



## Focus op Security Governance:

Privileged Account Management  
Security Information & Event Management



Bob Lannoy  
Kristof Verslype

Onderzoek  
Maart 2012

## Agenda

- 
- Context & trends
  - Information Security Governance
  - Privileged Account Management
  - Security Information & Event Management



## Context

### 2.3 million consumer financial records stolen

Former Fidelity National Information Services broker sold information

### Former Sys Admin Gets 8 Years for Computer Sabotage

By The Associated Press • 12/14/2006

A former UBS PaineWebber systems administrator was sentenced Wednesday to eight years and one month in prison for attempting to profit by detonating a "logic bomb" program that prosecutors said caused millions of dollars in damage to the brokerage's computer network in 2002.

### Fired techie created virtual chaos at pharma company

A former IT staffer has pleaded guilty to using a secret vSphere console to wipe company servers

LEADER (U.S.) | JANUARY 25, 2008

### French Bank Rocked by Rogue Trader

Société Générale Blames \$7.2 Billion in Losses On a Quiet 31-Year-Old

Feds: IT admin plotted to erase Fannie Mae 'Server Graveyard' narrowly averted

By Dan Goodin in San Francisco • Get more from this author

Posted in Crime, 29th January 2009 20:18 GMT

A fired computer engineer for Fannie Mae has been arrested and charged with plotting to use a malicious software script designed to permanently destroy millions of files from all 4,000 servers operated by the mortgage giant.



ANONYMOUS

3

### Wikileaks Afghanistan: leak inquiry centres on US intelligence analyst

The investigation into the biggest leak in US military history centres on a US Army intelligence analyst who allegedly boasted online that he was going to reveal "the truth" about the war in Afghanistan.



PAM - SIEM

Bob Lannoy & Kristof Verslype - Onderzoek

## Beveiligingsincidenten Statistieken (1/4)



Verizon data breach report 2011



PAM - SIEM

Bob Lannoy & Kristof Verslype - Onderzoek

4

## Beveiligingsincidenten Statistieken (2/4)



### 92% grote bedrijven (+20%)

- Gemiddeld **45** inbreuken (+30)
- Gemiddeld **280.000€-690.000€** ergste incident



### 83% kleine bedrijven (+38%)

- Gemiddeld **14** inbreuken (+6)
- Gemiddeld **27.500€-55.000€** ergste incident



PRICEWATERHOUSECOOPERS  Information Security Breaches Survey 2010

PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

5

## Beveiligingsincidenten Statistieken (3/4)

- 2010 ⇔ 2008



Virus  
62% (+41%)



Inbraak  
15% (+2%)



Denial of Service  
25% (+14%)



Verlies/diefstal data via personeel  
46%

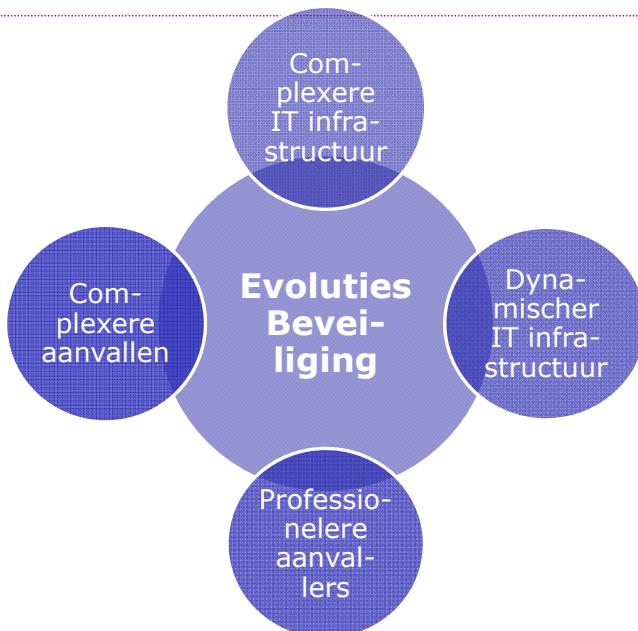


PRICEWATERHOUSECOOPERS  Information Security Breaches Survey 2010

PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

6

## Information security trends (1/3)



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

7

## Information security trends (2/3)



*The financial impact caused by successful cyberattacks by hackers and cybercriminals will not begin to decline until 2021.*

**Gartner** (29 november 2011)



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

8

## Information security trends (3/3)



### Reguleringen

- Sarbanes-Oxley, Hipaa, PCI DSS, ...
- Meer in USA, minder in EU



### Bedrijfspolicies

- Eigen security
- Outsourcing
- Klanten
- Standaarden (ISO 27001, ...)



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

9

## Agenda

- 
- Context & trends
  - Information Security Governance
  - Privileged Account Management
  - Security Information & Event Management



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

10

## Information Security Governance Aanpak (1/2)

Information Security  
Governance & Management

**Beleid / Processen**

**Implementatie  
/ Tools**



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

11

## Information Security Governance Aanpak (2/2)



Preventie

- Ontradenend
- Informerend

**PAM, SIEM**



Detectie

- Fysiek
- Virtueel

**SIEM**



Verhinderung

- Fysiek
- Virtueel

**PAM**



Reactie

- Bestraffend
- Technisch

**SIEM**



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

12

## Information Security Governance

### Technische veiligheidsmaatregelen (1/4)



**Beheer van gebruikers & rechten**

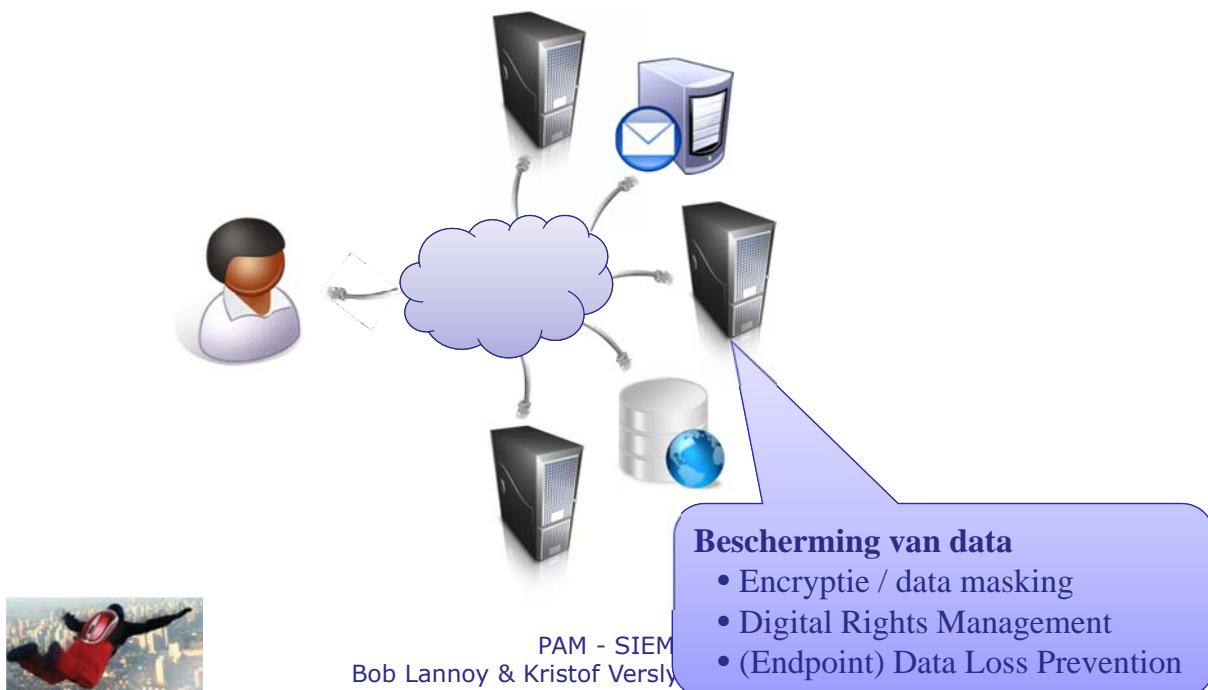
- Provisioning / deprovisioning
- Entitlements (access)
- Geprivilegerde accounts

PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

13

## Information Security Governance

### Technische veiligheidsmaatregelen (2/4)



**Bescherming van data**

- Encryptie / data masking
- Digital Rights Management
- (Endpoint) Data Loss Prevention

PAM - SIEM  
Bob Lannoy & Kristof Verslype

## Information Security Governance

### Technische veiligheidsmaatregelen (3/4)



**Bescherming van transport**

- Beveiligde verbindingen U2A, A2A
- NAC

PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

15

## Information Security Governance

### Technische veiligheidsmaatregelen (4/4)



**Monitoring & alerting**

- Logging
- Database Activity Monitoring
- Intrusion Detection
- **Security Information & Event Monitoring (SIEM)**

Bob Lannoy & Kristof Verslype - Onderzoek

## Agenda

- 
- Context & trends
  - Information Security Governance
  - Privileged Account Management
    - Wat is het?
    - Aanpak
    - Software & demo's
    - Niet-toolgebonden aspecten
    - Conclusies
  - Security Information & Event Management



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

17

## Insider Threat (1/2)



- 
- Doelbewust
    - AI dan niet uitgebreide toegangsrechten
    - Hacking technieken (privilege escalation)
    - Toegang tot gevoelige data/systemen
  - Onbewust
    - Gewone gebruikers met (teveel) rechten
    - Gevoelige gegevens meenemen/verliezen
    - (Doel van hack-aanval)



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek



## Insider Threat (2/2)

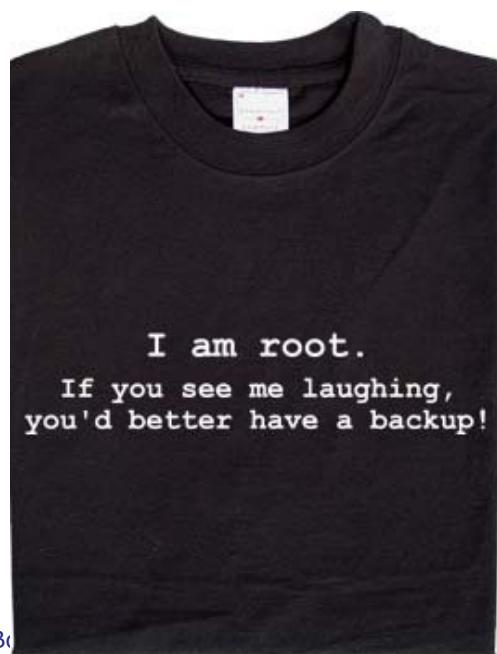
- Insider threat ~ 20 à 40 % incidenten
    - 10 à 20% doelbewust → ~ 5%
-  Impact omgekeerd evenredig



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

19

## Wat is "Privileged account management"?



Bo

20

## Wat is "Privileged account management"? Termen & acroniemen

Access  
Account  
Identity  
User  
Privileged Management

PAM  
PIM  
PUM

Super User Privilege Management	SUPM
Application to Application Password Management	AAPM
Shared-Account/Software-Account Password Management	SAPM
Privileged Account Activity Management	PAAM



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

21

## Wat is "Privileged account management"? Termen & acroniemen

- Privileged Account
- Shared-Account/Software Account
- Application to Application
- Activity



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

22

## Wat is "Privileged account management"? Privileged account / Shared-account

### Gewone account

Gebruiker met eigen credentials (uid/pw, eid/pin, ...)  
Gebonden aan gebruiker  
Gebruiker is 'verantwoordelijk'



### Privileged account / Shared-account

Account met hogere rechten  
Niet gebonden aan gebruiker  
Gedeeld met verschillende gebruikers  
Beheeraccounts software/hardware



## Wat is "Privileged account management"? Privileged account / Shared-account

### • Voorbeelden

- OS: Administrator (Windows), root (Linux)
- DB : SYS / SYSTEM (Oracle), ...
- Virtualisatiesoftware console
- Netwerk toestellen
- Service accounts, ...



## Wat is "Privileged account management"? Application to Application

- Wachtwoorden in applicaties
  - Toegang tot database
  - Communicatie tussen toepassingen
- Opslag wachtwoord
  - Embedded
  - Configuratiebestand



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

25

## Wat is "Privileged account management"? Activity

- Logging van activiteit van gebruiker
  - Wie / waar / wanneer
  - Session logging
- Ondersteuning voor audit / compliance



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

26

## Wat is "Privileged account management"? Probleem (1/2)

- Default accounts met vast wachtwoord
- Gedeeld → groep gebruikers
  - Hoe wordt het gedeeld?
  - Veiligheid/bescherming van wachtwoord  
*Complexiteit, vernieuwing na x tijd, ...*
- Operaties met die account → wie was het?
- Mensen die bedrijf verlaten, wachtwoord veranderd?
- Gebruik van virtualisatie of private cloud, vergroot mogelijke schade



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

27

## Wat is "Privileged account management"? Probleem (2/2)

- **Risico's**
  - Verlies van confidentiële gegevens
  - Serviceonderbrekingen
  - Imagoschade



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

28

## Agenda

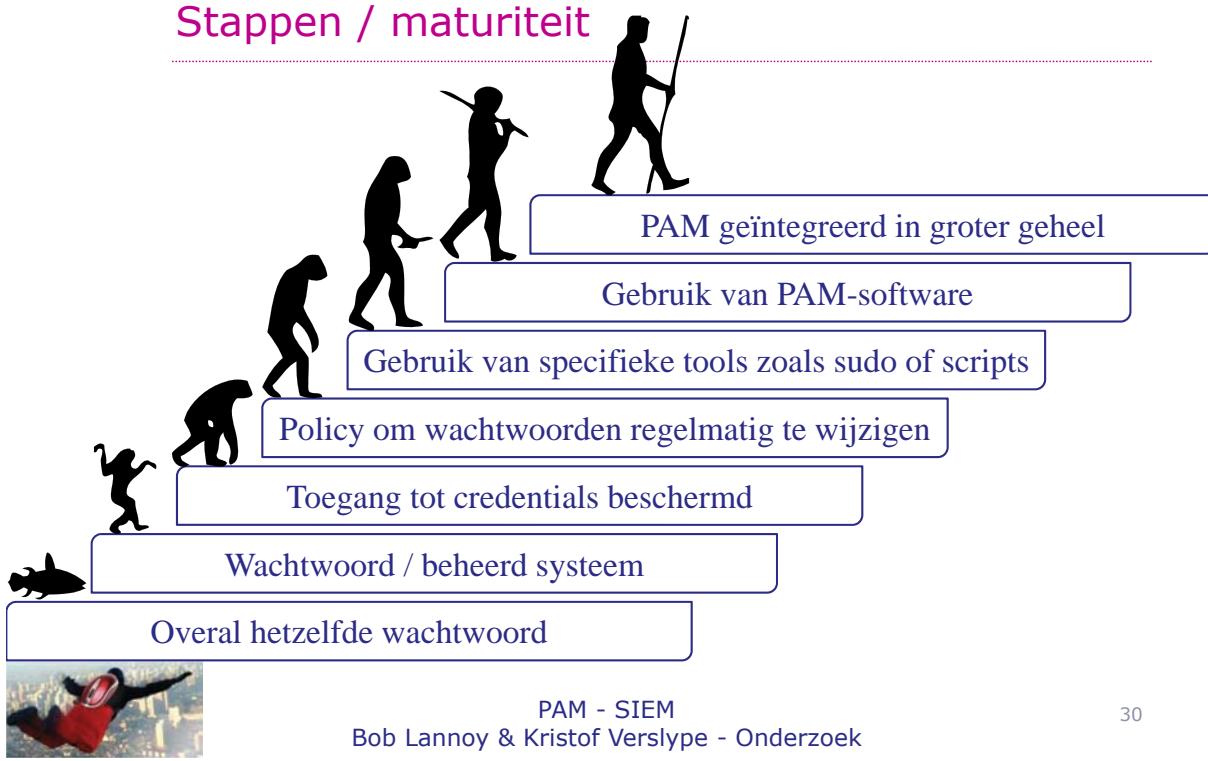
- Context & trends
- Information Security Governance
- Privileged Account Management
  - Wat is het?
  - Aanpak
  - Software & demo's
  - Niet-toolgebonden aspecten
  - Conclusies
- Security Information & Event Management



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

29

## Aanpak Stappen / maturiteit



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

30

## Aanpak Principes

### Gewone account

Tijdelijke verhoging van rechten

### Administrator

Administratie account naast gewone account

One-time passwords

Toegang tot shared account in noodsituaties



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

31

## Agenda

- Context & trends
- Information Security Governance
- Privileged Account Management
  - Wat is het?
  - Aanpak
  - Software & demo's
  - Niet-toolgebonden aspecten
  - Conclusies
- Security Information & Event Management



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

32

## Aanpak Software

- Privilege elevation in OS
  - Sudo (Linux), Runas (Windows)
  - Role based Access Control (Solaris)
  - Specifieke softwarepakketten (Windows, Linux)



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

33

## DEMO - Sudo

- Privilege elevation: "*sudo <commando>*"
- Configuratie in "*sudoers*" bestand
- Configuratie is niet zonder gevaren
- Centralisatie configuratie mogelijk (LDAP)
- I/O logging (sedert 1.7.3)
- Plugin architectuur (sedert 1.8), met bijvoorbeeld plugin van *Quest Privilege manager for sudo*



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

34

## Aanpak Software

► **beyondtrust**®

**ca**  
technologies

**Cyber-Ark**®



**LIEBERMAN SOFTWARE™**

**QUEST  
SOFTWARE**®

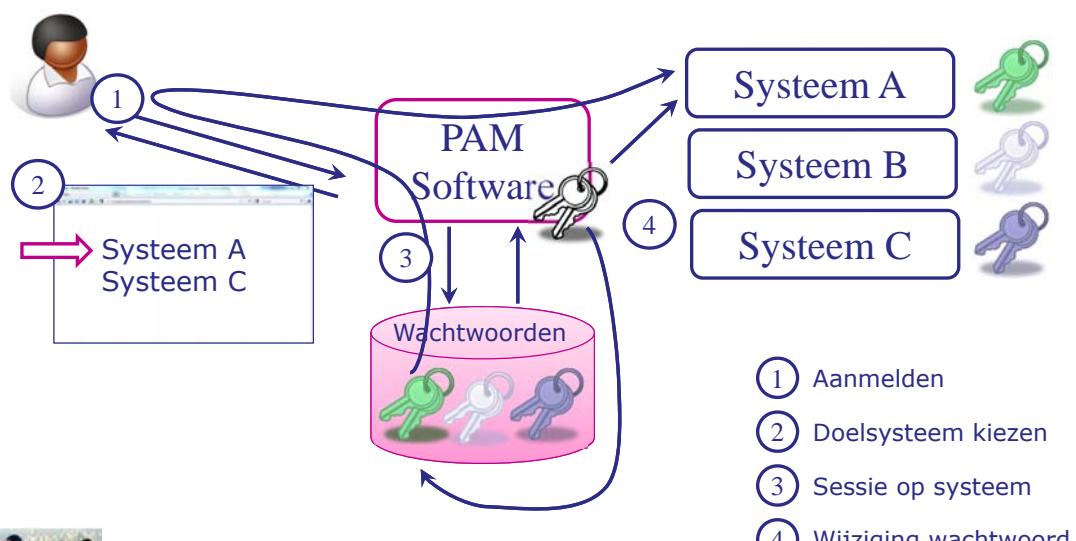
...



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

35

## Software Werkingsprincipe



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

36

## Software Eigenschappen

- Centrale wachtwoord database
  - ~ Agent-less
  - Connectoren
  - Robuust & veilig
  - Appliance of software
- Productspecifieke connectoren  
SSH, Telnet  
HTTP(S)  
ODBC  
...
- Encryptie  
Disaster recovery  
High availability



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

37

## Software Eigenschappen

- Discovery
  - Beheer PW
  - Toegangscontrole
- Identificeren van *privileged accounts*  
Via AD, DNS, portscan, CMDB, ...
- Automatisch wijzigen (policy)  
Coördinatie / orchestratie  
Consistentie controle
- Gebruikersinformatie  
Context  
Workflow



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

38

## Software Eigenschappen

- Wachtwoorden gebruiker
  - Tonen
  - Copy/paste buffer
  - Sessie openen
  - Privilege elevation
  
- Wachtwoorden toepassing
  - PAM API
  - Authenticatie !!
  
- Rapportering/logging
  - Algemene logging
  - Session recording
  - Rapport
  
- Integratie ticket-systeem (ITIL)

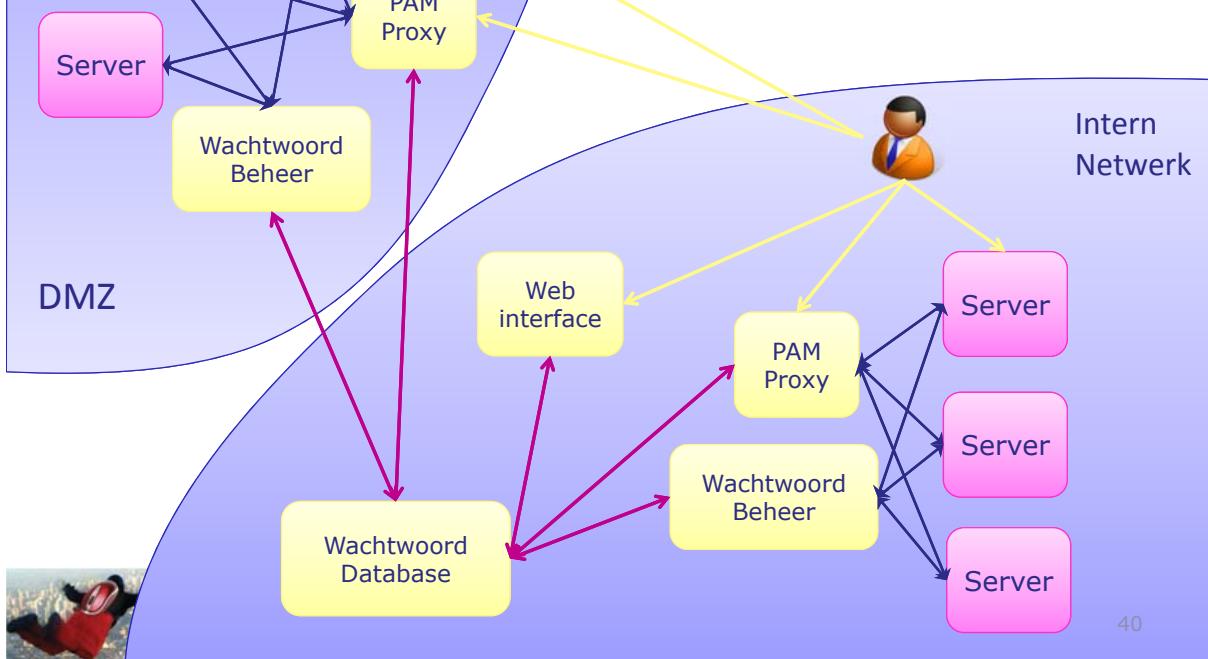


PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

39

03/2012

## Topologie



40

## DEMO - PAM-tool

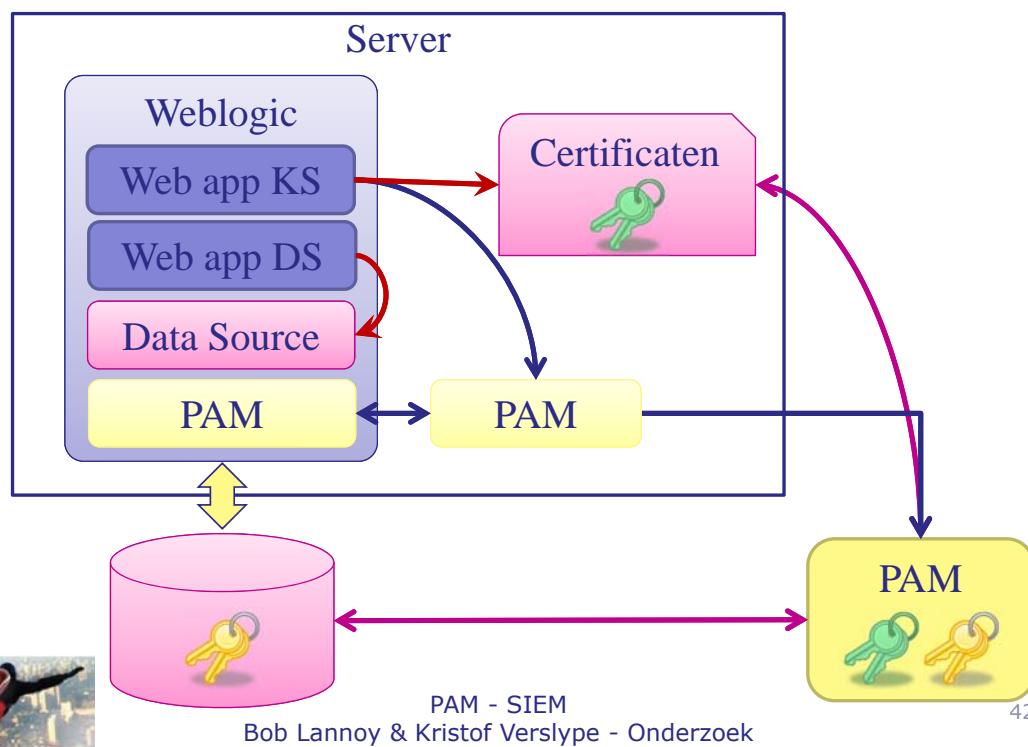
- Windows
- Unix
- Database



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

41

## DEMO - toepassingen



## Software Vaststellingen (1/2)

- Redelijk vlot voor standardsystemen
  - Scripting voor tuning van command prompts
- Soms browserafhankelijk gedrag
- Topologie heeft invloed op implementatie
  - firewall die (Windows) traffiek blokkeert
- Veranderend serverpark
  - koppeling met tool nodig (API)
- Gelijktijdig gebruik zelfde gedeelde account 



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

43

## Software Vaststellingen (2/2)

- Integratie in applicaties
  - ➔ complexiteit ↑ (API, deployments)
  - ➔ geen wachtwoordbeheer meer in app
- Wachtwoord caches & wijzigingen
  - Account lockout
  - Tuning
- Huidige aanpak elk team (Windows, Unix, DB, ...) verschillend

PAM = project



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

44

## Software Prijsmodellen

---

- / eindgebruiker
- Software
  - / Softwareinstantie
  - / Appliance
- Wachtwoorden
  - / beheerd wachtwoord
  - / beheerde server
- Session recording
  - / server
  - Concurrent sessions



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

45

## Agenda

---

- Context & trends
- Information Security Governance
- Privileged Account Management
  - Wat is het?
  - Aanpak
  - Software & demo's
  - Niet-toolgebonden aspecten
  - Conclusies
- Security Information & Event Management



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

46

## Niet-toolgebonden aspecten

- Ken uw (nieuw) personeel
- **Opleidingen:** maak mensen bewust van risico's
- **Segregation-of-duties:** combinatie van taken geeft aanleiding tot risico
- **Monitoring/logging** naar extern systeem beheerd door andere personen



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

47

## Agenda

- Context & trends
- Information Security Governance
- Privileged Account Management
  - Wat is het?
  - Aanpak
  - Software & demo's
  - Niet-toolgebonden aspecten
  - Conclusies
- Security Information & Event Management



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

48

## Conclusies (1/3)

- Beperk de risico's en neem beheer van privileged accounts in handen
- PAM deel van groter geheel
  - Klassiek Identity/Access management
  - Monitoring
  - ...
- PAM ≠ 1 tool
  - Beleid / policies / processen / technologie
  - Segregation-of-duties
  - Bewustmaking gebruikers
  - Auditproces (gescheiden van IT)



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

49

## Conclusies (2/3)

- Zonder PAM-tool
  - Minimum : Wachtwoord / systeem
  - Administrators ≠ shared accounts
  - Gewone gebruikers: "sudo"
  - Wachtwoordenlijst beveiligen
  - Wachtwoorden veranderen
  - Automatisatie/centralisatie beheer
  - Logging / monitoring



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

50

## Conclusies (3/3)

- Met PAM-tool
  - Risico maximaal beperkt tot beheerder van tool
  - Let op gewenste functionaliteit
  - Impact van topologie/architectuur op kostprijs
  - Gebruiksvriendelijkheid van oplossing
  - Verhoging complexiteit <-> verhoging veiligheid
  - Beschikbaarheid
- Risico <-> Kost



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

51



bob.lannoy@smals.be

 @boblannoy



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

52

## Agenda

- 
- Context & trends
  - Information Security Governance
  - Privileged Account Management
  - Security Information & Event Management
    - Basisprincipes
    - AlienVault
    - ArcSight
    - Managed SIEM
    - Tot slot



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

53

# Basis- Principes

## Uitdaging

- Miljoenen logs, slechts enkele incidenten...



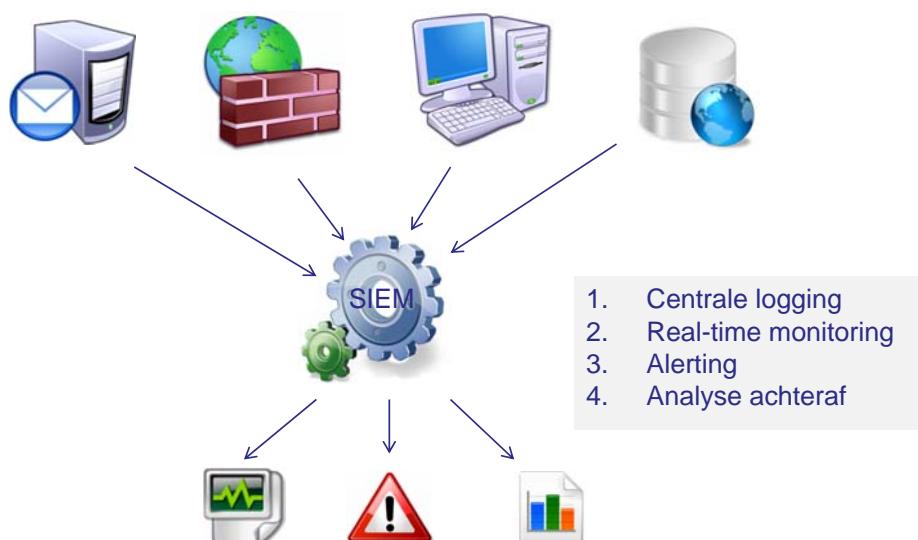
→ **Onmogelijk manueel**



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

55

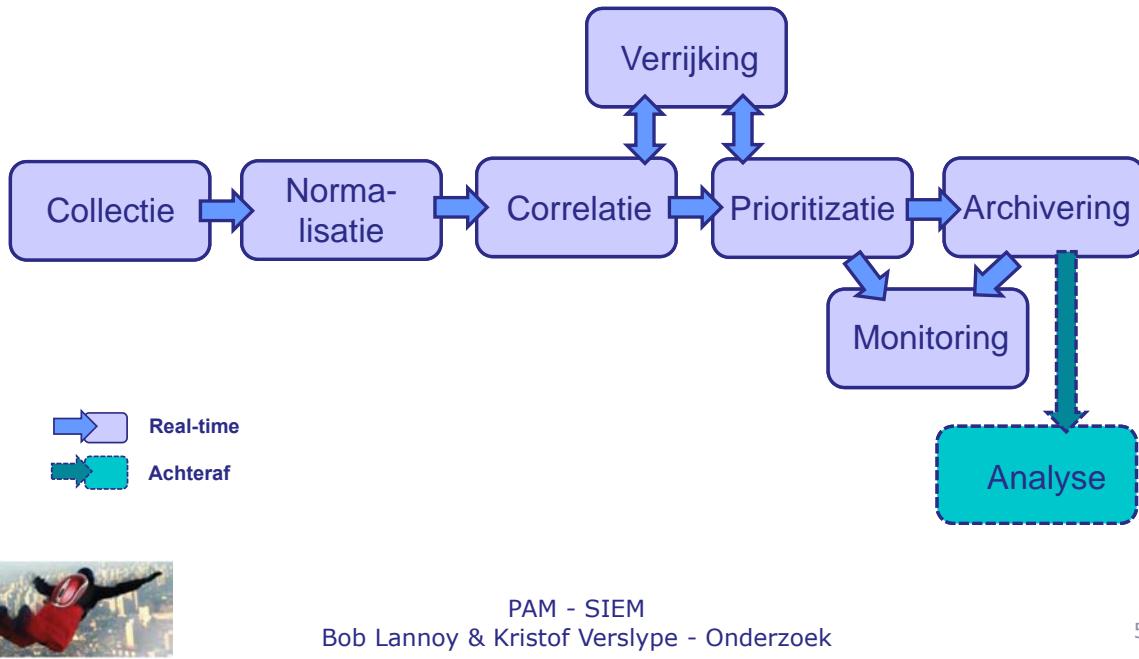
## De essentie



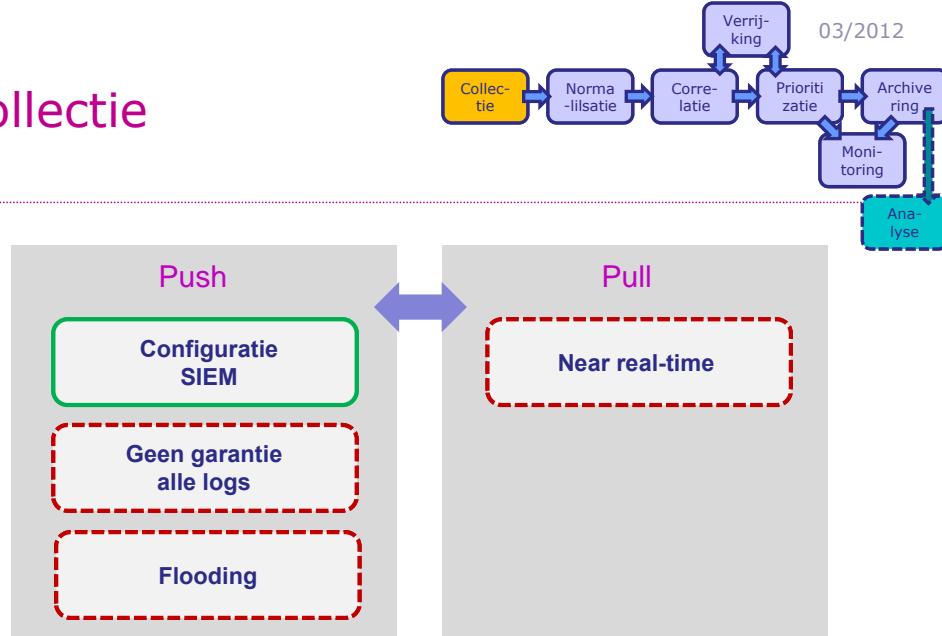
PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

56

# Verwerkingsproses



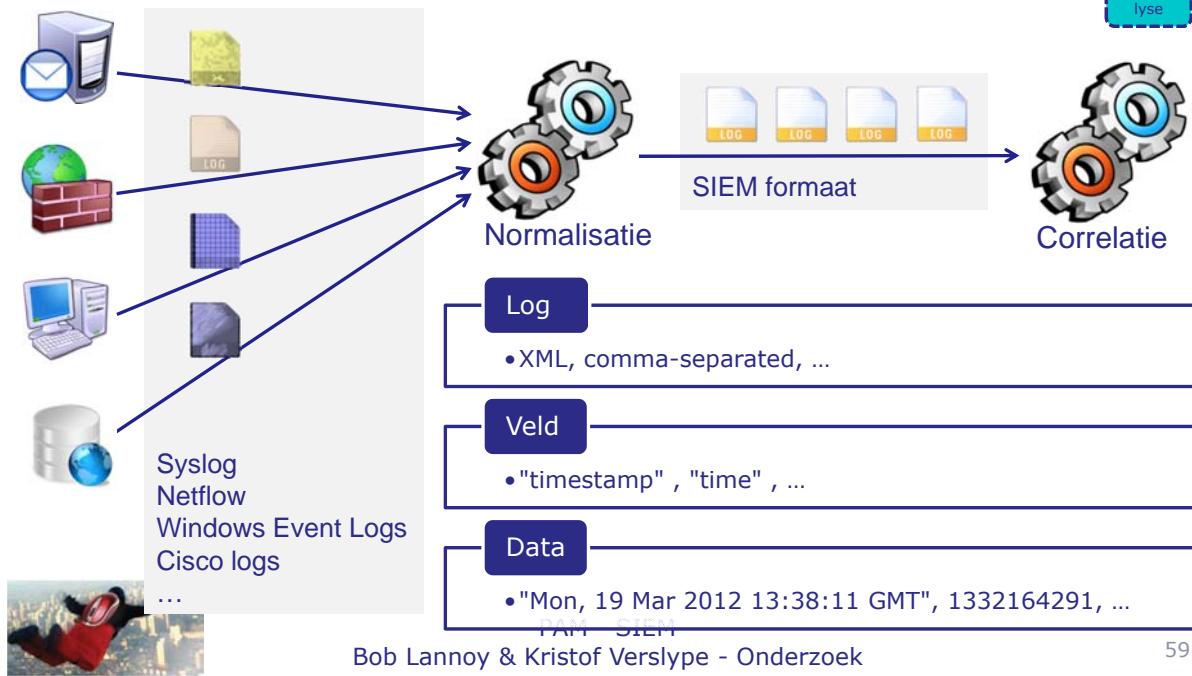
# Collectie



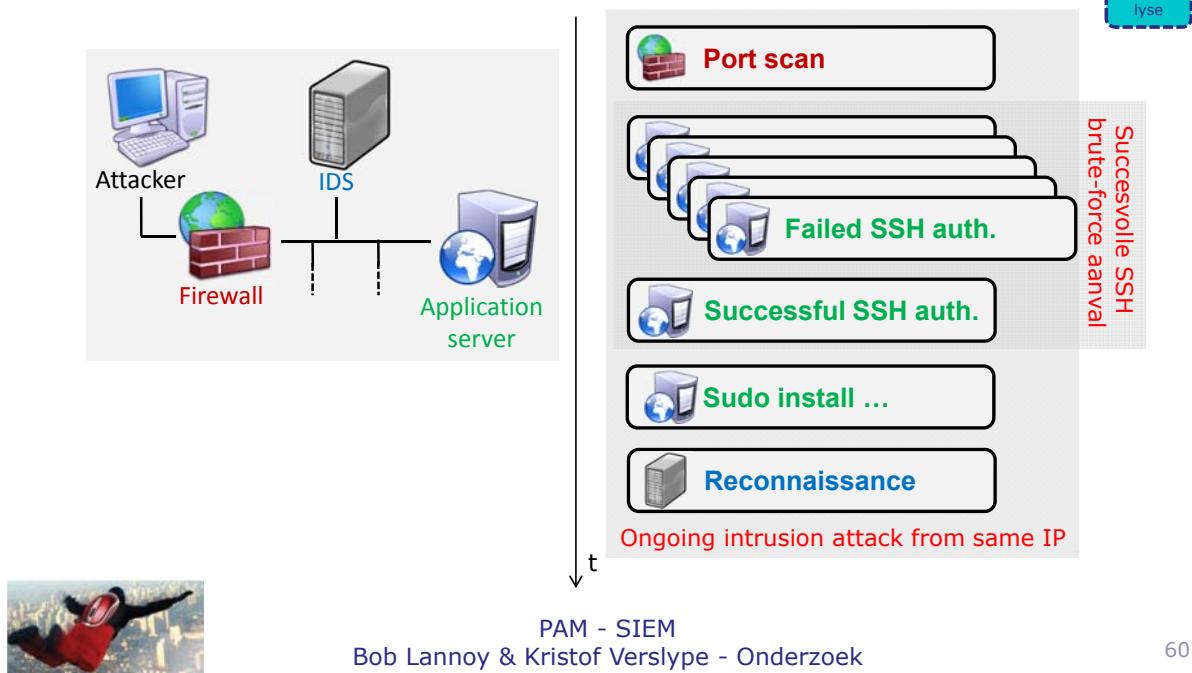
- ➡ Ondersteunt SIEM de bron?
  - ➡ Soms agent op device nodig
  - ➡ Meestal push



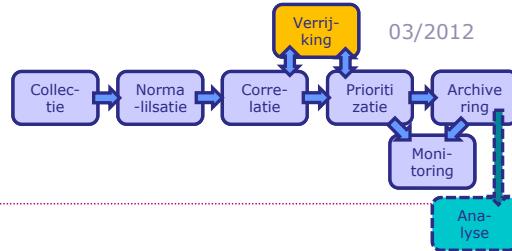
## Normalisatie



## Correlatie

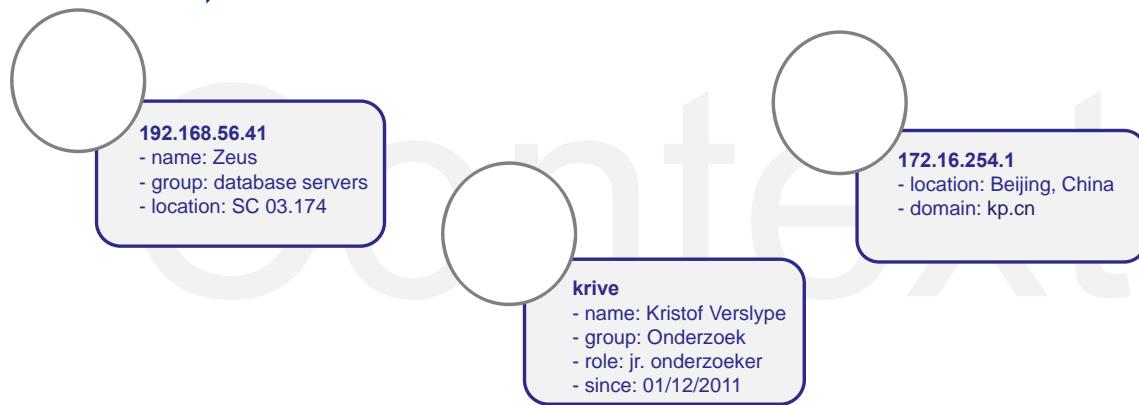


## Verrijking



"Mar 20 08:44:35 192.168.56.41 sshd[263] Accepted pass for **krive** from 216.101.197.234 port 56946 ssh2"

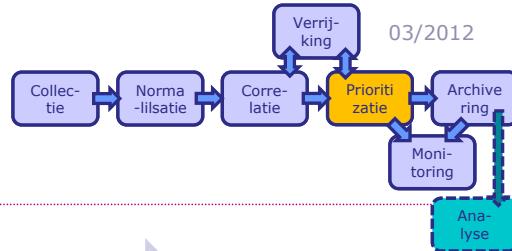
➡ Externe bronnen: DNS, user directories, ...



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

61

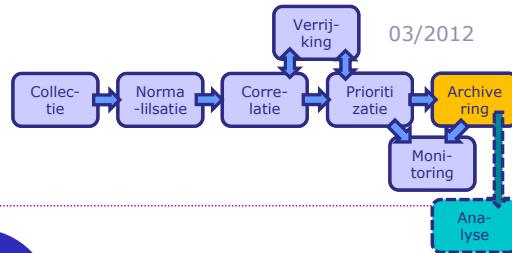
## Prioritazie



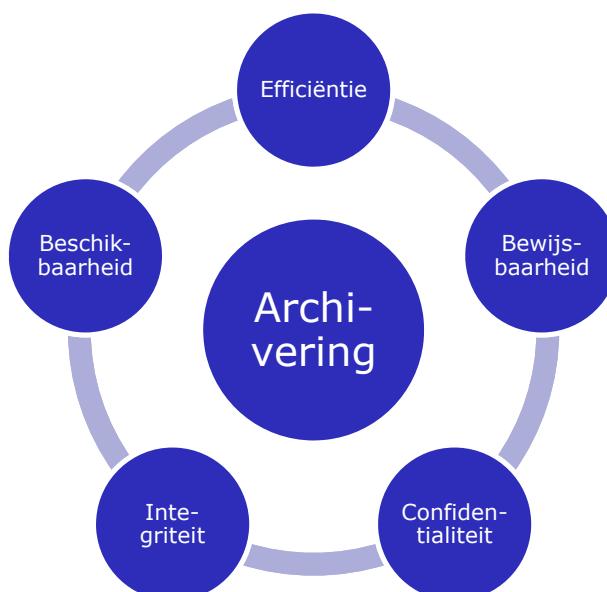
PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

62

## Archivering



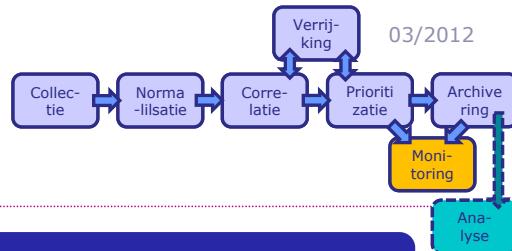
03/2012



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

63

## Monitoring



03/2012



### Evaluieren

- Kwetsbaarheden
- Verdachte activiteit
- Incidenten



### Dashboards

- Remote login
- Idealiter enkele high-priority events



### Alarm

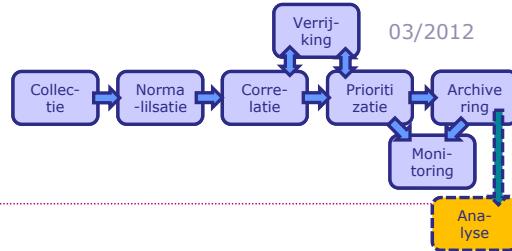
- Dashboard
- E-Mail, SMS, ...



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

64

## Analyse



Middel	Reden
Rapporten	Kennis eigen security
Queries	Forensisch onderzoek
	Compliancy



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

65

03/2012

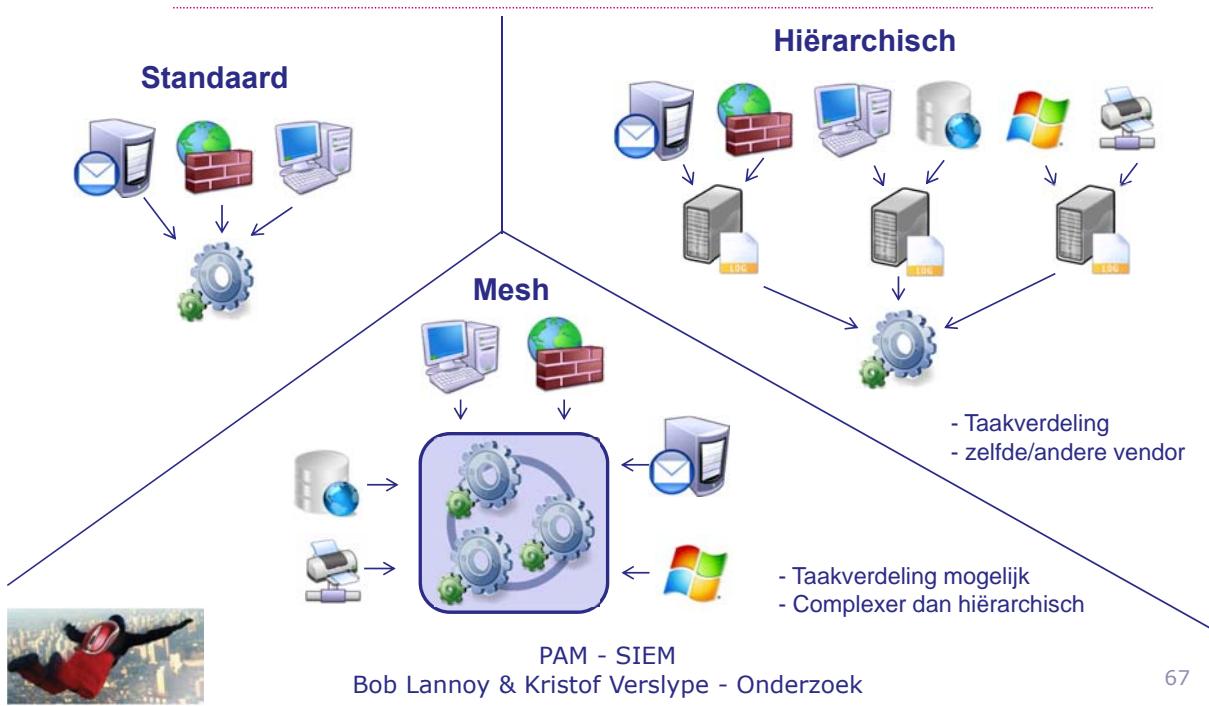
## Evolutie



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

66

## Topologie



## Beschikbare systemen

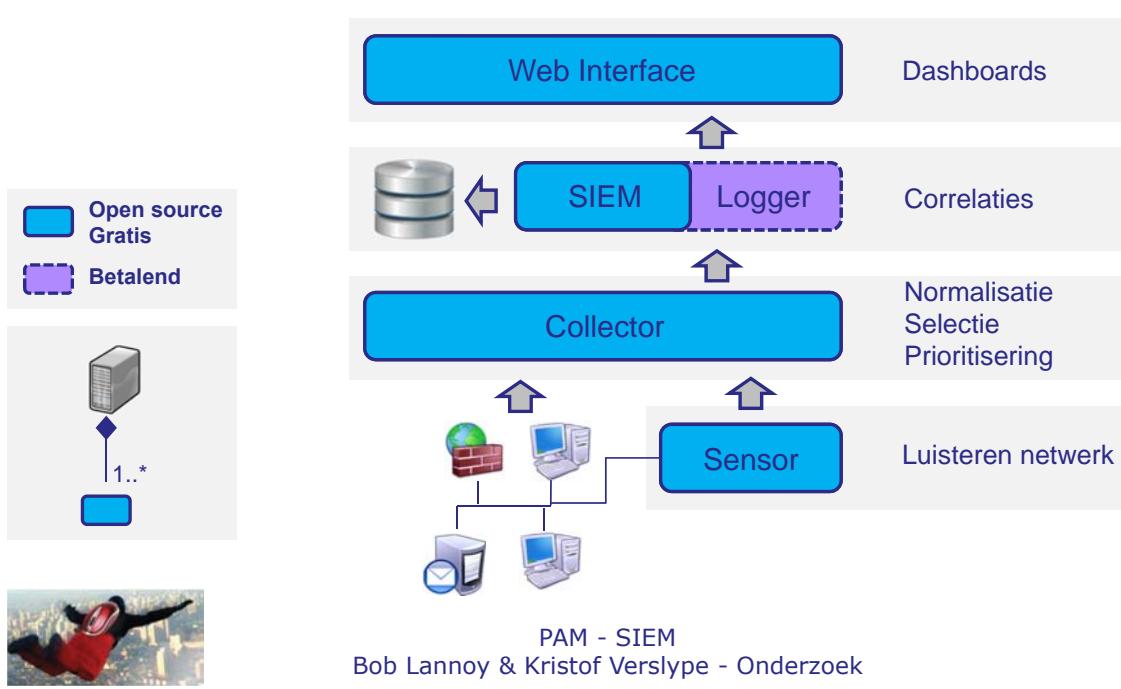




Basisprincipes ➤ AlienVault ➤ ArcSight ➤ Managed SIEM ➤ Tot slot



## Componenten



## Bouwbladen

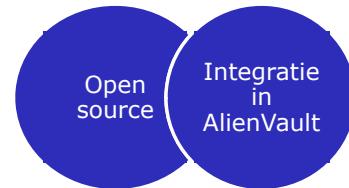
OCS next generation  
inventory

**Nagios®**



P0f

NFSen/NFDump



Inprotect



Passive Asset Detection System

**OSVDB**



 OSSEC



PAM - SIEM

Bob Lannoy & Kristof Verslype - Onderzoek

71

## Correlaties (1/3)

DoS

Spoofing

MAC address change

Reconnaissance

Traffic

Torrent

Command execution

/etc/passwd access

SSL tunnel

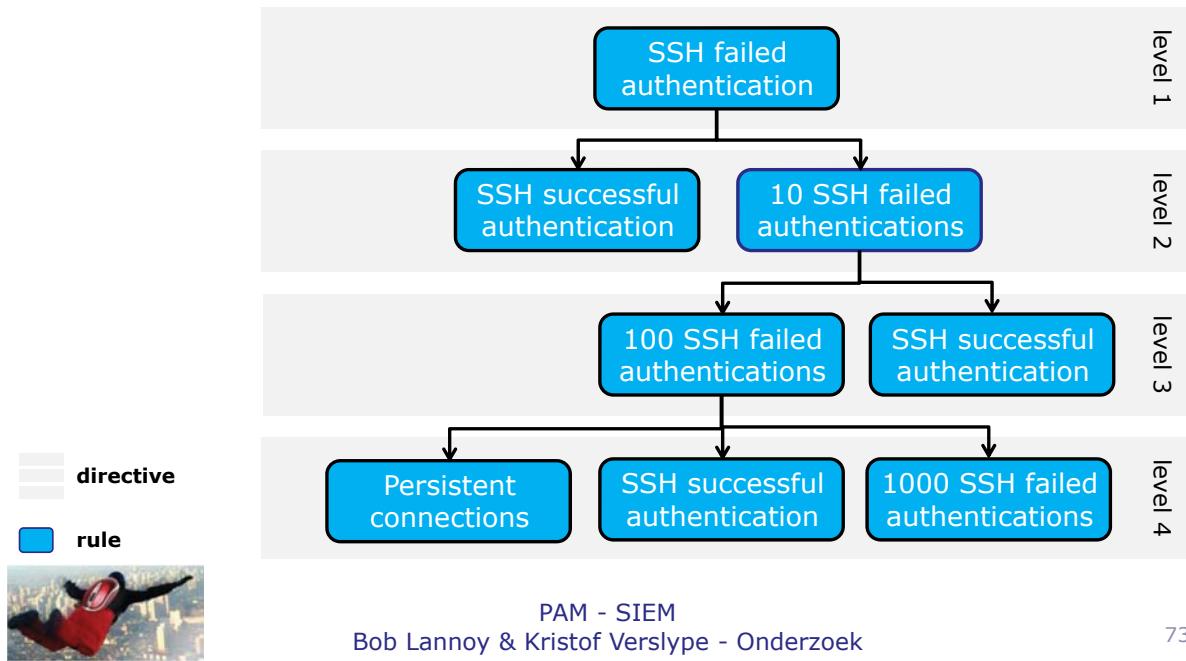
Flooding

Malware infection/activity

...



## Correlaties (2/3)



## Correlaties (3/3)

```
<directive id="500000" name="SSH Brute Force Attack Against DST_IP" priority="4">
...
<rule type="detector" name="SSH Authentication failure (10 times)"
reliability="2" occurrence="10"
from="1:SRC_IP" port_from="ANY"
to="1:DST_IP" port_to="ANY"
time_out="40"
plugin_id="4003" plugin_sid="1,2,3,4,5,6,9,10,12,13,14,15,16,20"
sticky="true"/>
...
</directive>
```

Ook via GUI

Standaard 92  
directieven



## Normalisatie (plugins)

```
event_type=event
regexp=(?P<\w{3}\s\w{3}\s\d{2}:\d{2}:\d{2}\s\w{4})|(\w{3}\s+\d{1,2}\s\d{2}:\d{2}:\d{2})(\]\s).*\s|(?P<emerg|alert|crit|error|warn|notice|info|debug))| ([client (?P<S+)])|(?P<.*)
date={normalize_date($date)}
plugin_sid={translate($type)}
src_ip={$src}
userdata1={$data}
```

Ondersteuning  
2395 bronnen

Geen DAM,  
PAM, ...

Geen GUI



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

75

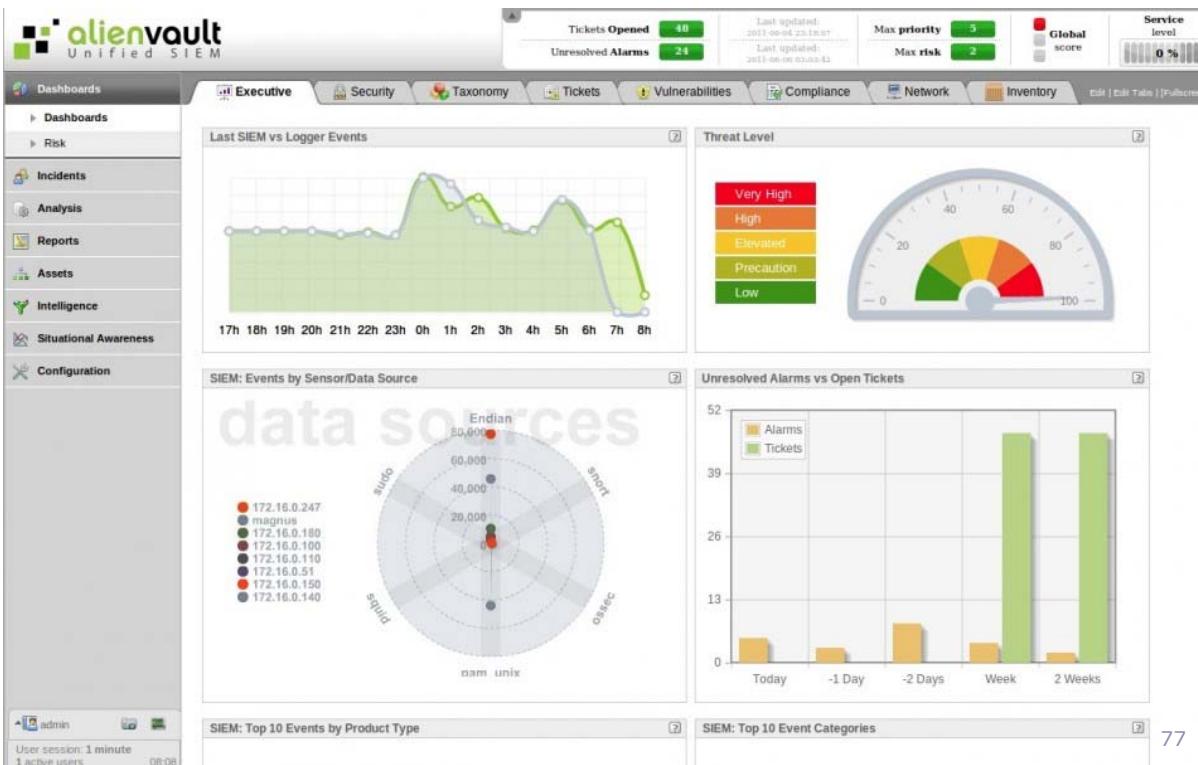
## Screenshots

- Overzicht
- Alarmen
- Kwetsbaarheden



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

76



**Alarms Report**

Filters, Actions and Options

(0-50 of 179) Next 50 -> Last ->>

#	Alarm	Risk	Sensor	Since	Last
<b>Sunday 07-Feb-2010 [Delete]</b>					
1	<b>AV Mariposa Botnet Activity on Server-Win</b> (13 events)	2	ossim	2010-02-07 17:03:35	2010-02-07 17:03:42
2	<b>AV Spyware Baidu.com Agent detected on Server-Win</b> (14 events)	3	ossim	2010-02-06 17:05:45	2010-02-07 16:20:55
-3	<b>AV Possible port 445 Worm Scan Behaviour on Server-Win</b> (4 events)	2	ossim	2010-02-07 06:21:06	2010-02-07 16:20:53
#	<b>Id</b>	Alarm	Risk	Date	
1	398945	<b>AV Possible port 445 Worm Scan Behaviour on Server-Win</b>	2	2010-02-07 16:20:53	
<b>Alarm Summary</b> [ Total Events: 2 - Unique Dst IPAddr: 2 - Unique Type: 2 ]					
+ 2 Total events matched after highest rule level, before timeout.					
<b>AV Trojan Downloader detected on Server-Win (Emo)</b> (3 events)					
#	<b>Id</b>	Alarm	Risk	Date	
1	398865	<b>AV Trojan Downloader detected on Server-Win (Emo)</b>	2	2010-02-07 16:20:52	
<b>Alarm Summary</b> [ Total Events: 2 - Unique Dst IPAddr: 2 - Unique Type: 2 ]					
+ 1 Total events matched after highest rule level, before timeout.					
<b>AV Malware Sality detected on Server-Win</b> (9 events)					
#	<b>Id</b>	Alarm	Risk	Date	
5	398866	<b>AV Malware Sality detected on Server-Win</b>	2	2010-02-07 08:33:21	2010-02-07 16:20:52
<b>Alarm Summary</b> [ Total Events: 2 - Unique Dst IPAddr: 2 - Unique Type: 2 ]					
+ 109 events					
#	<b>Id</b>	Alarm	Risk	Date	
6	398867	<b>AV Anonymous Proxy usage on 192.168.1.1 (Judge)</b> (109 events)	2	2010-02-07 08:32:28	2010-02-07 16:20:52

Vulnerabilities Reports Jobs Threats Database Profiles | Settings

**By Severity**

Severity	Count
High	41
Medium	23
Low	48
Info	169

**By Services - Top 10**

Service	Count
http (tcp/80)	6
microsoft-ds (tcp/445)	4
netbios-ns (udp/137)	4
netbios-ssn (tcp/139)	4
ssh (tcp/22)	4
epmap (tcp/135)	3
unknown (tcp/49154)	3
unknown (tcp/5357)	3
mysql (tcp/3306)	3
https (tcp/443)	3

**Top 10 Networks**

Network	Count
Buzz (192.168.1.0/24)	281

**Top 10 Hosts**

Host	Count
ossim (192.168.1.9)	43
monster (192.168.1.4)	41
192.168.1.33	40
192.168.1.60	38
192.168.1.55	28
Ext Gateway (192.168.1.11)	26
192.168.1.1	22
dell (192.168.1.5)	19
my.router (192.168.1.222)	15
juanma (192.168.1.50)	5

**Current Vulnerabilities**

Host - IP	Date/Time	Profile	Serious	High	Medium	Low	Info	Actions
All			0	41	23	48	169	
ossm (192.168.1.9)	2010-02-12 11:42:02	Info	0	6	5	3	29	
	2010-02-19 12:35:31	Default	0	6	4	3	28	
	2010-02-12 11:08:11	jose	0	0	0	0	1	



## Aandachtspunten



### Configuratie

- Setup Bronnen (syslog)
- Asset info
- Correlatieregels
- Plugins(normalisatie)



### Krachtige servers

- Normaliseren
- Correleren



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

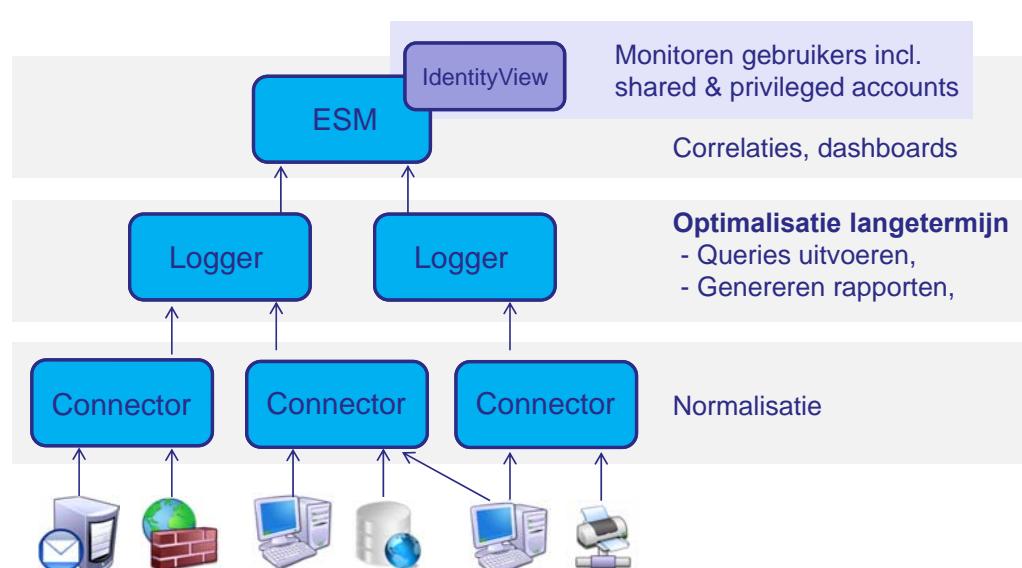


# ArcSight An HP Company

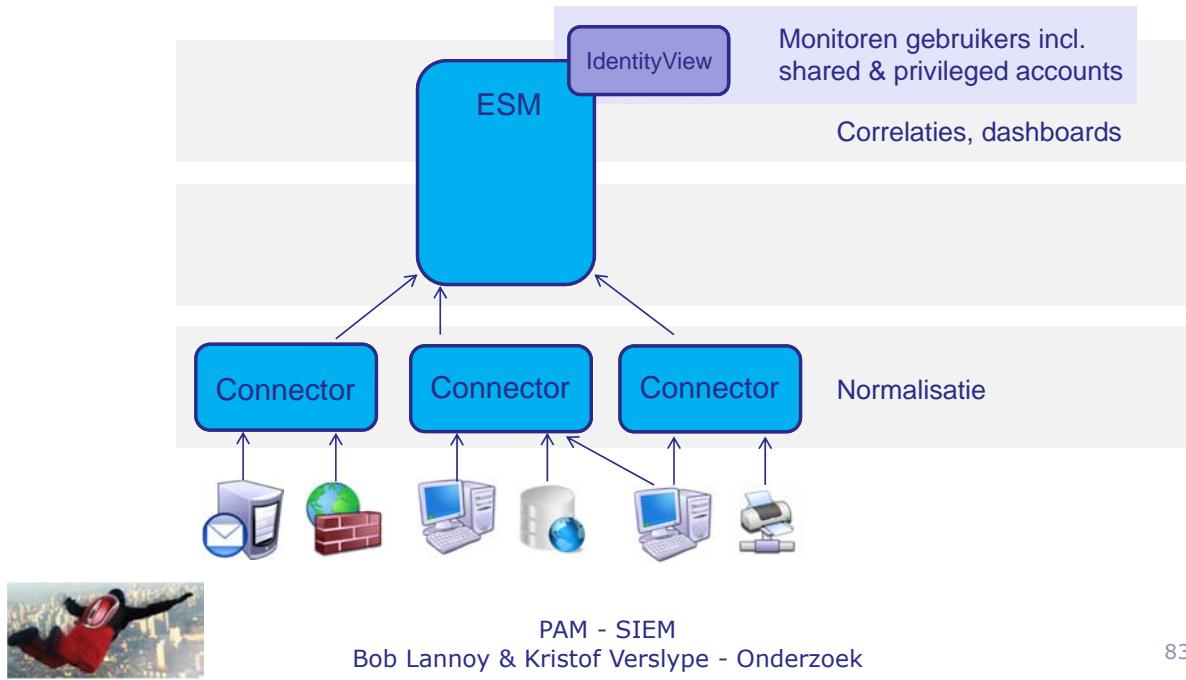
Basisprincipes ➤ AlienVault ➤ ArcSight ➤ Managed SIEM ➤ Tot slot



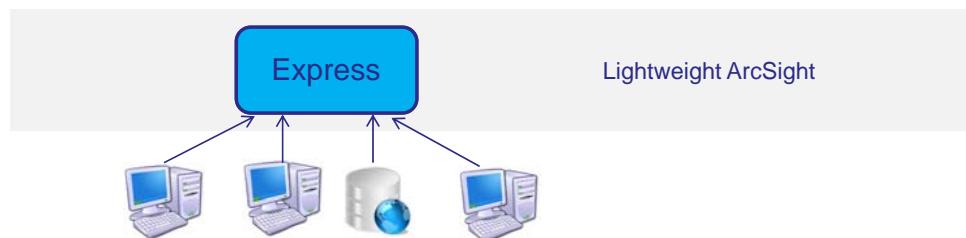
## Componenten (1/3)



## Componenten (2/3)



## Componenten (3/3)



## Screenshots

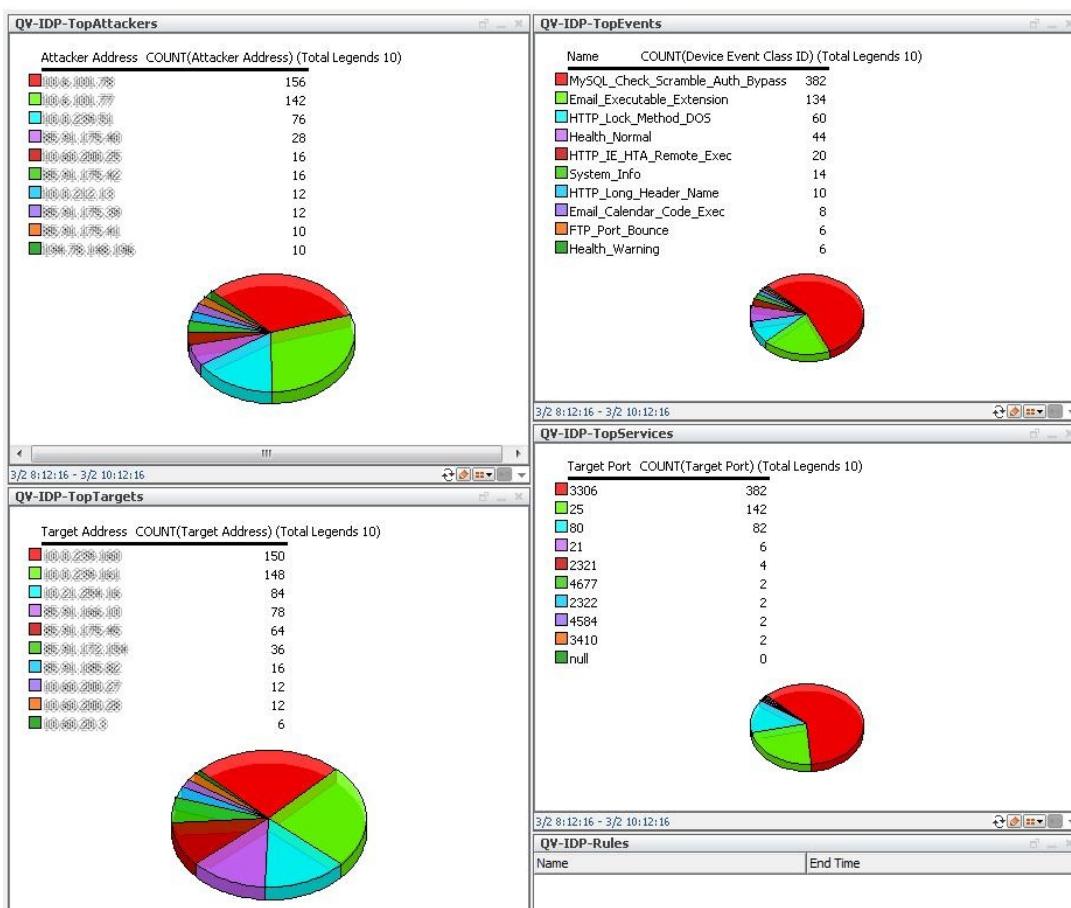
---

- Top-10
- Events
- Actuele aanvallen
- Statistieken



PAM - SIEM  
 Bob Lannoy & Kristof Verslype - Onderzoek

85



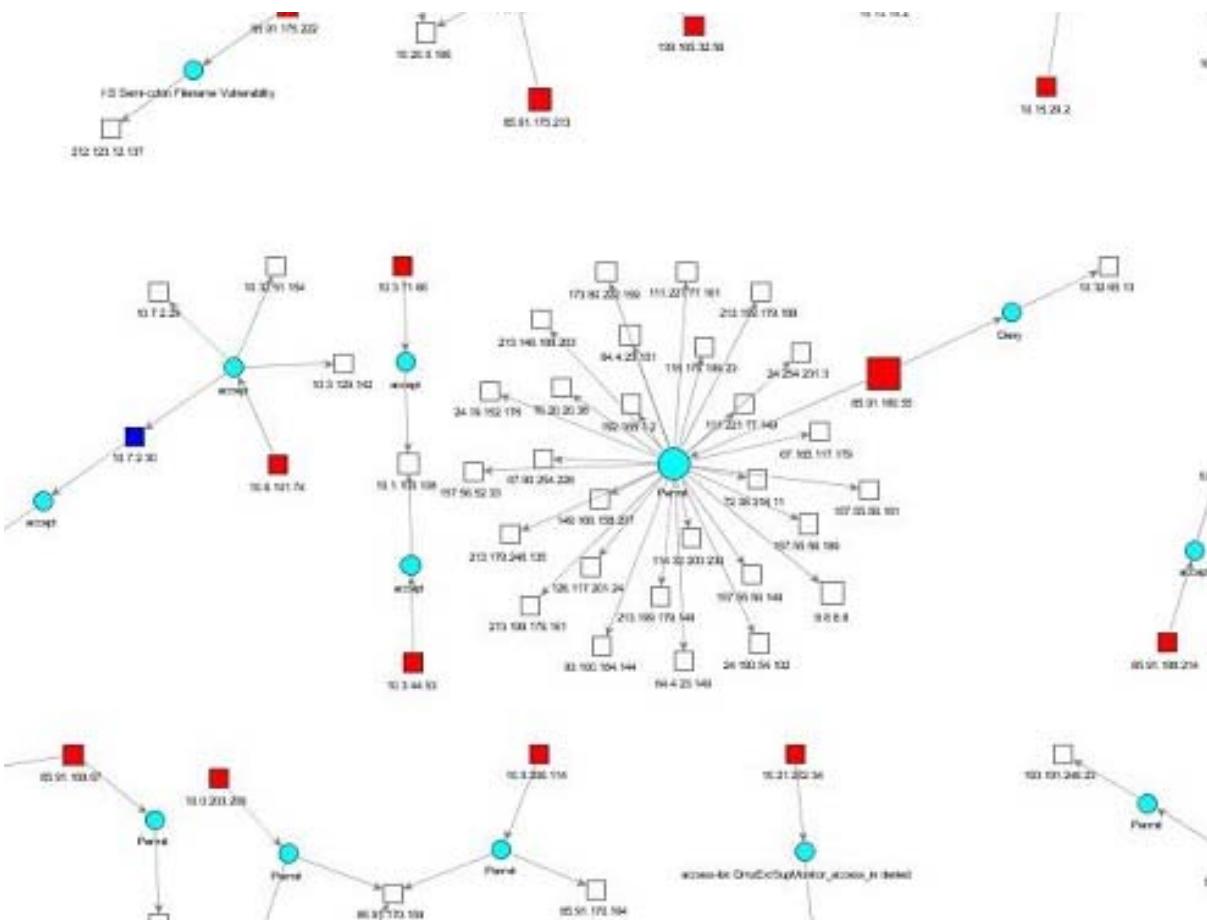
86

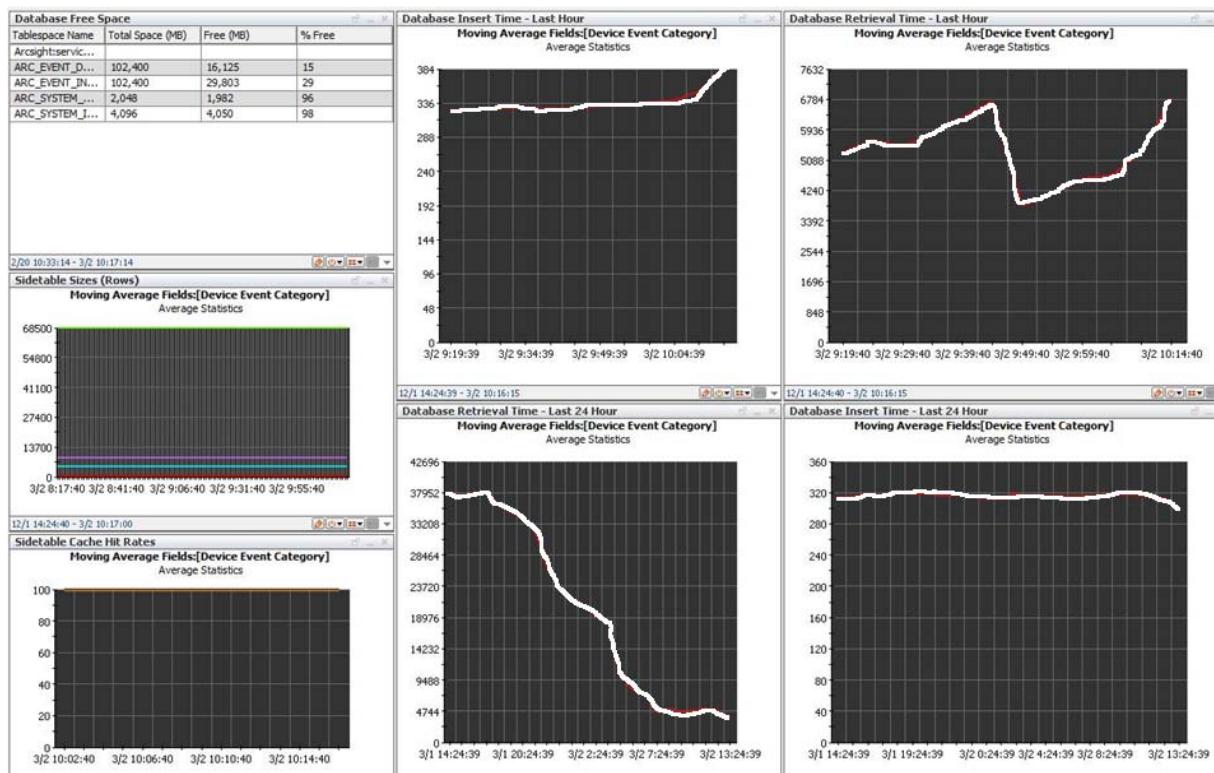
Start Time: 2 Mar 2012 09:43:47 CET  
 End Time: 2 Mar 2012 11:43:47 CET  
 Filter: Agent ID = "IBM SiteProtector"  
 Inline Filter: No Filter  
 Verified Rules: No Rule

Very High: 2  
 High: 237  
 Medium: 1,430  
 Low: 56  
 Very Low: 0

### Radar

Manager Receipt Time ↑	End Time ↓	Name ↓	Attacker Address ↓	Target Address ↓	Priority ↓
2 Mar 2012 10:04:44 CET	2 Mar 2012 10:13:14 CET	MySQL_Check_Scramble_Auth_Bypass	0.21.284.22	10.20.16.28	9
2 Mar 2012 10:04:44 CET	2 Mar 2012 10:13:14 CET	MySQL_Check_Scramble_Auth_Bypass	0.21.284.22	10.20.16.28	9
2 Mar 2012 10:04:44 CET	2 Mar 2012 10:13:20 CET	TCP_Port_Scan	0.20.0.129	10.20.0.122	5
2 Mar 2012 10:04:44 CET	2 Mar 2012 10:13:19 CET	TCP_Port_Scan	0.20.0.128	10.20.0.122	5
2 Mar 2012 10:04:44 CET	2 Mar 2012 10:12:18 CET	TCP_Port_Scan	0.20.0.129	10.20.0.122	5
2 Mar 2012 10:04:29 CET	2 Mar 2012 10:11:53 CET	TCP_Port_Scan	0.20.0.129	10.20.0.121	5
2 Mar 2012 10:04:29 CET	2 Mar 2012 10:12:55 CET	TCP_Port_Scan	0.20.0.129	10.20.0.121	5
2 Mar 2012 10:04:29 CET	2 Mar 2012 10:12:57 CET	TCP_Port_Scan	0.20.0.128	10.20.0.122	5
2 Mar 2012 10:04:29 CET	2 Mar 2012 10:11:58 CET	TCP_Port_Scan	0.20.0.128	10.20.0.121	5
2 Mar 2012 10:04:29 CET	2 Mar 2012 10:11:55 CET	TCP_Port_Scan	0.20.0.128	10.20.0.122	5
2 Mar 2012 10:04:29 CET	2 Mar 2012 10:11:58 CET	TCP_Port_Scan	0.20.0.129	10.20.0.121	5
2 Mar 2012 10:04:29 CET	2 Mar 2012 10:13:01 CET	TCP_Port_Scan	0.20.0.129	10.20.0.121	5
2 Mar 2012 10:04:29 CET	2 Mar 2012 10:12:59 CET	TCP_Port_Scan	0.20.0.128	10.20.0.121	5
2 Mar 2012 10:03:49 CET	2 Mar 2012 10:11:15 CET	TCP_Port_Scan	0.20.0.129	10.20.0.122	5
2 Mar 2012 10:03:49 CET	2 Mar 2012 10:12:17 CET	TCP_Port_Scan	0.20.0.129	10.20.0.122	5
2 Mar 2012 10:03:49 CET	2 Mar 2012 10:12:18 CET	TCP_Port_Scan	0.20.0.128	10.20.0.121	5
2 Mar 2012 10:03:49 CET	2 Mar 2012 10:12:18 CET	TCP_Port_Scan	0.20.0.129	10.20.0.122	5
2 Mar 2012 10:03:34 CET	2 Mar 2012 10:12:04 CET	TCP_Port_Scan	0.20.185.246.28	10.20.146.7	5
2 Mar 2012 10:03:29 CET	2 Mar 2012 10:12:11 CET	Connector Raw Event Statistics			3
2 Mar 2012 10:03:29 CET	2 Mar 2012 10:10:51 CET	TCP_Port_Scan	0.20.0.129	10.20.0.121	5
2 Mar 2012 10:03:29 CET	2 Mar 2012 10:11:53 CET	TCP_Port_Scan	0.20.0.129	10.20.0.121	5
2 Mar 2012 10:03:29 CET	2 Mar 2012 10:10:56 CET	TCP_Port_Scan	0.20.0.128	10.20.0.121	5
2 Mar 2012 10:03:29 CET	2 Mar 2012 10:10:53 CET	TCP_Port_Scan	0.20.0.128	10.20.0.122	5
2 Mar 2012 10:03:29 CET	2 Mar 2012 10:10:56 CET	TCP_Port_Scan	0.20.0.129	10.20.0.121	5
2 Mar 2012 10:03:29 CET	2 Mar 2012 10:11:54 CET	TCP_Port_Scan	0.20.0.129	10.20.0.122	5





## Functionaliteit (1/2)



### Real-Time monitoring

- Aanpasbaar window (vb. 2u)
- 'Near-time' -> 2 à 5 min.



### Reactie

- Triggeren zelf geschreven scripts
- Risico's!



### Backup

- Standaard enkel inzelfde ESM
- NAS kan



## Functionaliteit (2/2)



### Asset management

- Import tool (kan beter)
- Momenteel nog veel manueel werk



### User management

- Toegangsrechten
- Gepersonaliseerde rapporten
- Gepersonaliseerde dashboards



### Filteren

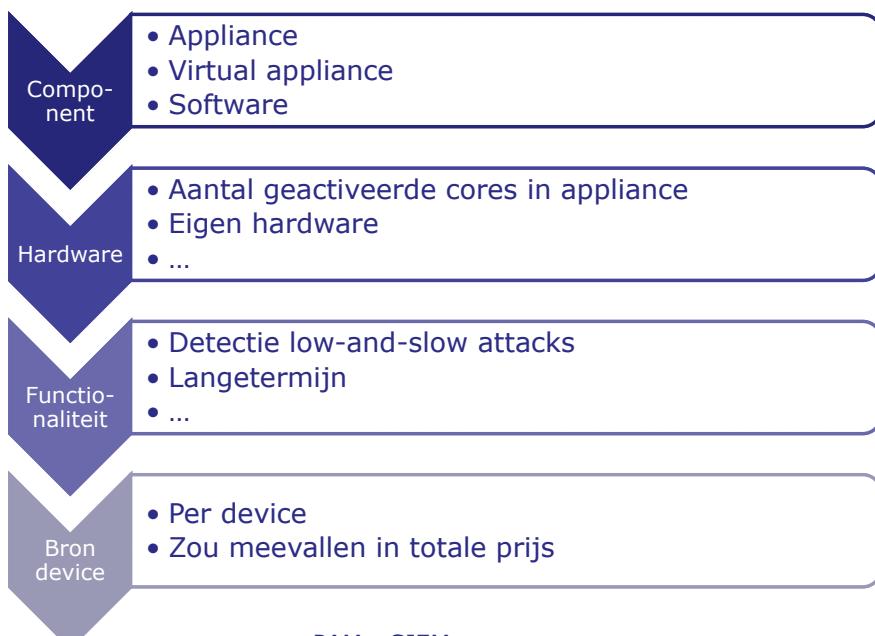
- |                     |               |
|---------------------|---------------|
| • Device            | -> connector? |
| • Connector, logger | -> ESM?       |
| • ESM               | -> Archief?   |
| • Dashboard         | -> user?      |



PAM - SIEM  
 Bob Lannoy & Kristof Verslype - Onderzoek

91

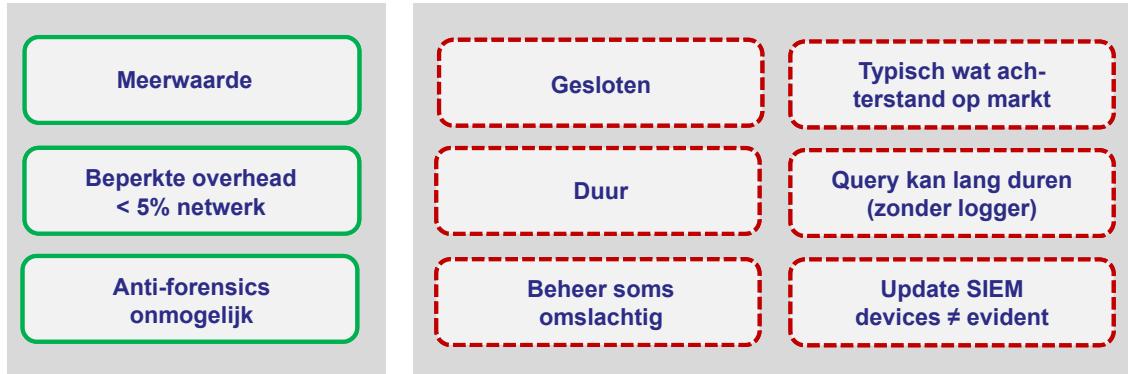
## Kostenmodel



PAM - SIEM  
 Bob Lannoy & Kristof Verslype - Onderzoek

92

## Ervaringen



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

93

# Managed SIEM

## SIEM



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

95

## Managed Siem



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

96

## Pro's & cons

Quasi geen investeringskosten	SIEM Expertise	Outsourcen Security
Minder onderhoud	Grotere security intelligence	Afhankelijkheid Internet
Schaalbaarheid	Escalatie naar andere bedrijven	Beperktere functionaliteit
24/7/365 monitoring		Beperktere HW/SW



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

97



## Managed Security Services

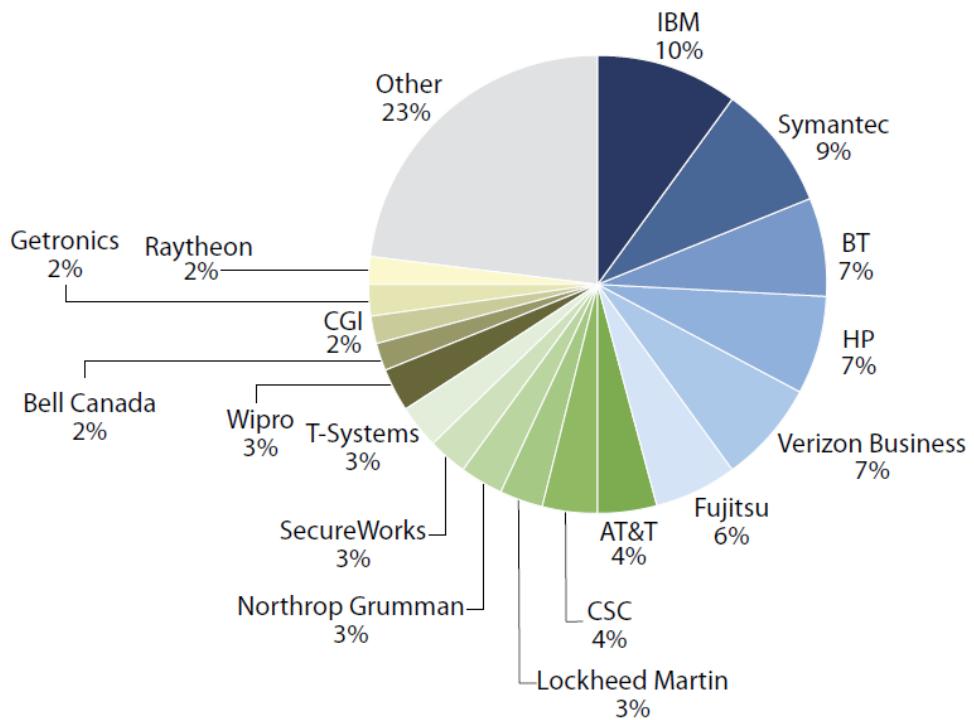
Company managed	Co-managed	Provider managed
<input checked="" type="checkbox"/> Bedrijf beheert eigen SIEM	<input checked="" type="checkbox"/> Provider beheert SIEM in bedrijf	<input checked="" type="checkbox"/> Logs -> provider
<input checked="" type="checkbox"/> Monitoring & escalatie door bedrijf	<input checked="" type="checkbox"/> Monitoring & escalatie door provider	<input checked="" type="checkbox"/> Monitoring & escalatie door provider
<input checked="" type="checkbox"/> Ondersteuning door provider	<input checked="" type="checkbox"/> [Provider beheert deel hardware]	<input checked="" type="checkbox"/> [Provider beheert deel hardware]
	<input checked="" type="checkbox"/> Switch company managed kan	



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

98

## Market Share Of Top Managed Security Services Providers



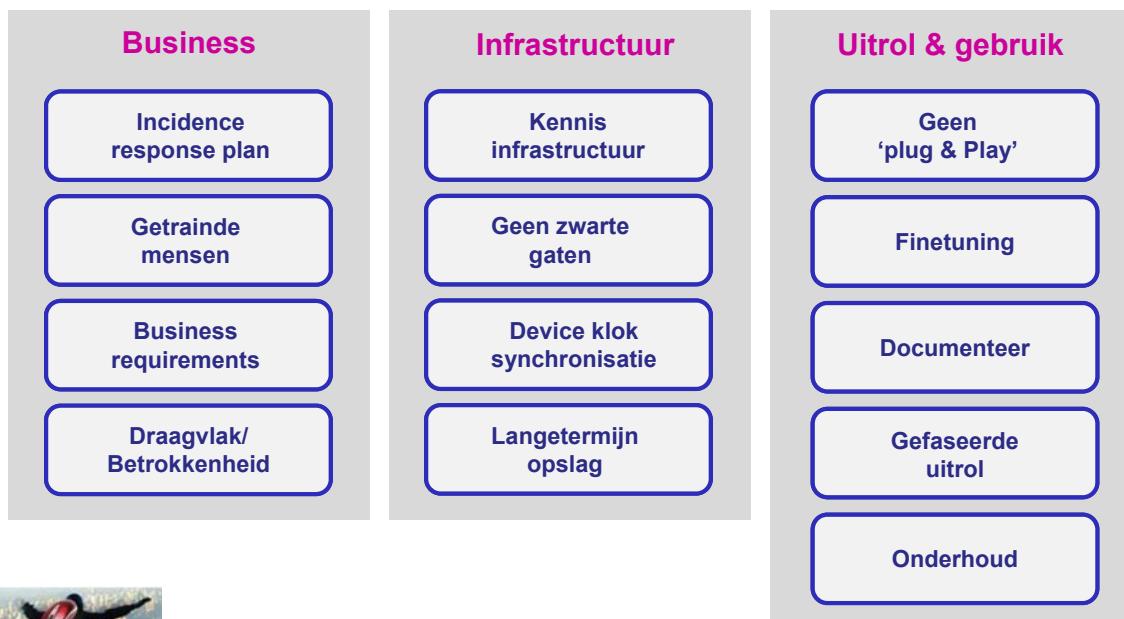
Source: Forrester estimate based on information provided by managed security service providers

2010

Source: Forrester Research, Inc.

# Tot slot

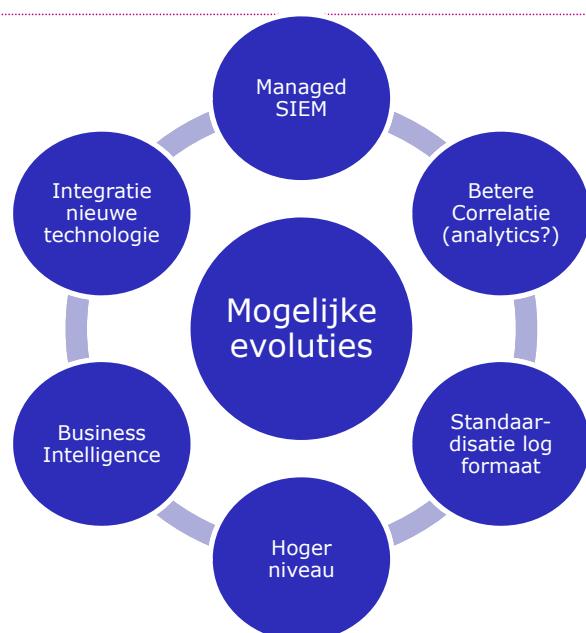
## Aandachtspunten



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

101

## Mogelijke evoluties



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

102

## Te onthouden

### SIEM is een P R O J E C T

-  Eerste goede security
-  Goede voorbereiding Technisch / MENSEN
-  Uitrol vergt tijd => 12-18 maand
-  SIEM in productie: onderhoud

### Gratis kennismaking

-  AlienVault
-  Weinig intrusief
-  Beperktere functionaliteit

Correlatieregels!



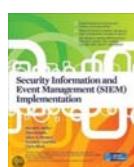
PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

103

## Literatuur



**2011 Data Breach Investigations Report**  
*Verizon*  
2011



**Security Information and Event Management (SIEM) Implementation**  
*Miller, Harris, Harper, VanDyke, Blask*  
10/2010



**Security Information and Event Management: Business Benefits and Security, Governance and Assurance Perspectives**  
*ISACA*  
12/2010



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

104

## Vragen



### Met dank aan

Bart Maes  
Marc Vael  
Johan Costrop  
David Tillemans  
Michel Brouyère

**kristof.verslype@smals.be**

Smals Onderzoek



PAM - SIEM

Bob Lannoy & Kristof Verslype - Onderzoek

105

## Referenties

### Publicaties Onderzoek

- "Authentification et signature digitale: concepts, techniques et applications internet", M. Laloy, 03/2001
- "Gebruikers- en toegangsbeheer", B. Lannoy, 10/2005
- "Beveiligde uitwisseling van gegevens", M. Laloy, 05/2007
- "Desktop Single Sign-On / Enterprise Single Sign-On" B. Lannoy, 07/2007
- "TrueCrypt v.5.1a - On-the-fly disk encryption software", P. Jorissen, 05/2008
- "Bescherming van de interne gegevens", P. Jorissen, 02/2009
- "La sécurisation des supports de données", T. Baignères, 05/2010
- "Gestion des certificats digitaux et méthodes alternatives de chiffrement", J. Cathalo, 05/2011



PAM - SIEM

Bob Lannoy & Kristof Verslype - Onderzoek

106

# Demo PAM

## Sudo commando

```
[normuser@ltsmapam001b ~]$ whoami
normuser
[normuser@ltsmapam001b ~]$ tail -f /var/log/messages
tail: cannot open '/var/log/messages' for reading: Permission denied
[normuser@ltsmapam001b ~]$ tail -f /var/log/secure
tail: cannot open '/var/log/secure' for reading: Permission denied
[normuser@ltsmapam001b ~]$ sudo tail -f /var/log/messages
Jan 12 15:15:01 ltsmapam001b ntpd[29899]: Listening on interface #3 eth1, fe80::250:56ff:fe8a:170#123 Enabled
Jan 12 15:15:01 ltsmapam001b ntpd[29899]: Listening on interface #4 lo, ::1#123 Enabled
Jan 12 15:15:01 ltsmapam001b ntpd[29899]: Listening on interface #5 eth0, fe80::250:56ff:fe8a:16f#123 Enabled
Jan 12 15:15:01 ltsmapam001b ntpd[29899]: Listening on interface #6 lo, 127.0.0.1#123 Enabled
Jan 12 15:15:01 ltsmapam001b ntpd[29899]: Listening on interface #7 eth0, 10.6.1.01#123 Enabled
Jan 12 15:15:01 ltsmapam001b ntpd[29899]: Listening on interface #8 eth1, 10.32.80.177#123 Enabled
Jan 12 15:15:01 ltsmapam001b ntpd[29899]: Listening on interface #9 eth2, 10.32.84.177#123 Enabled
Jan 12 15:15:01 ltsmapam001b ntpd[29899]: Listening on routing socket on fd #26 for interface updates
Jan 12 15:15:01 ltsmapam001b ntpd[29899]: kernel time sync status 2040
Jan 12 15:15:01 ltsmapam001b ntpd[29899]: frequency initialized 19.588 PPM from /var/lib/ntp/drift
^C[normuser@ltsmapam001b ~]$ sudo tail -f /var/log/secure
[sudo] password for normuser:
Sorry, user normuser is not allowed to execute '/usr/bin/tail -f /var/log/secure'
as root on ltsmapam001b.smals-mvm.be.
[normuser@ltsmapam001b ~]$
```

## Sudo configuratie (sudoers)

```
# runas_alias --
# host_alias --
# cmnd_alias --
Cmnd_Alias CHECKRAIDCONF = /home/confmon/raidinfo/
Cmnd_Alias SHELLS = /bin/sh,/bin/bash,/bin/ash,/bin/bsh,/bin/ksh,/usr/bin/ksh,/u
sr/bin/pdksh,/bin/tcsh,/bin/csh
Cmnd_Alias SU = /bin/su
Cmnd_Alias CHECKSYSLOGS = /bin/cat /var/log/messages,/usr/bin/tail -f /var/log/m
essages
Cmnd_Alias REBOOT = /sbin/halt,/sbin/shutdown,/sbin/reboot,/sbin/init,/sbin/teli
nit
Cmnd_Alias PROCESSMGMT = /bin/kill
Cmnd_Alias SERVICEMGMT = /etc/init.d/
Cmnd_Alias TESTCMD = /bin/vi, /opt/scripts/testsudo.sh

Defaults:normuser log_input,log_output
# user_spec --
%confmon ALL = NOPASSWD: CHECKRAIDCONF
%operators ALL=<ALL> NOPASSWD: CHECKSYSLOGS, REBOOT, PROCESSMGMT, SERVICEMGMT
%localadmins ALL=<ALL> NOPASSWD: ALL
root ALL=<ALL> ALL
wheel ALL=<ALL> NOPASSWD: ALL
%ltsmapam001b-admins ALL=<ALL> NOPASSWD: ALL
%linux-admins ALL=<ALL> NOPASSWD: ALL
%ltsmapam001b-operators ALL=<ALL> NOPASSWD: CHECKSYSLOGS, REBOOT, PROCESSMGMT, S
ERVICEMGMT
%linux-operators ALL=<ALL> NOPASSWD: CHECKSYSLOGS, REBOOT, PROCESSMGMT, SERVICEM
GMT
%weblogic ALL=<weblogic> NOPASSWD: ALL
normuser ALL=<ALL> NOPASSWD: CHECKSYSLOGS
normuser ALL=<ALL> NOPASSWD: TESTCMD
#normuser ALL=<ALL> NOPASSWD: TESTCMD, NOEXEC: TESTCMD
```

## Sudo – shell escaping & noexec

```
root [root@ltsmapam001b normuser]# tail /var/log/secure
Jan 12 15:12:47 ltsmapam001b sudo: normuser : command not allowed ; TTY=pts/3 ;
PWD=/home/normuser ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/secure
Jan 12 15:13:34 ltsmapam001b sudo: normuser : TTY=pts/3 ; PWD=/home/normuser ; U
SER=root ; TSID=000002 ; COMMAND=/bin/vi
Jan 12 15:15:08 ltsmapam001b sudo: normuser : TTY=pts/3 ; PWD=/home/normuser ; U
SER=root ; TSID=000001 ; COMMAND=/usr/bin/tail -f /var/log/messages
Jan 12 15:15:39 ltsmapam001b sudo: pam_succeed_if(sudo:auth): requirement "user
= root" not met by user "normuser"
Jan 12 15:15:39 ltsmapam001b sudo: pam_succeed_if(sudo:auth): requirement "user
ingroup rusers" not met by user "normuser"
Jan 12 15:15:39 ltsmapam001b sudo: pam_succeed_if(sudo:auth): requirement "user
notingroup ldap-rusers" was met by user "normuser"
Jan 12 15:15:43 ltsmapam001b sudo: pam_sss(sudo:account): Access denied for user
normuser: 10 <User not known to the underlying authentication module>
Jan 12 15:15:43 ltsmapam001b sudo: normuser : command not allowed ; TTY=pts/3 ;
PWD=/home/normuser ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/secure
Jan 12 15:16:40 ltsmapam001b sudo: normuser : TTY=pts/3 ; PWD=/home/normuser ; U
SER=root ; TSID=000002 ; COMMAND=/opt/scripts/testsudo.sh
Jan 12 15:17:22 ltsmapam001b sudo: normuser : TTY=pts/3 ; PWD=/home/normuser ; U
SER=root ; TSID=000003 ; COMMAND=/bin/vi
[root@ltsmapam001b normuser]# exit
exit
[normuser@ltsmapam001b ~]$ sudo /bin/vi
```

```
Cannot execute shell /bin/bash
```

```
Cannot execute shell /bin/bash
[normuser@ltsmapam001b ~]$ sudo /opt/scripts/testsudo.sh
/opt/scripts/testsudo.sh: line 2: /usr/bin/tail: Permission denied
[normuser@ltsmapam001b ~]$
```

## PAM-tool web-login



## Wachtwoord opties & tonen wachtwoord

A screenshot of the Cyber-Ark Privileged Identity Management account management interface. The left sidebar shows "Views" like "Account Views" (Favorites, Recently, Locked accounts, New accounts) and "Requests Views" (My Requests, Incoming Requests). The main area displays a "Favorites" table with columns: User Name, Address, Safe, Policy ID, and several icons. A "Show Password" dialog box is overlaid on the screen, containing the password "QpLl2Ob]" in a text field with a "Copy" button next to it. The dialog also has a timer at the bottom stating "Window will be closed in: 2 seconds" and a "Close" button. The entire "Show Password" dialog and its surrounding area are highlighted with a red rectangle. The top right of the main interface shows a user "normal" and a "Logout" link.

## Integratie lokale software (Tunnelier) (1/2)

The screenshot shows the CyberArk Privileged Identity Management interface. In the center, there is a table titled 'Favorites' listing accounts: CYBERARK (User Name: CYBERARK, Address: Itsmapam001a, Safe: database, Policy ID: Oracle), cyberark (User Name: cyberark, Address: Itsmapam001b, Safe: unix, Policy ID: UnixSSH), and bl (User Name: bl, Address: wtsmapam001a, Safe: windows, Policy ID: WinServerLocal). A context menu is open over the 'bl' account, with the 'Tunnelier' option highlighted and enclosed in a red box. The menu also includes options like 'RDP', 'Remove from Favorites', 'Add to Cart', 'Display account usages', and 'Display failed account usages'.

## Integratie lokale software (Tunnelier) (2/2)

The screenshot shows a Windows desktop environment. In the foreground, a 'Bitvise Tunnelier - Itsmapam001a.tlp - wtsmapam001a:22' window is open, displaying a log of a successful connection attempt. The log entries include:

- 10:14:01.558 Connected.
- 10:14:01.562 Starting first key exchange.
- 10:14:01.562 Server version string: SSH-2.0-1.04 FlowSsh: WinSSHD 5.15
- 10:14:01.593 New host key received. Algorithm: ssh-dss, Size: 1024 bits, MD5 Fingerprint: 2ae1:f5:9e:a9:91:b6:eb:d0:2f:8d:19:fd:42:88:75, Bubble-Bobble: xulok-baguc-rides-vituk-nisut-nihem-silo-fkyvu-sygot-tfet-glux.
- 10:14:01.602 First key exchange completed.
- 10:14:01.602 Key exchange: diffie-hellman-group14-sha1. Session encryption: aes256-ctr, MAC: hmac-sha1, compression: none.
- 10:14:01.606 Attempting 'password' authentication.
- 10:14:01.612 Authentication completed.
- 10:14:01.613 Auto opening Remote Desktop session.
- 10:14:01.614 Listening for Remote Desktop client-2-server connection on 127.0.0.1:47657 succeeded.
- 10:14:01.650 Remote Desktop Connection launched successfully.
- 10:14:02.031 Accepted Remote Desktop client-2-server connection from 127.0.0.1:63173 to 127.0.0.1:3389.

In the background, the Windows Server Manager is visible, showing the 'Event Viewer' node under 'Diagnostics'.

## Workflow (1/2)

**Connect with Account**

You are required to specify a reason for this operation:

**Request Timeframe**

Access is required:  
From: 12/01/2012 08:00 To: 14/01/2012 17:00 GMT+01:00  
 Multiple access is required during this period

**Confirmation**

Operation: Retrieve password Unix via SSH-cyberark-ltsmapam001b  
Status: 1 user(s) must confirm the request

OK Cancel

**Access Requests**

Search: Leave empty to search all Go

Back Confirm Reject

**Request Details**

**Details**  
Status: Request is waiting: 1 more user(s) must confirm the request  
Requested on: 12/01/2012 09:51:01  
Requestor: normal  
Operation: Retrieve password Unix via SSH-cyberark-ltsmapam00...  
Safe name: unix  
Reason: (ConnectionClient=PuTTY) Maintenance  
Access Type: Single operation  
Authorization required from  
Administrator  
bob

**Account Details - Unix via SSH-cyberark-ltsmapam...**

Policy ID:	Unix via SSH
Device Type:	Operating System
Safe:	unix
Name:	Operating System-UnixSSH-ltsmapam001b-bl
Last verified:	13/12/2011 09:10:34
Last modified:	PasswordManager (11/01/2012 17:37:48)
Last used:	normal (12/01/2012 09:43:28)
User Name:	cyberark
Address:	ltsmapam001b

**Authorize Access**  
Reason: Authorized

Confirm Reject

Confirm the request

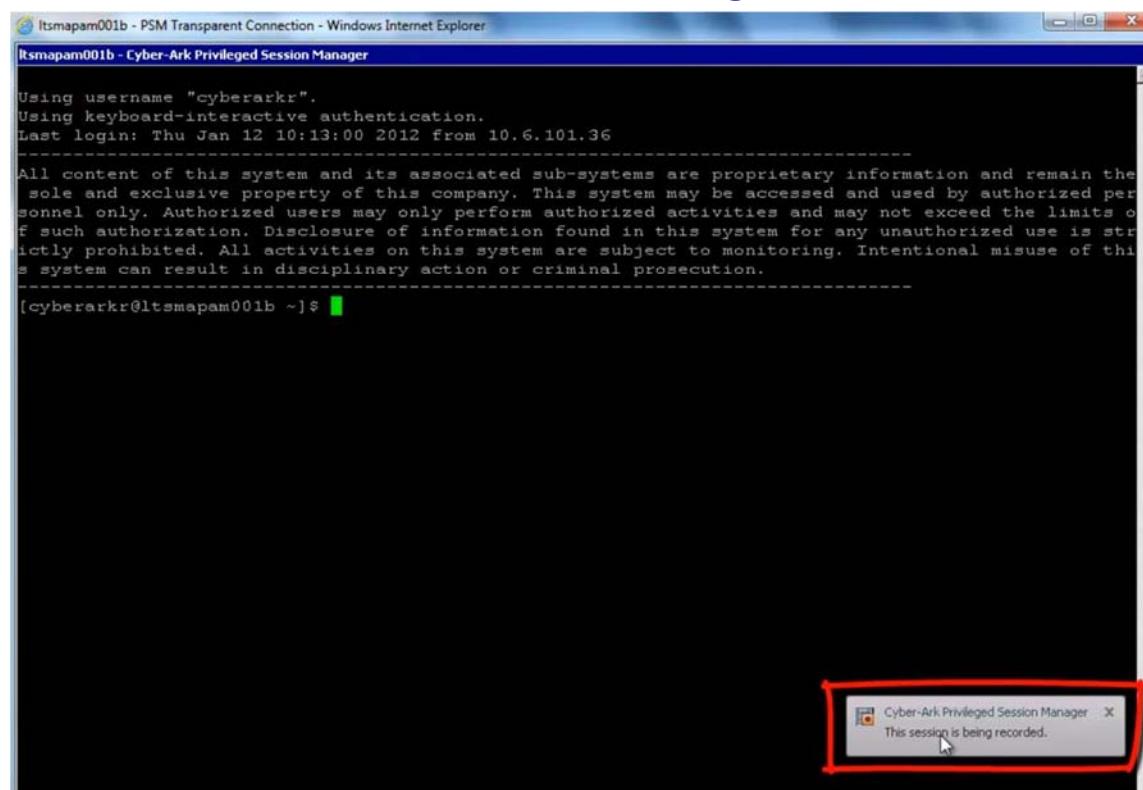
Copyright © 2000-2012 CyberArk Software, Ltd. All Rights Reserved.

## Account - detailscherm

The screenshot shows the Cyber-Ark Privileged Identity Management interface. The top navigation bar includes the logo and links for 'About' and 'Logoff'. Below the header, a toolbar with icons for 'Change', 'Reconcile', 'Verify', 'Send Link', and 'Refresh' is visible. The main content area is titled 'Account Details: Unix via SSH-cyberark-ltsmapam001b'. On the left, there's a form with fields for 'Password' (containing '\*\*\*\*\*') and 'PutTY' (selected in a dropdown). Buttons for 'Show', 'Copy', and 'Connect' are present. To the right, tabs for 'CPM', 'Activities', and 'Versions' are shown, with 'CPM' selected. Under 'Logon Account', it says 'Reconcile Account: Unix record-cyberark-ltsmapam'. Under 'Account Group', 'Group:' is set to '[None]'. Below the tabs, detailed account information is listed:

Policy ID:	Unix via SSH
Device Type:	Operating System
Safe:	unix
Name:	Operating System-UnixSSH-ltsmapam001b-bl
Last verified:	13/12/2011 09:10:34
Last modified:	PasswordManager (11/01/2012 17:37:48)
Last used:	normal (12/01/2012 09:43:28)
User Name:	cyberark
Address:	ltsmapam001b

## Session recording



## Session recording – search/keystrokes/video

The screenshot shows a software interface for managing session recordings. At the top, there is a search bar with the text "Search recordings: All recordings, session contains: passwd". Below the search bar is a table with columns: User, Account User Name, Account Address, Account Policy ID, Start, Duration, Vid..., and three icons. One row in the table is highlighted with a red border, showing "normal" as the user, "cyberarkr" as the account name, "itsmapam001b" as the account address, "UnixSSHRecord" as the account policy, and a timestamp of "12/01/2012 11:08:54". The duration is "00:00:31" and the file size is "36KB". Below the table is a section titled "Keystrokes" with a single entry: "# 1 cat /etc/passwd". A mouse cursor is hovering over the "cat /etc/passwd" entry. To the right of the keystroke list is a video player window titled "Raspiagent01 - CyberArk Pivileged Session Manager". The video player displays a terminal session with the command "cat /etc/passwd" being run. The terminal output lists various system users and their details. A red arrow points from the "cat /etc/passwd" entry in the keystroke list down to the corresponding line in the terminal output.

## Applicatie integratie

### Datasources

Application that uses WebLogic datasource. The WebLogic JDBC data source uses a plugin to get the Oracle Db password.

[Go to Datasource application](#)

### Application - Protected keystore

An application requests the password of a local Java keystore from the Vault in order to be able to open it.

[Go to Keystore application](#)

## Applicatie integratie – weblogic datasource (1/2)

The screenshot shows the Oracle WebLogic Server Administration Console. The left sidebar displays the 'Domain Structure' for the 'Cyberarkdomain'. Under the 'Services' section, the 'JDBC' category is expanded, showing 'Data Sources', 'Multi Data Sources', 'Data Source Factories', and other options like 'Persistent Stores' and 'Foreign JNDI Providers'. The main panel is titled 'Settings for db.database.cyberark' and shows the 'Notes' tab selected. A note is present with the text:  
Query>Safe=database;Folder=root;  
Object=oracle

## Applicatie integratie – weblogic datasource (2/2)

The screenshot shows the Cyber-Ark Privileged Identity Management interface. The top navigation bar includes 'Accounts' and the date '13/01/2012 | About'. Below the navigation is a toolbar with icons for Edit, Change, Verify, Delete, Move, Send Link, and Refresh. The main area displays 'Account Details: Oracle-CYBERARK-Itsmapam001a'. The account details include:  
Policy ID: Oracle  
Device Type: Database  
Safe: database  
Name: oracle  
Last verified: 13/12/2011 13:32:56  
Last modified: PasswordManager (13/01/2012 13:17:04)  
Last used: bobl (13/01/2012 13:16:31)  
User Name: CYBERARK  
Database: TPAM1  
Port: 2003  
Address: Itsmapam001a

To the right, there is a 'Reconcile Account' section with tabs for CPM, Activities, and Recovery. It shows the 'Account Group' is set to '[None]'. There is also a 'Reconcile Now' button.

## Applicatie integratie – Java API

```
    @see javax.servlet.http.HttpServlet#doGet(javax.servlet.http.HttpServlet)
    /
    @Override
    protected void doGet(HttpServletRequest req, HttpServletResponse resp) throws
        PrintWriter out = new PrintWriter(resp.getOutputStream());
        PSDKPassword password = null;
    try {
        PSDKPasswordRequest passRequest = new PSDKPasswordRequest ();

        passRequest.setAppID ("KeyStoreServlet");
        passRequest.setSafe ("apps");
        passRequest.setFolder ("root");
        passRequest.setObject ("IntegrationsoakKS");
        passRequest.setReason ("Keystore test");
        // Sending the request to get the password
        password = javapasswordsdk.PasswordSDK.getPassword (passRequest);
        // Analyzing the response
        //out.println ("The password content is : " + password);
        //out.println ("The password Address is : " + password);
        //out.println ("The password keystore path is : " + password);
    }
    catch (PSDKEException ex)
```

## Applicatie integratie - authentication

The screenshot shows the Oracle Database Control interface with the 'Authentication' tab selected. There are three entries listed:

- Type: Hash (1 item)  
Value: A0A4E55D657D02B8433C9B12C8B4065C05992068
- Type: OS User (1 item)  
Value: weblogic
- Type: Path (1 item)  
Value: /bea/user\_projects/domains/Cyberarkdomain/servers/AdminS... (with a cursor pointing at it)

## Wachtwoordbeheer via logon-account

The screenshot shows the Cyber-Ark Privileged Identity Management interface. The title bar reads "Cyber-Ark® Privileged Identity Management". The top navigation bar includes links for "About", "Logoff bob!", "Search", and "Go". The main menu bar has tabs for "Accounts", "Edit", "Change", "Reconcile", "Verify", "Delete", "Move", "Send Link", "Refresh", "Add Account", and "Customize". Below the menu is a toolbar with icons for "New", "Edit", "Change", "Reconcile", "Verify", "Delete", "Move", "Send Link", and "Refresh". The main content area displays "Account Details: Keystore". On the left, there is a password field with "\*\*\*\*\*" and buttons for "Show" and "Copy". To the right of the password field are buttons for "Connect" and "Copy Shortcut". Below this are several status fields:

- Policy ID: Keystore
- Device Type: Special
- Safe: apps
- Name: IntegrationsoaKS
- Last verified: N/A
- Last modified: bobl (13/01/2012 13:49:10)
- Last used: bobl (13/01/2012 13:49:10)
- KeyStoreName: /tmp/integrationsoa.jks

On the right side of the screen, there is a "CPM" tab selected, followed by "Activities", "Recordings", "Versions", and "Advanced". Under the "CPM" tab, there is a section titled "Logon Account" which contains the text "Unix via SSH-cyberark-ltsmapam001b". This section is highlighted with a red border. Below this is a "Account Group" section with a "Group" dropdown set to "[None]" and buttons for "Modify" and "Create New". At the bottom of the interface, a copyright notice reads "Copyright © 1999-2011 Cyber-Ark® Software, Ltd. All Rights Reserved."