Splunk>

Kateřina Nová

Splunk

- Co je to splunk?
- Jaká data zpracovává?
- Vyhledávání v datech
- Prezentování výsledků
- Výstrahy
- Spolupráce
- Reference

Co je to splunk?

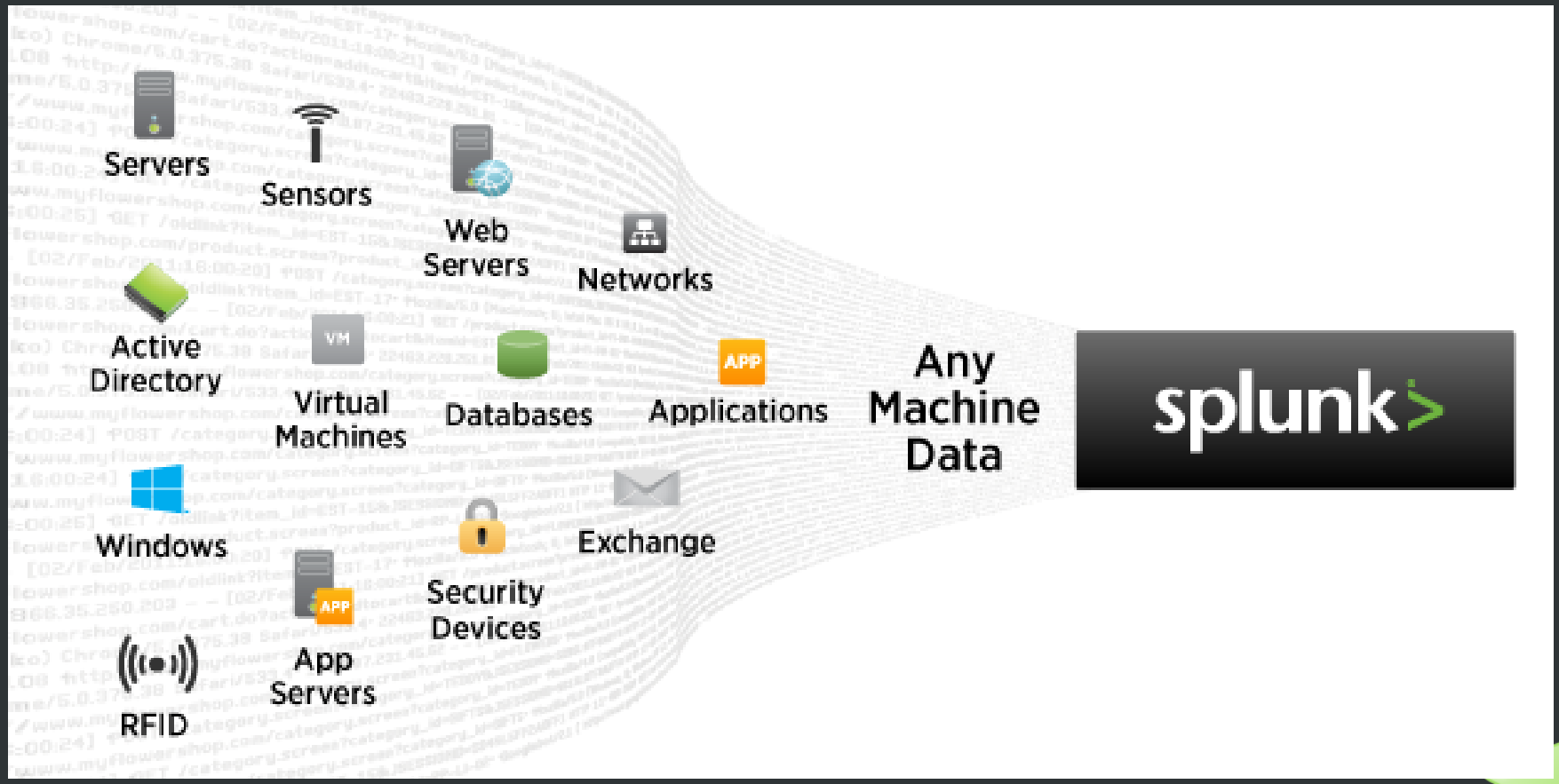
- Software, který indexuje data z aplikací, serverů či síťových zařízení
- Umožňuje procházet, prohledávat, analyzovat a vizualizovat různá data z jednoho místa
- V reálném čase nebo nad historickými daty

Instalace

- Zdrarma 60-ti denní Enterprice licence, poté přechod na omezenou Free verzi
- Snadná a rychlá instalace
- Po spušťění přístup přes webové rozhranní
- Přenositelnost na všechna zařízení

Vložení dat

- Jakákoli data – nestrukturovaná, různé zroje
- Lokální x vzdálená

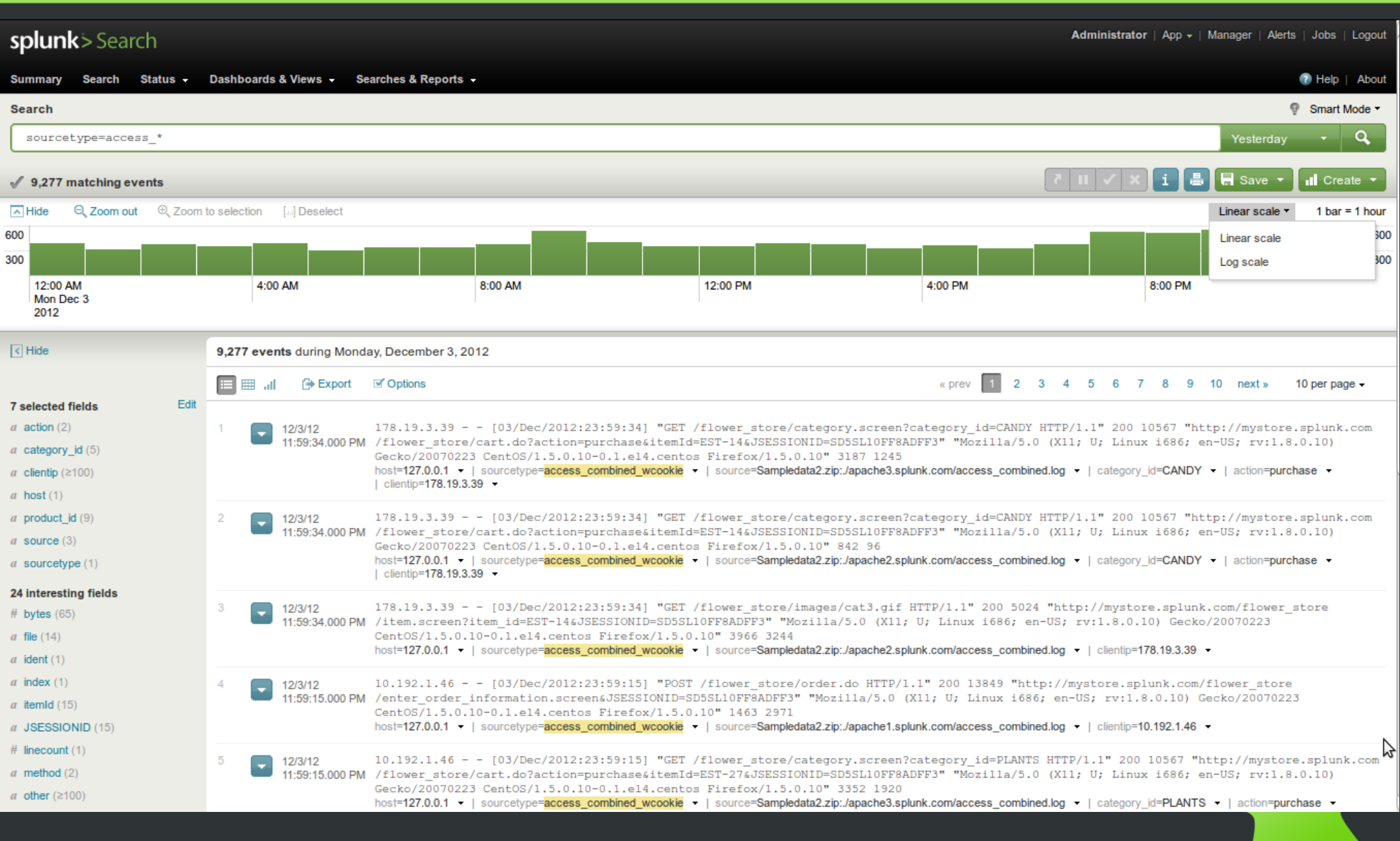


Zdroj: splunk.com

Data+

- Fields – označení, jaká data co znamenají
  - Defaultní – host, sourcetype
  - Vlastní – definované regulárními výrazy
- Přidání dodatečných dat, která budou dobře vypadat na reportech (př. tabulku číslo produktu - název)

Prohledávání dat

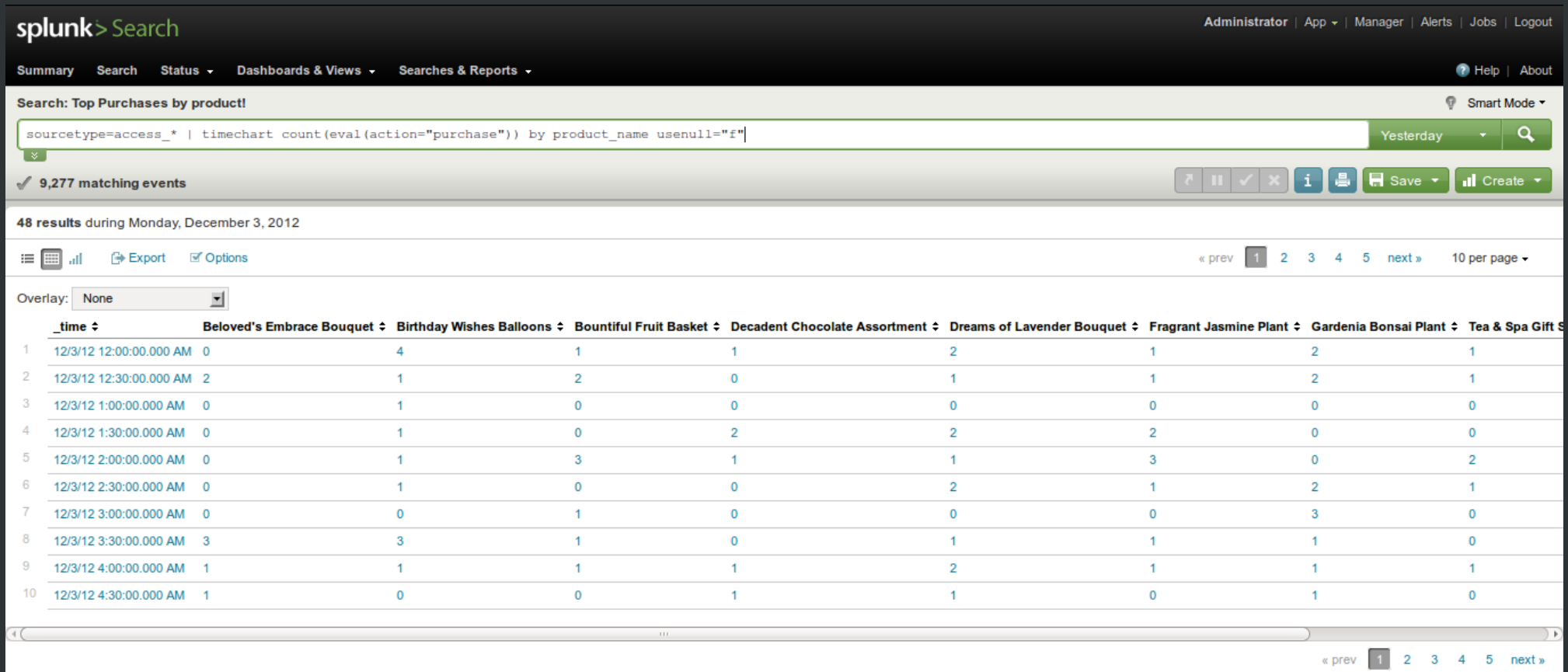


Vyhledávací jazyk

- CLI
- Fieldy
- Pipeline
- Subserch
- Funkce
- Regulární výrazy

Př: Přístupy dle produktů

sourcetype=access_* | timechart count(eval(action="purchase")) by product_name usenull="f"



	_time	Beloved's Embrace Bouquet	Birthday Wishes Balloons	Bountiful Fruit Basket	Decadent Chocolate Assortment	Dreams of Lavender Bouquet	Fragrant Jasmine Plant	Gardenia Bonsai Plant	Tea & Spa Gift S
1	12/3/12 12:00:00.000 AM	0	4	1	1	2	1	2	1
2	12/3/12 12:30:00.000 AM	2	1	2	0	1	1	2	1
3	12/3/12 1:00:00.000 AM	0	1	0	0	0	0	0	0
4	12/3/12 1:30:00.000 AM	0	1	0	2	2	2	0	0
5	12/3/12 2:00:00.000 AM	0	1	3	1	1	3	0	2
6	12/3/12 2:30:00.000 AM	0	1	0	0	2	1	2	1
7	12/3/12 3:00:00.000 AM	0	0	1	0	0	0	3	0
8	12/3/12 3:30:00.000 AM	3	3	1	0	1	1	1	0
9	12/3/12 4:00:00.000 AM	1	1	1	1	2	1	1	1
10	12/3/12 4:30:00.000 AM	1	0	0	1	1	0	1	0

« prev 1 2 3 4 5 next »

Prezentace výsledků

- Reporty
  - Zobrazení výsledků vyhledávání – grafy
- Dashboardy
  - Sdružování reportů
  - Export: PDF, e-mail

Př: přístupy dle produktů

splunk> Search

Administrator | App | Manager | Alerts | Jobs | Logout

Summary | Search | Status | Dashboards & Views | Searches & Reports | Help | About

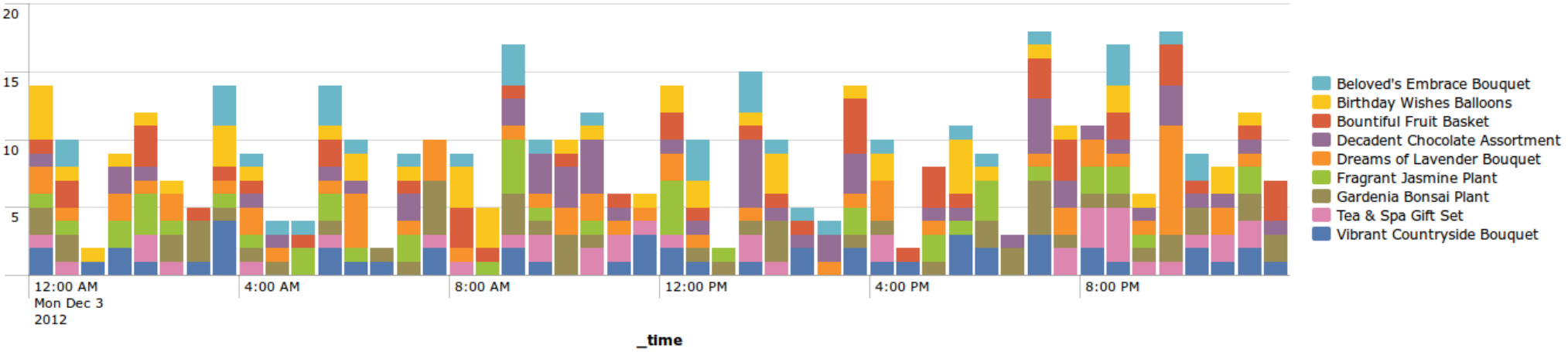
Report: Top purchases by Product -report!

9,277 matching events

Save results | Share results... | View previous jobs | View events | Generate PDF

Chart

Top purchases by Product



Table

Overlay: None | Enable Preview | Export

« prev 1 2 3 4 5 next » 10 per page

	_time	Beloved's Embrace Bouquet	Birthday Wishes Balloons	Bountiful Fruit Basket	Decadent Chocolate Assortment	Dreams of Lavender Bouquet	Fragrant Jasmine Plant	Gardenia Bonsai Plant	Tea & Spa Gif
1	12/3/12 12:00:00.000 AM	0	4	1	1	2	1	2	1
2	12/3/12 12:30:00.000 AM	2	1	2	0	1	1	2	1
3	12/3/12 1:00:00.000 AM	0	1	0	0	0	0	0	0
4	12/3/12 1:30:00.000 AM	0	1	0	2	2	2	0	0
5	12/3/12 2:00:00.000 AM	0	1	3	1	1	3	0	2
6	12/3/12 2:30:00.000 AM	0	1	0	0	2	1	2	1

Výstrahy

- Definování zajímavých (nebezpečných) událostí
- Vygenerování výstrahy
- Reakce na výstrahu
  - Poslání e-mailu
  - Spuštění skriptu

Spolupráce

- Cisco
  - Zabezpečení webu, emailu, řešení spamu
- Microsoft
  - Zabezpečení, řešení problémů
- F5
  - Real-time prohledávání a analýza dat

Splunk Apps

- Stovky doplňků, rozšíření, usnadnění..
- Poskytují uživatelský komfort pro různé role a případy užití

- Sledování systému – Windows, Linux
- Cisco security suite
- Splunk on Splunk
- Google maps pro zobrazení výsledků na mapě

Reference

- Enterprice licenci má přes 4 400 společností
- Ve více než 80 zemích
- University of Texas, Austin
    - Více než 50 000 studentů, přes 120 000 zařízení
- American University of Sharjah

Proč právě Splunk?

- Snadná instalace i používání
- Přístup ke všem datům z jednoho místa v reálném čase
- Automatické upozornění na podezřelé události
- Pro všechny uživatele – CLI i klikací
- Spuštění na rozdílných HW
- Dokáže zpracovat desítky terabytů dat denně
- Bezpečnost

- Děkuji za pozornost