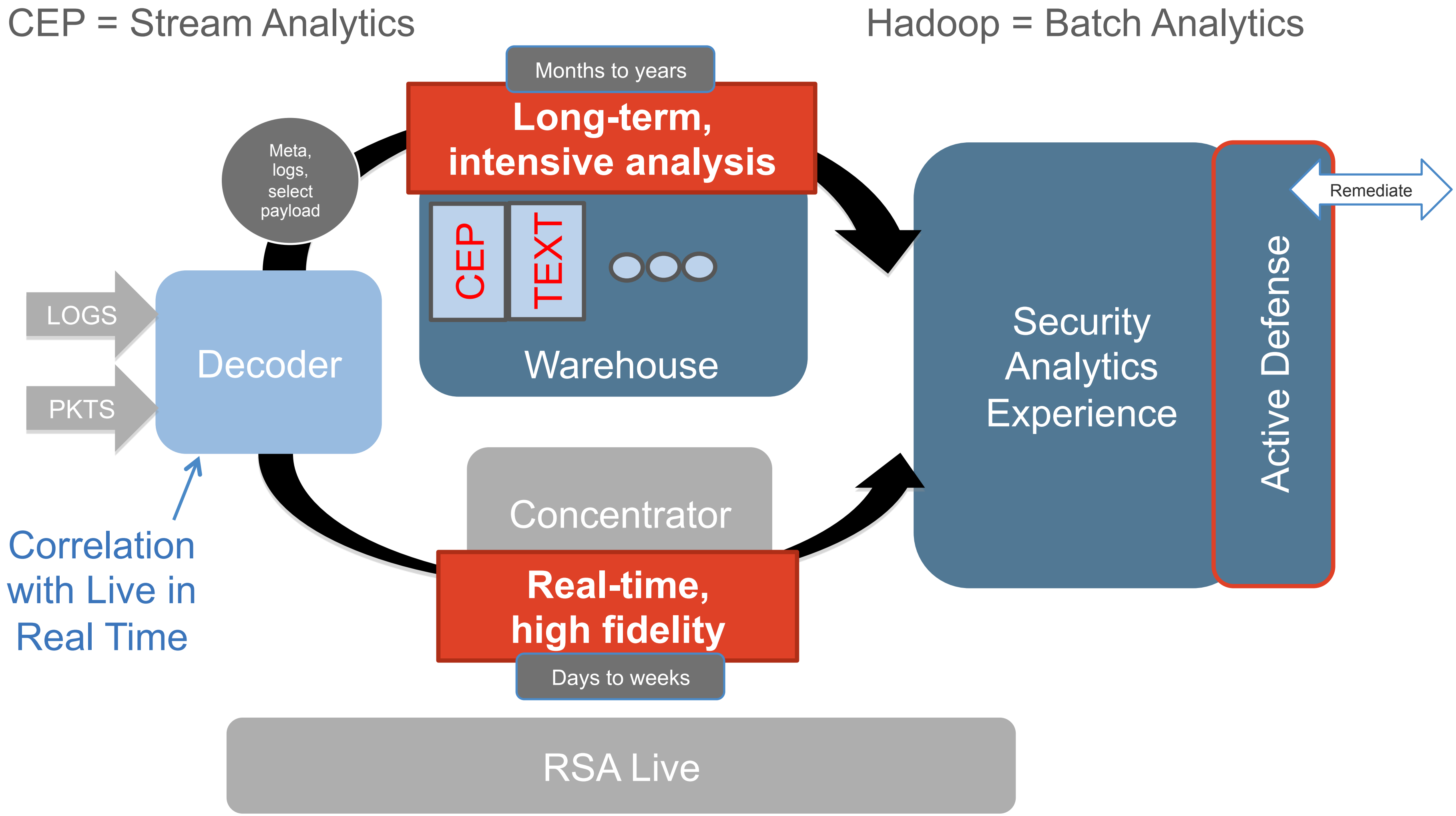
Security Analytics Topology



SA v10.2 Malware Analysis

SA 10.2 Features – Malware Analysis

- Integration into the Security Analytics Infrastructure
  - Flexera Licensing Support
    - Simple on/off functionality in 10.2
    - More granular control in subsequent releases
  - New Investigation Workflow
    - Right-click from Investigation to scan a subset of sessions for malware
  - New Scoring Visualization
    - Scoring wheel
    - Uses color-coding to show relationship between scoring methodologies
    - More new visualizations in subsequent releases
- Submission Methods
  - Ad-Hoc Scan from Investigation
  - Manual File Upload
  - Continuous Scanning

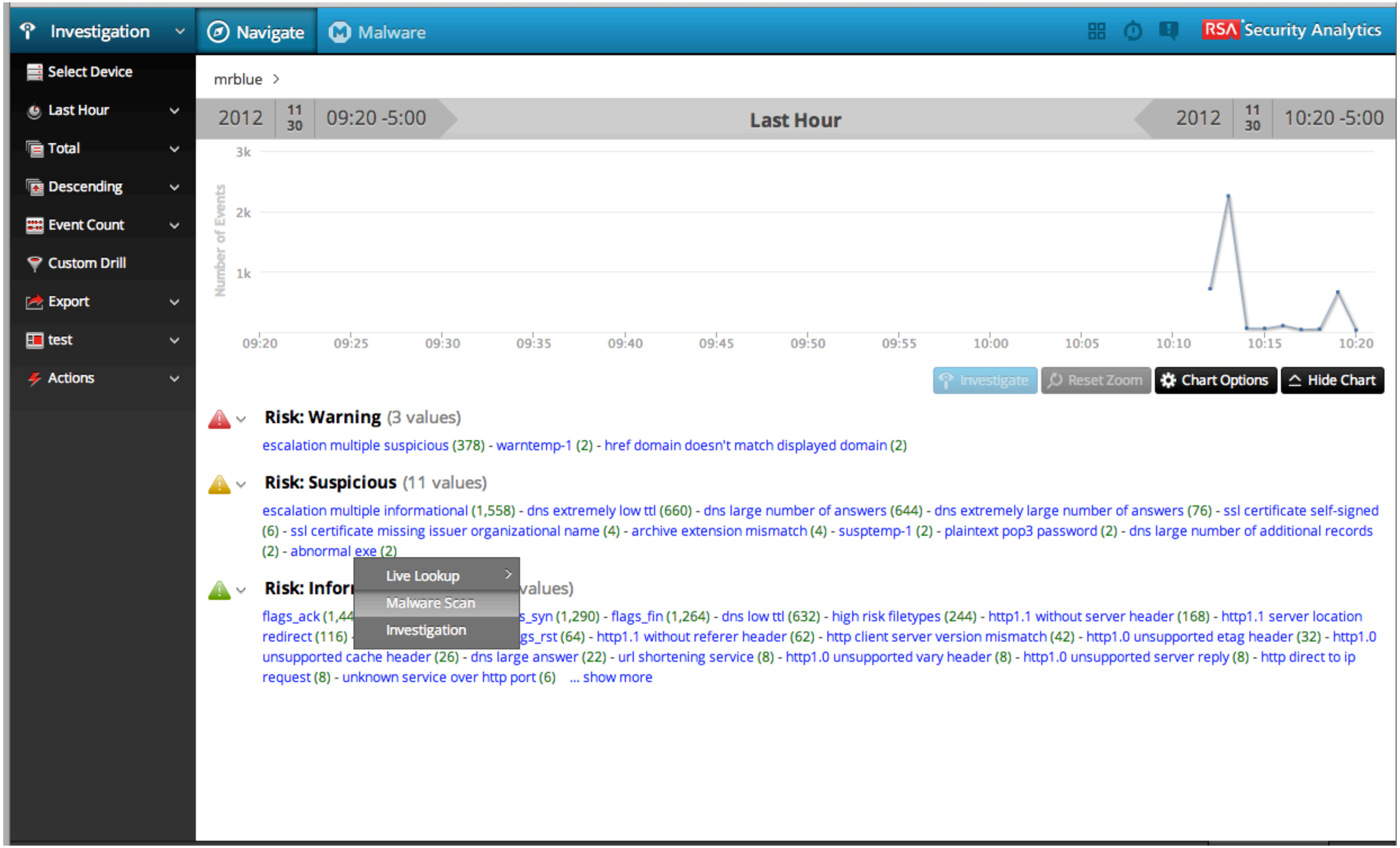
SA 10.2 Features – Malware Analysis

- Deeper ThreatGRID functionality
  - Click out to the ThreatGRID GUI from the event detail page
- Tiered Submission Levels
  - Free
    - 100 sample scans (network, static & community) per day
    - 5 sandbox submissions per day
    - Included with all SA Server installations
  - Standard Subscription
    - Unlimited sample scans
    - 1000 sandbox submissions per day
    - Requires appliance purchase
  - Enterprise Subscription
    - Unlimited sample scans
    - 5000 sandbox submissions per day
  - Local Sandbox Provided by ThreatGRID

SA 10.2 Features – Malware Analysis

- Scan Resubmit Functionality
  - Ability to resubmit Ad-Hoc or Manual Upload scans
    - Override any file type restrictions set in service configuration
    - Queue Prioritization
- Custom Scoring
  - All scoring rules can be enabled/disabled as well as weighted to fit customer environments
  - High Confidence denotation
    - Escalates score when rule fires
    - Sortable in event view
  - Reset to OOB default if needed
- Performance Enhancements
  - Asynchronous Sandbox Submission
    - Allows threads to be freed up as opposed to waiting for results

Malware Scan from Investigator



Risk: Warning (3 values)

escalation multiple suspicious (378) - warntemp-1 (2) - href domain doesn't match displayed domain (2)

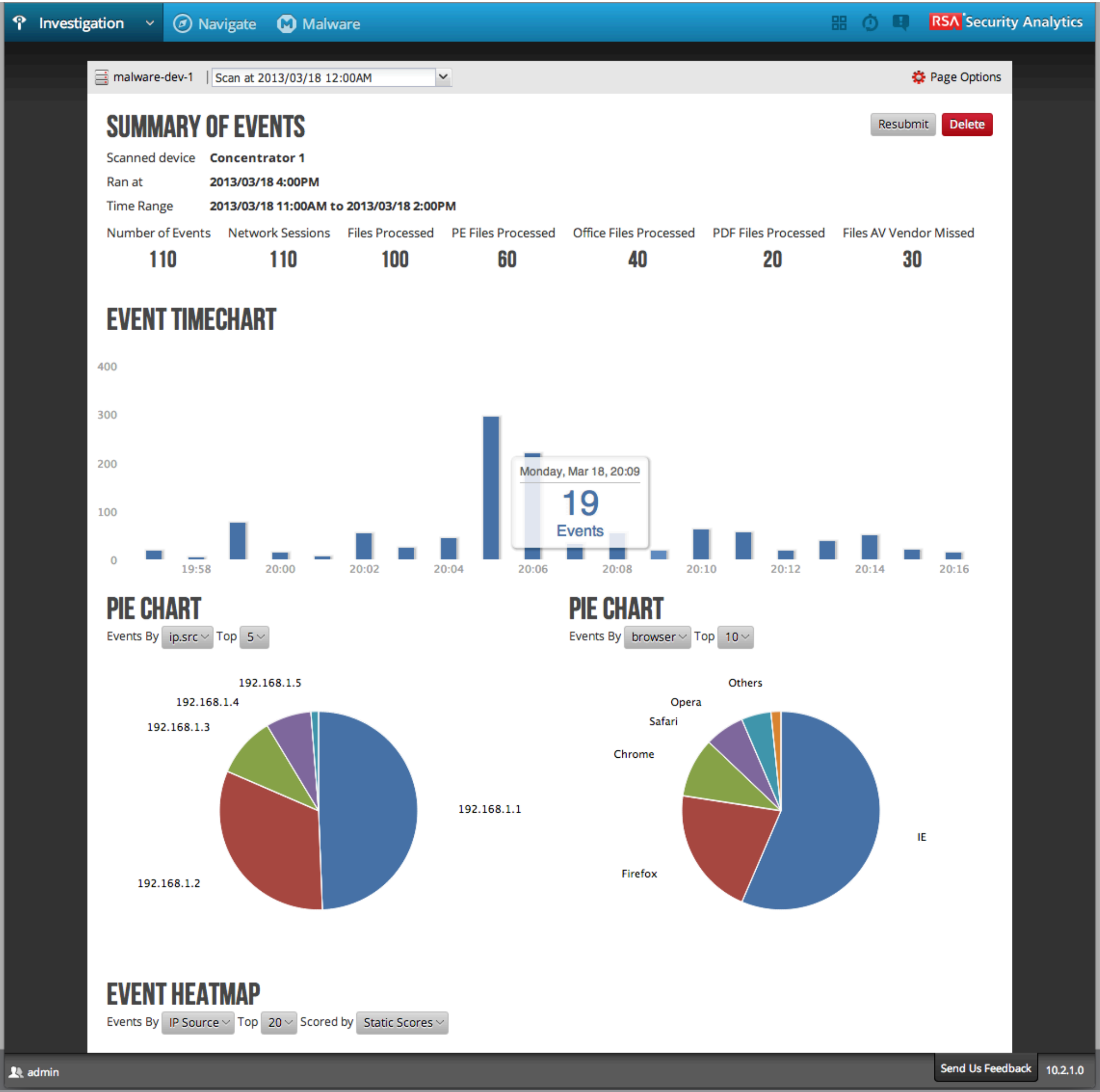
Risk: Suspicious (11 values)

escalation multiple informational (1,558) - dns extremely low ttl (660) - dns large number of answers (644) - dns extremely large number of answers (76) - ssl certificate self-signed (6) - ssl certificate missing issuer organizational name (4) - archive extension mismatch (4) - susptemp-1 (2) - plaintext pop3 password (2) - dns large number of additional records (2) - abnormal exe (2)

Risk: Infor values)

flags_ack (1,44 s_syn (1,290) - flags_fin (1,264) - dns low ttl (632) - high risk filetypes (244) - http1.1 without server header (168) - http1.1 server location redirect (116) - gs_rst (64) - http1.1 without referer header (62) - http client server version mismatch (42) - http1.0 unsupported etag header (32) - http1.0 unsupported cache header (26) - dns large answer (22) - url shortening service (8) - http1.0 unsupported vary header (8) - http1.0 unsupported server reply (8) - http direct to ip request (8) - unknown service over http port (6) ... show more

Malware Summary



SUMMARY OF EVENTS

Scanned device **Concentrator 1**

Ran at **2013/03/18 4:00PM**

Time Range **2013/03/18 11:00AM to 2013/03/18 2:00PM**

Number of Events	Network Sessions	Files Processed	PE Files Processed	Office Files Processed	PDF Files Processed	Files AV Vendor Missed
110	110	100	60	40	20	30

EVENT TIMECHART

PIE CHART

Events By ip.src Top 5

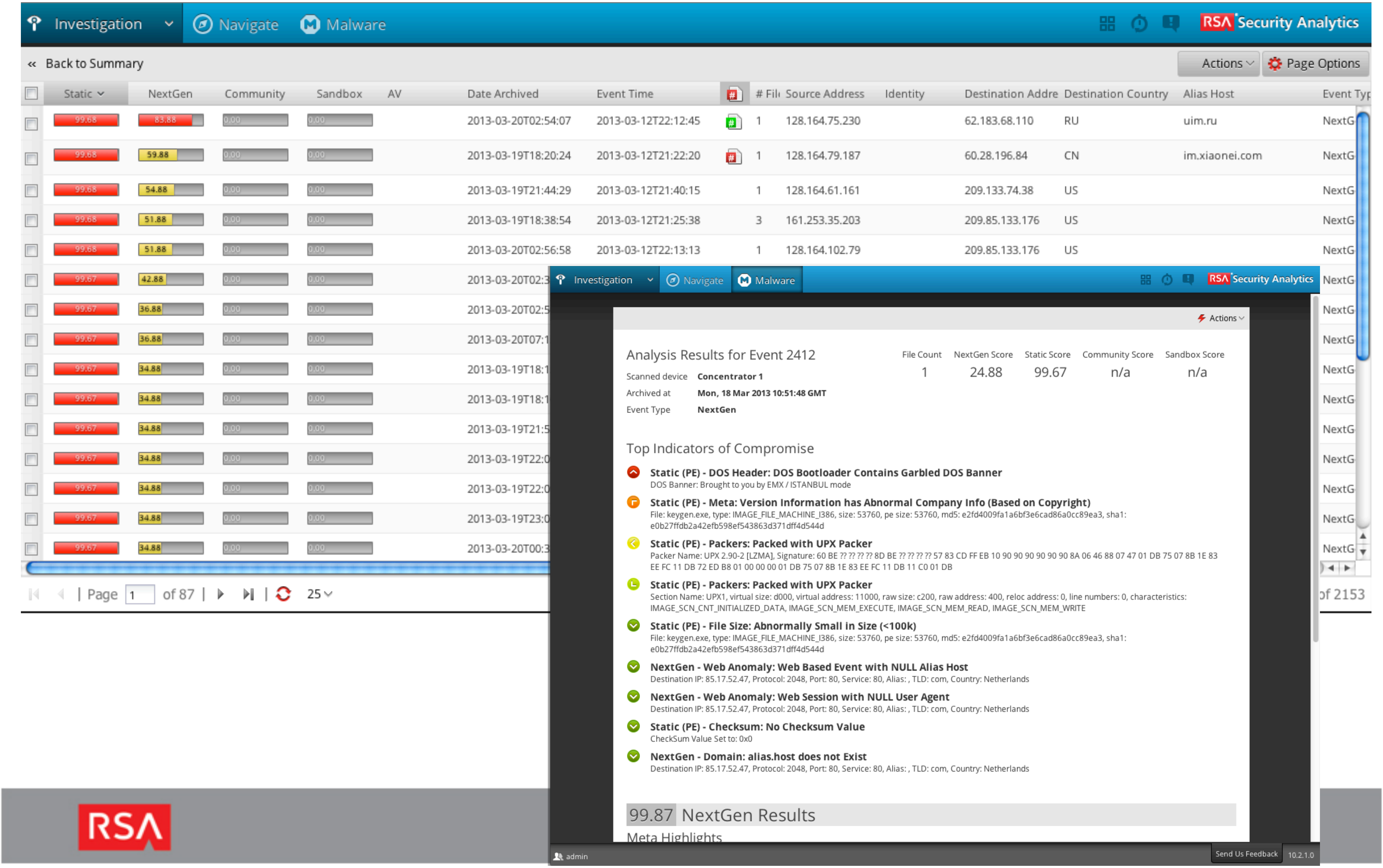
PIE CHART

Events By browser Top 10

EVENT HEATMAP

Events By IP Source Top 20 Scored by Static Scores

Malware Events



☐	Static	NextGen	Community	Sandbox	AV	Date Archived	Event Time	#	# Fil	Source Address	Identity	Destination Addre	Destination Country	Alias Host	Event Typ
☐	99.68	83.88	0.00	0.00		2013-03-20T02:54:07	2013-03-12T22:12:45	#	1	128.164.75.230		62.183.68.110	RU	uim.ru	NextG
☐	99.68	59.88	0.00	0.00		2013-03-19T18:20:24	2013-03-12T21:22:20	#	1	128.164.79.187		60.28.196.84	CN	im.xiaonei.com	NextG
☐	99.68	54.88	0.00	0.00		2013-03-19T21:44:29	2013-03-12T21:40:15		1	128.164.61.161		209.133.74.38	US		NextG
☐	99.68	51.88	0.00	0.00		2013-03-19T18:38:54	2013-03-12T21:25:38		3	161.253.35.203		209.85.133.176	US		NextG
☐	99.68	51.88	0.00	0.00		2013-03-20T02:56:58	2013-03-12T22:13:13		1	128.164.102.79		209.85.133.176	US		NextG
☐	99.67	42.88	0.00	0.00		2013-03-20T02:3									NextG
☐	99.67	36.88	0.00	0.00		2013-03-20T02:5									NextG
☐	99.67	36.88	0.00	0.00		2013-03-20T07:1									NextG
☐	99.67	34.88	0.00	0.00		2013-03-19T18:1									NextG
☐	99.67	34.88	0.00	0.00		2013-03-19T18:1									NextG
☐	99.67	34.88	0.00	0.00		2013-03-19T21:5									NextG
☐	99.67	34.88	0.00	0.00		2013-03-19T22:0									NextG
☐	99.67	34.88	0.00	0.00		2013-03-19T22:0									NextG
☐	99.67	34.88	0.00	0.00		2013-03-19T23:0									NextG
☐	99.67	34.88	0.00	0.00		2013-03-20T00:3									NextG

Page 1 of 87 | 25 … of 2153

Analysis Results for Event 2412

File Count	NextGen Score	Static Score	Community Score	Sandbox Score
1	24.88	99.67	n/a	n/a

Scanned device **Concentrator 1**
Archived at **Mon, 18 Mar 2013 10:51:48 GMT**
Event Type **NextGen**

Top Indicators of Compromise

Static (PE) - DOS Header: DOS Bootloader Contains Garbled DOS Banner
DOS Banner: Brought to you by EMX / ISTANBUL mode

Static (PE) - Meta: Version Information has Abnormal Company Info (Based on Copyright)
File: keygen.exe, type: IMAGE_FILE_MACHINE_I386, size: 53760, pe size: 53760, md5: e2fd4009fa1a6bf3e6cad86a0cc89ea3, sha1: e0b27ffdb2a42efb598ef543863d371dff4d544d

Static (PE) - Packers: Packed with UPX Packer
Packer Name: UPX 2.90-2 [LZMA], Signature: 60 BE ?? ?? ?? ?? 8D BE ?? ?? ?? ?? 57 83 CD FF EB 10 90 90 90 90 90 90 8A 06 46 88 07 47 01 DB 75 07 8B 1E 83 EE FC 11 DB 72 ED B8 01 00 00 00 01 DB 75 07 8B 1E 83 EE FC 11 DB 11 C0 01 DB

Static (PE) - Packers: Packed with UPX Packer
Section Name: UPX1, virtual size: d000, virtual address: 11000, raw size: c200, raw address: 400, reloc address: 0, line numbers: 0, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Static (PE) - File Size: Abnormally Small in Size (<100k)
File: keygen.exe, type: IMAGE_FILE_MACHINE_I386, size: 53760, pe size: 53760, md5: e2fd4009fa1a6bf3e6cad86a0cc89ea3, sha1: e0b27ffdb2a42efb598ef543863d371dff4d544d

NextGen - Web Anomaly: Web Based Event with NULL Alias Host
Destination IP: 85.17.52.47, Protocol: 2048, Port: 80, Service: 80, Alias: , TLD: com, Country: Netherlands

NextGen - Web Anomaly: Web Session with NULL User Agent
Destination IP: 85.17.52.47, Protocol: 2048, Port: 80, Service: 80, Alias: , TLD: com, Country: Netherlands

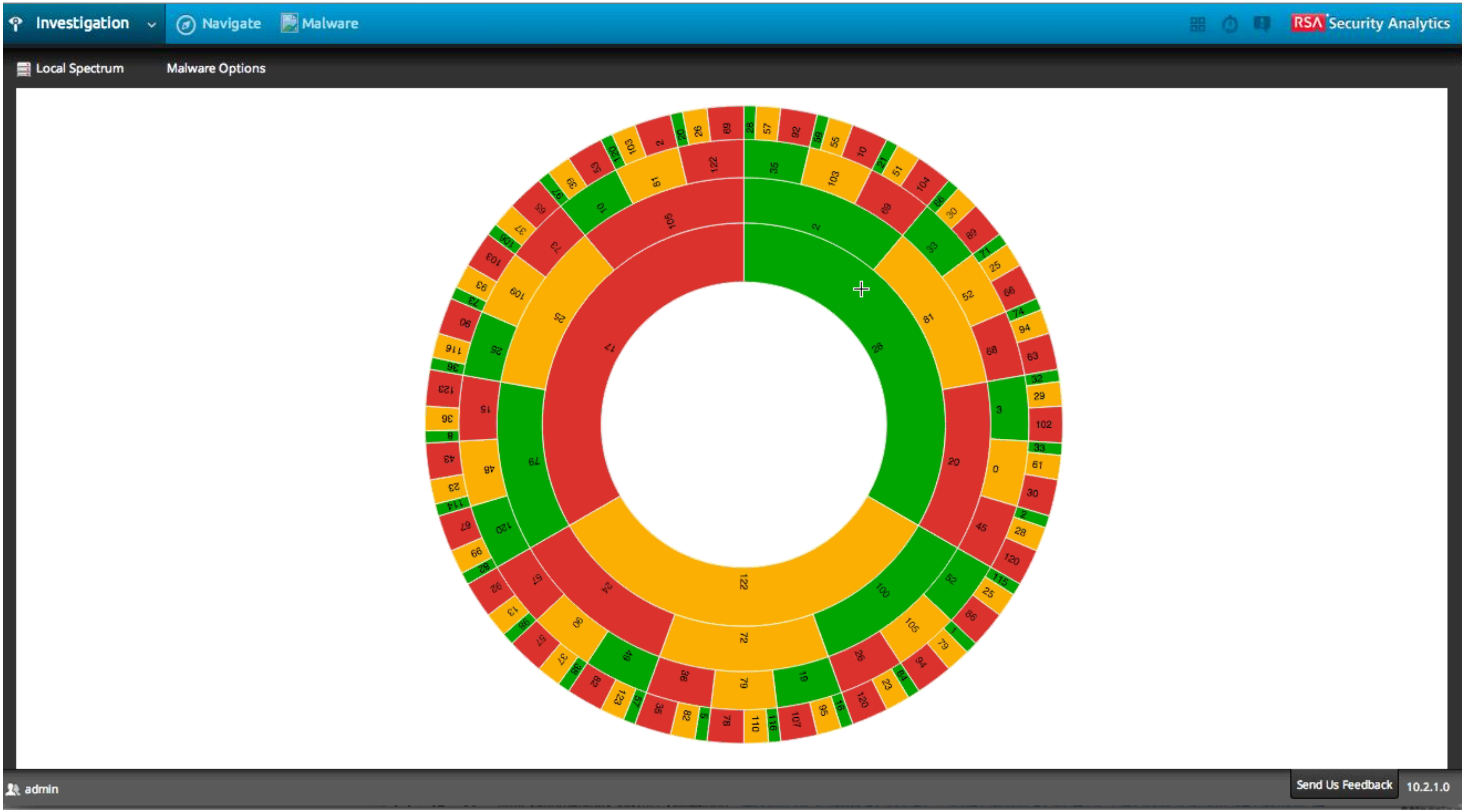
Static (PE) - Checksum: No Checksum Value
CheckSum Value Set to: 0x0

NextGen - Domain: alias.host does not Exist
Destination IP: 85.17.52.47, Protocol: 2048, Port: 80, Service: 80, Alias: , TLD: com, Country: Netherlands

99.87 NextGen Results

Meta Highlights

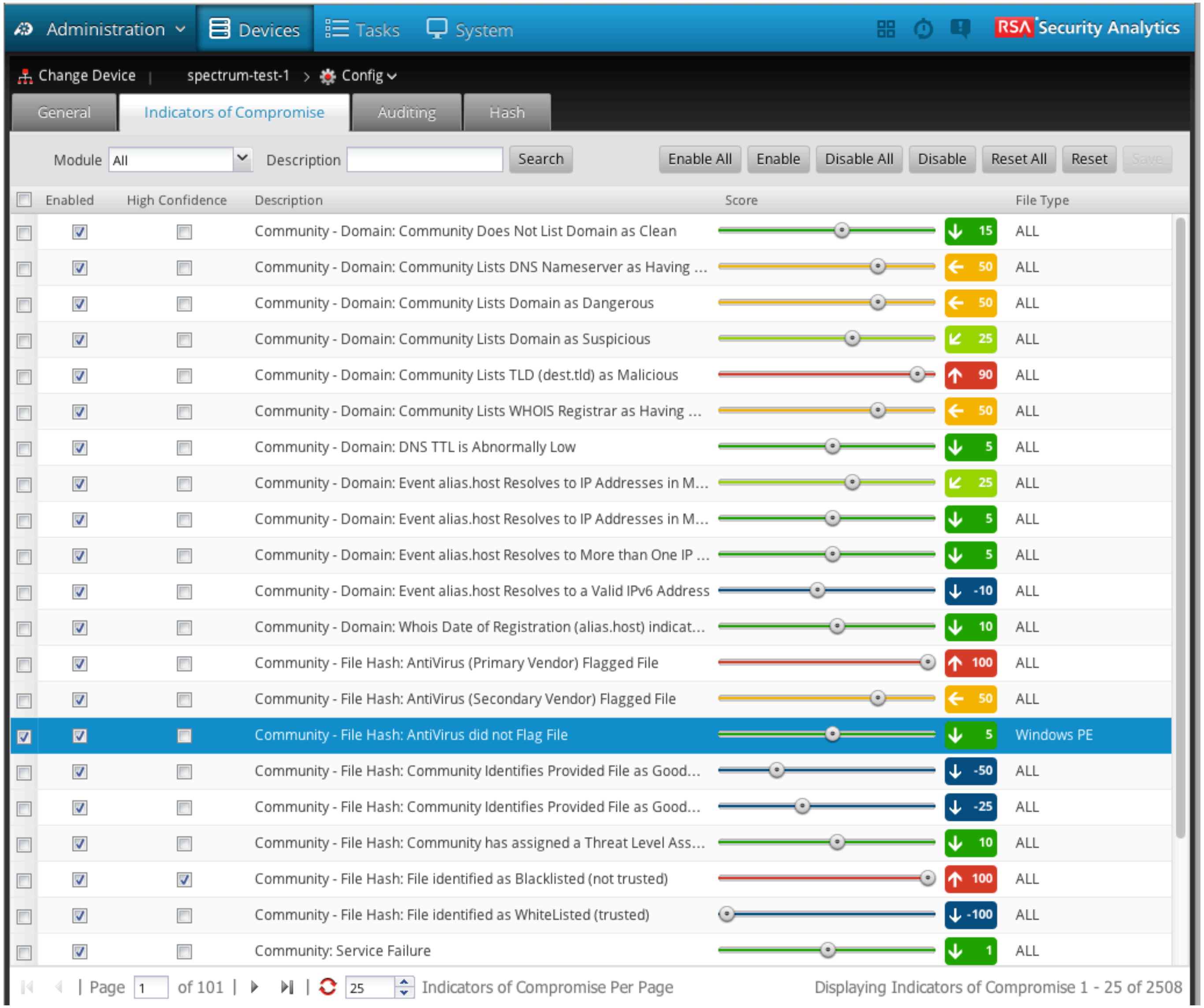
Malware Universe Rating



RSA

EMC²

Malware Scoring



Module: All

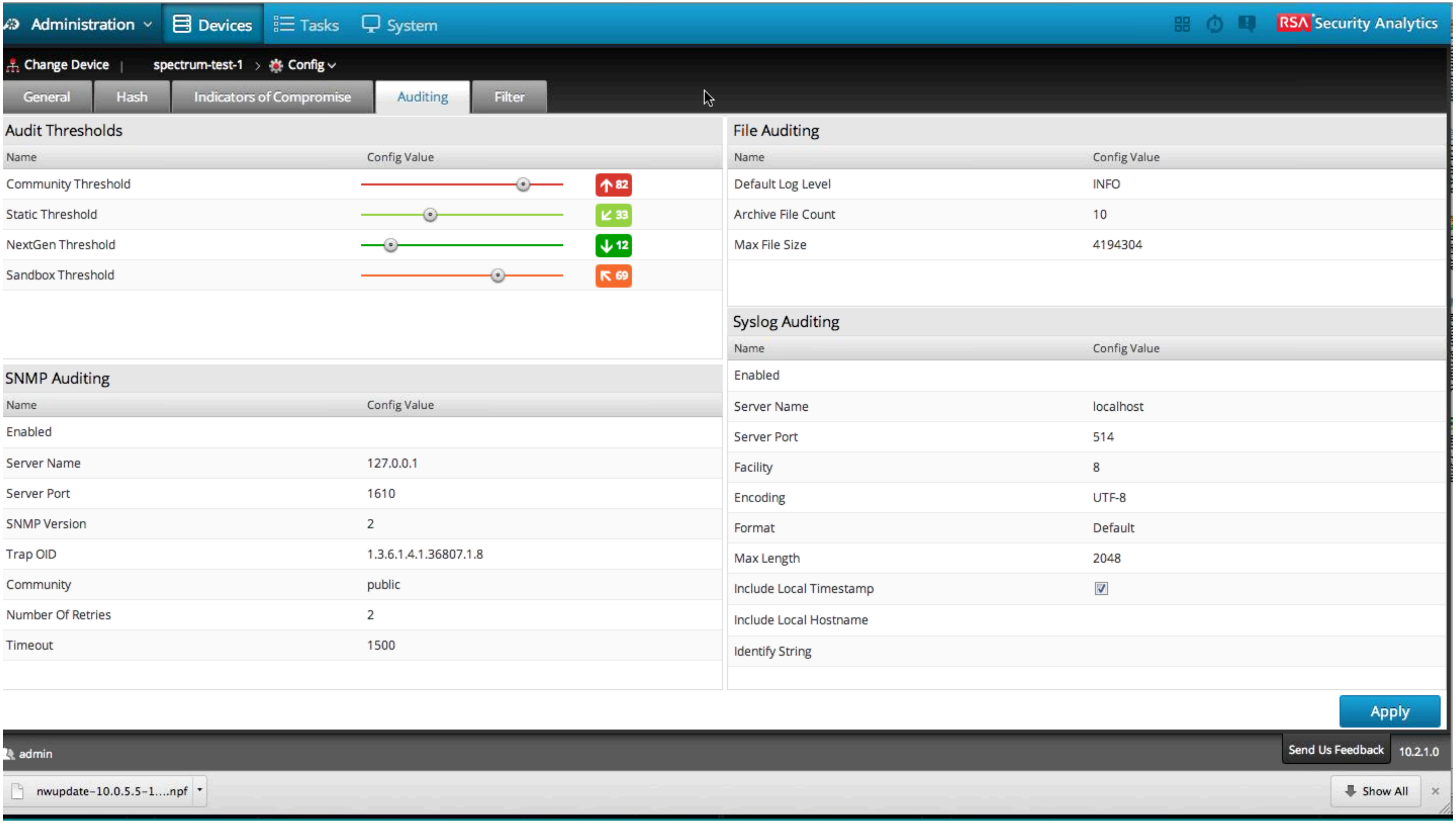
Description:

□	Enabled	High Confidence	Description	Score	File Type
□	☑	□	Community - Domain: Community Does Not List Domain as Clean	↓ 15	ALL
□	☑	□	Community - Domain: Community Lists DNS Nameserver as Having ...	← 50	ALL
□	☑	□	Community - Domain: Community Lists Domain as Dangerous	← 50	ALL
□	☑	□	Community - Domain: Community Lists Domain as Suspicious	↙ 25	ALL
□	☑	□	Community - Domain: Community Lists TLD (dest.tld) as Malicious	↑ 90	ALL
□	☑	□	Community - Domain: Community Lists WHOIS Registrar as Having ...	← 50	ALL
□	☑	□	Community - Domain: DNS TTL is Abnormally Low	↓ 5	ALL
□	☑	□	Community - Domain: Event alias.host Resolves to IP Addresses in M...	↙ 25	ALL
□	☑	□	Community - Domain: Event alias.host Resolves to IP Addresses in M...	↓ 5	ALL
□	☑	□	Community - Domain: Event alias.host Resolves to More than One IP ...	↓ 5	ALL
□	☑	□	Community - Domain: Event alias.host Resolves to a Valid IPv6 Address	↓ -10	ALL
□	☑	□	Community - Domain: Whois Date of Registration (alias.host) indicat...	↓ 10	ALL
□	☑	□	Community - File Hash: AntiVirus (Primary Vendor) Flagged File	↑ 100	ALL
□	☑	□	Community - File Hash: AntiVirus (Secondary Vendor) Flagged File	← 50	ALL
☑	☑	□	Community - File Hash: AntiVirus did not Flag File	↓ 5	Windows PE
□	☑	□	Community - File Hash: Community Identifies Provided File as Good...	↓ -50	ALL
□	☑	□	Community - File Hash: Community Identifies Provided File as Good...	↓ -25	ALL
□	☑	□	Community - File Hash: Community has assigned a Threat Level Ass...	↓ 10	ALL
□	☑	☑	Community - File Hash: File identified as Blacklisted (not trusted)	↑ 100	ALL
□	☑	□	Community - File Hash: File identified as WhiteListed (trusted)	↓ -100	ALL
□	☑	□	Community: Service Failure	↓ 1	ALL

Page 1 of 101 | 25 Indicators of Compromise Per Page

Displaying Indicators of Compromise 1 - 25 of 2508

Malware Configuration - Auditing



Audit Thresholds

Name	Config Value
Community Threshold	82
Static Threshold	33
NextGen Threshold	12
Sandbox Threshold	69

File Auditing

Name	Config Value
Default Log Level	INFO
Archive File Count	10
Max File Size	4194304

SNMP Auditing

Name	Config Value
Enabled	
Server Name	127.0.0.1
Server Port	1610
SNMP Version	2
Trap OID	1.3.6.1.4.1.36807.1.8
Community	public
Number Of Retries	2
Timeout	1500

Syslog Auditing

Name	Config Value
Enabled	
Server Name	localhost
Server Port	514
Facility	8
Encoding	UTF-8
Format	Default
Max Length	2048
Include Local Timestamp	☑
Include Local Hostname	
Identify String	

SA v10.2 Log Collection

Log Collection

- Log Collector
  - Protocols Added (doubled the number of protocols supported from 10.1)
    - SDEE, VMWare, SNMP, remaining File readers including XML file handler
  - Features
    - Live Integration for updating collector content (GOTS\GFTS)

- Remote Log Collector
  - Protocols Added (doubled the number of protocols supported from 10.1)
    - SDEE, VMWare, SNMP, remaining File readers including XML file handler
    - Syslog
  - Features
    - Live Integration for updating collector content (GOTS\GFTS)
    - MSSP RLC Tagging
    - Connection Failover

Log Collection

- Live Integration
  - Log Collector Content (GOTS/GFTS) allows the Log Collector to transform logs from their native format to a one line Syslog format
  - Currently the Log Collector Content is applied via an RPM
  - In 10.2 the user can select the Log Collector Content in Live, subscribe, and deploy it to Log Collectors, whether local to the Log Decoder or Remote (RLC)

Log Collection

- Connection Failover
  - Customers require the ability to continue collection in the event of outages
  - Connection Failover allows the Admin to configure a RLC with multiple Log Collector s to forward logs to under Administration->Devices->RLC->Config->General tab
  - The RLC will forward logs to the Primary (first) Log Collector
  - Should the first Log Collector become unavailable for a configurable amount of time, the RLC will start sending logs to the next configured Log Collector

SA v10.2 Report Engine

SA 10.2 Features – Report Engine

- Live, Static Charting and Dynamic Charting
  - Static Charts in Reports-Supported for all data sources i.e, Warehouse Reporting, NWDB, IPDB.
    - Test Rule supports different chart format
    - Report Definition of report you can change the chart format.
    - In the view of the report change the format of chart
  - Live Charting Dashboard- Supported for NWDB data source
    - You can add any chart rule to dashboard and configure it.
  - Dynamic Charting- Supported for NWDB data source
    - Create chart rule, schedule and view dynamic chart in time and summary series format.
- RBAC
  - Action based Access Control for Rule, Report, Charting, List, Alerting
  - Define roles via Administration→ System→ Security page and define access like Read/Read Write/No Access in Reporting and Alerting modules.
- I18n
  - International charsets content to be supported for all data sources (except IPDB data source) in reporting.
  - International charsets content viewable in report output.

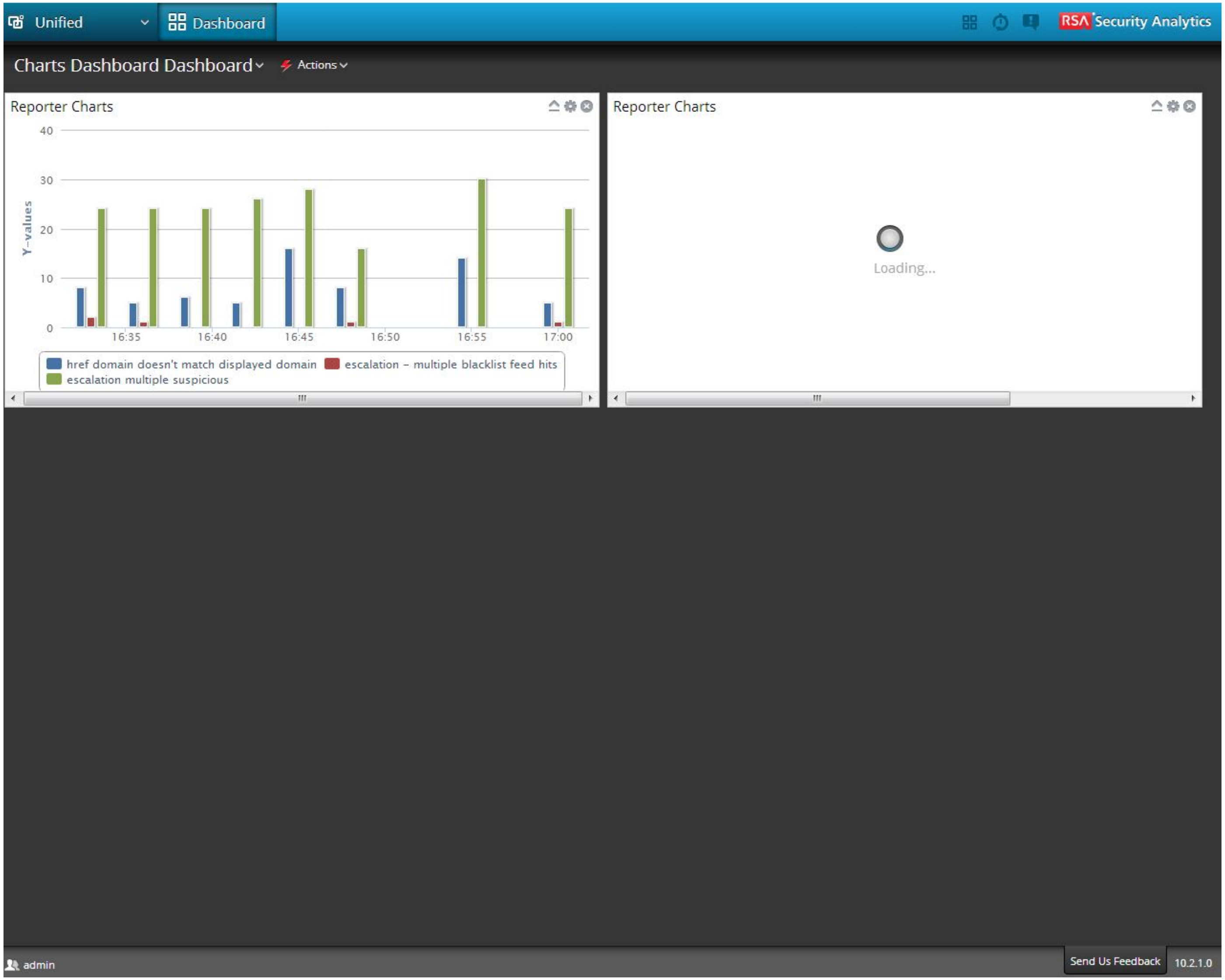
SA 10.2 Features – Report Engine

- Integration with Security Analytics Warehouse
  - Provides Compliance Reporting across large data sets
    - Reports can be scheduled or ad-hoc
  - Report Engine HIVE Query Interfaces
    - Basic HIVE Rule Builder
      - Provides easy to use and familiar interface for basic HIVE queries
      - Consistent user experience as other rule builders
      - Targets compliance use cases
    - Expert HIVE Rule Builder
      - Provides expert mode for advanced HIVE operations
      - Free form HIVE expression support
  - Table support for meta and raw partitions
    - Table space support for meta and raw partitions
    - Allows users to focus on query instead of tedious details behind building HIVE tables across backend partitioning
- IPDB Adapter
  - Support for Multi-Site IPDB. Following deployment scenarios are supported.
    - An OVF that includes a CENTOS6 image with the IPDB Extractor installed.
    - IPDB Extractor RPM that could be installed on any 4S appliance.
    - R710 based image.

SA 10.2 Features – Report Engine

- Enhancements
  - Linking to investigator from alert view page and via alert output actions.
  - Dynamic list will let you direct the output of report to a list. Configuring dynamic list lets you option to overwrite or append to an existing list.
  - Alert variance dashlet added in dashboard.
  - In all the alert dashlet in the dashboard, you can change the time range.
  - Engine supports new font packages (Latin American Spanish, Arabic, Japanese, French)
  - Click on the test rule meta to link to investigator
  - User would be able to view the report even if one or more rule fails with appropriate error messages in report.
  - Support different data sources rule in single report.
  - Different icons for different data sources rule.
  - For some of the meta there are alias defined and support of the same in the output of the report by default for all the data sources.
  - Support for eagle product via reporting. Basically data source decoder/log decoder can be selected via reporting.

Reporting – Dashboard Charts



Reporting – Pie Chart Time Series

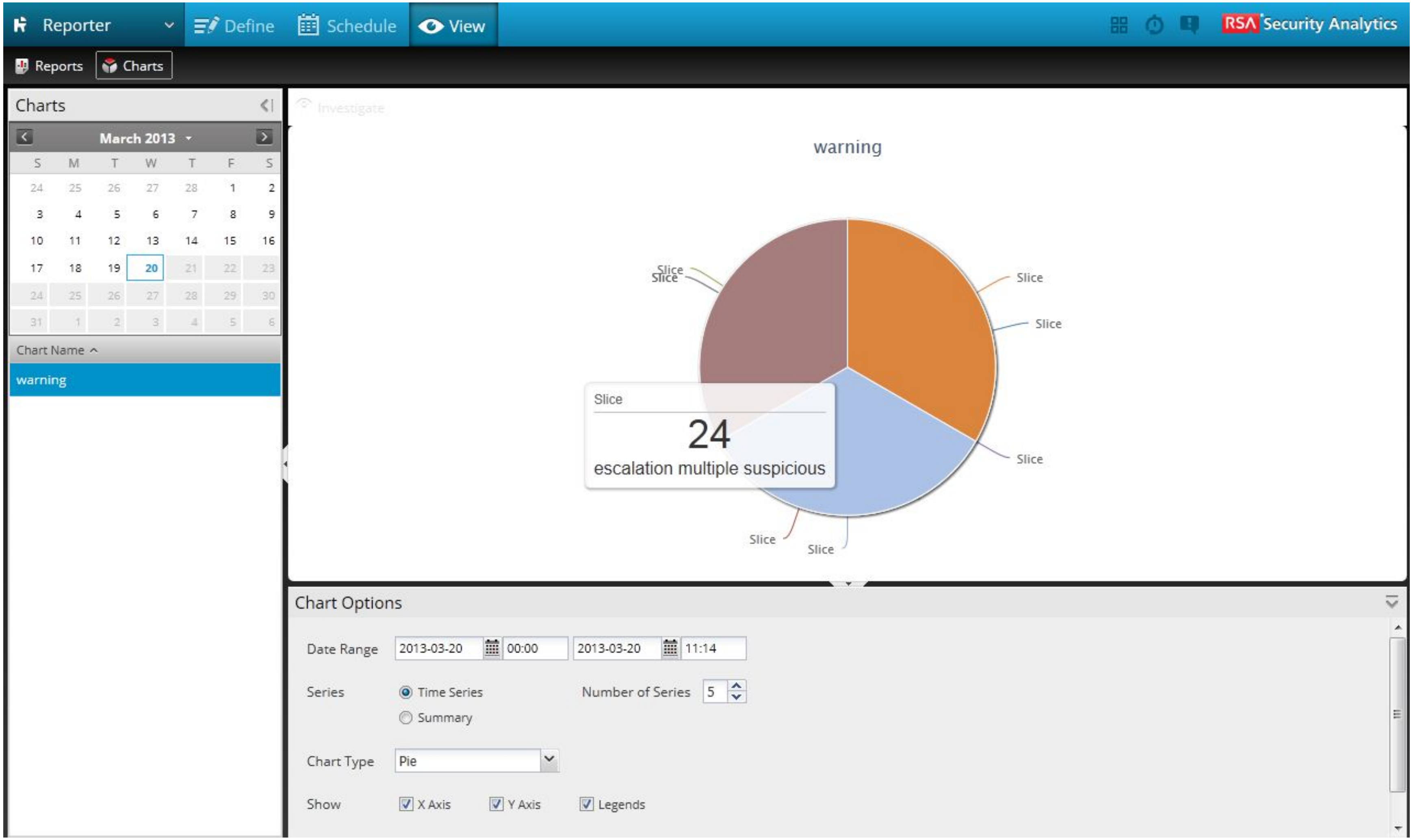


Chart Options

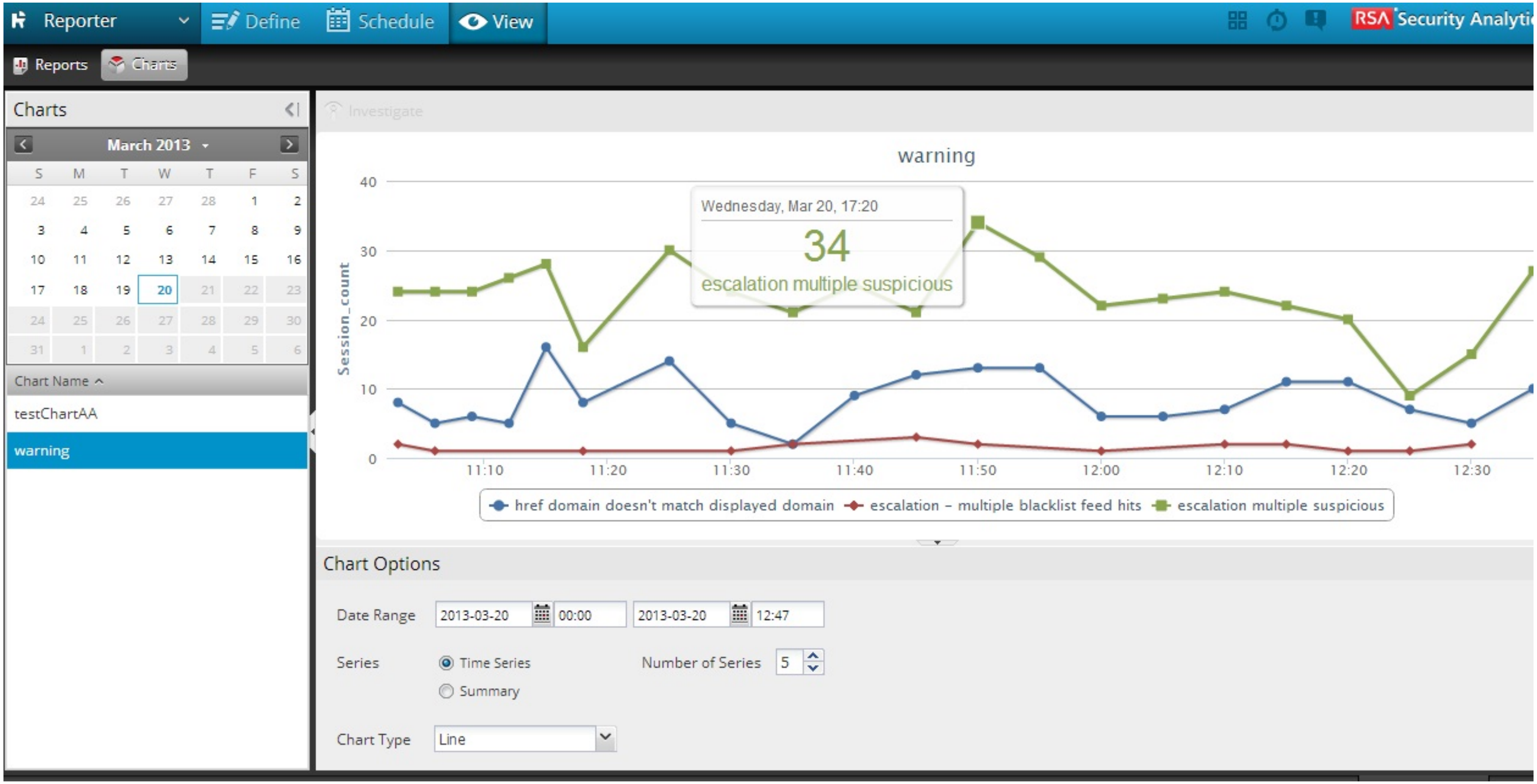
Date Range 2013-03-20 00:00 2013-03-20 11:14

Series ● Time Series ○ Summary Number of Series 5

Chart Type Pie

Show ☑ X Axis ☑ Y Axis ☑ Legends

Reporting – Dynamic Line Time Series



March 2013

S	M	T	W	T	F	S
24	25	26	27	28	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Chart Name

- testChartAA
- warning

Chart Options

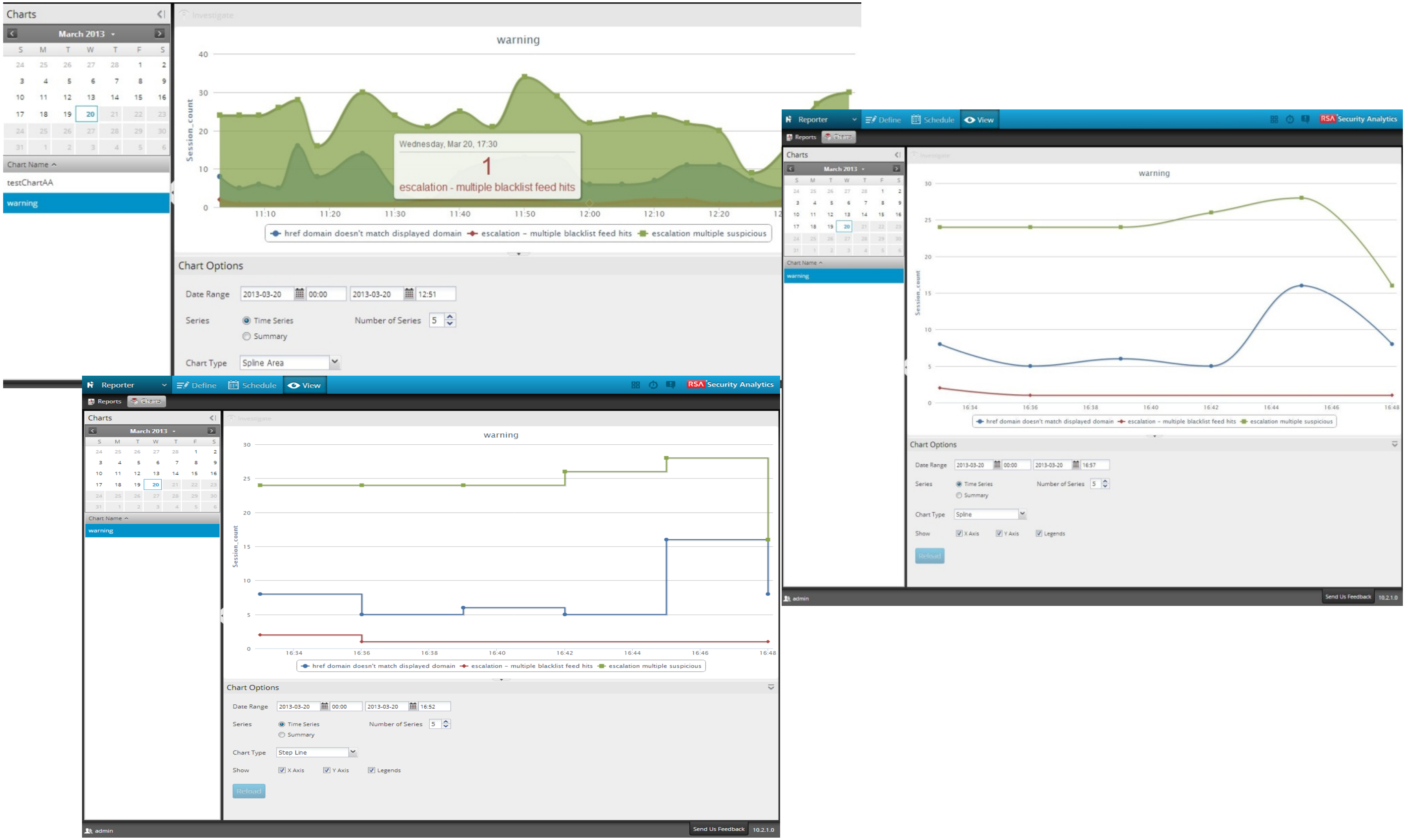
Date Range: 2013-03-20 00:00 – 2013-03-20 12:47

Series: ● Time Series ○ Summary

Number of Series: 5

Chart Type: Line

Reporting – Dynamic Time Series



Wednesday, Mar 20, 17:30
1
escalation - multiple blacklist feed hits

Chart Options

Date Range 2013-03-20 00:00 2013-03-20 12:51

Series ● Time Series ○ Summary Number of Series 5

Chart Type Spline Area

Chart Options

Date Range 2013-03-20 00:00 2013-03-20 16:52

Series ● Time Series ○ Summary Number of Series 5

Chart Type Step Line

Show ☑ X Axis ☑ Y Axis ☑ Legends

Reload

Chart Options

Date Range 2013-03-20 00:00 2013-03-20 16:57

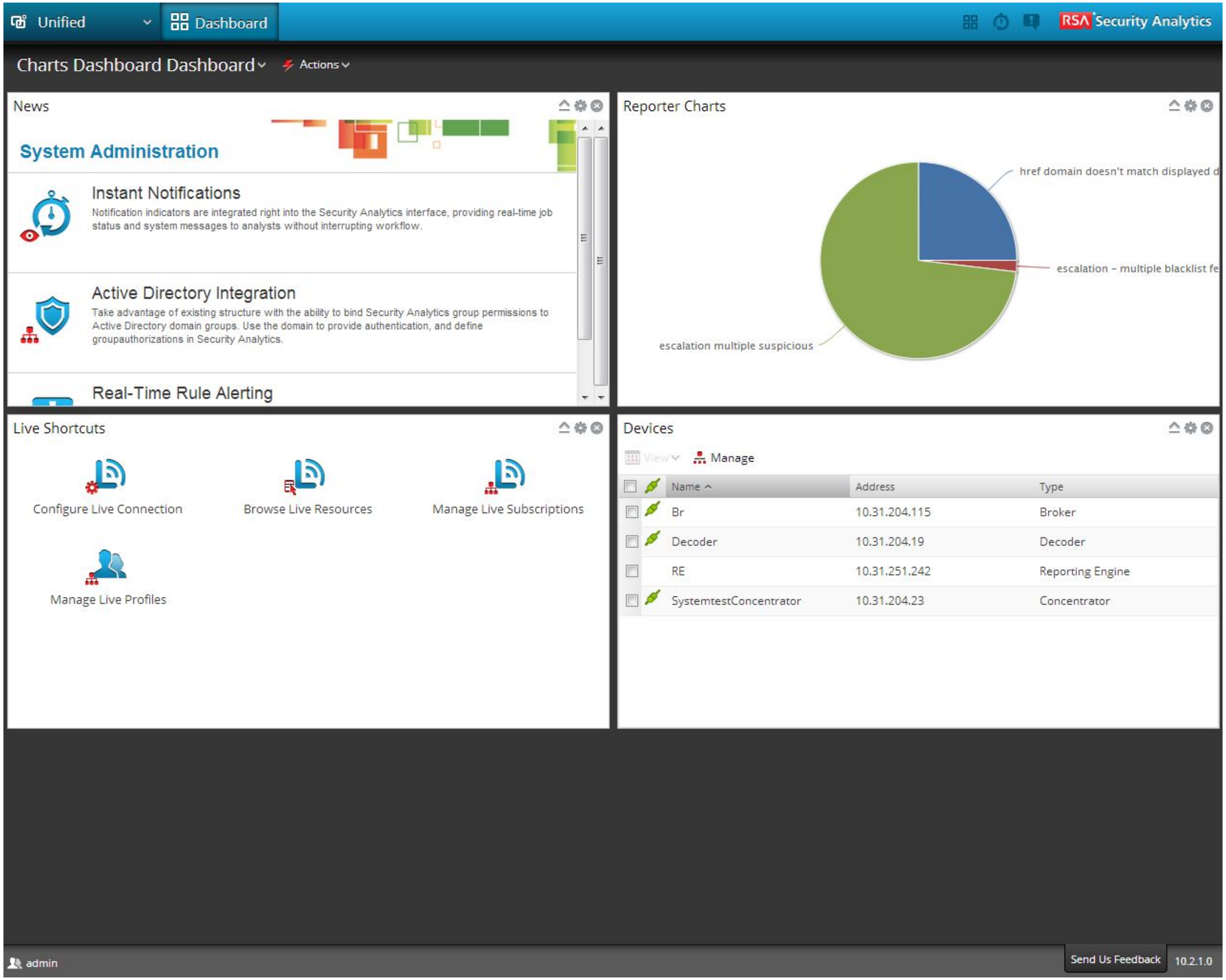
Series ● Time Series ○ Summary Number of Series 5

Chart Type Spline

Show ☑ X Axis ☑ Y Axis ☑ Legends

Reload

Reporting – Live Pie Chart Dashlet


Unified
Dashboard
RSA Security Analytics
Charts Dashboard Dashboard
Actions
News
Reporter Charts
href domain doesn't match displayed d
escalation – multiple blacklist fe
escalation multiple suspicious
Live Shortcuts
Configure Live Connection
Browse Live Resources
Manage Live Subscriptions
Manage Live Profiles
Devices
View
Manage
admin
Send Us Feedback
10.2.1.0

System Administration

Instant Notifications

Notification indicators are integrated right into the Security Analytics interface, providing real-time job status and system messages to analysts without interrupting workflow.

Active Directory Integration

Take advantage of existing structure with the ability to bind Security Analytics group permissions to Active Directory domain groups. Use the domain to provide authentication, and define groupauthorizations in Security Analytics.

Real-Time Rule Alerting

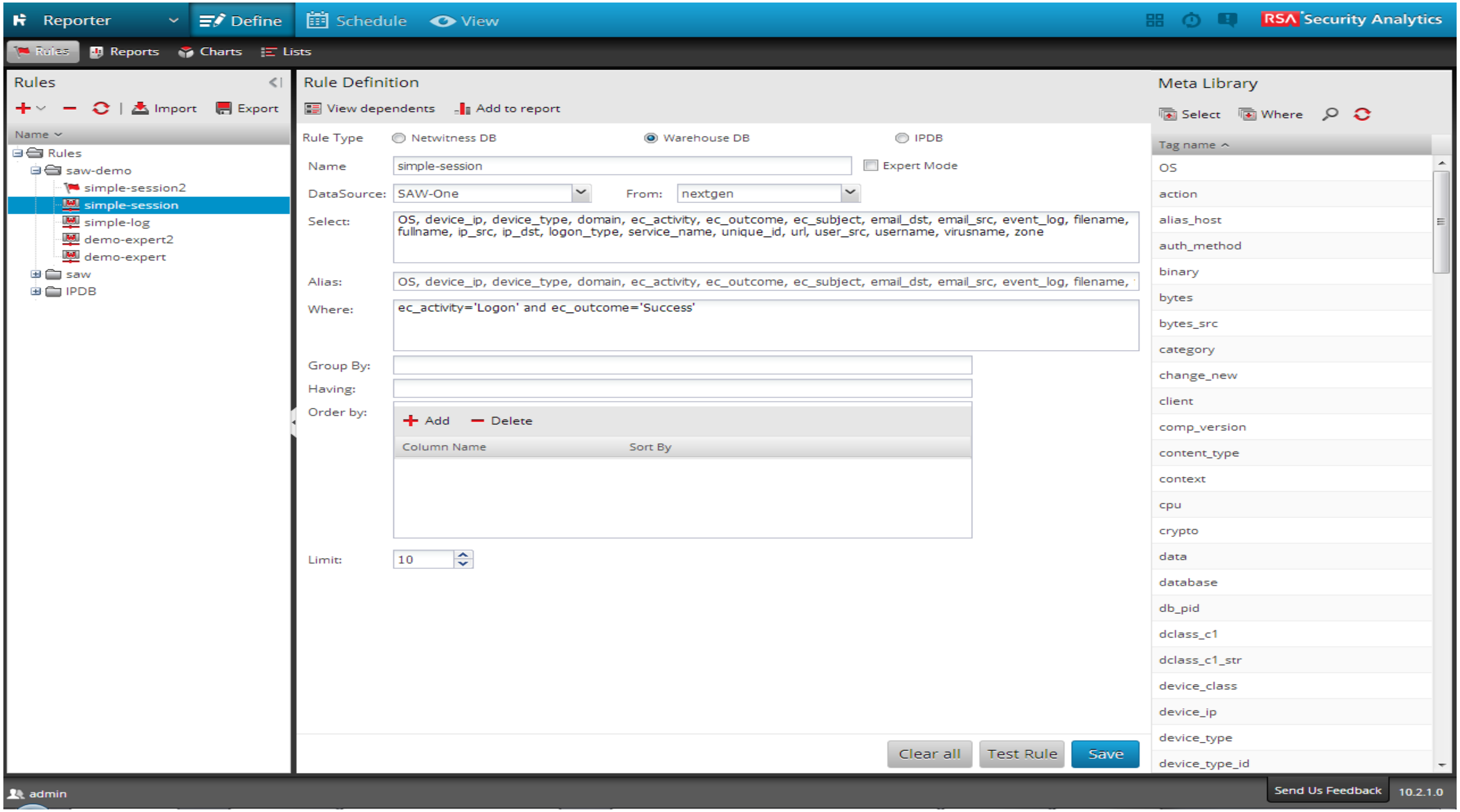
Name	Address	Type
Br	10.31.204.115	Broker
Decoder	10.31.204.19	Decoder
RE	10.31.251.242	Reporting Engine
SystemtestConcentrator	10.31.204.23	Concentrator

SA v10.2 SAW

Analytics Warehouse

- RAW Logs and Meta Namespaces
  - RAW log data partition stored and accessible via “logs” table space, allows analytics on RAW logs via HIVE %LIKE% and RegEx expressions
  - META partition stored and accessible via “session”, this includes both log and packet meta
- Integration with Report Engine for Compliance Use Cases
  - Both “session” and “logs” namespaces accessible via HIVE rule builder
  - Reporting Content for common SIEM use cases
  - Complexities of internal partition management abstracted from user experience
  - Reports can be scheduled or ad-hoc
- SWFT Agent
  - Provides Non-NFS data movement between Decoders\Concentrators to SAW
- Various HDFS Enhancements and Bug Fixes
  - Enhancements
    - Need list
  - Bug Fixes
    - Need list

Analytics Warehouse Reporting



Rule Type ○ Netwitness DB ● Warehouse DB ○ IPDB

Name: simple-session □ Expert Mode

DataSource: SAW-One From: nextgen

Select: OS, device_ip, device_type, domain, ec_activity, ec_outcome, ec_subject, email_dst, email_src, event_log, filename, fullname, ip_src, ip_dst, logon_type, service_name, unique_id, url, user_src, username, virusname, zone

Alias: OS, device_ip, device_type, domain, ec_activity, ec_outcome, ec_subject, email_dst, email_src, event_log, filename,

Where: ec_activity='Logon' and ec_outcome='Success'

Group By:

Having:

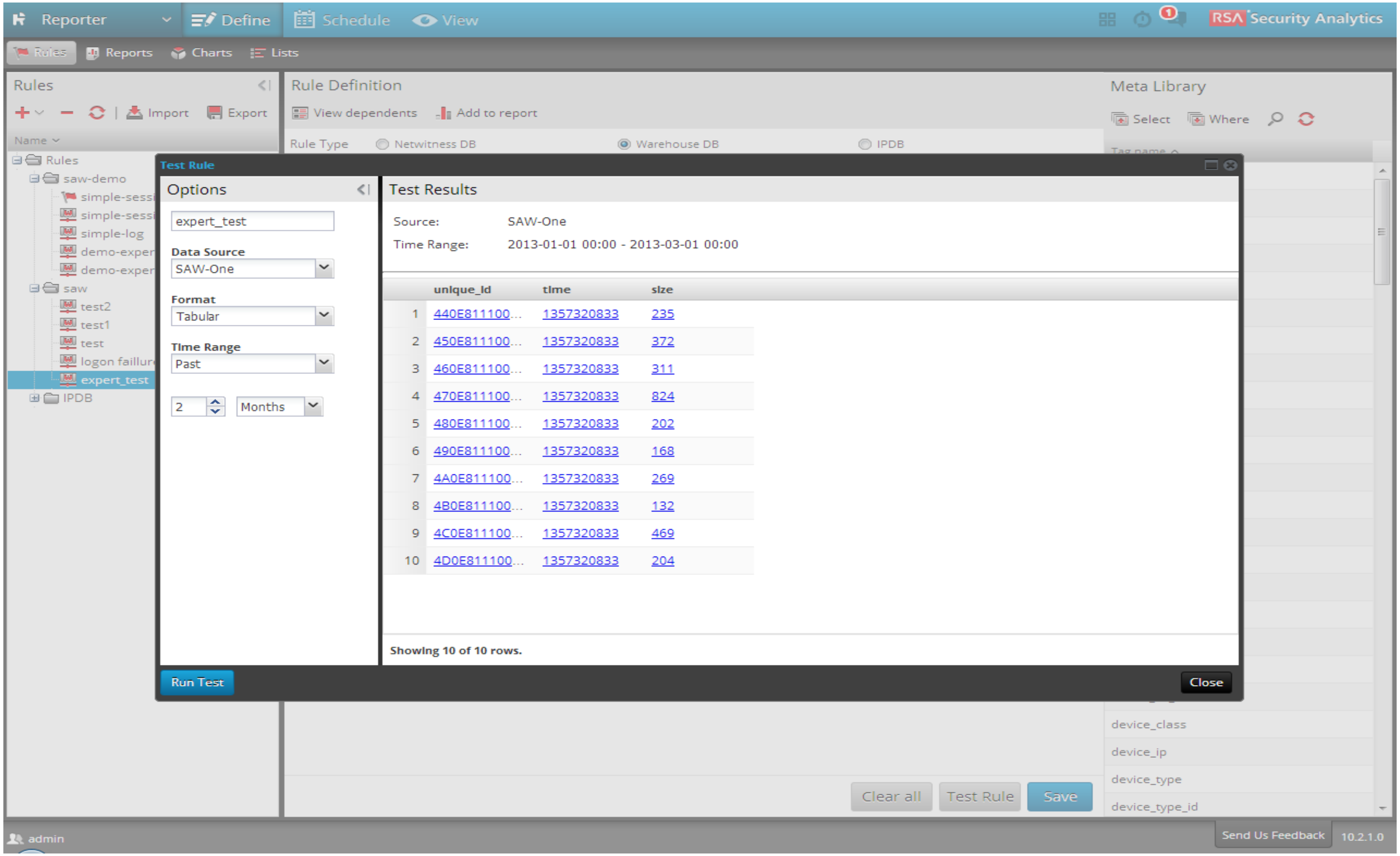
Order by:

Column Name	Sort By

Limit: 10

*** Preliminary lab results, with one simple rule and unconstrained I/O

Analytics Warehouse Reporting



Rule Type ○ Netwitness DB ● Warehouse DB ○ IPDB

Test Rule

Options

expert_test

Data Source
SAW-One

Format
Tabular

Time Range
Past

2 Months

Test Results

Source: SAW-One
Time Range: 2013-01-01 00:00 - 2013-03-01 00:00

	unique_id	time	size
1	440E811100...	1357320833	235
2	450E811100...	1357320833	372
3	460E811100...	1357320833	311
4	470E811100...	1357320833	824
5	480E811100...	1357320833	202
6	490E811100...	1357320833	168
7	4A0E811100...	1357320833	269
8	4B0E811100...	1357320833	132
9	4C0E811100...	1357320833	469
10	4D0E811100...	1357320833	204

Showing 10 of 10 rows.

Run Test

Close

*** Preliminary lab results, with one simple rule and unconstrained I/O

SA v10.2 Complex Event Processing

CEP

Capabilities

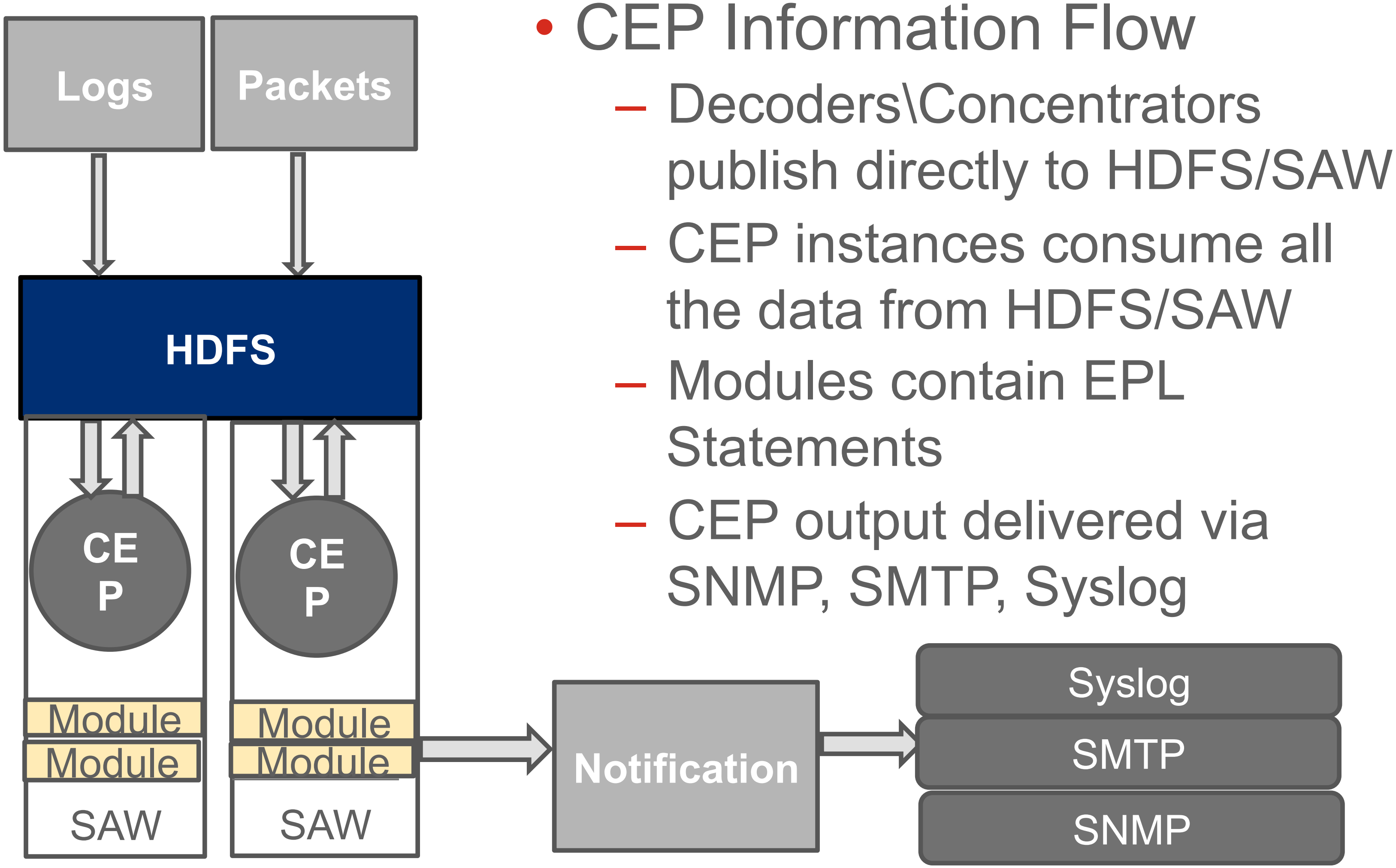
- Core functions:
  - Correlate data arriving in multiple streams
  - Correlate data that arrives out of order
  - Logical and temporal causality (followed-by)
  - Filter Events
  - Alert Suppression
  - Compute percentages or ratios
  - Average, count, min and max
  - Regex support
- Leverages proven CEP technology from the business automation and finance markets

Differentiators

- Logs + Pkt Meta + Enrichment Data (Intel, Vuln, Asset, Identity)
- Scale & Performance
  - 6 SAW compute nodes can correlate 4.5 Billion EPS … and scale up***
- Nested & Dependent Correlations
- Historical/Retro-Active Processing
- Complexity & Scope of Processing
  - Sliding windows, tumbling windows, named windows, combine windows, window sharing, shrinking/expanding windows
  - Grouping, aggregations, sort, filter, merge, upsert, split, inner-joins
  - Rate limiting, enumeration methods, context dimensions
  - Etc…

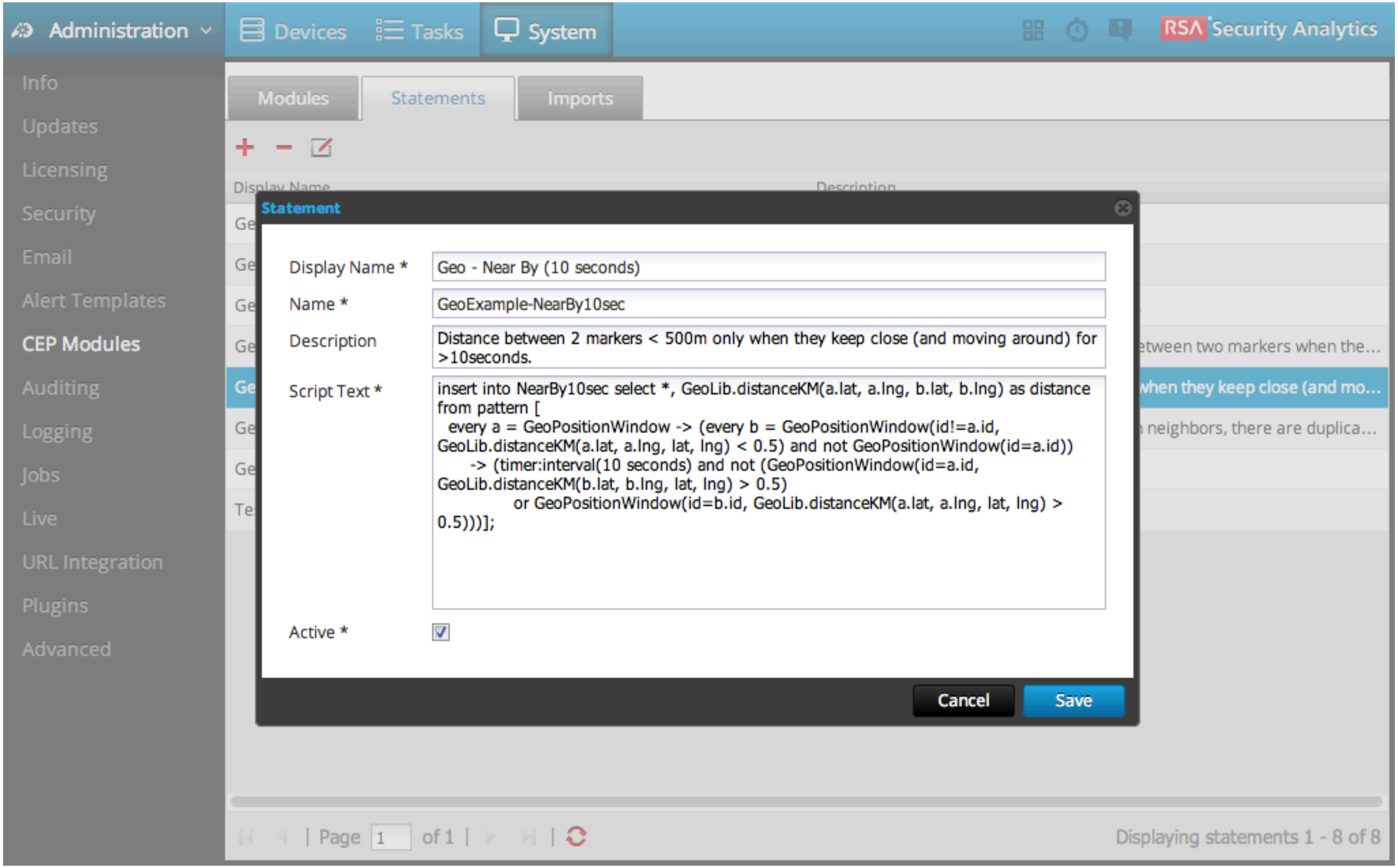
*** Preliminary lab results, with one simple rule and unconstrained I/O

Complex Event Processing



- CEP Information Flow
  - Decoders\Concentrators publish directly to HDFS/SAW
  - CEP instances consume all the data from HDFS/SAW
  - Modules contain EPL Statements
  - CEP output delivered via SNMP, SMTP, Syslog

CEP Statements Configuration



Display Name * Geo - Near By (10 seconds)

Name * GeoExample-NearBy10sec

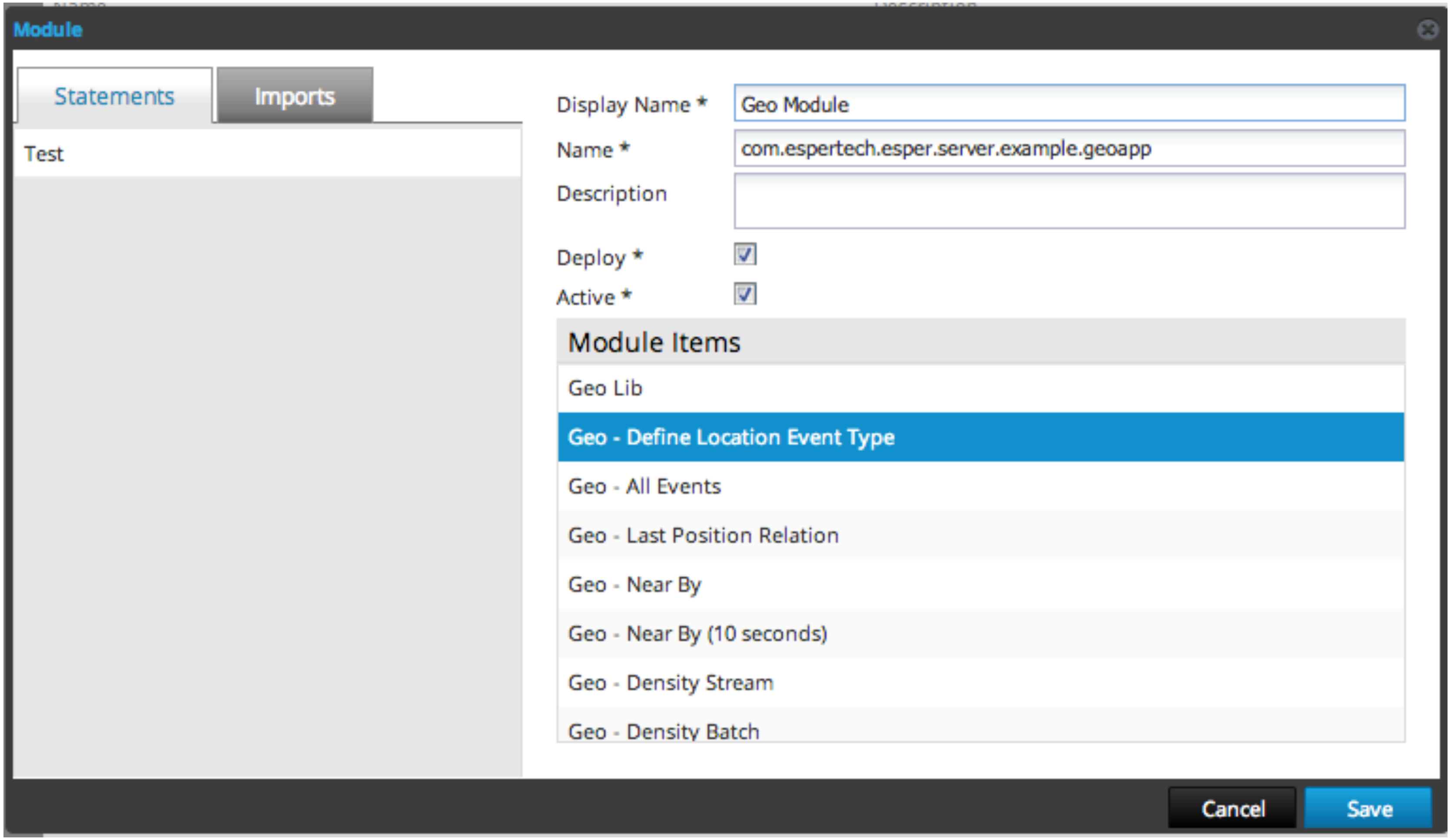
Description Distance between 2 markers < 500m only when they keep close (and moving around) for >10seconds.

Script Text *

```
insert into NearBy10sec select *, GeoLib.distanceKM(a.lat, a.lng, b.lat, b.lng) as distance
from pattern [
  every a = GeoPositionWindow -> (every b = GeoPositionWindow(id!=a.id,
GeoLib.distanceKM(a.lat, a.lng, lat, lng) < 0.5) and not GeoPositionWindow(id=a.id))
      -> (timer:interval(10 seconds) and not (GeoPositionWindow(id=a.id,
GeoLib.distanceKM(b.lat, b.lng, lat, lng) > 0.5)
              or GeoPositionWindow(id=b.id, GeoLib.distanceKM(a.lat, a.lng, lat, lng) >
0.5)))];
```

Active * ☑

CEP Module Configuration



Display Name * Geo Module

Name * com.espertech.esper.server.example.geoapp

Description

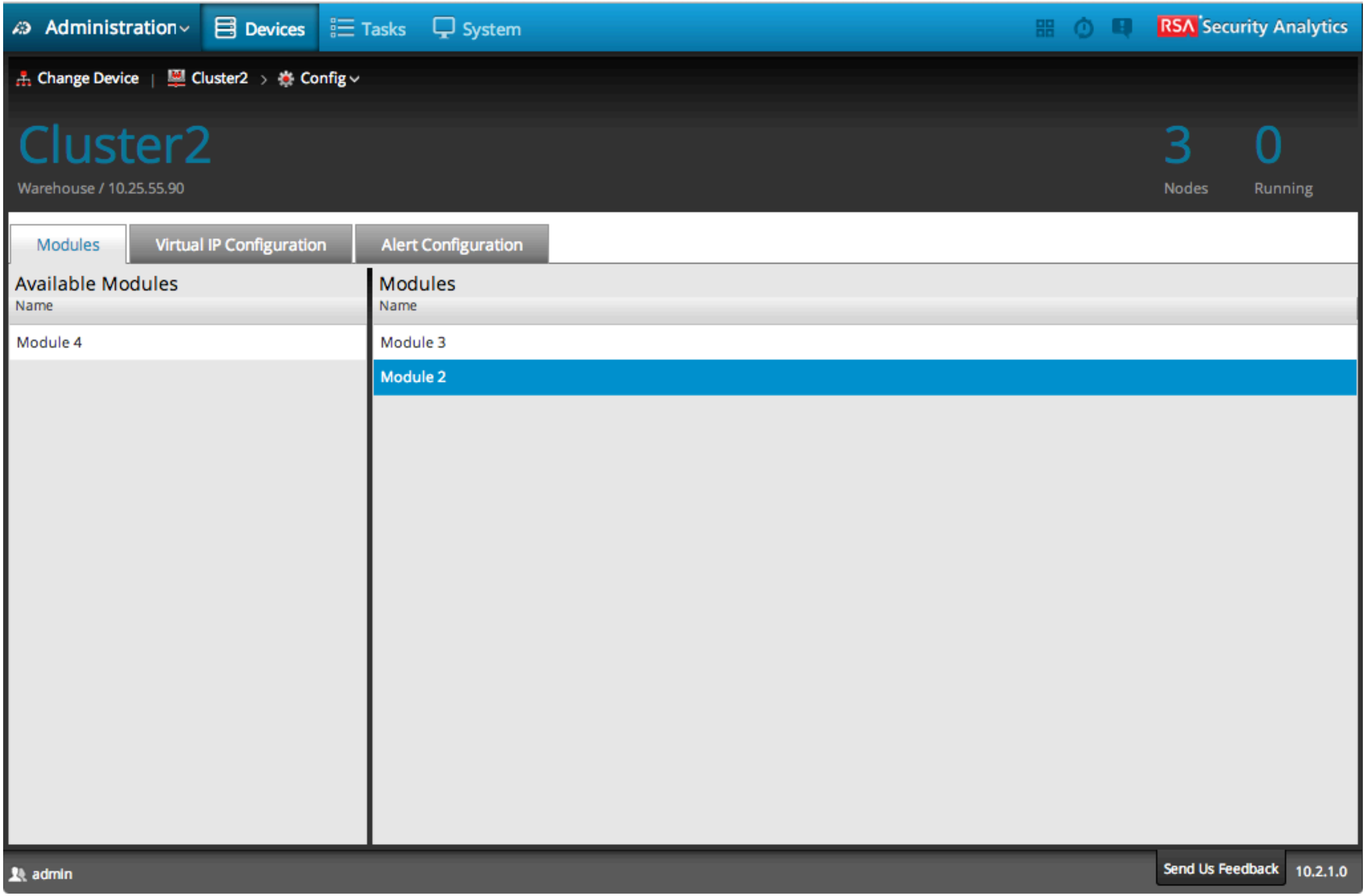
Deploy * ☑

Active * ☑

Module Items

- Geo Lib
- Geo - Define Location Event Type
- Geo - All Events
- Geo - Last Position Relation
- Geo - Near By
- Geo - Near By (10 seconds)
- Geo - Density Stream
- Geo - Density Batch

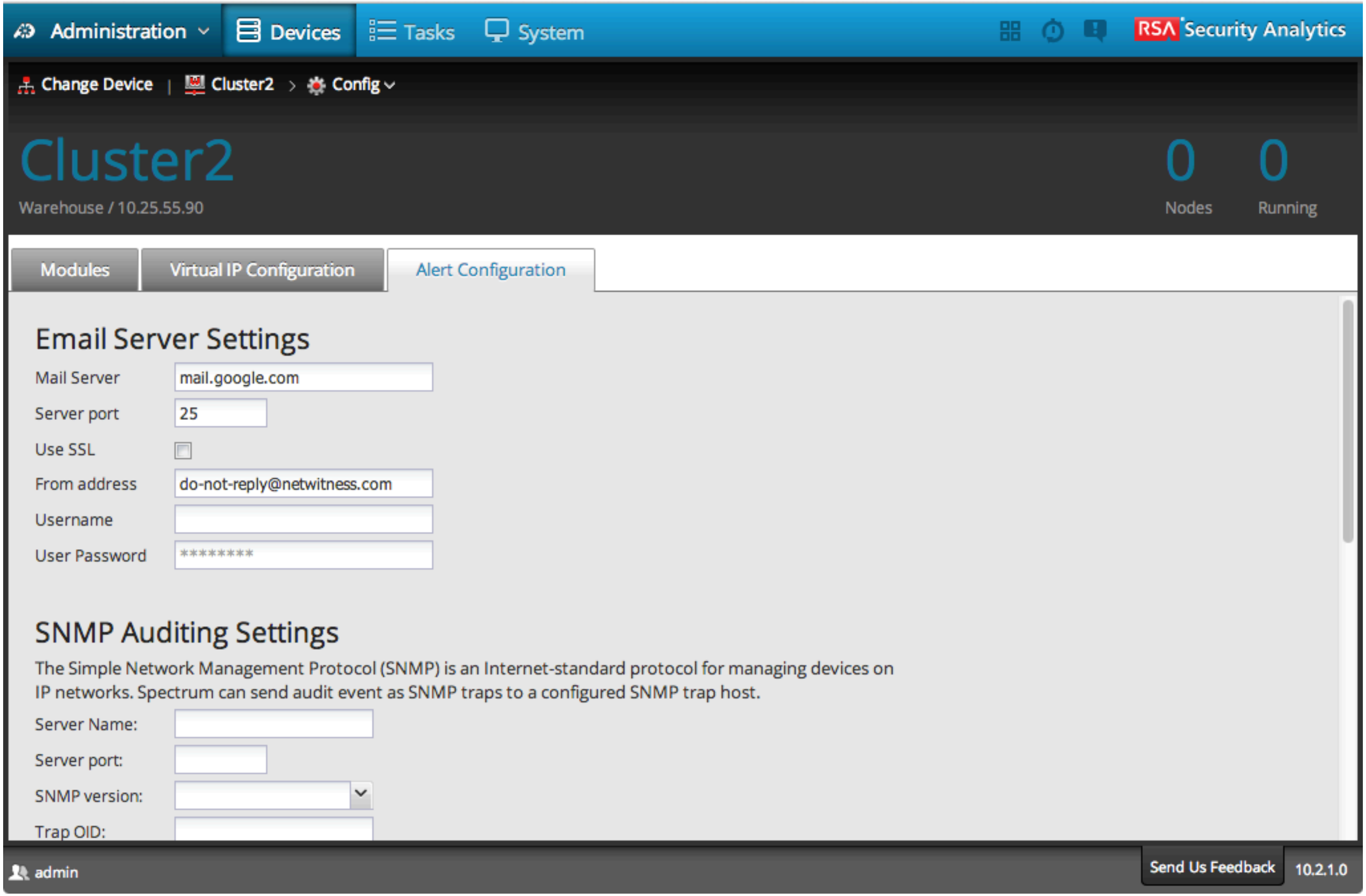
CEP Module Selection



Available Modules
Name
Module 4

Modules
Name
Module 3
Module 2

CEP Alerts Configuration



Cluster2

Warehouse / 10.25.55.90

0 Nodes

0 Running

Email Server Settings

Mail Server	mail.google.com
Server port	25
Use SSL	□
From address	do-not-reply@netwitness.com
Username	
User Password	********

SNMP Auditing Settings

The Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. Spectrum can send audit event as SNMP traps to a configured SNMP trap host.

Server Name:	
Server port:	
SNMP version:	
Trap OID:	

SA v10.2 Content

SA 10.2 Features – Content

- SAW Compliance Reports
  - Delivery via the Compliance Report Template
    - Includes 38 template reports
    - Covers NWDB, and Warehouse DB
    - IPDB not supported
  - Available via Live post 10.2 GA

- Complex Event Processing Examples
  - Cover typical SIEM use cases
    - Focus on log use cases
    - Provides examples for compliance
  - Advanced analytic content not targeted for 10.2

- Defined Chart Types included in Report Packages
  - Report Packages are pre-bundled sets of reports and charts
  - Report Packages delivered for specific problem domains, such as Compliance Reports, Insider Activity, Bittorent, etc…

Protocol Parsers – Lua

- Lua advantages
  - Faster
  - Greater functionality
  - Replace binary parsers, greater flexibility
- 10.2 decoders have Lua support enabled by default
- A user can run ***both*** Flex and Lua parsers simultaneously on a single decoder
- End goal is to transition entire Flex library to Lua
- As users add new Lua content, they will have to unsubscribe/remove it's flex counterpart or they will generate duplicate meta and expend unnecessary system resources