



NStreamAware: Real-Time Visual Analytics for Data Streams to Enhance Situational Awareness

Fabian Fischer and Daniel A. Keim

Fabian Fischer | Data Analysis and Visualization Group | University of Konstanz

Motivation: Heterogeneous Data Streams

- Network Alerts (e.g., OSSEC)
- Syslog Messages
- NetFlow Data

Analyzing Data Streams = Crucial for security in your network!





DATA CHALLENGE How to make stream analysis <u>scalable</u>?

NStreamAware: Scalable Infrastructure



Apache Spark[™] is a fast and general engine for large-scale data processing which can run on a distributed computer cluster.

Integrated Perspec

- Real-Time Data Stream Mo ٠
- Real-Time Sliding Slices (N ٠
- **Visual Feature Selection** •
- Summarized Sliding Slices ٠
- Event Timeline & Insights ٠
- Search & Exploration ٠

File Tools View Help

Real-Time Data Stream

Perspectives	Ever See See See See See See See See See S		Markan Markan<
ta Stream Monitoring ding Slices (NVisAware) e Selection Sliding Slices e & Insights oration	Image: second		
S or Cyber Security Real-Time Sliding Slices Visual Feature Se	election Summarized Sliding S	Slices Event Timeline & Insigh	ts Search & Exploration

Real-Time Data Stream Monitoring



Demo



File Tools View Help

Real-Time Data Stream Real-Time Sliding Slices Visual Feature Selection Summarized Sliding Slices Event Timeline & Insights Search & Exploration

Data Streams	Data Stream
Real-Time Overview	🗰 2014-08-04T21:S1:24.000 - bali - pam_umix(cron:session): session closed for user XXXX
▼ System Status	★ 2014-08-04T21:46:01.000 - dbvis - pam_unix(cron:session): session opened for user XXXX by (uid=0)
	★ 2014-08-04721:46:01.000 - dbvis - (root) CMD (/root/scripts/check-dovecot.sh 2>61 > /dev/null)
VACS-REST: 1.0.0 VACS-Spark: 1.0.0	★ 2014-08-04721:46:01.000 - dbvis - pam_unix(cron:session): session closed for user XXXX
	★ 2014-08-04T21:46:22.000 - dbvis - TMAP(XXXXX): Disconnected for inactivity bytes=42/2782
 RabbitMQ: 3.2.1 MonooDB: 2.4.10 	★ 2014-08-04T21:46:22.000 - dbvis - TMAP(XXXXX): Disconnected for inactivity bytes=127/1253
Spark Streaming: 1.0.0	* 2014-08-04T21:46:27.000 - dbvis - imap-login: Login: Log
ElasticSearch: 1.1.0	* 2014-08-04T21:46:28.000 - dbvis - imap-login: Login: Log
	★ 2014-08-04T21:51:58.000 - bali - Alert Level: 3; Rule:XX:XX:XX:XX user: jacekle: Aug 4 21:46:XX:XX:XX method=FLAIN, rip=95.XXX.XXX.XXX, lip=134.XXX.XXX.XXX, lip=134.XXXX.XXX.XXX, lip=134.XXX.XXX.XXX, lip=134.XXX.XXX.XXX, lip=134.XXX.XXX.XXX, lip=134.XXX.XXX.XXX, lip=134.XXXX.XXX.XXX, lip=134.XXX.XXX.XXX, lip=134.XXXXXXXXXXX, lip=134.XXXXXXXXXXXXXXX, lip=134.XXXXXXXXXXXXXXX, lip=134.XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Real-Time Filter	★ 2014-08-04T21:51:58.000 - bali - Alert Level: 3; Rule:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX
gateway (7)	* 2014-08-04T21:46:41.000 - optiplex.dbvis - stack : TTY=pts/33 ; FND=/opt/stack/cinder : USER=root ; COMMOND=/usr/local/bin/cinder-rootwrap /etc/cinder/rootwrap.conf env LC_ALL=C vgsnoheadingsunit=g -0 name, size, free, lv_count, uuidseparator :nosuffix stack-volumes-lumdriver-1
dbvis (70) 🗸	* 2014-08-04T21:46:41.000 - optiplex.dbvis - pam_unix(sudo:session): session opened for user XXXX by (uid=0)
bali (52)	★ 2014-08-04T21:46:42.000 - optiplex.dbvis - pam_unix(sudo:session): session closed for user XXXX
www.group (3)	* 2014-08-04T21:52:20.000 - bali - Alert Level: 3; Rule:XX:XX:XX optiplex.dbvis sudo: stack : TTY=pts/33 ; FMD=/opt/stack/cinder ; USER=root ; COMMAD=/usr/local/bin/cinder.rootwrap /etc/cinder/xootwrap.comf env IC_ALL=C vgsnoheadingsunit=g - o name, size, free, lv_count, uuidseparator :nosuffix stack-volumes-
wwwpub (3)	lvadriver-1
storage.dbvis.de (16)	
compute (6)	Geographic Locations
proxy (16)	



🖈 2014-07-30Tl6:20:01.000 - atlantis - pam_unix(cron:session): session opened for user root by (uid=0)	🖈 2014-07-30T16:20:01.000 - atlantis - pam_unix(cron:session): session opened for user root by (uid=0)
★ 2014-07-30T16:20:01.000 - atlantis - (root) CMD (if [-x /etc/munin/plugins/apt_all]; then /etc/munin/plugins/apt_all update 7200 12 >/dev/null; elif [-x /etc/munin/plugins/apt]; then /etc/munin/plugins/apt update 7200 12 >/dev/null; fi)	★ 2014-07-30T16:20:01.000 - atlantis - (root) CMD (if [-x /etc/munin/plugins/apt_all]; then /etc/munin/plug: update 7200 12 >/dev/null; fi)
🖈 2014-07-30T16:20:01.000 - atlantis - pam_unix(cron:session): session closed for user root	🖈 2014-07-30T16:20:01.000 - atlantis - pam_unix(cron:session): session closed for user root
* 2014-07-30T16:20:07.000 - optiplex.dbvis - stack : TTY=pts/33 ; FWD=/opt/stack/cinder ; USER=root ; COMMAND=/usr/local/bin/cinder-rootwrap /etc/cinder/rootwrap.conf env LC_ALL=C vgsnoheadingsunit=g -o name, size, free, lv_count, uuidseparator :nosuffix stack-volumes-lvmdriver-1	★ 2014-07-30T16:20:07.000 - optiplex.dbvis - stack : TTY=pts/33 ; PWD=/opt/stack/cinder ; USER=root ; COMMAND= name,size,free,lv_count,uuidseparator :nosuffix stack-volumes-lvmdriver-1
🖈 2014-07-30T16:20:07.000 - optiplex.dbvis - pam_unix(sudo:session): session opened for user root by (uid=0)	🖈 2014-07-30T16:20:07.000 - optiplex.dbvis - pam_unix(sudo:session): session opened for user root by (uid=0)
🖈 2014-07-30T16:20:07.000 - optiplex.dbvis - pam_unix(sudo:session): session closed for user root	🖈 2014-07-30T16:20:07.000 - optiplex.dbvis - pam_unix(sudo:session): session closed for user root
★ 2014-07-30T16:20:11.000 - proxy - (CRON) error (grandchild #27732 failed with exit status 1)	★ 2014-07-30T16:20:11.000 - proxy - (CRON) error (grandchild #27732 failed with exit status 1)
🖈 2014-07-30T16:20:11.000 - proxy - (CRON) info (No MTA installed, discarding output)	🖈 2014-07-30T16:20:11.000 - proxy - (CRON) info (No MTA installed, discarding output)
🖈 2014-07-30T16:20:11.000 - proxy - pam_unix(cron:session): session closed for user munin	🖈 2014-07-30T16:20:11.000 - proxy - pam_unix(cron:session): session closed for user munin
* 2014-07-30T16:21:07.000 - optiplex.dbvis - stack : TTY=pts/33 ; PWD=/opt/stack/cinder ; USER=root ; COMMAND=/usr/local/bin/cinder-rootwrap /etc/cinder/rootwrap.conf env LC_ALL=C vgsnoheadingsunit=g -o name, size, free, lv_count, uuidseparator :nosuffix stack-volumes-lvmdriver-1	★ 2014-07-30T16:21:07.000 - optiplex.dbvis - stack : TTY=pts/33 ; FWD=/opt/stack/cinder ; USER=root ; COMMAND= name,size,free,lv_count,uuidseparator :nosuffix stack-volumes-lvmdriver-1
🖈 2014-07-30T16:20:01.000 - atlantis - pam_unix(cron:session): session opened for user root by (uid=0)	🖈 2014-07-30T16:20:01.000 - atlantis - pam_unix(cron:session): session opened for user root by (uid=0)
2014-07-30T16:20:01.000 - atlantis - (root) CMD (if [-x /etc/munin/plugins/apt_all]; then /etc/munin/plugins/apt_all update 7200 12 >/dev/null; elif [-x /etc/munin/plugins/apt]; then /etc/munin/plugins/apt update 7200 12 >/dev/null; fi)	★ 2014-07-30T16:20:01.000 - atlantis - (root) CMD (if [-x /etc/munin/plugins/apt_all]; then /etc/munin/plugi update 7200 12 >/dev/null; fi)
🖈 2014-07-30T16:20:01.000 - atlantis - pam_unix(cron:session): session closed for user root	🖈 2014-07-30T16:20:01.000 - atlantis - pam_unix(cron:session): session closed for user root
* 2014-07-30T16:20:07.000 - optiplex.dbvis - stack : TTY=pts/33 ; PWD=/opt/stack/cinder ; USER=root ; COMMAND=/usr/local/bin/cinder-rootwrap /etc/cinder/rootwrap.conf env LC_ALL=C vgsnoheadingsunit=g -o name, size, free, lv_count, uuidseparator :nosuffix stack-volumes-lvmdriver-1	★ 2014-07-30T16:20:07.000 - optiplex.dbvis - stack : TTY=pts/33 ; FWD=/opt/stack/cinder ; USER=root ; COMMAND= name,size,free,lv_count,uuidseparator :nosuffix stack-volumes-lvmdriver-1
🖈 2014-07-30T16:20:07.000 - optiplex.dbvig - new wniv(sudorsession), session opened for user root bu (uid-0)	★ 2014-07-30T16:20:07.000 - optiplex.dbvis - pam_unix(sudo:session): session opened for user root by (uid=0)
🖈 2014-07-30T16:20:07.000 - optiplex.dbvis	🖈 2014-07-30T16:20:07.000 - optiplex.dbvis - pam_unix(sudo:session): session closed for user root
	★ 2014-07-30T16:20:11.000 - proxy - (CRON) error (grandchild #27732 failed with exit status 1)
	2014-07-30T16:20:11.000 - proxy - (CRON) info (No MTA installed, discarding output)
🖈 2014-07-30T16:20:11.000 - proxy - pam_ur	🖈 2014-07-30T16:20:11.000 - proxy - pam_unix(cron:session): session closed for user munin
★ 2014-07-30T16:21:07.000 - optiplex.dbvis name, size, free, lv_count, uuidseparator :	★ 2014-07-30T16:21:07.000 - optiplex.dbvis - stack : TTY=pts/33 ; PMD=/opt/stack/cinder ; USER=root ; COMMAND= name,size,free,lv_count,uuidseparator :nosuffix stack-volumes-lvmdriver-1
	🖈 2014-07-30T16:20:01.000 - atlantis - pam_unix(cron:session): session opened for user root by (uid=0)
* 2014-07-30T16:20:01.000 - atlantis - (rc update 7200 12 >/dev/null; fi)	<pre></pre>
🖈 2014-07-30T16:20:01.000 - atlantis - pam	🖈 2014-07-30T16:20:01.000 - atlantis - pam_unix(cron:session): session closed for user root
★ 2014-07-30T16:20:07.000 - optiplex.dbvis name,size,free,lv_count,uuidseparator :	★ 2014-07-30T16:20:07.000 - optiplex.dbvis - stack : TTY=pts/33 ; FWD=/opt/stack/cinder ; USER=root ; COMMAND= name,size,free,lv_count,uuidseparator :nosuffix stack-volumes-lvmdriver-1
★ 2014-07-30T16:20:07.000 - optiplex.dbvis	★ 2014-07-30T16:20:07.000 - optiplex.dbvis - pam_unix(sudo:session): session opened for user root by (uid=0)
★ 2014-07-30T16:20:07.000 - optiplex.dbvis	🖈 2014-07-30T16:20:07.000 - optiplex.dbvis - pam_unix(sudo:session): session closed for user root
* 2014-07-30T16:20:11.000 - proxy - (CRON)	★ 2014-07-30T16:20:11.000 - proxy - (CRON) error (grandchild #27732 failed with exit status 1)
★ 2014-07-30T16:20:11.000 - proxy - (CRON)	★ 2014-07-30T16:20:11.000 - proxy - (CRON) info (No MTA installed, discarding output)
★ 2014-07-30T16:20:11.000 - proxy - pam_ur	🖈 2014-07-30T16:20:11.000 - proxy - pam_unix(cron:session): session closed for user munin
* 2014-07-30T16:21:07.000 - optiplex.dbvis - stack : TTY=pts/33 ; PWD=/opt/stack/cinder ; USER=root ; COMMAND=/usr/local/bin/cinder-rootwrap /etc/cinder/rootwrap.conf env LC_ALL=C vgsnoheadingsunit=g -o name, size, free, lv_count, uuidseparator :nosuffix stack-volumes-lvmdriver-1	★ 2014-07-30T16:21:07.000 - optiplex.dbvis - stack : TTY=pts/33 ; FND=/opt/stack/cinder ; USER=root ; COMMAND= name,size,free,lv_count,uuidseparator :nosuffix stack-volumes-lvmdriver-1
🖈 2014-07-30T16:20:01.000 - atlantis - pam_unix(cron:session): session opened for user root by (uid=0)	★ 2014-07-30T16:20:01.000 - atlantis - pam_unix(cron:session): session opened for user root by (uid=0)
* 2014-07-30T16:20:01.000 - atlantis - (root) CMD (if [-x /etc/munin/plugins/apt_all]; then /etc/munin/plugins/apt_all update 7200 12 >/dev/null; elif [-x /etc/munin/plugins/apt]; then /etc/munin/plugins/apt update 7200 12 >/dev/null; fi)	★ 2014-07-30T16:20:01.000 - atlantis - (root) CMD (if [-x /etc/munin/plugins/apt_all]; then /etc/munin/plugi update 7200 12 >/dev/null; fi)
🖈 2014-07-30T16:20:01.000 - atlantis - pam_unix(cron:session): session closed for user root	🖈 2014-07-30T16:20:01.000 - atlantis - pam_unix(cron:session): session closed for user root
* 2014-07-30T16:20:07.000 - optiplex.dbvis - stack : TTY=pts/33 ; PWD=/opt/stack/cinder ; USER=root ; COMMAND=/usr/local/bin/cinder-rootwrap /etc/cinder/rootwrap.conf env LC_ALL=C vgsnoheadingsunit=g -o name, size, free, lv_count, uuidseparator :nosuffix stack-volumes-lvmdriver-1	★ 2014-07-30T16:20:07.000 - optiplex.dbvis - stack : TTY=pts/33 ; FND=/opt/stack/cinder ; USER=root ; COMMAND= name,size,free,lv_count,uuidseparator :nosuffix stack-volumes-lvmdriver-1
x 2014-07-30Tl6:20:07.000 - optiplex.dbvis - pam_unix(sudo:session): session opened for user root by (uid=0)	<pre> 2014-07-30T16:20:07.000 - optiplex.dbvis - pam_unix(sudo:session): session opened for user root by (uid=0) </pre>
x 2014-07-30Tl6:20:07.000 - optiplex.dbvis - pam_unix(sudo:session): session closed for user root	2014-07-30T16:20:07.000 - optiplex.dbvis - pam_unix(sudo:session): session closed for user root
★ 2014-07-30T15:20:11.000 - proxy - (CRON) error (grandchild #27732 failed with exit status 1)	2014-07-30T16:20:11.000 - proxy - (CRON) error (grandchild #27732 failed with exit status 1)
★ 2014-07-30T16:20:11.000 - proxy - (CKON) into (No MTA installed, discarding output)	* 2014-07-30T16:20:11.000 - proxy - (CRON) info (No MTA installed, discarding output)
★ 2014-0/-30T16120111.000 - proxy - pam_unix(cron:session): session closed for user munin	2014-07-30T16:20:11.000 - proxy - pam_unix(cron:session): session closed for user munin
x 2014-0/-30116:21:07.000 - optiplex.dovis - stack : Himpts/33 ; PWD=/opt/stack/cinder ; USER=root ;	2014-07-30T16:21:07.000 - optiplex.dbvis - stack : ITY=pts/33 ; PND=/opt/stack/cinder ; USER=root ; COMMAND= name,size,free,lv_count,uuidseparator :nosuffix stack-volumes-lvmdriver-1
★ 2014-07-30T16:20:01.000 - atlantis - pam_unix(cron:session): session opened for user root by (uid=0)	★ 2014-07-30T16:20:01.000 - atlantis - pam_unix(cron:session): session opened for user root by (uid=0)
★ 2014-07-30T16:20:01.000 - atlantis - (root) CMD (if [-x /etc/munin/plugins/apt_all]; then /etc/munin/plugins/apt_all update 7200 12 >/dev/null; elif [-x /etc/munin/plugins/apt]; then /etc/munin/plugins/apt update 7200 12 >/dev/null; fi)	★ 2014-07-30T16:20:01.000 - atlantis - (root) CMD (if [-x /etc/munin/plugins/apt_all]; then /etc/munin/plugi update 7200 12 >/dev/null; fi)
* 2014-0/-30716:20:01.000 - atlantis - pam_unix(cron:session): session closed for user root	★ 2014-07-30T16:20:01.000 - atlantis - pam_unix(cron:session): session closed for user root
* 2014-0/-30116:20:07.000 - optiplex.dovis - stack : TIY=pts/33 ; PMD=/opt/stack/cinder ; USER=root ; COMMAND=/usr/local/bin/cinder-rootwrap /etc/cinder/rootwrap.conf env LC_ALL=C vgsnoheadingsunit=g -o name, size, free, Jv_count, uuidseparator :nosuffix stack-volumes-lvmdriver-1	★ 2014-07-30T16:20:07.000 - optiplex.dbvis - stack: TTY=pts/33; PND=/opt/stack/cinder; USER=root; COMMAND= name,size,free,lv_count,uuidseparator:nosuffix stack-volumes-lvmdriver-1
* 2014-0/-30T16:20:07.000 - optiplex.dbvis - pam_unix(sudd:session): session opened for user root by (uid=0)	★ 2014-07-30T16:20:07.000 - optiplex.dbvis - pam_unix(sudo:session): session opened for user root by (uid=0)
* 2014-07-30T15:20:07.000 - optiplex.dbvis - pam_unix(sudo:seession closed for user root	★ 2014-07-30T16:20:07.000 - optiplex.dbvis - pam_unix(sudo:session): session closed for user root
★ 2014-0/-30116:2011.000 - proxy - (CKON) erfor (granden) a #2//32 failed with exit status 1)	★ 2014-07-30116:20:11.000 - proxy - (CRON) error (grandchild #27732 failed with exit status 1)
× 2014-0/-30116120111.000 - proxy - (CKON) info (No NIA installed, discarding output)	★ 2014-07-30116:20:11.000 - proxy - (CRON) info (No MTA installed, discarding output)
zuiteu/-suitezu:ii.uuu - proxy - pam unix(cron:session): session closed for user munin	2014-07-30116:20:11.000 - proxy - pam unix(cron:session): session closed for user munin

* 2014-07-30T16:21:07.000 - optiplex.dbvis - stack : TTY=pts/33 ; PWD=/opt/stack/cinder ; USER=root ; COMMAND=/usr/local/bin/cinder-rootwrap /etc/cinder/rootwrap.conf env LC_ALL=C vgs --noheadings --unit=g -o

★ 2014-07-30T16:21:07.000 - optiplex.dbvis - stack : TTY=pts/33 ; PWD=/opt/stack/cinder ; USER=root ; COMMAND=

NVisAware: Analytics



Visual Analytics Approach: Calculate and visualize sliding slices. (based on sliding windows)



- Calculate **Sliding Slice Summary** for each sliding window.
- **Push** *slice*_t to web application.

Real-Time Sliding Slice

Feature	Type	\mathbf{Stream}
# events	count	Syslog
timestamps	set	Syslog
# programs	count	Syslog
#hosts	count	Syslog
# frequent Words	count	Syslog
programs	key-value list	Syslog
hosts	key-value list	Syslog
frequentWords	key-value list	Syslog
newHosts	new-set	Syslog
newPrograms	new-set	Syslog
srcAddr	key-value list	NetFlow
dstAddr	key-value list	NetFlow
srcPorts	key-value list	NetFlow
dstPorts	key-value list	NetFlow
topTalker	key-array list	NetFlow
#srcAddr	count	NetFlow
#dstAddr	count	NetFlow
#srcPorts	count	NetFlow
#dstPorts	count	NetFlow
ossecAlerts	key-value list	OSSEC



• Interactive Widgets

- Treemaps
- Counters
- Node-link diagrams

Interactions

- Star/Annotate slice
- Remove slice
- Retrieve data
- Color Encoding
 - Background for similarity
 - Importance of alerts

slice₊

Demo





File Tools View Help

Real-Time Data Stream Real-Time Sliding Slices Visual Feature Selection Summarized Sliding Slices Event Timeline & Insights Search & Exploration



-

| | L3

 | L3 | L3
 | L5 | L3 | L3 | илания
водинализирор-занали в колучу
L3
 | L5 | L3 L10 | L5 L3 | L5 | L5 L10
 | L5 L1 | 0 L5 | La La | L3
 | L3 | L3 | L3 | L3
 | L5 | L3 | илистраница, нологоди и К | индика и классија 🔭 1
ЦЗ | L5
 | L3 L10 | L5 |

--
---|---|--
--	--	---	--
---	---	--	--
--	--	--	--
---	--	--	--
--	--	--	------------------------------
	1041 13 10		

 | di 59 mili 5 mili 6 mili
22. 23. 23. 23. 25.
decerrencial rivin
mili mili 10. 10. 10.
decerrencial rivin
mili 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. | 265 and
Super-Supe | 60 8 4 | 59 | 2329 | n 256 mm 8 mpm 8 mm
 | 120 | 60 and 8 and 7 and 8 and 7 and 9 and 9 and 9 | 60 mm 7 mmm 3 mm
fischer mmm location
scholar den and and and and and and and and and an | 59 mm 4 mun 6 mm
Difference 1 mm 1 | 28 4 4
the an end and an end | 29 2 2
Description
optiplex
fischersshd
 | 90 | an 60 and 5 maps 3 and
an an a | A 384 rests 10 respect 11 rest | 57 | 1041 13 10
 | 59 mmb 5 mman 6 mmb | 265 | 60 | 59 mm 6 mapping 3 mm
4 mm 7 mm 7 mm 7 mm
14 mm 7 mm 7 mm
14 mm 7 mm
14 mm 7 mm
14 mm 7 mm
14 mm | 2329
 | 256 mm 8 mm 8 mm | 120 mt 6 mpm 3 mm 6 | Const. 8 march 7 mar
22 Annual Annua | 50 7 |
| entin cron | and a second sec

 | All of details waterials are seen in the second sec | For example, and the second se | for down and the set of the set o | Alter to USEP (types) and the up of | Victoria de la compansión | And a second sec | too to | not sum of etc. = 40
 | A second | And the second s | news science | dbvis fatures (new Provide
tailed with rule for pert
location rule) for the second second
location rule for the second second
disconnecting | - fordbyls optiple
byel shift stars was not by the stars
for dbyls optiple
byel shift shift stars works | The second | manual and the party state with the second state of the secon | dev dev transformer under som en ander
dev dev dev dev dev dev dev dev dev dev
dev dev dev dev dev dev dev dev dev dev
 | Tool was an | The deal and an and the second | Contraction of the second seco | Singly and the second s | A start use USEP to what is a start use USEP to what is a start use use a start use to be a start use | An and a second | And the second s | alled dbyls user rot rot rot concerned auto potential | n mi etc. 44 n
 | alert
salert
nate eary |
| X.XXX | Remaining and an and an and an and an

 | Ossec Cron Dever | Cron Case an Det
 | Ossec Sshd ^{tow} C | 92.xxx.xxx.xxx | Cron Ossec | Terranae

 | Ossec Sshd bornd | TE-mail and an | Dessec Sshd Spend | 192.xxx.xxx.xxx
Ossec Cron Sshd | 192.xxx.xxx.xxx
 | Ossec Sshd | Ossec Sshd Spard | 192.xxx.xxx.xxx | Ossec Cron
 | 192.xxx.xxx
 | 700 Million Ann | 192.xxx.xxx.xxx
ossec Cron over | Cron from an and
 | Ossec Sshd burd | 192.xxx.xxx - | Cron Ossec | Cron _ 640 | ssec Sshd burs be
 | | Dssec |
| 0101 | 100 00 00 00 00 00 00 00 00 00 00 00 00

 | 2 223 235 327 | 10.075 00 00 00 00 00 00 00 00 00 00 00 00 00
 | 0.05 1.05 - 0
201230
201230
201230 | n n n n n n n n n n n n n n n n n n n | |
 | 2.05 2.05 2.05
ACT 2.0 | | COLORE CONTRACTOR | 0.05, 0.05, 0.05, 0.05
0.00, 0.0
0.00, 0.0
0.00, 0.0
0.00, 0.0
0.00, 0.0
0.00, 0.0
0.00, 0.0
0.0
0.0
0.0
0.0
0.0
0.0
0.0
0.0
0.0 | 044
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075)
(1075 | 10.00 (0.00) | NATURAL AND A CONTRACT | | FIR ROS
 | 0105 0105 00
0105 0105 00
0000 00
00 | 310 | 235 295 314 | ILEX No. 10 10 10 10 10 10 10 10 10 10 10 10 10
 | ALLER STREET | 2015 0005 00 00 00
2010 0 00 00 00 00
2010 0 0 00 00 00 00 00 00
2010 0 0 00 00 00 00 00 00
2010 0 0 00 00 00 00 00 00
2010 0 0 0 00 00 00 00 | |
 | | PELID C | |
| L3
5 8, 8 | 60 8

 | 4 59 6 3. | L3
 | L3 | L5 | 3 60 8 | L10 L5
 | L3 L5 | 6 28 4 | L10 L5 | L10 L5 | 60 5
 | L3
3 384 10 | L3 | . 7 | L3
 | 6 265 8, | 8 60 8 | 4 59 6 | L3
3 2329 16
 | L3
12 256 8 | 8 120 6 | L3 L | L5 | .3 L5
 | 28 4 4 | 29 |
| USET | in i

 | ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
ther
t | (a) (a) (b) (b) (b) (b) (b) (b) (b) (b) (b) (b
 | | authentication | the second | An and a second | | lacation
 | the second secon | diana dia dia dia dia dia dia dia dia dia di | Covered and a covered and | Harris Contraction of the second seco | | | A constraint of the second of | With the second | and in
 | her
to the second seco | | | authentication | And And And And And And And And And
 | fischer wird und die state wird in die state wir | | fischer
plages and possible
transfer and possible
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fischer
fisc | dbr |
| Session units of the second | fordbyistering
and
and
and
and
and
and
and
and
and
and

 | 192.xxx.xxx |
 | PART SCIENCE OF THE PART OF TH | deconnecting and the | International Control of Control | munin
r: cron
ML answer
ML ans | X ² Part
af
for frame-pineter
balance point user
failed sension
fischer
fischer X ² Part
af
for frame-pineter
balance
failed sension
fischer 192.xxxx.xxxx.xxxx | auth level
and level
auth entication
authentication
g | Toot authentical discovering
 | tion
for development of the second se | iplex
isation
192.xxx.xxx.xxx | The second secon | on and an and an and an an and an | The second secon | Representation of the second s | SET Iog
Digiti
Marking Stream of the second
Digiti of the second | | Plog
 | And uses a second secon | And the second s | deconnecting automatic | Mer on the second secon | nin nin nin hand we want hand be want hand b | or fischer under USCR ach Level | sthd for examples of the state | h 25.000 |
| 1 | Ner Ossec Ssho

 | d Dear
Deser Cron men
and Dear
Deser Deser and | Image: Cron Output Image:
 | Cron Cuto | Ossec Sshd | Sound for Cron an | Ossec Sshd | Spend Ossec Cron S
 | Sshd and Cron Ossec Ss | hd 114 Ossec Ssh | nd Ossec Sshd our | and a real Dovecot Osse
 | ec Ossec Cron | AND IN A CONTRACT OF A CONTRAC | | Contraction of the second seco | | feet Ossec Ssho | tournel
on
on
on
on
on
on
on
on
on
on
 | | Cron della | P Ossec Sshd
 | | Ossec Sshd Her | Ossec Cron Sshd | Cron Ossec Sshd | dati OSS |
| L5 L1 | L5

 | L10 L5 | interest and the second | NUM Reserve of second
 | 2012/04
Secure 10:000 | L3 | L3 | алунааны до
 | L5 | L3 | или К аланданан (т | лад * 2000
Эндэр эндэр эндэгээ
ЦЗ
 | кисто Колональная
Станальноватара-такалая
L5 | L10
L3 | L10 L5 | L3 L5 | L5
 | L10 L5 | L10 L5 | Carlos II
Security Discourse Production of the Carlos of | Note: Note: State of the second secon | Nipri * Second physics and the second physics | L3 | L3
 | L3 | L5 | 3 |
| 4 4
a a a an a | . 29 2

 | 2 | 60 5
 | 3 | 11 57 5
 | . 7 1041 13. | Anna 10 and 59 and 5 and | 6 265 8
 | Hanning Street S | | 3 | 12 | 8 tak 120 ant 6 man
 | Sura 60 and 8 appen | 7 | 3 59 4 | 6 28 4
28 4
5 | 4 29 2
 | 2 | 6 | 3 | 1 57 5
 | | 59 5 6. | 265 | 60 8 4

 | . 59 |
| Session log et social de la session de la se | dbvis fatures rear of
fature definition of
fature definition of the
fature definition of the
fat | destth
sart
sart
tion
tion
 | - Shift and a second se | A Contract of the second secon | | | All, the second | | | X talante - Alexandro and Spanish and Span | | The second se | authentication | anny sha
ann tsha
lager | sing and a start a | Market for desired and the second sec | auchi sector and and auchieve and auchieve and and auchieve and and auchieve and auchieve and auchieve | dbvis fischer sche
dbvis fature, mar bog to re
author war bog to re
boat authenticat | loath
at the second sec | - Staffer plan and and a staffer plan and a staffer | tip location distance and the second | A second | A the second sec | And the second s | Contraction of the second seco | sthd and the second sec | |
| x.xxxx.xxxx |

 | by by at a series and a series and a series at a serie | | F
 | ΧΡΙ | $\cap R$ | ΔΤΙ | | |
 | ~нΔ | | NGF |
 | | The second secon | | for fischer | authentication |
 | akert splyd fatures | 192.xxx.xxx.xxx | | 192.xxx.xxx.xxx
 | | 192.300X.300X | Analysis and a second stands with an analysis and a second stands with a second stands with a second stand stand stands with a second stand stan | | 192.x |
| Ossec Sshd % | Cossec Sshi

 | Id Ossec |
 | | | |
 | | | | | •
 | | | Cosec Sahd | opend Ossec Cron Sst
 | Cron Ossec Ssh | d 400 Ossec Sshi | d Ossec Sshd hund |
 | | Ando Cron Uncedary
cron cron
in the intervention of the control | | | | Ossec Sshd turn
 | Osse |
| L5 | L5 6 28 4

 | L10
. 4 29. |
 | | | |
 | | | | |
 | | . 8 120 | .5 L10 L3 | L10 L5
 | L3 | 5 • L5 | L10 L5 | L10 L5
 | | 3 L: | L3 | L3 | L3
 | L3 | 8 |
| optiplex local | tion
numb
Sur the surget services of the service services of the services of the services of the service services of the service services of the service services of the service services of the services of t

 | 4 205 25 |
 | \mathbf{O} | W | |) E
 | | | | | | |
 | | | In an | |
 | Lex location
or dby Same
bit and the same
bit | er optig
nor og et
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optigert
optig | Deex
Prost | Construction C | Constant and the second | |
 | | | |
| shd formetine
night preken rang
on ver USET auth
failed session
fischer | authentication

 | name obvis
plex rout
name routin |
 | | | |
 | | | | |
 | | or and the second secon | by Secure and Secure a | | ind the second s | strangen up and a strangen autor a strangen autor a strangen autor a strangen autor | section and the section of the secti | Base parameters
of unreacting and the standard s | Soptiplex
state former
state state
state former
state state
state former
state state
state state
state
state state
state state state
state state state
state state state
state state state state
state state sta | Bang Malana Up
Sama
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Salar
Sa | Store and a store | CODE UNITY OF A CODE OF A | And and a second | been to be the second s | A POOL IN A |
| sec Cron Ssh | d Tron Ossec S

 | Bshd Will Osse |
 | | | |
 | | | | |
 | | City Ossec S | Sshd turn for Cron water | Ossec
 | Sshd apend Ossec C | ron Sshd 🚎 Cron Oss | ec Sshd With Ossec | Sshd Ossec Sst
 | Id ^{3yerd} Dovecot | Ossec Ossec Cron | 192.000.000 | | Ossec Cron Com
 | Cron team | |
| | ere affekten pro

 | лордина
предокалога власти |
 | | | / 5 |
 | | IG | 51 | | 25
 | | anto sa nos | 15 110 |
 | 1 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - | -1.00
 | ерии
ре-ликиталице × • • • • • • • • • • • • • • • • • • |
 | | 1000 / 10 | славать какодо жили на | 2
2
2
2
2
2
2
2
2
2
2
2
2
2
2
2
2
2
2 | антантия К антантана
13
 | ************************************** | Cases o pays |
| 384 10 |

 | 5 |
 | | | |
 | | | | |
 | | | 2 | 9
 | 5 | 10 | 5 | 13 10 59
 | 5 | 8 ₁₁₁₁₁ 81111 80 | B | angun 3 2329 11 | ingen 12.un 256.mn 8.mp
 | | 3 |
| Area race with Electron and
a manufacture of the second se | | USE
Sector 2000 Sector 2000 S | La conserva de la co | eted right
and right
and the set of the set
and the set of the set | The second secon | population fischer
population fischer
and | See the second s | | USA STATES AND | tication
formers shd
dbvis ratee | by is an analysis of the second secon | In the second se | iplex location
intervent of auton
intervent | scher
¹ den | ptiplex
scher shd
fatures for part
on IOS top formation
on IOS | SCREET | A set of the set of th | Image: Strategy and the strategy a | USE Control of the second seco | The second secon | the rest of the re | | fischer
Diex talaren
Strate in tuter
inter in tuter
level inter inter inter inter inter inter
officiel inter inter inter inter inter inter inter
officiel inter inter inter inter inter inter inter inter
officiel inter inter inter inter inter inter inter inter inter
officiel inter in | The same is a part of the same is a | The second secon | authentica | ition
Frailures sch |
| TE BRANCE THE THE SECOND AND AND AND AND AND AND AND AND AND A | SSION

 | SOCOCION Terreral di Antonio di A | All years data of the form
the set of the s | ESSION Open
(1 option
XX.XXXX
 | | bvis one part of the part of t | AND | | ession can reach and the second secon | fischer ware and an and an and an and an and an | IX many munin
IX many munin
many munin | PUPIFEX Service for failed on the failed of | scher authen
 | Preservery foot all sication mumin contract of the second mumin contract of the second | discenecting | byls optiplex
atures as acation 192.xxx.x | COSIN method
systemin insetter
COX.XXXX | Session
 | COX.XXXX Transman | All the second state of the first second state of the second state | SSID Data
t option
0X.X00X | | alert me log
 | COSTON OF THE CO | And Andrew Service Ser | n can be and the set of the set o | presum |
| Ossec Cron | Cron

 | Cron and Aller | Ossec Cr
 | on Detroit Cron interest | an a | C Sshd twe Ossec C | zon men han Cron Osee
 | Re manual and a second | Code
OSSEC | Sin sun sun sun sun sun sun sun sun sun su | Ossec | Sshd ⁰ jand
0

 | Cron Sshd ar Cron C | Issec Sshd our Ossec | Sshd Ossec | Sshd and a sum a s | Ossec Cr | on and and and and and and and and and an
 | | Anno and Anno Anno Anno Anno Anno Anno Anno An | on Devour | ter
 | Sshd tourid
 | The second secon | na bala na bal | Ossec Ssh | d seed |
| 3 | L3

 | L3 | LS
 | L3 | или жаларыны жаларын жаларын жанарын жанарын каларын жанарын жанарын жанарын жанарын жанарын жанарын жанарын ж
Цз | инала
иналариянара, выявля в колор
L3 | L5
 | L3 L1 | L5 L3 | L5 | L5 L10 | L5 L10
 | L5 | L3 | L3 | L3
 | L3 | L3 | L3 | L5 L3
 | L3 | на ж.
воластоница – родитарии на
L3 | ликалананан калана
Макаланан калан
ЦЗ | L5 | L3 L10
 | L5 L3 | L |
| 13 10 | 59 meth 5 meter 6 met
decorrected from
decorrected from
transformet tado

 | | 60 8 4 5
 | 9 and 6 august 3 and 2 | 329 16 12 | 256 | 120 ant 6 man 3 and
 | 60 | 60 7 3
fischer | 59 4 6
EX EX EX EX
optiplex location
optiplex or other and | 28 4 | 29 2 2
29 2
poptiplex
fischer wid
 | 90 and 9 mars 6 and
prost bases on a choracting
prost bases on a choracting
and a set of the set of the set of the set
of the set of the se | 60 5 | at 384 men 10 men 11 m | m 57 5 | 1041 13 10
 | 59 cmb 5 cmpers 6 cmb | 265 | 60 8 4
A | 59 resk 6 regent 3 rok
 | 2329 16 12 | 256 | 120 6 | 60 | 0
 | 59 |
| All the second s | rule count a week with the part of the second a | Contraction of the second seco | for dbvistment of the second s | All the USEP (christ) ing
All the path are and days
and the second days
and the second days
ing the second day | user
1001 | And the second s | too a bet of the server of the | sum and etc = etc = etc = etc
login
root = etcalest
HUSET unix Date munif | and a second sec | The second secon | marks session log en
period session log rate to con-
mentation optiples
and for manager of the dbvis
and for manager of marks
and for manager of marks
authentication | dbvis fatures fully prouch
fatled vitring for part
learning to the state of the state
learning for the state of the state
authentication
disconnecting | for dbvis optiple | | Description of the second state in the second state in the second state in the second state is the se | A set of the set of th | and the part of | All cloud a soft VI and the soft of the so | 2000 growth of the data of the | sthd opt 20 break | All the second s | X do)
USBF
10 ¹ m TOOL man | The second secon | to a formation of the second s | un al etc 01 | aldt - Loog - Lo | 2 - Sshd ftor
10 - rate |
| | 92.3000.3000

 | | 00000 Sebul ³⁰ Oc
 | 2.xxx.xxx.xxx | 1000 ag mon of Mail 11 on 2000 | |
 | | | | 192.300.30X.30X | The second secon
 | Alert spig landers une location | 192.xxx.xxx | Tenner and a start | | |
 | | Total Total <th< th=""><th></th><th>192.xxx.xxx</th><th>Implying and an end of the second s</th><th></th><th></th><th></th><th>nor Sabi Deni</th><th>92.000.0</th></th<> | | 192.xxx.xxx | Implying and an end of the second s |
 | | | nor Sabi Deni | 92.000.0 |
| | 220 235 335 -

 | 1010
1015 | Anna Anna Anna Anna Anna Anna Anna Anna
 | | 2011/00/00 (2011/00/00/00/00/00/00/00/00/00/00/00/00/ | | POR NOR SUR CONTR
 | | | | ACCINE. SOLID THE STREET STREE | South Contraction
 | | | | 2012/01 0100 000 000 000 000 000 000 000 000 |
 | 10.000 0000 0000 0000 00000000000000000 | And the second s | Contraction of the second of t | 2015 0.05 m m | 10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10.10
10 | 2012/21/C
 | | | | |
| 3
13., 10 | L3
59 5 6

 | L3
265 8 8 | L5
60 8 4 5
 | L3
9 6 | L3 | L3
256 8 | L5 L5
 | L3 L10 | 60 7 3 | L5 • | L5 L10 | L5 L10
 | 90 9, 6 | L3 | L3 | L3
 | L3
1041 13 10 | L3
59 5 6 | L3
265 8, 8 | L5 L3
 | L3
59 6 | L3
2329 16 12 | L3
256 8 | L5 L10 | L3 L10
 | L5 L3
Restlet
0 7 | 59 |
| | Math Math Math discorrocted risin Uppl minimum discorrocted risin Uppl minimum discorrocted risin Uppl minimum discorrocted risin Uppl risin discorrocted risin Uppl minimum discorrocted risin Uppl risin discorrocted risin <th>An An A</th> <th>optiplex reasons and and and and and and and and and and</th> <th>A DE DATE DE CONTRACTOR DE LA CONTRACTOR</th> <th></th> <th>COMPARENT OF CONTRACTOR OF CON</th> <th>authentication</th> <th>The second secon</th> <th>fischer with the organization</th> <th>optiplex location
in fall Surger at auto
for control of the surger at auto
for control of the surger at auto
for control of the surger at a surger</th> <th>fischer
plagis upgenord returns
incase session to the session
incase session
incase</th> <th>optiplex
fischer stid
dbvis fatures for and</th> <th>prosthere</th> <th>Covecol_stat Covecol_stat Covecovecol_stat Covecol_stat Covecol_stat Covecol_stat</th> <th>A Construction of the second s</th> <th></th> <th></th> <th>decorrected risks
with the second risks
wit</th> <th>Mode Address Made Made www.www.www.www.www.www.www.www.www.ww</th> <th>sthd</th> <th>A Construction of the second s</th> <th>The second secon</th> <th>Bark Bark Bark Bark </th> <th>authentication</th> <th>R. 2. R. R. R. F. F. F. Start Start</th> <th>scher international and and and and and and and and and and</th> <th>optir
optir</th> | An A | optiplex reasons and | A DE DATE DE CONTRACTOR DE LA CONTRACTOR | | COMPARENT OF CONTRACTOR OF CON | authentication | The second secon | fischer with the organization | optiplex location
in fall Surger at auto
for control of the surger at auto
for control of the surger at auto
for control of the surger at a surger | fischer
plagis upgenord returns
incase session to the session
incase | optiplex
fischer stid
dbvis fatures for and | prosthere | Covecol_stat Covecovecol_stat Covecol_stat Covecol_stat Covecol_stat | A Construction of the second s | | | decorrected risks
with the second risks
wit | Mode Address Made Made www.www.www.www.www.www.www.www.www.ww | sthd | A Construction of the second s | The second secon | Bark Bark Bark Bark | authentication | R. 2. R. R. R. F. F. F. Start | scher international and | optir
optir |

Visual Feature Selection

Selected Ranked Features

Visual Analytics Approach: Aggregate / Summarize according interest function (visually steered by the expert)



Example: Using Visual Analytics for Interactive Summarization



Demo





<u>^</u>

Application to Real-Time Social Media Analysis (VAST Challenge 2014 MC3)

- Real-Time Monitoring Task: Discover major events in the stream to support an ongoing police operation.
- Available Data Stream: Real-time feeds of microblogs and emergency calls.
- Successful participation: "Award for Outstanding Comprehensive Mini-Challenge 3 Submission"





Further Challenges and Future Work

- Challenge: Parameter adjustment for sliding slices and clustering.
- Automated merging of sliding slices based on the interest function.
- Performance Evaluation for a large network using security operational data stream.
- Responsiveness issues

when increasing the number of complex interactive visualizations.

• Data retention and rotation for the visualization interface.

Contributions

DATA CHALLENGE How to make stream analysis <u>scalable</u>? • NStreamAware – Building a *web-based visual* analytics system using scalable technologies.

SA CHALLENGE How to <u>reduce</u> the cognitive load? • NVisAware – *Sliding Slices Visualization* with embedded visualization widgets.

EXPLORATION CHALLENGE How to <u>explore</u> many sliding slices? • NVisAware – *Summarized Sliding Slices* steered using interactive visualizations.

Thank you very much for your attention!

Questions?

For more information about this work please contact

Fabian Fischer Tel. +49 7531 88-2780 Fabian.Fischer@uni-konstanz.de

http://ff.cx/

	optiplex [30] auth=dicementation	The SECK VAP auth The for these events and the sector of the sector and the sector sector of the sector and the sec	Abrit UIIX is a star of the st	all = == FOO
	000000 2555 00 00 00 00 000000 0000000000	Cosee Sudo Con	192.xxx.xxx	1500000 1000000000000000000000000000000
	51.575 40.575	33.25% 26.0% um um	425	50.00%
		0		
		Alert Lovel: 10		
		Alert Level	H	
		Removed leasers	Mark My Mark	m
twitter		· Alen Jent & Mary	malan	
@f2cx				
GILCA				

1.3

1.3

13

Fabian Fischer | NStreamAware: Real-Time Visual Analytics for Data Streams to Enhance Situational Awareness