Smals
ICT for society

Focus op Security Governance:

Privileged Account Management

Security Information & Event Management

Bob Lannoy
Kristof Verslype

Onderzoek
Maart 2012

Smals
ICT for society

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

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

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.

Feds: IT admin plotted to erase Fannie Mae

'Server Graveyard' narrowly averted

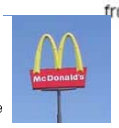
By Dan Goodin in San Francisco • Get more from this author

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

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

Fired techie created virtual chaos at pharma company

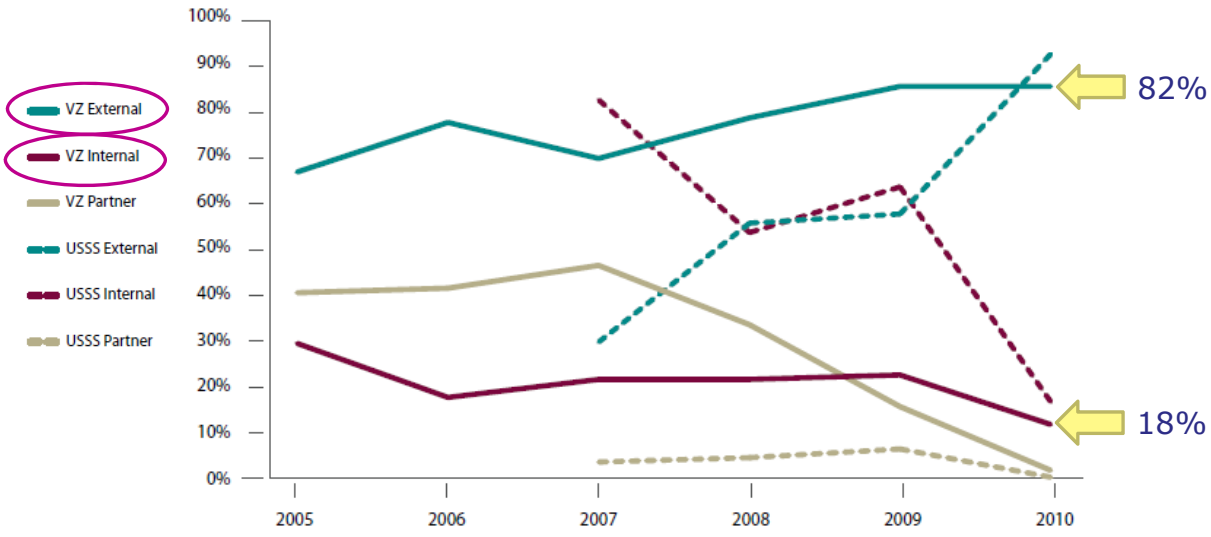
A former IT staffer has pleaded guilty to using a secret vSphere console to wipe company servers



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 boasting online that he was going to reveal "the truth" about the war in Afghanistan.

Beveiligingsincidenten
Statistieken (1/4)



Verizon data breach report 2011

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*

Smals ICT for society
03/2012

Beveiligingsincidenten
Statistieken (3/4)

- 2010 ⇔ 2008

Virus
62% (+41%)

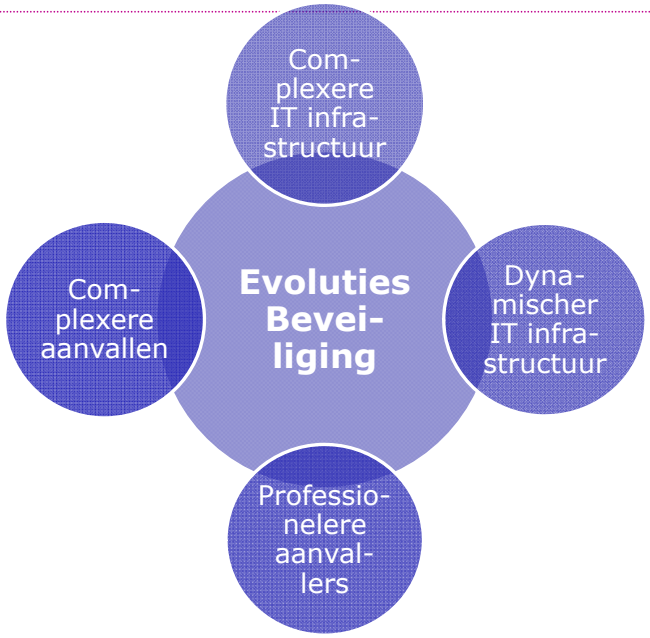
Inbraak
15% (+2%)

Denial of Service
25% (+14%)

Verlies/diefstal data via personeel
46%

PRICEWATERHOUSECOOPERS *Information Security Breaches Survey 2010*

Information security trends (1/3)



Information security trends (2/3)

Gartner (29 november 2011)

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, …)

Agenda

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

Information Security Governance
Aanpak (1/2)

Information Security
Governance & Management

Beleid / Processen

Implementatie / Tools

Information Security Governance
Aanpak (2/2)

Preventie
- Ontradend
- Informerend

PAM, SIEM

Detectie
- Fysiek
- Virtueel

SIEM

Verhindering
- Fysiek
- Virtueel

PAM

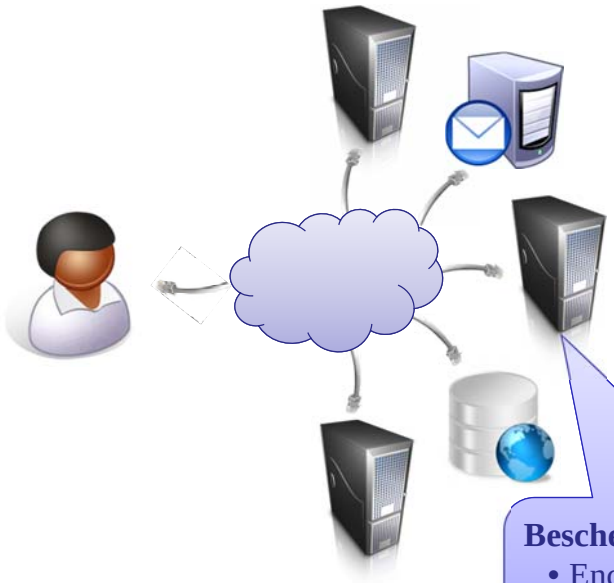
Reactie
- Bestraffend
- Technisch

SIEM

Information Security Governance
Technische veiligheidsmaatregelen (1/4)

Beheer van gebruikers & rechten
- Provisioning / deprovisioning
- Entitlements (access)
- Geprivilegieerde accounts

Information Security Governance
Technische veiligheidsmaatregelen (2/4)

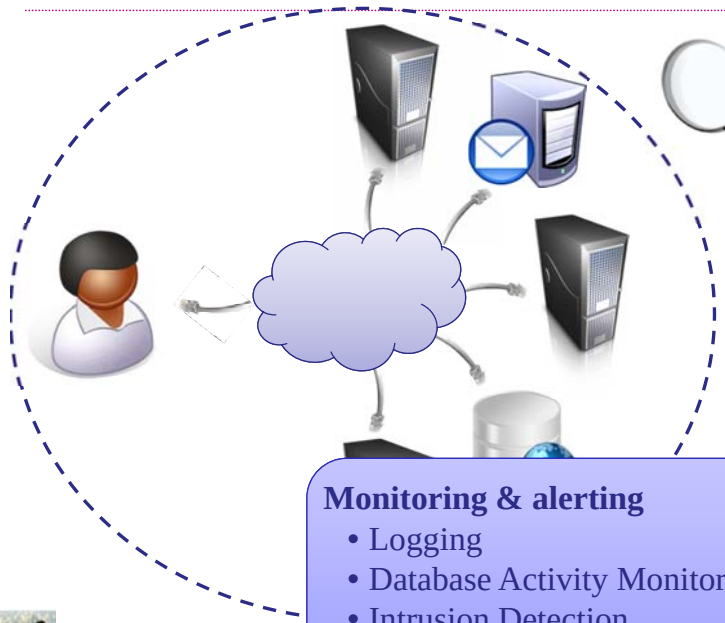


Bescherming van data
- Encryptie / data masking
- Digital Rights Management
- (Endpoint) Data Loss Prevention

Information Security Governance
Technische veiligheidsmaatregelen (3/4)

Bescherming van transport
- Beveiligde verbindingen U2A, A2A
- NAC

Information Security Governance
Technische veiligheidsmaatregelen (4/4)



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

Agenda

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

Insider Threat (1/2)

- Doelbewust
  - Al dan niet uitgebreide toegangsrechten
  - Hacking technieken (privilege escalation)
  - Toegang tot gevoelige data/systemen

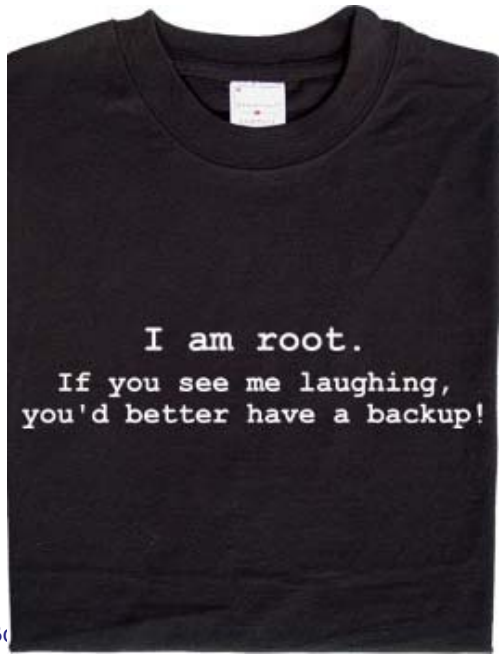
- Onbewust
  - Gewone gebruikers met (teveel) rechten
  - Gevoelige gegevens meenemen/verliezen
  - (Doel van hack-aanval)

Insider Threat (2/2)

- Insider threat ~ 20 à 40 % incidenten
  - 10 à 20% doelbewust ➔ ~ 5%

⚠ Impact omgekeerd evenredig

Wat is "Privileged account management"?



Wat is "Privileged account management"?
Termen & acroniemen

Privileged Access Account Identity User 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

Smals ICT for society
03/2012

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

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

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

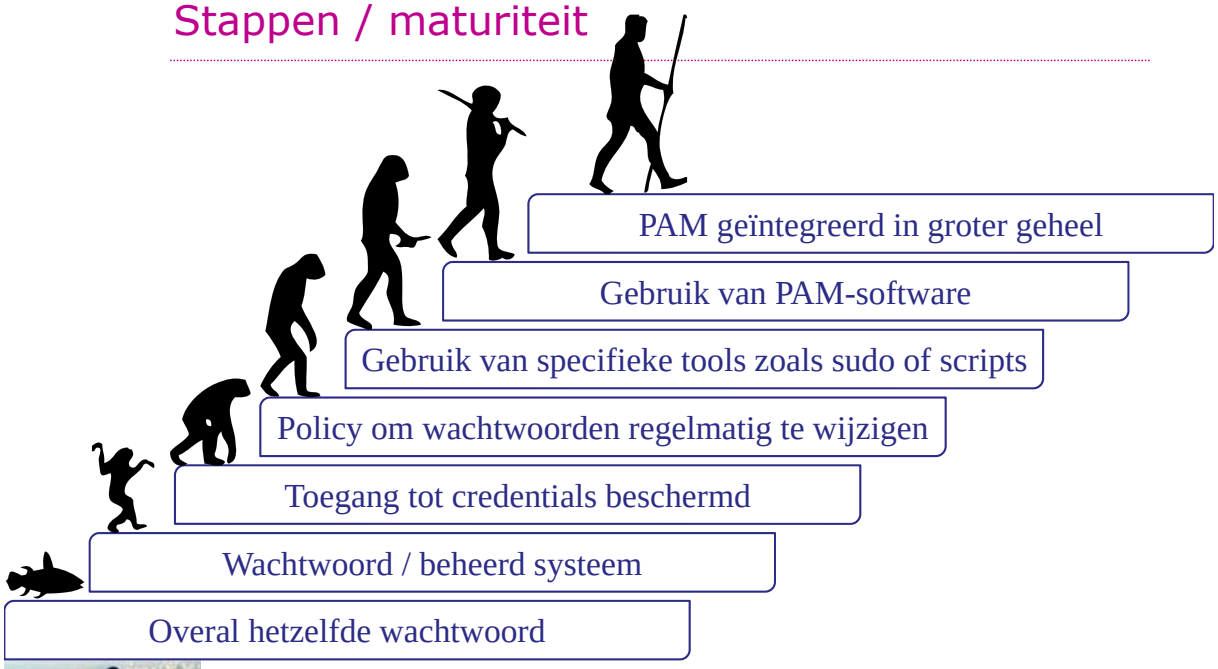
Wat is "Privileged account management"?
Probleem (2/2)

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

Agenda

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

Aanpak
Stappen / maturiteit



Aanpak
Principes

Gewone account

Tijdelijke verhoging van rechten

Administrator

Administratie account naast gewone account
One-time passwords
Toegang tot shared account in noodsituaties

Agenda

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

Aanpak
Software

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

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*

Aanpak
Software

beyondtrust

ca technologies

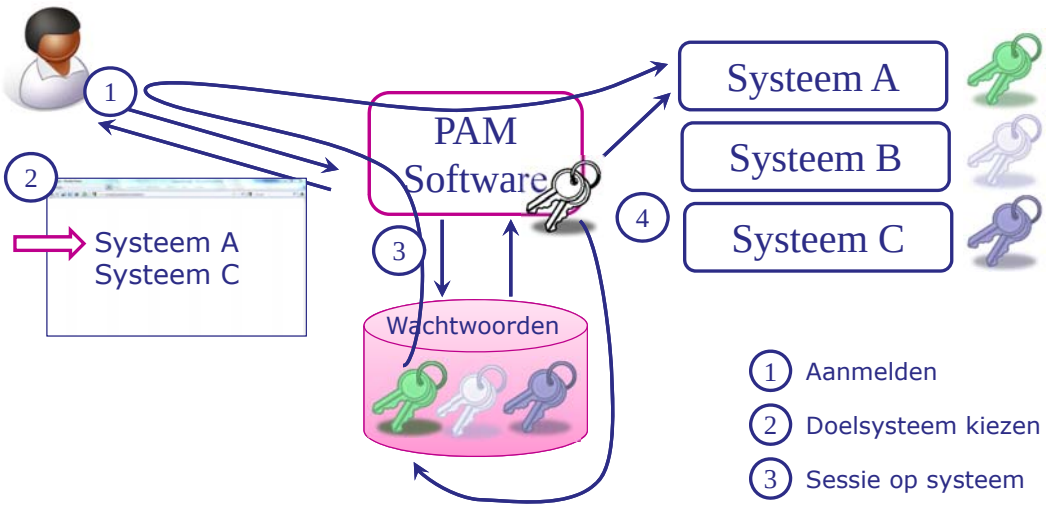
Cyber-Ark

LIEBERMANSOFTWARE

QUEST SOFTWARE

...

Software
Werkingsprincipe



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

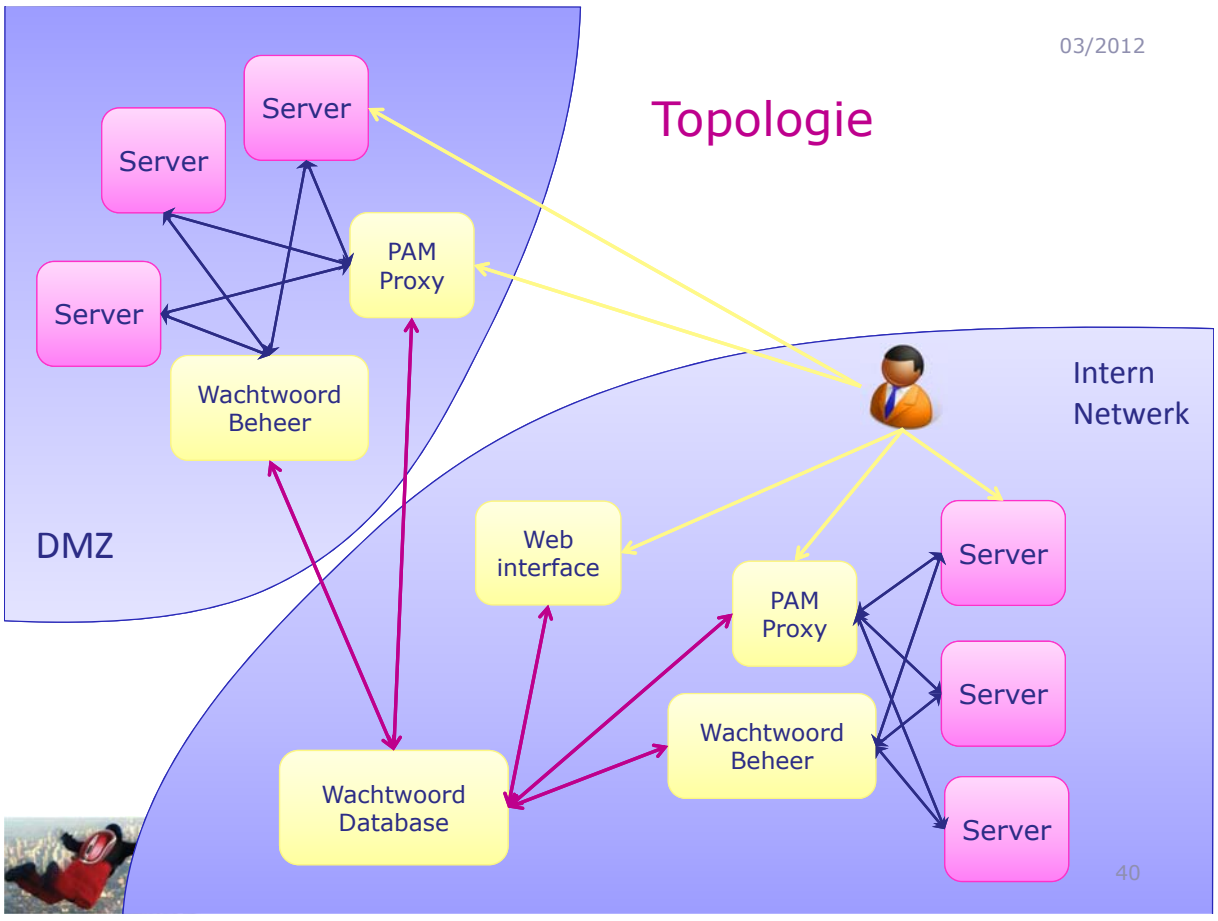
Software
Eigenschappen

- 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)

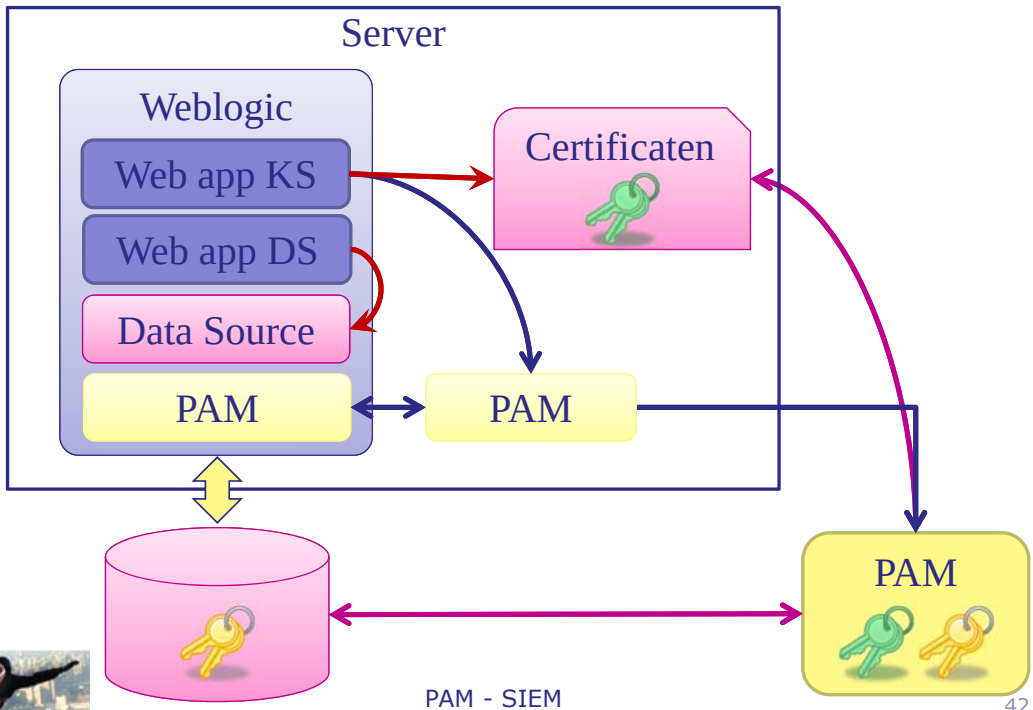
Topologie



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) traffiek blokkeert
- Veranderend serverpark
  - koppeling met tool nodig (API)
- Gelijktijdig gebruik zelfde gedeelde account 

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

Software
Prijsmodellen

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

Agenda

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

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

Agenda

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

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)

Conclusies (2/3)

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

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

bob.lannoy@smals.be
@boblannoy

Agenda

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

Basis-Principes

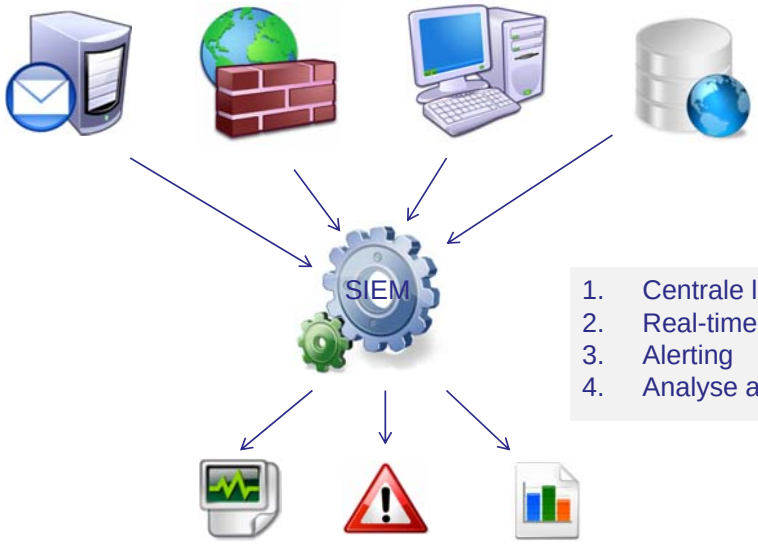
Uitdaging

- Miljoenen logs, slechts enkele incidenten...



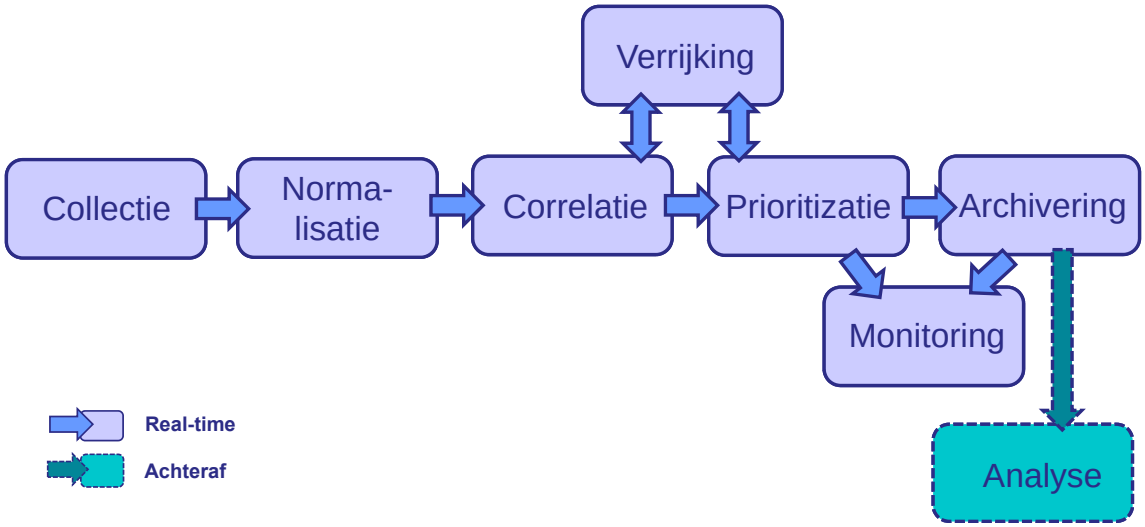
⇨ **Onmogelijk manueel**

De essentie

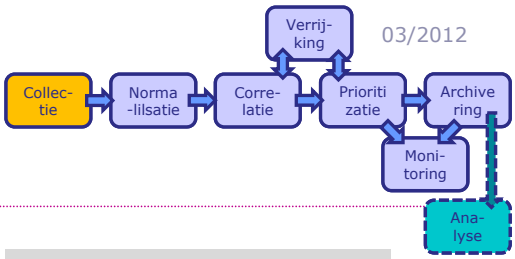


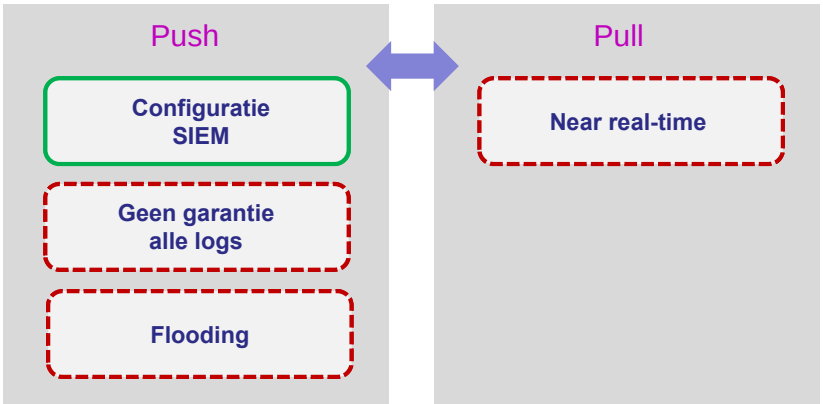
1. Centrale logging
2. Real-time monitoring
3. Alerting
4. Analyse achteraf

Verwerkingsproces



Collectie

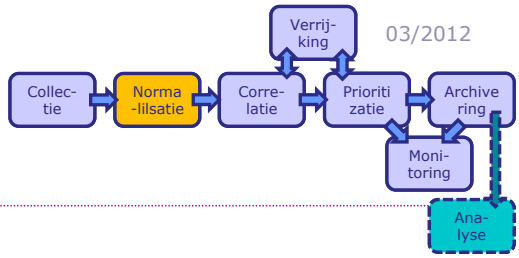


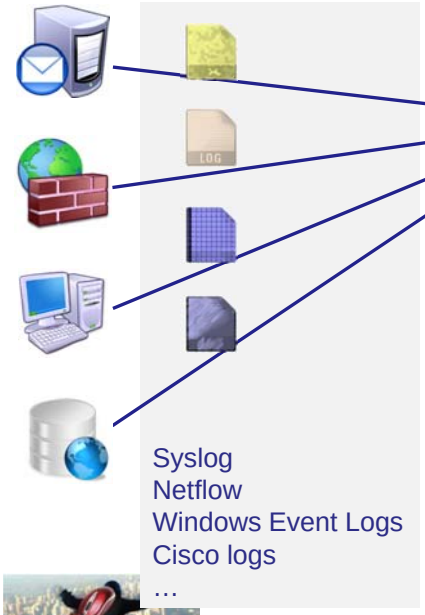


- ⇨ **Ondersteunt SIEM de bron?**
- ⇨ **Soms agent op device nodig**
- ⇨ **Meestal push**

Smals
ICT for society

Normalisatie





Normalisatie

SIEM formaat

Correlatie

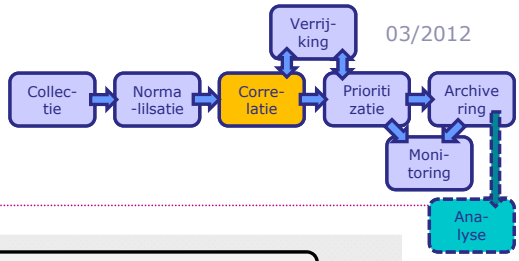
Log
- XML, comma-separated, …

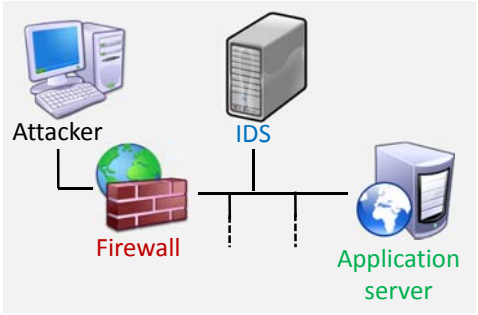
Veld
- "timestamp" , "time" , …

Data
- "Mon, 19 Mar 2012 13:38:11 GMT", 1332164291, …

Smals
ICT for society

Correlatie





Port scan

Failed SSH auth.

Successful SSH auth.

Succesvolle SSH brute-force aanval

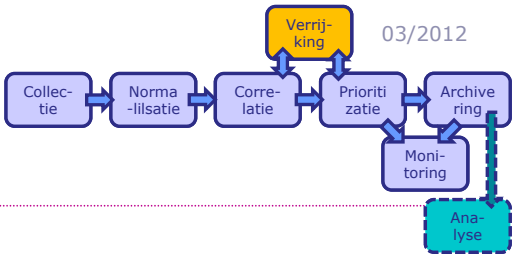
Sudo install …

Reconnaissance

Ongoing intrusion attack from same IP

t

Verrijking



03/2012

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

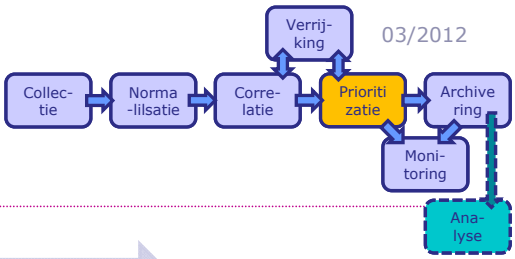
⇨ **Externe bronnen**: DNS, user directories, …

192.168.56.41
- name: Zeus
- group: database servers
- location: SC 03.174

krive
- name: Kristof Verslype
- group: Onderzoek
- role: jr. onderzoeker
- since: 01/12/2011

172.16.254.1
- location: Beijing, China
- domain: kp.cn

Prioritizatie

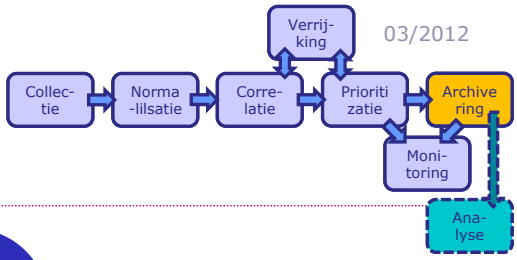


03/2012

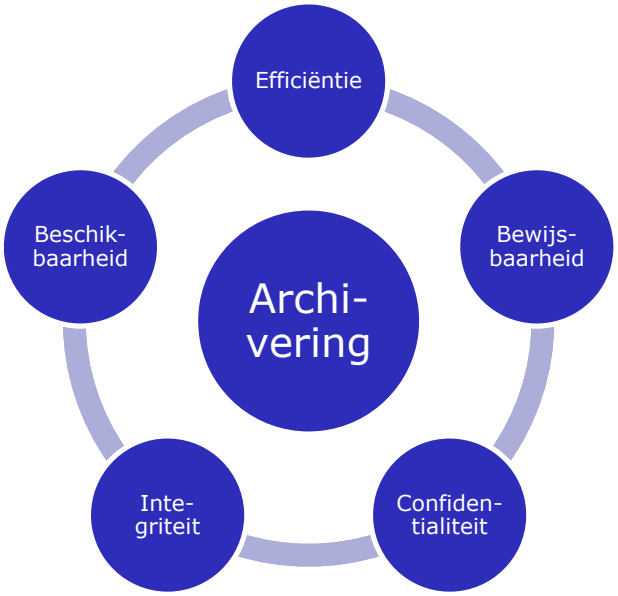
Waarde asset	• Client computer • Kritische server • Idealiter CMDB
Impact bij succes	• Toegang met beperkte privileges • root access • Onafhankelijk van waarde asset
Waarschijnlijkheid op succes	• 2 gefaalde SSH toegangen • 20000 gefaalde SSH toegangen
…	

RISICO

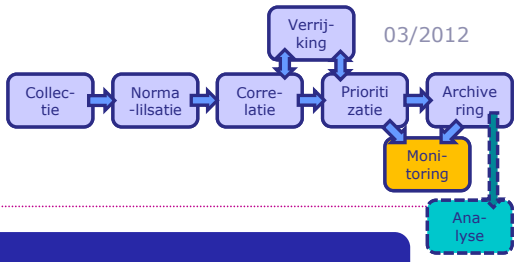
Archivering



03/2012



Monitoring



03/2012

Evalueren

- Kwetsbaarheden
- Verdachte activiteit
- Incidenten

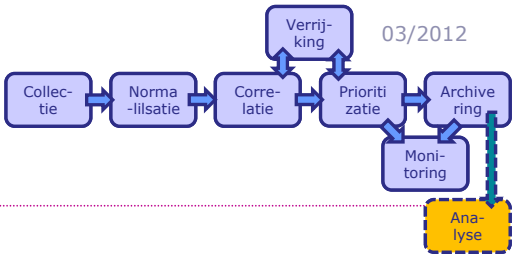
Dashboards

- Remote login
- Idealiter enkele high-priority events

Alarm

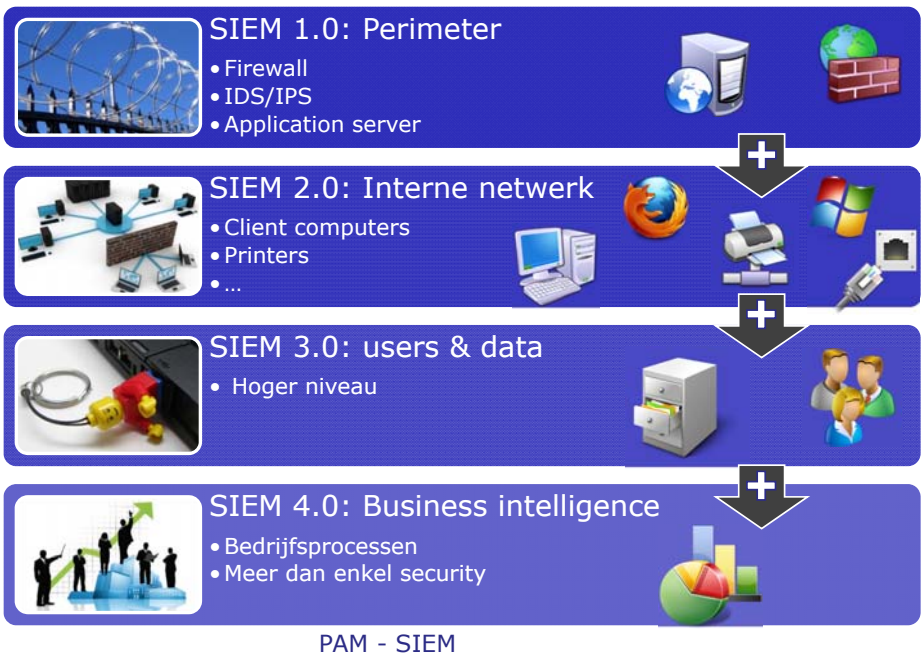
- Dashboard
- E-Mail, SMS, …

Analyse

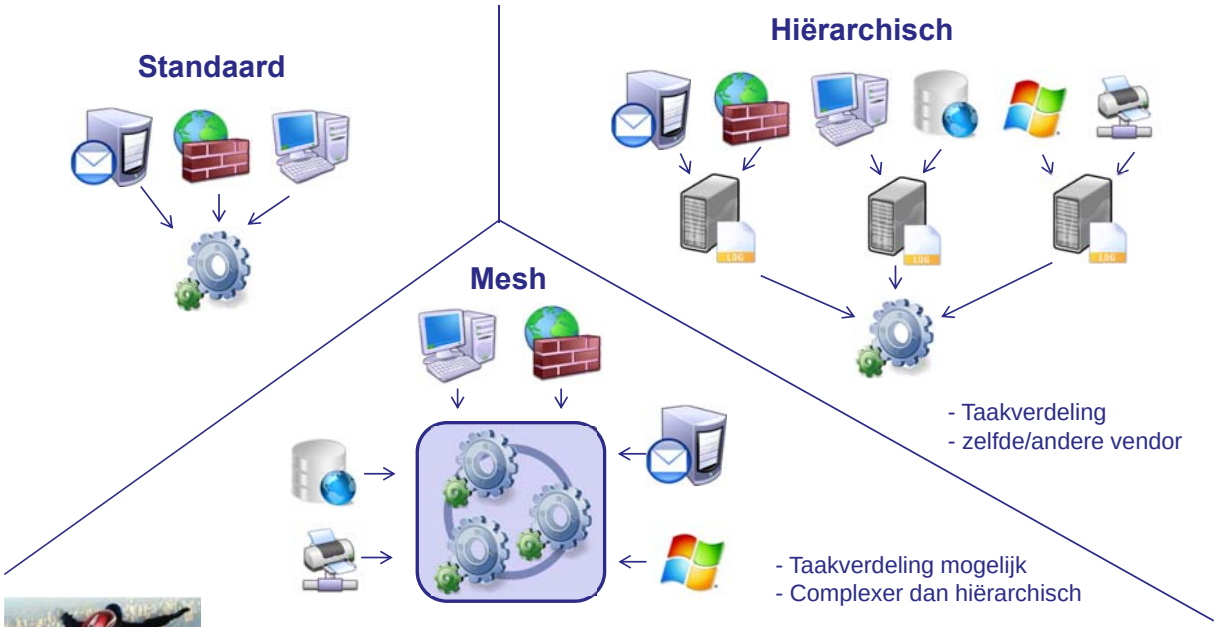


Middel	Reden
Rapporten	Kennis eigen security
Queries	Forensisch onderzoek
	Compliancy

Evolutie



Topologie



Beschikbare systemen

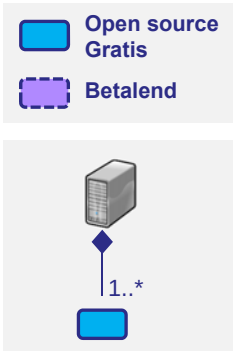
	IBM	QRadar
	McAfee	NITROVIEW
➡	hp	ArcSight (An HP Company)
	RSA EMC²	RSA enVision
➡	alienvault	alienvault
	...	

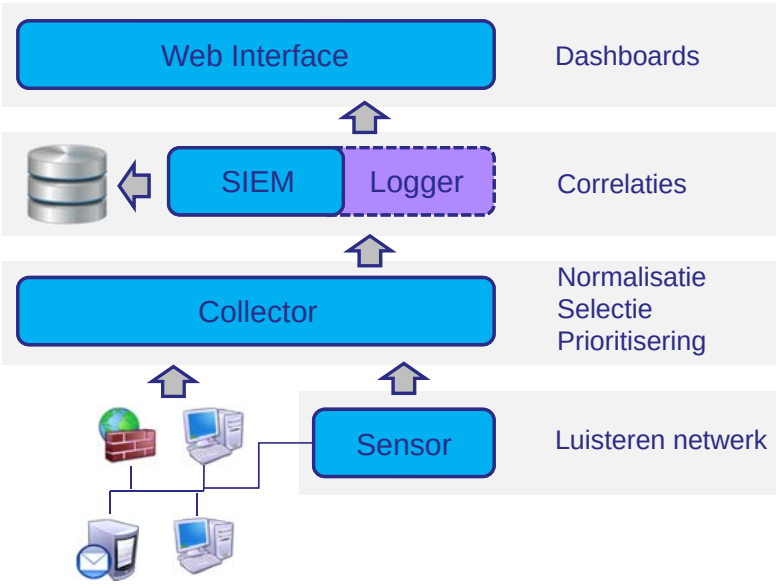
alienvault

Smals ICT for society

alienvault

Componenten





Smals ICT for society

alienvault

Bouwblokken

OCS next generation inventory

Nagios

SNORT

Open source

Integratie in AlienVault

Inprotect

P0f

NFSen/NFDump

ntop

Passive Asset Detection System

osvdb

OSSEC

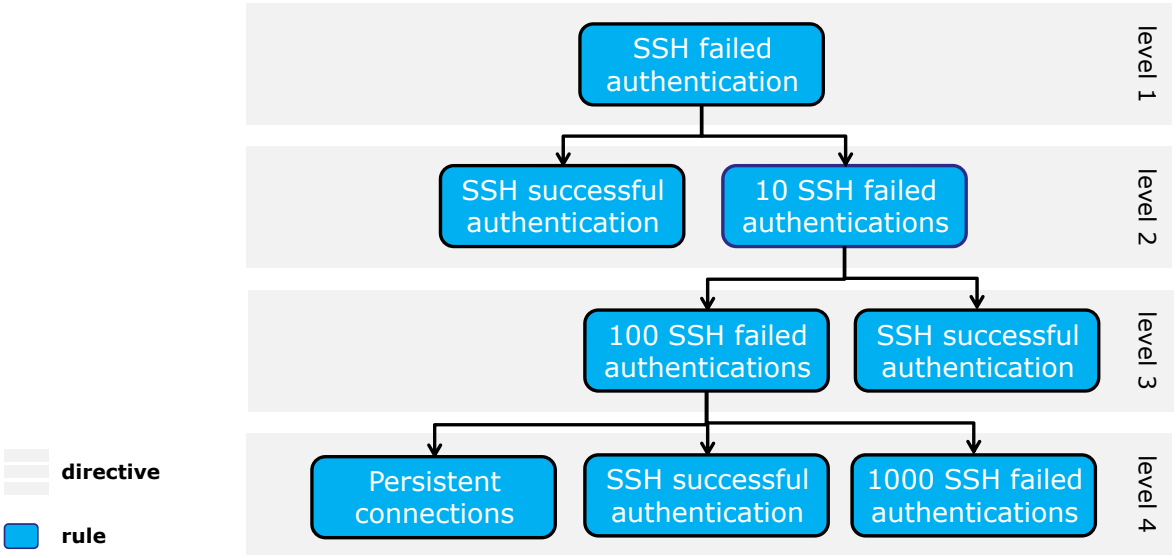
OpenVAS

Smals ICT for society

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}
```

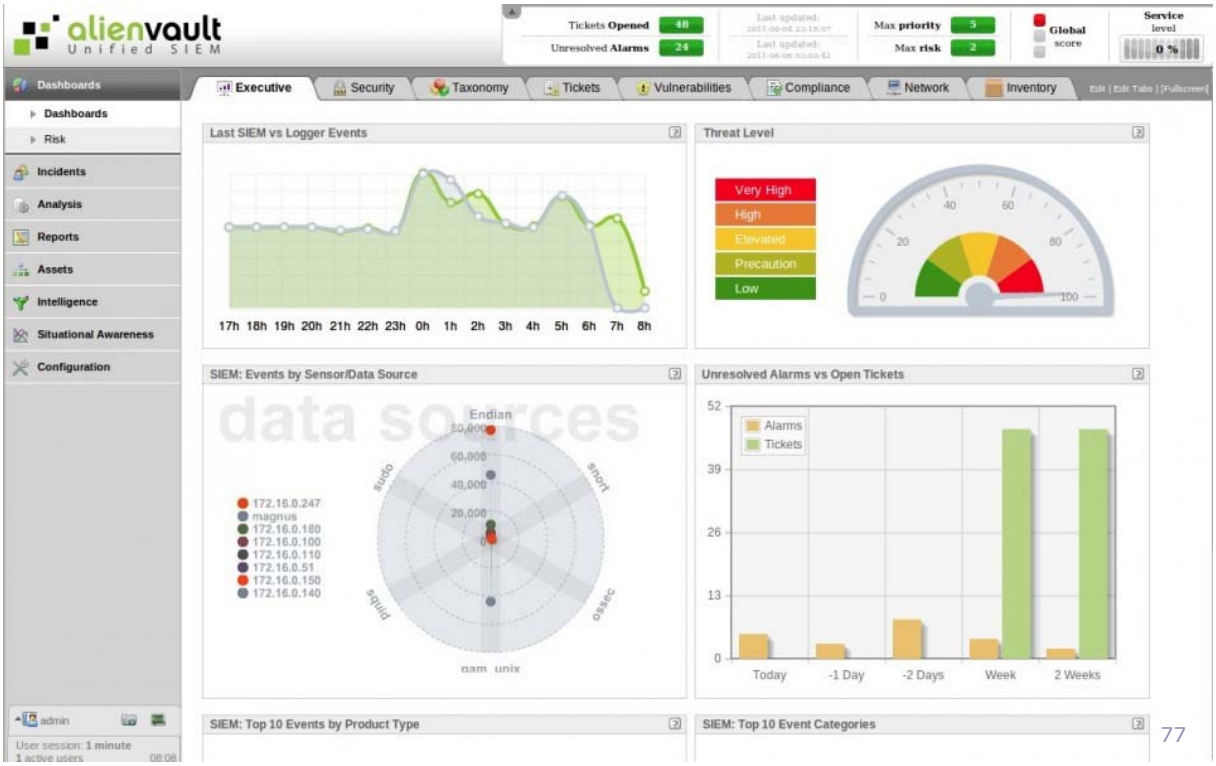
Ondersteuning 2395 bronnen

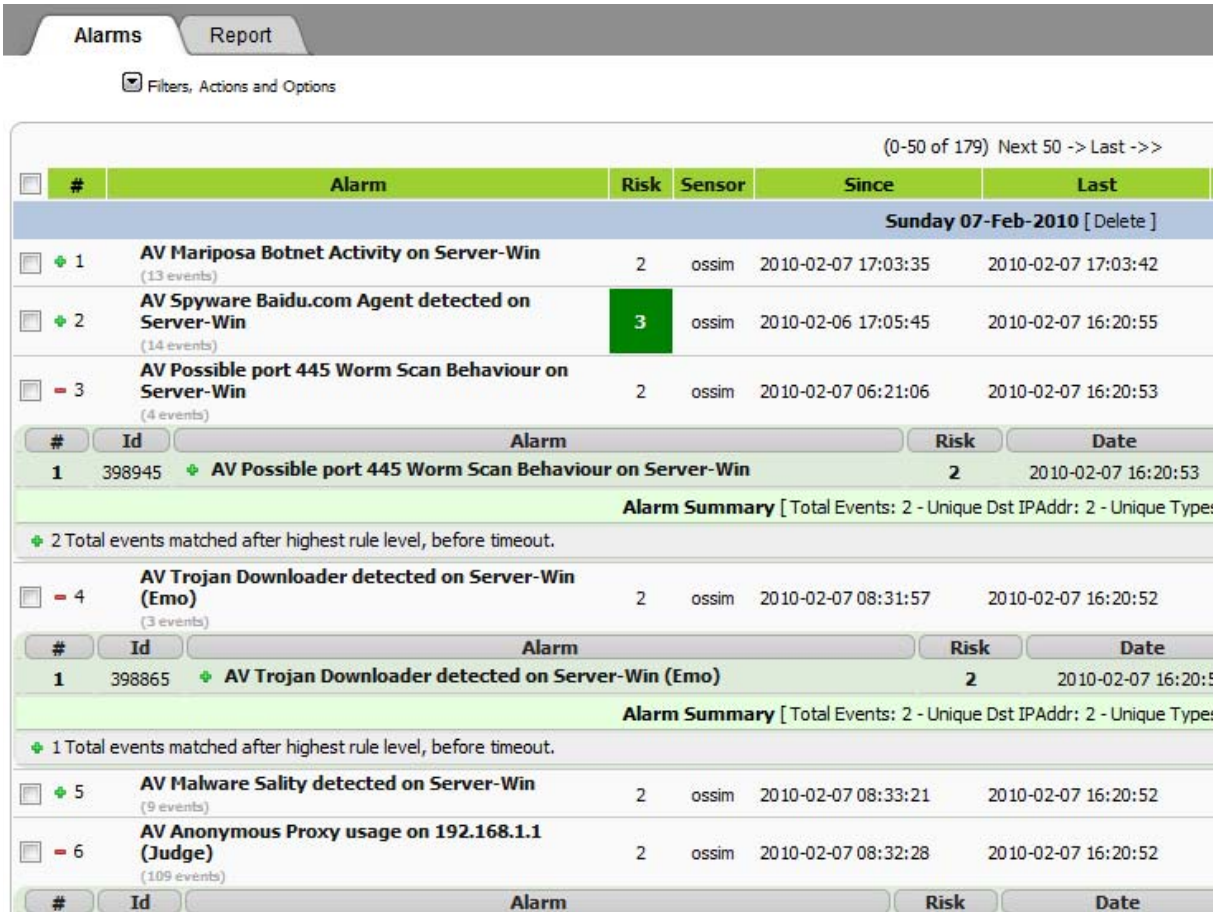
Geen DAM, PAM, …

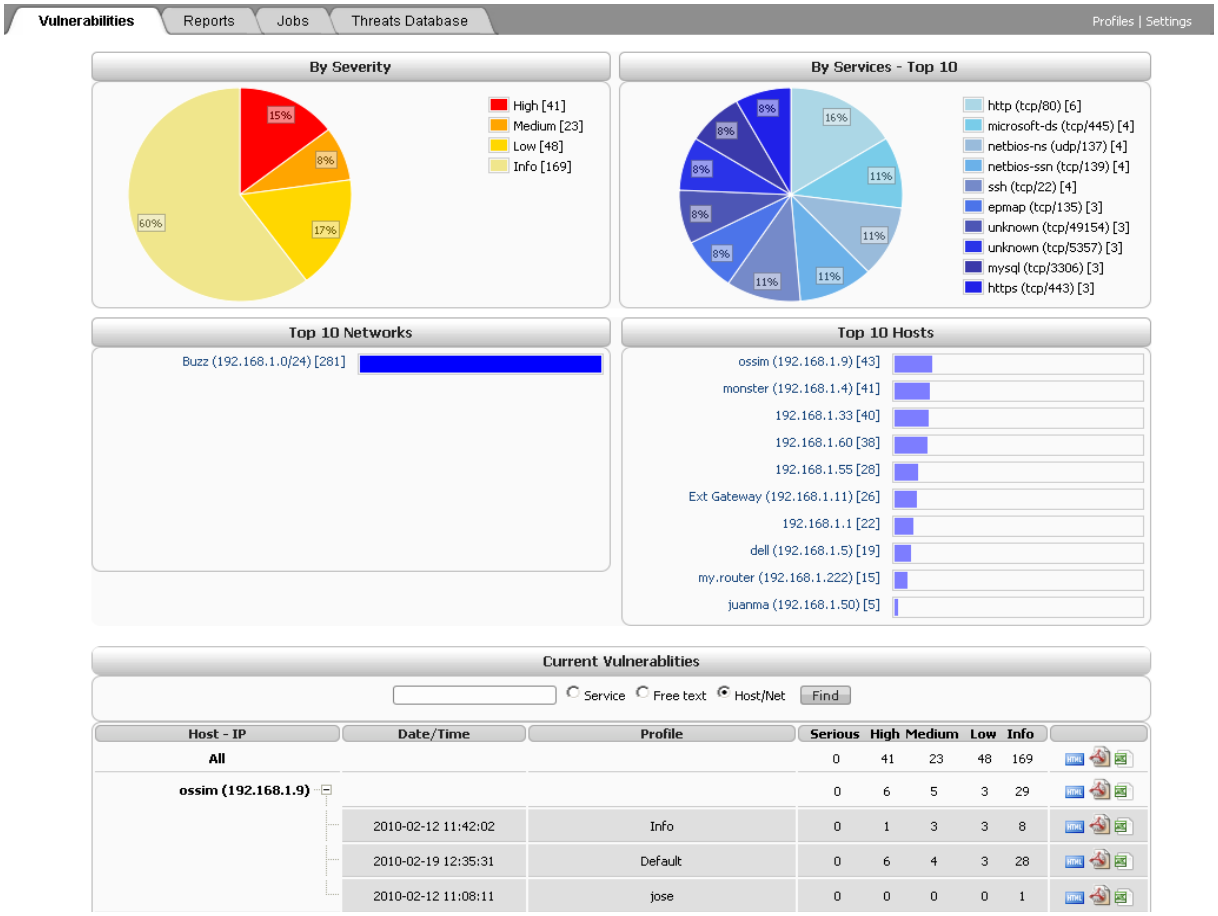
Geen GUI

Screenshots

- Overzicht
- Alarmen
- Kwetsbaarheden


alienvault
Unified SIEM
Tickets Opened 48
Unresolved Alarms 24
Max priority 5
Max risk 2
Global score
Service level 0 %
Dashboards
Dashboards
Risk
Incidents
Analysis
Reports
Assets
Intelligence
Situational Awareness
Configuration
Executive
Security
Taxonomy
Tickets
Vulnerabilities
Compliance
Network
Inventory
Last SIEM vs Logger Events
17h 18h 19h 20h 21h 22h 23h 0h 1h 2h 3h 4h 5h 6h 7h 8h
Threat Level
Very High
High
Elevated
Precaution
Low
SIEM: Events by Sensor/Data Source
data sources
Endian
snort
osiris
pnbs
nessus
nam unix
172.16.0.247
magnus
172.16.0.180
172.16.0.100
172.16.0.110
172.16.0.51
172.16.0.150
172.16.0.140
Unresolved Alarms vs Open Tickets
Alarms
Tickets
Today
-1 Day
-2 Days
Week
2 Weeks
SIEM: Top 10 Events by Product Type
SIEM: Top 10 Event Categories


Alarms
Report
Filters, Actions and Options
(0-50 of 179) Next 50 -> Last ->>
Alarm Risk Sensor Since Last
Sunday 07-Feb-2010 [Delete]
1 AV Mariposa Botnet Activity on Server-Win (13 events) 2 ossim 2010-02-07 17:03:35 2010-02-07 17:03:42
2 AV Spyware Baidu.com Agent detected on Server-Win (14 events) 3 ossim 2010-02-06 17:05:45 2010-02-07 16:20:55
3 AV Possible port 445 Worm Scan Behaviour on Server-Win (4 events) 2 ossim 2010-02-07 06:21:06 2010-02-07 16:20:53
Id Alarm Risk Date
1 398945 AV Possible port 445 Worm Scan Behaviour on Server-Win 2 2010-02-07 16:20:53
Alarm Summary [Total Events: 2 - Unique Dst IPAddr: 2 - Unique Type
2 Total events matched after highest rule level, before timeout.
4 AV Trojan Downloader detected on Server-Win (Emo) (3 events) 2 ossim 2010-02-07 08:31:57 2010-02-07 16:20:52
Id Alarm Risk Date
1 398865 AV Trojan Downloader detected on Server-Win (Emo) 2 2010-02-07 16:20:5
Alarm Summary [Total Events: 2 - Unique Dst IPAddr: 2 - Unique Type
1 Total events matched after highest rule level, before timeout.
5 AV Malware Sality detected on Server-Win (9 events) 2 ossim 2010-02-07 08:33:21 2010-02-07 16:20:52
6 AV Anonymous Proxy usage on 192.168.1.1 (Judge) (109 events) 2 ossim 2010-02-07 08:32:28 2010-02-07 16:20:52
Id Alarm Risk Date



Smals ICT for society

alienvault

Aandachtspunten

Configuratie

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

Krachtige servers

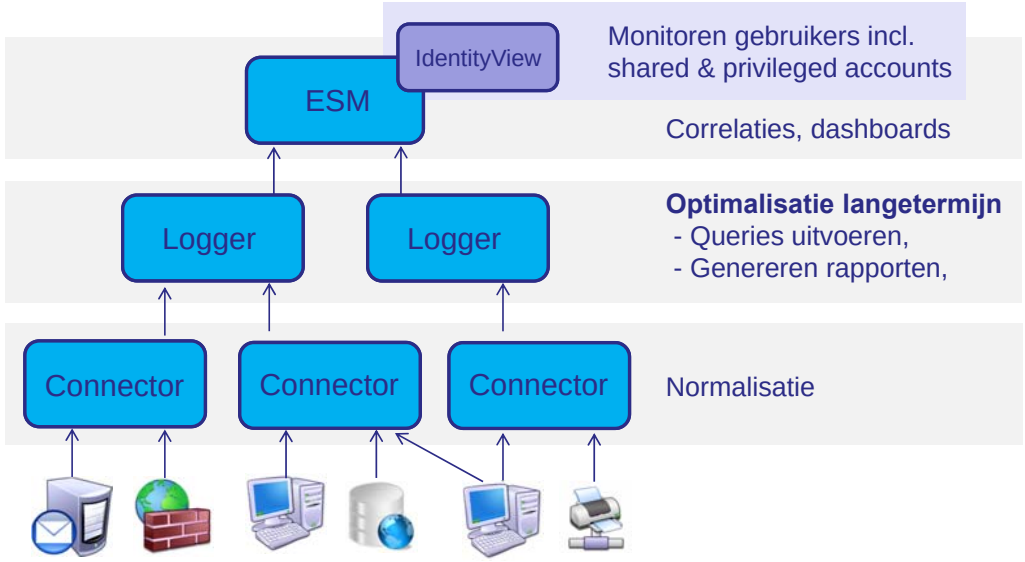
- Normaliseren
- Correleren

ArcSight™ An HP Company

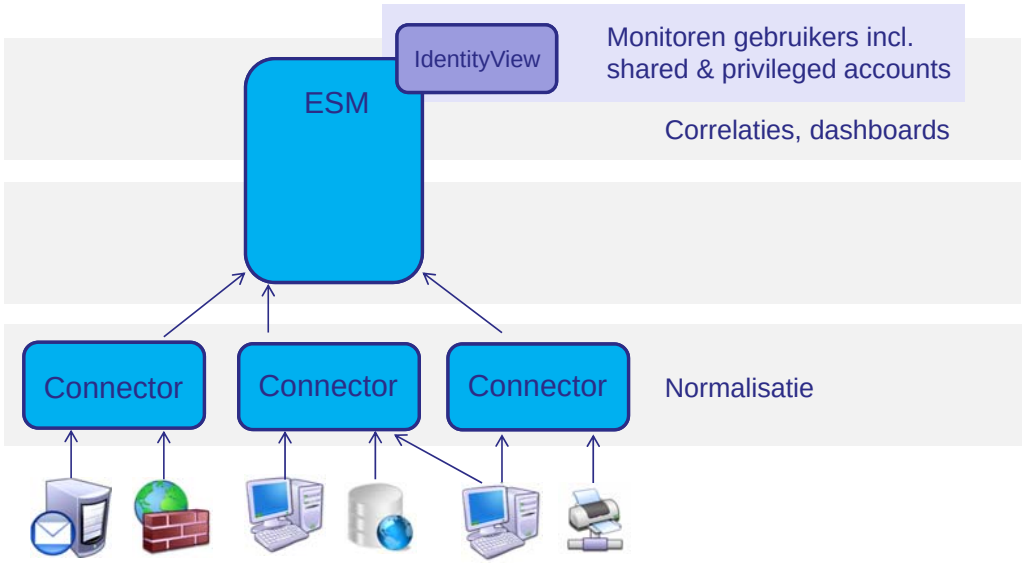
Smals ICT for society

ArcSight An HP Company

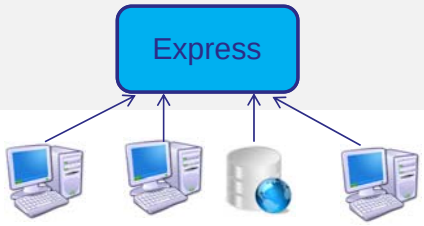
Componenten (1/3)



Componenten (2/3)

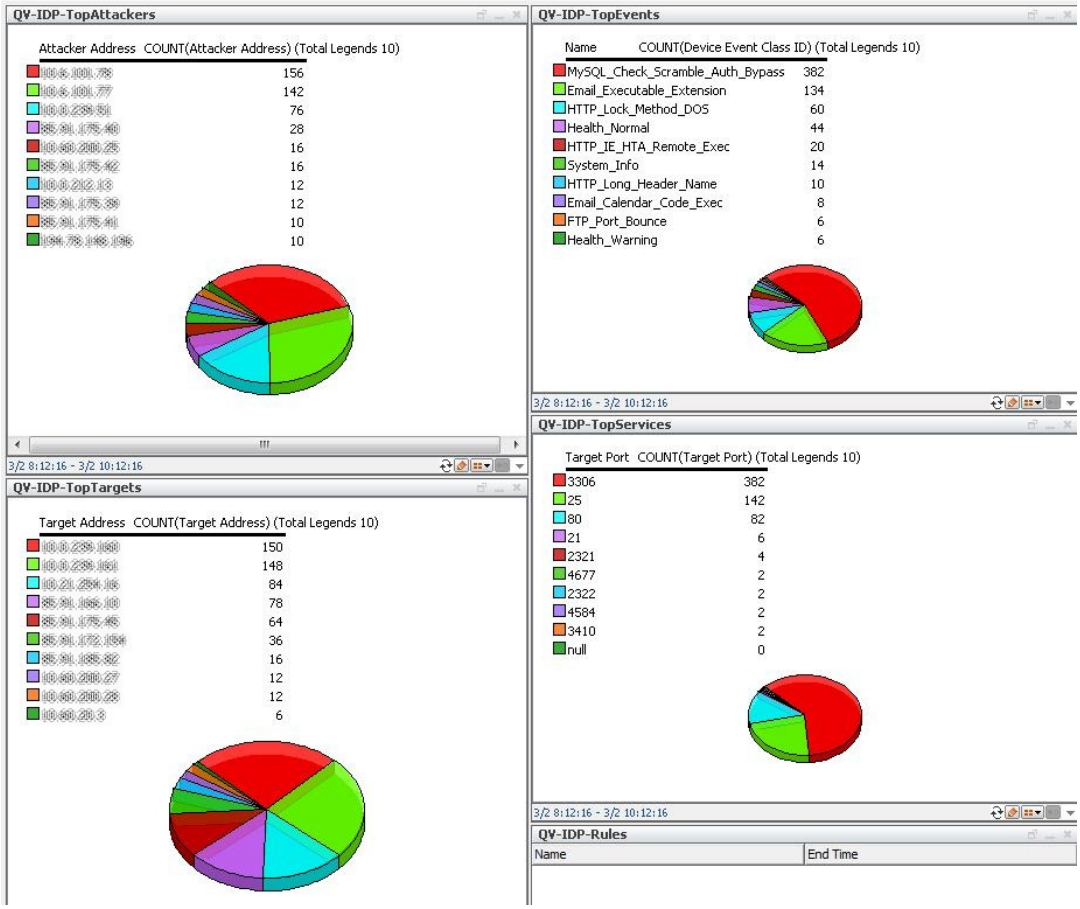


Componenten (3/3)



Screenshots

- Top-10
- Events
- Actuele aanvallen
- Statistieken

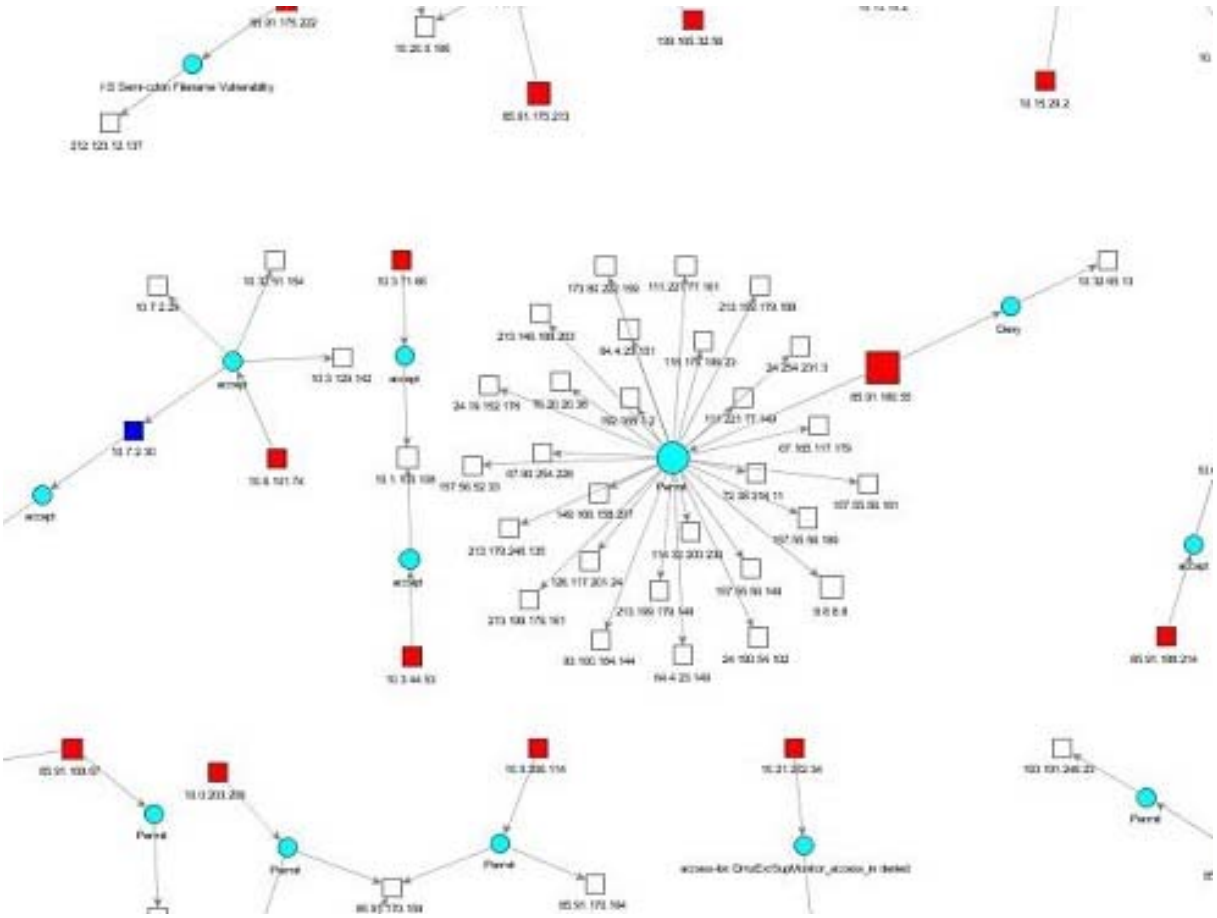


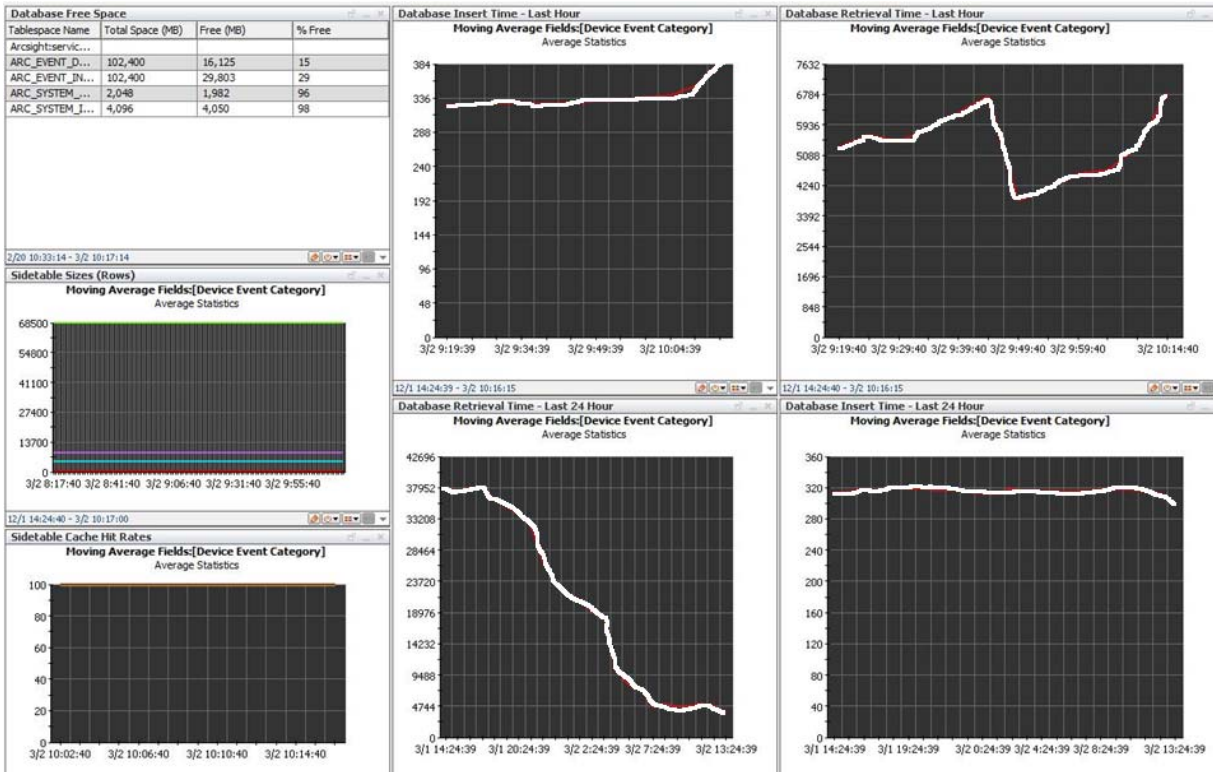
Start Time: 2 Mar 2012 09:43:47 CET
End Time: 2 Mar 2012 11:43:47 CET
Filter: Agent ID = "IBM SiteProtector"
Inline Filter: No Filter
Verified Rules: No Rule

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	[redacted]	[redacted]	5
2 Mar 2012 10:04:44 CET	2 Mar 2012 10:13:14 CET	MySQL_Check_Scramble_Auth_Bypass	[redacted]	[redacted]	5
2 Mar 2012 10:04:44 CET	2 Mar 2012 10:13:20 CET	TCP_Port_Scan	[redacted]	[redacted]	5
2 Mar 2012 10:04:44 CET	2 Mar 2012 10:13:19 CET	TCP_Port_Scan	[redacted]	[redacted]	5
2 Mar 2012 10:04:44 CET	2 Mar 2012 10:12:18 CET	TCP_Port_Scan		[redacted]	5
2 Mar 2012 10:04:29 CET	2 Mar 2012 10:11:53 CET	TCP_Port_Scan	[redacted]	[redacted]	5
2 Mar 2012 10:04:29 CET	2 Mar 2012 10:12:55 CET	TCP_Port_Scan	[redacted]	[redacted]	5
2 Mar 2012 10:04:29 CET	2 Mar 2012 10:12:57 CET	TCP_Port_Scan	[redacted]	[redacted]	5
2 Mar 2012 10:04:29 CET	2 Mar 2012 10:11:58 CET	TCP_Port_Scan	[redacted]	[redacted]	5
2 Mar 2012 10:04:29 CET	2 Mar 2012 10:11:55 CET	TCP_Port_Scan	[redacted]	[redacted]	5
2 Mar 2012 10:04:29 CET	2 Mar 2012 10:11:58 CET	TCP_Port_Scan	[redacted]	[redacted]	5
2 Mar 2012 10:04:29 CET	2 Mar 2012 10:13:01 CET	TCP_Port_Scan	[redacted]	[redacted]	5
2 Mar 2012 10:04:29 CET	2 Mar 2012 10:12:59 CET	TCP_Port_Scan	[redacted]	[redacted]	5
2 Mar 2012 10:03:49 CET	2 Mar 2012 10:11:15 CET	TCP_Port_Scan		[redacted]	5
2 Mar 2012 10:03:49 CET	2 Mar 2012 10:12:17 CET	TCP_Port_Scan	[redacted]	[redacted]	5
2 Mar 2012 10:03:49 CET	2 Mar 2012 10:12:18 CET	TCP_Port_Scan	[redacted]	[redacted]	5
2 Mar 2012 10:03:49 CET	2 Mar 2012 10:12:18 CET	TCP_Port_Scan	[redacted]	[redacted]	5
2 Mar 2012 10:03:34 CET	2 Mar 2012 10:12:04 CET	TCP_Port_Scan	[redacted]	[redacted]	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	[redacted]	[redacted]	5
2 Mar 2012 10:03:29 CET	2 Mar 2012 10:11:53 CET	TCP_Port_Scan	[redacted]	[redacted]	5
2 Mar 2012 10:03:29 CET	2 Mar 2012 10:10:56 CET	TCP_Port_Scan	[redacted]	[redacted]	5
2 Mar 2012 10:03:29 CET	2 Mar 2012 10:10:53 CET	TCP_Port_Scan	[redacted]	[redacted]	5
2 Mar 2012 10:03:29 CET	2 Mar 2012 10:10:56 CET	TCP_Port_Scan	[redacted]	[redacted]	5





Functionaliteit (1/2)

Real-Time monitoring

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

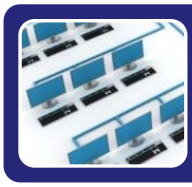
Reactie

- 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?

Kostenmodel

Compo-nent
- Appliance
- Virtual appliance
- Software

Hardware
- Aantal geactiveerde cores in appliance
- Eigen hardware
- …

Functio-naliteit
- Detectie low-and-slow attacks
- Langetermijn
- …

Bron device
- Per device
- Zou meevallen in totale prijs

Ervaringen

Meerwaarde	Gesloten
Beperkte overhead < 5% netwerk	Duur
Anti-forensics onmogelijk	Beheer soms omslachtig
	Typisch wat ach-terstand op markt
	Query kan lang duren (zonder logger)
	Update SIEM devices ≠ evident

Managed SIEM

SIEM

- Investerings-kosten
- Onderhoud
- Expertise
- 24/7/364 monitoring

Managed Siem

MSSP (Managed Security Service provider)

Pro's & cons

- Quasi geen in-vesteringskosten
- SIEM Expertise
- Minder onderhoud
- Grotere security intelligence
- Schaalbaarheid
- Escalatie naar andere bedrijven
- 24/7/365 monitoring

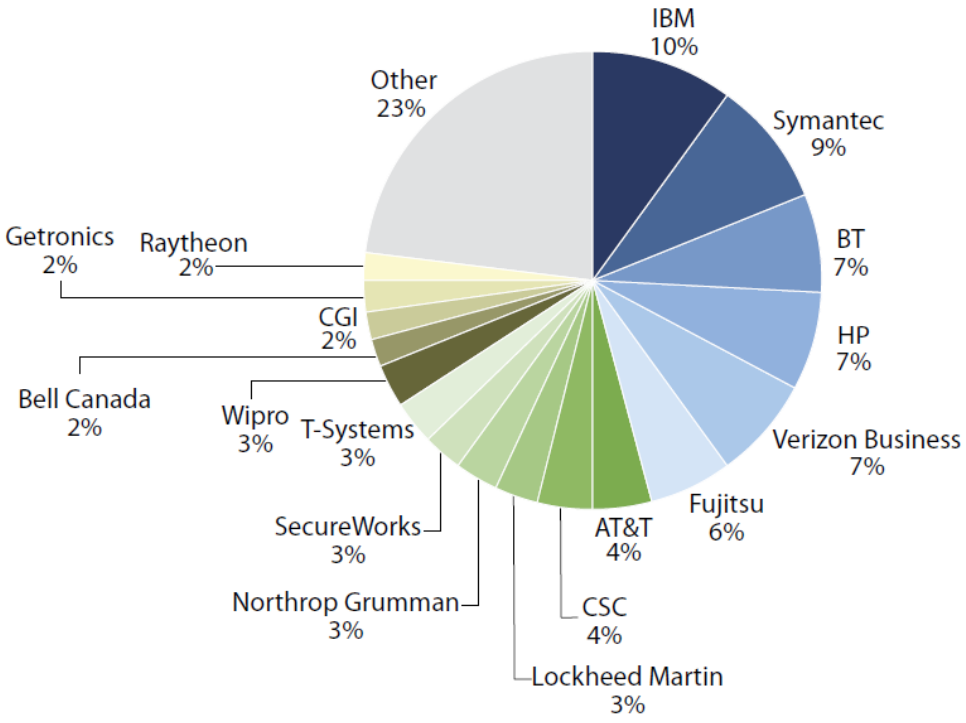
- Outsourcen Security
- Afhankelijkheid Internet
- Beperktere functionaliteit
- Beperktere HW/SW

- Beheers kosten?

Managed Security Services

Company managed	Co-managed	Provider managed
Bedrijf beheert eigen SIEM	Provider beheert SIEM in bedrijf	Logs -> provider
Monitoring & escalatie door bedrijf	Monitoring & escalatie door provider	Monitoring & escalatie door provider
Ondersteuning door provider	[Provider beheert deel hardware]	[Provider beheert deel hardware]
	Switch company managed kan	

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

Business

- Incidence response plan
- Getrainde mensen
- Business requirements
- Draagvlak/ Betrokkenheid

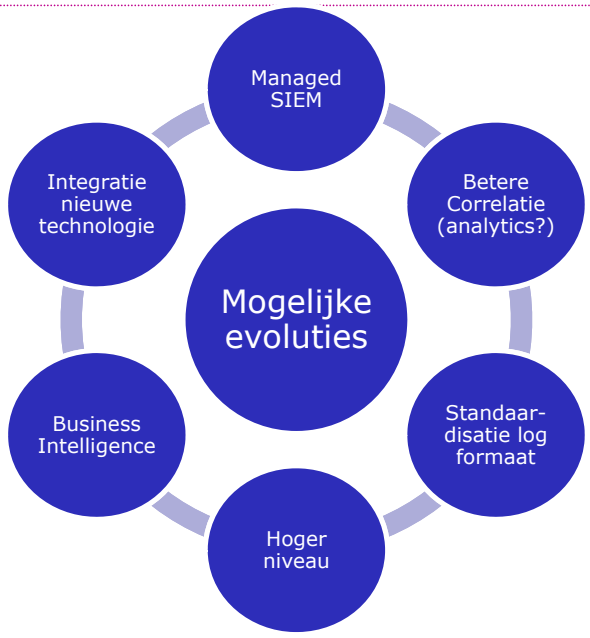
Infrastructuur

- Kennis infrastructuur
- Geen zwarte gaten
- Device klok synchronisatie
- Langetermijn opslag

Uitrol & gebruik

- Geen ‘plug & Play’
- Finetuning
- Documenteer
- Gefaseerde uitrol
- Onderhoud

Mogelijke evoluties



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

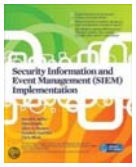
Gratis kennismaking

- AlienVault
- Weinig intrusief
- Beperktere functionaliteit

Correlatieregels!

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

Vragen

Met dank aan
Bart Maes
Marc Vael
Johan Costrop
David Tillemans
Michel Brouyère

kristof.verslype@smals.be
Smals Onderzoek

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

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 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 ~]$
```

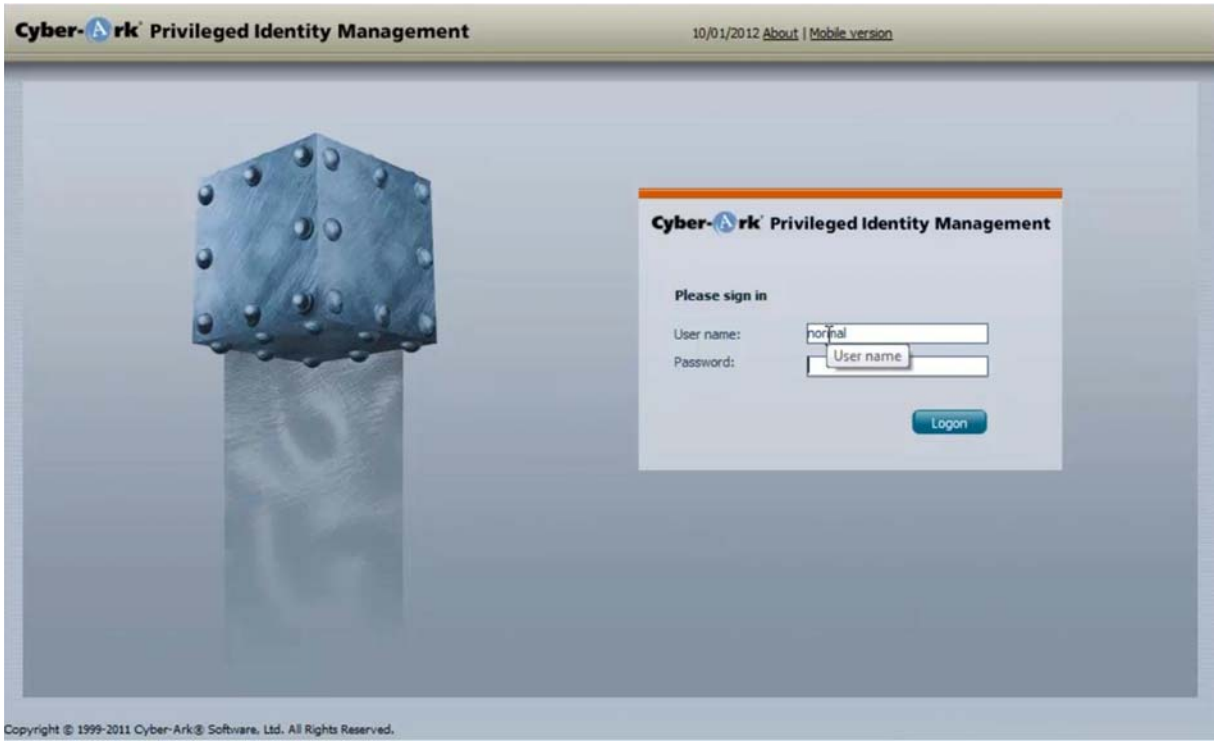
Sudo configuratie (sudoers)

```
# 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
```

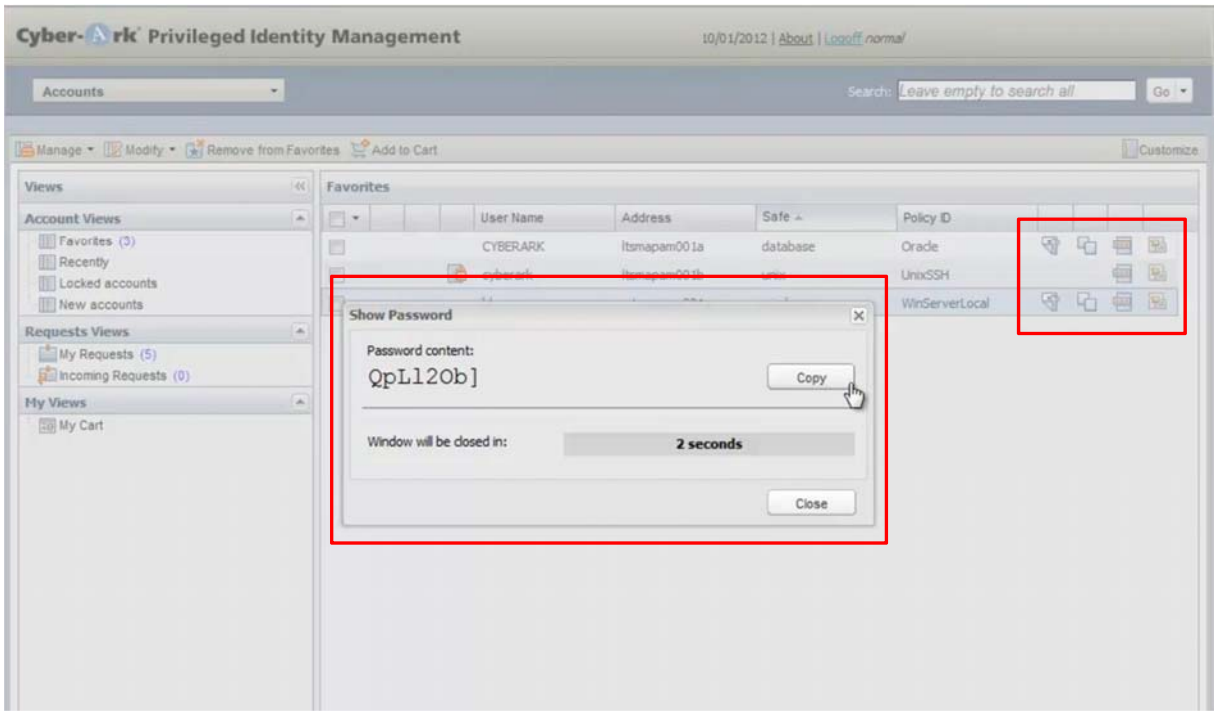
Sudo – shell escaping & noexec

```
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 rsausers" not met by user "normuser"
Jan 12 15:15:39 ltsmapam001b sudo: pam_succeed_if(sudo:auth): requirement "user
notingroup ldap-rsausers" 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 ~]$
```

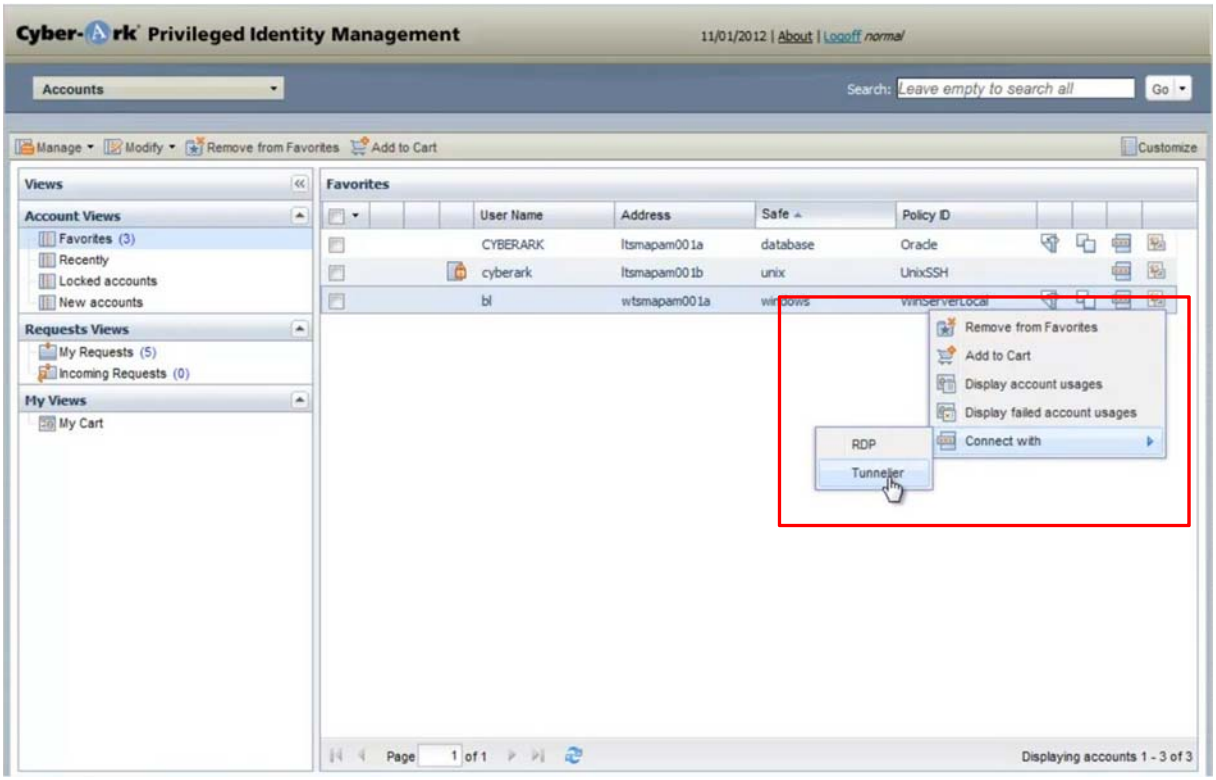
PAM-tool web-login



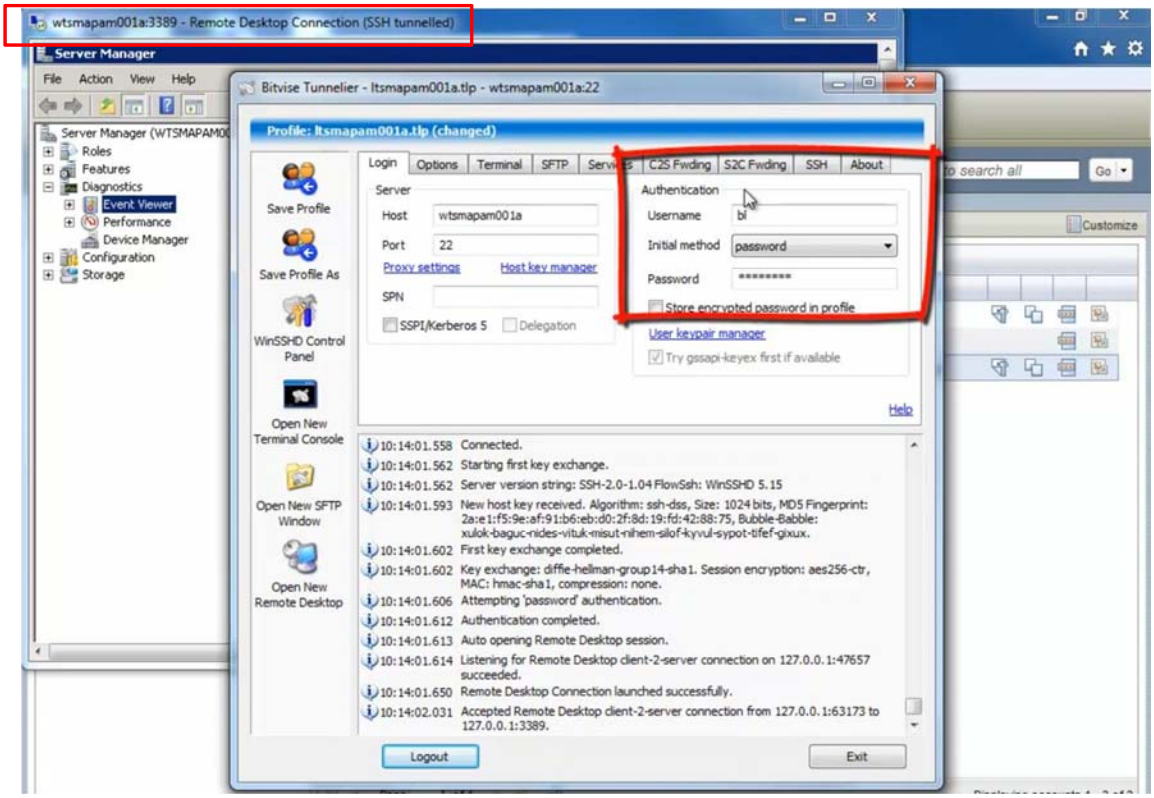
Wachtwoord opties & tonen wachtwoord



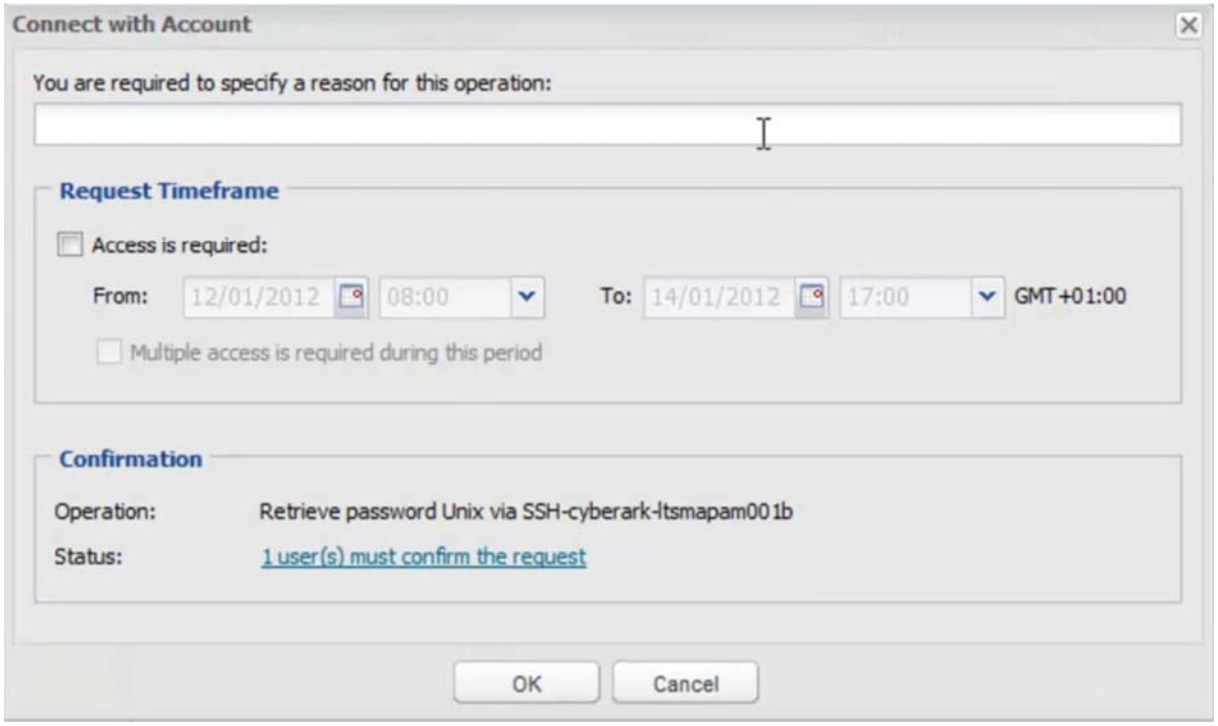
Integratie lokale software (Tunnelier) (1/2)

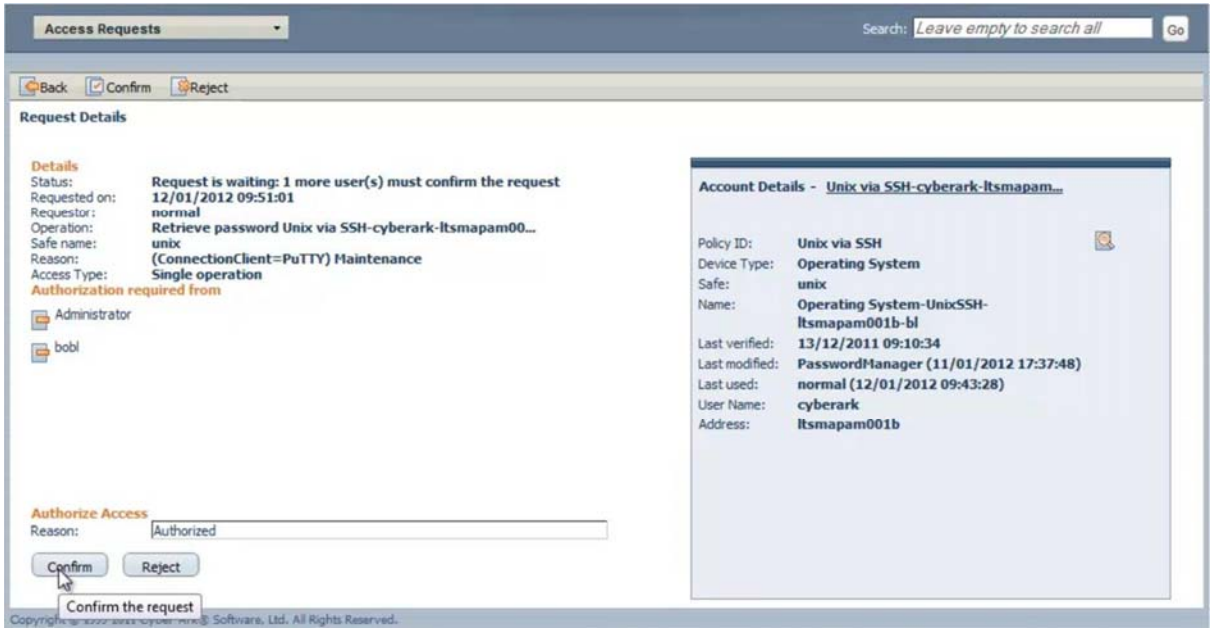


Integratie lokale software (Tunnelier) (2/2)



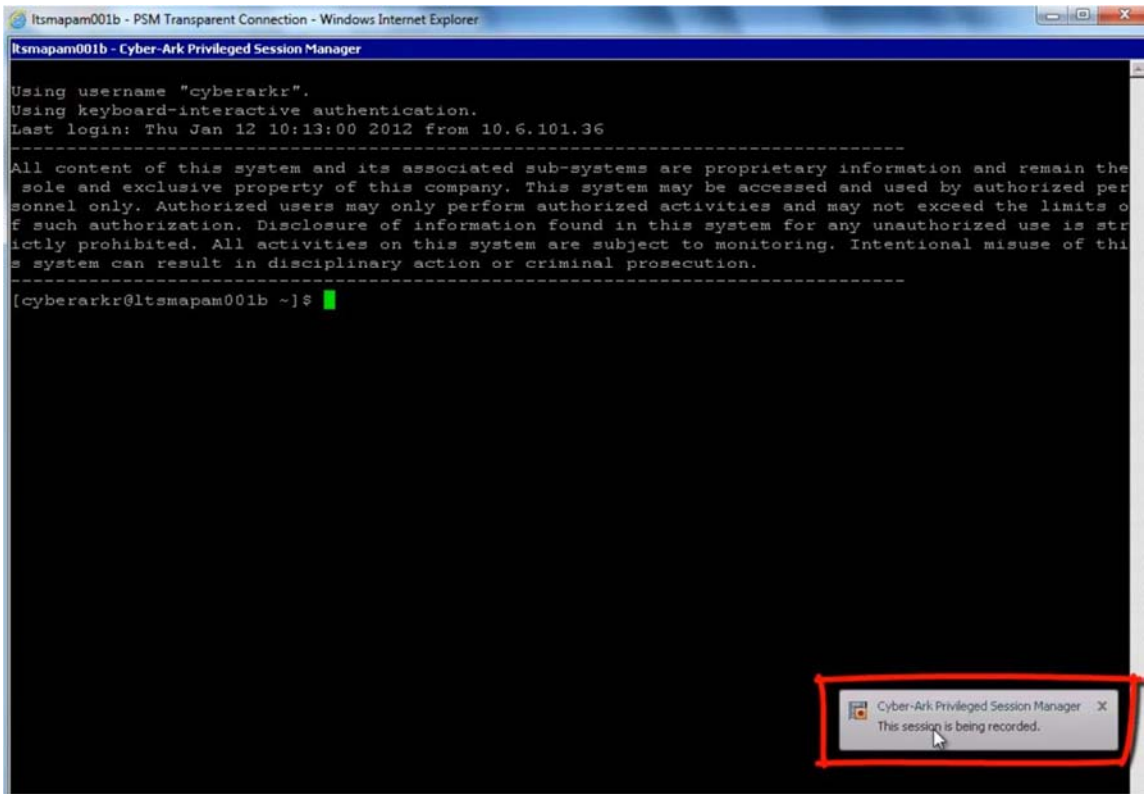
Workflow (1/2)


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

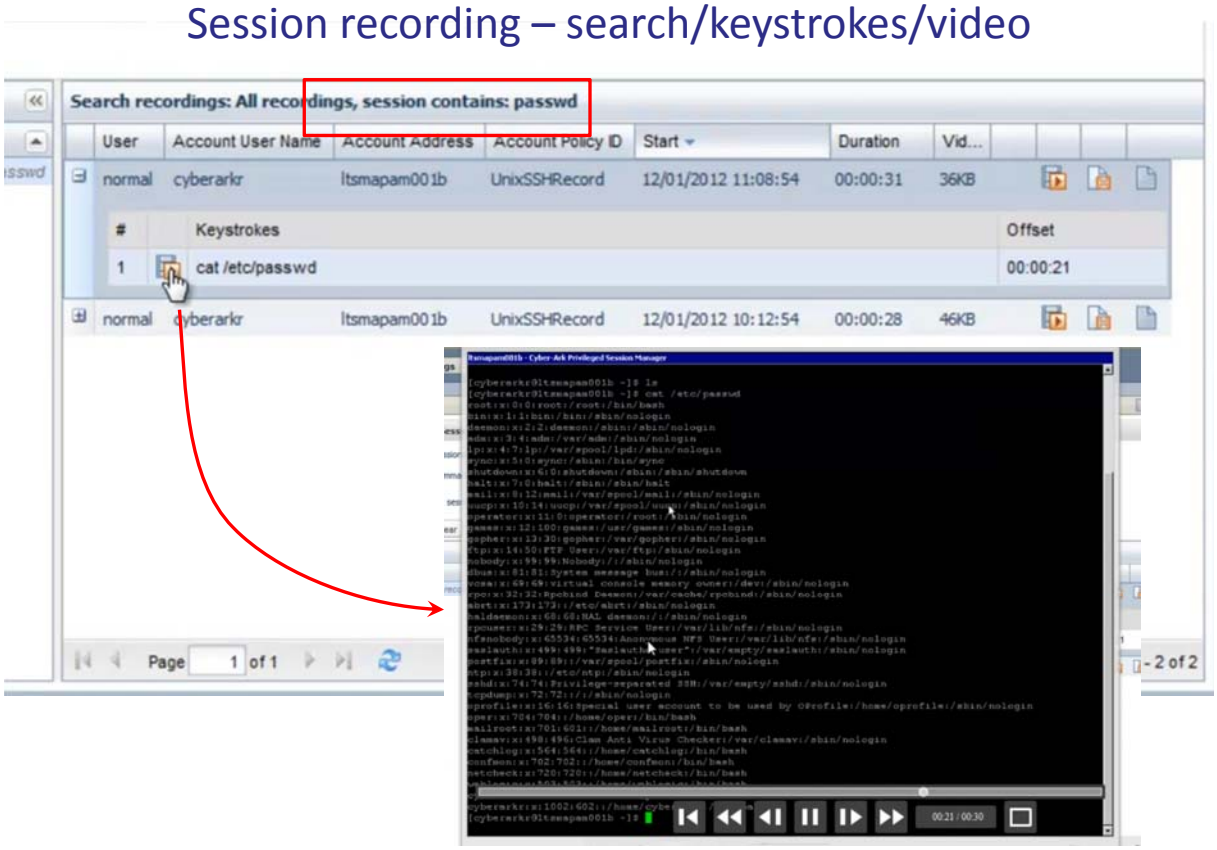

Access Requests
Search: Leave empty to search all
Go
Back
Confirm
Reject
Request Details
Details
Status: Request is waiting: 1 more user(s) must confirm the request
Requested on: 12/01/2012 09:51:01
Requestor: normal
Operation: Retrieve password Unix via SSH-cyberark-ltsmapam00...
Safe name: unix
Reason: (ConnectionClient=PuTTY) Maintenance
Access Type: Single operation
Authorization required from
Administrator
bobl
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

Account - detailscherm

Session recording



Session recording – search/keystrokes/video



Applicatie integratie

Datasources

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

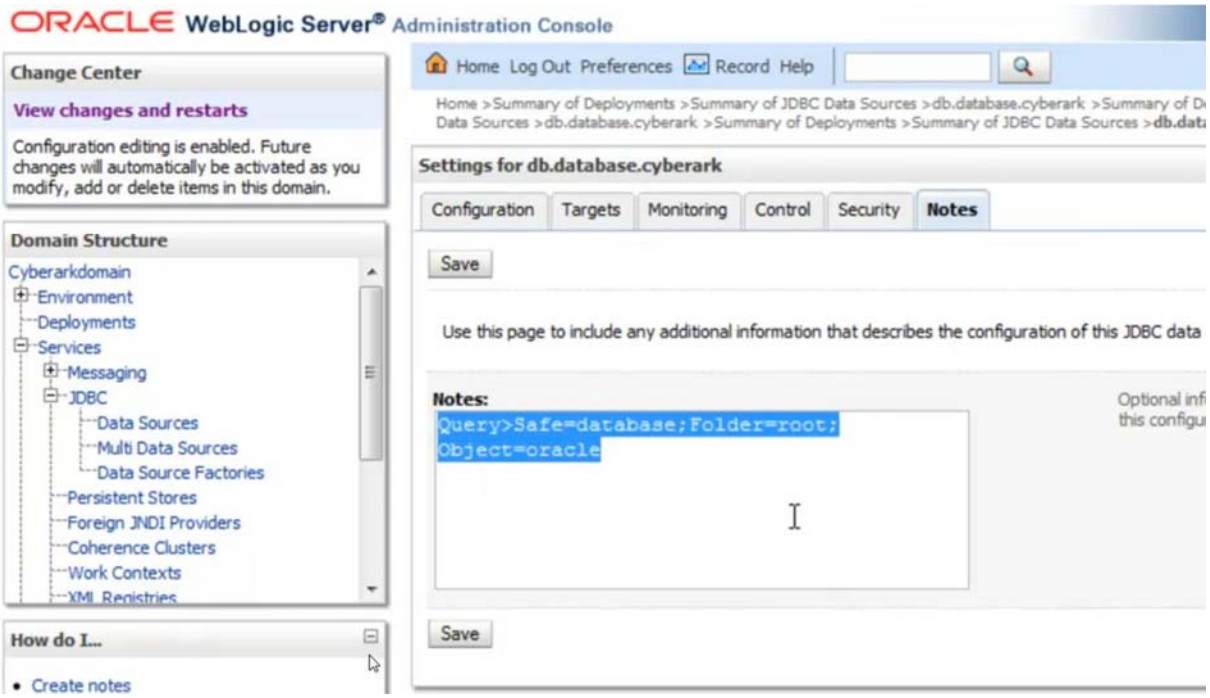
Go to Datasource application

Application - Protected keystore

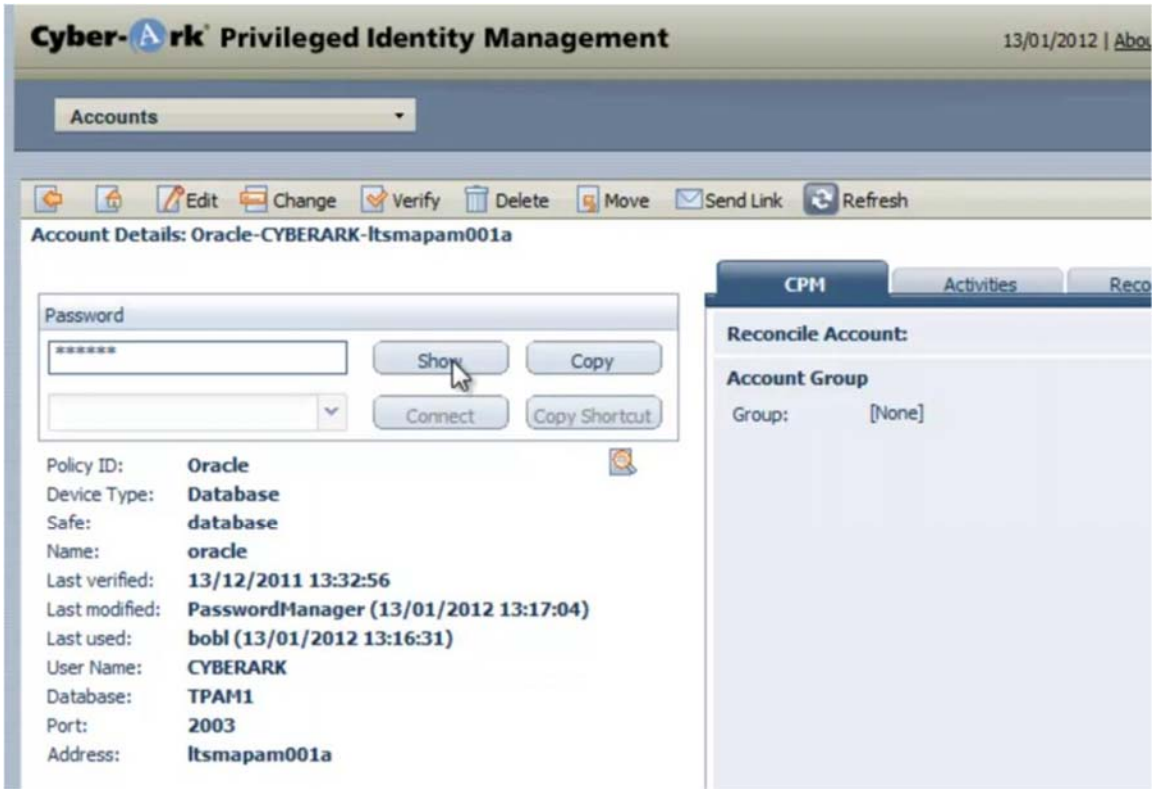
An application requests the password of a local Java keystore from the Vault in order to be able to open it.

Go to Keystore application

Applicatie integratie – weblogic datasource (1/2)



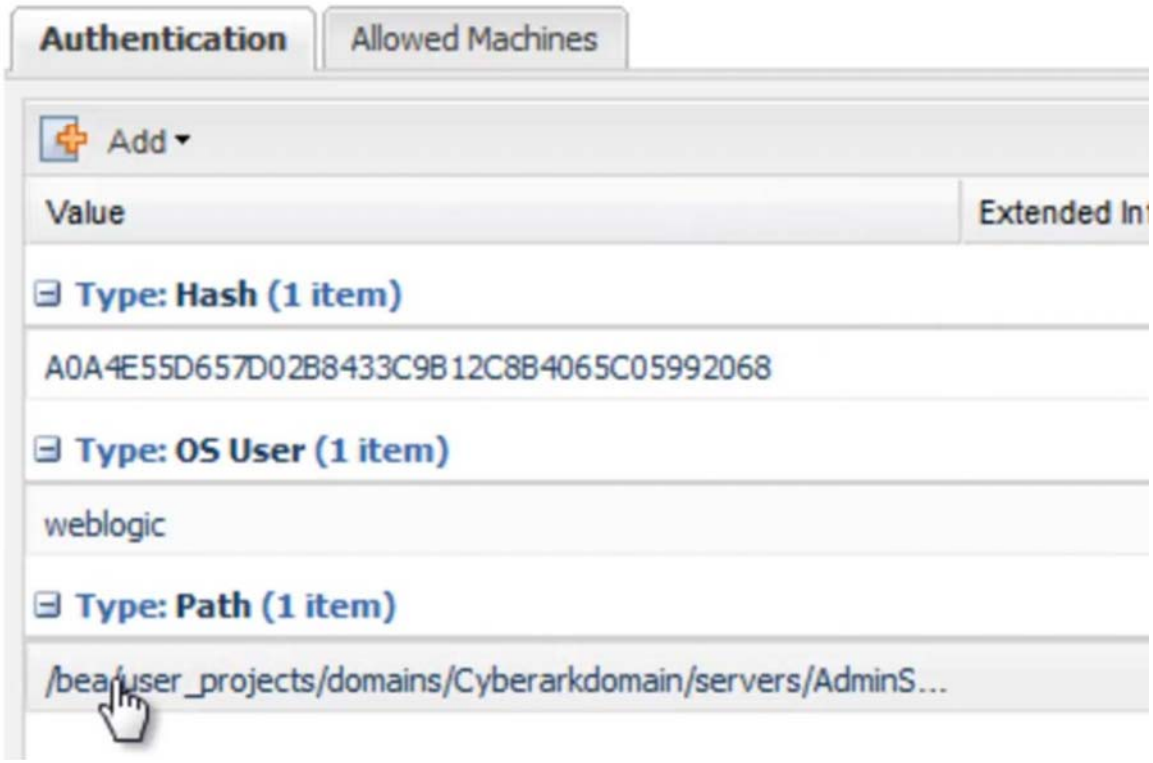
Applicatie integratie – weblogic datasource (2/2)



Applicatie integratie – Java API

```
@see javax.servlet.http.HttpServlet#doGet(javax.servlet.http.HttpServletI
*/
@Override
protected void doGet(HttpServletRequest req, HttpServletResponse resp) throw
    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 : " +                passwo
        //out.println ("The password Address is : " +                passwo
        //out.println ("The password keystore path is : " +          passwo
    }
    catch (PSDKException ex)
```

Applicatie integratie - authentication



Wachtwoordbeheer via logon-account