performante pty ltd

ITSECURITYForum2013

The IT Security Challenge

#ITWebITSecurity

iTWeb events

An interactive discussion on how a business case should be constructed:

- Hettie Booysen, head: operational risk, IT Risk Standard Bank
- Lynette Botha, senior manager information security and compliance, MTN
- Vernon Fryer, chief technology security officer, Vodacom SA
- Shamalan Soobiah, former chief information officer, Standard Bank SA

The Communicator

- The vote only opens once you hear and see the countdown clock.
- When the vote is open, please press the number that corresponds with the option of your choice.

We are THE number 1 nation on the planet

1. Go bokka!

2. Go Proteas!

3. Go Bafana Bafana!

4. USA USA USA!

By your company having an interest in SIEM you mean?

❶ It helps me with my audit exceptions

43%

❷ I heard some BU's showing interest in SIEM

23%

❸ Everyone goes SIEM - I go SIEM

2%

❹ SIEM is the solution to most of my problems

32%

In order to have a business case I will:

❶ Have a workshop

❷ Have long nights

❸ Have a team working on it

❹ Let the partner write it

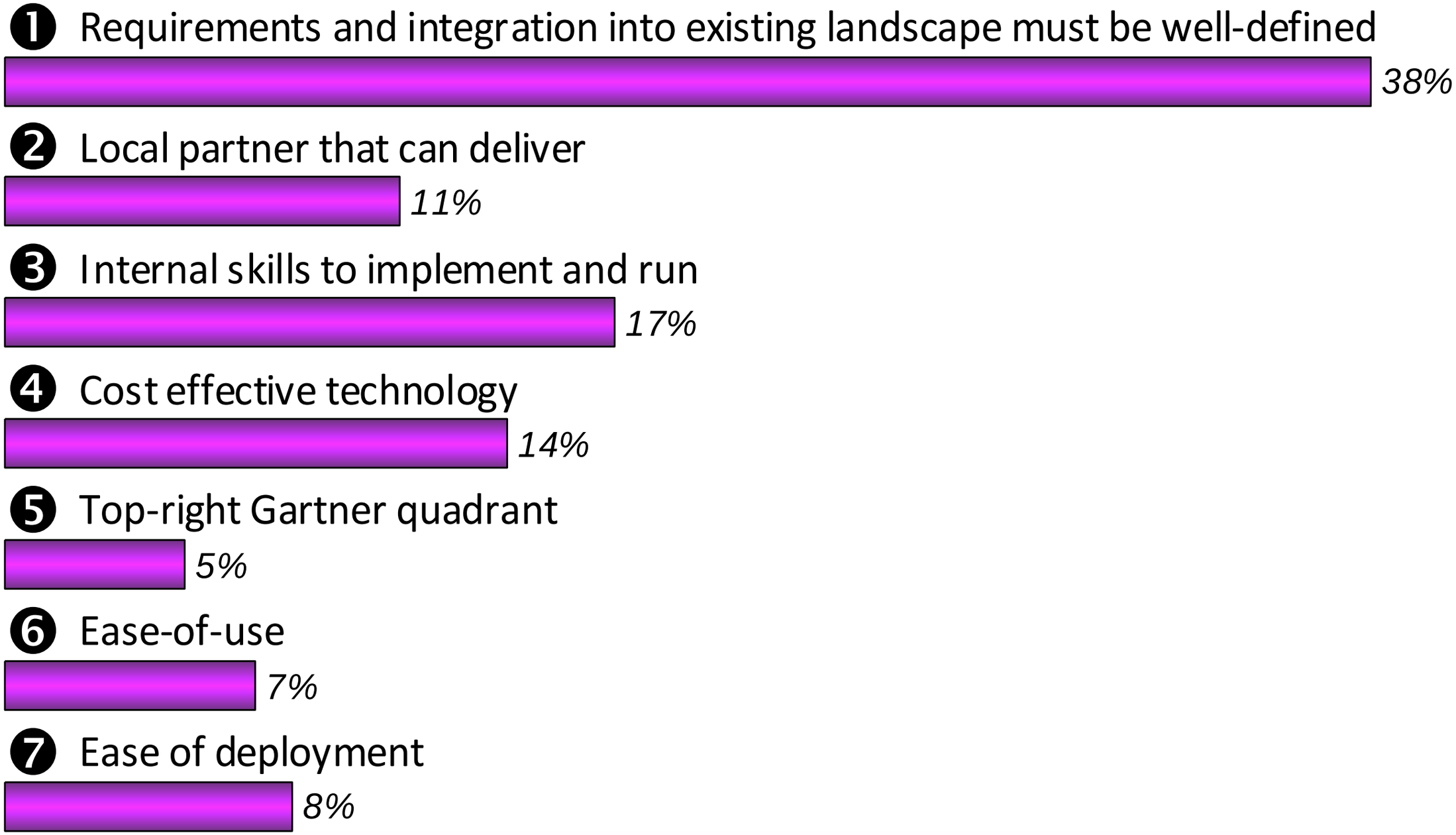
When building a business case the following is important to my organisation:

❶ To already have a budget

❷ To have executive buy-in

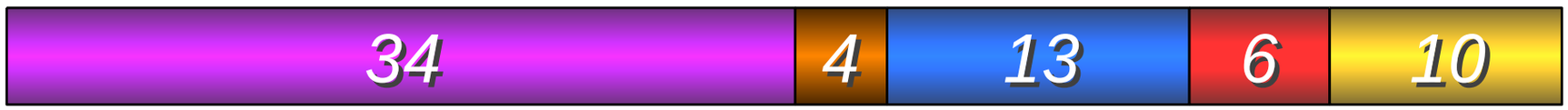
❸ To base it on negative past experience

When I choose the right technology the following two are the most important:



When I technically scope the project I usually involve **(Order of importance):**

❶ CIO/CISO

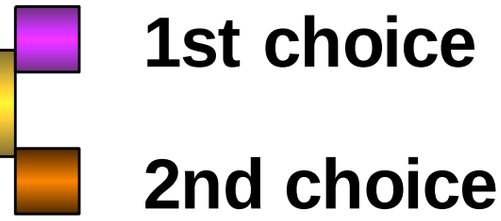


❷ Security architect

❸ Security operations

❹ Fraud and Forensics

❺ Auditors/ Risk and Compliance



Once choosing a SIEM technology:

❶ I'll do everything internally with my existing resources.

18%

❷ I'll partner and make sure there is skills transfer.

73%

❸ I'll outsource it completely.

9%

In my organisation the MAIN beneficiary for a SIEM project is:

❶ Risk and Compliance

❷ Business & Board of Directors

❸ Technical management team

❹ Security and CIRT response team

To show success on a project:

❶ I go Big Bang. This is the only way we get traction here.

2%

❷ I go big. This way I do not need to do multiple convincing and internal selling.

8%

❸ I go phased approach. Step by step. Starting small and then going big.

87%

❹ I start small. Then at least it is not my neck on the line if it fails.

3%

I research a SIEM technology and eventually decide based on:

❶ What my peers do

9%

❷ What "Group" recommends

21%

❸ Go with the flavour of the day

0%

❹ Gartner/ Industry Reference sites

34%

❺ RFI

36%

In my organisation SIEM is owned by:

1. IT Security — *52%*
2. Business — *7%*
3. IT Operations — *17%*
4. Forensics & Fraud — *1%*
5. Risk and compliance — *22%*
6. Auditors — *1%*

When I decide to motivate for SIEM I:

❶ Consult with Risk/ take Legislation into consideration.

❷ Use known sales tactics that are applicable to my company.

❸ Lobby with all parties involved beforehand.

❹ Learn from other organisations how they did it and apply exactly the same.

When I deploy SIEM a project plan agreed and signed by all parties:

❶ Is always prepared. That's the ONLY way!

❷ It is partial. We leave 20% for future and unknown.

❸ It is a 50-50 plan. Anyway it is a massive project.

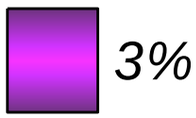
❹ Plan? You must be kidding me!

When I deploy SIEM I report on progress to:

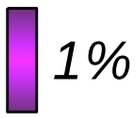
❶ My manager

❷ Steering committee

❸ No need to report. It is internal anyway.



❹ How should I know?



To guarantee success of the SIEM project I will:

❶ Set KPA/ KPI measurements.

54%

❷ Set reports fitting all levels.

11%

❸ Keep business constantly engaged.

19%

❹ Automate SIEM.

16%

A SIEM project is finished when:

❶ Budget is over.

4%

❷ Business is engaged.

21%

❸ Response Team (CIRT) is fully operational.

67%

❹ Technical stuff is installed.

8%

Who should run the SIEM project?

❶ Me! Only I can deliver the best project.

4%

❷ A project manager or project office.

61%

❸ Risk and compliance.

17%

❹ Affected Business Units.

18%

Is Security Operations Centre (SOC) part of my project?

❶ Never! Who needs one

4%

❷ Absolutely!

63%

❸ Only once SIEM is implemented

28%

❹ Only once we have our first major incident

5%

Business Case process to completion

1. Client expresses interest in SIEM
2. Initial workshop to gauge interest in solution – showcase approach to SIEM implementation
3. Identify budget and C-level engagement
4. Determine whether compliance driven or fraud driven
5. Determine competitors pitching
6. Determine the key players within customer and their respective roles esp. main driver
7. Scope initial solution technically
8. Workshop proposal with customer and refine solution
9. Prepare draft BOM with technical solution
10. Pitch solution to key players.

Business Case process to completion

11. Make refinements and submit
12. Begin process to hire/train identified resources
13. Build pilot/POC approach with key players/internal drivers
14. Target fraud and “pain” areas within the business units
15. Build targeted approach to show ROI to the above BU’s
16. Build use cases with key players and BU’s
17. Implement pilot/POC and use cases
18. Build presentation for C-Level board with key player
19. Present findings (non – threatening) and raise awareness internally of value of solution
20. Place PO!

Business Case process to completion

21. Define support team
22. Define support processes and compile support documentation
23. Pick team members and place team within organisation
24. Place infrastructure orders
25. Roll-out necessary hardware and Connectors
26. Build agreed upon Use Cases
27. Commence main SIEM deployment
28. Initiate project management meetings
29. Generate reports for business units – show value

Questions?

Thank you