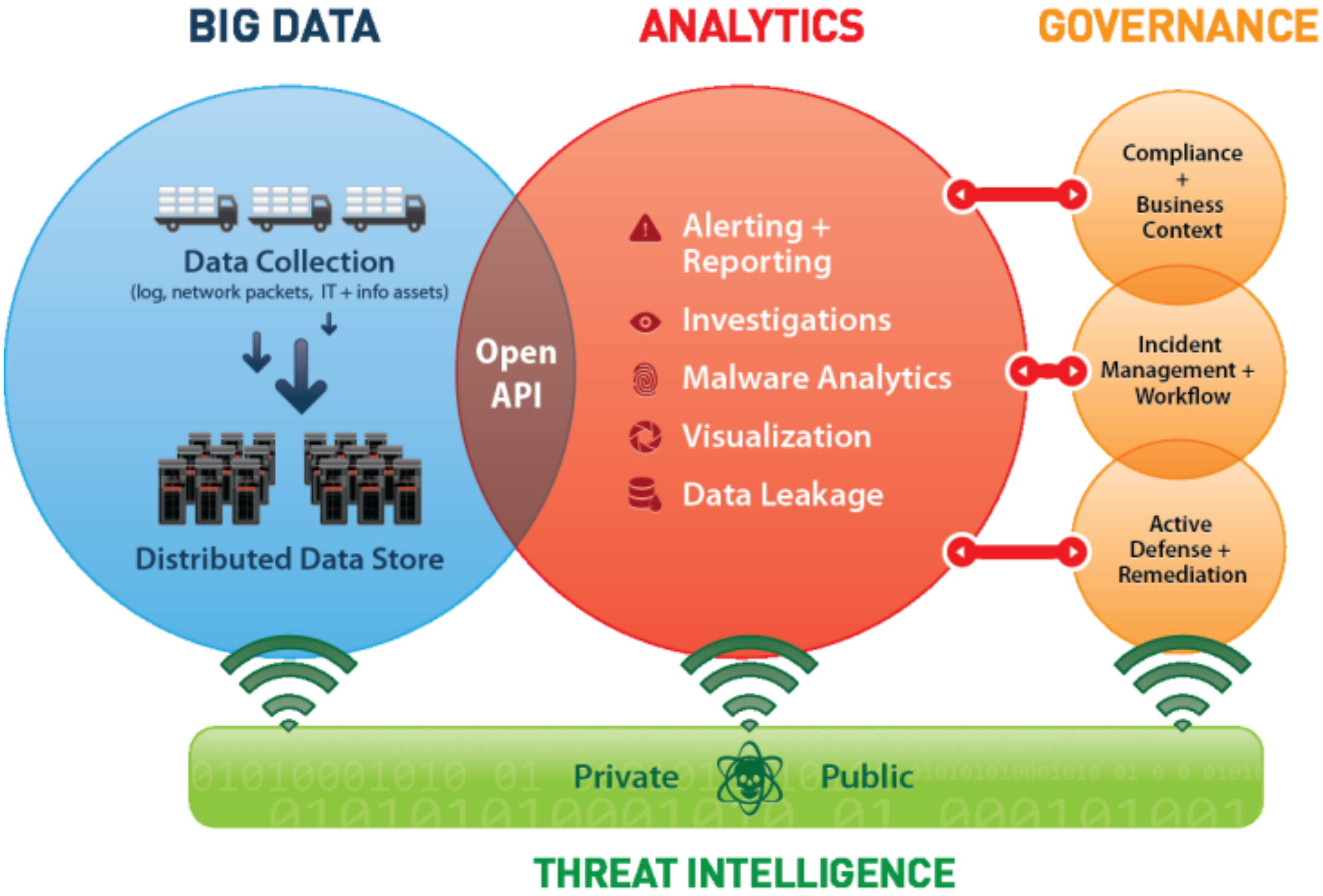
RSA® Security Analytics

Bernard Montel
Directeur Technique RSA

RSA Security Management Compliance Vision

Delivering Visibility, Intelligence and Governance



Traditional Security Is Not Working

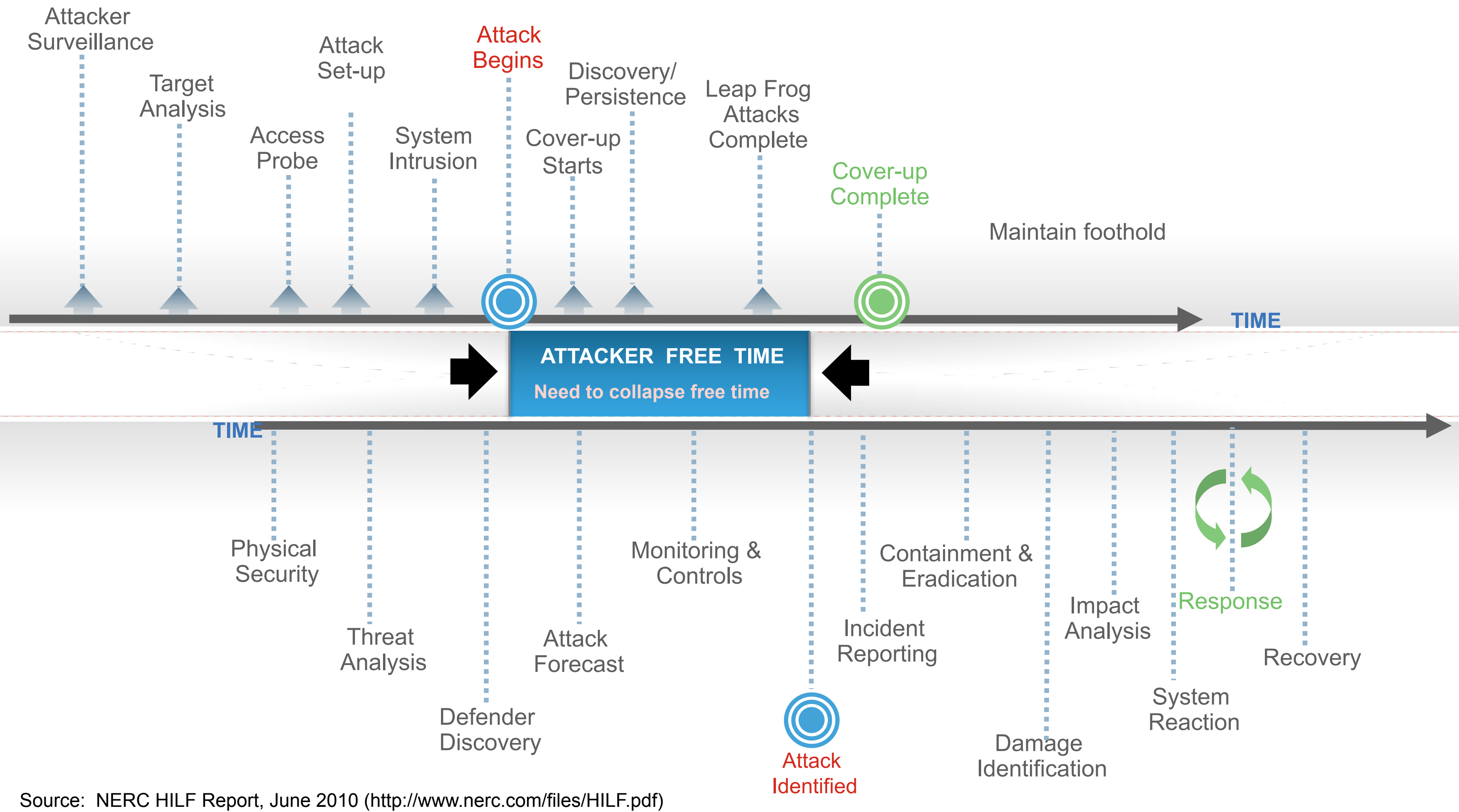
99% of breaches led to compromise within "days" or less with 85% leading to data exfiltration in the same time

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
		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			

85% of breaches took "weeks" or more to discover

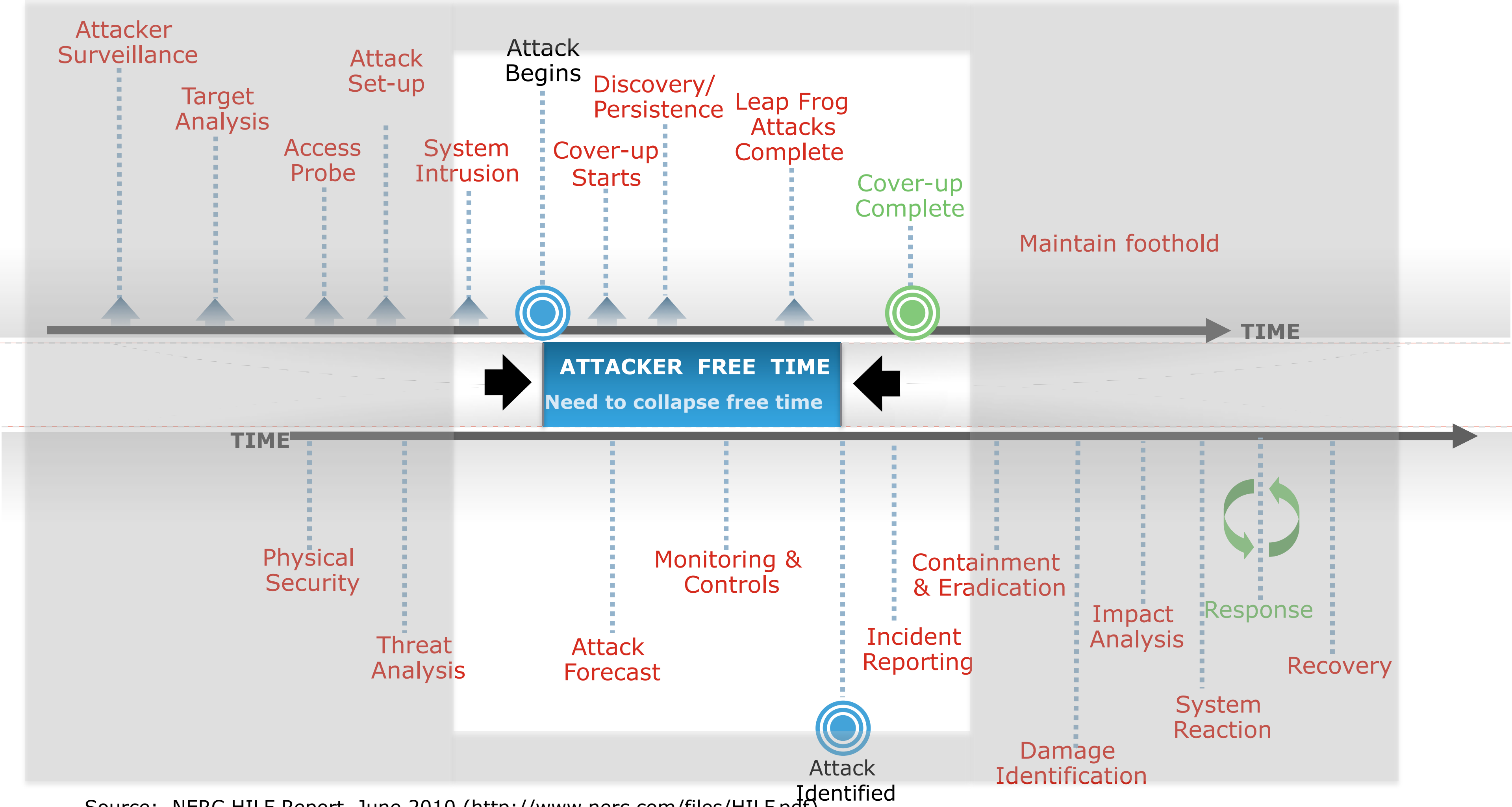
Source: Verizon 2012 Data Breach Investigations Report

Reducing Attacker Free Time



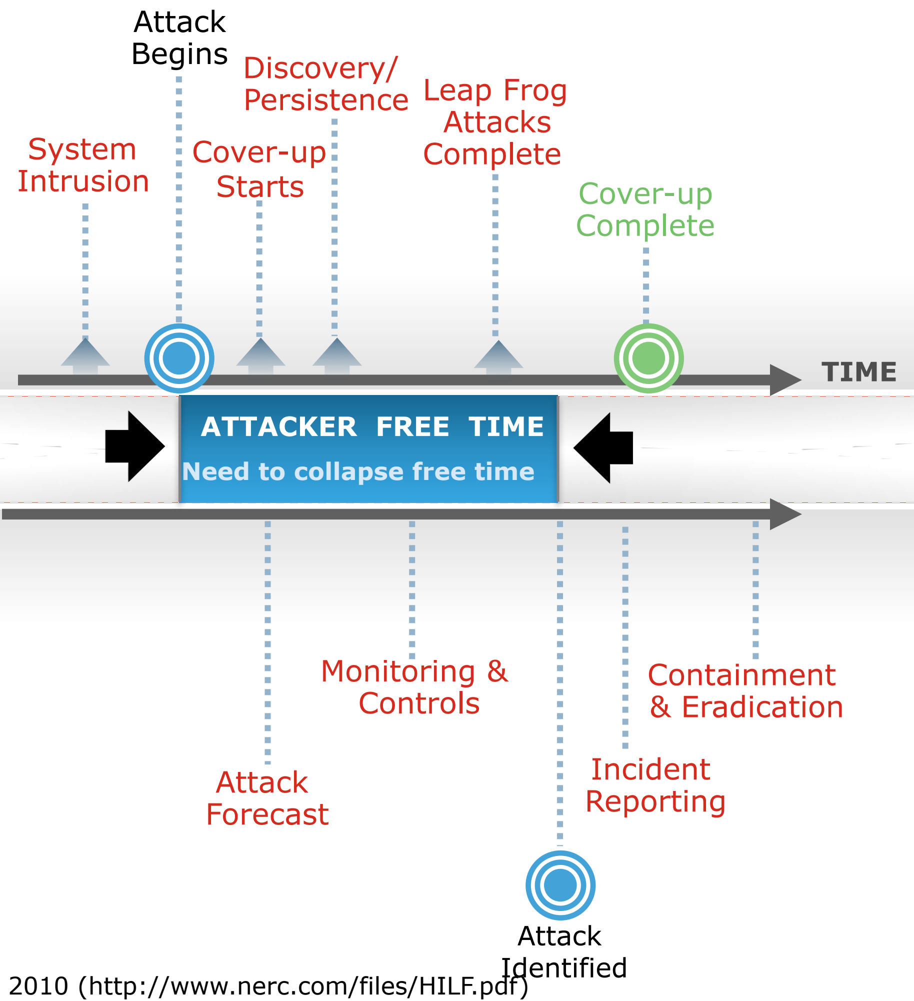
Source: NERC HILF Report, June 2010 (http://www.nerc.com/files/HILF.pdf)

Reducing Attacker Free Time



Source: NERC HILF Report, June 2010 (http://www.nerc.com/files/HILF.pdf)

Reducing Attacker Free Time



Source: NERC HILF Report, June 2010 (http://www.nerc.com/files/HILF.pdf)

Security Is Becoming A Big Data Problem

- More determined adversary means more data needed to identify attacks
- More complex IT environment means even simple attacks can hide in plain sight
- Security professionals are struggling to keep up[1]
  - 40% of all survey respondents are overwhelmed with the security data they already collect
  - 35% have insufficient time or expertise to analyze what they collect

[1] EMA, The Rise of Data-Driven Security, Crawford, Aug 2012
Sample Size = 200

Today’s Security Requirements

Big Data Infrastructure

“Need a fast and scalable infrastructure to conduct short term and long term analysis”

Comprehensive Visibility

“See everything happening in my environment and normalize it”

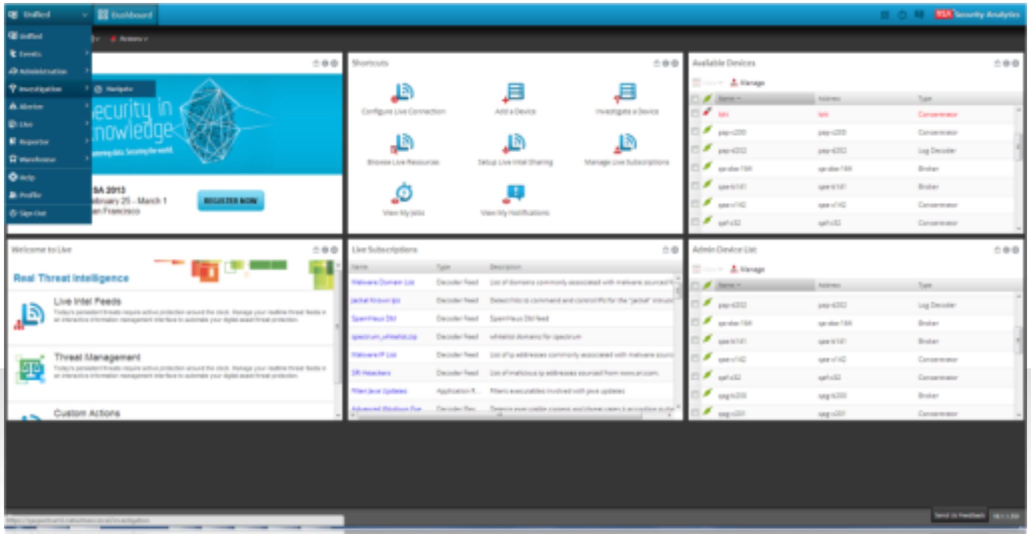
High Powered Analytics

“Give me the speed and smarts to discover and investigate potential threats in near real time”

Integrated Intelligence

“Help me understand what to look for and what others have discovered”

What is RSA Security Analytics?



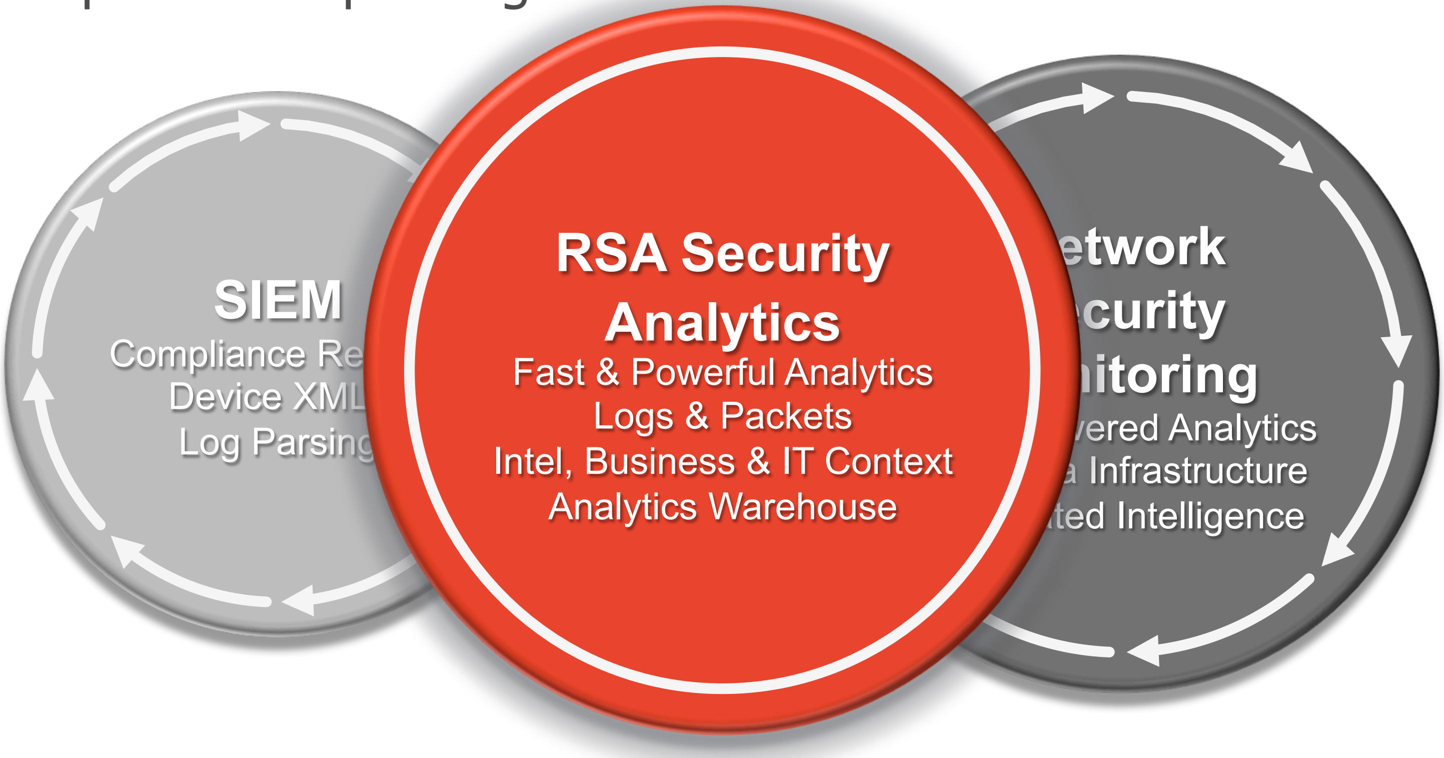
- Unified platform for:
  - Security monitoring
  - Incident investigations
  - Compliance reporting

- Brings together SIEM, Network Security Monitoring, Big Data Management & Analytics

- RSA Security Analytics is a new approach to combating advanced threats

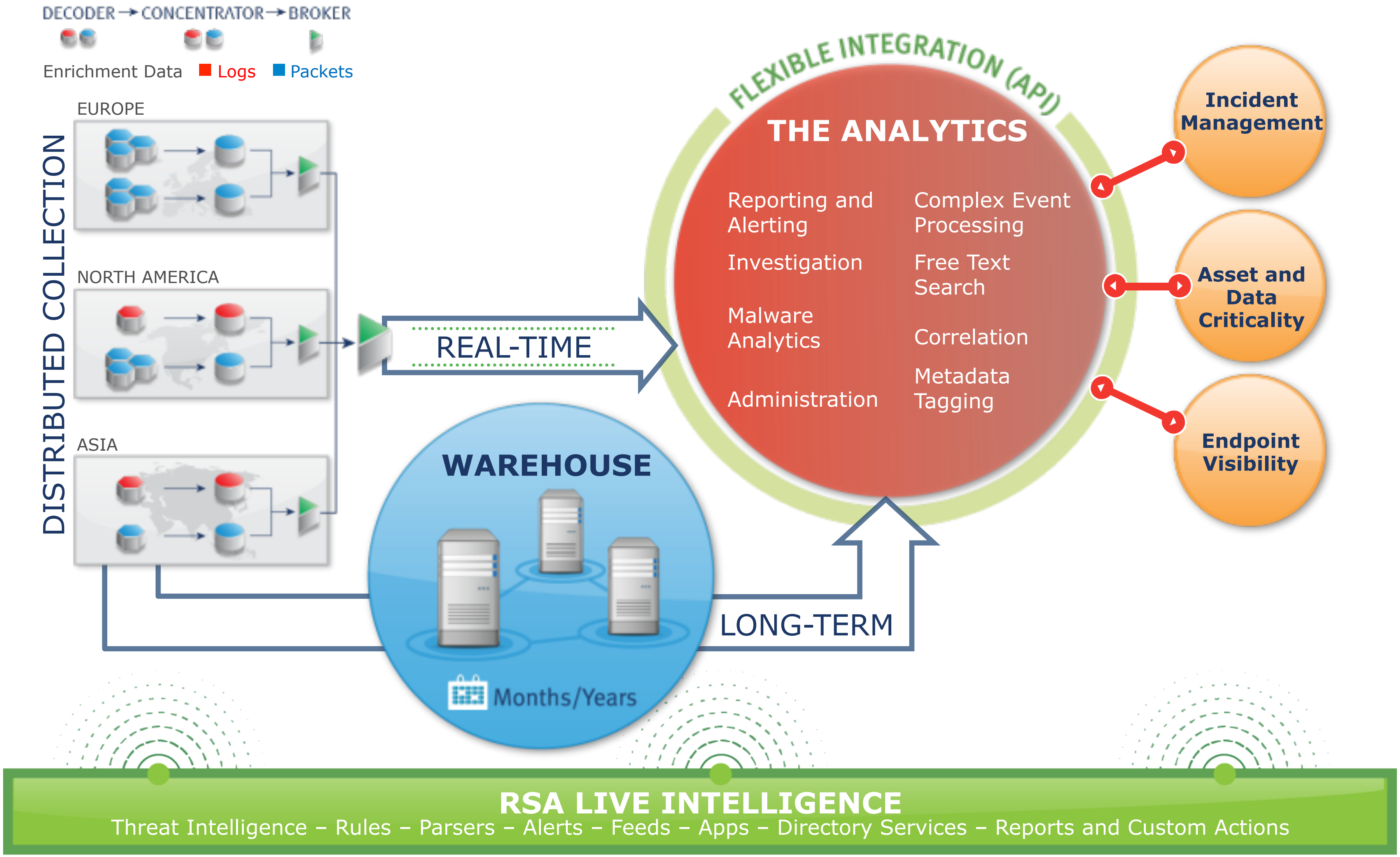
RSA Security Analytics: Changing The Security Management Status Quo

Unified platform for security monitoring, incident investigations and compliance reporting

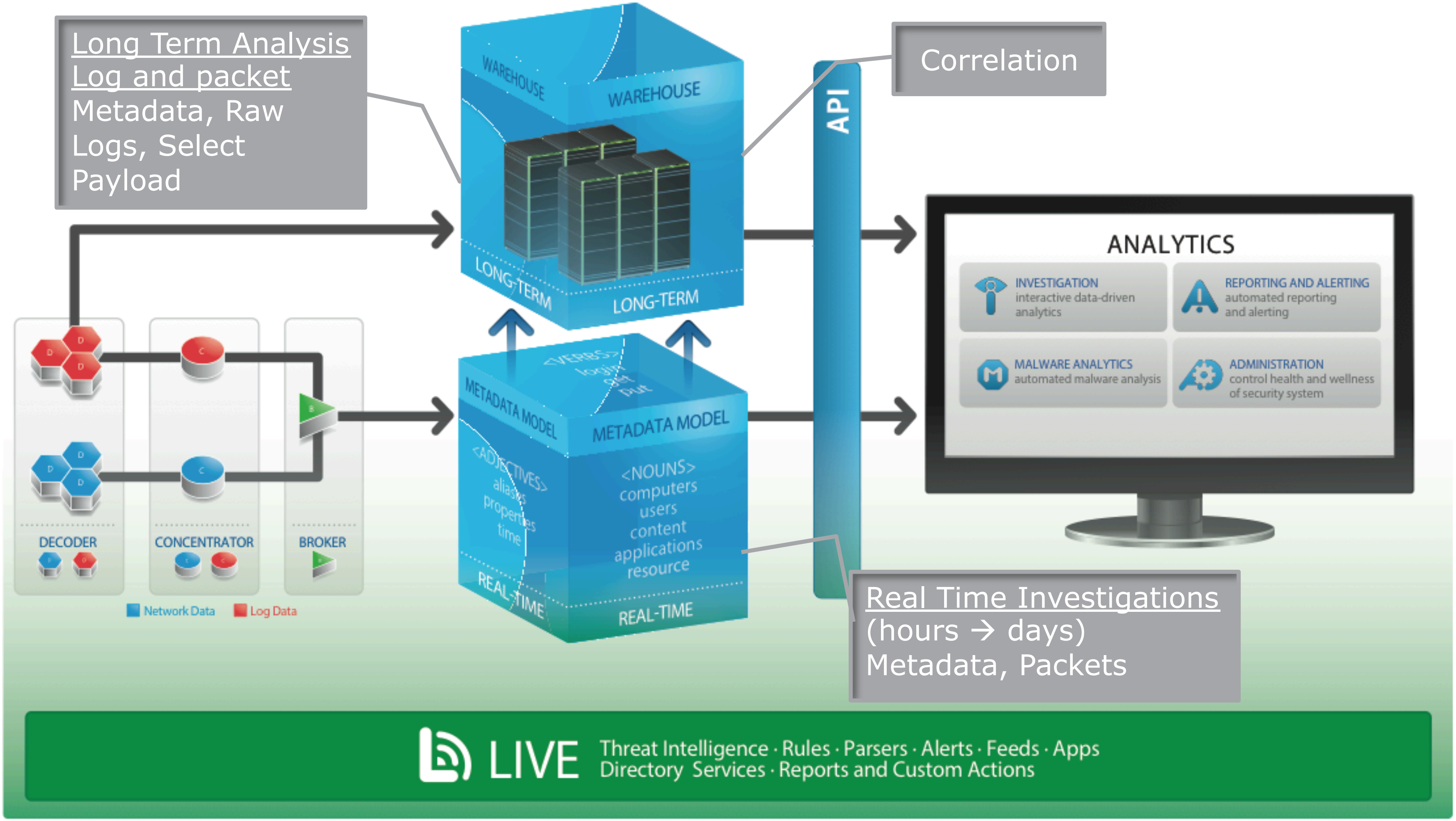


**SEE DATA YOU DIDN'T SEE BEFORE,
UNDERSTAND DATA YOU DIDN'T EVEN CONSIDER BEFORE**

Security Analytics Architecture



RSA Security Analytics Architecture

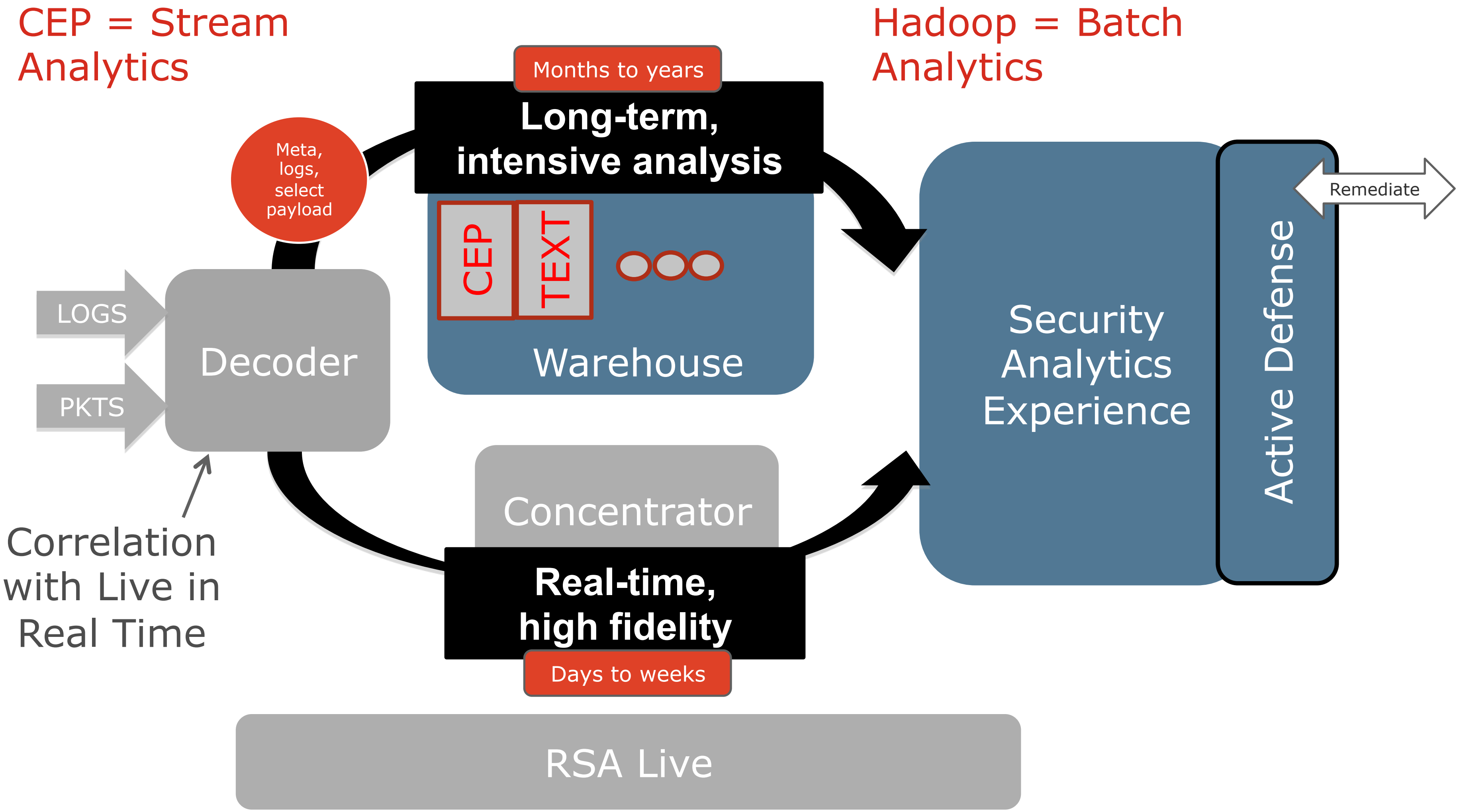


Long Term Analysis
Log and packet
Metadata, Raw Logs, Select Payload

Correlation

Real Time Investigations
(hours → days)
Metadata, Packets

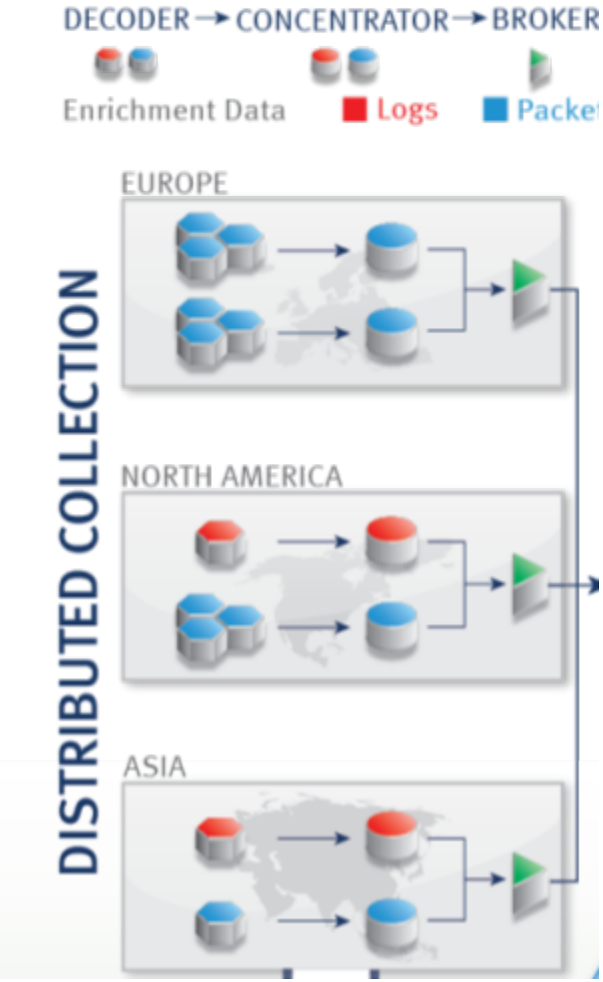
Security Analytics Topology



What Makes Security Analytics Different?

- Big Data Infrastructure
  - Fast and scalable
  - Security data warehouse plus proven NetWitness infrastructure
- Comprehensive Visibility
  - See everything happening in an environment
  - Normalizes diverse data including logs, packets and intelligence
- High Powered Analytics
  - Speed and smarts to detect and investigate advanced threats
  - Provides short term and long term analytics plus compliance
  - Removes the hay versus digging for needles
- Integrated Intelligence
  - Operationalize intelligence by fusing it with your data
  - Understand what to look for and what others have found

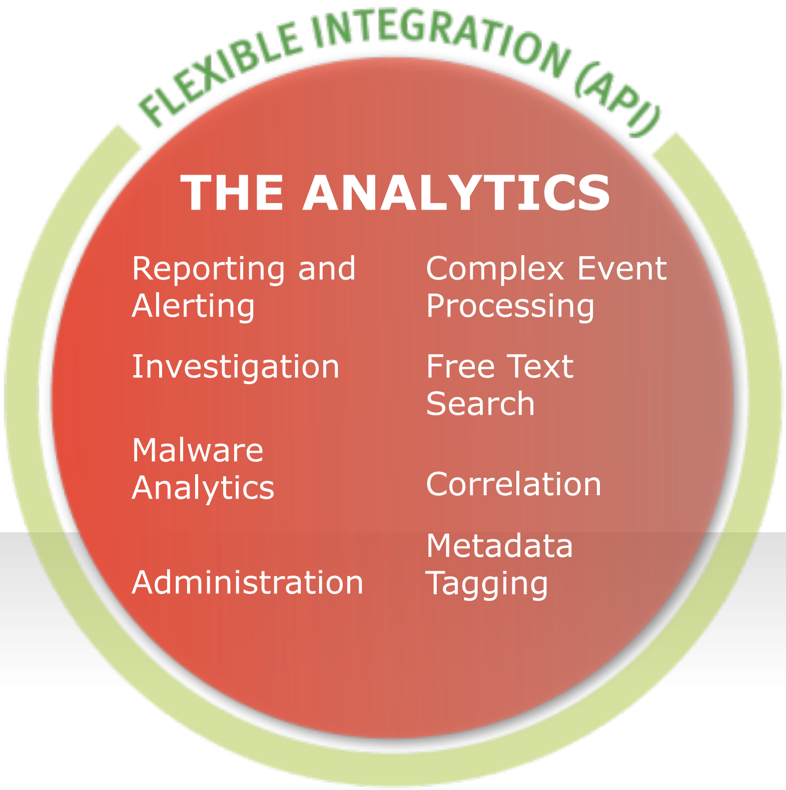
Big Data Infrastructure



- Single platform for capturing and analyzing large amounts of network and log data
- Distributed, “scale-out” architecture
- Unique architecture to support both “speed” and “smarts” for threat analysis
- Security data warehouse for long term analytics & compliance
- Proven NetWitness infrastructure
- Session based, full reconstruction

High Powered Analytics

- Eliminates blind spots to achieve comprehensive visibility across the enterprise
- Real-time and “after-the-fact” investigations
- Uses the industry’s most comprehensive and easily understandable analytical workbench
- Proven, patented analytics applies business context to security investigations
- Automates the generation of compliance reports and supports long term forensic analysis



FLEXIBLE INTEGRATION (API)

THE ANALYTICS

Reporting and Alerting

Complex Event Processing

Investigation

Free Text Search

Malware Analytics

Correlation

Administration

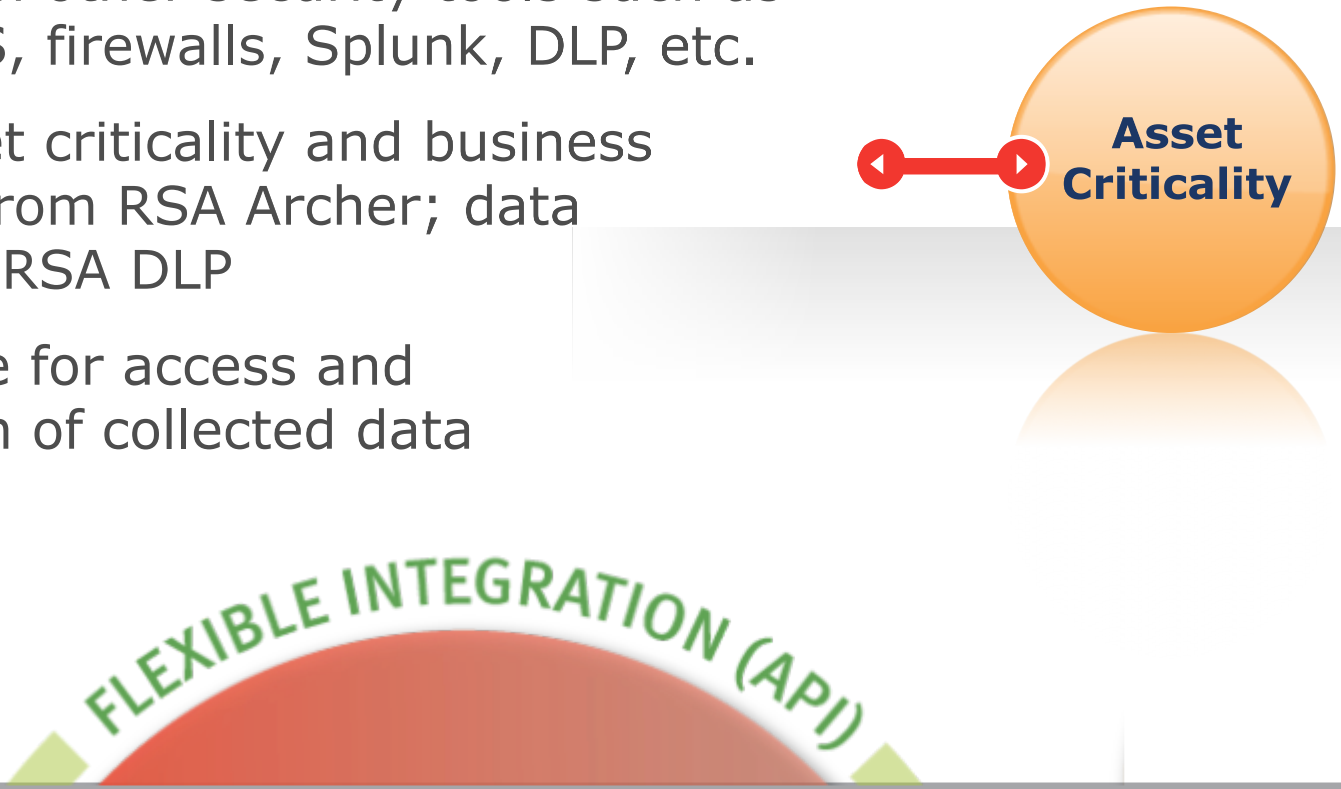
Metadata Tagging

The Security Analytics Warehouse

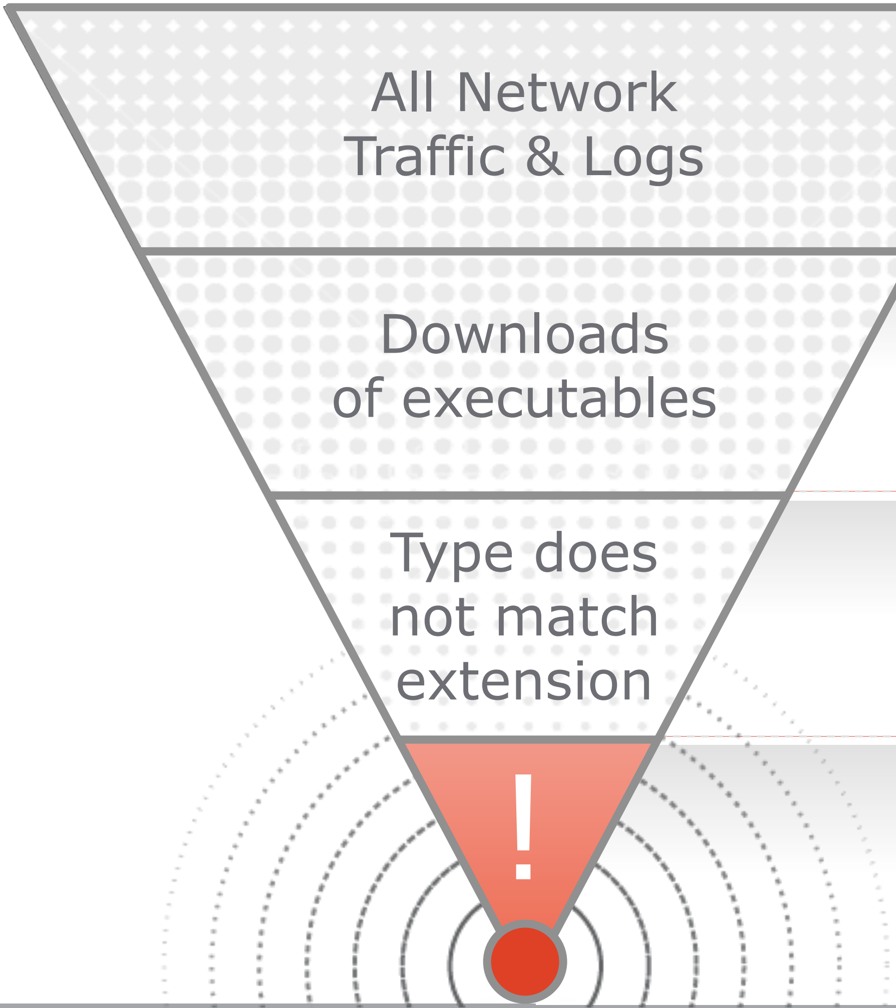
- Long Term Data Retention and Analysis
  - Security data focused warehouse
  - Packet & Log Metadata, Raw Logs, Select Payload
- Hadoop-based architecture for maximum scale and flexibility
- Complex Event Processing
- "Google-like" free text search
- Achieves requirements for compliance

Flexible Integration

- API flexibility allows RSA Security Analytics to form heart of security ecosystem
- Integrates with other security tools such as SIEM, IDS/IPS, firewalls, Splunk, DLP, etc.
- Integrate asset criticality and business context data from RSA Archer; data discover from RSA DLP
- Open interface for access and transformation of collected data



Reimagining Security Analysis: Removing Hay vs. Digging For Needles



Terabytes of data
100% of total

Thousands of data points
5% of total

Hundreds of data points
0.2% of total

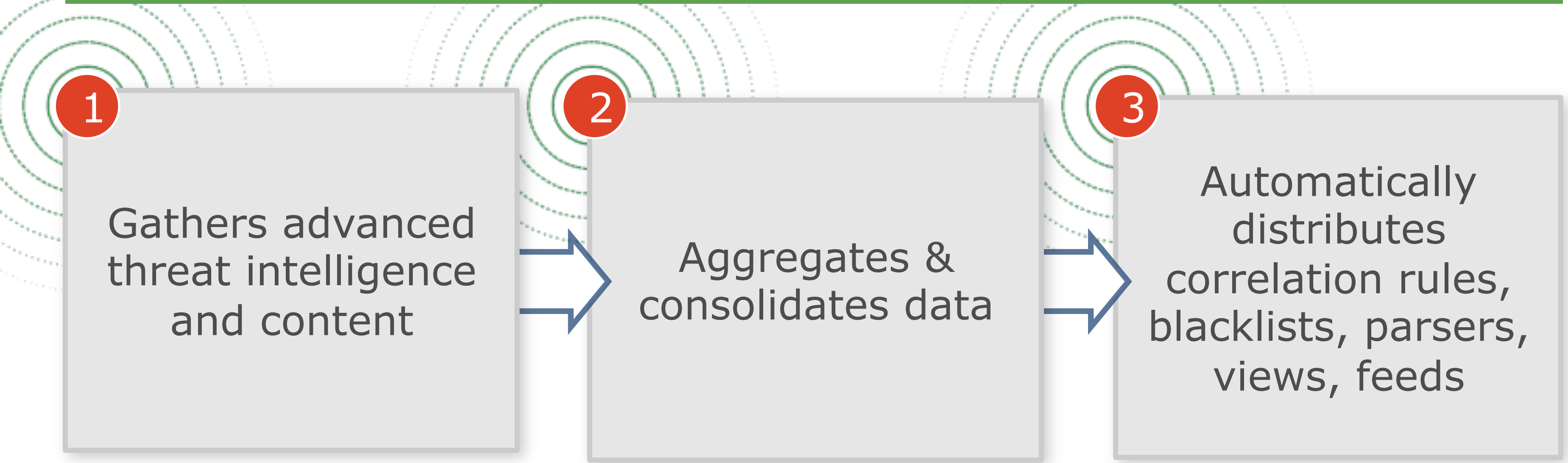
Create alerts to/from critical assets
A few dozen alerts

Integrated Intelligence

Know What To Look For

RSA LIVE INTELLIGENCE SYSTEM

Threat Intelligence – Rules – Parsers – Alerts – Feeds – Apps – Directory Services – Reports and Custom Actions



1 Gathers advanced threat intelligence and content

2 Aggregates & consolidates data

3 Automatically distributes correlation rules, blacklists, parsers, views, feeds

OPERATIONALIZE INTELLIGENCE:

Take advantage of what others have already found and apply against your current and historical data

RSA FirstWatch®

- RSA 's elite, highly trained global threat research & intelligence team
- Providing covert and strategic threat intelligence on advanced threats & actors
- Focused on threats unknown to the security community
  - Malicious code & content analysis
  - Threat research & ecosystem analysis
  - Profiling threat actors
- Research operationalized automatically via RSA Live

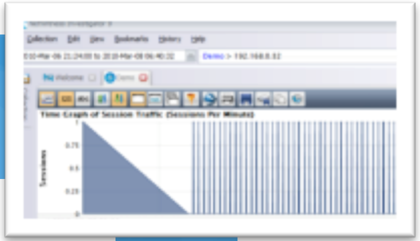
Days of Investigation Completed In Hours

ALERT!!... Multiple indicators to escalate a potential incident

Abnormal EXE structure, crafted HTTP header, RSA Live indicates traffic coming from known malicious actor

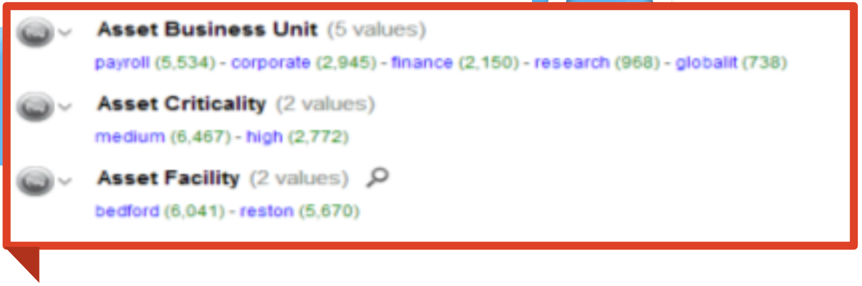
Session Recreated

Privilege escalation, attempted FTP upload of documents, Other similar traffic from targeted account, other traffic from IP address



Additional Context

Incident involves highly critical server from the accounting department, data targeted includes company financials and PCI data



Asset Business Unit (5 values)

payroll (5,534) - corporate (2,945) - finance (2,150) - research (968) - globalit (738)

Asset Criticality (2 values)

medium (6,467) - high (2,772)

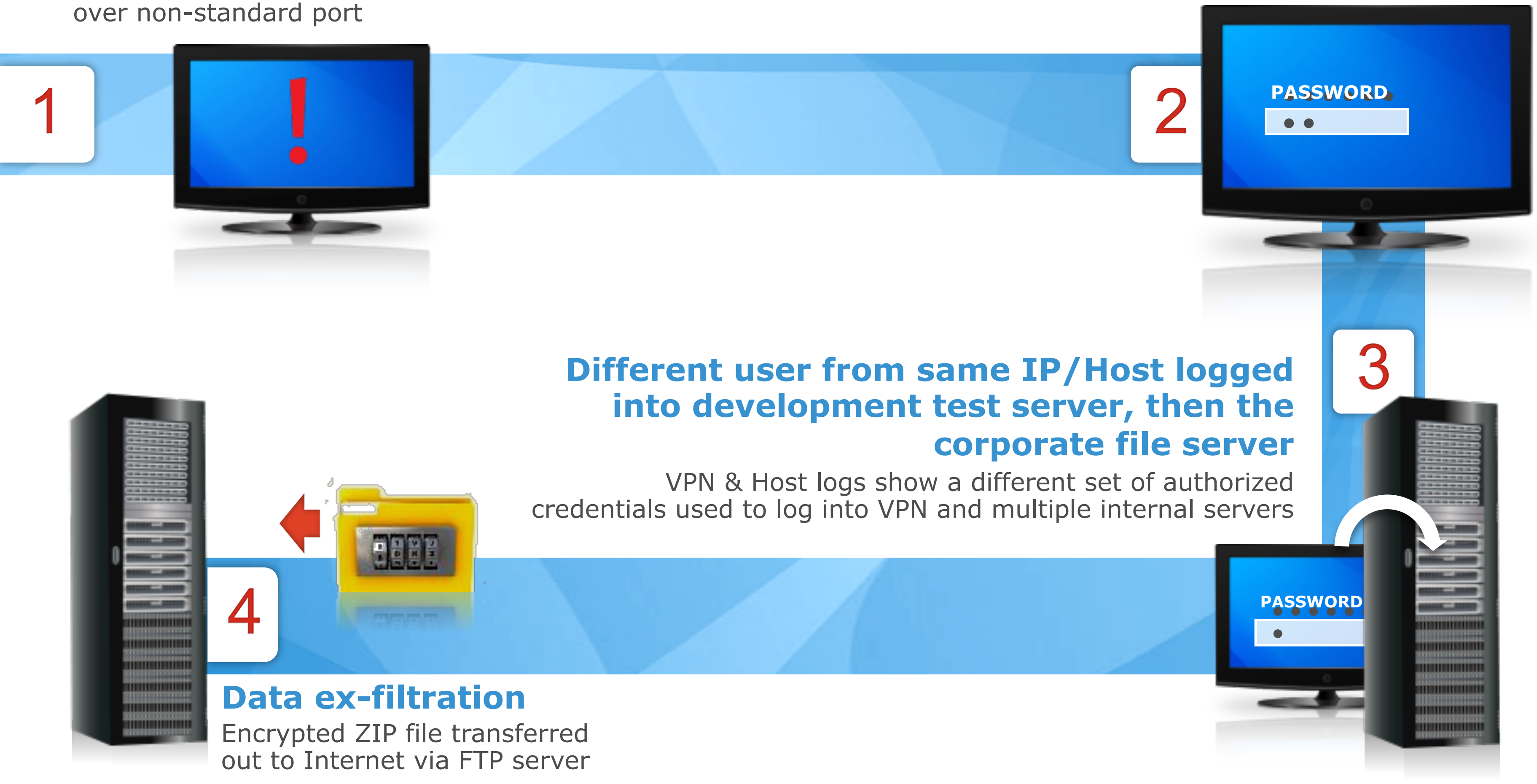
Asset Facility (2 values)

bedford (6,041) - reston (5,670)

Incident Management

Incident escalated, owner notified, remediation case opened, endpoint inspected

Suspect Attack Scenario: Data Ex-filtration



ALERT!!... Suspect Network Traffic

IP Address shows multiple connections tunneled over non-standard port

Authorized User Logged in to AD

AD Logs drill-down show user logged in from suspect IP with authorized credentials

Different user from same IP/Host logged into development test server, then the corporate file server

VPN & Host logs show a different set of authorized credentials used to log into VPN and multiple internal servers

Data ex-filtration

Encrypted ZIP file transferred out to Internet via FTP server

Only RSA Security Analytics Can Tell You The Impact Of The Attack

Attack Step	Traditional SIEM	RSA Security Analytics
Alert for access over non-standard port	No	Yes
Recreate activity of suspect IP address across environment	No	Yes
Show user activity across AD and VPN	Yes	Yes
Alert for different credentials used for AD and VP	Yes	Yes
Reconstruct exfiltrated data	No	Yes

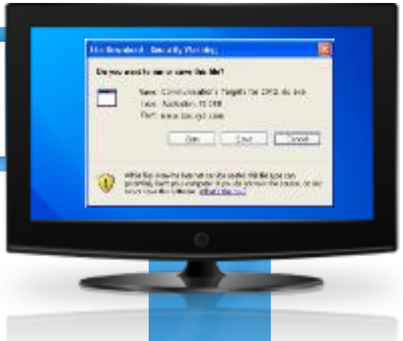
Investigation Scenario

1

Find compromised Server or Workstation acting as SPAM host

Multiple outbound SMTP connections from workstation.
Multiple internet DNS connections from workstation

2



File Download - Security Warning

Do you want to run or save this file?

Name: Communication's Targets for 2012.doc.exe
Type: Application, [illegible] KB
From: www.[illegible].com

Run | Save | Cancel

[illegible]

Find out how the workstation got infected

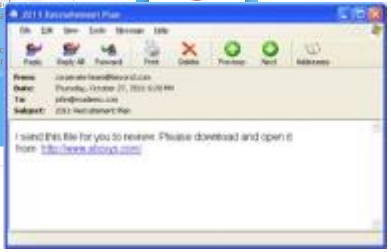
User clicked on the link and got infected by Trojan from drive-by download.

3

Recreate phishing e-mail message

Determine whether targeted phishing attack at play

The image cannot be displayed. Your
computer may not have enoug
to open the image, or the ima
been corrupted. Restart your
and then open the file again.
still appears, you may have to
image and then insert it agair



2011 Recruitment Plan

From: [illegible]
Date: Thursday, October 27, 2011 [illegible]
To: [illegible]
Subject: 2011 Recruitment Plan

I send this file for you to review. Please download and open it from http://www.[illegible].com/

4

Analyze malware

Determine whether targeted or vanilla malware in use

Only RSA Security Analytics Can Tell If This Is A Targeted Attack

Attack Step	Traditional SIEM	RSA Security Analytics
Alert for suspected SPAM host	Yes	Yes
Show all WWW requests where executable downloaded	No	Yes
Recreate email with suspect link	No	Yes
Analyze malware and incorporate community intelligence	No	Yes
Determine whether attack is part of a targeted campaign	No	Yes

Summary

- Traditional security is not working
- Security is becoming a Big Data problem
- RSA Security Analytics is a new approach to combating advanced threats
- RSA Security Analytics brings together traditional SIEM, Network Security Monitoring, Big Data Management & Analytics
- Key pillar to an intelligence-driven security strategy
  - Big Data Infrastructure
  - Comprehensive Visibility
  - High Powered Analytics
  - Integrated Intelligence

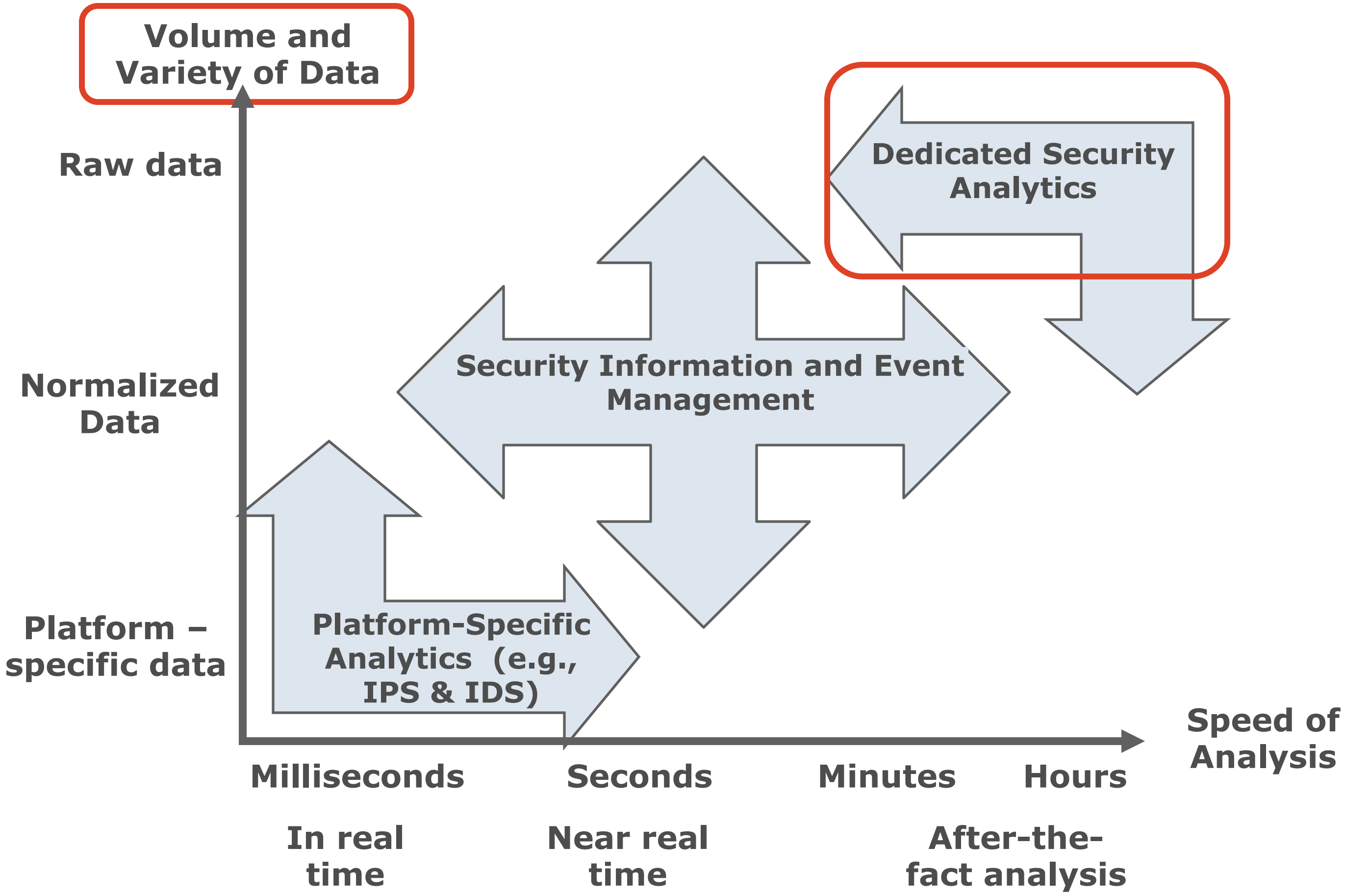
RSA®

EMC²®

Appendix: Intros

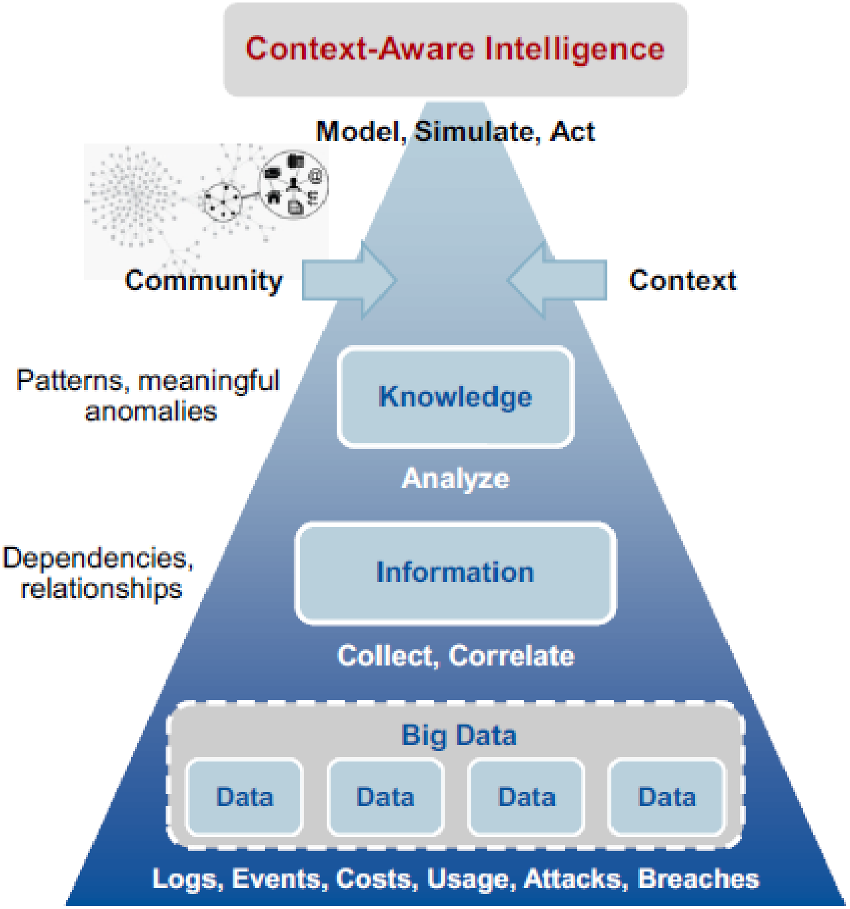
Analyst Proof Points

SIEM Needs To Evolve Into Security Analytics



Gartner, Information Security is Becoming a Big Data Analytics Problem, Neil Macdonald, Mar. 23, 2012

Context-Aware Security Intelligence: Risk-Prioritized, Actionable Insight


Context-Aware Intelligence
Model, Simulate, Act
Community
Context
Patterns, meaningful anomalies
Knowledge
Analyze
Dependencies, relationships
Information
Collect, Correlate
Big Data
Data
Data
Data
Data
Logs, Events, Costs, Usage, Attacks, Breaches

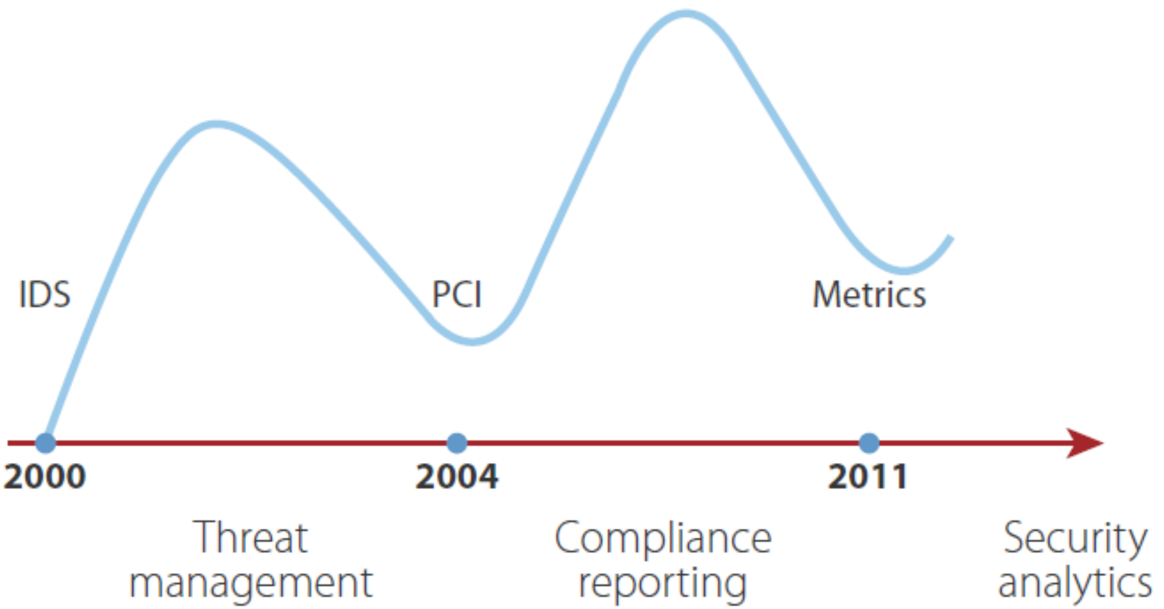
Gartner

Source: Gartner (March 2012)

Gartner, Information Security is Becoming a Big Data Analytics Problem, Neil Macdonald, Mar. 23, 2012

SIEM Needs To Evolve

Figure 1 The Evolution Of SIM



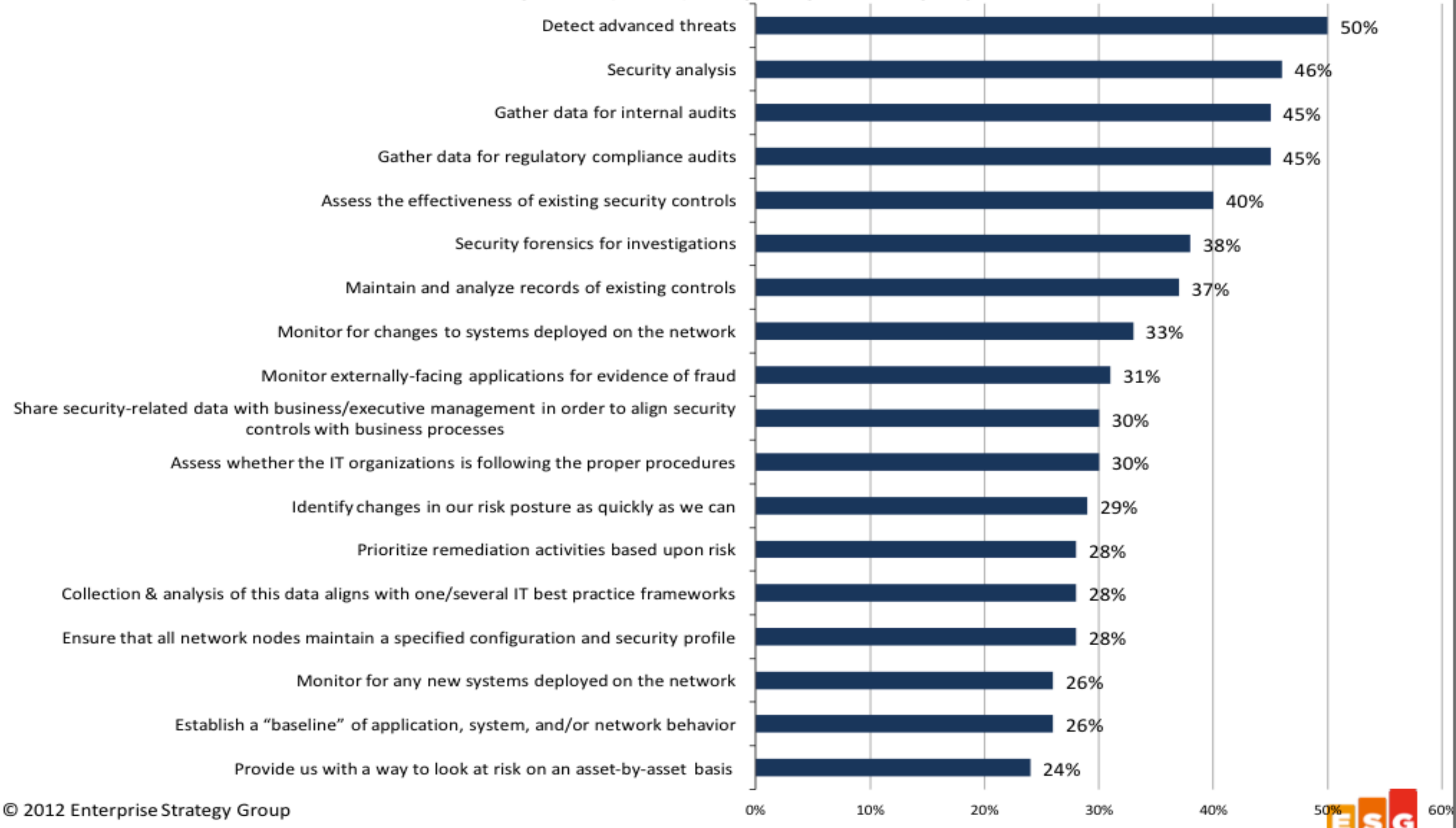
61554

Source: Forrester Research, Inc.

Forrester, Dissect Data to Gain Actionable INTEL, Shey & Kindervag, August 9, 2012

Drivers For Big Data Security Analysis

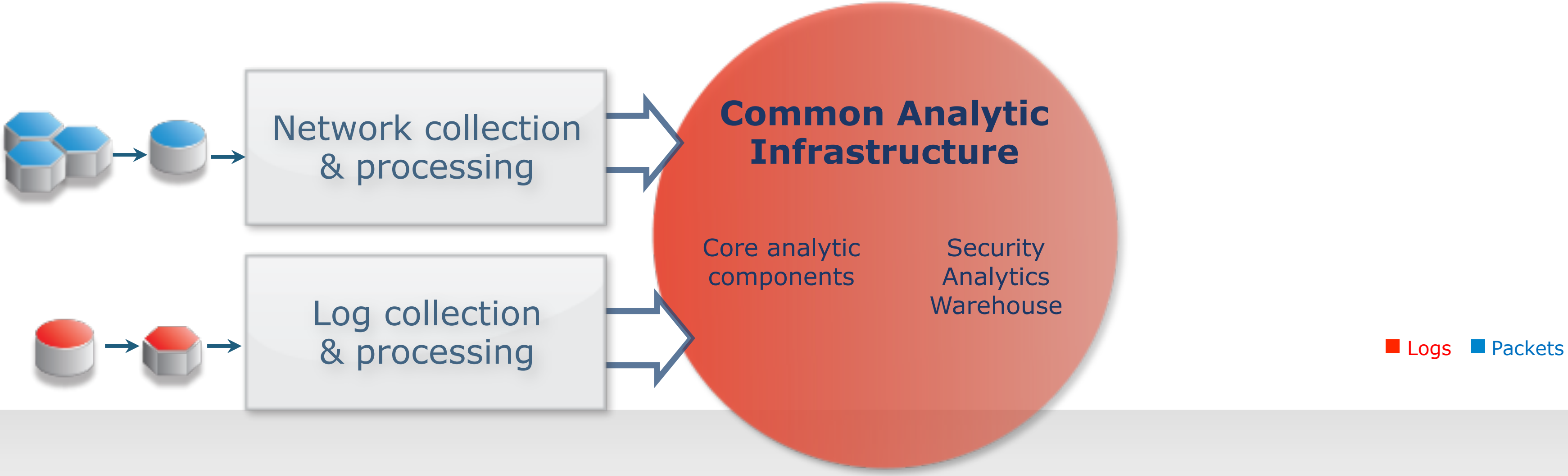
What are the biggest drivers for your organization to collect and analyze data as part of its security strategy? (Percent of respondents, N=257, multiple responses accepted)



© 2012 Enterprise Strategy Group

Deployment Options

Security Analytics Deployment Choices



Network collection & processing

Log collection & processing

Common Analytic Infrastructure

Core analytic components

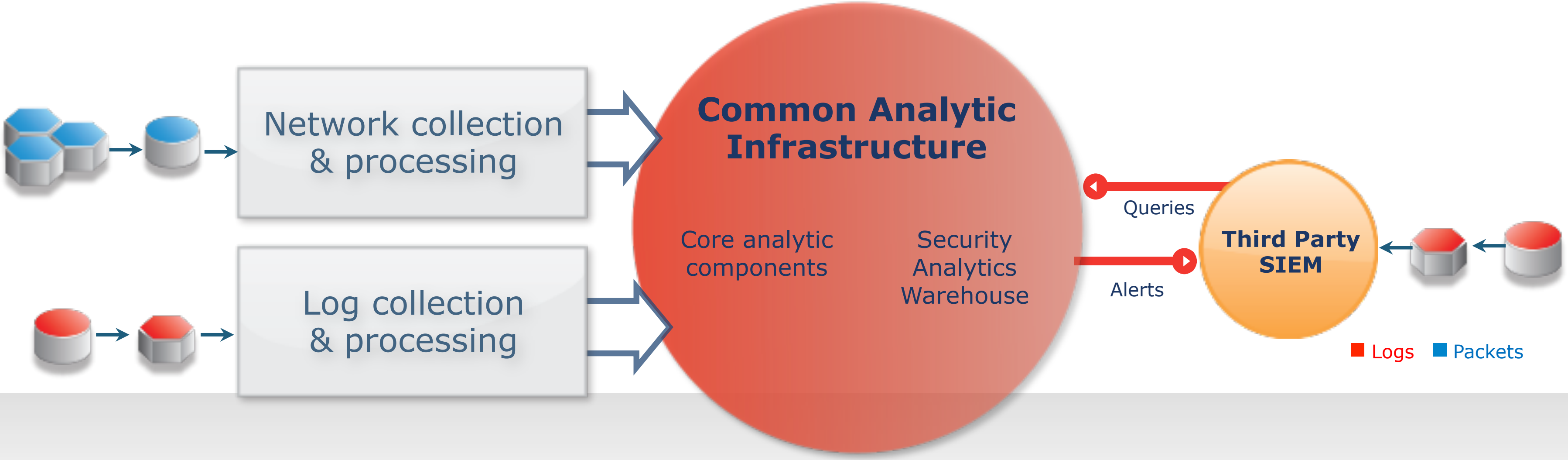
Security Analytics Warehouse

🟥 Logs 🟦 Packets

Customers can buy

- Log analysis, packet analysis or both
- Core components for short term analytics, warehouse for longer term & more intensive analytics, or both

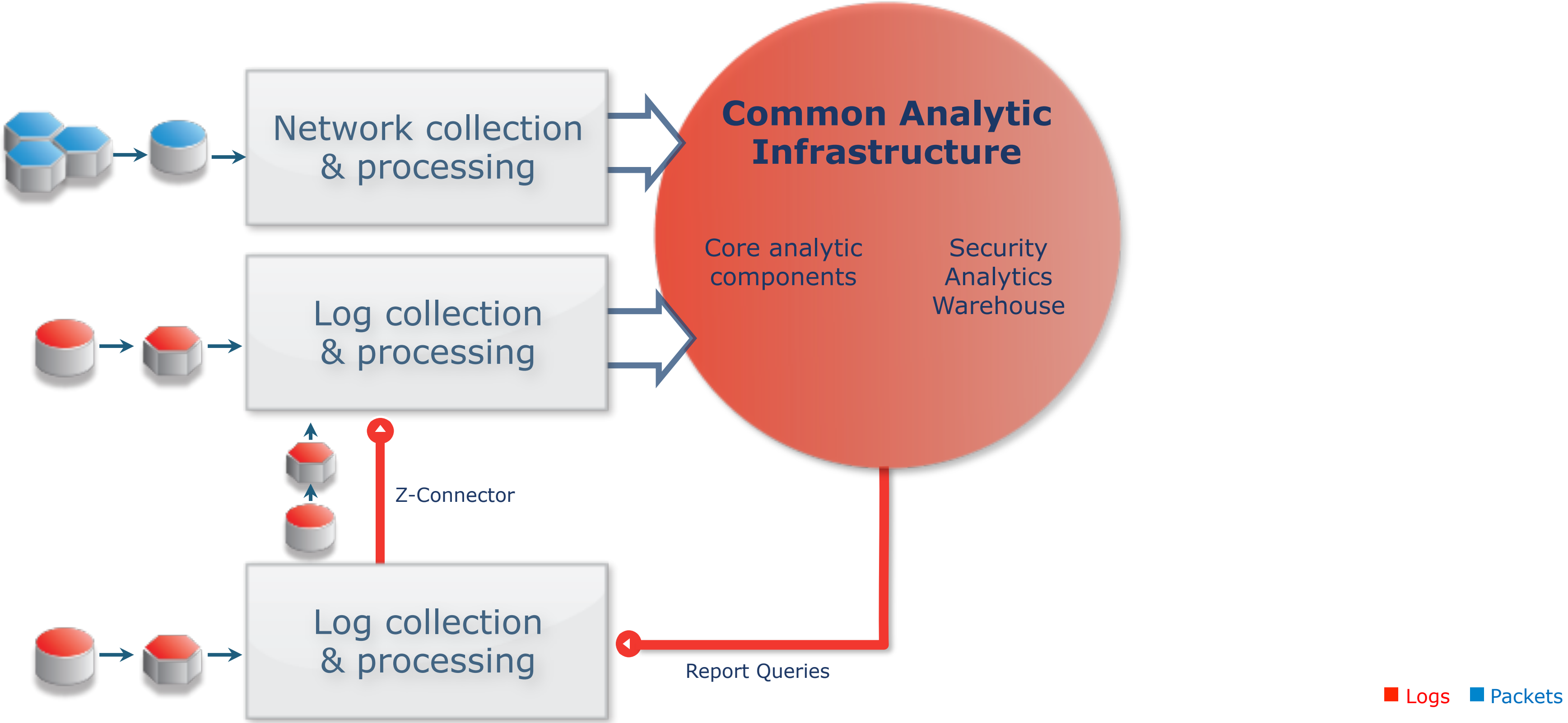
Security Analytics & SIEM


Network collection & processing
Log collection & processing
Common Analytic Infrastructure
Core analytic components
Security Analytics Warehouse
Queries
Alerts
Third Party SIEM
🟥 Logs
🟦 Packets

Security Analytics Integrates with SIEM

- Exports alerts as logs to SIEM
- Executes queries from SIEM (e.g. investigate this IP)
- Two separate interfaces – no native correlation across logs and packet data
- No warehouse for complex analytics

Security Analytics & enVision


Network collection & processing
Log collection & processing
Log collection & processing
Common Analytic Infrastructure
Core analytic components
Security Analytics Warehouse
Z-Connector
Report Queries
🟥 Logs
🟦 Packets

Transition allows for mixed mode deployment

- Logs can be forwarded to SA to take advantage of better performance and analytic firepower
- Capability to query enVision from within SA UI for legacy data

Technical Details

Security Analytics Warehouse (SAW)

- SAW
  - Proper Data Warehouse
  - Security data focus
  - Hadoop-based
- Flexible access / analysis
  - Network metadata and Log data
- RSA SA reporting and full text search UI
  - Open interface for access and transformation of collected data
    - PIG & HIVE
- Modular Scale
  - Single to hundreds to thousands of nodes
- Platform
  - Advanced security analytic tools (CEP)
  - Archive Log Compression
  - Resiliency and high availability

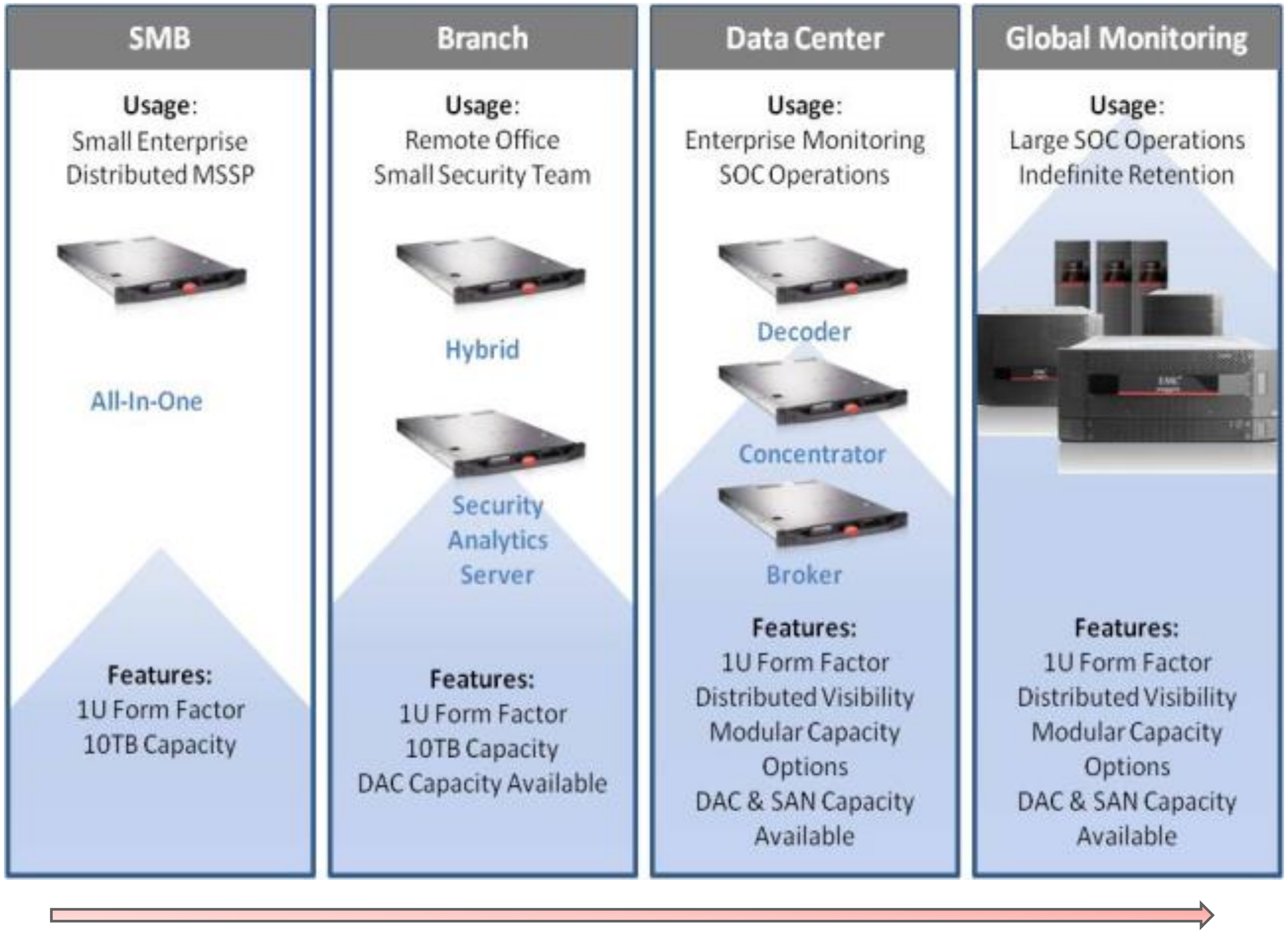
Security Analytics Warehouse (SAW)

- Ultra Performance – for more powerful analytics
  - A cluster of 4S appliances
  - 1U Rackspace per node
  - Each node rated @ 20k EPS sustained collection
- High Capacity – for archiving and less analytics
  - A cluster of 4S appliances with DACs
  - 4U Rackspace per node
  - 3 node cluster retains 6000 average EPS for 2 years
  - Each node rated to 20k EPS sustained collection

Security Analytics Preliminary Stats

- Processing
  - A single Log Decoder can process 30K EPS, with peak beyond 80K EPS, double other SIEM tools
  - 350 supported log sources
- Compression
  - SA Warehouse 9:1
  - 50% more than other SIEM tools
- Consumption
  - Security Analytics Warehouse (3 compute nodes) can consume at 500K EPS...and scale up
- Correlation
  - Security Analytics Warehouse Complex Event Processing (6 compute nodes) can correlate 4.5 Billion EPS … and scale up
- Reporting
  - Queries that took hours now takes minutes

Security Analytics – Platform Options



SMB	Branch	Data Center	Global Monitoring
Usage: Small Enterprise Distributed MSSP	**Usage:** Remote Office Small Security Team	**Usage:** Enterprise Monitoring SOC Operations	**Usage:** Large SOC Operations Indefinite Retention
All-In-One	Hybrid Security Analytics Server	Decoder Concentrator Broker	
Features: 1U Form Factor 10TB Capacity	**Features:** 1U Form Factor 10TB Capacity DAC Capacity Available	**Features:** 1U Form Factor Distributed Visibility Modular Capacity Options DAC & SAN Capacity Available	**Features:** 1U Form Factor Distributed Visibility Modular Capacity Options DAC & SAN Capacity Available

- Various platform options to meet the specific needs and use cases of customers
- Software-only versions of these platforms are available

Taking A Closer Look

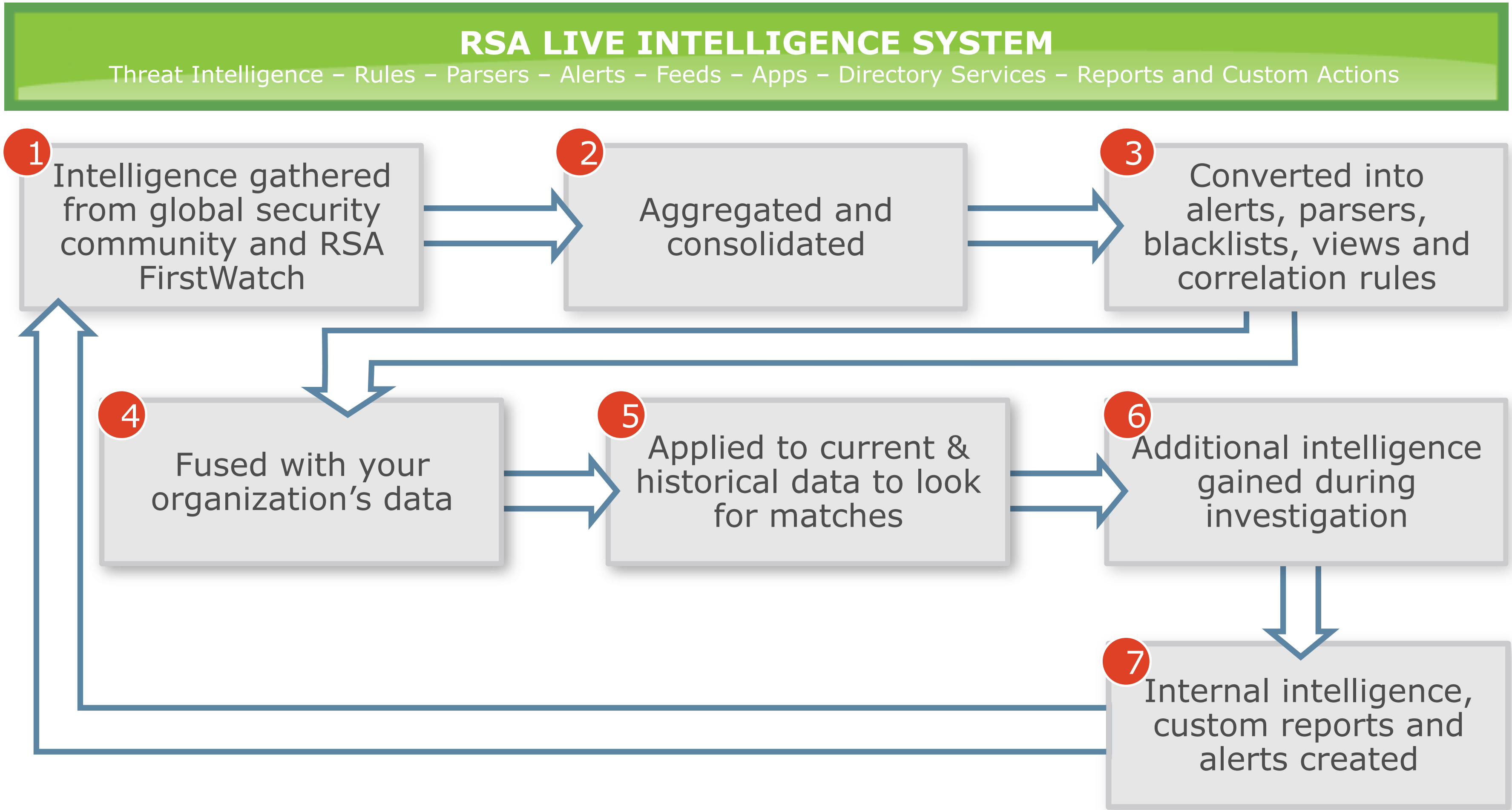
Integrated Intelligence In Action: The VOHO Campaign

Benefits of Integrated Intelligence

- There is intelligence and there are the tools needed to make intelligence operational. RSA Security Analytics delivers both
- Operationalized intelligence is far greater than detached intelligence
- Analysts need to understand what to look for and take advantage of what others have found
- RSA Live integrated the best of global intelligence as well as proprietary research from RSA FirstWatch
- Compare intelligence with historical data to see if indicators of compromise were found
- Apply in real-time to defend against future attacks

The Lifecycle Of Intelligence

Know What To Look For



RSA LIVE INTELLIGENCE SYSTEM

Threat Intelligence – Rules – Parsers – Alerts – Feeds – Apps – Directory Services – Reports and Custom Actions

1 Intelligence gathered from global security community and RSA FirstWatch

2 Aggregated and consolidated

3 Converted into alerts, parsers, blacklists, views and correlation rules

4 Fused with your organization's data

5 Applied to current & historical data to look for matches

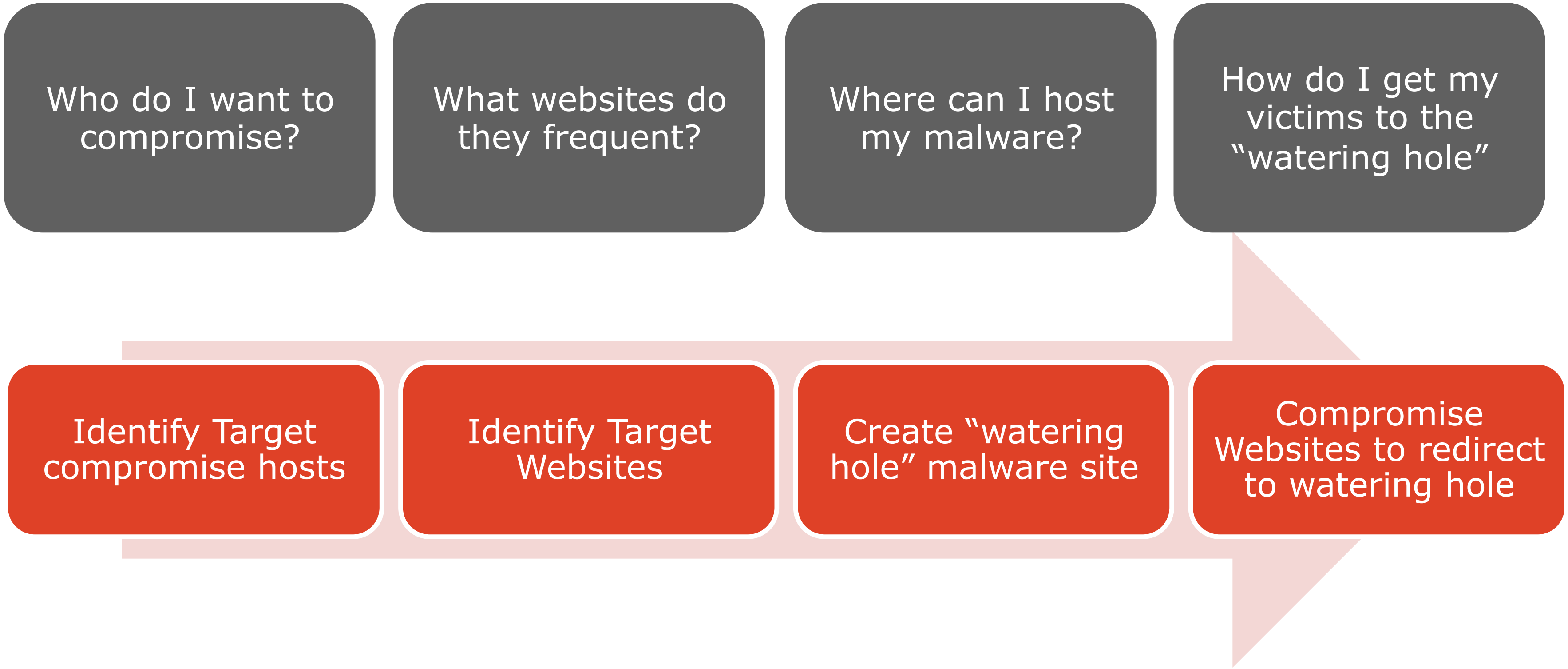
6 Additional intelligence gained during investigation

7 Internal intelligence, custom reports and alerts created

What Is The VOHO Campaign?

- Discovered in July 2012 by RSA FirstWatch
  - Infrastructure was shared for multiple threat campaigns
  - Trojan payload via browser-based exploits to delivers exploits to website visitors
- At first glance appeared to be “garden variety” drive by attack
- However, victims seemed to be geographically clustered
- Further research by RSA First Watch team found campaign used brand new attack approach utilizing ‘water holing’ method
- Multistage Campaign: Redirection with a heavy dependency on JavaScript on two specific domains for majority of promulgation

VOHO Waterholing Attack Flow



Who do I want to compromise?

What websites do they frequent?

Where can I host my malware?

How do I get my victims to the "watering hole"

Identify Target compromise hosts

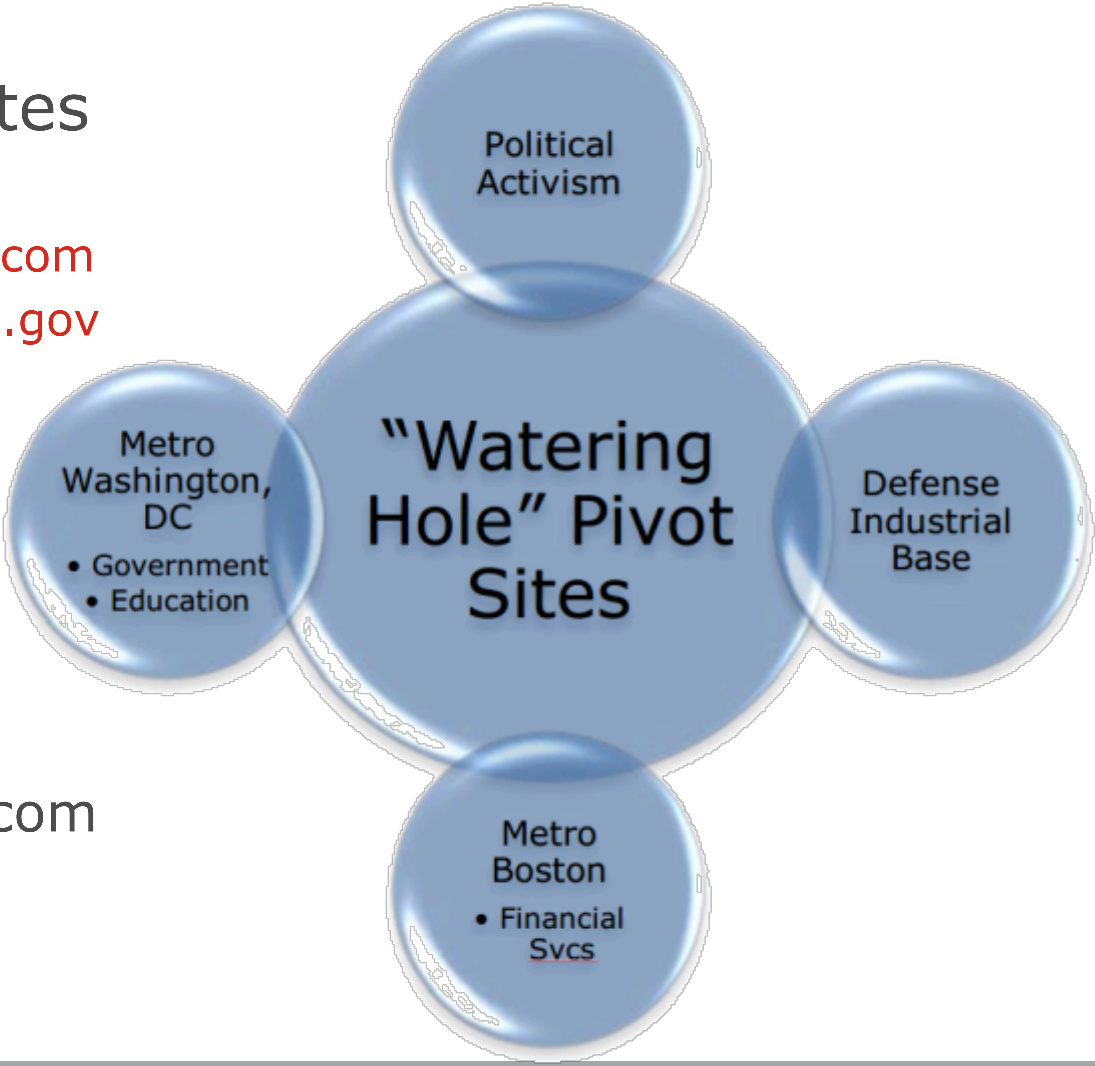
Identify Target Websites

Create "watering hole" malware site

Compromise Websites to redirect to watering hole

VOHO Watering Hole Leveraged Industries and Regions

- Sample targeted websites (redacted)
  - hxxp://www.xxxxxxxxtrust.com
  - hxxp://xxxxxxxxxcountymd.gov
  - hxxp://xxxxxxcenter.org
  - hxxp:/xxxxxxxpolitics.com
  - hxxp://www.xxxxxantennas.com
- Water Hole site (redacted)
  - hxxp://xxxxxxxcurling.com



Malware Specifics

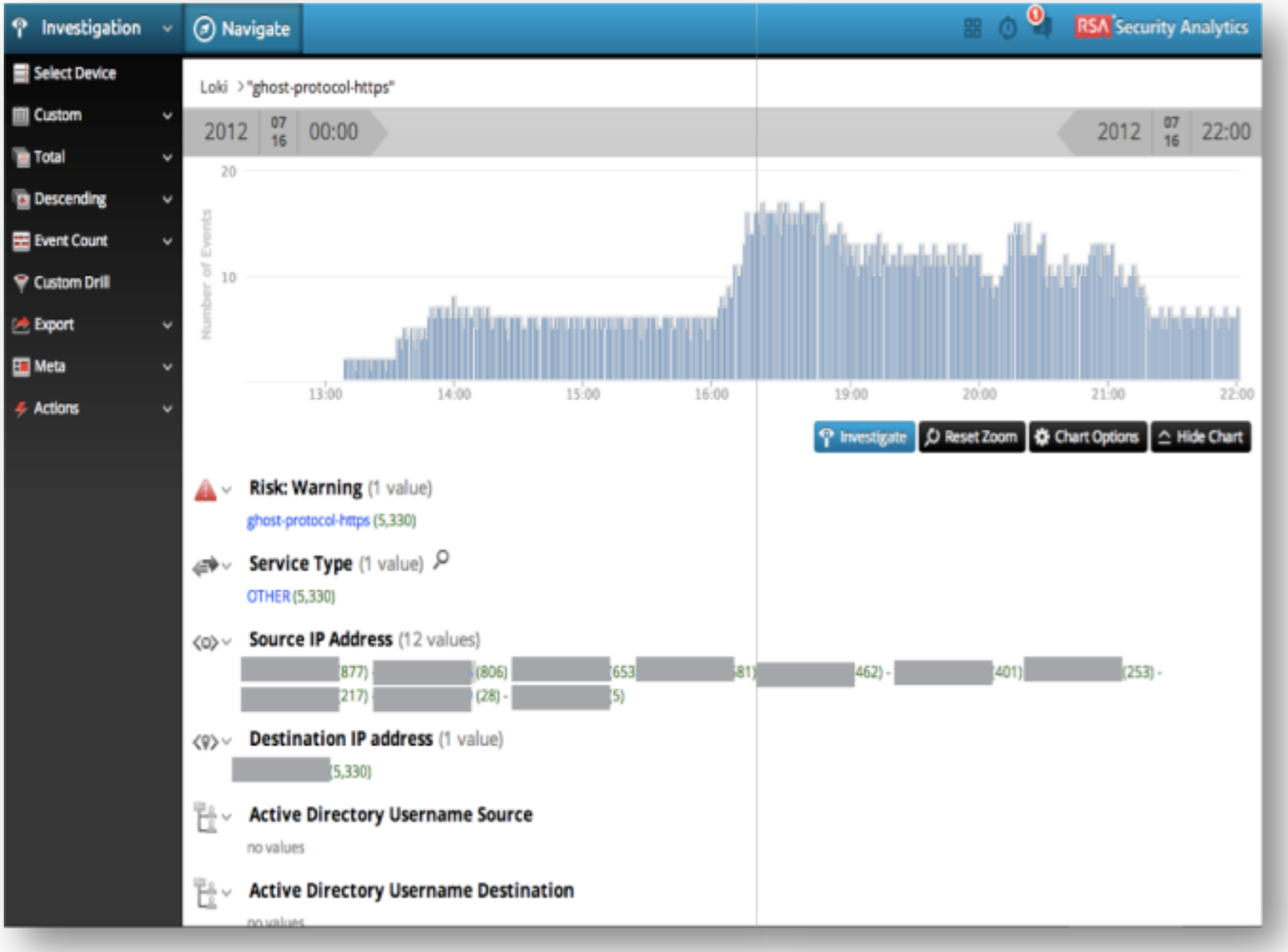
- Installed Variant of Gh0st RAT on compromised endpoint
  - Gh0st is a Remote Access Tool (RAT) allowing control of compromised endpoint
  - Typically masquerades as Symantec or MS update
  - Exploits zero day or known vulnerability
    - Microsoft XML Core Services – CVE-2012-1889
    - Java Exploit – CVE-2012-1723

How did RSA FirstWatch detect this?

- Look for communication with blacklisted hosts
  - Known C2 sites
  - Known malware domains
- Look for suspect network traffic
  - "Gh0st" or "HTTPS" in first 5 packets of non-RFC compliant session
  - Use of web redirect using xKungFoo script
- Indicators are automatically distributed and regularly updated via RSA Live

Indicators Defined To Help Identify Attack

- Look for Command and Control (C2) IP addresses → Look for Control Channel IP addresses → Parser created



Risk: Warning (1 value)

ghost-protocol-https (5,330)

Service Type (1 value)

OTHER (5,330)

Source IP Address (12 values)

[redacted] (877) [redacted] (806) [redacted] (653 [redacted] 81) [redacted] 462) - [redacted] (401) [redacted] (253) -
[redacted] 217) [redacted] (28) - [redacted] 5)

Destination IP address (1 value)

[redacted] (5,330)

Active Directory Username Source

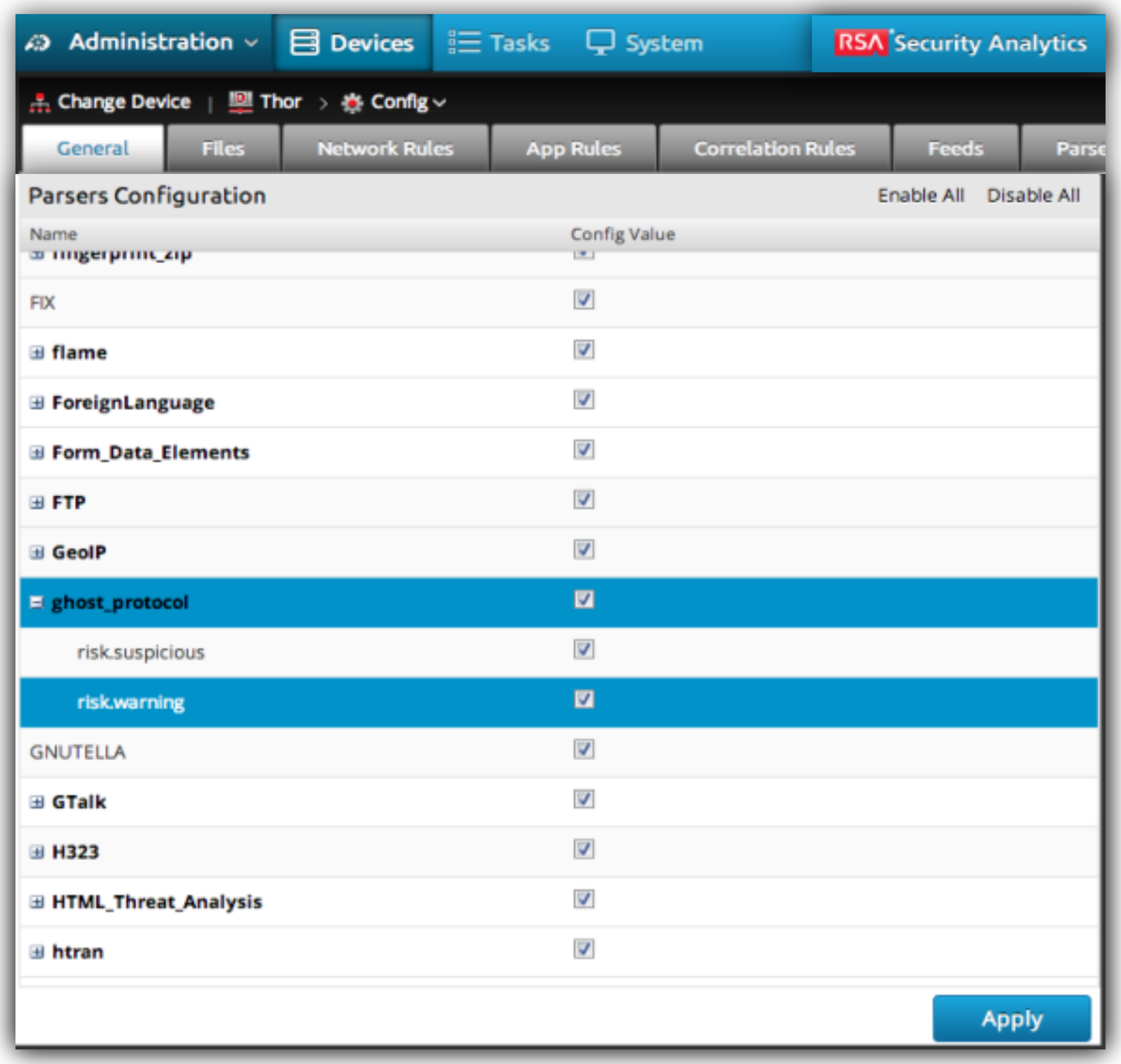
no values

Active Directory Username Destination

no values

Intelligence Feeds Automatically Updated

- RSA FirstWatch feeds updated with VOHO related IP addresses and domains
- Users have the ability to choose which intelligence feeds to enable

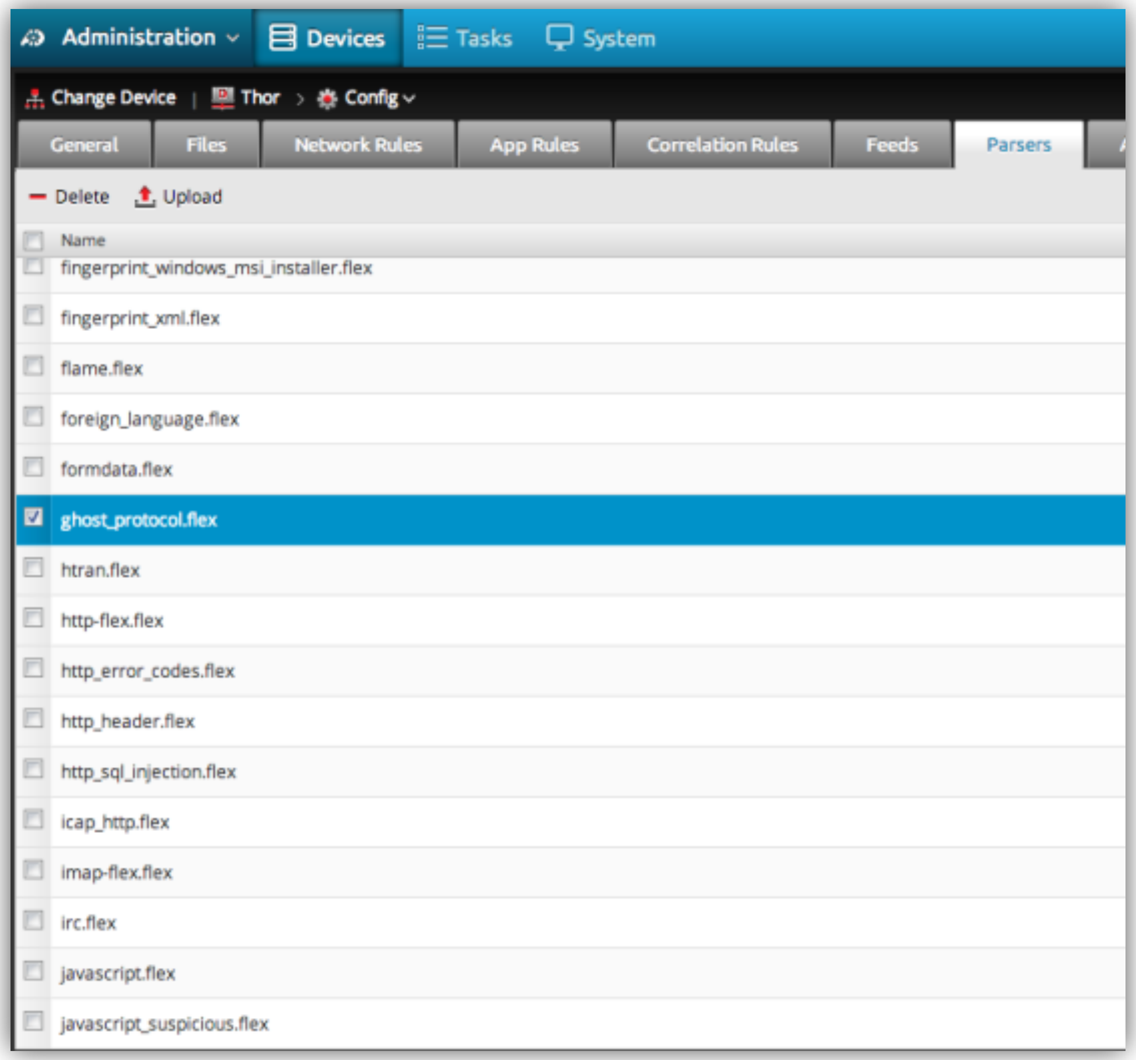


Parsers Configuration

Name	Config Value
⊞ fingerprint_zip	☑
FIX	☑
⊞ flame	☑
⊞ ForeignLanguage	☑
⊞ Form_Data_Elements	☑
⊞ FTP	☑
⊞ GeoIP	☑
⊟ ghost_protocol	☑
risk.suspicious	☑
risk.warning	☑
GNUTELLA	☑
⊞ GTalk	☑
⊞ H323	☑
⊞ HTML_Threat_Analysis	☑
⊞ htran	☑

Intelligence Converted Into An Operationalized Format

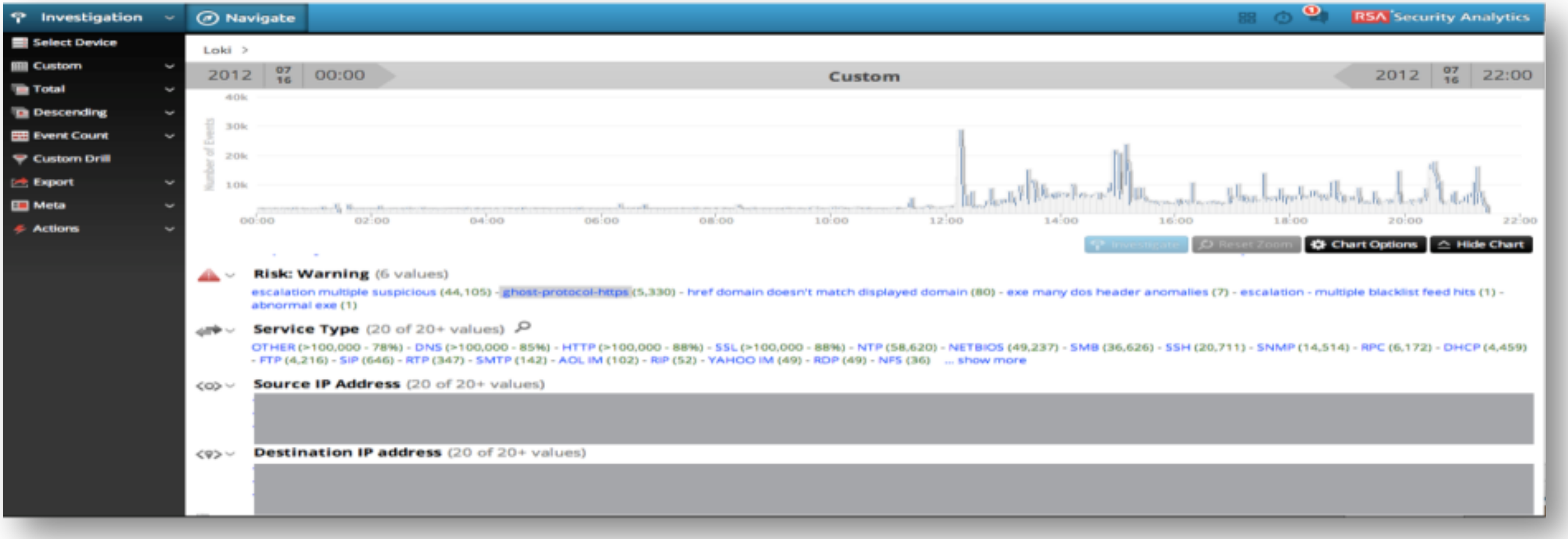
- Indicators converted into ‘Gh0st Protocol’ parser
- Parser helps search for specific behavior within a feed
  - Removes hay to help find needles



□ fingerprint_windows_msi_installer.flex
□ fingerprint_xml.flex
□ flame.flex
□ foreign_language.flex
□ formdata.flex
☑ ghost_protocol.flex
□ htran.flex
□ http-flex.flex
□ http_error_codes.flex
□ http_header.flex
□ http_sql_injection.flex
□ icap_http.flex
□ imap-flex.flex
□ irc.flex
□ javascript.flex
□ javascript_suspicious.flex

Examples Of Findings

- Parser fused with organizational data to find compromised hosts within their environment
- Lateral movement indicative of promulgation found via host based forensic analysis



Risk: Warning (6 values)

escalation multiple suspicious (44,105) - ghost-protocol-https (5,330) - href domain doesn't match displayed domain (80) - exe many dos header anomalies (7) - escalation - multiple blacklist feed hits (1) - abnormal exe (1)

Service Type (20 of 20+ values)

OTHER (>100,000 - 78%) - DNS (>100,000 - 85%) - HTTP (>100,000 - 88%) - SSL (>100,000 - 88%) - NTP (58,620) - NETBIOS (49,237) - SMB (36,626) - SSH (20,711) - SNMP (14,514) - RPC (6,172) - DHCP (4,459) - FTP (4,216) - SIP (646) - RTP (347) - SMTP (142) - AOL IM (102) - RIP (52) - YAHOO IM (49) - RDP (49) - NFS (36) ... show more

Source IP Address (20 of 20+ values)

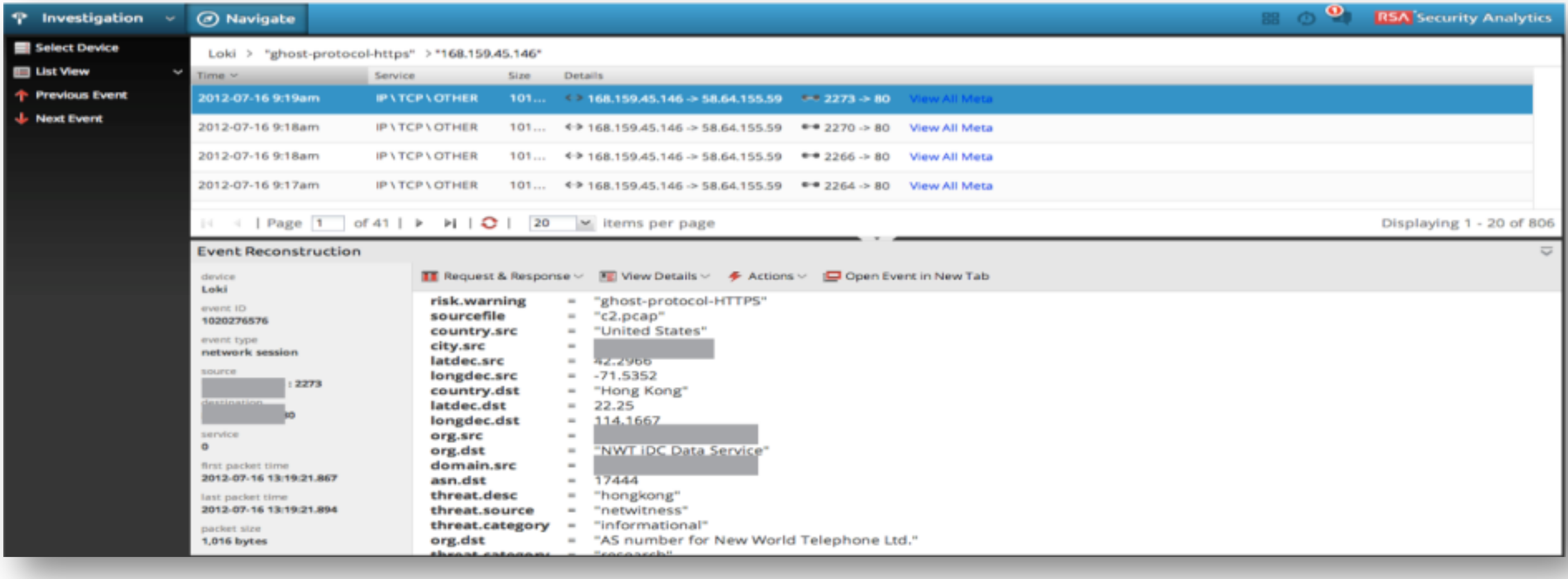
[redacted]

Destination IP address (20 of 20+ values)

[redacted]

Examples Of Findings

- Parser fused with organizational data to find compromised hosts within their environment
- Lateral movement indicative of promulgation found via host based forensic analysis



Loki > "ghost-protocol-https" > "168.159.45.146"

Time	Service	Size	Details		
2012-07-16 9:19am	IP \ TCP \ OTHER	101...	168.159.45.146 -> 58.64.155.59	2273 -> 80	View All Meta
2012-07-16 9:18am	IP \ TCP \ OTHER	101...	168.159.45.146 -> 58.64.155.59	2270 -> 80	View All Meta
2012-07-16 9:18am	IP \ TCP \ OTHER	101...	168.159.45.146 -> 58.64.155.59	2266 -> 80	View All Meta
2012-07-16 9:17am	IP \ TCP \ OTHER	101...	168.159.45.146 -> 58.64.155.59	2264 -> 80	View All Meta

| Page 1 of 41 | 20 items per page

Displaying 1 - 20 of 806

Event Reconstruction

device
Loki

event ID
1020276576

event type
network session

source
[redacted] : 2273

destination
[redacted]

service
0

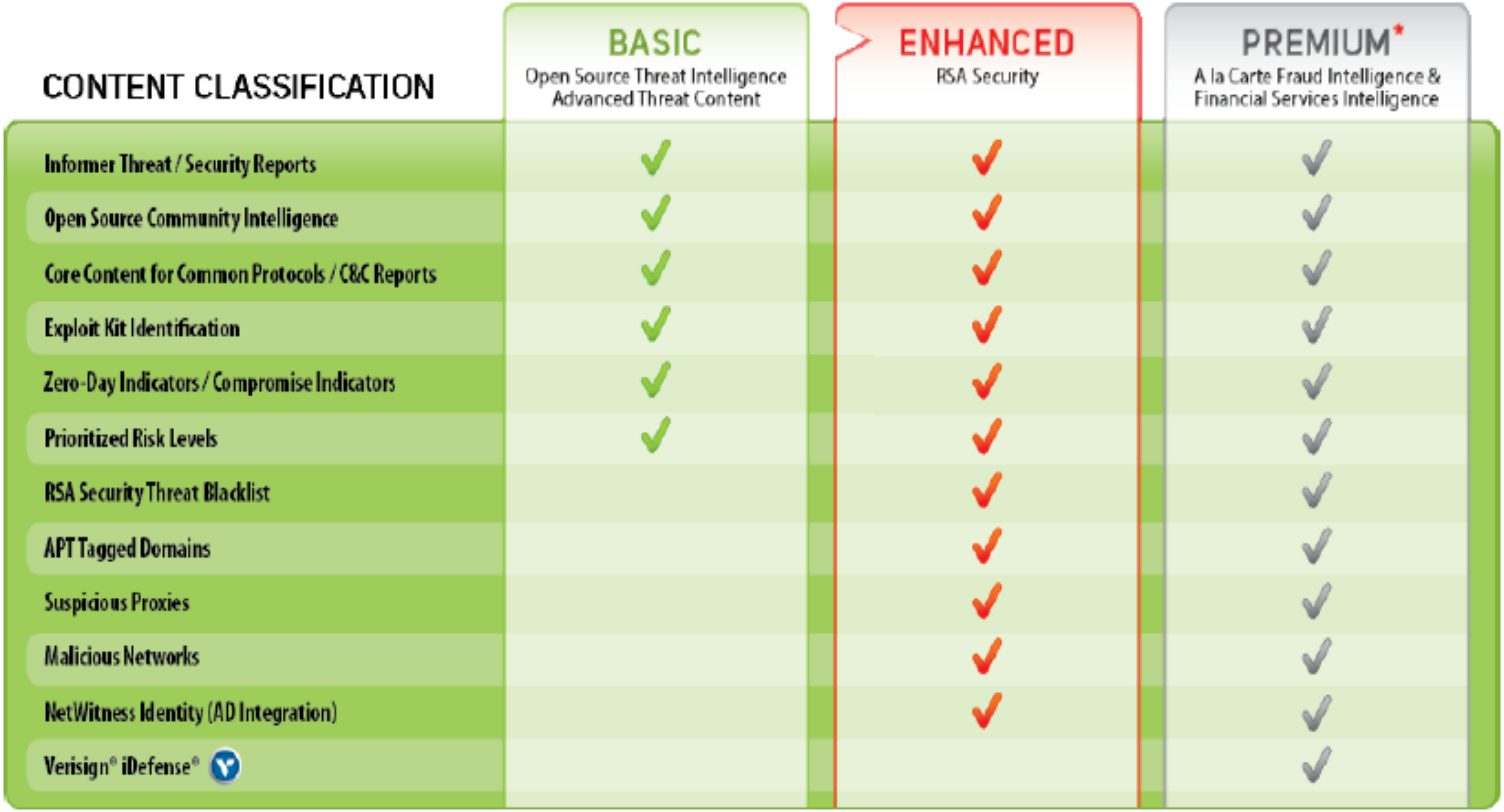
first packet time
2012-07-16 13:19:21.867

last packet time
2012-07-16 13:19:21.894

packet size
1,016 bytes

```
risk.warning     =  "ghost-protocol-HTTPS"
sourcefile       =  "c2.pcap"
country.src      =  "United States"
city.src         =  [redacted]
latdec.src       =  42.2966
longdec.src      =  -71.5352
country.dst      =  "Hong Kong"
latdec.dst       =  22.25
longdec.dst      =  114.1667
org.src          =  [redacted]
org.dst          =  "NWT iDC Data Service"
domain.src       =  [redacted]
asn.dst          =  17444
threat.desc      =  "hongkong"
threat.source    =  "netwitness"
threat.category  =  "informational"
org.dst          =  "AS number for New World Telephone Ltd."
threat.category  =  "research"
```

RSA Live Subscription Offering



CONTENT CLASSIFICATION	BASIC Open Source Threat Intelligence Advanced Threat Content	ENHANCED RSA Security	PREMIUM* A la Carte Fraud Intelligence & Financial Services Intelligence
Informer Threat / Security Reports	✓	✓	✓
Open Source Community Intelligence	✓	✓	✓
Core Content for Common Protocols / C&C Reports	✓	✓	✓
Exploit Kit Identification	✓	✓	✓
Zero-Day Indicators / Compromise Indicators	✓	✓	✓
Prioritized Risk Levels	✓	✓	✓
RSA Security Threat Blacklist		✓	✓
APT Tagged Domains		✓	✓
Suspicious Proxies		✓	✓
Malicious Networks		✓	✓
NetWitness Identity (AD Integration)		✓	✓
Verisign® iDefense®			✓

Summary: Intelligence Driven Security In Action

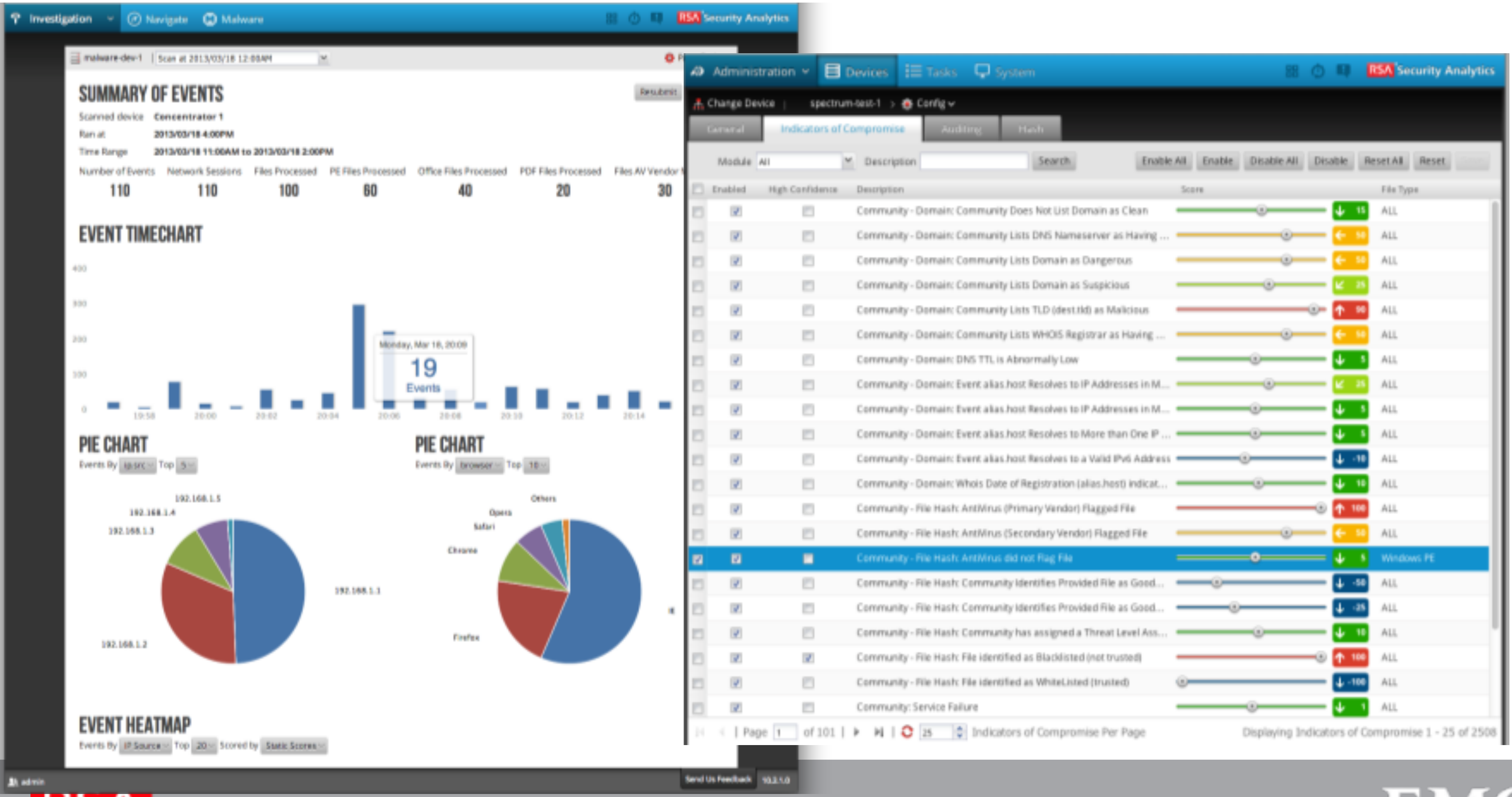
- Operationalized intelligence is far greater than detached intelligence
- Analysts need to understand what to look for and take advantage of what others have found
- Compare intelligence with historical data to see if indicators of compromise were found
- Apply in real-time to defend against future attacks

Taking A Closer Look

Malware Analysis

RSA Security Analytics Malware Analysis

An analytical workbench that utilizes multiple analytical methods to identification and analysis of malware-based attacks, including attacks not seen before.



malware-dev-1 | Scan at 2013/03/18 12:00AM

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
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

Change Device | spectrum-test-1 > Config

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

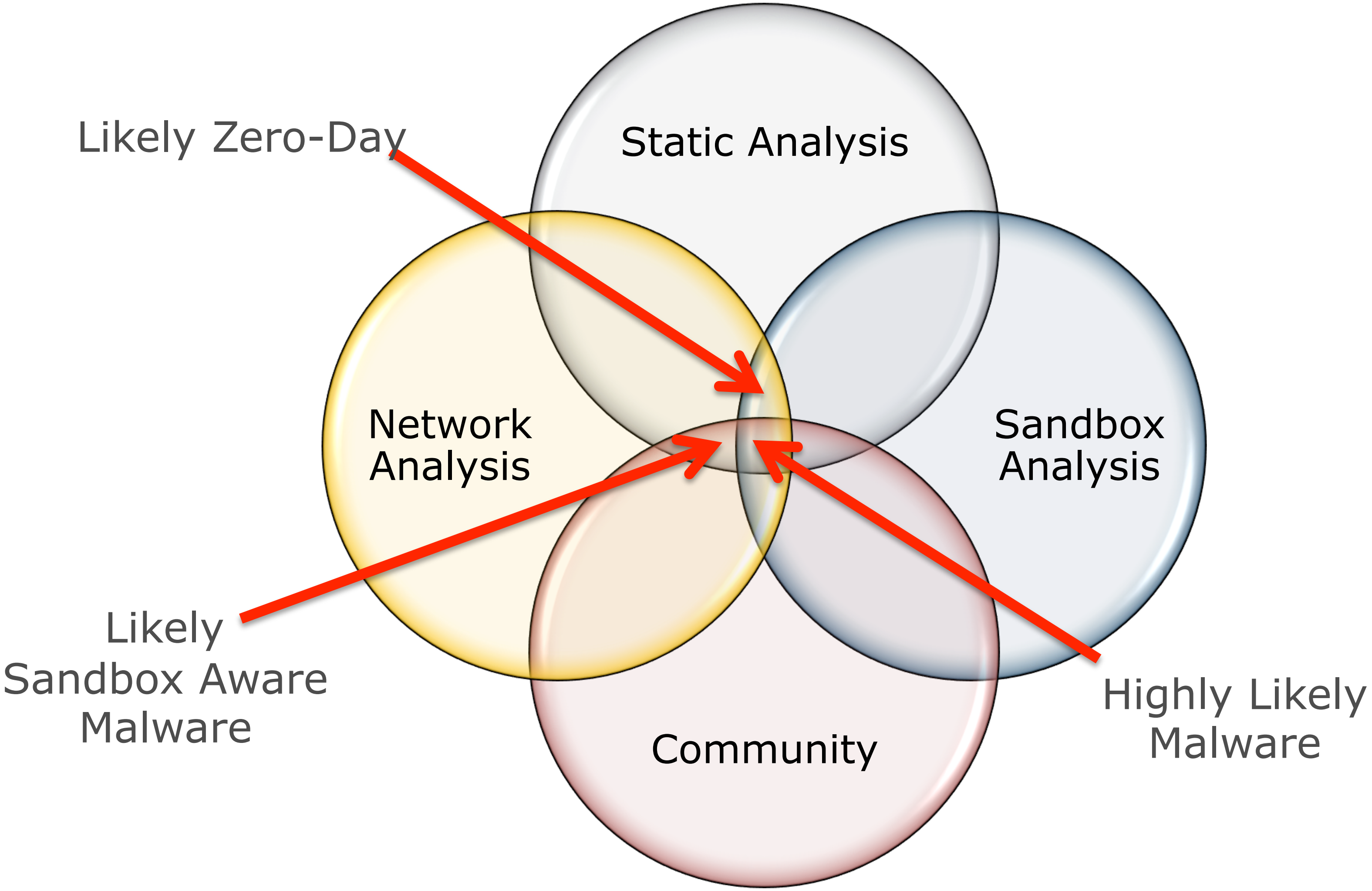
Displaying Indicators of Compromise 1 - 25 of 2508

Malware Analysis

- The widest spectrum of malware-based attacks, including zero-day attacks
  - Gain insight into attacks missed by both traditional and modern approaches to malware protection
  - Consider all the network data and behavior to provide the full context of an attack
- Analyze attacks by utilizing a wide spectrum of investigation techniques
  - Combine sandboxing, community intelligence, file content and network behavior analysis
  - Automatically answer thousands of questions to help determine an attacker’s intent, their potential targets and the level of threat they pose
- Increase the speed and accuracy of investigations
  - Replicate and automate the workflow of an advanced malware analyst
  - Save hours of work and ensure analysts focus on the most critical malware-related events

Malware Analysis

Multiple analytical methods in one tool



Replicate & Automate Advanced Analyst Workflow

NETWORK

Ask Hundreds of Questions About the Originating and Related Network Sessions

- Recursive and Referring Session Analysis
- Examples: Country of Origin, Time of Day, Size of Content, Referring Site, TLD and Country Match, JavaScript / Obfuscation, PDF Executable, Alerts present, Streaming Analysis of the Content, intelligence indicators, etc..

STATIC

Inspection for Signs of Malicious Code

- Static file content malware analysis
- Size, Meta Tags, Cleaned, Packed, Obfuscated, etc..

COMMUNITY

Community-based review by intelligence and reputation partners

- Extensible list of SaaS intelligence and whitelist partners
- Virus checking-providers, internet-based intelligence, known good/bad

SANDBOX

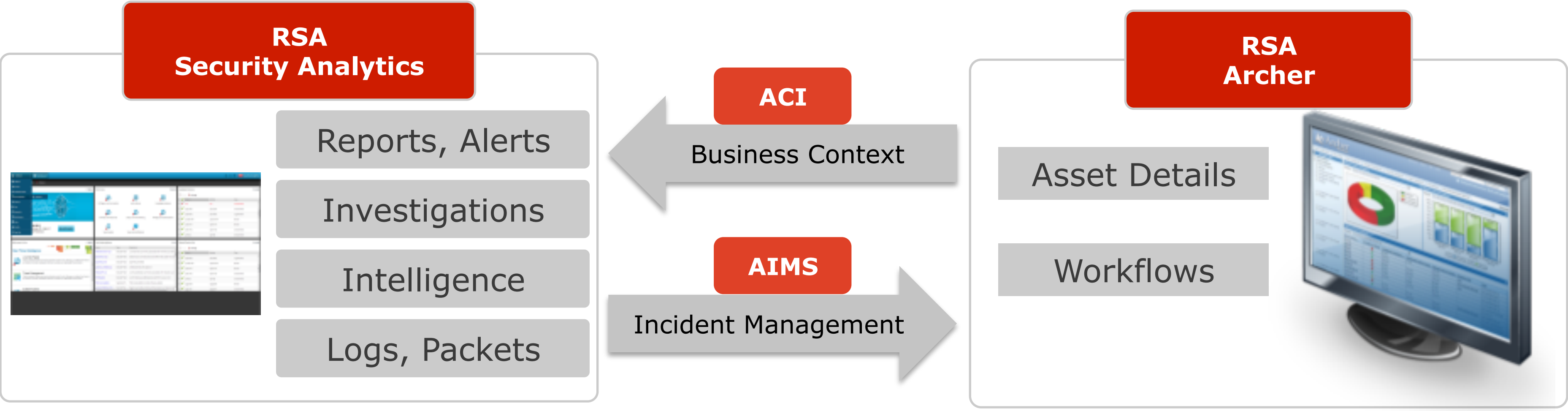
Local and cloud dynamic analysis

- Out-of-the-box integration with industry leading dynamic malware analysis sandbox
- On premise and cloud-based dynamic analysis modules

RSA Archer & DLP Integrations

Enabling Business Context and Advanced Incident Management for RSA Security Analytics

What is ACI and AIMS?



RSA Security Analytics

Reports, Alerts

Investigations

Intelligence

Logs, Packets

ACI

Business Context

AIMS

Incident Management

RSA Archer

Asset Details

Workflows

Asset Criticality Intelligence (ACI)

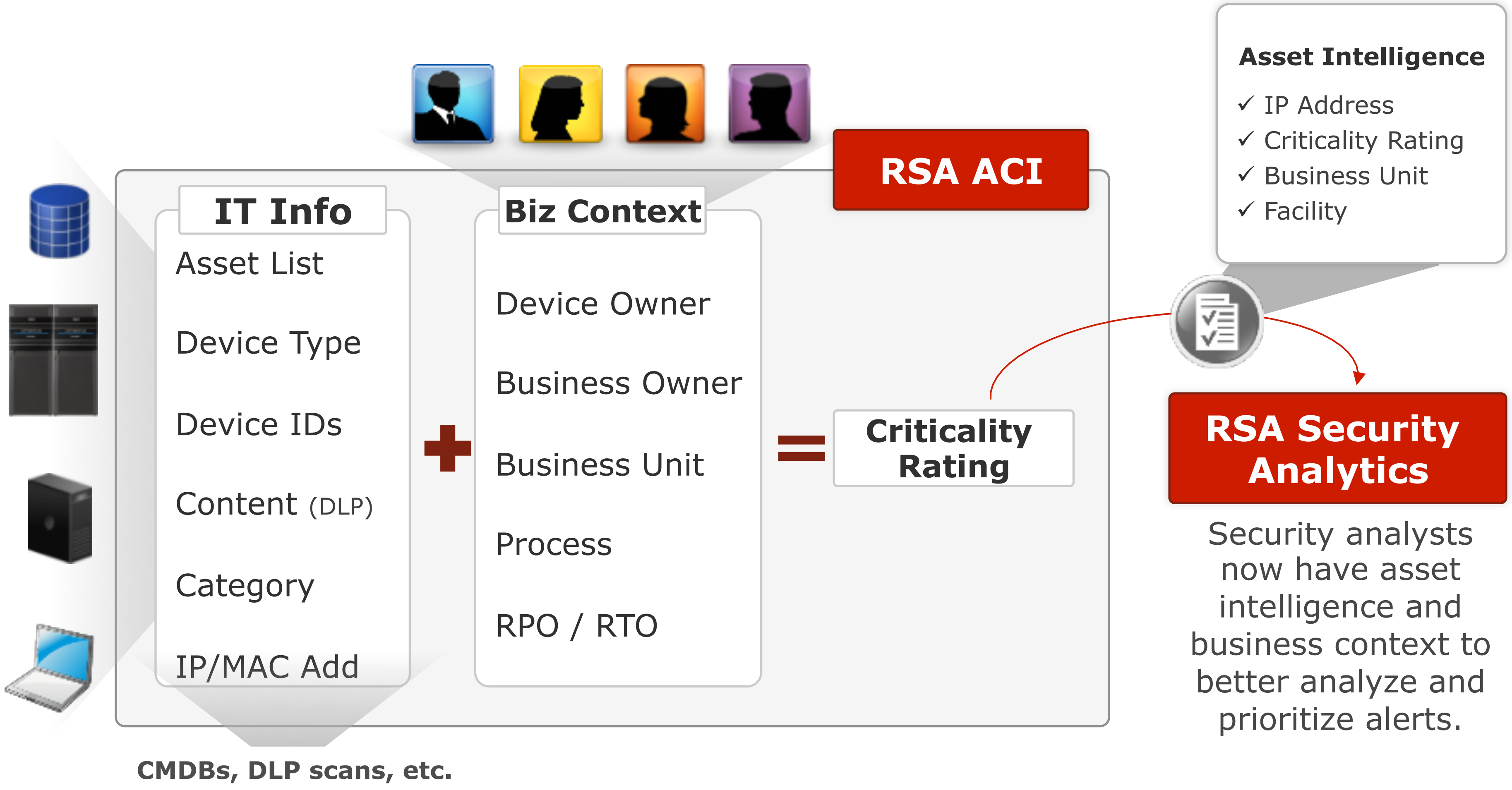
- Business Context to Security Analysts to Prioritize Investigations

Advanced Incident Management for Security (AIMS)

- Automate incident management workflow, effectively track progress and engage key business stakeholders

Asset Criticality Intelligence

Overview



Asset Intelligence

- ✓ IP Address
- ✓ Criticality Rating
- ✓ Business Unit
- ✓ Facility

RSA ACI

IT Info

Asset List

Device Type

Device IDs

Content (DLP)

Category

IP/MAC Add

+

Biz Context

Device Owner

Business Owner

Business Unit

Process

RPO / RTO

=

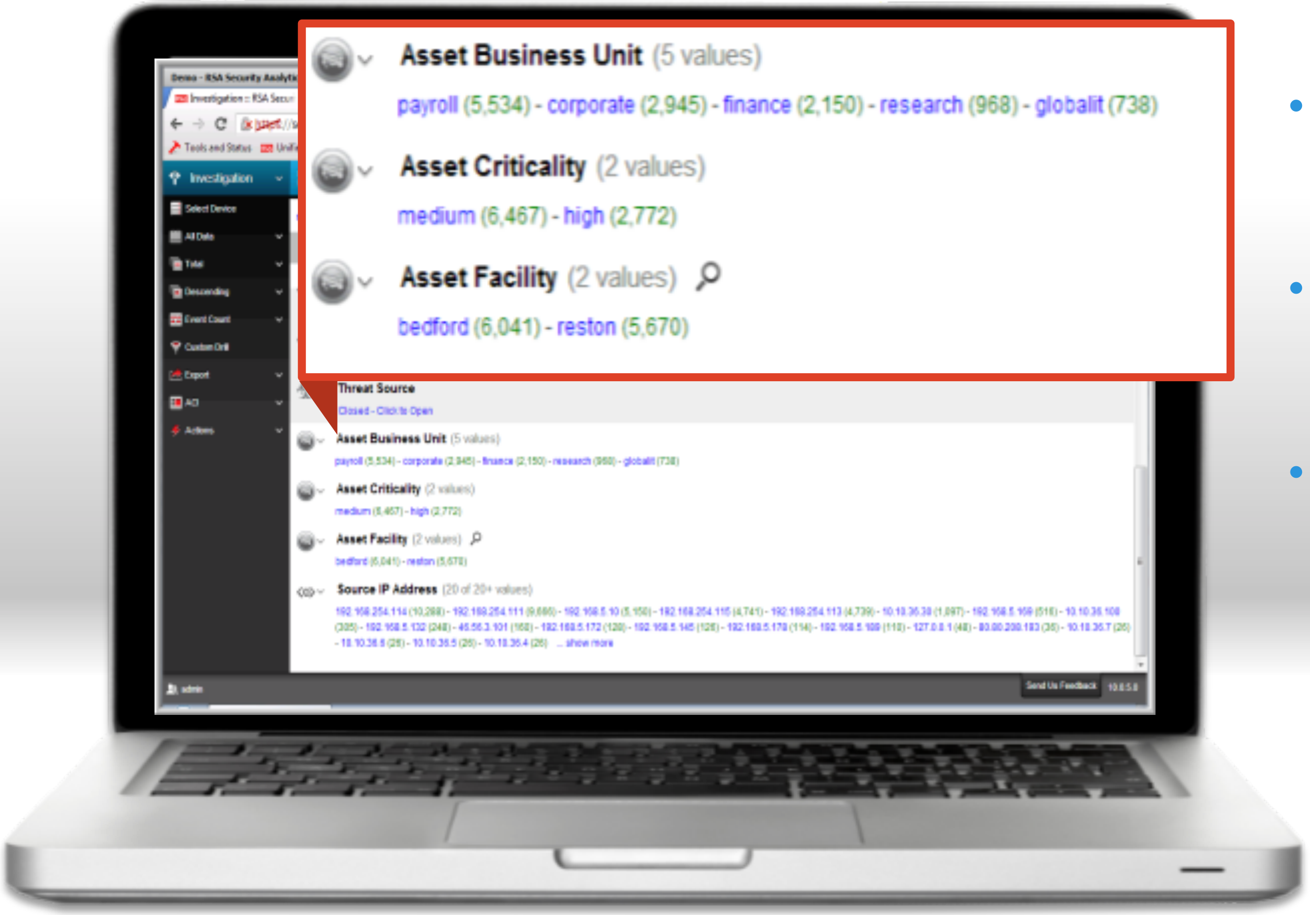
Criticality Rating

RSA Security Analytics

Security analysts now have asset intelligence and business context to better analyze and prioritize alerts.

CMDBs, DLP scans, etc.

Asset Criticality Intelligence in Security Analytics



Asset Business Unit (5 values)

payroll (5,534) - corporate (2,945) - finance (2,150) - research (968) - globalit (738)

Asset Criticality (2 values)

medium (6,467) - high (2,772)

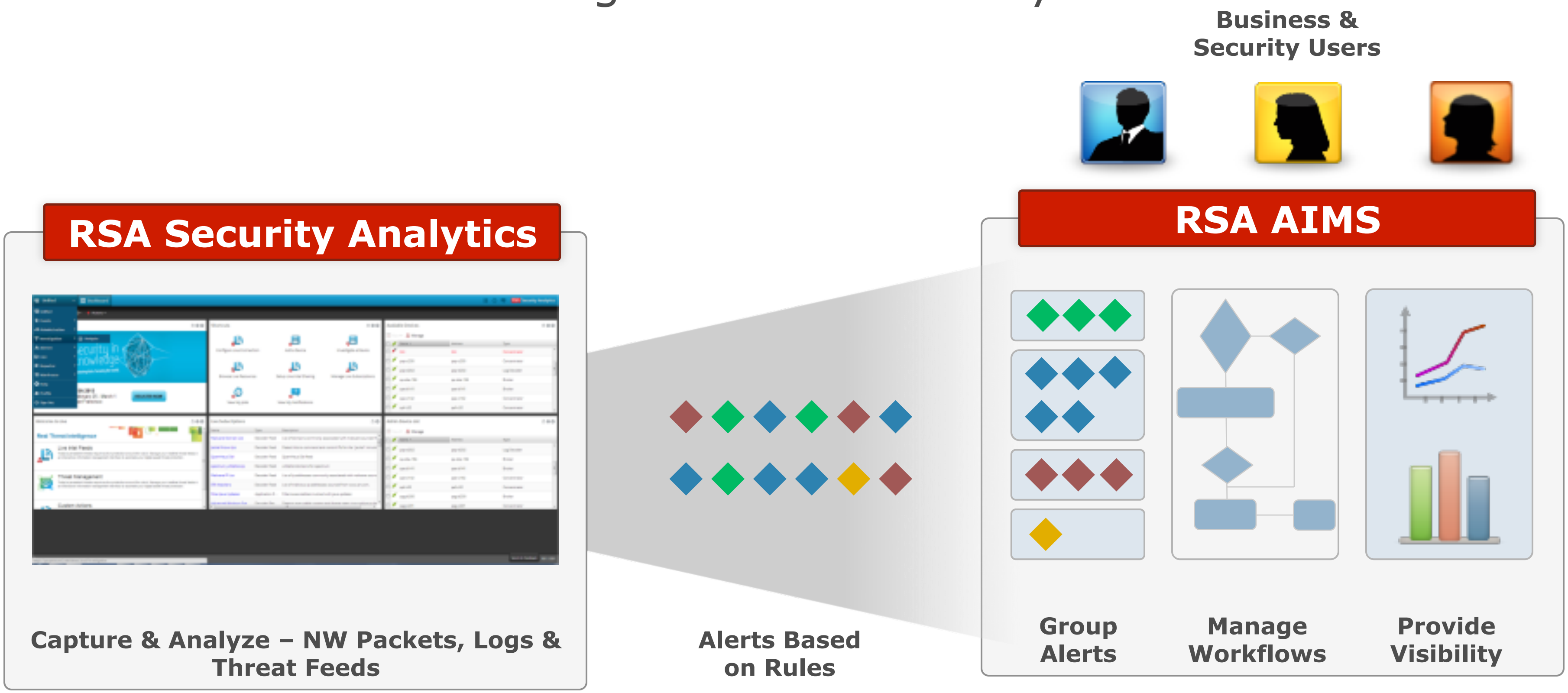
Asset Facility (2 values)

bedford (6,041) - reston (5,670)

- Helps analyst better understand risk
- To prioritize investigation & response
- Asset criticality represented as metadata

RSA AIMS Overview

Advanced Incident Management for Security



Business & Security Users

RSA Security Analytics

Capture & Analyze – NW Packets, Logs & Threat Feeds

Alerts Based on Rules

RSA AIMS

Group Alerts

Manage Workflows

Provide Visibility

Advanced Incident Management

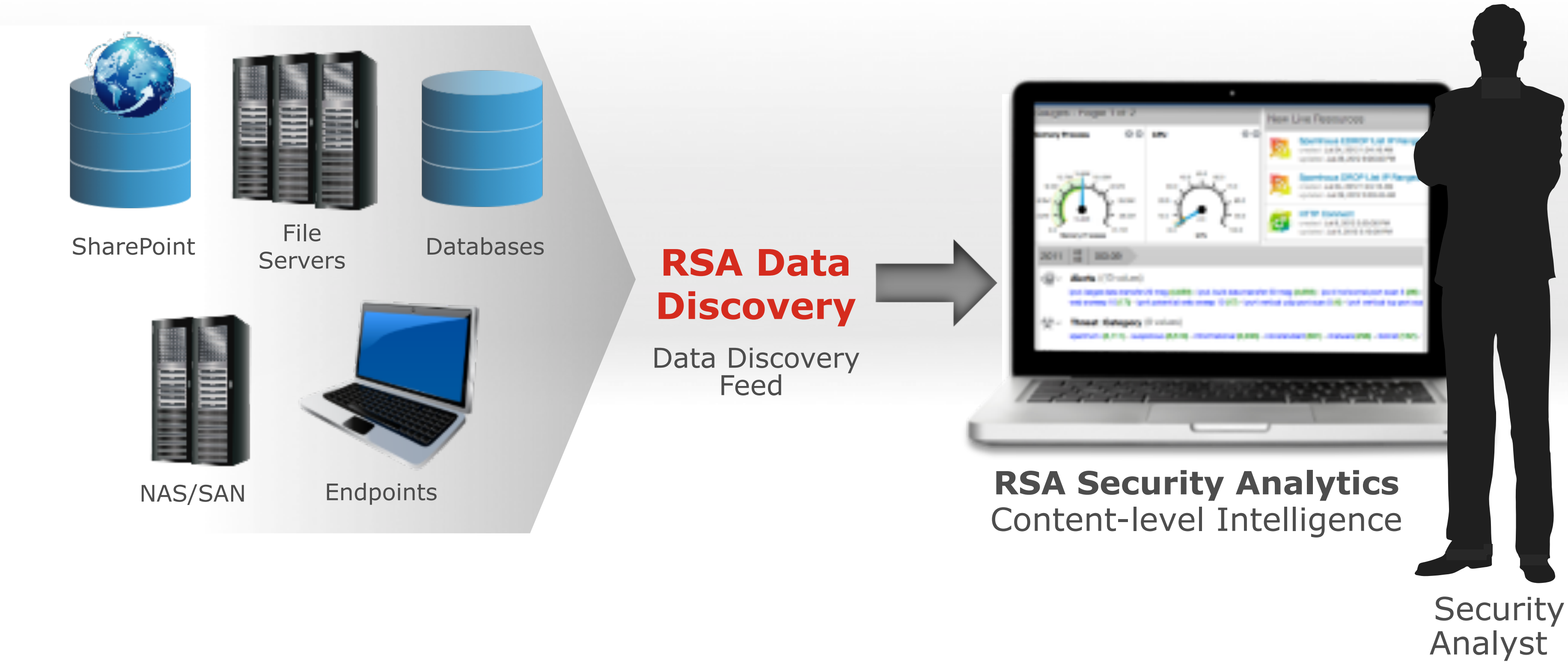
Incident ID	Date/Time Reported	Incident Summary	Priority	Status	Category	Affected Business Unit
[illegible]	10/20/2012 2:17 PM	test incident 2		New		
[illegible]	10/20/2012 2:17 PM	Test incident 1		New		
[illegible]	10/20/2012 2:00 PM	summary		New	Fraud Blackmail	

Investigation Owner	Count of Investigation Owner
Analyst, Joe	1
Hevlek, Scott	1

- Offload response from security analyst
- Enhances management visibility
- Accelerates remediation
- Manage entire incident lifecycle

RSA Data Discovery for Security Analytics

Discover sensitive data & improve investigations with DLP



SharePoint

File Servers

Databases

NAS/SAN

Endpoints

RSA Data Discovery

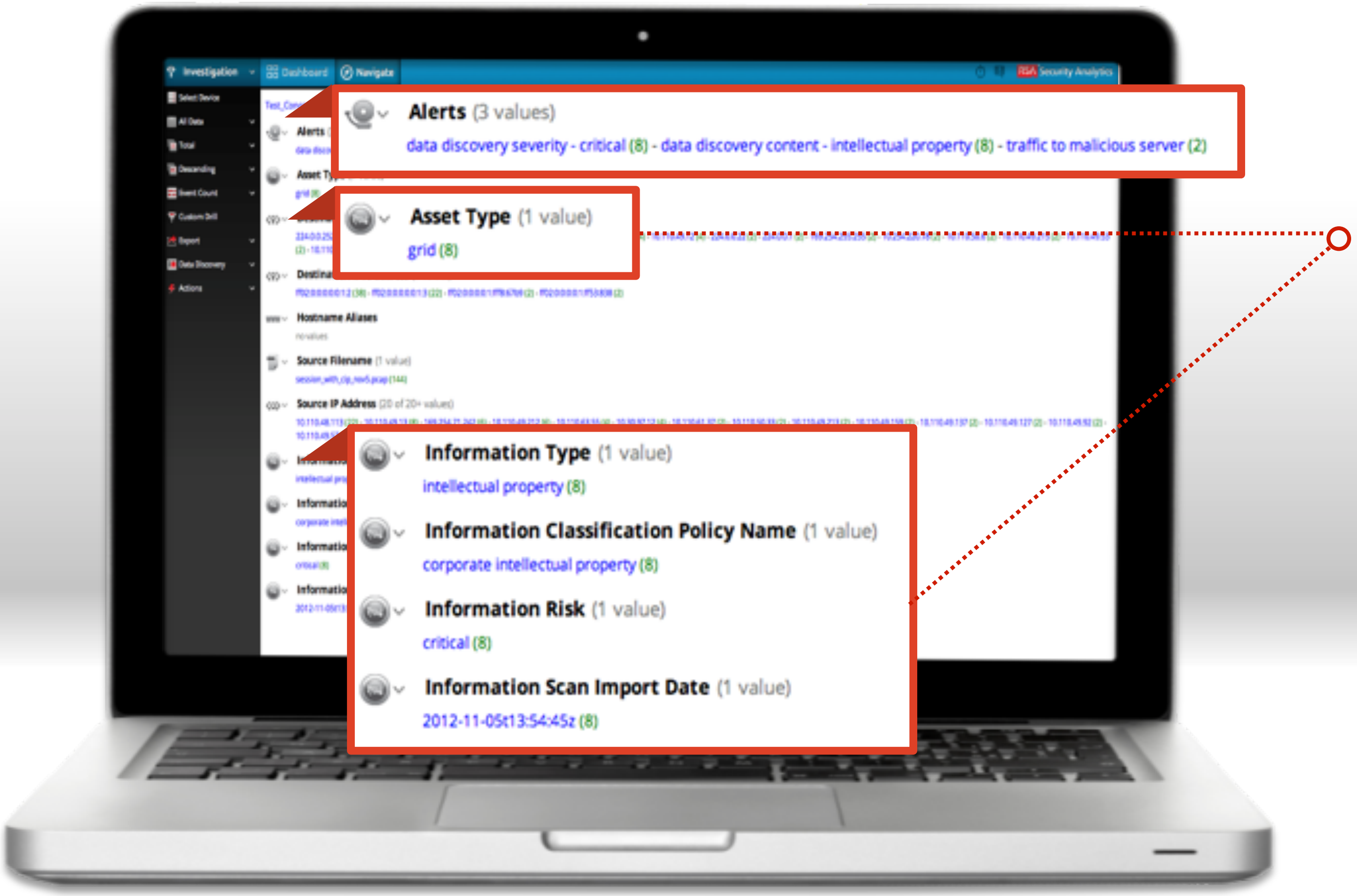
Data Discovery Feed

RSA Security Analytics
Content-level Intelligence

Security Analyst

RSA Data Discovery for Security Analytics

Investigative Interface



Alerts (3 values)

data discovery severity - critical (8) - data discovery content - intellectual property (8) - traffic to malicious server (2)

Asset Type (1 value)

grid (8)

Information Type (1 value)

intellectual property (8)

Information Classification Policy Name (1 value)

corporate intellectual property (8)

Information Risk (1 value)

critical (8)

Information Scan Import Date (1 value)

2012-11-05t13:54:45z (8)

Data Discovery attributes available in **SA Investigation** UI help Security Analysts identify high risk assets and prioritize investigations

Endpoint Visibility

RSA Security Analytics and RSA ECAT

Introducing RSA ECAT

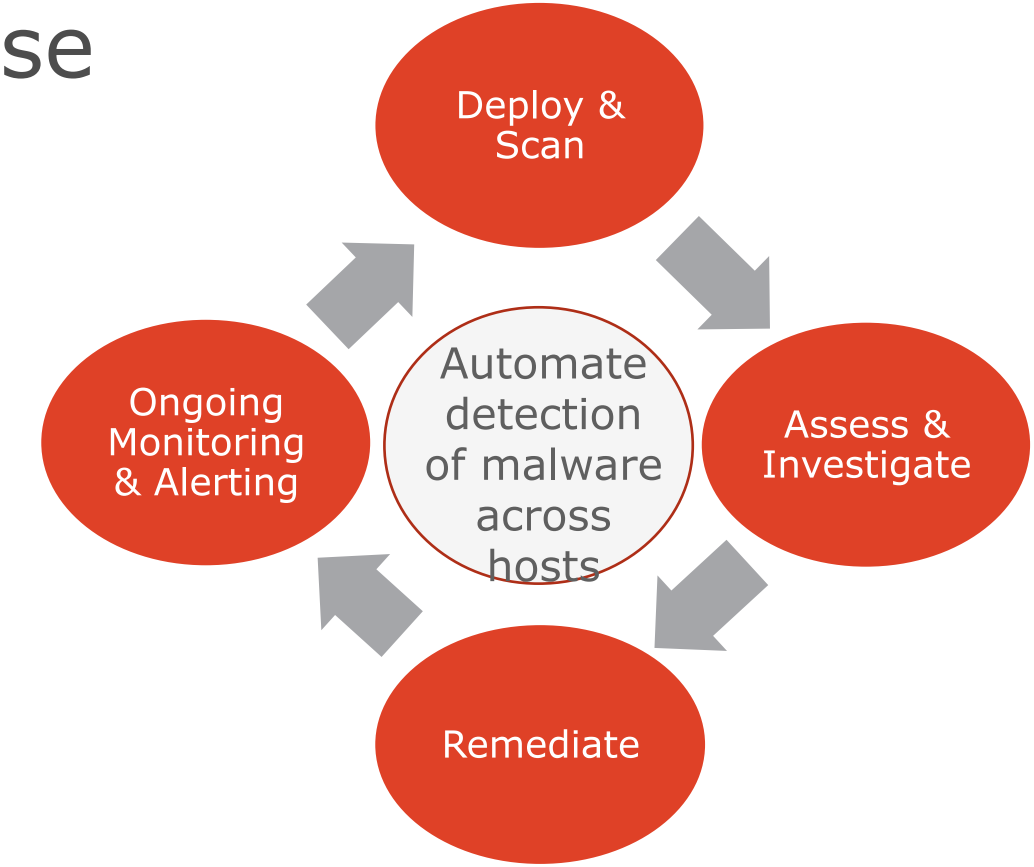
RSA ECAT

- ECAT= **E**nterprise **C**ompromise **A**ssessment **T**ool
- **Detect, Analyze & Respond** to advanced malware on endpoints

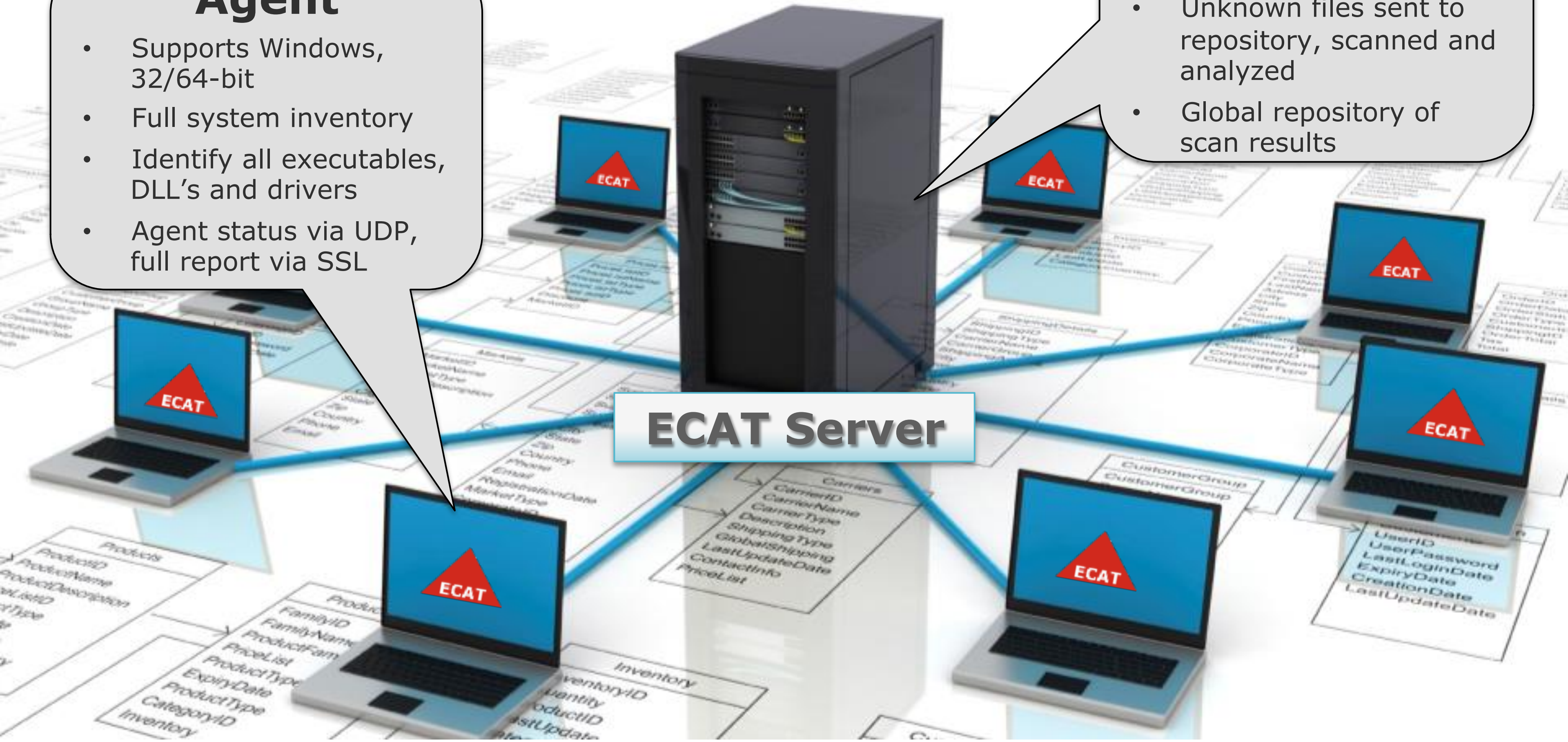
- Signature-less malware detection
- In-depth endpoint visibility
- Gain actionable intelligence for rapid breach detection
- Increase SOC/CIRC Efficiency

RSA ECAT: Use Cases

- Incident Response
- Assessments
- Monitoring


Deploy & Scan
Assess & Investigate
Remediate
Ongoing Monitoring & Alerting
Automate detection of malware across hosts

How RSA ECAT Works



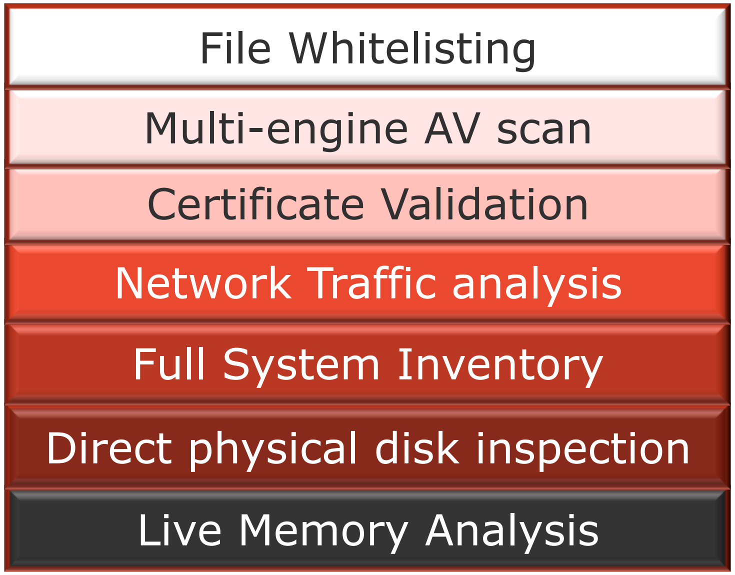
Agent

- Supports Windows, 32/64-bit
- Full system inventory
- Identify all executables, DLL's and drivers
- Agent status via UDP, full report via SSL

Server

- Up to 5K agents
- Scan report 0.5MB on the wire
- Unknown files sent to repository, scanned and analyzed
- Global repository of scan results

RSA ECAT Key Functionality & Benefits



File Whitelisting

Multi-engine AV scan

Certificate Validation

Network Traffic analysis

Full System Inventory

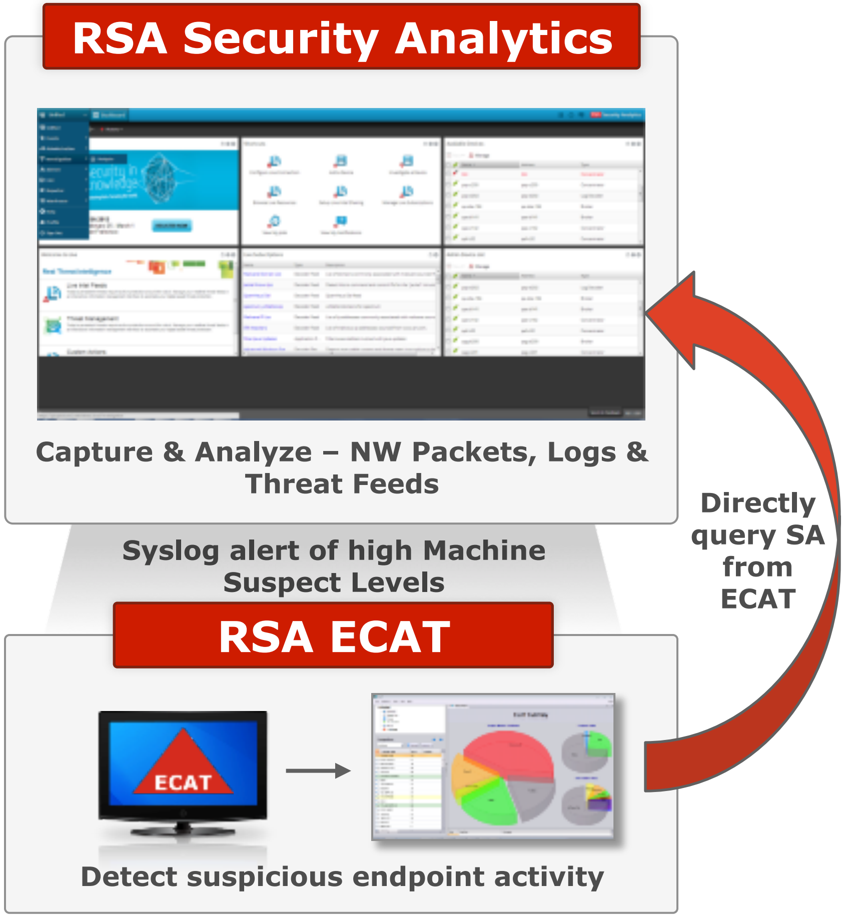
Direct physical disk inspection

Live Memory Analysis

- X-ray view of what’s happening on endpoints
- Identify behavior related to malware
- Highlight likely infections with Machine Suspect Level (MSL)
- Quickly triage results to gain actionable intelligence
- Find other infected machines & gauge scope of breach
- Forensic data gathering

Complete Endpoint & Network Visibility

RSA ECAT & RSA Security Analytics



RSA Security Analytics

Capture & Analyze – NW Packets, Logs & Threat Feeds

Syslog alert of high Machine Suspect Levels

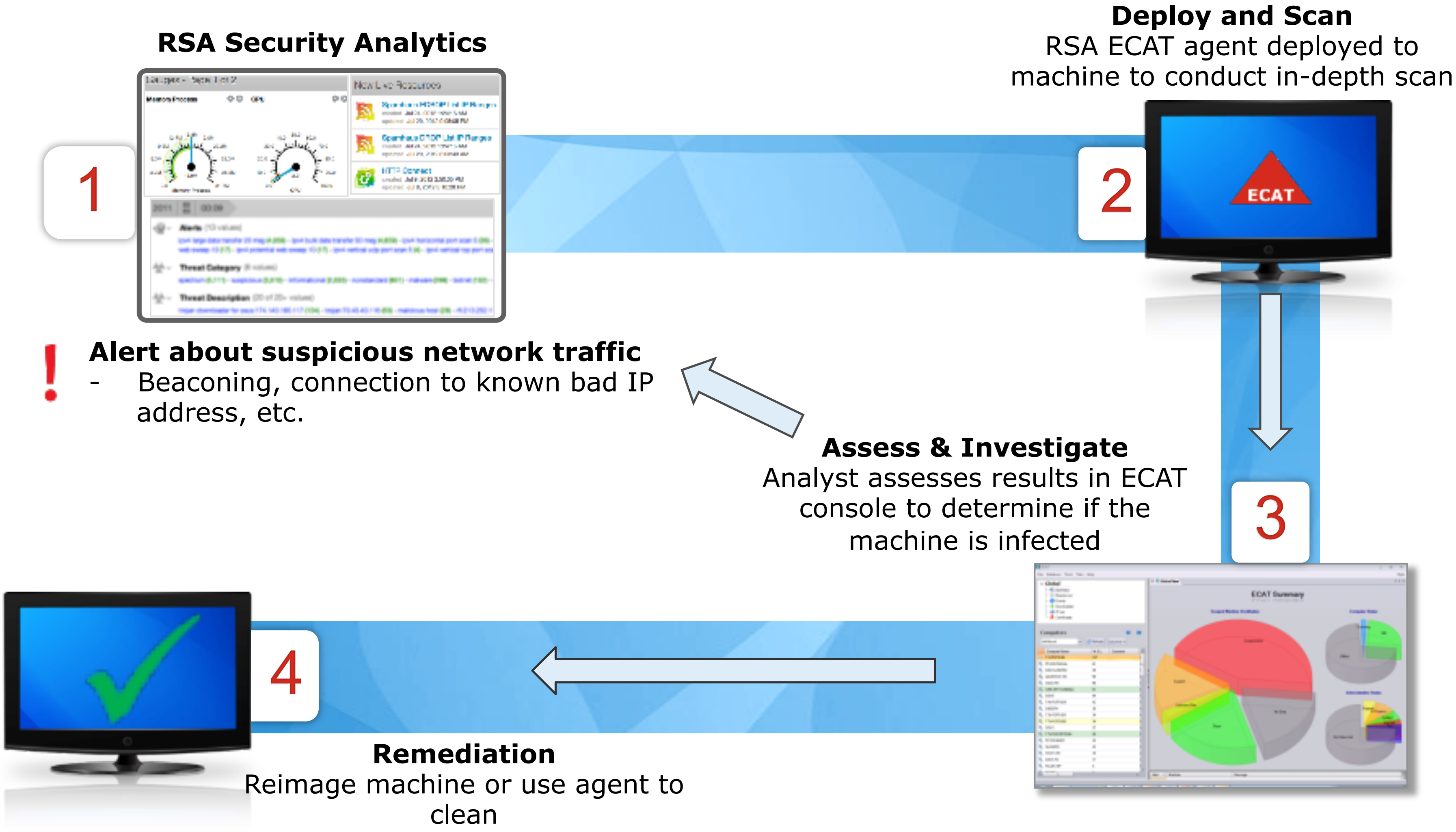
RSA ECAT

Detect suspicious endpoint activity

Directly query SA from ECAT

- Advanced threat detection on endpoints
- Complete network and endpoint visibility
- Faster investigations to shorten attacker dwell time

Incident Response



RSA Security Analytics

Alert about suspicious network traffic

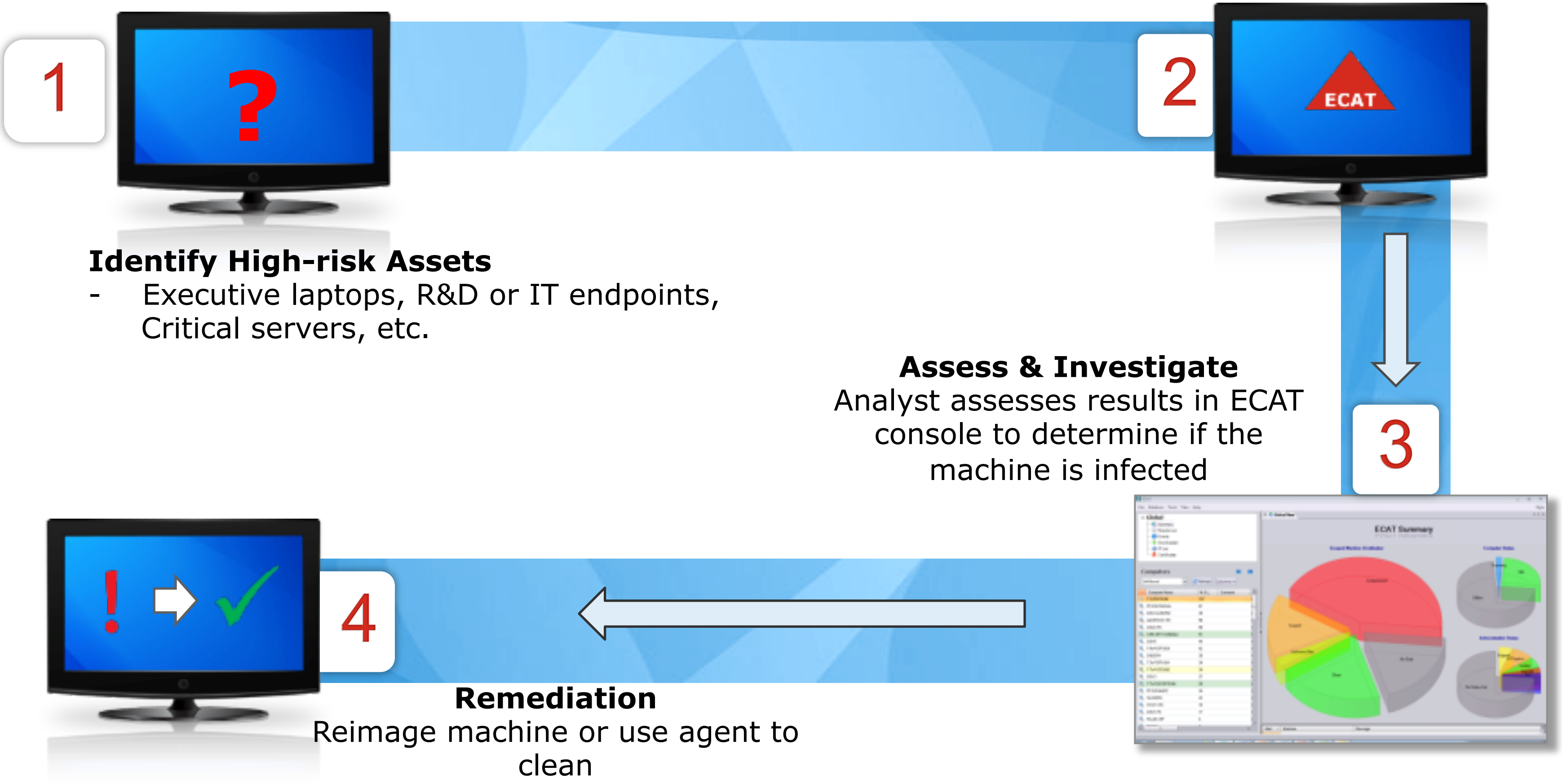
- Beaconing, connection to known bad IP address, etc.

Deploy and Scan
RSA ECAT agent deployed to machine to conduct in-depth scan

Assess & Investigate
Analyst assesses results in ECAT console to determine if the machine is infected

Remediation
Reimage machine or use agent to clean

Proactive Assessments



Deploy and Scan
RSA ECAT agent deployed to machine to conduct in-depth scan

Identify High-risk Assets

- Executive laptops, R&D or IT endpoints, Critical servers, etc.

Assess & Investigate
Analyst assesses results in ECAT console to determine if the machine is infected

Remediation
Reimage machine or use agent to clean

RSA®

EMC^2®