pointsecure
Security and Auditing for OpenVMS

system detective

Host Based Intrusion Detection and Monitoring Application for OpenVMS Systems

```
[Selector] Username Testpriv
    [Trigger] Image *sysexe]sysgen.exe
    [Action] Forcex
    [Action] Notify = You are not authorized to run sysgen.
```

Configure rules to meet security requirements.

```
$ sysdet advise 233

Entering advisory mode. Keyboard input enabled. Type CTRL-B to exit.

sho proc

 4-JAN-2006 10:11:27.99     User: TESTPRIV     Process ID:  00000233
                            Node: VENUS     Process name: "TESTPRIV"

Terminal: TNA10: (Host: 172.17.1.52 Port: 1520)
User Identifier: [TESTPRIV]
Base priority: 4
Default file spec: SYS$SYSROOT:[SYSEXE]
Number of Kthreads: 1

Devices allocated: VENUS$TNA10:

Soft CPU Affinity: off
$
```

Advise interactive users on the system.

```
System Detective message on node VENUS     14-DEC-2005 09:56:56
You are not authorized to run sysgen.
```

Restrict access to sensitive areas and notify users.

```
%%%%%%%%%%% OPCOM 14-DEC-2005 09:56:56.09 %%%%%%%%%%%
Message from user TESTPRIV on VENUS
System Detective Event - This user is trying to run sysgen.
```

Receive real-time alert messages.

overview

PointSecure's System Detective is a powerful, host-based intrusion detection, real-time security monitoring and access control application. System Detective's features provide a comprehensive defense mechanism against internal and external security threats. System Detective allows organizations to customize security settings in ways that reinforce corporate policies. It also provides rich functionality for tracking session data required by several regulatory bodies as well as providing a more secure environment.

why system detective?

This security and compliance application can enforce user accountability by recording terminal activity as well as enhancing the OpenVMS access control capabilities by taking away privileges or restricting access to images/files. System Detective also enables System Administrators to log user sessions down to the keystroke level as well as monitor user sessions in real-time.

key benefits

- Control access to files or images
- Hold users accountable for their actions on the system
- Be alerted in real-time when a security breach or policy violation occurs
- Automated response to predefined security events
- Protects against downtime and loss of confidential data
- Extensive and customizable alert notification capabilities
- Delivers trusted log collection to a central repository for storage and analysis
- Removes painstaking work of combing for specific events within log files
- Inactive session monitor helps prevent unauthorized access to unattended systems
- Promotes regulatory compliance for security mandates such as HIPAA and GLBA

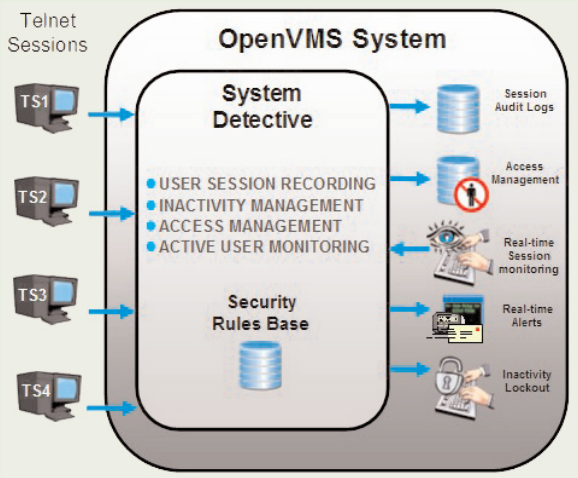
business partner

hp invent

pointsecure
Security and Auditing for OpenVMS

system detective

Host Based Intrusion Detection and Monitoring Application for OpenVMS Systems



System Detective Architecture

technical features

- Monitor and log terminal sessions down to the keystroke level to record all users accessing the system and recording their actions within the system
- Restrict access to files and images using an automated rules-based engine
- Manage unattended or inactive terminal sessions by locking the keyboard and/or terminating processes
- Search and playback recorded user sessions down to the keystroke level
- Generate reports on security events or policy violations that have occurred in the OpenVMS system
- Search log files for unique events or ids (character string)
- Receive an alert message in the form of an e-mail or page if a security rule is triggered
- Attach a command procedure to a security rule and send alert notification with the event record
- Selectively monitor and log the terminal sessions for one or more users with or without their knowledge
- Real-time terminal session component to actively monitor users by pulling up the session of a specific user and seeing each keystroke
- Send messages to users in real-time

system requirements

- The system account or a system privileged account with at least SYSPRV, SYSNAM, WORLD, TMPMBX, CMKRNL, SYSGBL, and PRMGBL privileges
- 5,000 blocks of available space
- Alpha OpenVMS version 7.3-2

contacts

PointSecure Corporate Headquarters
802 Lovett Boulevard
Houston, TX USA 77006
Phone: 713-868-1222
Fax: 713-862-5210
www.pointsecure.com
Sales Information: sales@pointsecure.com
General Information: info@pointsecure.com