- Started with VMS V2 in 1981

- Technical lead for PointSecure since 2002

- Founded DECUS security SIG in mid-1980s.

Warren Kahle

CSA CSE Security+ CISSP

PointSecure

Protecting Your OpenVMS System With System Detective

Warren Kahle

CSA CSE Security+ CISSP

PointSecure

Protecting your system - agenda

- Who is PointSecure?
- System Detective overview
- System Detective primary functions
- Why use System Detective?
- System Detective configuration
- Rules and how they work
- Creating reports from the event database
- Reviewing or playing back a session
- Advising an interactive session
- Examples
- Questions

Who is PointSecure

- The leader in OpenVMS security solutions
- Established and proven products
- Fortune 500 customer base

System Detective - Overview

- Leading security product for protecting OpenVMS systems
- Versions protecting OpenVMS sites for over 15 years
- Declared “virtually unhackable” at Defcon
- Comply with security policies and government regulations
- Host based intrusion detection
- Real time observation and selective logging of user sessions
- Inactivity monitoring and protective action initiation
- Implemented as execlet code
- Rules defined using language-like block structure

System Detective primary functions

- Create security events
- Log interactive user activity
- Restrict access to sensitive files and information
- Secure or terminate idle sessions
- Monitor or take control of interactive sessions
- Create customized alerts and notifications
- Generate comprehensive reports

Why does security matter?

- What would happen if your systems are compromised?
  - Financial cost of recovery
  - Business disruption
  - Corporate embarrassment
  - Regulatory difficulties

Why use System Detective?

- OpenVMS is the most secure operating system out of the box
- Security on any system can be improved

- System Detective enhances OpenVMS security:
  - Demonstrate regulatory compliance
  - Protect the system from privileged users
  - Maintain audit trails
  - Assist users

System Detective Configuration

- Defaults for System Detective parameters
  - Optionally encrypt session logs
  - Change the session lock character
  - Optionally inhibit user's ability to lock their own sessions
  - Optionally inhibit user's ability to permit others to advise
- Locations for databases and files
  - Table of remote or local locations
  - Proxy access to remote systems
  - Suggested session log file names
- List of users who can shut down System Detective

Rules and how they work

- Rules are language-like block structures containing triggers and actions
- Select a rule for a process
- Trigger the rule by a process activity
- Qualify a rule based on its environment
- Primary actions
- Secondary actions

Rules selected for a process based on

- [No]Username
- [No]UIC group
- [No]Identifier
- [No]Captive

Rules triggered based on

- Login (process discovery)
- File access (via the XQP)
- Image activation (via the image activator)
- Image exit (via exit handler)
- Idle time (via one minute timer)
- Ignore

Rules qualified by

- [No]Priority
- [No]Privilege
- [No]Process privilege
- [No]Authorized privilege
- [No]Current privilege
- [No]Port
- [No]Terminal
- Time of day
- Weekend
- Master process or subprocess
- Mode

Rule initiated primary actions

- Idle rules checking on or off
- Delete process
- Force image exit
- Force security event
- Log session temporarily or permanently
- Log session input only
- Stop temporary session logging
- Lock user's keyboard (user unlock)
- Manager lock keyboard
- Exclude rules until end of block
- Ignore this process

Rule initiated secondary actions

- Send a message to operator(s)
- Notify (send a message to) the user
- Execute a DCL command in a batch job

Reporting on security events

Command: sysdetect report

/before	/since	/epid
/user	/action_type	/event_type
/port	/name	/node
/username	/terminal	/exclude
/output	/full	/message_file
/database	/help	

Session log review or playback

- Command: sysdetect review or sysdetect playback
- Use whichever utility works best for your system
- Move around in the session log file
- Playback speed is adjustable
- Translated events are displayed during review

Advising an interactive process

- Interact with a hacker's process
- Help desk tool
- Controlled by identifiers
- Input allowed or view only modes
- User authorized advising
- Optional notification

How it works

- Triggers from callouts from XQP, image activator, exit handler, etc.
- Kernel and executive mode threads in process context for efficiency and account billing
- Implemented as execlets
- Logging from class/port driver interface
- Only required data stored in system space
- Process related data is pageable
- Install or upgrade without reboot
- SDA extension for examining data structures
- Debug mode for debugging rules

Examples of uses

- The privileged executive who logs in on weekends.
- Payroll clerk who leaves terminal unattended.
- Formatting a session log
- Advising an interactive process
- Forced encryption

Executive login on weekend example

- A highly privileged executive is not expected to log in on weekends and he is not good at hiding his password.

- The site security manager would like for operations to be alerted and the session activity logged if his account is ever active on weekends

Executive login on weekend rule

```
[Selector] Username george
        [Trigger] Login          ! Anytime he logs in
        [Time] weekend           ! on a weekend
        [Action] Temp_Log        ! log him and tell operator.
        [Action] opcom=(central) George logged in.
```

Executive login event

TIME : 27-FEB-2013 10:00:15.87
NODE : I64
EPID : 210614D0
USERNAME : GEORGE
LNAME : GEORGE
TERMINAL : _TNA48:
PORT : Host: 172.17.3.1 Port: 1372
EVENT_TYPE : LOGIN
ACTION_TYPE : LOG_TEMP
OPENV$SD_M_LOG_TEMP_DISCOVERY Logged temporarily from discovery

Payroll idle rule example

The payroll account is only used by the payroll clerk in the accounting department.

Only the payroll clerk account can modify the payroll database.

Sometimes the payroll clerk takes a break without logging out.

Payroll idle rule set

- [selector] username payroll
- [trigger] idle 30
- [action] notify = Idle for 30 minutes - another 15 to lock.

- [selector] username payroll
- [trigger] idle 45
- [action] notify = Idle for 45 minutes - another 15 to delete.
- [action] lock_keyboard

- [selector] username payroll
- [trigger] idle 60
- [action] notify = Idle too long - deleting process.
- [action] delete

Formatting a session log for printing example

The legal department wants a printed copy of the session log of the account of George to show that he did not corrupt the customer's database resulting in a law suit.

The printout must be the whole record of the session so that a business records affidavit may attest to its correctness.

Formatting a session log for printing example

The corporate security officer issues the command:

$ sysdetect format –
GEORGE _2013-02-20-103648_00009557.SESSIONLOG_WK –
/output=sys$login:george_log.txt

The security officer then prints sys$login:george_log.txt, executes the business records affidavit, and delivers both to the legal department.

Advising an interactive process example

The hospital help desk is called from a nursing station where the nurse is trying to enter the proper diagnosis code in a patient record.

The nurse has the doctor's notes but does not know the proper diagnosis code to enter into the patient's record.

Advising an interactive process

The help desk user has been granted the identifier OPENVSSDIS_I_NURSE and the nurse has been granted the identifier NURSE so the help desk operator may advise and enter input into the interactive session of the nurse.

The help desk operator asks the nurse for the terminal name she is using and enters the command:

$ sysd advise/notify="I'm here, Maggie" FTA24

The nurse displays the doctor's notes and the helpdesk operator enters the proper diagnosis code.

Forced encryption example

At this site there are a group of users who edit sensitive information from remote sites where unencrypted traffic might be observed.

It was decided that these users would only be allowed to connect to the OpenVMS system using encrypted protocols so they would not be allowed to use telnet or ftp.

Forced encryption example

The following two rules were added to the configuration file to delete the processes of the target group if they were telnet or ftp.

```
[Selector] uic 700
        [Trigger] login
        [Qualifier] terminal = *TNA* ! Telnet login
        [Action] delete
[Selector] uic 700
        [Trigger] image *TCPIP$FTP_CHILD.EXE ! FTP
        [Action] delete
```

Suggestions are appreciated!

Warren Kahle, CSA, CSE, Security+, CISSP

PointSecure Technologies Inc

802 Lovett Blvd

Houston, TX 77006-3906

Warren.Kahle@PointSecure.com

Cell: 713-906-5600

Office: 713-868-1222 ext 2

Auditing Your OpenVMS System With PointAudit

Warren Kahle

CSA CSE Security+ CISSP

PointSecure

Auditing your system - agenda

- Who is PointSecure?
- PointAudit overview
- PointAudit primary functions
- Why use PointAudit?
- PointAudit planning
- PointAudit configuration
- PointAudit scanning
- PointAudit reports
- Screen shots
- Questions

Who is PointSecure

- The leader in OpenVMS security solutions
- Established and proven products
- Fortune 500 customer base

PointAudit - Overview

- Leading auditing product for securing OpenVMS systems
- Auditing OpenVMS sites for over 15 years
- Comply with security policies and government regulations
- Audit disabling of accounts of users no longer authorized
- Report on unused accounts or infrequently used accounts
- Report on privileged accounts
- Audit system patches
- Audit system generation parameters
- Audit system licenses
- Audit the system audit server
- 96 provided reports and custom reports easily generated

PointAudit primary functions

- Create security related audit reports
- Assist the system manager
- Provide separation of audit data from systems
- Separation of audit and system management duties

Why does security matter?

- What would happen if your systems are compromised?
  - Financial cost of recovery
  - Business disruption
  - Corporate embarrassment
  - Regulatory difficulties

Why use PointAudit?

- OpenVMS is the most secure operating system
- Security on any system can be improved
- Many system managers are overworked and under educated
- PointAudit enhances and simplifies OpenVMS security reporting and auditing

PointAudit Planning

- Where to locate the PointAudit system
  - In the audit office with physical security
  - Outside the access area of operational personnel
  - At the disaster recovery site
- Communications protocol to use
  - SSH is recommended
  - TELNET is available if needed
- Create PointAudit accounts on all the systems to be audited
  - Grant privileges: NETMBX, SECURITY, SYSLCK, SYSPRV, TMPMBX
  - Use a complex password – nobody has to remember it
  - The username and password may be different on each audited system
  - Setup the accounts to not use any menus or ask questions during login
  - There is no agent to install on the audited system

PointAudit Configuration

- Use the Add Server Wizard to create the server entries
  - Connection settings – server name, host IP, license key
  - Server properties – Company, manager, location, department
- Use the New Scan Wizard to create scans
  - Select the servers to run the scan
  - Name the scan and select the connection protocol and port
  - Optionally enter a description
  - Optionally enter email addresses to be notified when the scan completes
  - Enter the username, password, and test the connection
  - Select the data to be gathered
  - Optionally enable scan to run at a specified interval

PointAudit Scanning

- Scan on demand
- Scan unattended on a schedule
- Scan data is stored in a database

Predesigned Reports

- 96 modifiable reports predesigned
- Accounts with specific privileges
- Accounts in privilege groups
- Accounts used/unused for a period of time
- Accounts never used
- Passwords not changed for a period of time
- Accounts with flags set

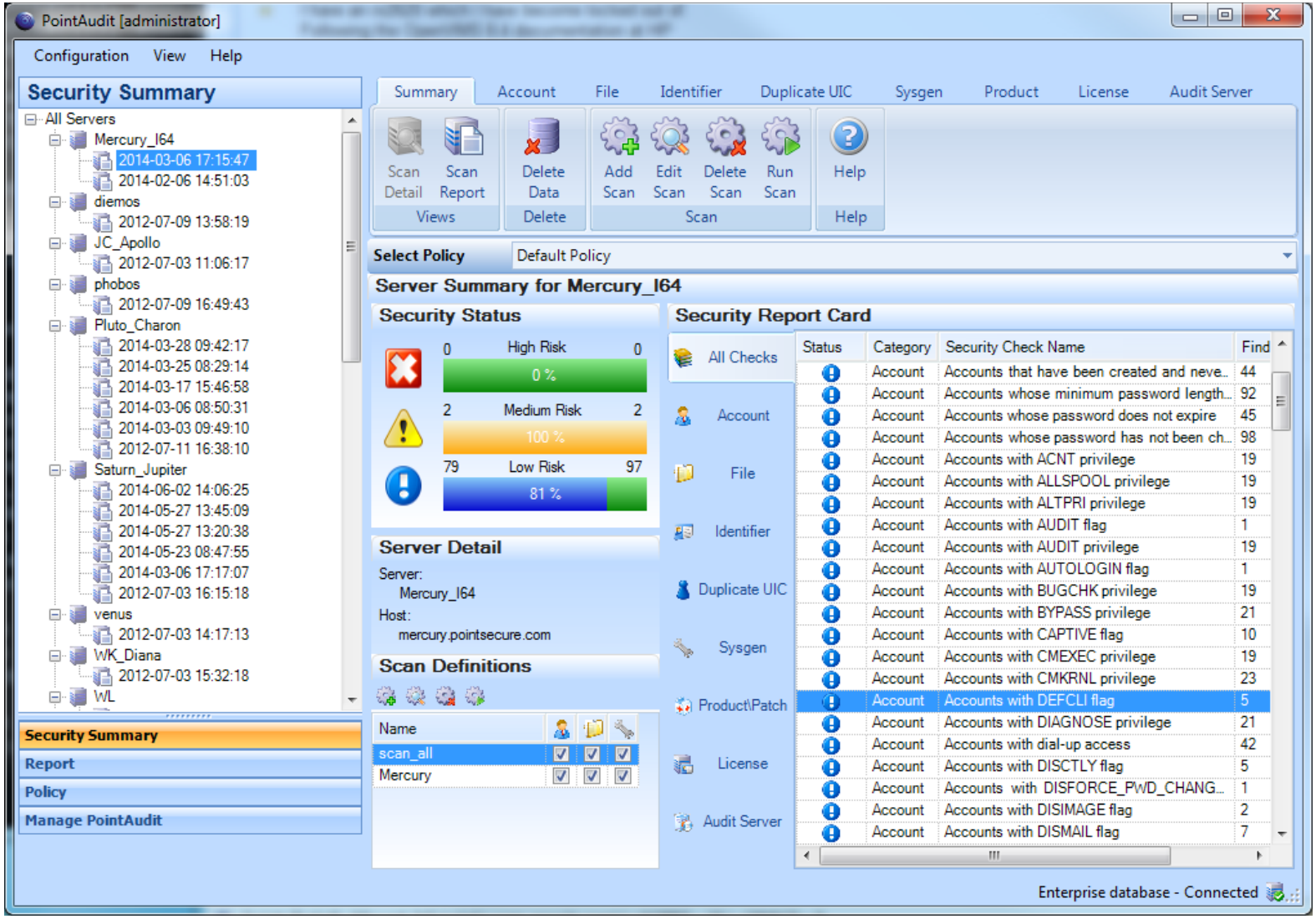
Predesigned Reports - continued

- Identifiers
- Audit server settings
- Patches applied/needed
- System generation parameters
- License inventory
- Compare differences between scans or servers

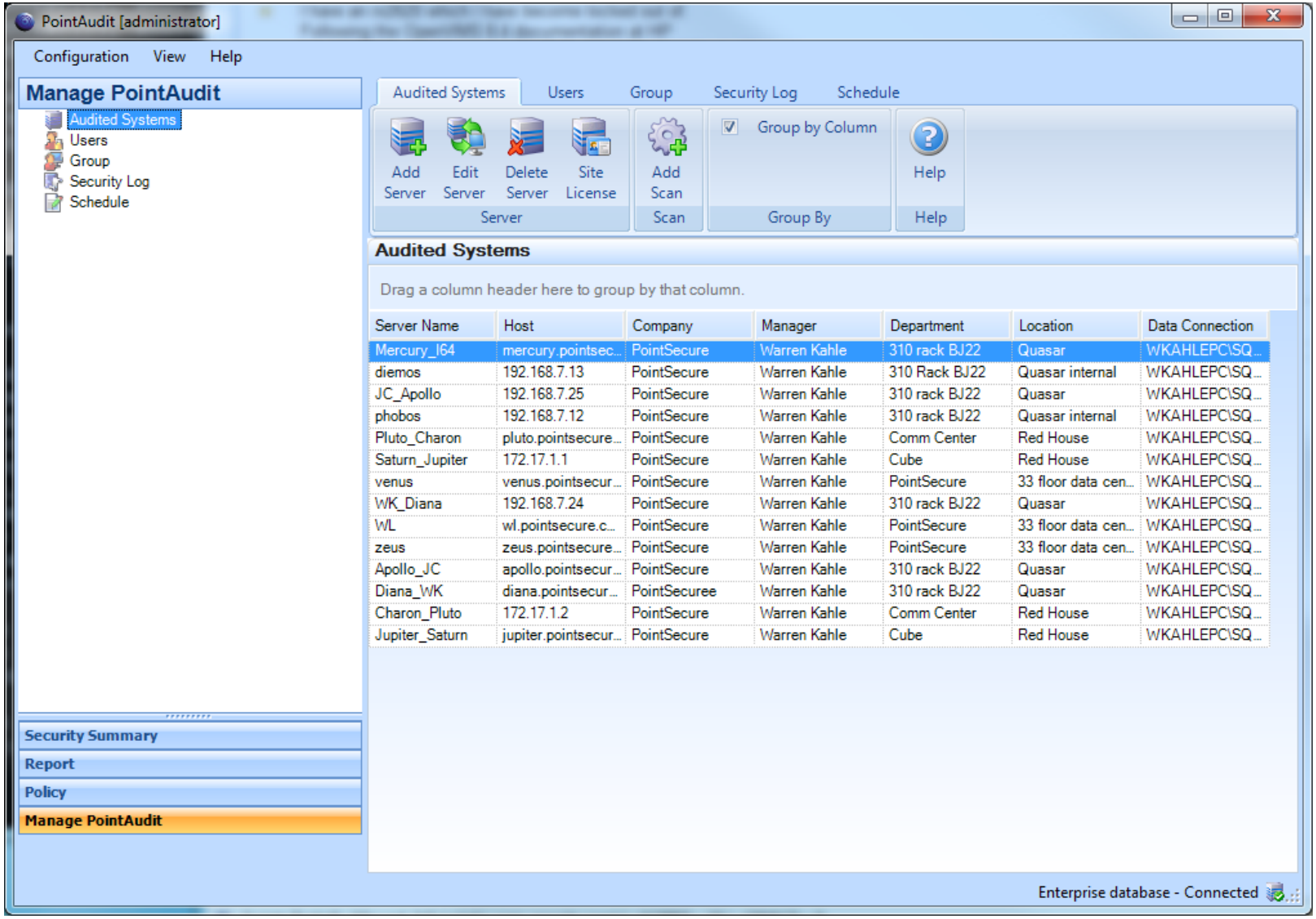
Custom Reports

- Modified standard reports
- New reports using any gathered data
- Create them any time
- Use them on any scanned data in database
- Match your site specific policies

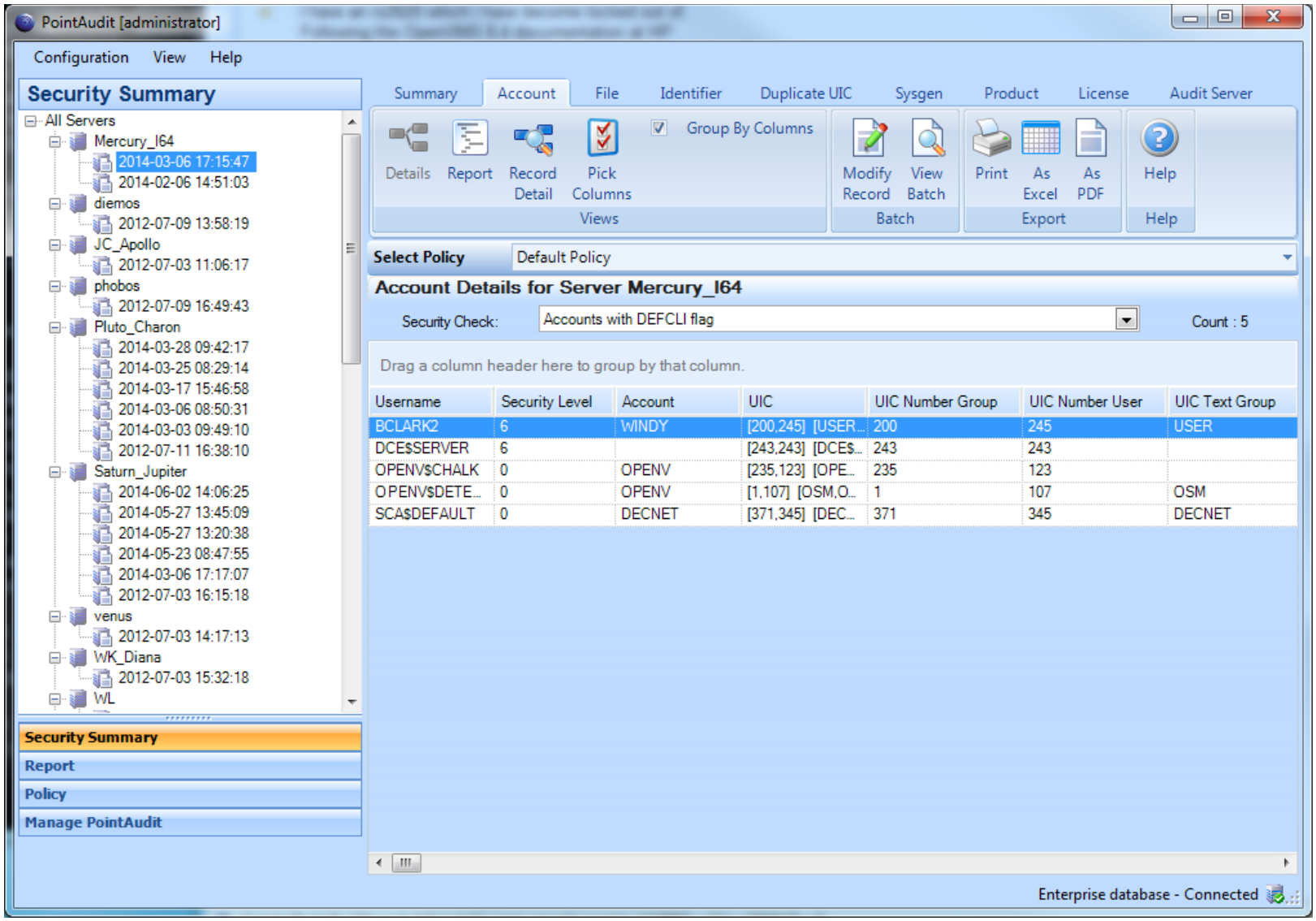
Summary Screen



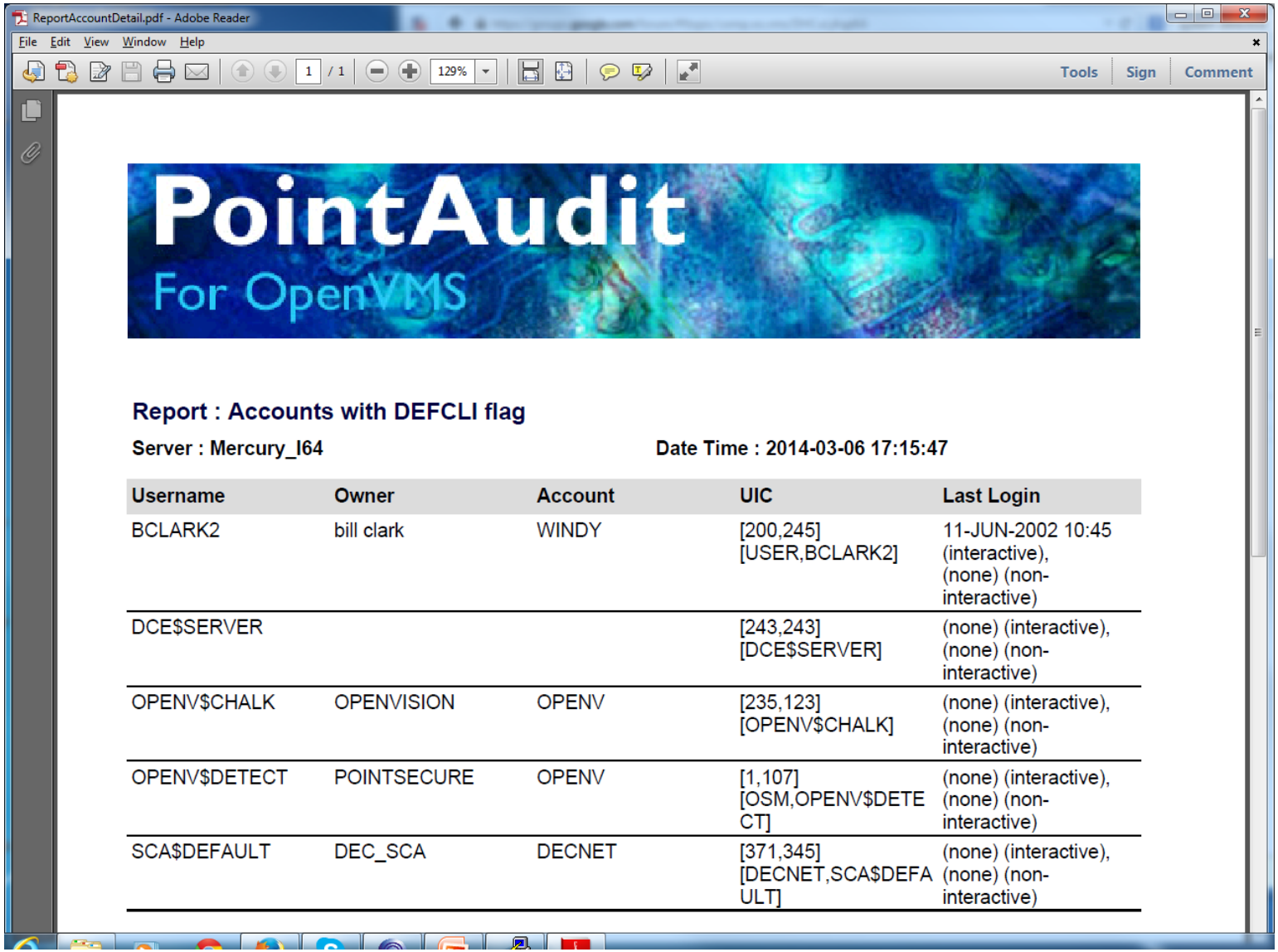
Management Screen



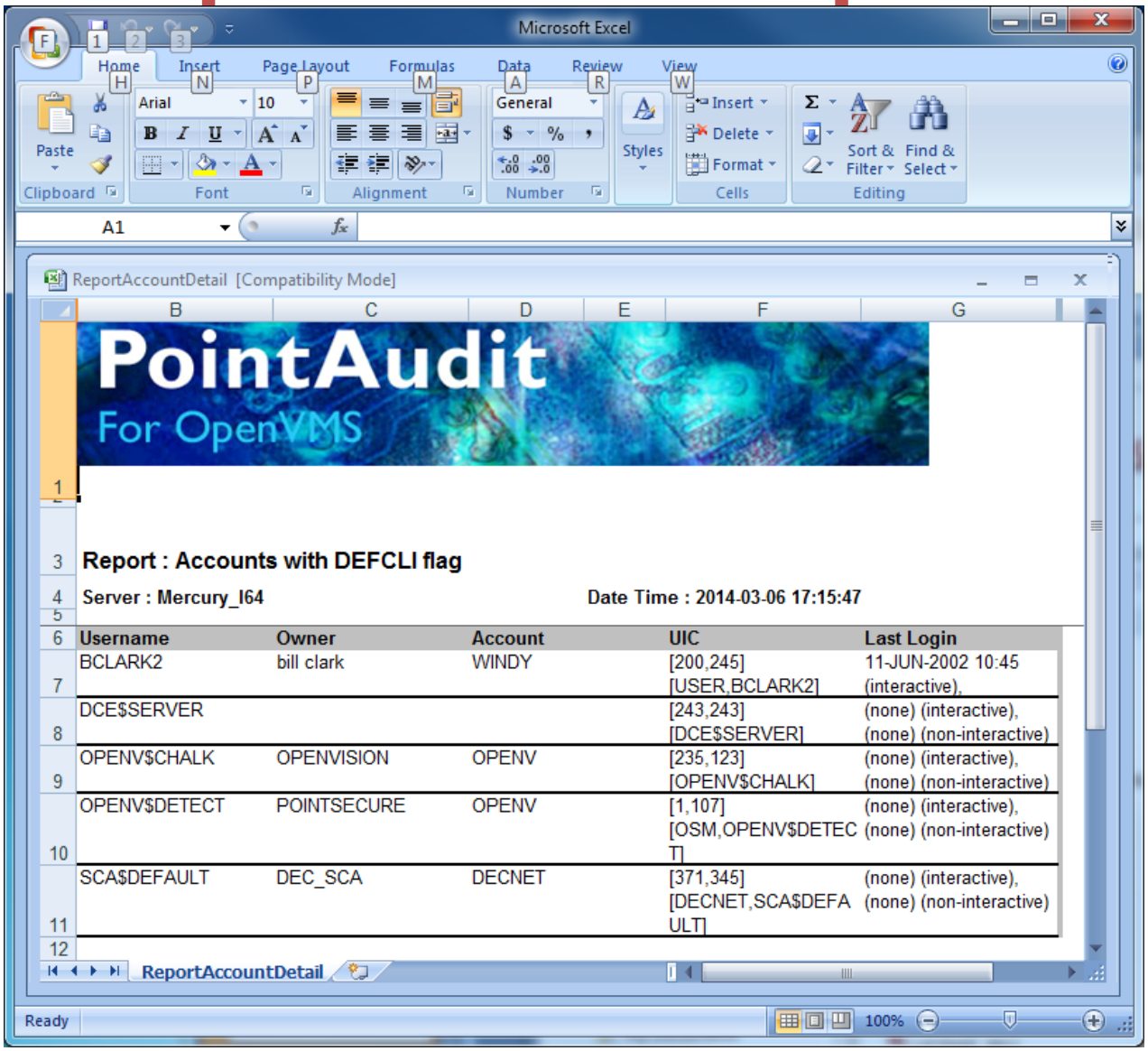
Online Report



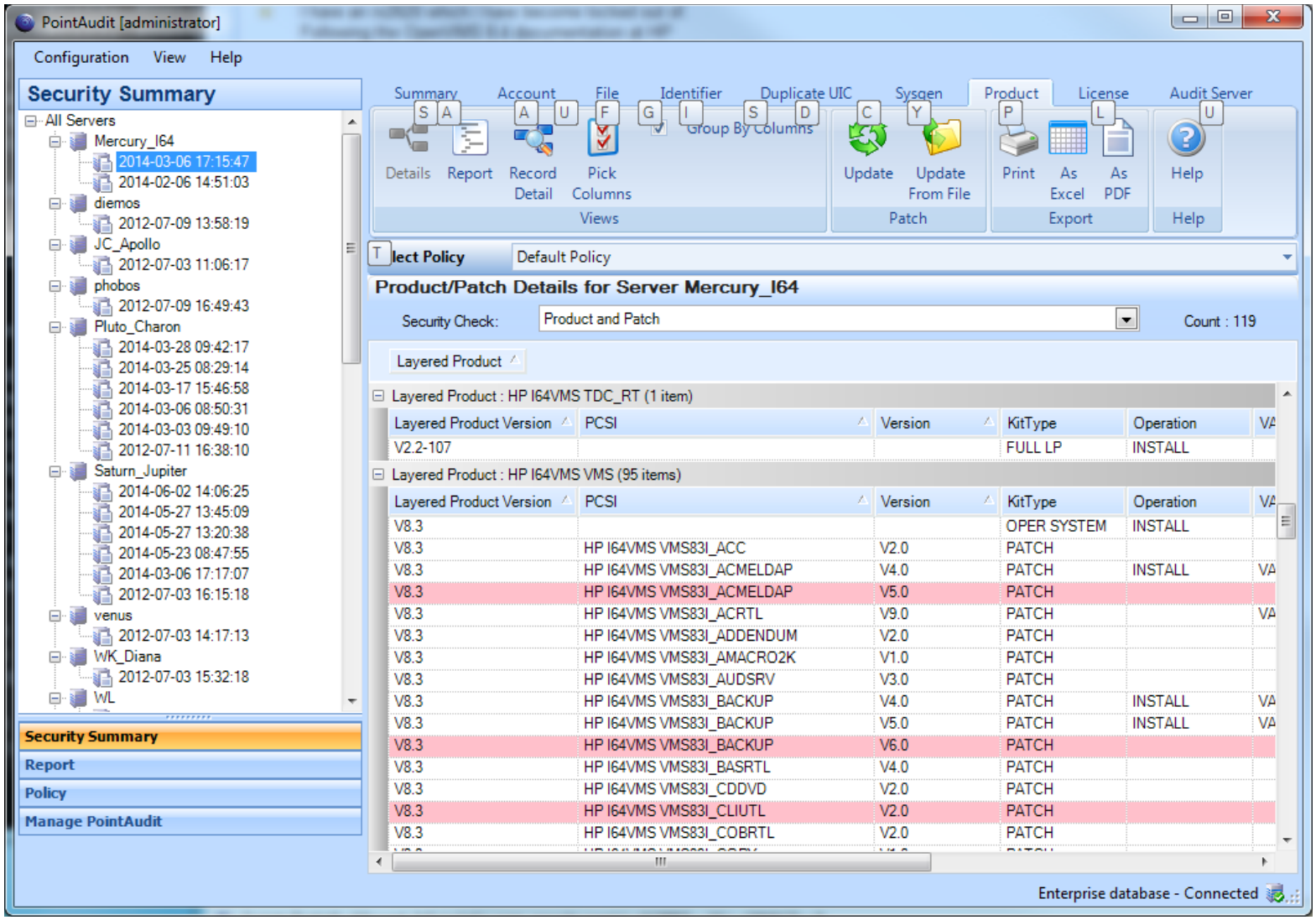
PDF Report


ReportAccountDetail.pdf - Adobe Reader
File Edit View Window Help
1 / 1
129%
Tools Sign Comment
PointAudit
For OpenVMS
Report : Accounts with DEFCLI flag
Server : Mercury_I64
Date Time : 2014-03-06 17:15:47
Username Owner Account UIC Last Login
BCLARK2 bill clark WINDY [200,245] [USER,BCLARK2] 11-JUN-2002 10:45 (interactive), (none) (non-interactive)
DCE$SERVER [243,243] [DCE$SERVER] (none) (interactive), (none) (non-interactive)
OPENV$CHALK OPENVISION OPENV [235,123] [OPENV$CHALK] (none) (interactive), (none) (non-interactive)
OPENV$DETECT POINTSECURE OPENV [1,107] [OSM,OPENV$DETECT] (none) (interactive), (none) (non-interactive)
SCA$DEFAULT DEC_SCA DECNET [371,345] [DECNET,SCA$DEFAULT] (none) (interactive), (none) (non-interactive)

Spreadsheet Report



Patch Installed/Available Report



Suggestions are appreciated!

Warren Kahle, CSA, CSE, Security+, CISSP

PointSecure Technologies Inc

802 Lovett Blvd

Houston, TX 77006-3906

Warren.Kahle@PointSecure.com

Cell: 713-906-5600

Office: 713-868-1222 ext 2