eTrust™ Network Forensics

Visualize, Uncover, Investigate

Ivan Masný, CISM
EMM, s.r.o.
31.5.2005

EMM®

Agenda

- Úvod do problematiky
- Možnosti *e*Trust Network Forensics
- Postavenie *e*Trust Network Forensics v *e*Trust riešeniach
- Novinky v *e*Trust Network Forensics r8
- Zhrnutie
- Praktická ukážka

© 2004 Computer Associates International, Inc. (CA). All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

Úvod do problematiky

© 2004 Computer Associates International, Inc. (CA). All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

Čo je to “forenzný“?

- Forenzný – súdny, týkajúci sa práva alebo súvisiaci so súdom
  - forenzné vedy
  - forenzné služby
  - forenzný audit
  - forenzné analýzy
  - forenzná psychológia
- Forenzní vedci preverujú a vysvetľujú fakty a dôkazy v právnych sporoch a poskytujú súdom alebo svojim klientom znalecké posudky o svojich zisteniach.

(zdroj: Klíma, Sičáková, Karchňák: Kontrola a jej úlohy v boji s korupciou, CPHR – Transparency International Slovensko)

© 2004 Computer Associates International, Inc. (CA). All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

Potrebujeme to?

- Central and Eastern Europe Information Society Benchmarking - Summary Report September 2004
  - 22% jednotlivcov a 40% spoločností s pripojením do Internetu malo v roku 2003 bezpečnostný problém v rámci ICT
  - 56% jednotlivcov a 68% spoločností s pripojením do Internetu v roku 2003 prijalo predbežné opatrenia v oblasti bezpečnosti ICT
  - najčastejšie prijaté opatrenia sú:
    - antivírová ochrana
    - firewall
    - zavedenie autentifikácie
  - Slovinsko – líder v prijatých opatreniach
    - 37% spoločností používa firewall
    - 12% spoločností používa šifrovanie
    - 23% spoločností autentifikáciu dokumentov
  - Slovensko – líder v off-site data backup (31% spoločností)

(zdroj: http://europa.eu.int/information_society/eeurope/2005/all_about/benchmarking/eeurope_plus_benchmark_report/index_en.htm)

© 2004 Computer Associates International, Inc. (CA). All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

Potrebujeme to?

- Stratégia informatizácie spoločnosti v podmienkach SR a Akčný plán, príloha 6 - Bezpečnosť a ochrana digitálneho prostredia
  - **analyzovať bezpečnostné problémy** súvisiace so zavádzaním postupov využívajúcich IKT a prevádzkou IKS a na základe získaných poznatkov navrhovať opatrenia (legislatívne, štandardizačné, organizačné, materiálne, finančné a i.), ktoré je potrebné na riešenie týchto problémov prijať na úrovni štátu
  - **zaistiť účinnú prevenciu a riešenie bezpečnostných incidentov**

(zdroj: www.telecom.gov.sk - Bezpečnosť informačných technológií (BIT), Výskumný ústav spojov, n. o.)

EMM®

© 2004 Computer Associates International, Inc. (CA). All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

Potrebujeme to?

- Akčný plán, bod 3.c - Integrácia informačnej bezpečnosti do IT transakcií
  - 3.c.1. Zdokonaliť celkovú bezpečnosť on-line transakcií
    - podporou certifikátov bezpečnosti, iniciovaných priemyslom prostredníctvom koordinácie úsilia a vzájomného uznania, zahrnujúc odbornú certifikáciu informačnej bezpečnosti
    - stimulovaním verejno-súkromnej spolupráce na zabezpečení spoľahlivosti informačných infraštruktúr (vrátane rozvoja **systémov včasného varovania**)
  - 3.c.2. Zabezpečiť školenia / vzdelávanie legislatívnych pracovníkov, súdneho personálu a priemyselných špecialistov v oblasti posilnenia práva, hi-tech kriminality a otázok bezpečnosti (ako je boj proti počítačovej kriminalite, zneužívaniu počítačov a pod.)
  - 3.c.3. Pripraviť sa na zapojenie SR do bezpečnostných štruktúr EÚ, a to najmä v súlade s programom vypracovaným skupinou “Digital Security Task Force”
  - 3.c.4. Zriadiť orgán (inštitúciu) pod gesciou splnomocnenca, ktorá bude riešiť problematiku tzv. „všeobecnej bezpečnosti“ IS, t.j. bezpečnosť IS, ktoré neobsahujú utajované skutočnosti

(zdroj: www.telecom.gov.sk - Bezpečnosť informačných technológií (BIT), Výskumný ústav spojov, n. o.)

© 2004 Computer Associates International, Inc. (CA). All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

Možnosti
*e*Trust Network Forensics

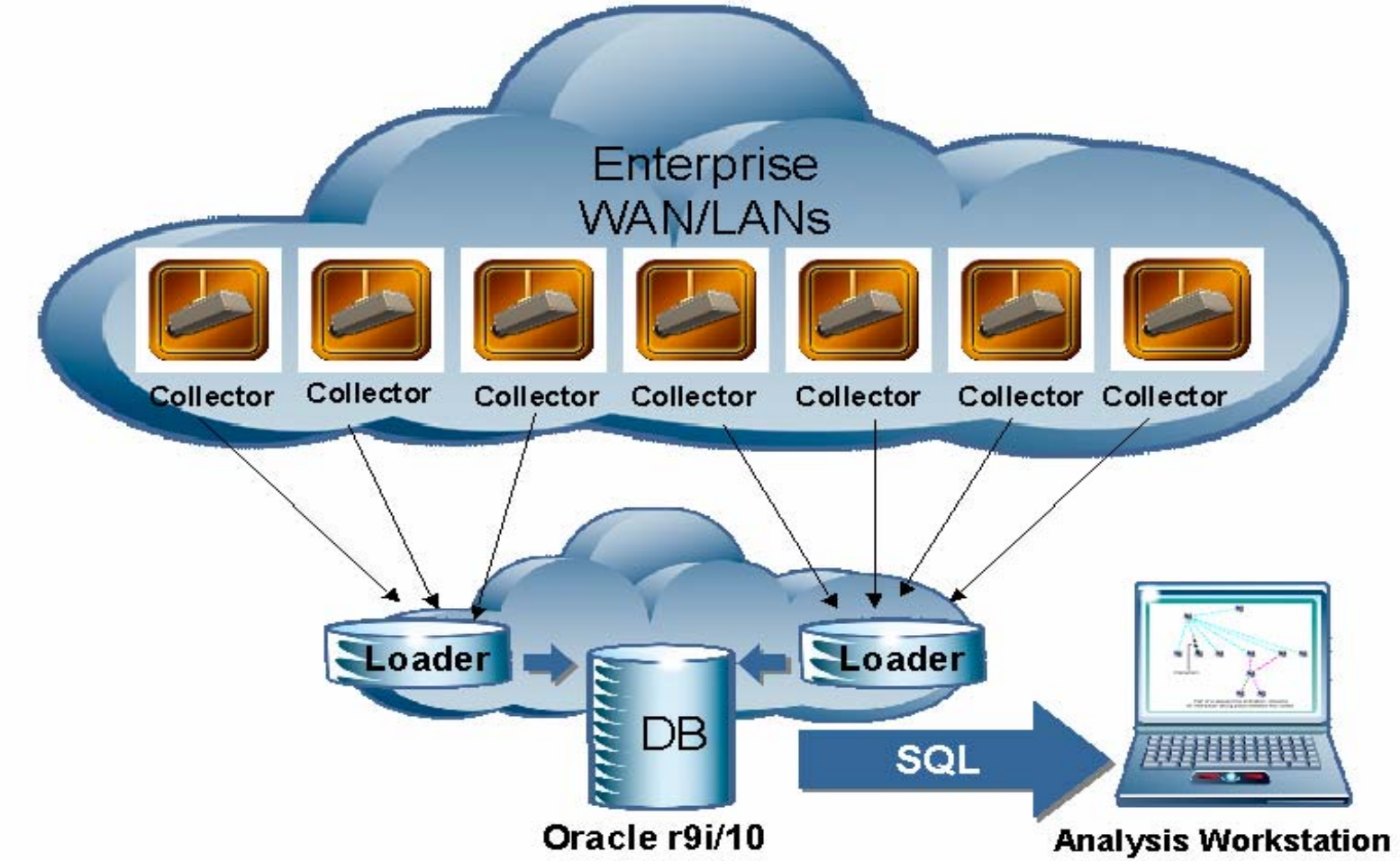
© 2004 Computer Associates International, Inc. (CA). All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

Čo vie riešiť

- Zbierať a analyzovať real-time sieťové dáta
- Zobrazovať sieťové aktivity
- Odkrývať anomálie v prenosoch dát
- Vyhľadávať bezpečnostné diery
- Zjednodušiť vyšetrovanie bezpečnostných incidentov
- Spracovať reporty
- Identifikovať zneužitia siete, krádeže dát a priestupky voči bezpečnostnej politike
- Analyzovať aj iné typy štruktúrovaných dát

© 2004 Computer Associates International, Inc. (CA). All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

Základná architektúra



EMM®

© 2004 Computer Associates International, Inc. (CA). All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

Komponenty

- *e*Trust Network Forensics Collector
- *e*Trust Network Forensics Context
- *e*Trust Network Forensics Forwarder a eTrust Network Forensics Loader
- *e*Trust Network Forensics Data Manager
- *e*Trust Network Forensics Analyzer
- *e*Trust Network Forensics Database
- *e*Trust Network Forensics Enterprise Messaging

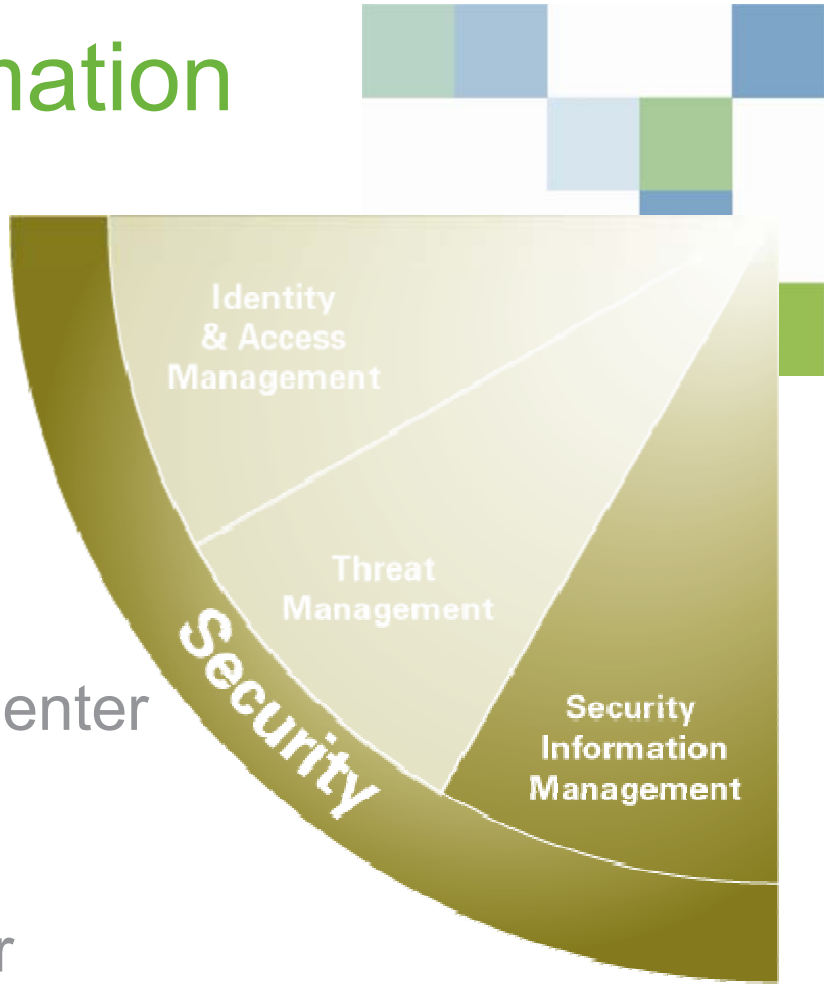
© 2004 Computer Associates International, Inc. (CA). All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

Postavenie eTrust™ Network Forensics v eTrust riešeniach

© 2004 Computer Associates International, Inc. (CA). All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

eTrust™ Security Information Management Solutions

- Kľúčové riešenia
  - eTrust™ 20/20
  - eTrust™ Network Forensics
  - eTrust™ Security Command Center
- Doplnkové technológie
  - eTrust™ Vulnerability Manager



EMM®

© 2004 Computer Associates International, Inc. (CA). All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

CAweek 2005
Holiday Inn, Bratislava 31.5. – 1.6. 2005

Novinky v *e*Trust Network Forensics r8

© 2004 Computer Associates International, Inc. (CA). All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

Nové vlastnosti

- Databáza Ingres r3 súčasťou *e*Trust Network Forensics Single Platform inštalácie
- HW zariadenie pre Collector a Loader
- Zefektívnenie Single Platform inštalácie
- Podpora Oracle r9 a r10
- Zvýšenie dostupnosti systému
- Zlepšenie manažmentu dát

EMM®

© 2004 Computer Associates International, Inc. (CA). All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

Zhrnutie

- *e*Trust Network Forensics
  - Zvyšuje ochranu aktív organizácie
  - Zlepšuje možnosti identifikácie bezpečnostných incidentov, zneužitia siete, krádeže dát a porušenie bezpečnostných politík
  - Sprehľadňuje sieťové aktivity
  - Odkrýva anomálie v sieťovej prevádzke
  - Zjednodušuje vyšetrovanie a dokumentovanie bezpečnostných incidentov
  - Zefektívňuje analýzu dát
  - Pomáha znižovať riziká
  - Podporuje naplnenie zhody s požiadavkami regulačných a legislatívnych orgánov

© 2004 Computer Associates International, Inc. (CA). All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

Praktická ukážka

© 2004 Computer Associates International, Inc. (CA). All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

eTrust™ Network Forensics

Visualize, Uncover, Investigate

Ivan Masný, CISM
EMM, s.r.o.
31.5.2005

EMM®