

Log management

Strumenti enterprise e soluzione freeware a confronto

DEFT Linux
Computer Forensics Live CD



Dott. Stefano Fratepietro
stefano@deftlinux.net



Creative Commons Attribution-Non opere derivate 2.5

Milano, 22 ottobre - Smau 2010
Fiera Milano city

Obiettivi del seminario

- Normativa del Garante Privacy per l'argomento
- Introduzione ai sistemi di log management
- Il quadrante di Gartner 2010
- Le offerte del mercato
- POC eseguiti

Dott. Stefano Fratepietro

- IT - Security specialist per il CSE Consorzio Servizi Bancari S.c.r.a.l
- Consulente di Informatica forense per tribunali, forze dell'ordine (Polizia Postale, Carabinieri e Guardia di Finanza) e privati
- Casi di importanza nazionale come Buongiorno! Vitaminic e Telecom Pirelli Ghioni
- DEFT Linux project manager

Garante privacy

La normativa di interesse

27 novembre 2008: misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema

<http://www.garanteprivacy.it/garante/doc.jsp?ID=1577499>

Garante privacy

La normativa di interesse

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di **completezza, inalterabilità** e possibilità di **verifica della loro integrità** adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a **sei mesi**.

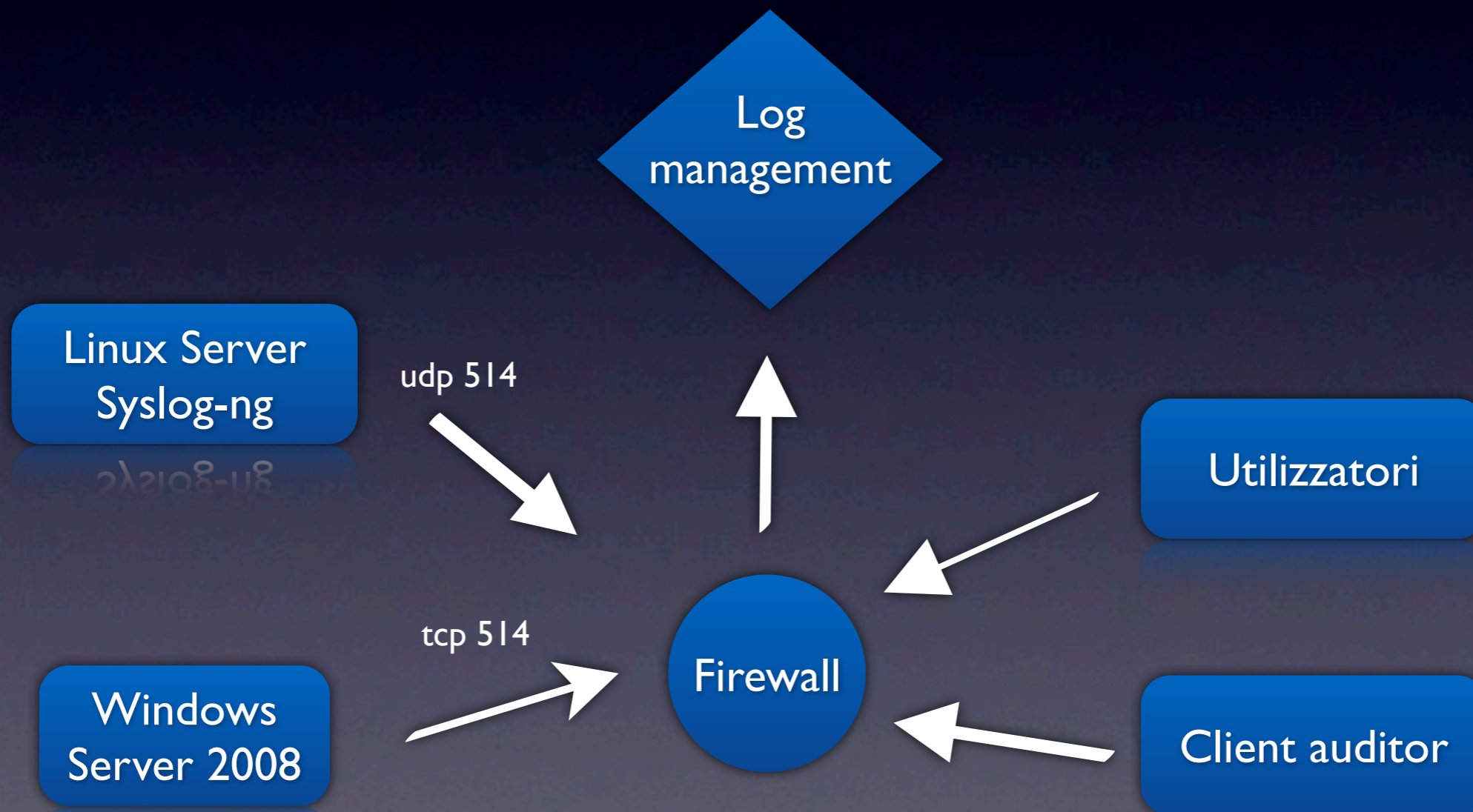
Come va interpretata la caratteristica di inalterabilità dei log?

Caratteristiche di mantenimento dell'integrità dei dati raccolti dai sistemi di log sono in genere disponibili nei più diffusi sistemi operativi, o possono esservi agevolmente integrate con apposito software. Il requisito può essere ragionevolmente soddisfatto con la strumentazione software in dotazione, nei casi più semplici, e con l'eventuale esportazione periodica dei dati di log su supporti di memorizzazione non riscrivibili. In casi più complessi i titolari potranno ritenere di adottare sistemi più sofisticati, quali i log server centralizzati e "certificati".

Definizione

Sistema in grado di ricevere, immagazzinare ed organizzare informazioni provenienti da sistemi o applicativi e all'occorrenza rendere accessibili le informazioni memorizzate mediante ricerche per evento, sistema o utente

Architettura tipo



Log management questo sconosciuto...

- Possibilità di ricevere in tempo reale log via syslogd (udp/tcp 514)
- Ove non supportato il syslog, elaborazione di soluzioni alternative come sftp o scp
- Supporto nativo ai principali sistemi in commercio con possibilità di creazione di custom parser
- Meccanismi di controllo di integrità del dato raccolto

Log management

questo sconosciuto...

- Meccanismi adeguati per lo svecchiamento dei log raccolti
- Esecuzione di ricerche di eventi, possibilmente in tempo reale, anche sui log svecchiati
- Possibilità di implementare soluzioni in HA - alta affidabilità
- Documentazione e supporto tecnico adeguato

Principali problematiche

- Features dichiarate inesistenti o di dubbia implementazione
- Parser ufficiali parzialmente funzionanti
- Soluzione derivante da soluzioni già esistenti e magari ancora in commercio, rivendute con un nuovo brand
- Appliance Linux based / Syslog based vulnerabili e instabili
- Supporto tecnico molto lento, quasi inesistente

Client SNARE

Event log agent multi piattaforma

Converte e o invia in formato testuale tutti i log che nativamente non sono inviati in formato syslog

The screenshot shows a web browser window titled "Intersect Alliance - Information Technology Security - Microsoft Internet Explorer". The address bar shows "http://localhost:6161/eventlog". The page header features the "INTERSECT ALLIANCE" logo and the text "SNARE for Windows". Below the header, there is a sidebar on the left with navigation links such as "Latest Events", "Network Configuration", "Remote Control Configuration", "Objectives Configuration", "View Audit Service Status", "Apply the Latest Audit Configuration", "Local Users", "Domain Users", "Local Group Members", "Domain Group Members", and "Registry Dump". The main content area is titled "Current Events" and displays a table with the following columns: Date, System, Event Count, EventID, Source, UserName, UserType, ReturnCode, and Strings.

Date	System	Event Count	EventID	Source	UserName	UserType	ReturnCode	Strings
Tue Aug 08 11:41:03 2006	flash.InterSect.local	92	643 (Account Management)	Security	SYSTEM	User	Success Audit	Domain Policy Changed: Password Policy modified Domain Name: INTERSECT Domain ID: %{\$S-1-5-21-4225700407-1522440742-3458925109} Caller User Name: FLASH\$ Caller Domain: INTERSECT Caller Logon ID: (0x0,0x3E7) Privileges: - Changed Attributes: Min. Password Age: - Max. Password Age: - Force Logoff: - Lockout Threshold: - Lockout Observation Window: - Lockout Duration: - Password Properties: - Min. Password Length: 6 Password History Length: - Machine Account Quota: - Mixed Domain Mode: - Domain Behavior Version: - OEM Information: -
Tue Aug 08 11:41:03 2006	flash.InterSect.local	91	1704 (None)	SecCli	Unknown User	N/A	Information	Security policy in the Group policy objects has been applied successfully.
Tue Aug 08 11:41:00 2006	flash.InterSect.local	90	538 (Logon/Logoff)	Security	SYSTEM	User	Success Audit	User Logoff: User Name: FLASH\$ Domain: INTERSECT Logon ID: (0x0,0x939E2) Logon Type: 3
Tue Aug 08 11:40:48 2006	flash.InterSect.local	89	538 (Logon/Logoff)	Security	SYSTEM	User	Success Audit	User Logoff: User Name: FLASH\$ Domain: INTERSECT Logon ID: (0x0,0x93938) Logon Type: 3

Client SNARE

Multi piattaforma

- Windows
- Linux
- Unix
- Aix
- Solaris

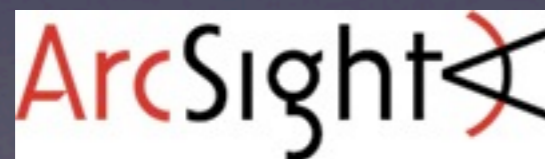
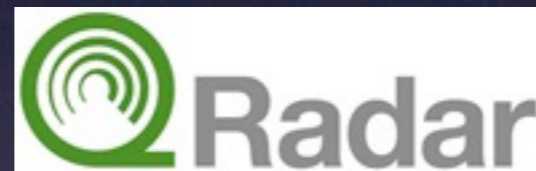


- ISA
- Microsoft IIS
- Lotus Notes
- Apache
- Squid

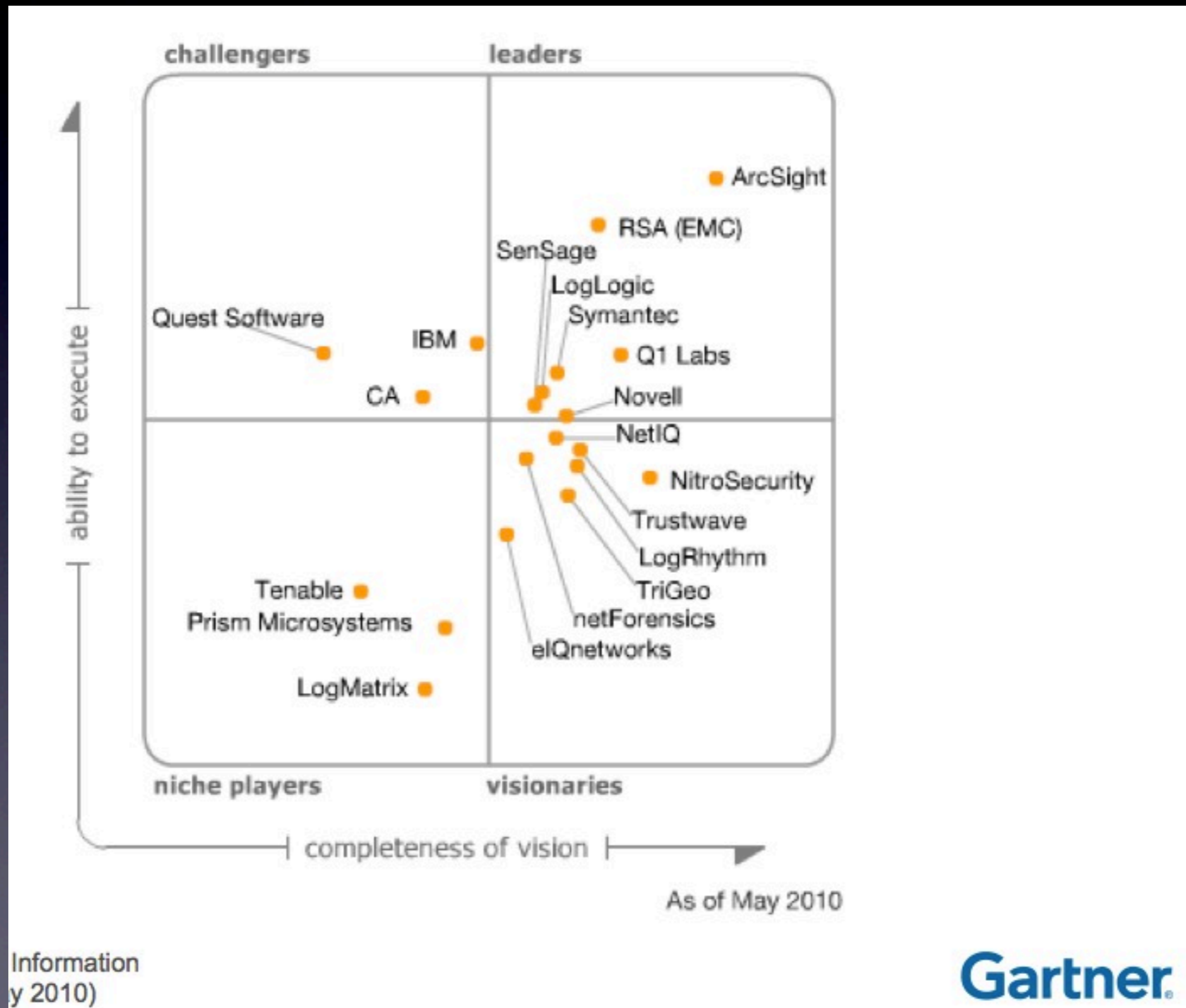
Sistemi di Log Management freeware

- Linux - Syslogng
- Splunk (fino ad un massimo di 500 mb al giorno)
- QI radar FE (virtual appliance)
- Molte altre soluzioni commerciali che permettono di testare il loro prodotto con limitazioni alla soluzione

Principali protagonisti



Il magico quadrante

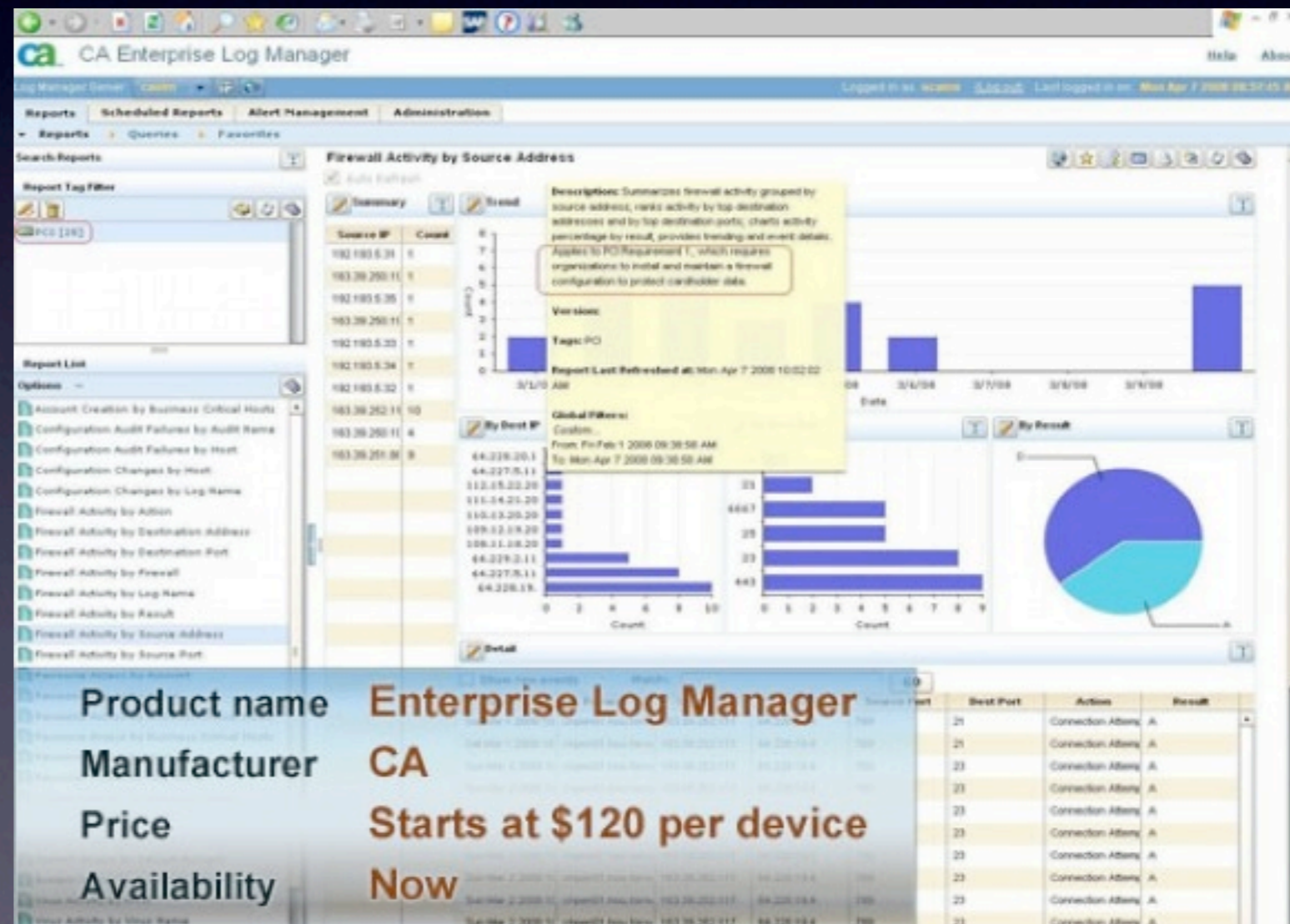


POC e sistemi usati per i test

- Cisco
- IBM Aix e RACF
- Linux
- Windows
- Oracle e DB2

Prova su strada CA E. Log Manager - PRO

- Supporto RACF nativo
- Supporto ai principali vendor leader del mercato
- Possibilità di effettuare ricerche anche sui log svecchiati e spostati in altro storage



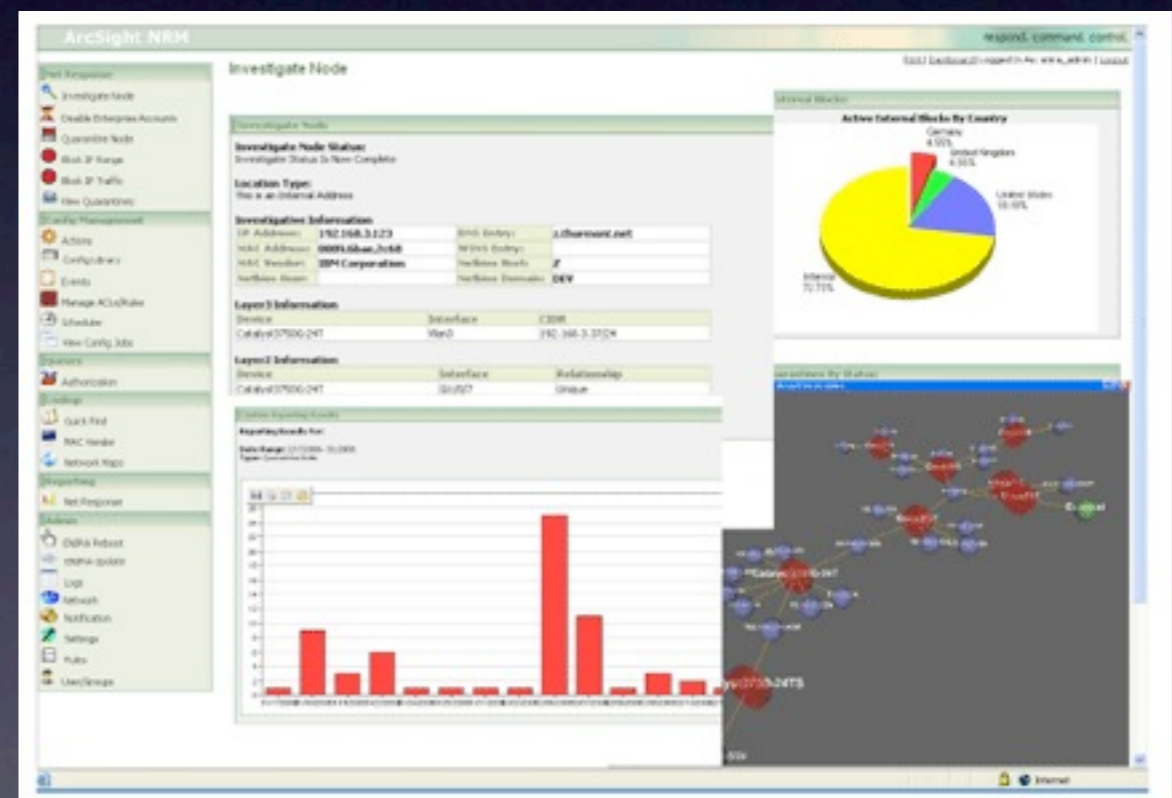
Prova su strada

CA E. Log Manager - CONTRO

- Interfaccia di management in Macromedia Flash funzionante solo su I.E
- Poco intuitivo e di difficile comprensione
- Soluzione onerosa in termini di hardware
- Al momento delle prove si sono riscontrate forti instabilità dell'appliance con frequenti crash

Prova su strada Arcsight - PRO

- Stabilità
- Supporto completo su tutti i principali vendor
- Potente motore di ricerca di eventi e generatore report
- Supporto ed assistenza competente e preparato
- Compressione dei log archiviati 10:1

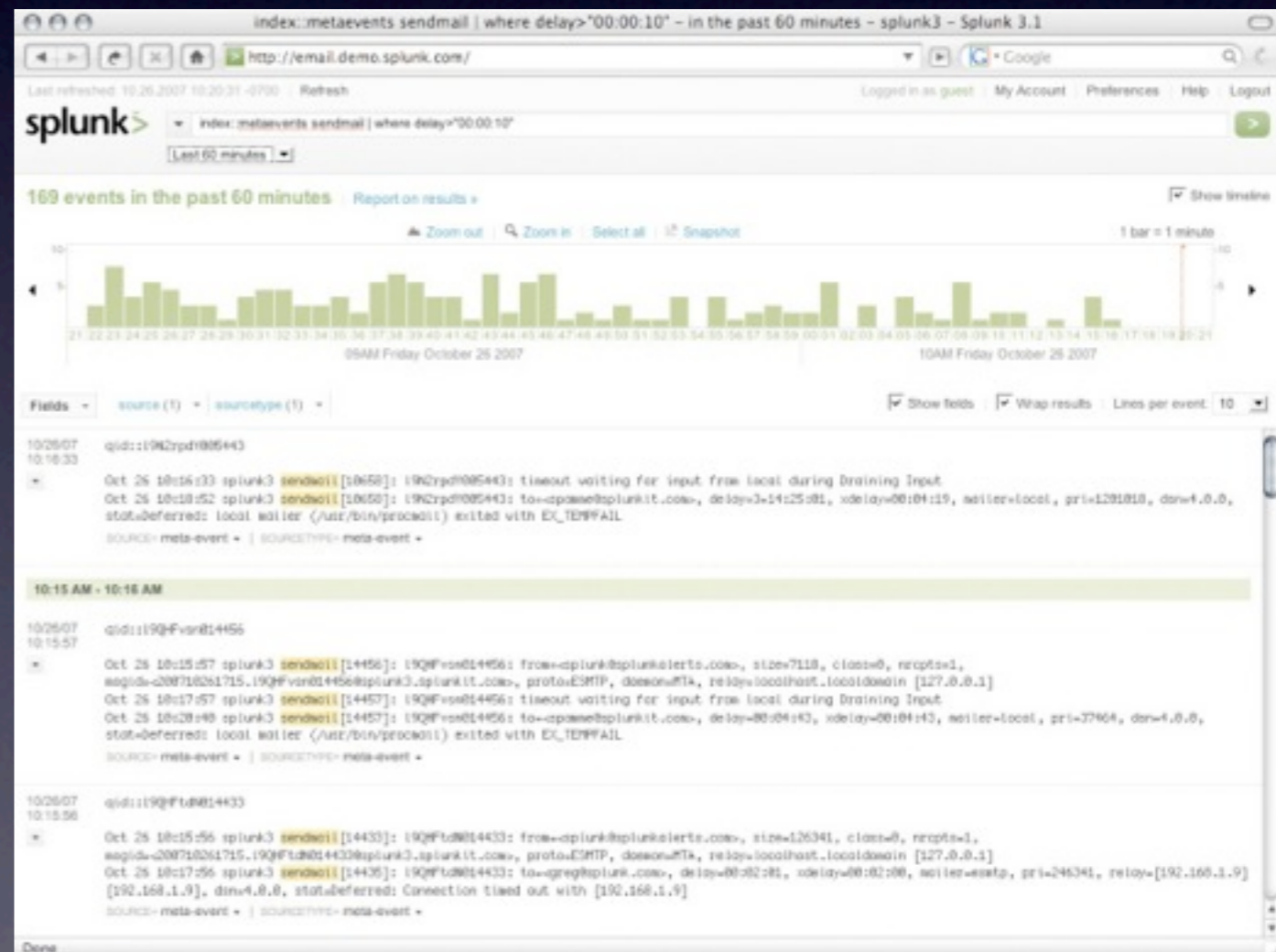


Prova su strada Arcsight - CONTRO

- Dai test fatti il sistema non è riuscito a interpretare correttamente i log RACF
- Soluzione onerosa sia in contesti economici che in contesti di hardware

Prova su strada Splunk - PRO

- Multi piattaforma
- Installazione immediata
- Potente linguaggio per la creazione dei parser
- Ottima compressione dei log ricevuti
- Apps create da vendor o dalla community

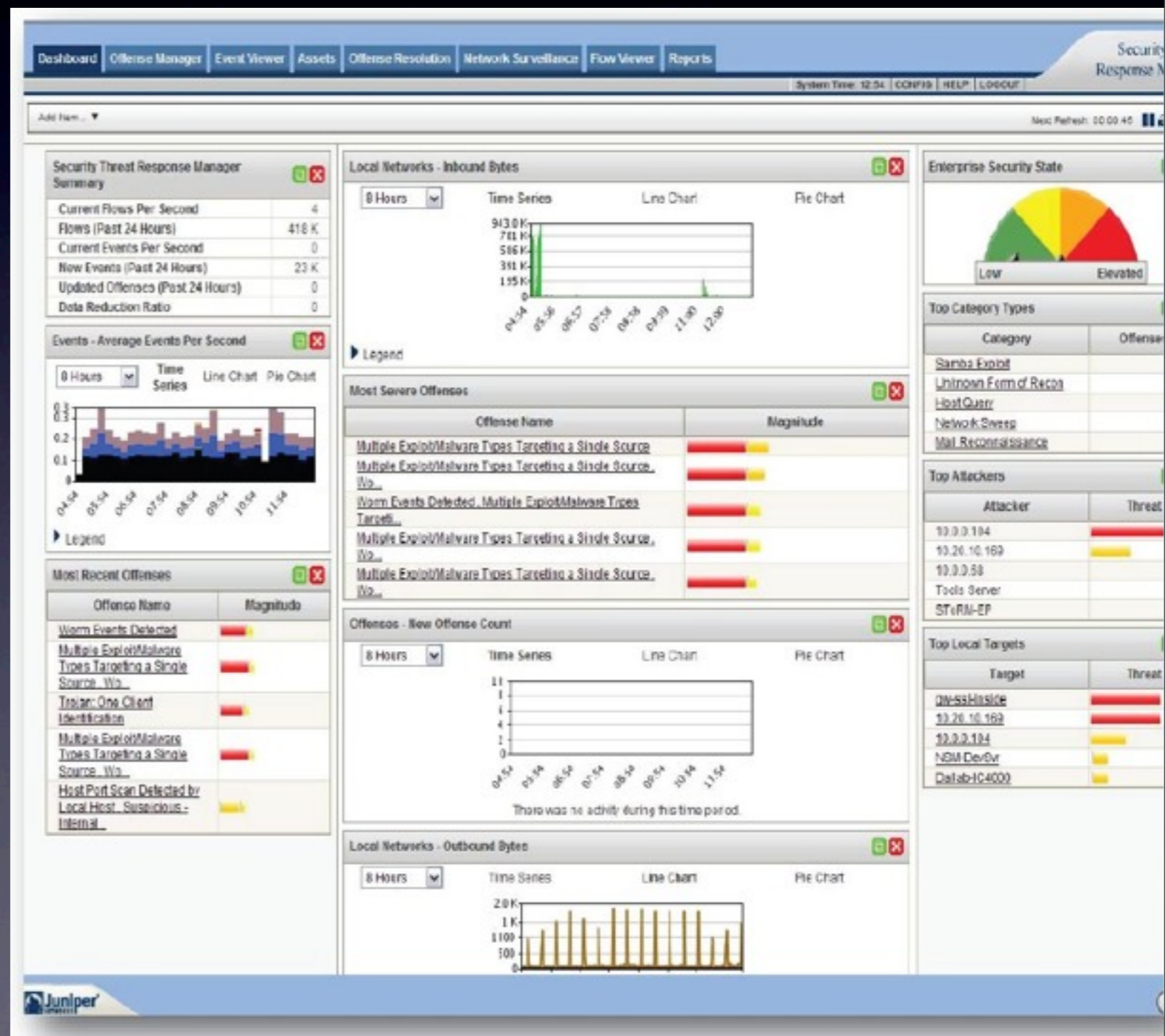


Prova su strada Splunk - Contro

- Acquisto di licenza basato su GB/giorno
- Non viene venduto alcun tipo di hardware
- Impossibilità di interrogazione di log svecchiati su storage esterno
- Non esiste supporto ufficiale per sistemi appartenenti al mondo Z di IBM

Prova su strada QI Radar - PRO

- Appliance hardware fornita dal vendor
- Visualizzazione di log in tempo reale con possibilità di eseguire filtri
- Parser già pronti per i principali vendor
- Supporto per il mondo IBM RACF e AIX



Prova su strada Q I Radar - Contro

- Creazione di custom parser complessa e scarsamente documentata
- Alcuni parser ufficiali non coprono completamente tutti gli eventi possibili
- Impossibilità di autenticare via ssh utenti ldap/tacas/radius
- Molte operazioni vanno eseguite da riga di comando e non da interfaccia grafica

Prova su strada Juniper strm - CONTRO

- Ultima release rimarchiata strm è la penultima delle release stabili rilasciate da QI Labs
- Hardware Juniper inferiore rispetto alla fornitura QI Labs
- Supporto tecnico/help desk quasi inesistente
 - Non è il core business di Juniper!
- Poche installazioni nel mondo - poco utilizzo del sistema e molti bug ancora non scoperti/corretti

Conclusioni

- Non fidatevi mai delle features dichiarate su carta
- Verificate la diffusione in scala mondiale della soluzione scelta
- Provate e stressate le soluzioni all'interno del vostro CED per molto tempo
- Con molti vendor si è riusciti ad ottenere sino al 60% di sconto sulla prima offerta

Domande?

DEFT Linux
Computer Forensics Live CD



Dott. Stefano Fratepietro
stefano@deftlinux.net



Creative Commons Attribution-Non opere derivate 2.5

Milano, 22 ottobre - Smau 2010
Fiera Milano city