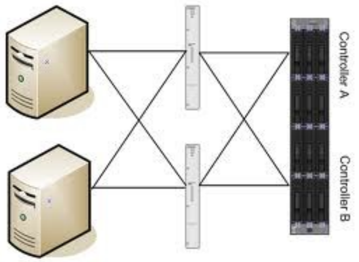
E-mail adres * Dit is een verplicht veld.

Telefoon * Dit is een verplicht veld.

Overige

Interactive Controls – Continuity

- If a component fails, the process continues (but security might be lost)
- Examples
  - Two lungs, two kidneys
  - redundant mail or domain name server
  - Clusters
  - Load balancer
  - hot standby communication lines



Interactive Controls – Resilience

- In previous versions of the OSSTMM this was called: resistance
- If a component fails, the security continues
- Example
  - if the firewall fails, there is no access at all
  - if electronic payment devices fail, you have to pay in another way or can’t take your grocery home

Process Controls – Non-repudiation

- A party can not deny (s)he was involved in an interaction
- The identity of that party must be certain
- Proof about the interaction must have been collected and preserved
- Example
  - Signature

Process Controls – Confidentiality

- The content of an interaction is hidden for other parties
- Examples
  - Encryption
  - Steganography

Process Controls – Privacy

- The interaction itself is hidden from other parties
- Not being noticed in the environment
- Examples
  - identical trunks swapped on station in drugs deal
  - proxy servers and load balancers hide components behind it
  - Tor-network

Process Controls – Integrity

- The sender or receiver will notice if something is changed during transit.
- Examples
  - seals on food and medicine
  - cryptographic hashes

Process Controls – Alarm

- Abnormal events are noticed and acted upon
- Examples
  - fire alarm, smoke alarm, burglar alarm
  - Intrusion detection system
  - SIEM

Limitations – Vulnerability

- Any flaw that defies protection where a person or process can give or deny access to others or hide within the scope
- Examples
  - Lock not functioning
  - Denial of Service

Limitations – Weakness

- A weakness is a flaw in an interactive control

COUNTY OF LOS ANGELES
Public Health
ENVIRONMENTAL HEALTH
A
THIS ESTABLISHMENT RECEIVED A SCORE OF 90-100%
AT THE TIME OF INSPECTION
The most recent food inspection report is available here for review upon request
112490

Limitations – Concern

- A concern is a flaw in an process control

- Formally the lack of privacy is not a limitation, because there is no control in the first place. But it's a nice picture.

Limitations – Exposure

- An exposure unintentionally gives detailed information
- It often leads to a new visibility and increases OPSEC

Limitations – Anomaly

- An event that can not be accounted for in normal operations

Any condition that does not match an expected one

RAV calculation

- Categorize all your observations
- Count the numbers
- Enter the results in the formula's

$$\Delta\beta_u = \beta_{\text{ultimate}} - \beta_{\text{member}} = \frac{\ln\left(\frac{LF_u}{LL_{75}}\right) - \ln\left(\frac{LF_1}{LL_{75}}\right)}{\sqrt{V_{LF}^2 + V_{LL}^2}}$$

$$= \frac{\ln\left(\frac{LF_u}{LF_1}\right)}{\sqrt{V_{LF}^2 + V_{LL}^2}} = \frac{\ln(R_u)}{\sqrt{V_{LF}^2 + V_{LL}^2}},$$

$$\Delta\beta_f = \beta_{\text{functionality}} - \beta_{\text{member}} = \frac{\ln\left(\frac{LF_f}{LL_{75}}\right) - \ln\left(\frac{LF_1}{LL_{75}}\right)}{\sqrt{V_{LF}^2 + V_{LL}^2}}$$

$$= \frac{\ln\left(\frac{LF_f}{LF_1}\right)}{\sqrt{V_{LF}^2 + V_{LL}^2}} = \frac{\ln(R_f)}{\sqrt{V_{LF}^2 + V_{LL}^2}}$$

and

$$\Delta\beta_d = \beta_{\text{damaged}} - \beta_{\text{member}} = \frac{\ln\left(\frac{LF_d}{LL_2}\right) - \ln\left(\frac{LF_1}{LL_{75}}\right)}{\sqrt{V_{LF}^2 + V_{LL}^2}}$$

$$= \frac{\ln\left(\frac{LF_d}{LF_1}\frac{LL_{75}}{LL_2}\right)}{\sqrt{V_{LF}^2 + V_{LL}^2}} = \frac{\ln\left(R_d\frac{LL_{75}}{LL_2}\right)}{\sqrt{V_{LF}^2 + V_{LL}^2}}, \qquad (11)$$

- Or use spreadsheet from http://www.isecom.org/ravs

Example RAV calculation

- A system responds open ports on 80 /tcp and 443 /tcp
- No response on all other ports (TCP, UDP and ICMP)
- On port 80 /tcp an HTTP protocol is spoken and one of the response headers says: Server: Apache/2.2.19 (Win32) PHP/5.2.17
- On port 443 /tcp an HTTPS protocol is spoken, supporting SSLv2 and cipher suites with keys of 40 and 56 bits
- The SSL certificate is self signed and two months expired
- One of the response headers for port 443 /tcp says:
  Via: 1.1 Cerberus
- Use the spread sheet to calculate the rav for the server

Answers

- *A system responds with open ports on 80 /tcp and 443 /tcp*
- The system is accessible on 2 ports, hence **2x access**
- Also the system is visible, hence **1x visibility**

Answers

- *There is no response on all other ports (TCP, UDP and ICMP)*
- According to the different RFC’s the server should notify the client about closed ports. Because these responses are not received, the responses are filtered by a firewall (or other filtering device), hence 1x authentication for each protected access.
- Total: **2x authentication**

Answers

- *On port 443 /tcp an HTTPS protocol is spoken.*
- HTTPS provides encryption and detects when the key negotiation is altered. Further it removes freedom from the visitor to use insecure communication. Therefore this is counted as **1x confidentiality, 1x integrity** and **1x subjugation**

Answers

- *Apache and PHP version numbers are leaked*
- This is counted as **2x exposure**

- Examining the known vulnerabilities in these versions can lead to more limitations

Answers

- The SSL certificate proves the identity of the server to the client. This can serve both as an authentication and non-repudiation control.
- However, knowing the identity of the server protects the visitor and not the server itself. Therefore this observation is not counted to calculate the RAV of the server.

Answers

- The SSLv2 protocol has serious flaws and it is recommended not to use since 1996.
- This is counted as 2**x concern** (limitation in confidentiality and integrity).

Answers

- Keys with lengths of 40 and 56 bits could be broken in the previous century and should not be used to protect confidential data.
- This is counted as another **1x concern** (weak ciphers).

Note:
This is actually a risk decision. If the data only has to be protected for a couple of minutes, then a 40 bit symmetric key still might be sufficient

Answers

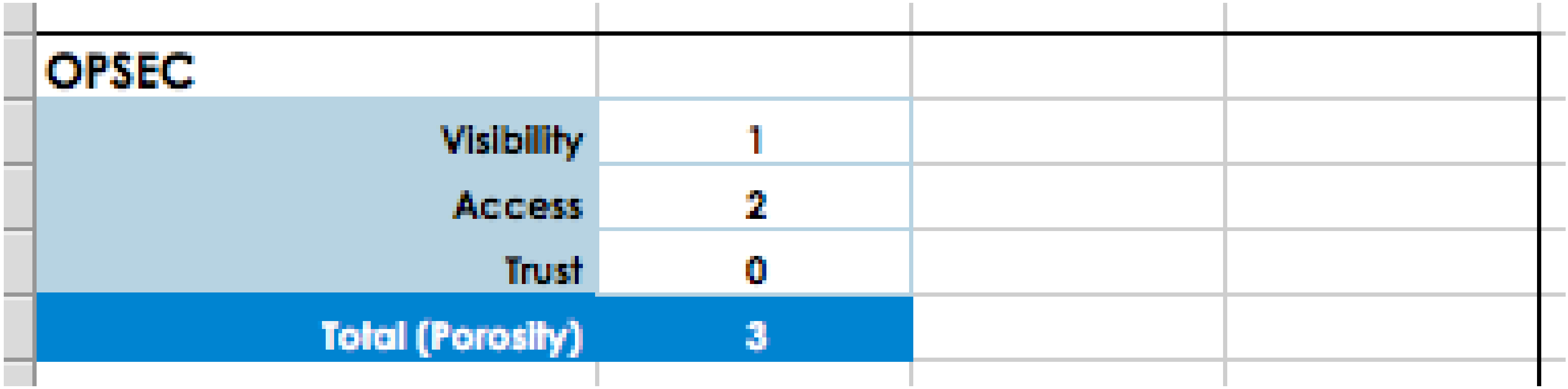
- *The SSL certificate is self signed and two months expired.*
- An SSL certificate is meant to prove the identity of the server. The server is not endangered by not having prove of its own identity.
- Therefore this observation is not counted to calculate the RAV of the server. It would count as a limitation when calculating the RAV of the visitor.

Answers

- *One of the response headers for port 443 /tcp says:*
  Via: 1.1 Cerberus
- A proxy server provides privacy and sometimes authentication.
- Hence **1x privacy**.
- A proxy server is discovered and can be attacked. If interactions with this proxy-server are possible, then 1x visibility and 1 or more accesses should be added.

Answers

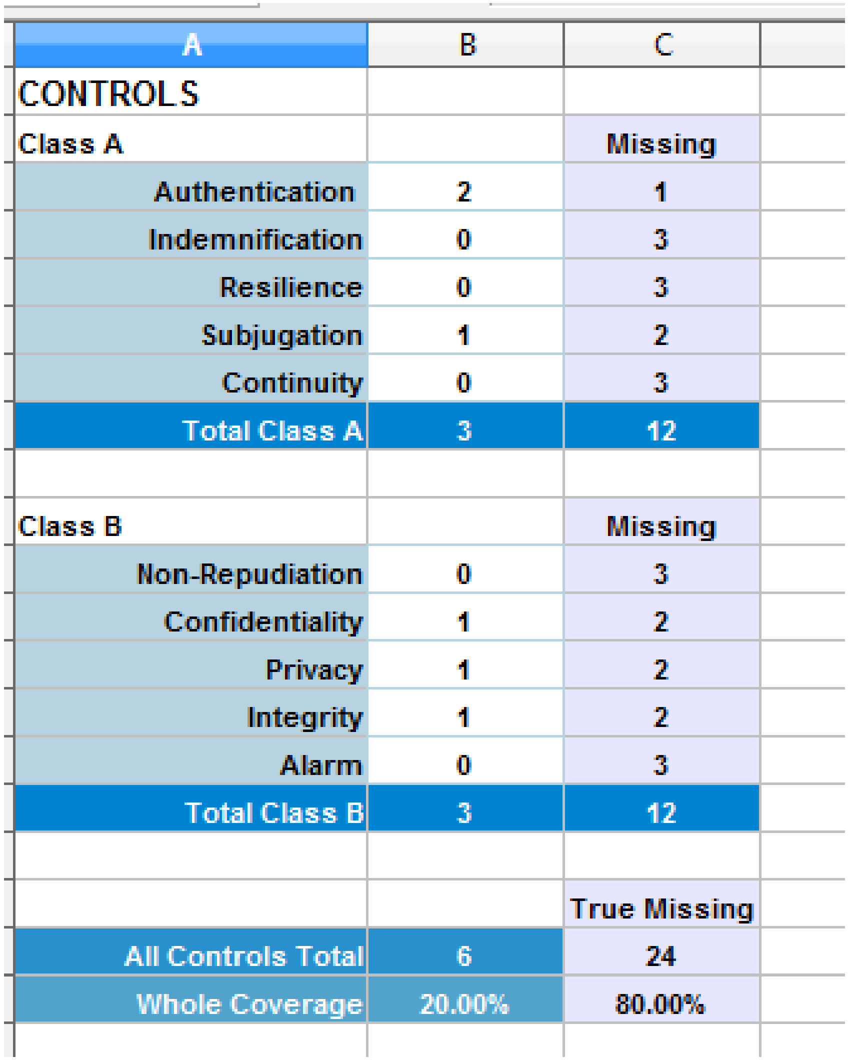
- Data is entered in the spreadsheet
- Here is the Porosity



OPSEC	
Visibility	1
Access	2
Trust	0
Total (Porosity)	3

Answers

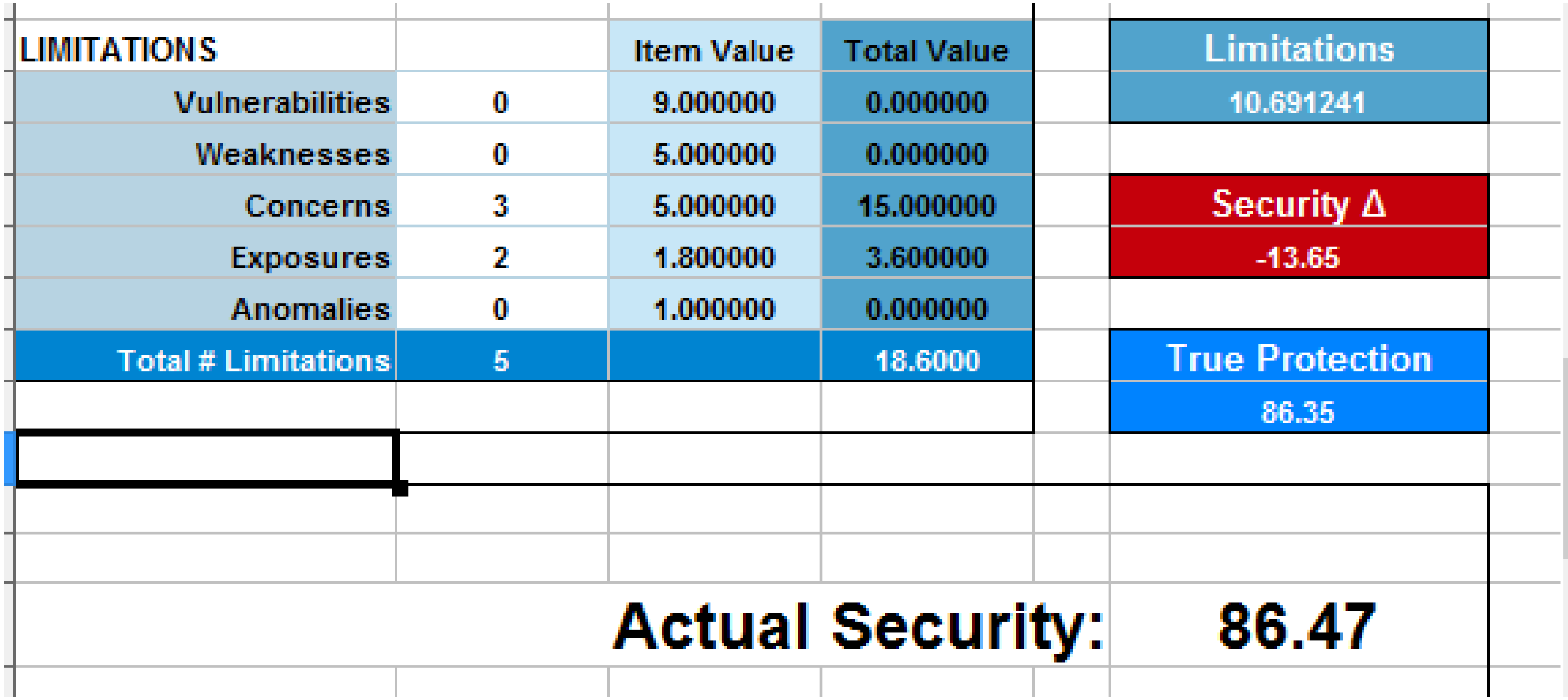
- These are the controls
- Controls increase security



A	B	C
CONTROLS		
Class A		Missing
Authentication	2	1
Indemnification	0	3
Resilience	0	3
Subjugation	1	2
Continuity	0	3
Total Class A	3	12
Class B		Missing
Non-Repudiation	0	3
Confidentiality	1	2
Privacy	1	2
Integrity	1	2
Alarm	0	3
Total Class B	3	12
		True Missing
All Controls Total	6	24
Whole Coverage	20.00%	80.00%

Answers

- These are the limitations, which are bad for security
- And we can read the resulting rav: 86.47
- on your school report it would look like a 7



LIMITATIONS		Item Value	Total Value
Vulnerabilities	0	9.000000	0.000000
Weaknesses	0	5.000000	0.000000
Concerns	3	5.000000	15.000000
Exposures	2	1.800000	3.600000
Anomalies	0	1.000000	0.000000
Total # Limitations	5		18.6000

Limitations
10.691241

Security Δ
-13.65

True Protection
86.35

Actual Security: 86.47

Answers

- Fixing limitations raises the rav to 96.85 (9+)

Answers

- If you want to raise the RAV even more, you can add more controls
- You can play “what if analysis” using the spreadsheet to determine which solution adds the most security or which adds the most security per dollar/euro/pound/yen

Solutions

- 1st: Remove unnecessary access
- If you remove unnecessary points of accesses, they don’t need protection.
- Each access needs 10 different controls to compensate
- Reducing access will increase the rav immediately, usually without much effort
  - We recognize this as a best/good practice: hardening

Solutions (continued)

- Solve the limitations found
- Some limitations are easy to solve and solving limitations increases the RAV more rapidly than adding new controls.
- Other limitations are harder to solve and sometimes even virtually impossible, e.g. because fixing a vulnerability breaks the functionality of the server.
- In that case consider to add more varied controls.

Solutions (continued)

- Add more varied controls
- If you still want to increase the RAV, add more varied controls.
- If you do, start with controls that are underrepresented or not used at all.
- It is more effective to add an underrepresented control than adding the next control of a type that overrepresented.
- Try to balance different types of controls.

Current and future developments

- RAV calculation is not very intuitive
- Often mistakes are made in RAV calculation
- Therefore ISECOM will help to simplify things

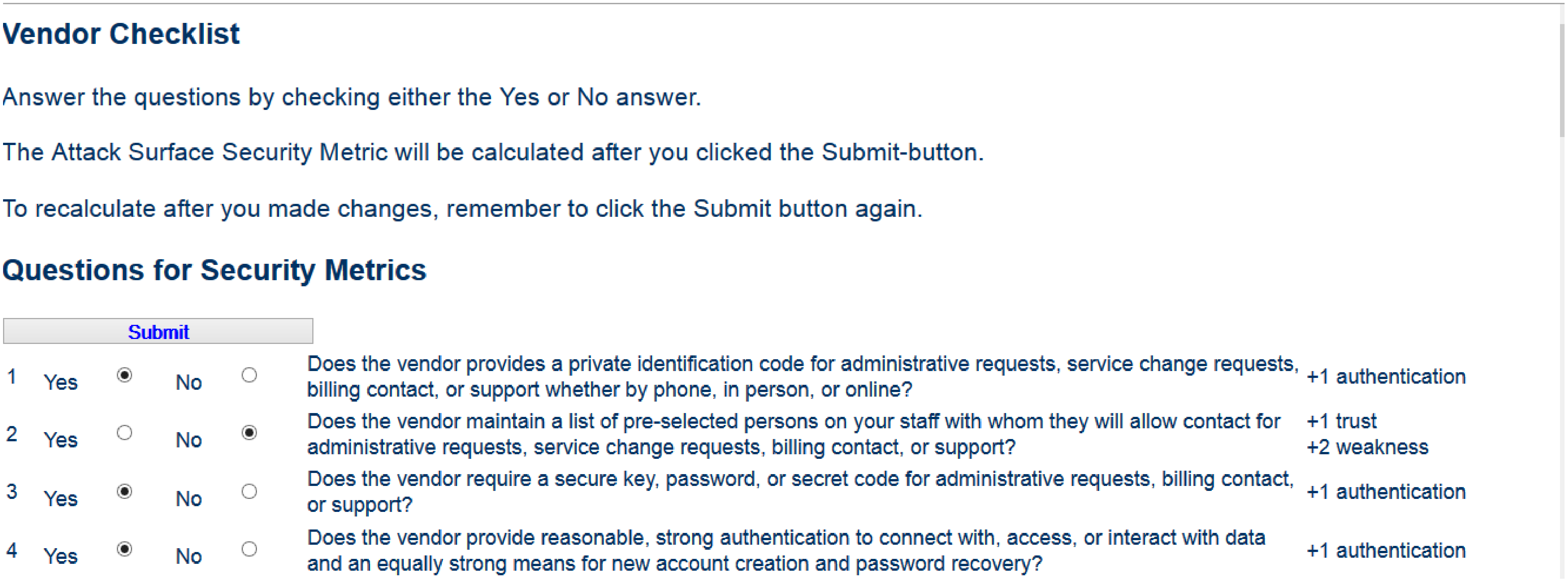
Standard rating

- Standard metrics for common observations makes the rating easier and consistent among analysts, eg:
  - HTTPS gives: 1x confidentiality, 1x integrity and 1x subjugation
  - SSLv2 gives: 2x concern
  - Filtered ports: 1x authentication per open port

Questionnaires

- Standard questionnaires
  - Yes/no answers are converted to appropriate metrics
  - All values are entered into the formula and result in a RAV
    - The simplified method leads to an approximation of the RAV
    - It's not as good as a full analysis and calculation, but it's better than qualitative risk rating
    - You can still find underrepresented controls and determine how much an intended control improves the RAV, hence improves the security

OPSEC questionnaire



Vendor Checklist

Answer the questions by checking either the Yes or No answer.

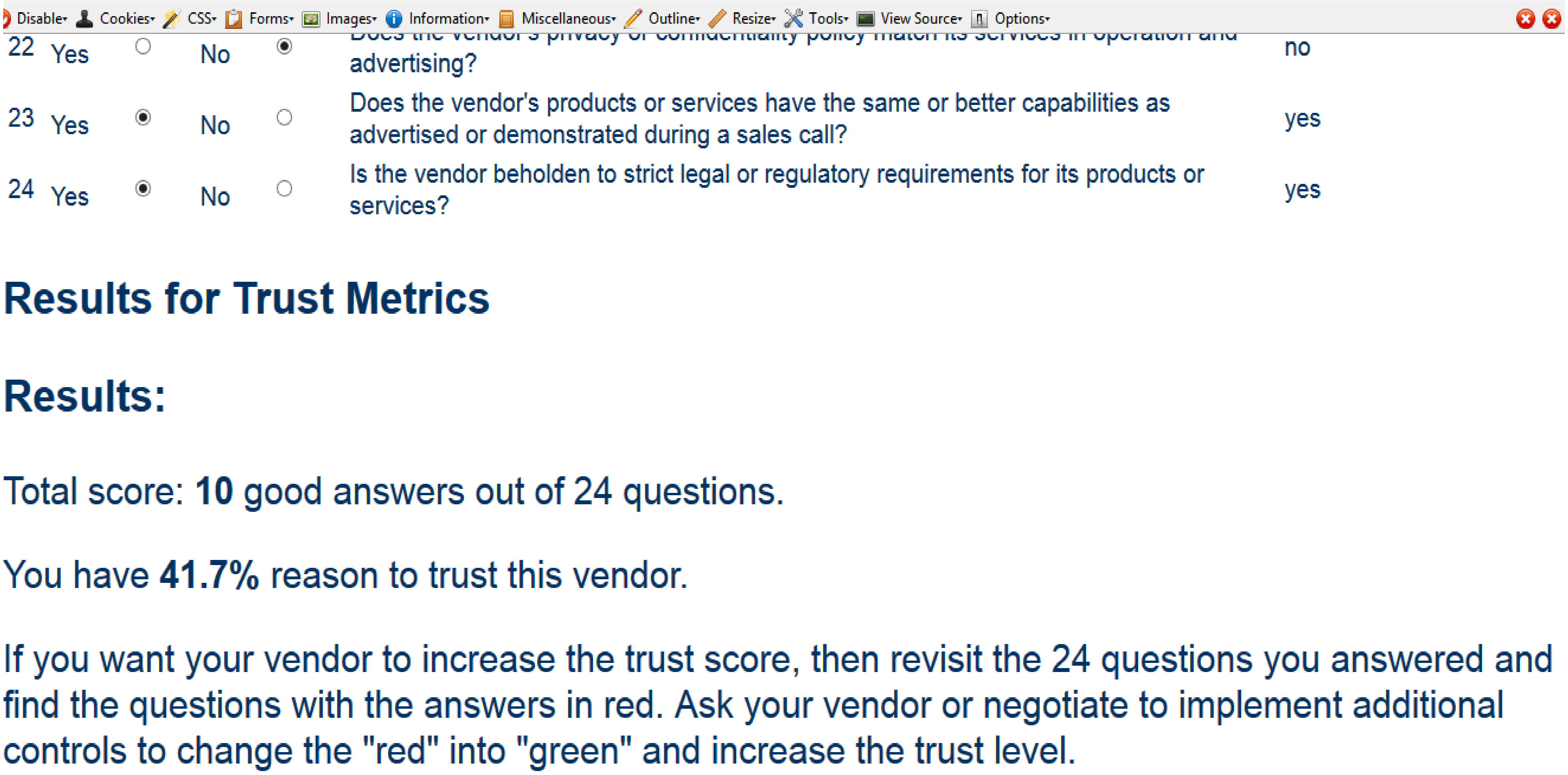
The Attack Surface Security Metric will be calculated after you clicked the Submit-button.

To recalculate after you made changes, remember to click the Submit button again.

Questions for Security Metrics

1	Yes	●	No	○	Does the vendor provides a private identification code for administrative requests, service change requests, billing contact, or support whether by phone, in person, or online?	+1 authentication
2	Yes	○	No	●	Does the vendor maintain a list of pre-selected persons on your staff with whom they will allow contact for administrative requests, service change requests, billing contact, or support?	+1 trust +2 weakness
3	Yes	●	No	○	Does the vendor require a secure key, password, or secret code for administrative requests, billing contact, or support?	+1 authentication
4	Yes	●	No	○	Does the vendor provide reasonable, strong authentication to connect with, access, or interact with data and an equally strong means for new account creation and password recovery?	+1 authentication

Trust questionnaire



22	Yes	○	No	●	Does the vendor's privacy or confidentiality policy match its services in operation and advertising?	no
23	Yes	●	No	○	Does the vendor's products or services have the same or better capabilities as advertised or demonstrated during a sales call?	yes
24	Yes	●	No	○	Is the vendor beholden to strict legal or regulatory requirements for its products or services?	yes

Results for Trust Metrics

Results:

Total score: **10** good answers out of 24 questions.

You have **41.7%** reason to trust this vendor.

If you want your vendor to increase the trust score, then revisit the 24 questions you answered and find the questions with the answers in red. Ask your vendor or negotiate to implement additional controls to change the "red" into "green" and increase the trust level.

Other developments

- OSSTMM version 4
  - Enhancements on V3
  - Trust analysis improved
  - Section added for testing web applications

"Excuse me, is this the Society for Asking Stupid Questions?"