dnevi slovenske informatike

"Nove razmere in priložnosti v informatiki kot posledica družbenih sprememb"

Kongresni center Grand hotel BernardinPortorož
Slovenija | 18. - 20. april 2011

18. konferenca
Dnevi slovenske informatike

BREZ ORODJA SIEM SO VARNOSTNI SISTEMI KOT SLEPE KURE

Matej Saksida, mag. var.

s&t

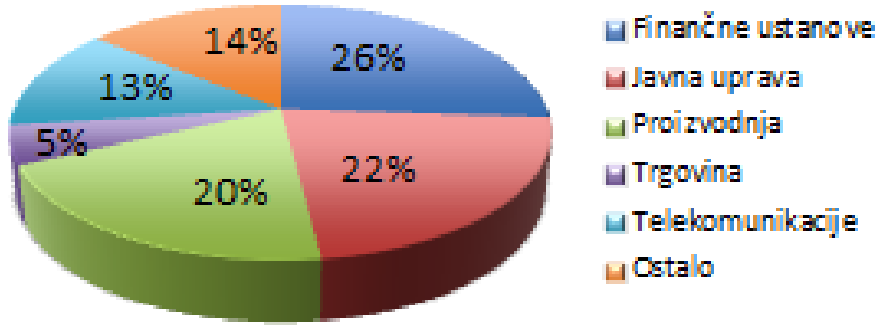
19. 04. 2011

S&T Slovenija d.d. v številkah

Hitra dejstva

- 42 mio € letnega prometa v 2010
- 229 zaposlenih
- Čez 150 certificiranih strokovnjakov
- Več kot 1000 različnih certifikatov
- Certifikat Družini prijazno podjetje
- Certifikat ISO/IEC 27001:2005

Delež prodaje po industrijah 2010



Strateška partnerstva

ORACLE, hp invent, EMC², SAP, IBM, CISCO, Microsoft, INFOR

Namen predavanja

- klasični varnostni sistemi niso kos sodobnim varnostnim izzivom
- orodja SIEM lahko dejansko pripomorejo k večji varnosti
- orodja SIEM so lahko učinkovita le, če so postavljeni temelji varnosti

Dongfan "Greg" Chung, Boeing Corporation

- 30-let vohunjenja
- 300k dokumentov
- 15-let zapora

Vir: http://goo.gl/GcHqB

Nekaj dejstev o notranjih napadalcih

- 59% zaposlenih odnaša podatke
- 87% je privilegiranih uporabnikov
- 67% bivših zaposlenih zlorabi podatke
- notranji : zunanji = 48% : 52% (+26%)
- notranji so nevarnejši (!)

Kriminalce zanimajo ljudje, ne tehnologija

- pridobljeni podatki o sistemu SecurID
- napad je bil izvršen nad zaposlenimi
- priponka v e-sporočilu je bila okužena

RSA®

The (un) Security Division of EMC

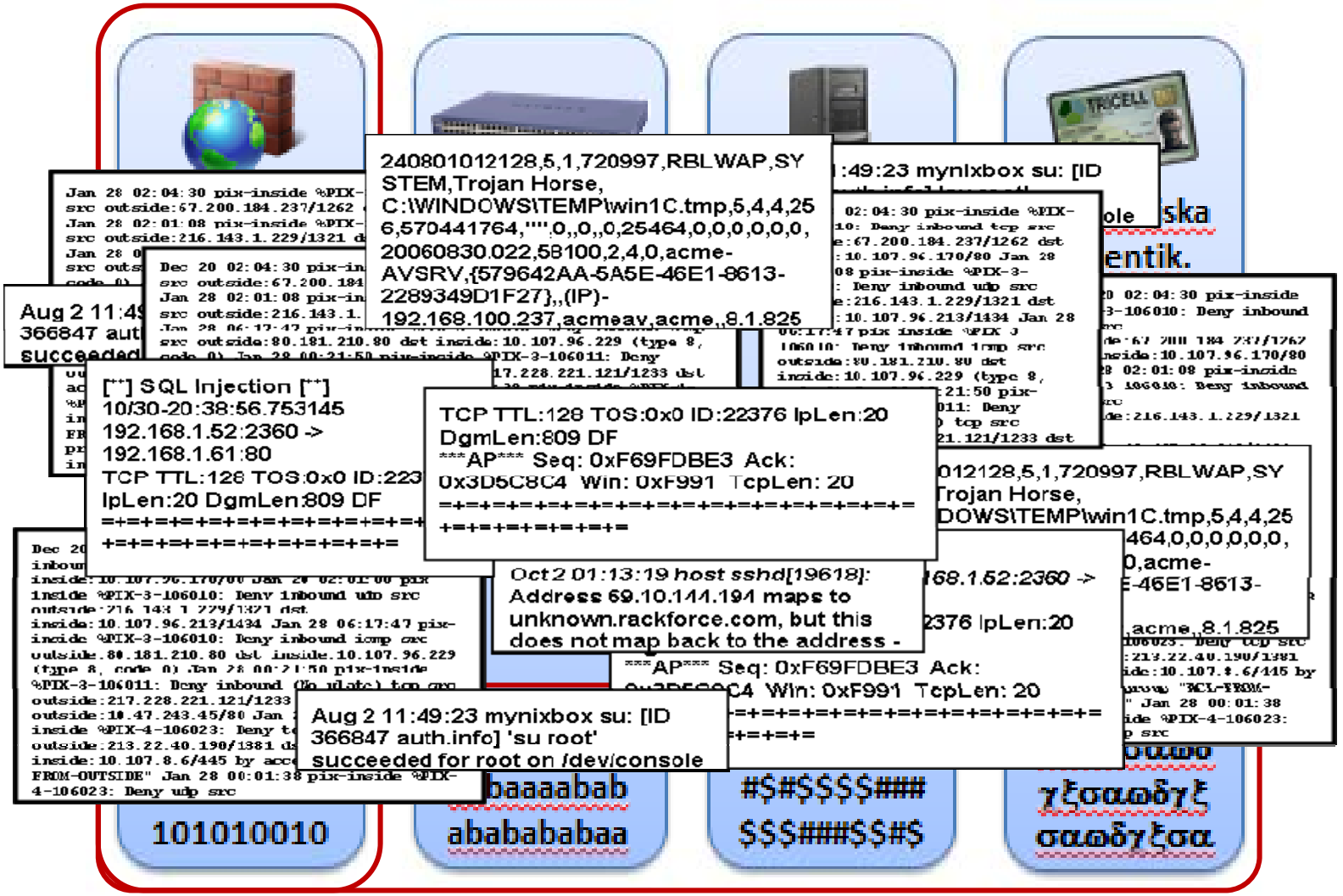
Vir: http://goo.gl/DU5pT

Varovanje informacij je vse bolj odvisno od zaposlenih!

- 28% napadov je usmerjenih v zaposlene
- napadi na zaposlene naraščajo (+16%)
- e-pošta in socialna omrežja
- napade je težko razkriti

Varnostni sistemi niso večni…

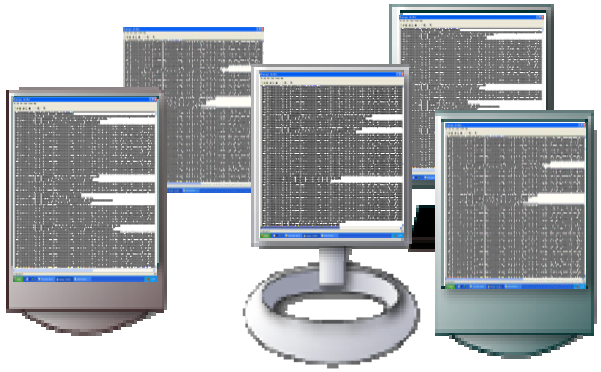
Zakaj varnostni sistemi ne nudijo varnosti?



Trije pristopi k zagotavljanju večje varnosti

Ročen pristop

Polavtomatiziran pristop

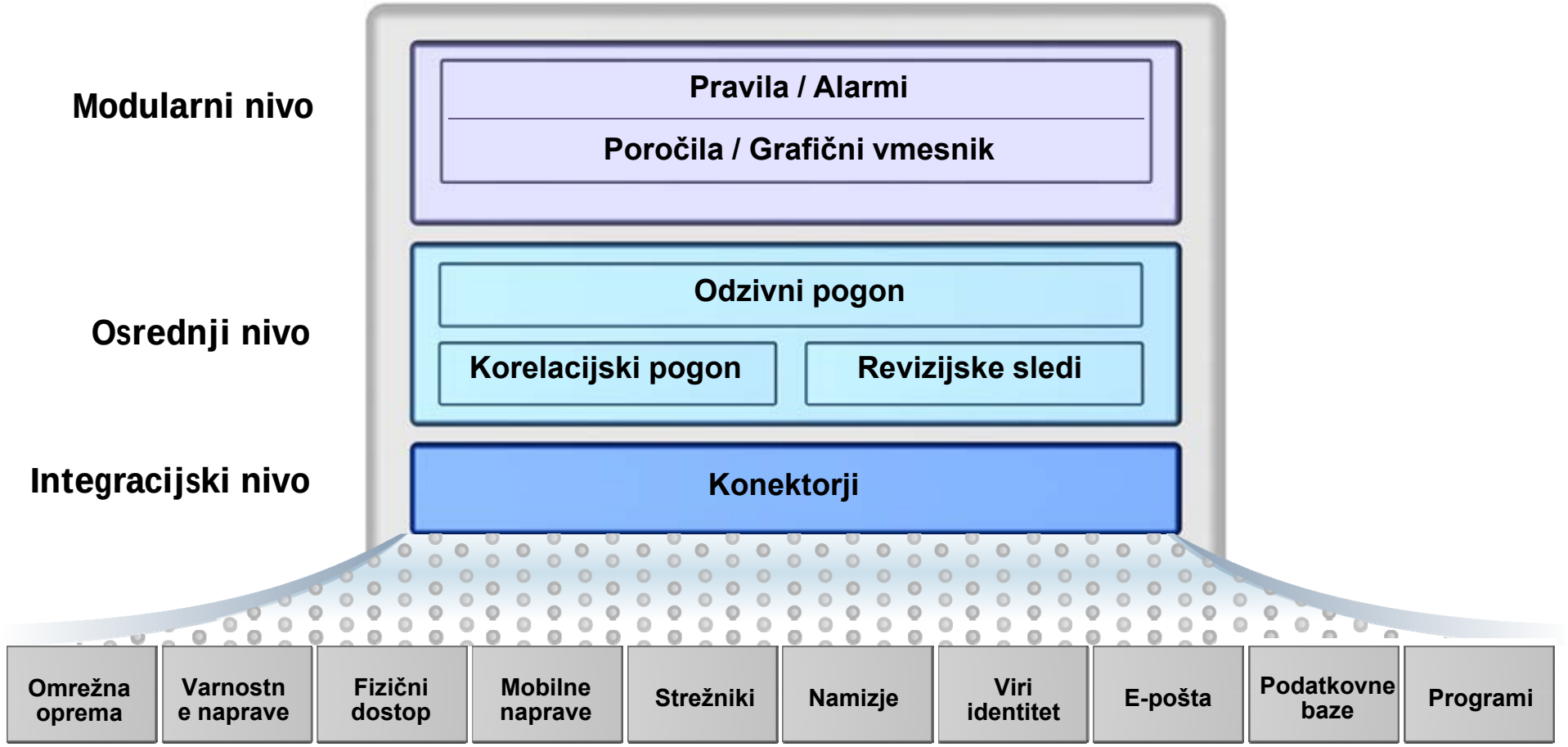


Avtomatiziran pristop

SIEM

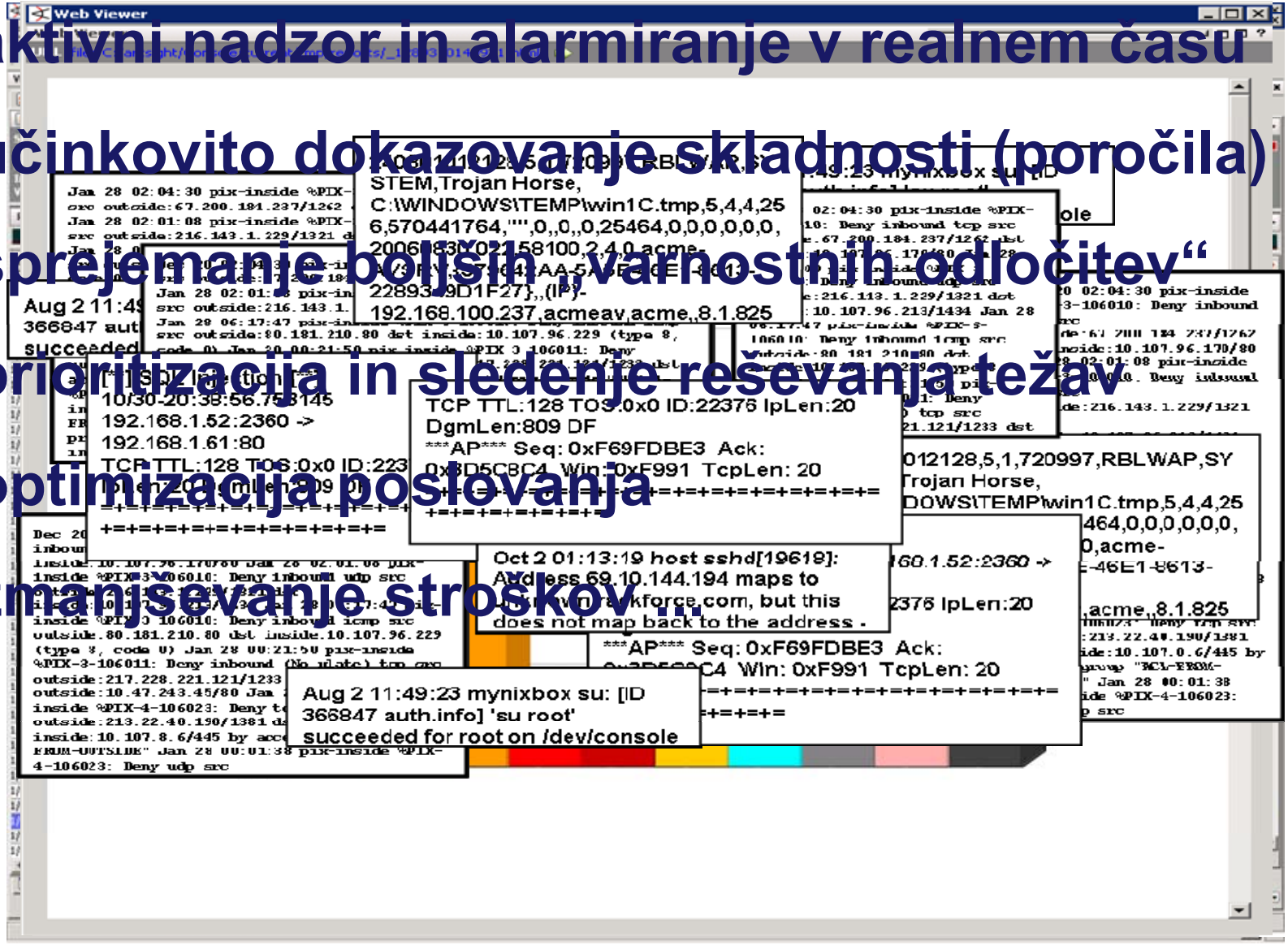
Ključne komponente orodij SIEM

Orodja SIEM zbirajo, shranjujejo, povezujejo in analizirajo dnevniške zapise varnostnih sistemov.



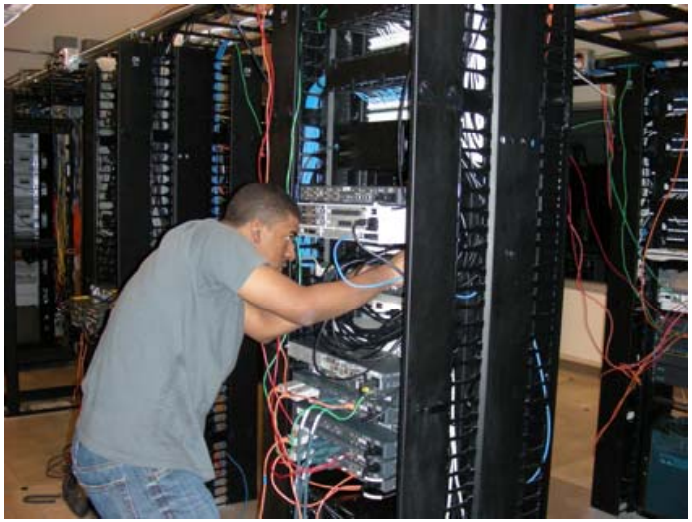
Dodane vrednosti orodji SIEM

- aktivni nadzor in alarmiranje v realnem času
- učinkovito dokazovanje skladnosti (poročila)
- sprejemanje boljših varnostnih odločitev“
- prioritizacija in sledenje reševanja težav
- optimizacija poslovanja
- zmanjševanje stroškov ...



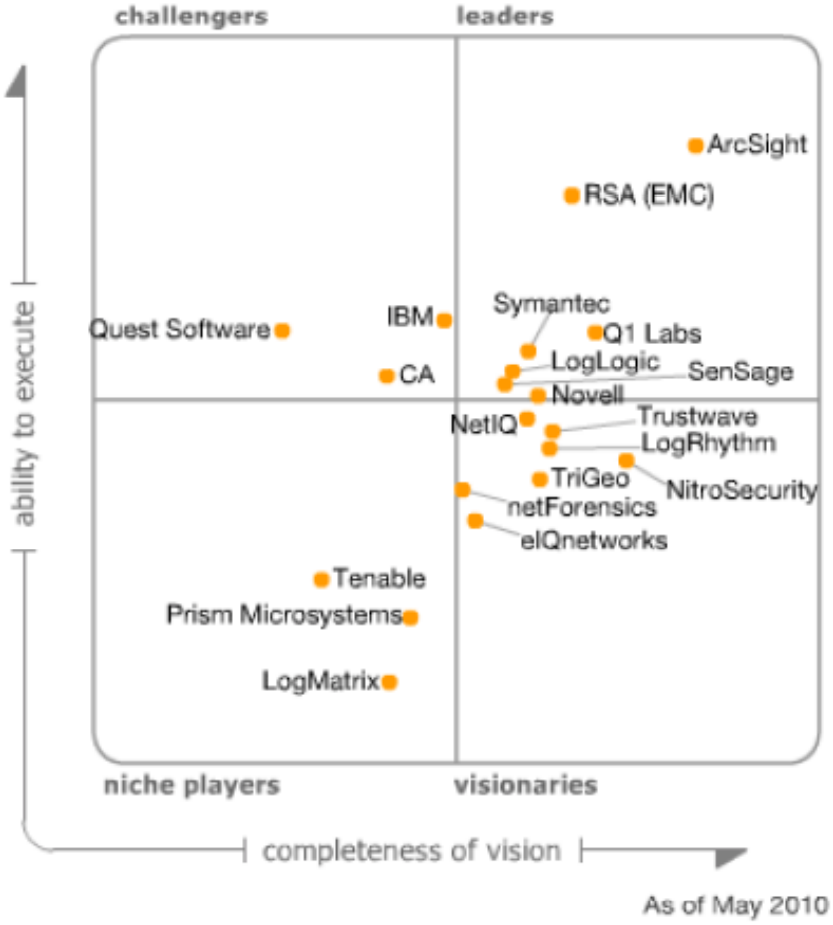
Kako postaviti sistem SIEM v praksi?

- Ugotovitev namena
- Določitev obsega
- Postavitev pilotnega projekta
- Priprava rešitve
- Implementacija
- Izobraževanje
- Podpora



Katera rešitev SIEM je najboljša?

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (May 2010)

Hvala za vašo pozornost!

Vprašanja in diskusija

matej.saksida@snt-world.com
www.snt.si