



## 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.

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 erase a "server graveyard" of malicious software script designed to permanently destroy millions of dollars worth of data from all 4,000 servers operated by the mortgage giant.

### Fired techie created virtual chaos at pharma company

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



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

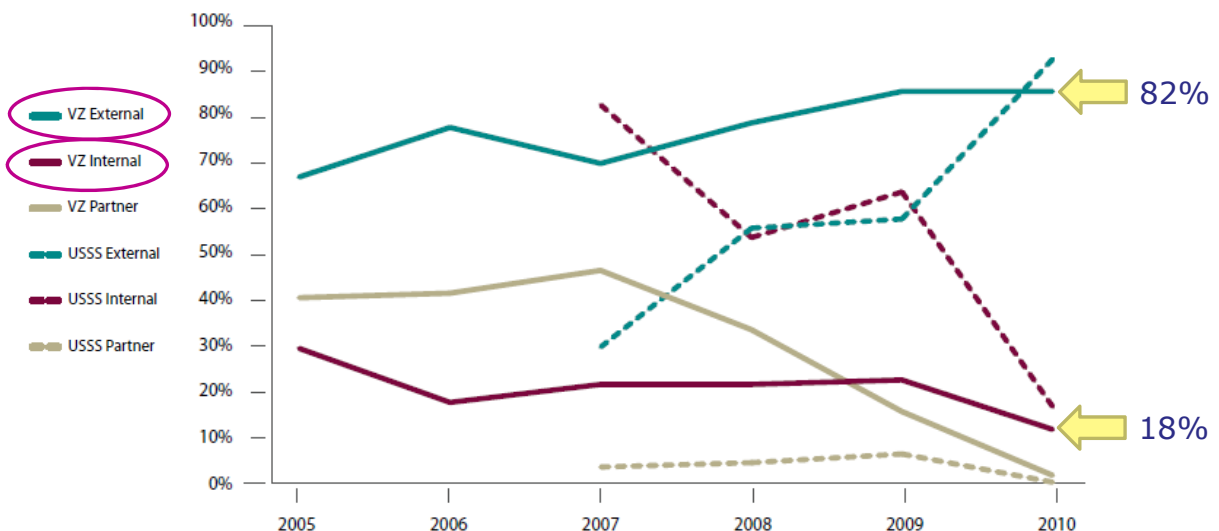
The investigation into the biggest leak in US military history centres on a US Army intelligence analyst who allegedly boasted online that he was going to reveal "the truth" about the war in Afghanistan.



ANONYMOUS  
3

PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

## Beveiligingsincidenten Statistieken (1/4)



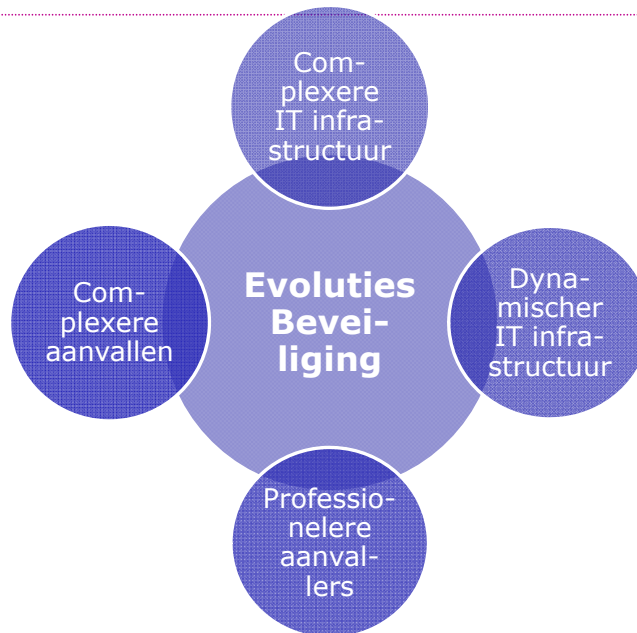
Verizon data breach report 2011



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek



## Information security trends (1/3)

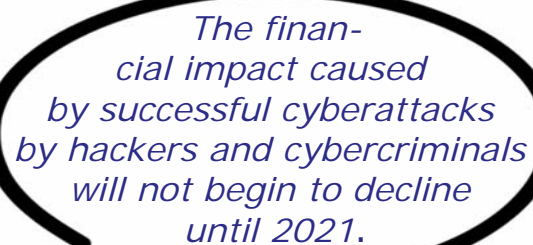


PAM - SIEM

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.*



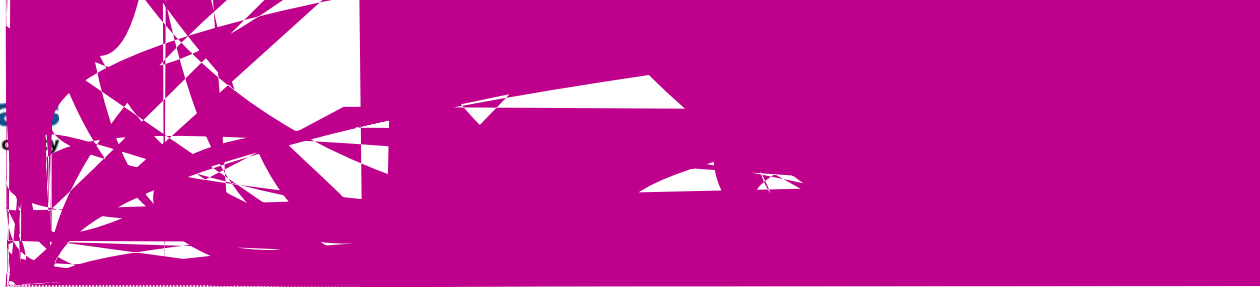
**Gartner.** (29 november 2011)



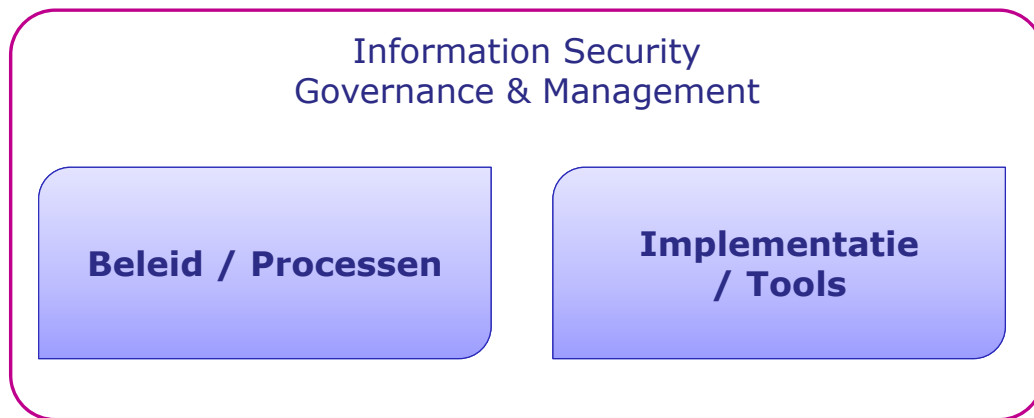
PAM - SIEM

Bob Lannoy & Kristof Verslype - Onderzoek

8



## Information Security Governance Aanpak (1/2)



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

11

## Information Security Governance Aanpak (2/2)



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

12

# Information Security Governance

## Technische veiligheidsmaatregelen (1/4)

---



### Beheer van gebruikers & rechten

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



PAM - SIEM

Bob Lannoy & Kristof Verslype - Onderzoek

## Inform Techni



A, A2A

PAM - SIEM  
oy & Kristof Verslype - Onc

Security  
ligheid

## 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
  - Al 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

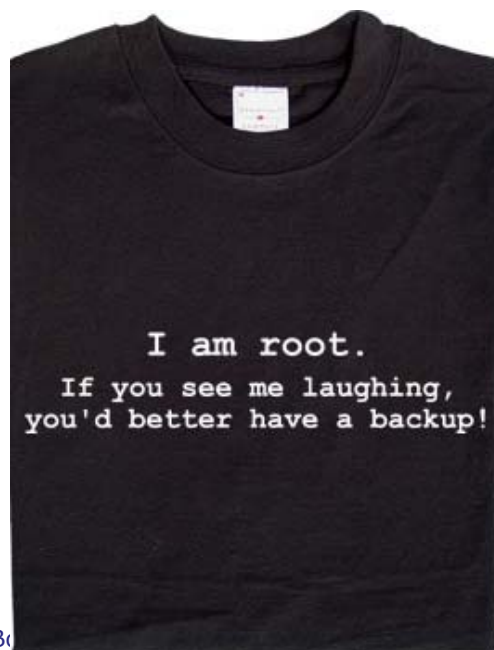


PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

19

## Wat is "Privileged account management"?

---

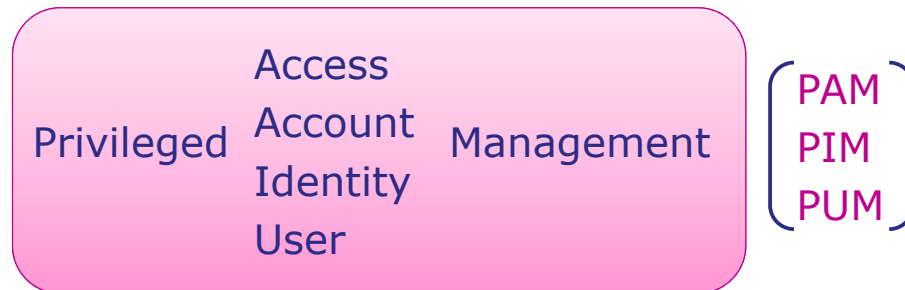


Bo

20

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

---



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



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

---

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



## 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



PAM - SIEM

Bob Lannoy & Kristof Verslype - Onderzoek

23

## 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, ...



PAM - SIEM

Bob Lannoy & Kristof Verslype - Onderzoek

24

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

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



## Wat is "Privileged account management"? Activity

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



## 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



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

---

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



by over the  
Measurement

ject

c

## 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



LIEBERMAN SOFTWARE™



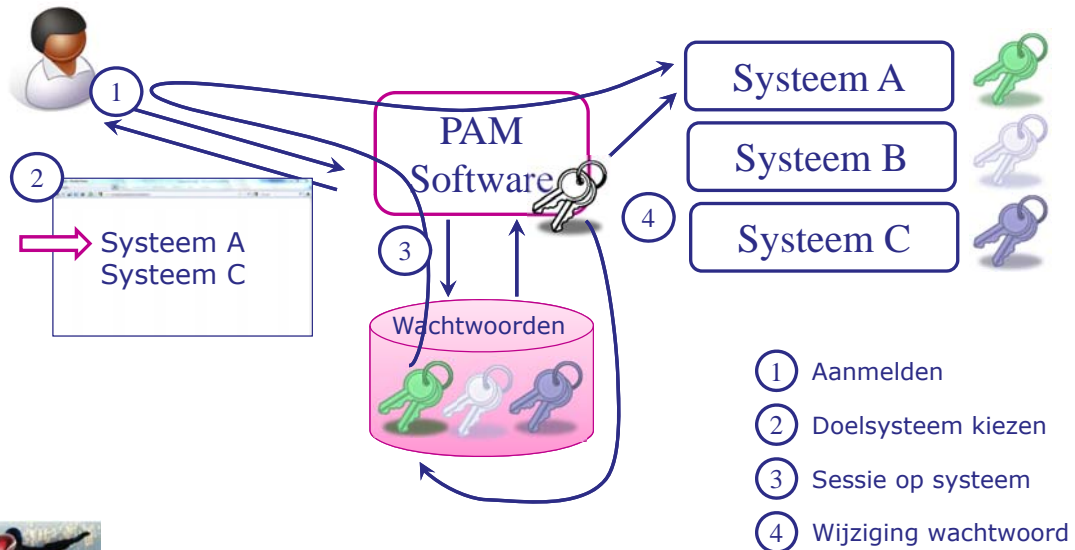
...



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

35

## Software Weringsprincipe



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

36

## Software Eigenschappen

---

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



## Software Eigenschappen

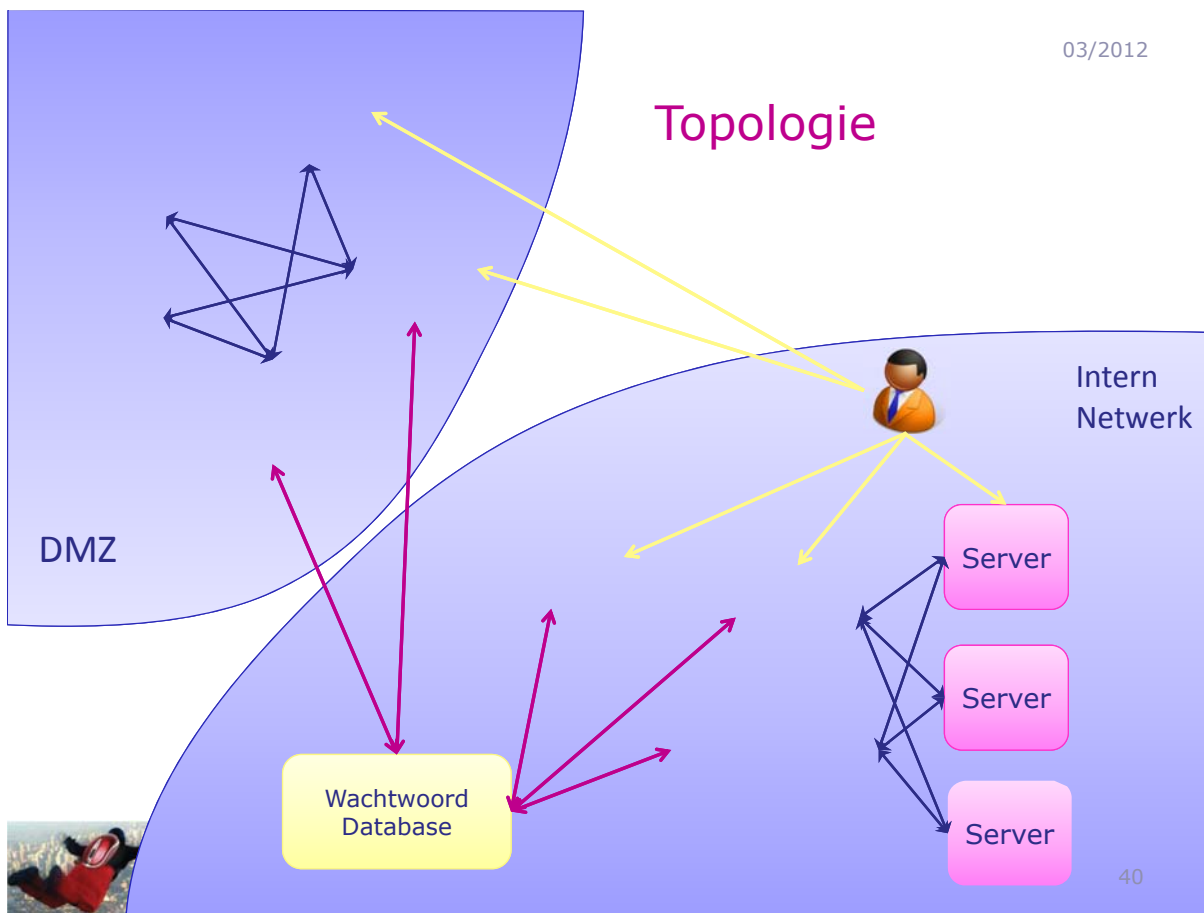
---

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



## 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)

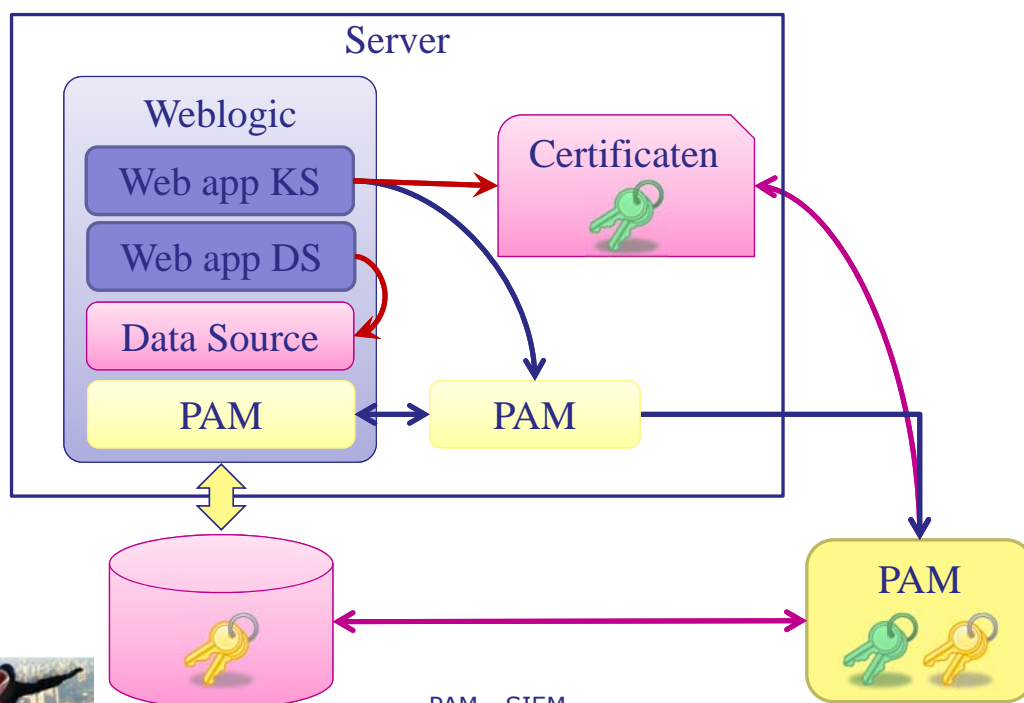


## DEMO - PAM-tool

- Windows
- Unix
- Database



## DEMO - toepassingen



## Software Vaststellingen (1/2)

---

- Redelijk vlot voor standaardsystemen
  - Scripting voor tuning van command prompts
- Soms browserafhankelijk gedrag
- Topologie heeft invloed op implementatie
  - firewall die (Windows) traffic 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](mailto:bob.lannoy@smals.be)

 [@boblannoy](https://twitter.com/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



## Uitdaging

- Miljoenen logs, slechts enkele incidenten...



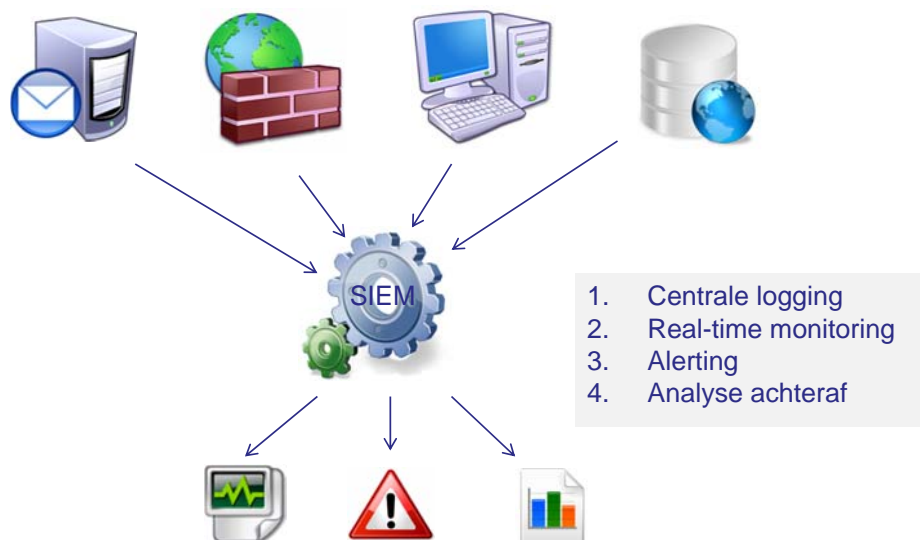
⇒ Onmogelijk manueel



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

55

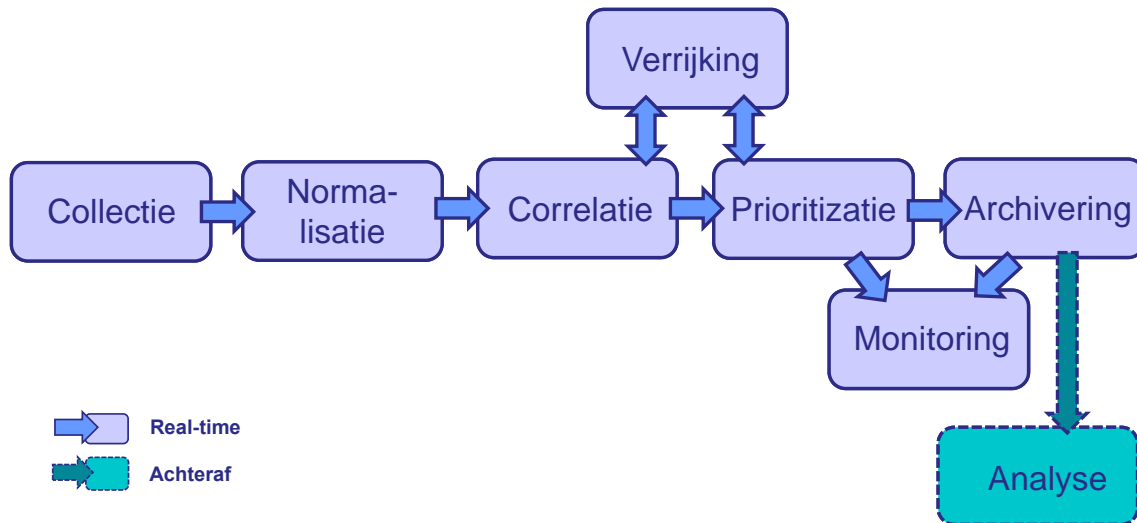
## De essentie



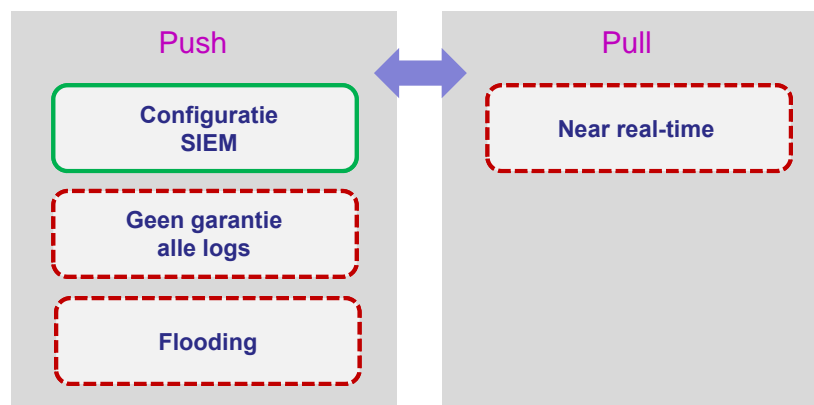
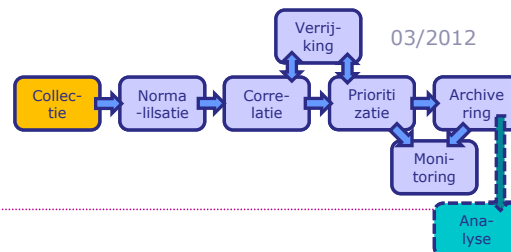
PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

56

## Verwerkingsproces



## Collectie

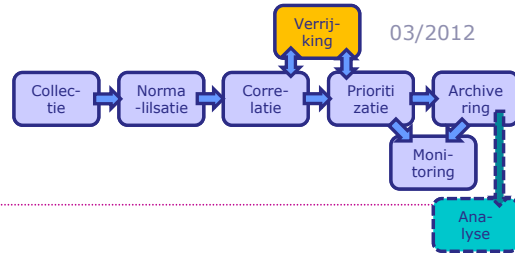


- ⇒ Ondersteunt SIEM de bron?
- ⇒ Soms agent op device nodig
- ⇒ Meestal push



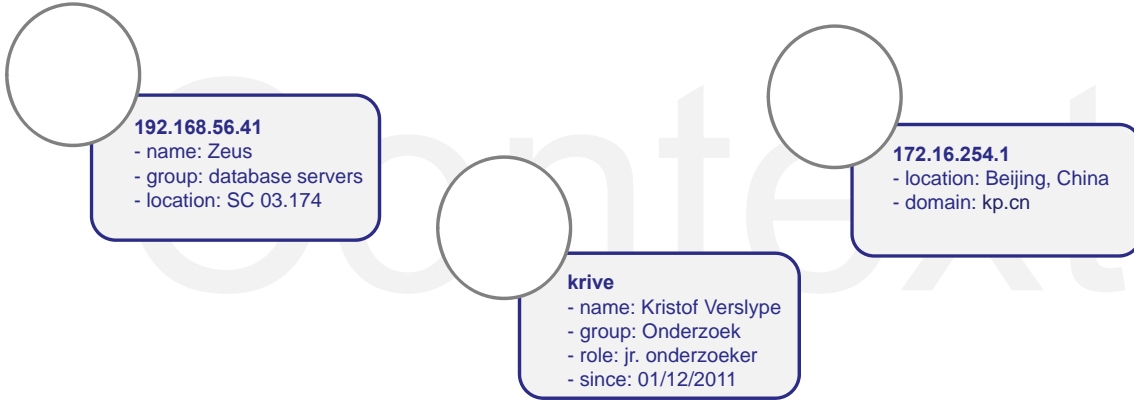


# Verrijking

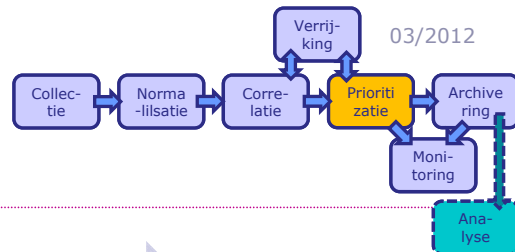


"Mar 20 08:44:35 192.168.56.41 sshd[263] Accepted pass for *krive* from 216.101.197.234 port 56946 ssh2"

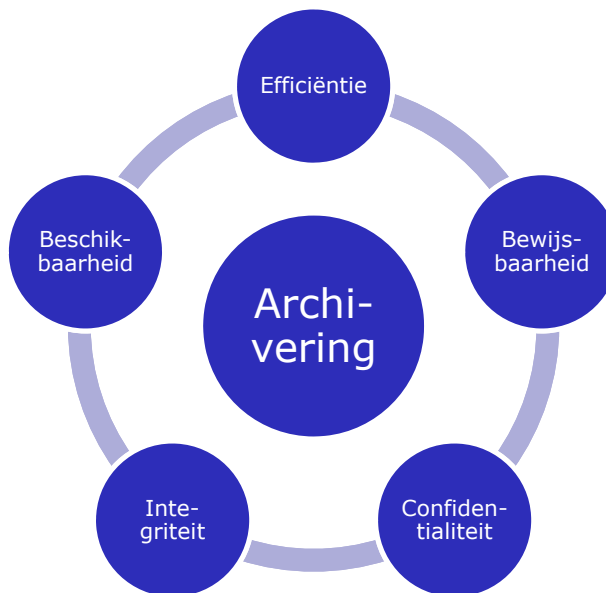
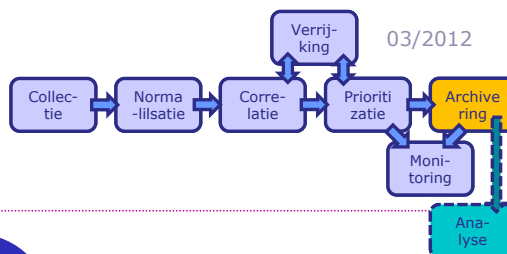
⇒ Externe bronnen: DNS, user directories, ...



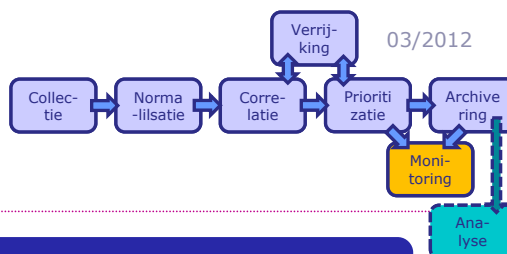
# Prioritizatie




# Archivering




# Monitoring






### Evaluëren

- Kwetsbaarheden
- Verdachte activiteit
- Incidenten



### Dashboards

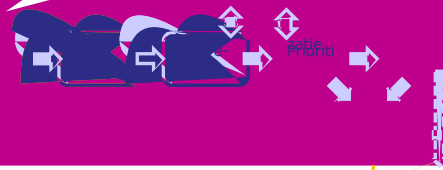
- Remote login
- Idealiter enkele high-priority events



### Alarm

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

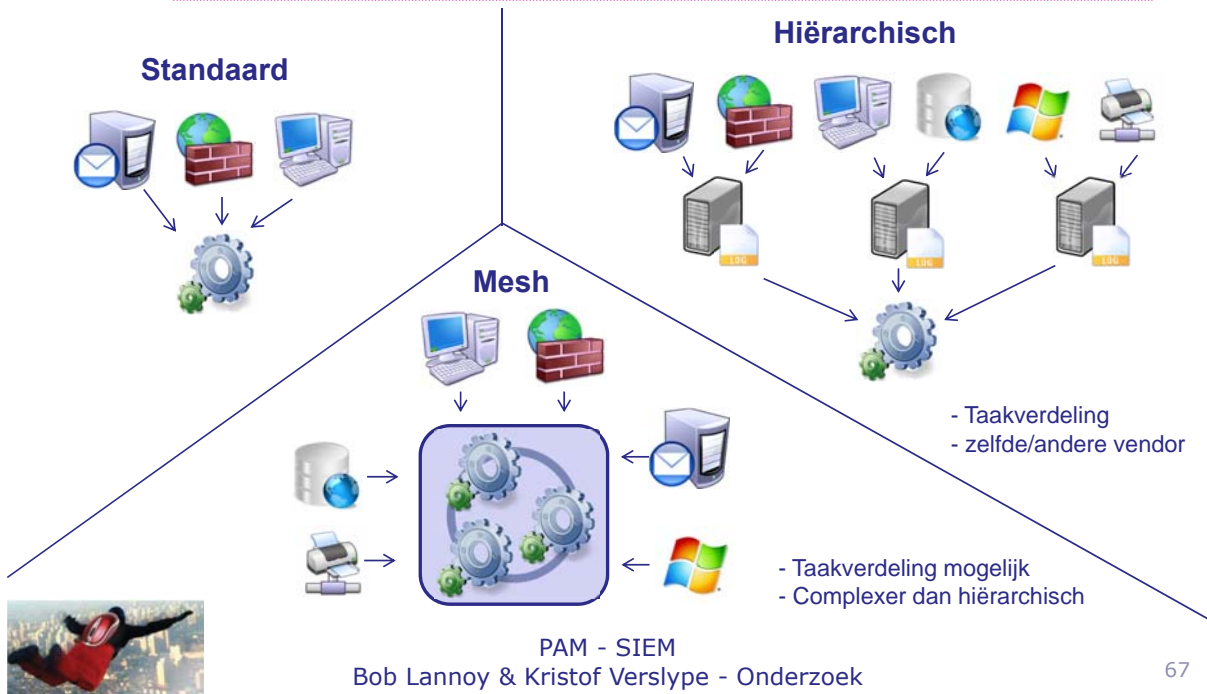




## Evolutie

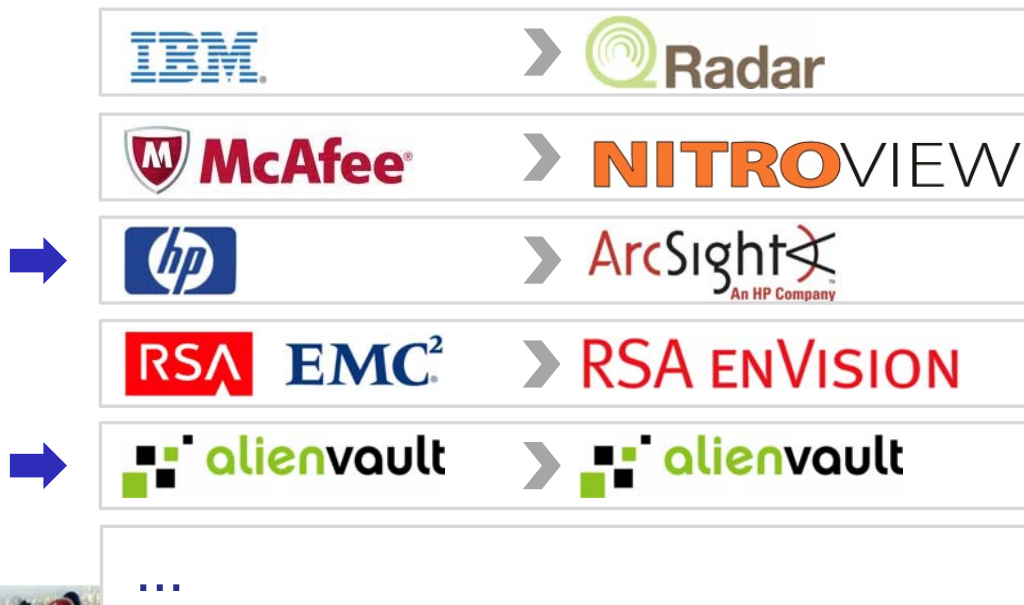


## Topologie



67

## Beschikbare systemen



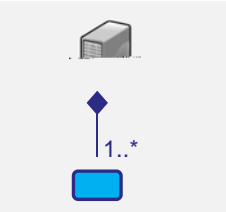
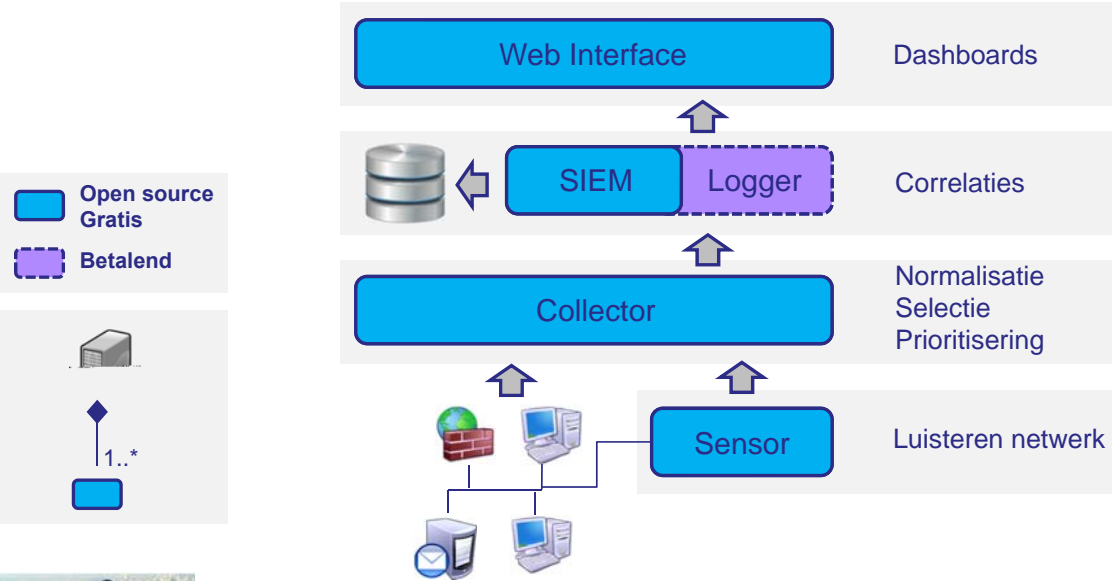
68



Basisprincipes > AlienVault > ArcSight > Managed SIEM > Tot slot



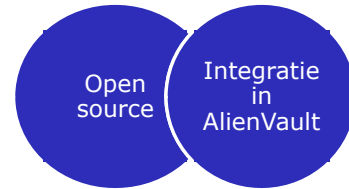
# Componenten



## Bouwblokken

**Nagios®**

**OCS** next generation  
inventory



Pof

NFSen/NFDump

Inprotect

**Passive Asset Detection System**



**osvdb**

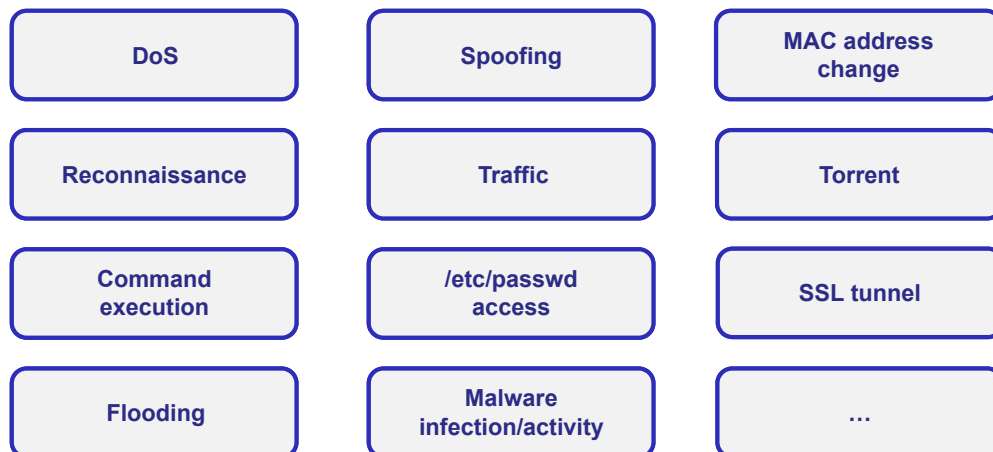


PAM - SIEM

Bob Lannoy & Kristof Verslype - Onderzoek

71

## Correlaties (1/3)



PAM - SIEM

Bob Lannoy & Kristof Verslype - Onderzoek

72

level 3

Failed Applications

level 4

73



## 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

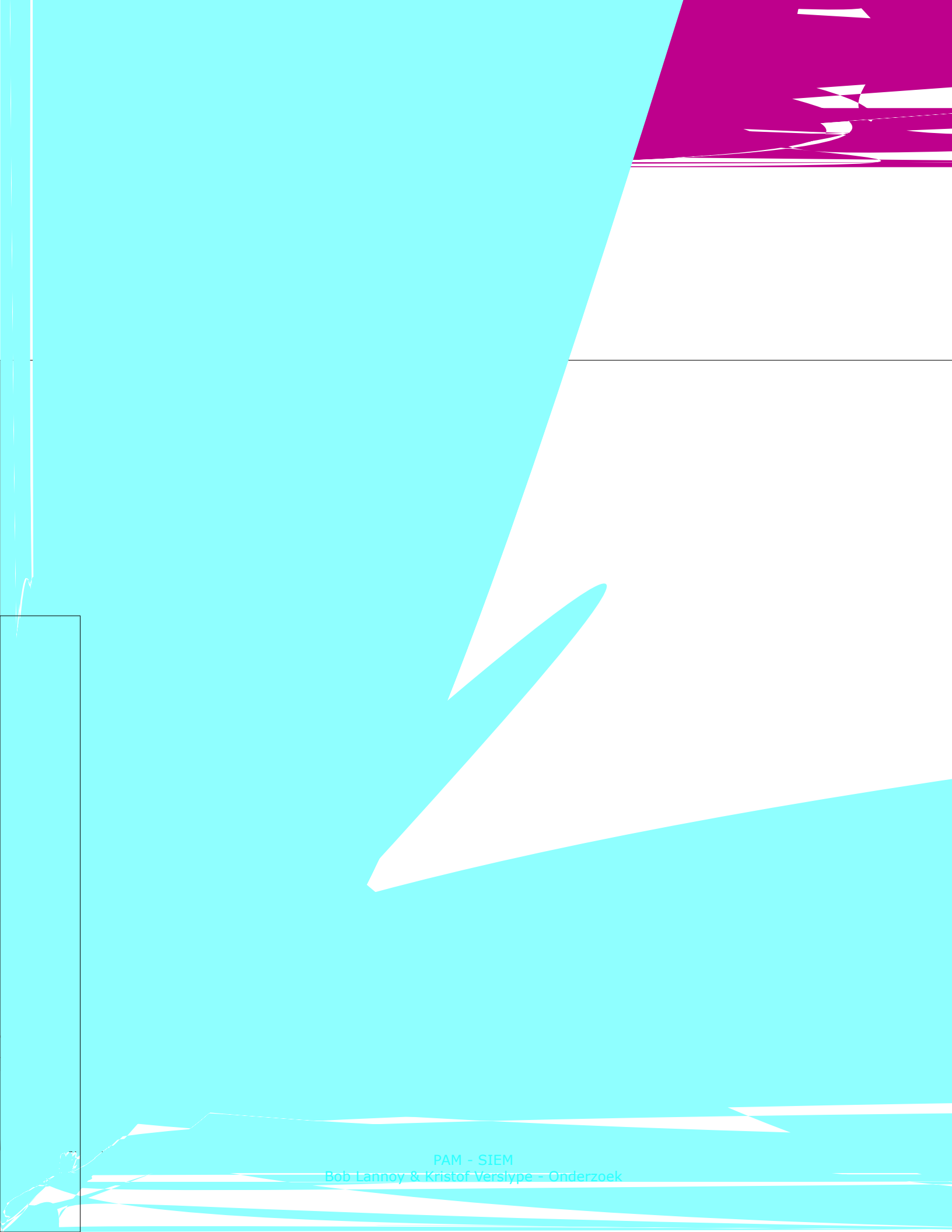
## Screenshots

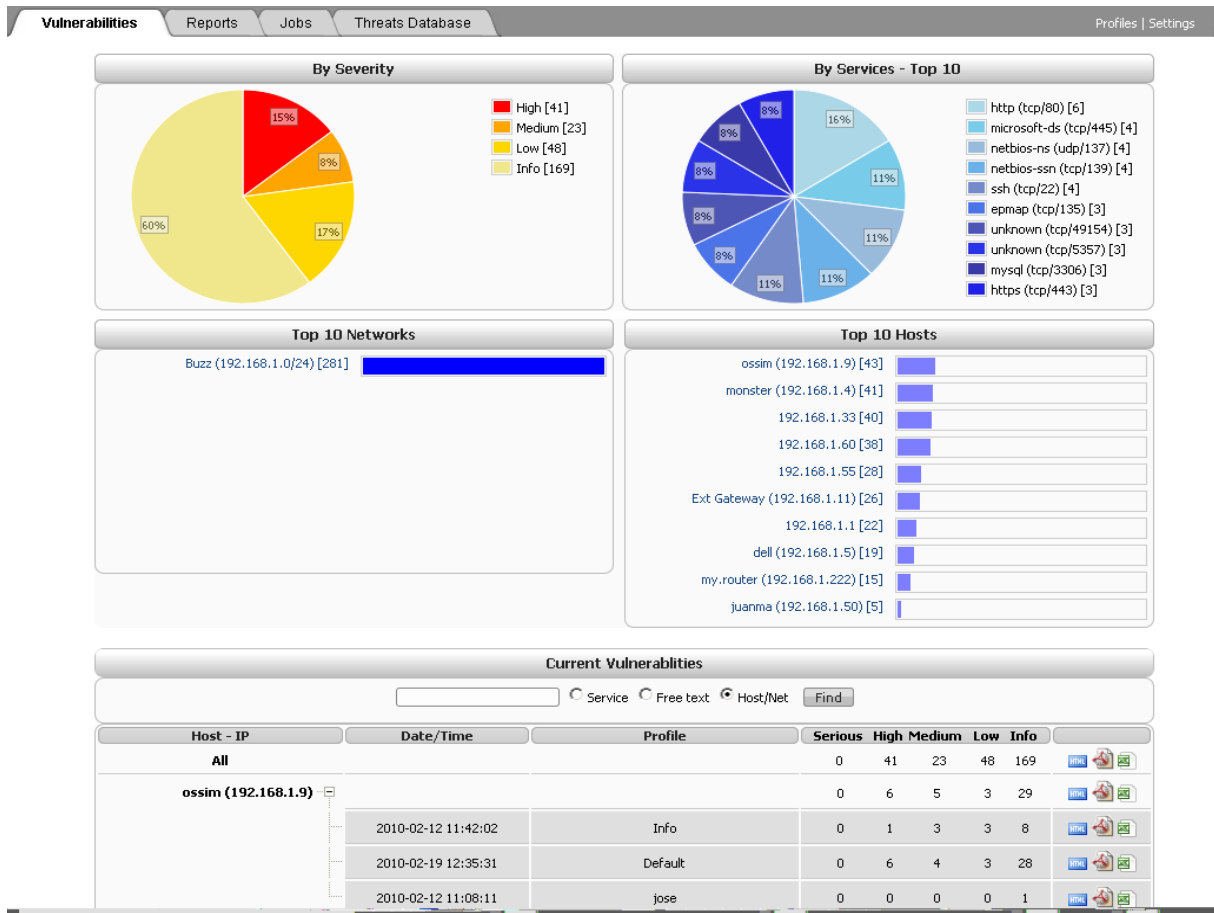
- Overzicht
- Alarmen
- Kwetsbaarheden



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

76





## Aandachtspunten

### Configuratie

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

### Krachtige servers

- Normaliseren
- Correleren

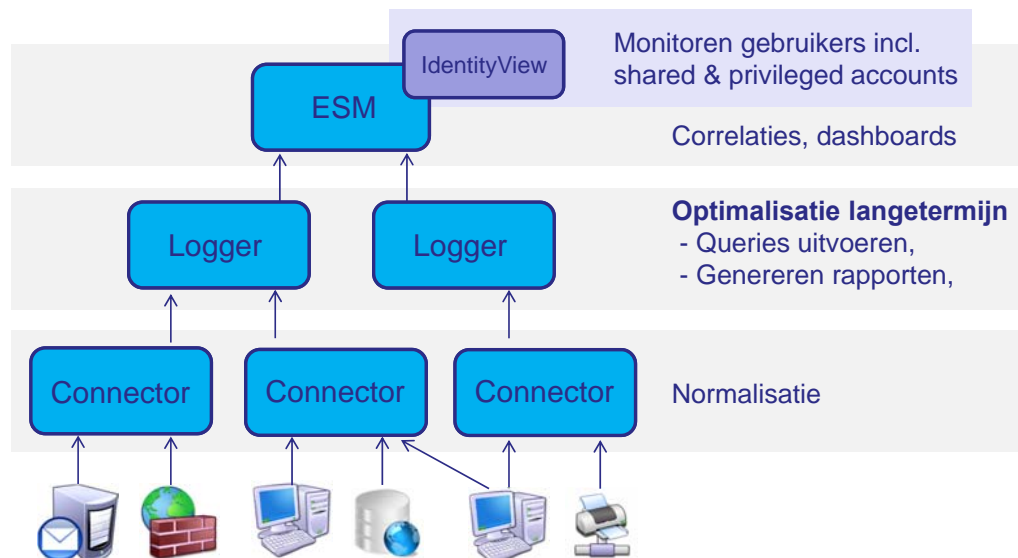




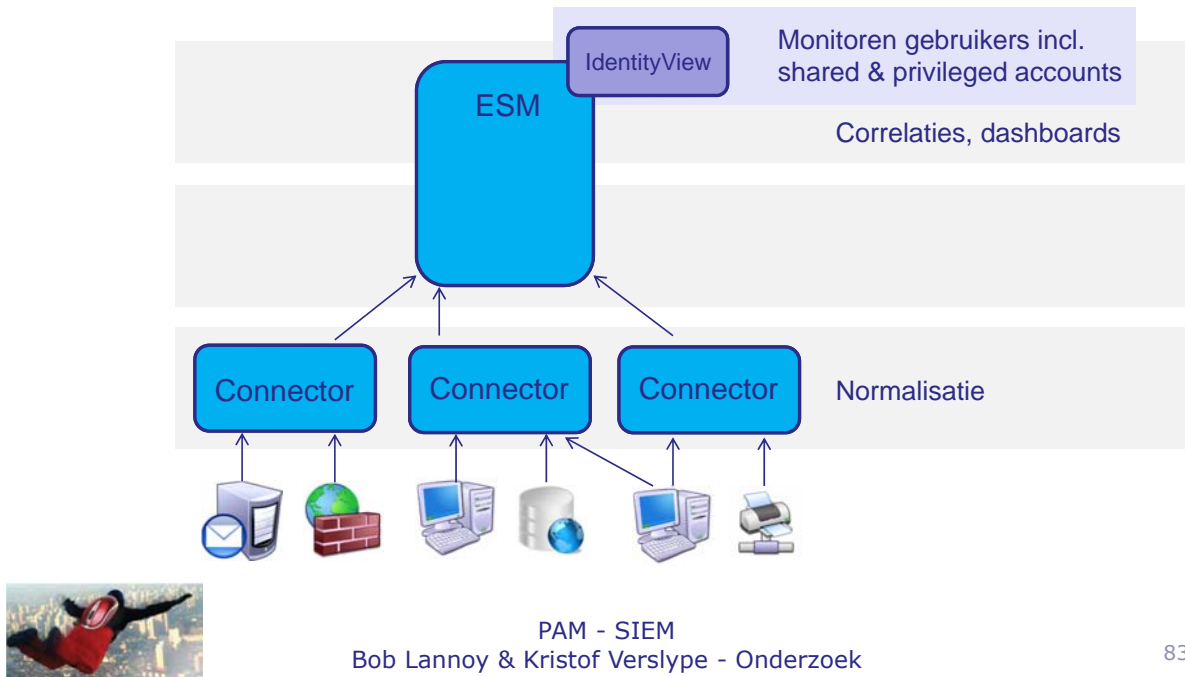
Basisprincipes > AlienVault > ArcSight > Managed SIEM > Tot slot



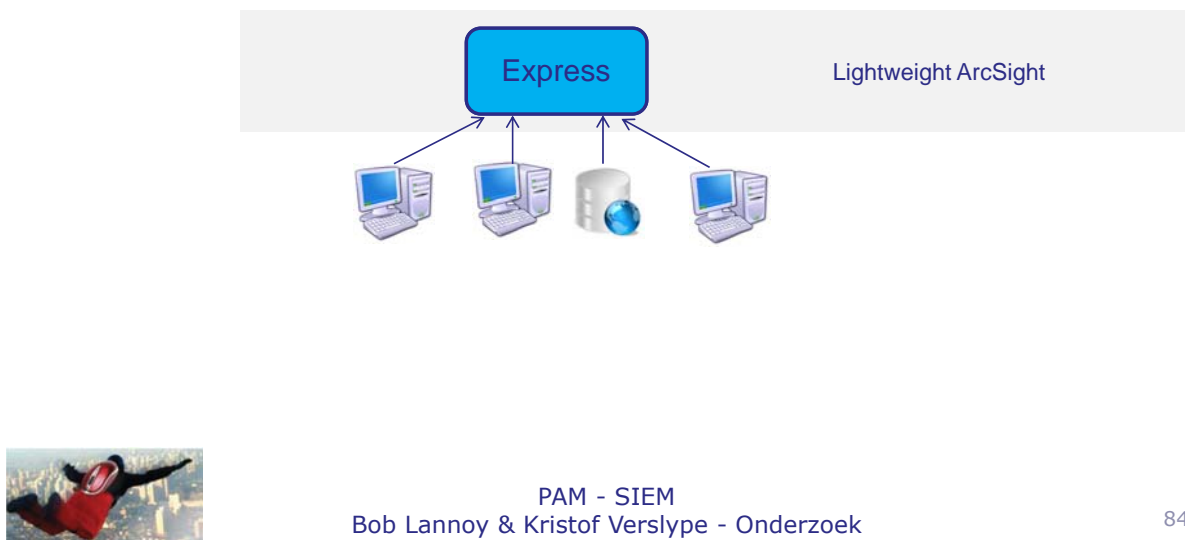
## Componenten (1/3)



## Componenten (2/3)



## Componenten (3/3)



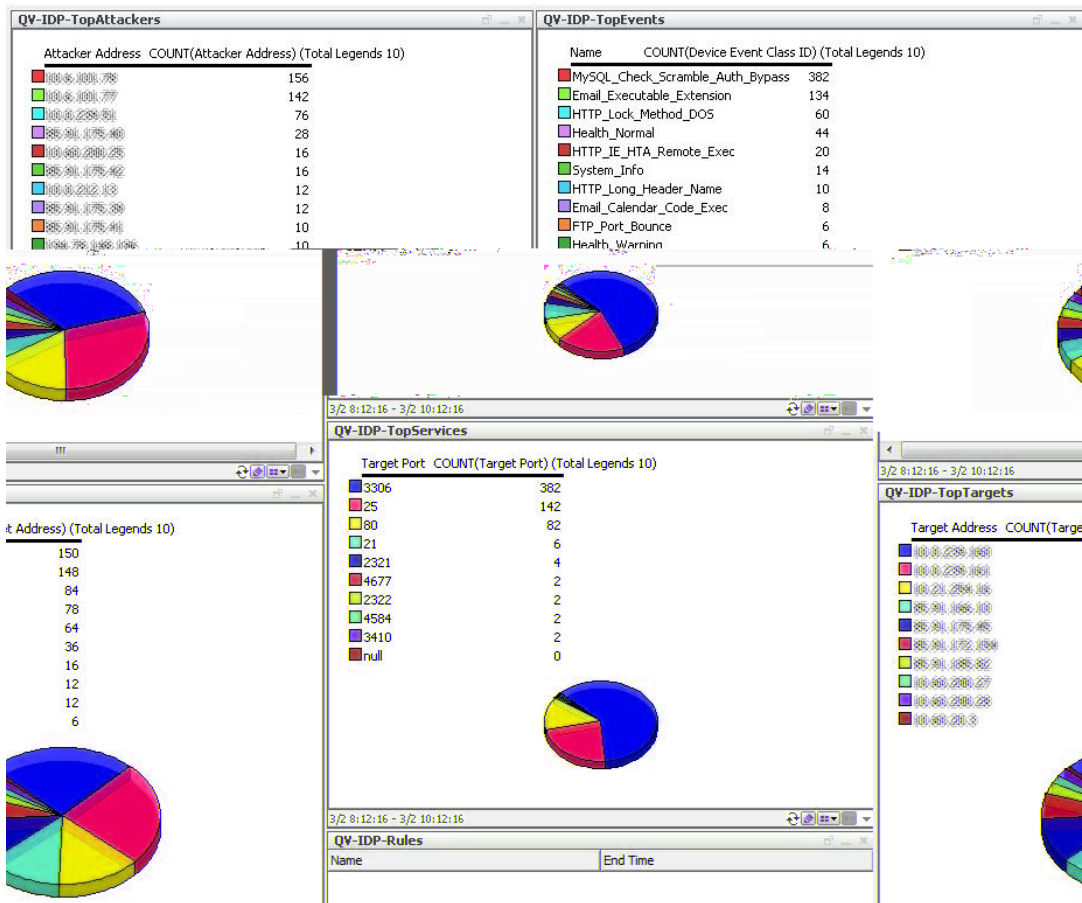
# Screenshots

- Top-10
- Events
- Actuele aanvallen
- Statistieken



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

85



86

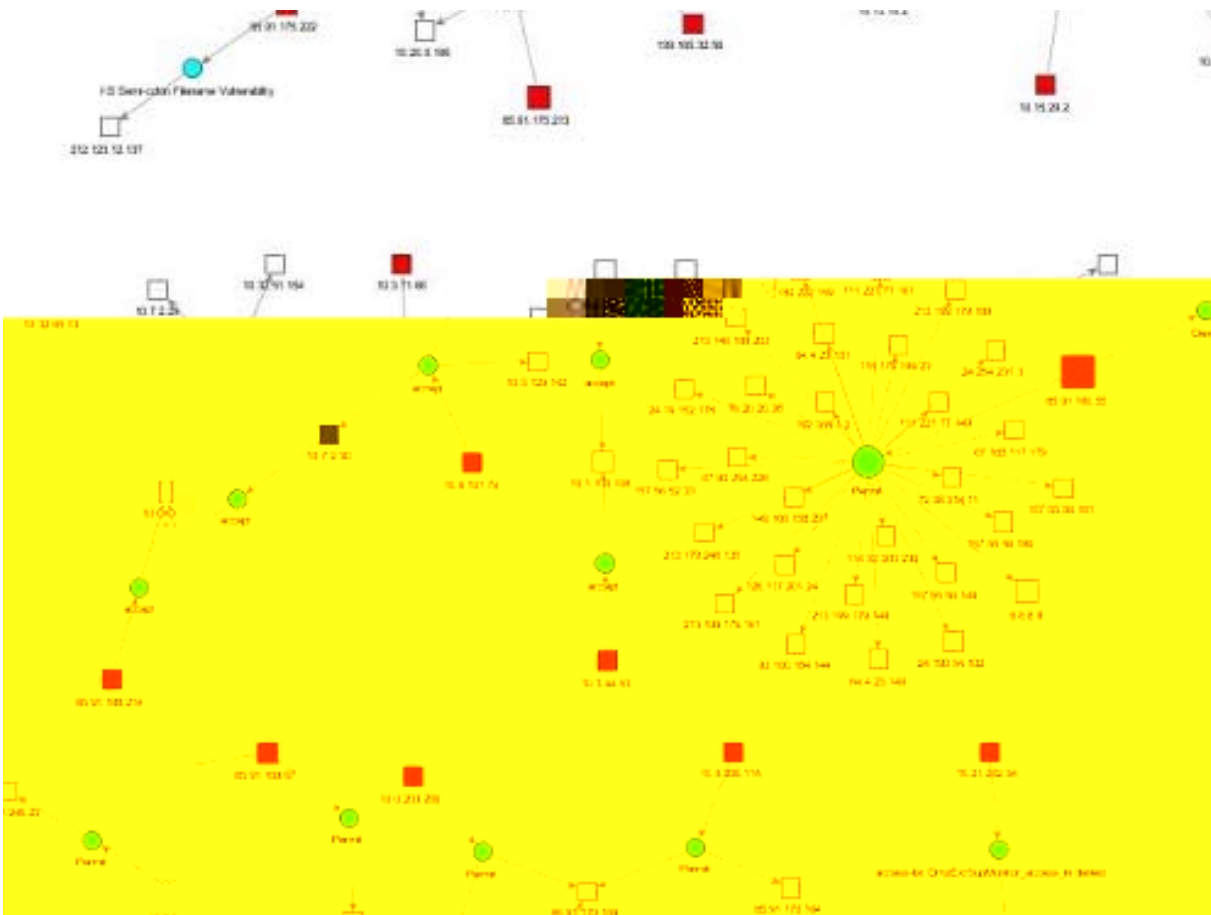
**Start Time:** 2 Mar 2012 09:43:47 CET  
**End Time:** 2 Mar 2012 11:43:47 CET  
**Filter:** Agent ID = "IBM SiteProtector"  
**Inline Filter:** No Filter  
**Verified Rules:** No Rule

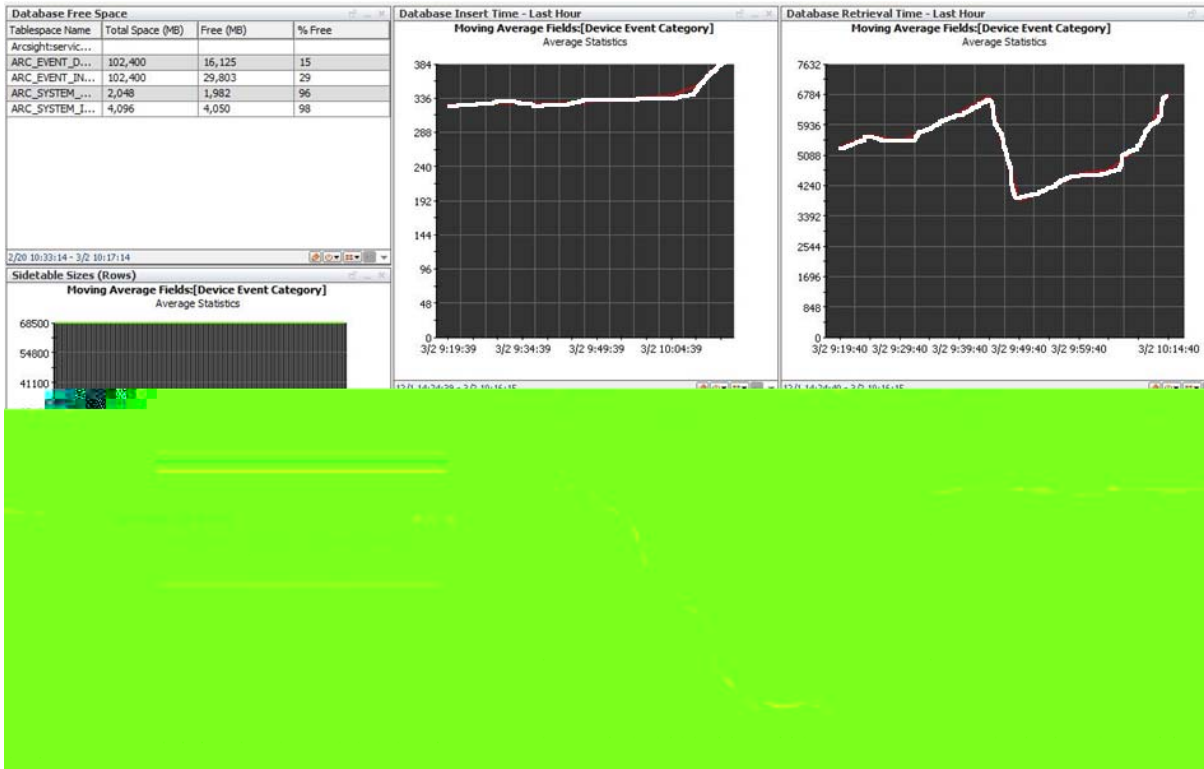
**Very High:** 2  
**High:** 237  
**Medium:** 1,430  
**Low:** 56  
**Very Low:** 0

**Radar**



| Manager Receipt Time ↑ 1 | 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 | 10.21.254.22       | 10.20.168.28     | 5          |
| 2 Mar 2012 10:04:44 CET  | 2 Mar 2012 10:13:14 CET | MySQL_Check_Scramble_Auth_Bypass | 10.21.254.22       | 10.20.168.28     | 5          |
| 2 Mar 2012 10:04:44 CET  | 2 Mar 2012 10:13:20 CET | TCP_Port_Scan                    | 10.20.0.129*       | 10.20.0.122      | 5          |
| 2 Mar 2012 10:04:44 CET  | 2 Mar 2012 10:13:19 CET | TCP_Port_Scan                    | 10.20.0.122        | 10.20.0.122      | 5          |
| 2 Mar 2012 10:04:44 CET  | 2 Mar 2012 10:12:18 CET | TCP_Port_Scan                    | 10.20.0.122        | 10.20.0.122      | 5          |
| 2 Mar 2012 10:04:29 CET  | 2 Mar 2012 10:11:53 CET | TCP_Port_Scan                    | 10.20.0.129*       | 10.20.0.121      | 5          |
| 2 Mar 2012 10:04:29 CET  | 2 Mar 2012 10:12:55 CET | TCP_Port_Scan                    | 10.20.0.129*       | 10.20.0.121      | 5          |
| 2 Mar 2012 10:04:29 CET  | 2 Mar 2012 10:12:57 CET | TCP_Port_Scan                    | 10.20.0.122        | 10.20.0.122      | 5          |
| 2 Mar 2012 10:04:29 CET  | 2 Mar 2012 10:11:58 CET | TCP_Port_Scan                    | 10.20.0.122        | 10.20.0.121      | 5          |
| 2 Mar 2012 10:04:29 CET  | 2 Mar 2012 10:11:55 CET | TCP_Port_Scan                    | 10.20.0.122        | 10.20.0.122      | 5          |
| 2 Mar 2012 10:04:29 CET  | 2 Mar 2012 10:11:58 CET | TCP_Port_Scan                    | 10.20.0.129*       | 10.20.0.121      | 5          |
| 2 Mar 2012 10:04:29 CET  | 2 Mar 2012 10:13:01 CET | TCP_Port_Scan                    | 10.20.0.129*       | 10.20.0.121      | 5          |
| 2 Mar 2012 10:04:29 CET  | 2 Mar 2012 10:12:59 CET | TCP_Port_Scan                    | 10.20.0.122        | 10.20.0.121      | 5          |
| 2 Mar 2012 10:03:49 CET  | 2 Mar 2012 10:11:15 CET | TCP_Port_Scan                    | 10.20.0.122        | 10.20.0.122      | 5          |
| 2 Mar 2012 10:03:49 CET  | 2 Mar 2012 10:12:17 CET | TCP_Port_Scan                    | 10.20.0.129*       | 10.20.0.122      | 5          |
| 2 Mar 2012 10:03:49 CET  | 2 Mar 2012 10:12:18 CET | TCP_Port_Scan                    | 10.20.0.122        | 10.20.0.122      | 5          |
| 2 Mar 2012 10:03:49 CET  | 2 Mar 2012 10:12:18 CET | TCP_Port_Scan                    | 10.20.0.129*       | 10.20.0.122      | 5          |
| 2 Mar 2012 10:03:34 CET  | 2 Mar 2012 10:12:04 CET | TCP_Port_Scan                    | 10.20.168.22       | 10.20.168.7      | 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                    | 10.20.0.129*       | 10.20.0.121      | 5          |
| 2 Mar 2012 10:03:29 CET  | 2 Mar 2012 10:11:53 CET | TCP_Port_Scan                    | 10.20.0.129*       | 10.20.0.121      | 5          |
| 2 Mar 2012 10:03:29 CET  | 2 Mar 2012 10:10:56 CET | TCP_Port_Scan                    | 10.20.0.122        | 10.20.0.121      | 5          |
| 2 Mar 2012 10:03:29 CET  | 2 Mar 2012 10:10:53 CET | TCP_Port_Scan                    | 10.20.0.122        | 10.20.0.122      | 5          |
| 2 Mar 2012 10:03:29 CET  | 2 Mar 2012 10:10:56 CET | TCP_Port_Scan                    | 10.20.0.129*       | 10.20.0.121      | 5          |
| 2 Mar 2012 10:03:29 CET  | 2 Mar 2012 10:11:55 CET | TCP_Port_Scan                    | 10.20.0.129*       | 10.20.0.121      | 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 in zelfde 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?

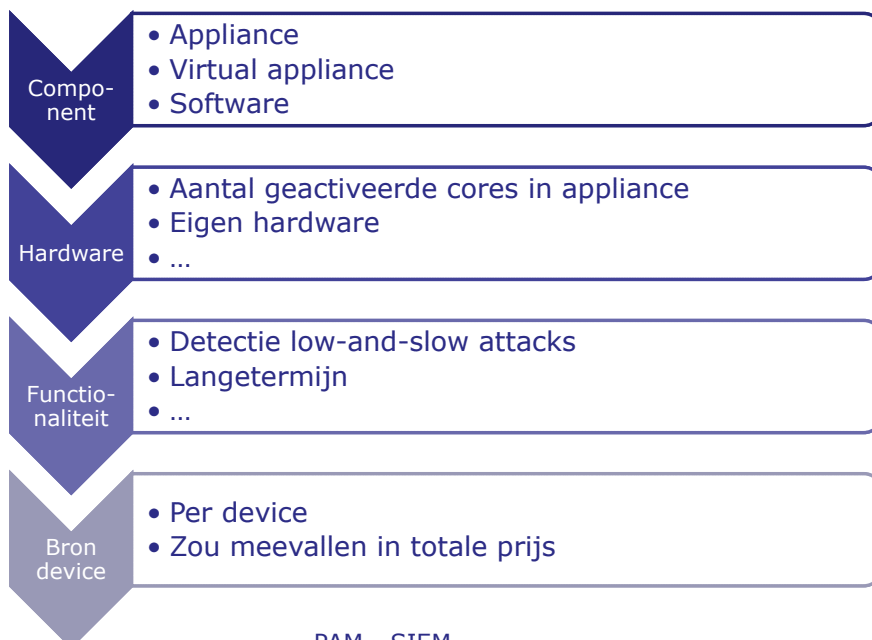


PAM - SIEM

Bob Lannoy & Kristof Verslype - Onderzoek

91

## Kostenmodel



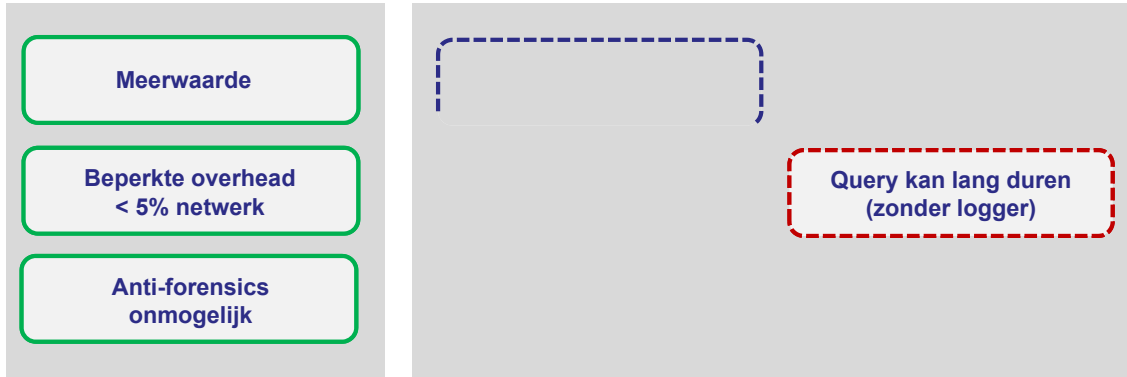
PAM - SIEM

Bob Lannoy & Kristof Verslype - Onderzoek

92

## Ervaringen

---



## SIEM



Investerings-  
kosten

Onderhoud

Expertise

24/7/364  
monitoring



PAM - SIEM

Bob Lannoy & Kristof Verslype - Onderzoek

95

## Managed Siem



MSSP (Managed Security  
Service provider)

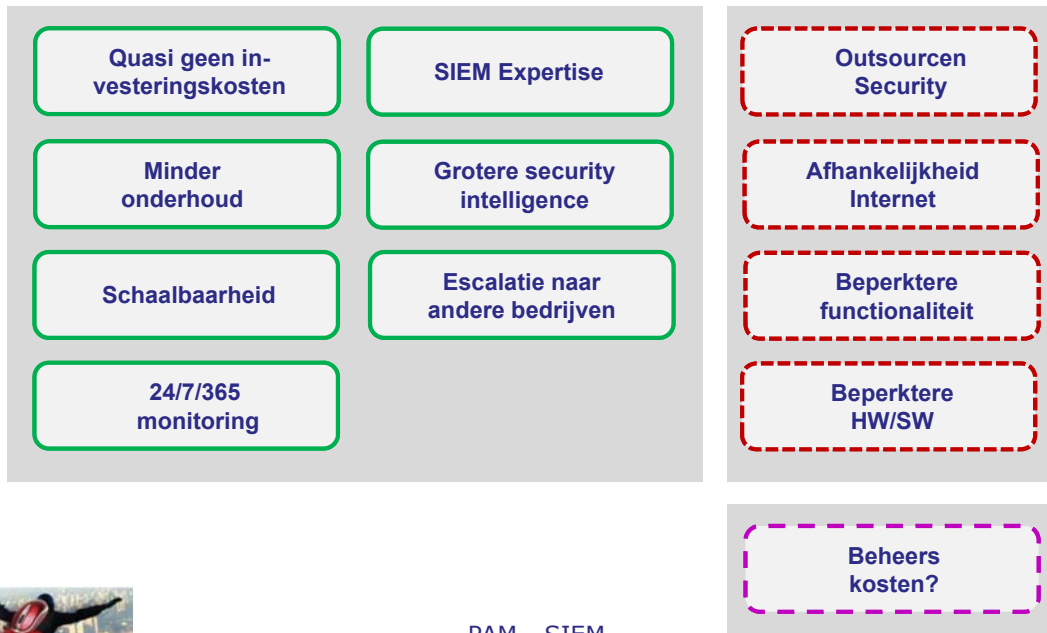


PAM - SIEM

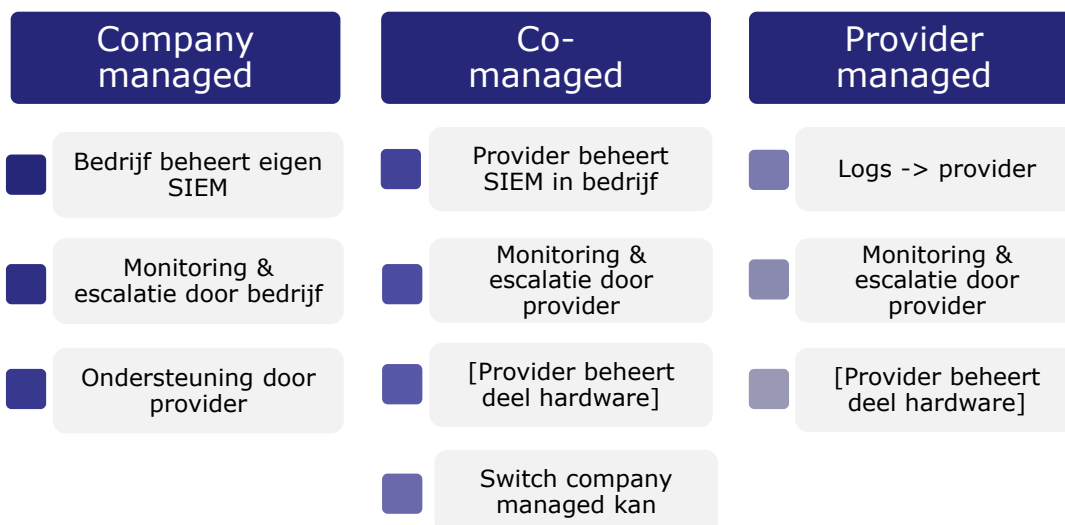
Bob Lannoy & Kristof Verslype - Onderzoek

96

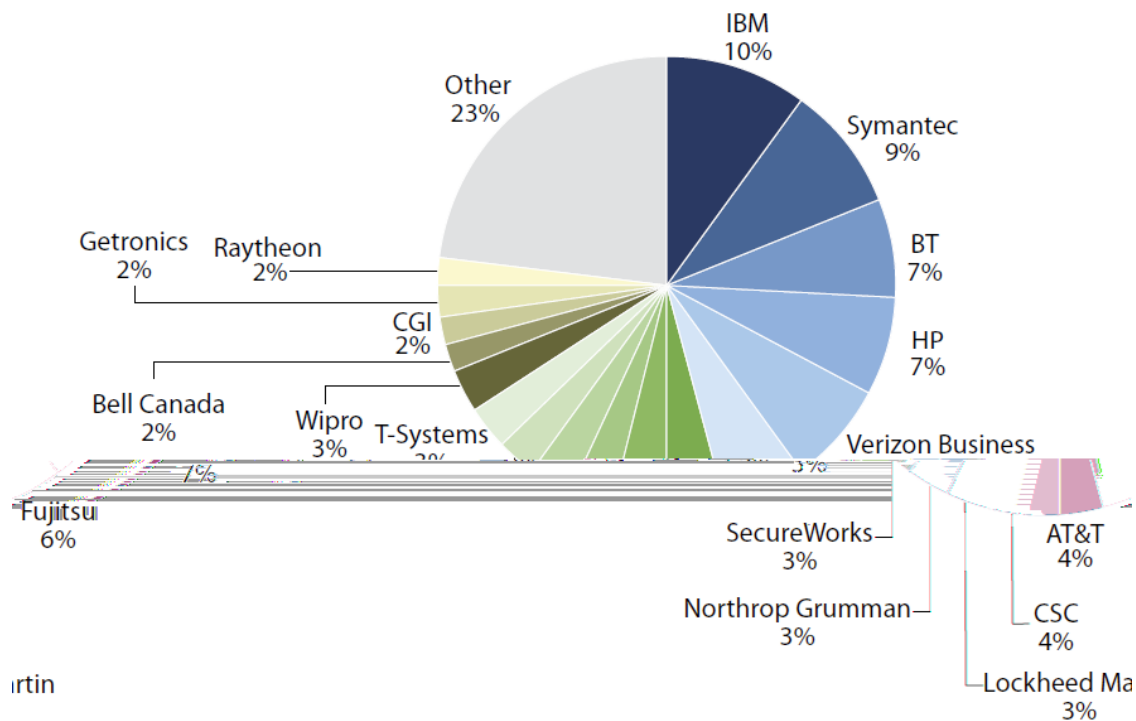
## Pro's & cons



## Managed Security Services



Market Share Of Top Managed Security Services Providers

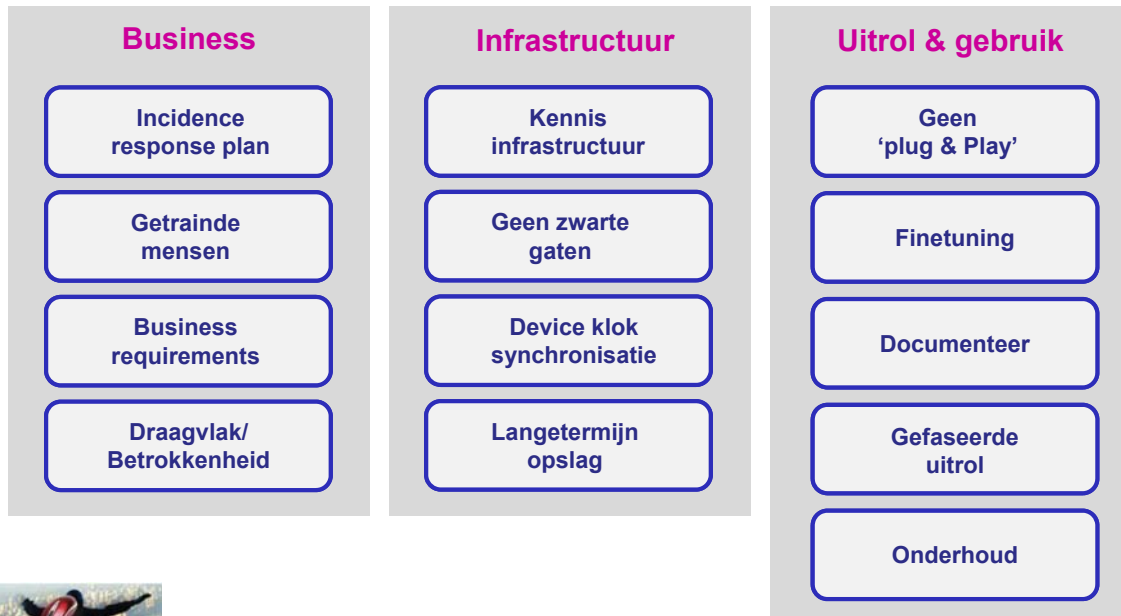


Managed security service providers Source: Forrester estimate based on information provided by mai

2015 Source: Forrester Research, Inc.

# Tot slot

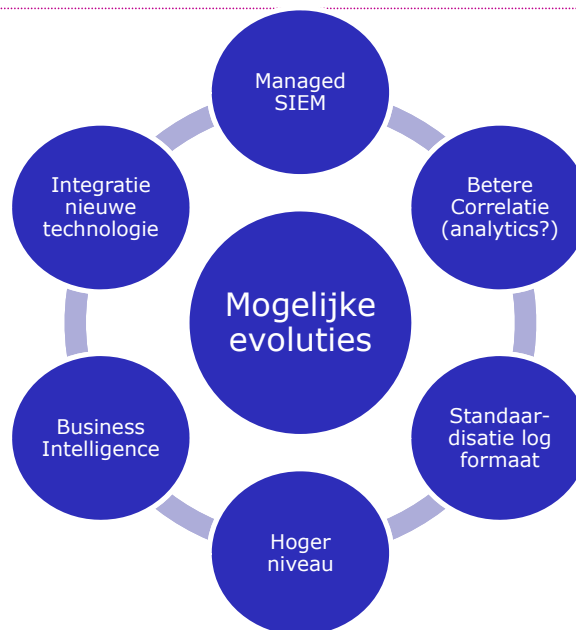
## Aandachtspunten



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

101

## Mogelijke evoluties



PAM - SIEM  
Bob Lannoy & Kristof Verslype - Onderzoek

102



## 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
01.49#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 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 --
# cmd_alias --
Cmd_Alias CHECKRAIDCONF = /home/confmon/raidinfo/
Cmd_Alias SHELLS = /bin/sh,/bin/bash,/bin/ash,/bin/bsh,/bin/ksh,/usr/bin/ksh,/u
sr/bin/pdksh,/bin/tcsh,/bin/csh
Cmd_Alias SU = /bin/su
Cmd_Alias CHECKSYSLOGS = /bin/cat /var/log/messages,/usr/bin/tail -f /var/log/m
essages
Cmd_Alias REBOOT = /sbin/halt,/sbin/shutdown,/sbin/reboot,/sbin/init,/sbin/tell
nit
Cmd_Alias PROCESSMGMT = /bin/kill
Cmd_Alias SERVICEMGMT = /etc/init.d/
Cmd_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
%ltsmam001b-admins ALL=(ALL) NOPASSWD: ALL
%linux-admins ALL=(ALL) NOPASSWD: ALL
%ltsmam001b-operators ALL=(ALL) NOPASSWD: CHECKSYSLOGS, REBOOT, PROCESSMGMT, S
ERVICEMGMT
%linux-operators ALL=(ALL) NOPASSWD: CHECKSYSLOGS, REBOOT, PROCESSMGMT, SERVICEM
GMT
%weblogic ALL=(weblogic) NOPASSWD: ALL
```

## Sudo – shell escaping & noexec

```
root
[root@ltsmam001b normuser]# tail /var/log/secure
Jan 12 15:12:47 ltsmam001b 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 ltsmam001b sudo: normuser : TTY=pts/3 ; PWD=/home/normuser ; U
SER=root ; TSID=000002 ; COMMAND=/bin/vi
Jan 12 15:15:08 ltsmam001b 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 ltsmam001b sudo: pam_succeed_if(sudo:auth): requirement "user
= root" not met by user "normuser"
Jan 12 15:15:39 ltsmam001b sudo: pam_succeed_if(sudo:auth): requirement "user
ingroup rsauers" not met by user "normuser"
Jan 12 15:15:39 ltsmam001b sudo: pam_succeed_if(sudo:auth): requirement "user
notingroup ldap-rsauers" was met by user "normuser"
Jan 12 15:15:43 ltsmam001b sudo: pam_sss(sudo:account): Access denied for user
normuser:10 (User not known to the underlying authentication module)
Jan 12 15:15:43 ltsmam001b 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 ltsmam001b sudo: normuser : TTY=pts/3 ; PWD=/home/normuser ; U
SER=root ; TSID=000002 ; COMMAND=/opt/scripts/testsudo.sh
Jan 12 15:17:22 ltsmam001b sudo: normuser : TTY=pts/3 ; PWD=/home/normuser ; U
SER=root ; TSID=000003 ; COMMAND=/bin/vi
[root@ltsmam001b normuser]# exit
exit
[normuser@ltsmam001b ~]$ sudo /bin/vi

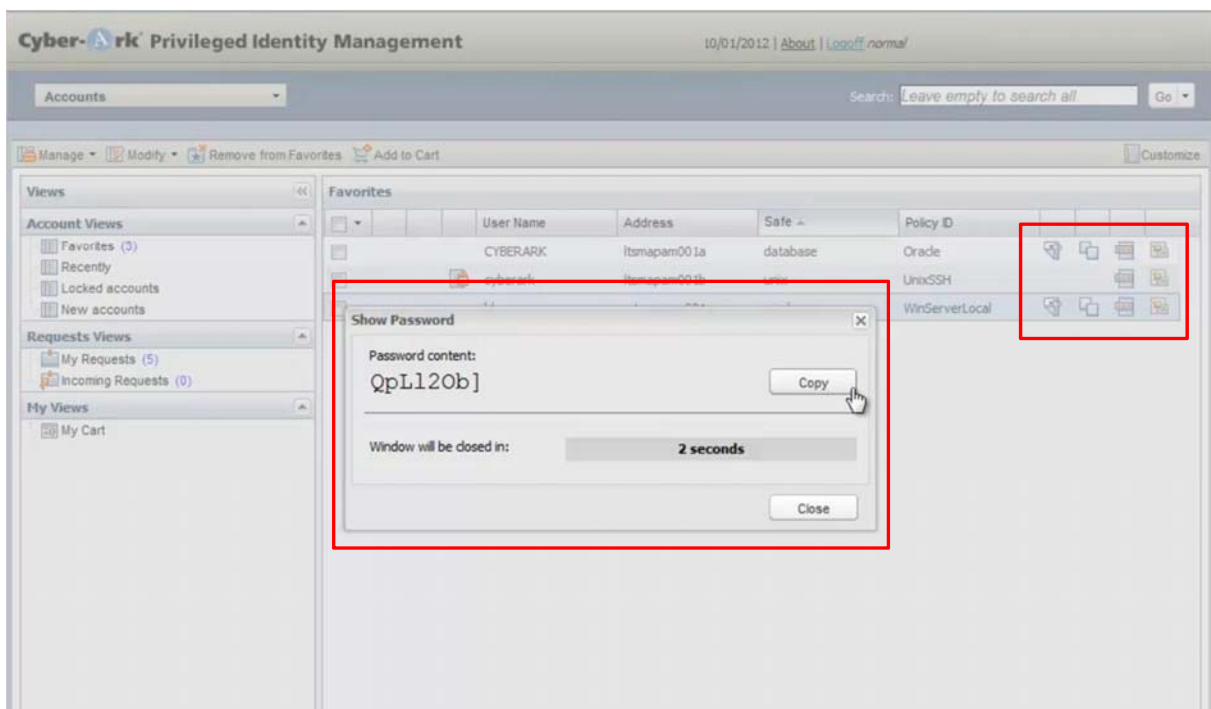
Cannot execute shell /bin/bash

[normuser@ltsmam001b ~]$ sudo /opt/scripts/testsudo.sh
/opt/scripts/testsudo.sh: line 2: /usr/bin/tail: Permission denied
[normuser@ltsmam001b ~]$
```

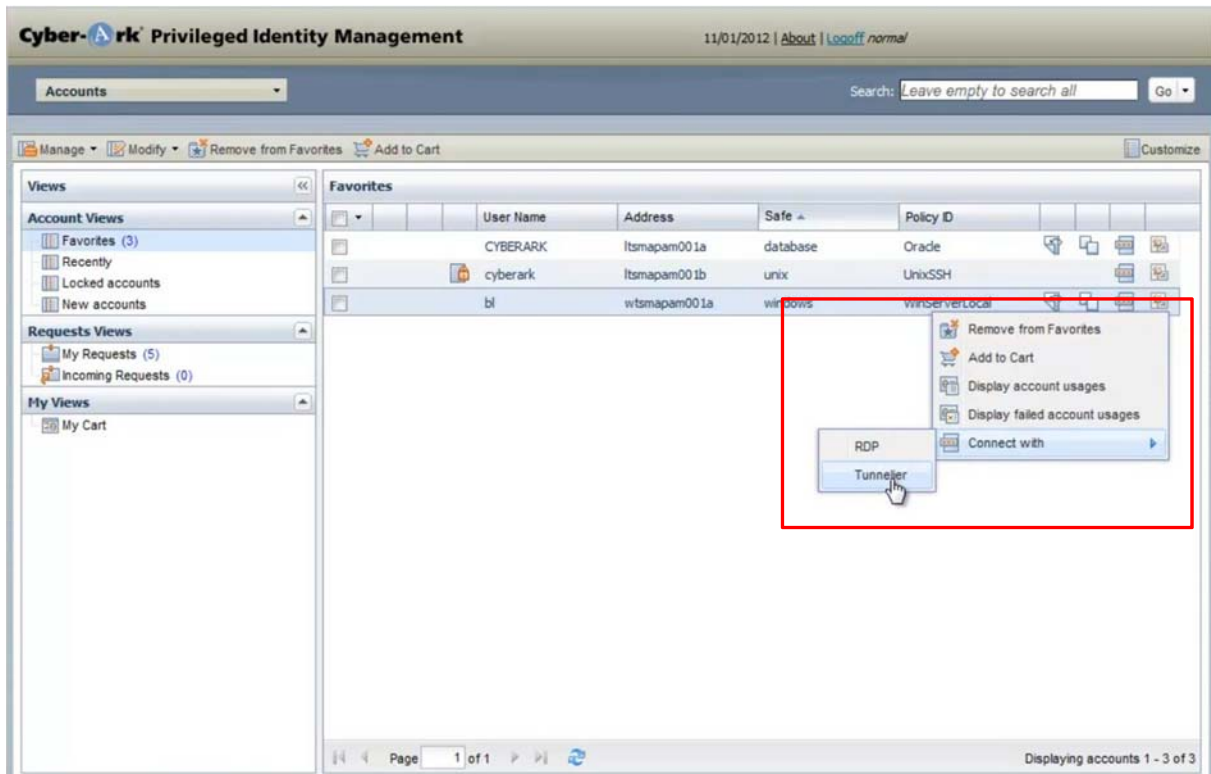
# PAM-tool web-login



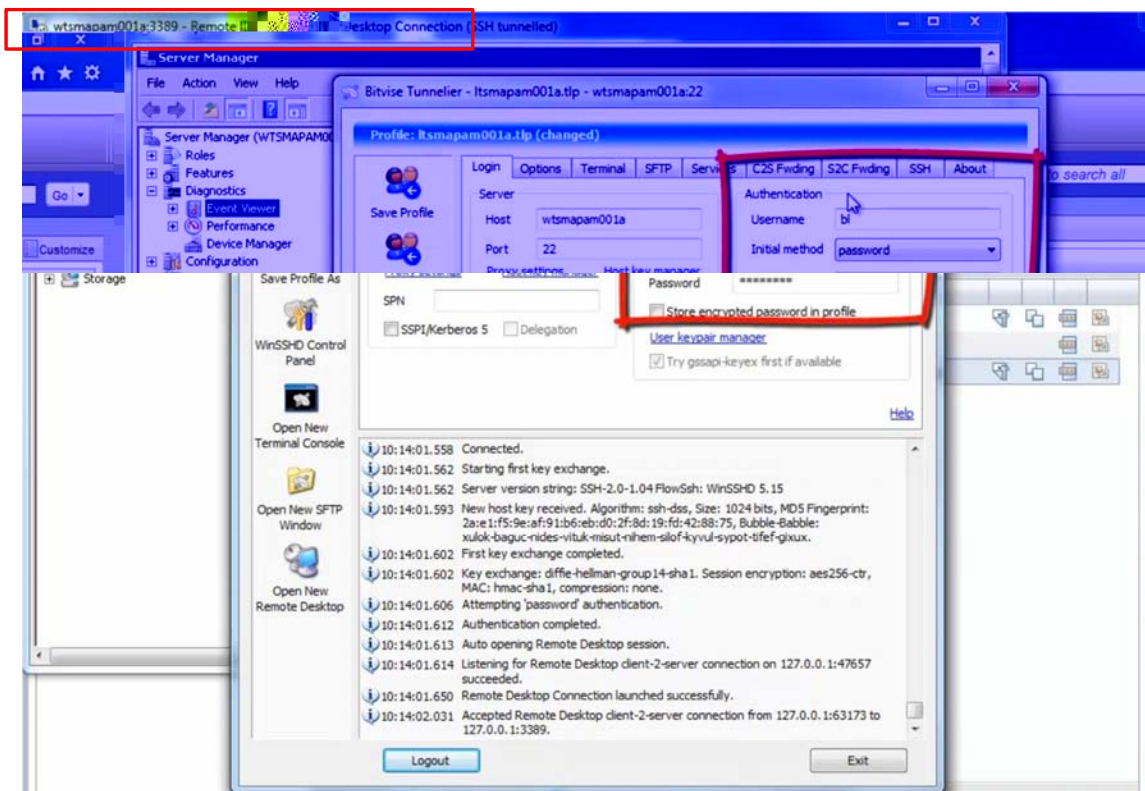
# Wachtwoord opties & tonen wachtwoord



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



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



## Workflow (1/2)

**Connect with Account** [Close]

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-itsmapam001b

Status: [1 user\(s\) must confirm the request](#)

OK Cancel

Access Requests Search:  Go

Back Confirm Reject

**Request Details:**

Request ID: 1107111  
Operation: Retrieve password Unix via SSH-cyberark-itsmapam001b  
Safe name: unix  
Reason: (ConnectionClient=PuTTY) Maintenance  
Access Type: Single operation  
Authorization required from:  
Administrator  
bobl

**Policy Details:**

Policy ID: Unix via SSH  
Device Type: Operating System  
Safe: unix  
Name: Operating System-UnixSSH-itsmapam001b-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: itsmapam001b

**Authorize Access**

Reason:

Confirm Reject

Confirm the request

Copyright © 2008-2012 CyberArk Software, Ltd. All Rights Reserved.

## Account - detailscherm

The screenshot displays the CyberArk Privileged Identity Management web interface. At the top, the logo and navigation links are visible. The main content area shows the 'Accounts' section with a dropdown menu. Below this, there are action buttons: Change, Reconcile, Verify, Send Link, and Refresh. The account details for 'Unix via SSH-cyberark-Itsmam001b' are shown, including a password field with a 'Show' button, a 'PuTTY' terminal emulator selection, and a 'Connect' button. A status indicator is also present. To the right, there are tabs for 'CPM', 'Activities', and 'Versions'. Below these tabs, the 'Logon Account' and 'Reconcile Account' fields are visible, along with the 'Account Group' section showing a group of '[None]'. A metadata table is located below the password field:

|                |  |
|----------------|--|
| Policy ID:     | Unix via SSH                           |
| Device Type:   | Operating System                       |
| Safe:          | unix                                   |
| Name:          | Operating System-UnixSSH-Itsmam001b-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:       | Itsmam001b                             |

## Session recording

The screenshot shows a Windows Internet Explorer browser window displaying a terminal session. The terminal window is titled 'Itsmam001b - Cyber-Ark Privileged Session Manager'. The terminal output shows the following text:

```
Using username "cyberarkr".
Using keyboard-interactive authentication.
Last login: Thu Jan 12 10:13:00 2012 from 10.6.101.36
-----
All content of this system and its associated sub-systems are proprietary information and remain the sole and exclusive property of this company. This system may be accessed and used by authorized personnel only. Authorized users may only perform authorized activities and may not exceed the limits of such authorization. Disclosure of information found in this system for any unauthorized user is strictly prohibited. All activities on this system are subject to monitoring. Intentional misuse of this system can result in disciplinary action or criminal prosecution.
-----
[cyberarkr@Itsmam001b ~]$
```

A red box highlights a notification in the bottom right corner of the terminal window that reads: 'Cyber-Ark Privileged Session Manager X This session is being recorded.'

## Session recording – search/keystrokes/video

The screenshot shows a search results table with columns: User, Account User Name, Account Address, Account Policy ID, Start, Duration, and Vid... The first row is highlighted, showing a recording of user 'normal' with account 'cyberarkr' and address 'ltsmapam001b'. A red box highlights the search criteria 'All recordings, session contains: passwd'. Below the table, a 'Keystrokes' table shows a single entry: '# 1 cat /etc/passwd' with an 'Offset' of '00:00:21'. A red arrow points from this entry to a video player window titled 'ltsmapam001b - CyberArk Privileged Session Manager'. The video player shows a terminal window with the command 'cat /etc/passwd' and its output, which lists system users and their home directories. The video player has a progress bar and playback controls.

| User   | Account User Name | Account Address | Account Policy ID | Start               | Duration | Vid... |
|--------|-------------------|-----------------|-------------------|---------------------|----------|--------|
| normal | cyberarkr         | ltsmapam001b    | UnixSSHRecord     | 12/01/2012 11:08:54 | 00:00:31 | 36KB   |

| # | Keystrokes      | Offset   |
|---|-----------------|----------|
| 1 | cat /etc/passwd | 00:00:21 |

```
ltsmapam001b - CyberArk Privileged Session Manager
[cyberarkr@ltsmapam001b ~]$ ls
[cyberarkr@ltsmapam001b ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/empty:/sbin/nologin
lpd:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:11:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:ftp:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody//:/sbin/nologin
dbus:x:81:81:system message bus://:/sbin/nologin
cvs:x:59:59:CVS daemon:/var/cvs:/sbin/nologin
postx:32:32:post:/var/spool/postfix:/sbin/nologin
smb:x:174:174:/etc/smb:/sbin/nologin
nlddaemon:x:60:60:NLD daemon//:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/rpc:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
sshdauth:x:499:499:"sshdauth user"//var/empty/sshauth:/sbin/nologin
postfix:x:89:89:/var/spool/postfix:/sbin/nologin
nfsd:x:28:28:/etc/nfs:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
oprofile:x:72:72//:/sbin/nologin
oprofile:x:16:16:special user account to be used by OProfile:/home/oprofile:/sbin/nologin
oper:x:704:704:/home/oper:/bin/bash
mailnews:x:701:701:/home/mailnews:/bin/bash
clmav:x:490:490:Clm Avir Checker:/var/clmav:/sbin/nologin
cvtchlog:x:564:564:/home/cvtchlog:/bin/bash
cvtfwsh:x:702:702//home/cvtfwsh:/bin/bash
cvtchck:x:720:720:/home/cvtchck:/bin/bash
cvtmrmn:x:803:803//home/cvtmrmn:/bin/bash
[cyberarkr@ltsmapam001b ~]$
```

## 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 main content area is titled "Settings for db.database.cyberark" and includes tabs for Configuration, Targets, Monitoring, Control, Security, and Notes. A "Notes" text area contains the following text: `Query>Safe=database; Folder=root; Object=oracle`. The left sidebar shows the "Domain Structure" tree with "JDBC" expanded to "Data Sources". A yellow notification box at the top left states: "view changes and restarts Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain."

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

The screenshot shows the CyberArk Privileged Identity Management console. The main content area displays "Account Details: Oracle-CYBERARK-Itsmapam001a". The "Password" field is masked with asterisks, and there are buttons for "Show", "Copy", "Connect", and "Copy Shortcut". The account details are as follows:

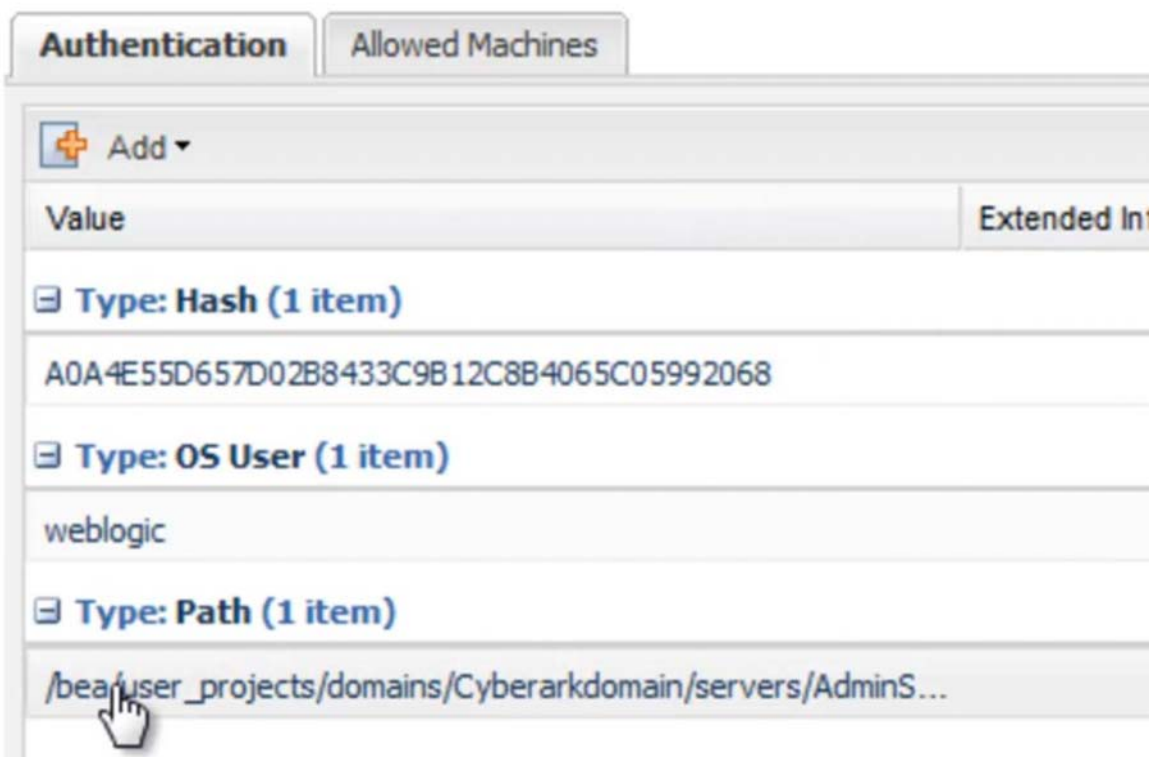
|                |                                       |
|----------------|---------------------------------------|
| Policy ID:     | Oracle                                |
| Device Type:   | Database                              |
| Safe:          | database                              |
| Name:          | 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                          |

On the right, the "Reconcile Account" section shows "Account Group" as "[None]".

## Applicatie integratie – Java API

```
@see javax.servlet.http.HttpServlet#doGet(javax.servlet.http.HttpServlet)
/
@Override
protected void doGet(HttpServletRequest req, HttpServletResponse resp) throws ServletException, IOException {
    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 ("Integrationsoaks");
        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.getContent());
        //out.println ("The password Address is : " + password.getAddress());
        //out.println ("The password keystore path is : " + password.getKeystorePath());
    } catch (PSDKException ex) {
    }
}
```

## Applicatie integratie - authentication



The screenshot shows a configuration window with two tabs: "Authentication" (selected) and "Allowed Machines". Below the tabs is a table with columns "Value" and "Extended Information". The table contains three sections of items:

- Type: Hash (1 item)**: A0A4E55D657D02B8433C9B12C8B4065C05992068
- Type: OS User (1 item)**: weblogic
- Type: Path (1 item)**: /bea/user\_projects/domains/Cyberarkdomain/servers/AdminS...

# Wachtwoordbeheer via logon-account

The screenshot displays the CyberArk Privileged Identity Management (PIM) web interface. At the top, the header shows the CyberArk logo and the text "Privileged Identity Management". The date "13/01/2012" and user information "About | Logout bobl" are visible on the right. Below the header, there is a navigation bar with a dropdown menu set to "Accounts" and a search field containing "Leave empty to search all" with a "Go" button. A toolbar contains various action icons: Edit, Change, Reconcile, Verify, Delete, Move, Send Link, Refresh, Add Account, and Customize.

The main content area is titled "Account Details: Keystore". It is divided into two main sections. On the left, there is a "Password" management section with a masked password field, "Show" and "Copy" buttons, a dropdown menu, and "Connect" and "Copy Shortcut" buttons. Below this, account metadata is listed: 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), and KeyStoreName: /tmp/integrationsoa.jks.

On the right, there are tabs for "CPH", "Activities", "Recordings", "Versions", and "Advanced". The "CPH" tab is active and shows a "Logon Account" section with the text "Unix via SSH-cyberark-itsmapam001b" highlighted by a red box. To the right of this text are "Clear", "Associate", and "Create New" buttons. Below this is an "Account Group" section with a "Group:" label and a "[None]" value, accompanied by "Modify" and "Create New" buttons.

At the bottom left of the interface, a copyright notice reads: "Copyright © 1999-2011 CyberArk® Software, Ltd. All Rights Reserved."