RSA Security Analytics

the complete approach to security monitoring
or how to approach advanced threats

Grzegorz Mucha
grzegorz.mucha@rsa.com

Advanced Threats

RSA EMC²

Threat Landscape

Criminals

Petty criminals

Unsophisticated

Organized crime

Organized, sophisticated supply chains (PII, financial services, retail)

Nation state actors

PII, government, defense industrial base, IP rich organizations

Non-state actors

Terrorists

PII, Government, critical infrastructure

Anti-establishment vigilantes

"Hacktivists" Targets of opportunity

RSA

EMC²

Threat Landscape

Of the 60 million variants

of malware in existence today

ONE-THIRD

were created last year alone

Source : RSA Security Brief, February 2011

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			

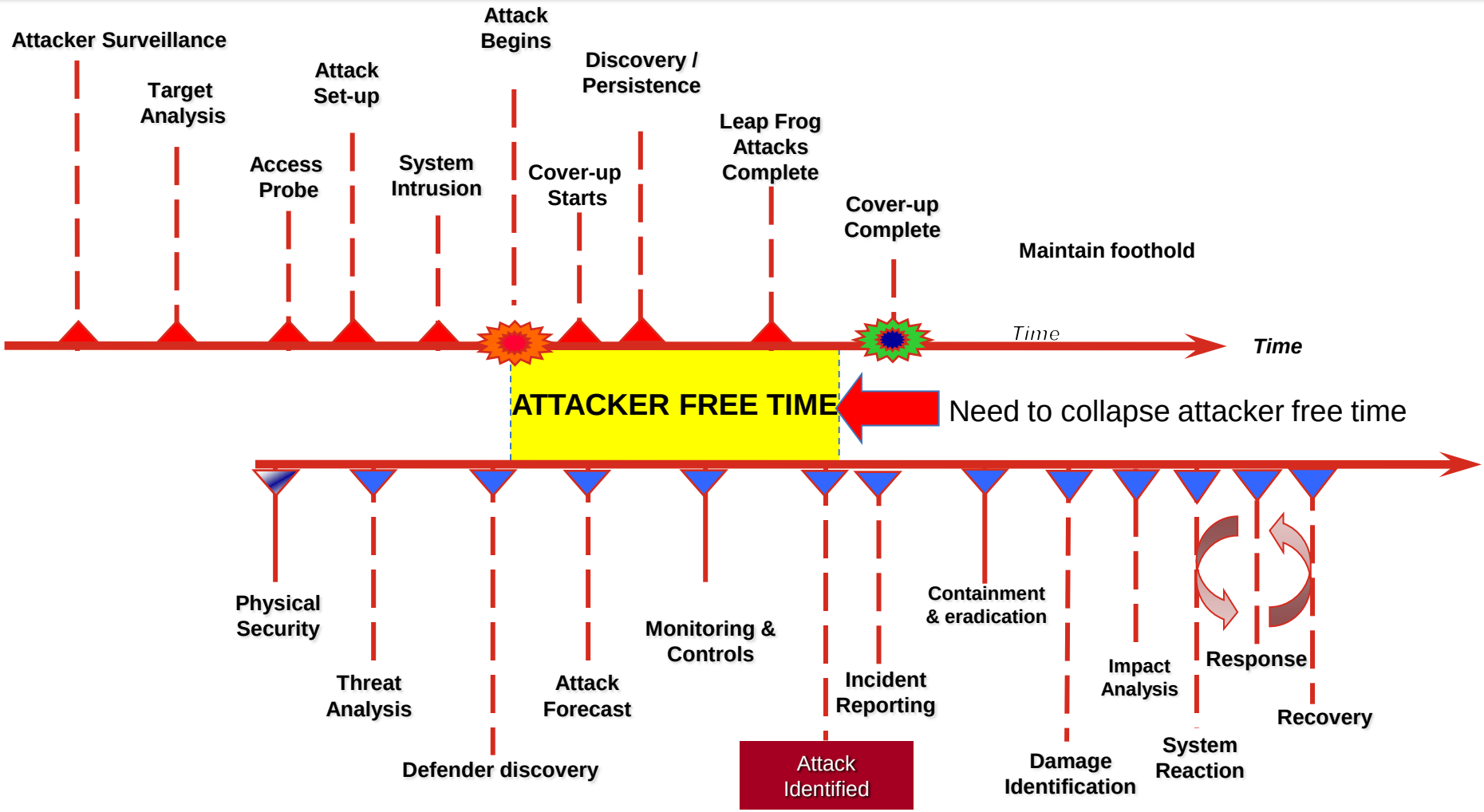
85% of breaches took “weeks” or more to discover

Source: Verizon 2012 Data Breach Investigations Report

Characteristics of advanced threats

- Single minded, determined and innovative
- Target individuals over systems
- Through reconnaissance will understand our processes, people & systems better than us
- Will exploit ANY weakness
- Countermeasures increase sophistication
- Custom malware, NOT detectable by signatures
- Are not in a hurry will take as long as it takes
- Goal is long term & persistent access

Model for advanced threat



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

Defending against APT

- Invest in detection and response, prevention alone is a failed strategy
- Develop detailed monitoring and response
- Solidify foundational controls and visibility
- Identify critical and high value assets
- Tune controls to protect critical assets

SIEM has been a good start

- SIEM can provide:
  - Valuable reporting on device and application activity
  - Basic alerting on known sequences (i.e. basic correlation)
  - Proof of compliance for internal and external auditors
  - Central view into disparate event sources being collected

In today's world…

Threats are multi-faceted, dynamic and stealthy

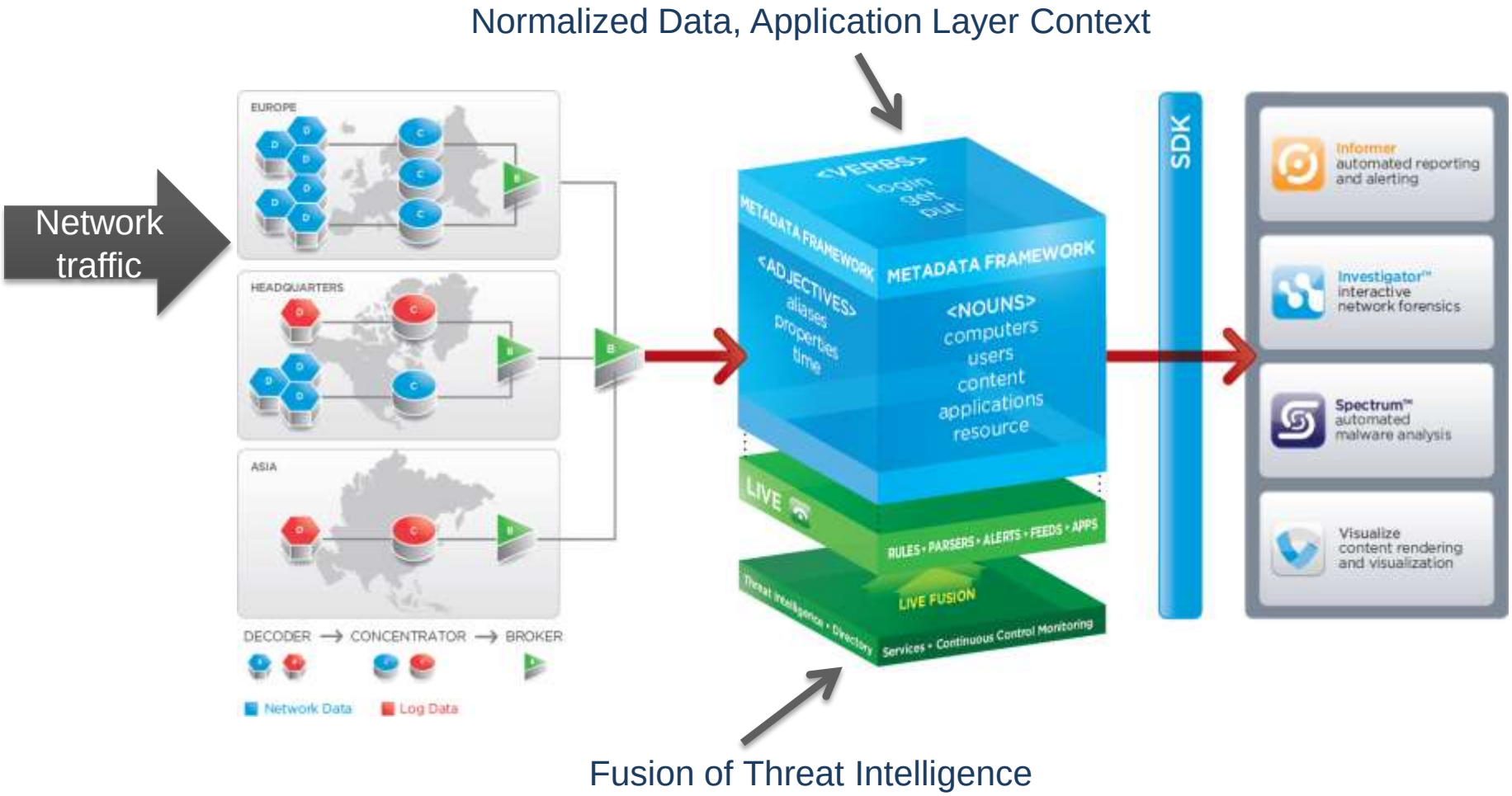
The most dangerous attacks have never been seen before

Threats often don't leave a footprint in logs

RSA NetWitness

gaining a total visibility of your network traffic

Let's start with RSA NetWitness Network Monitoring Platform



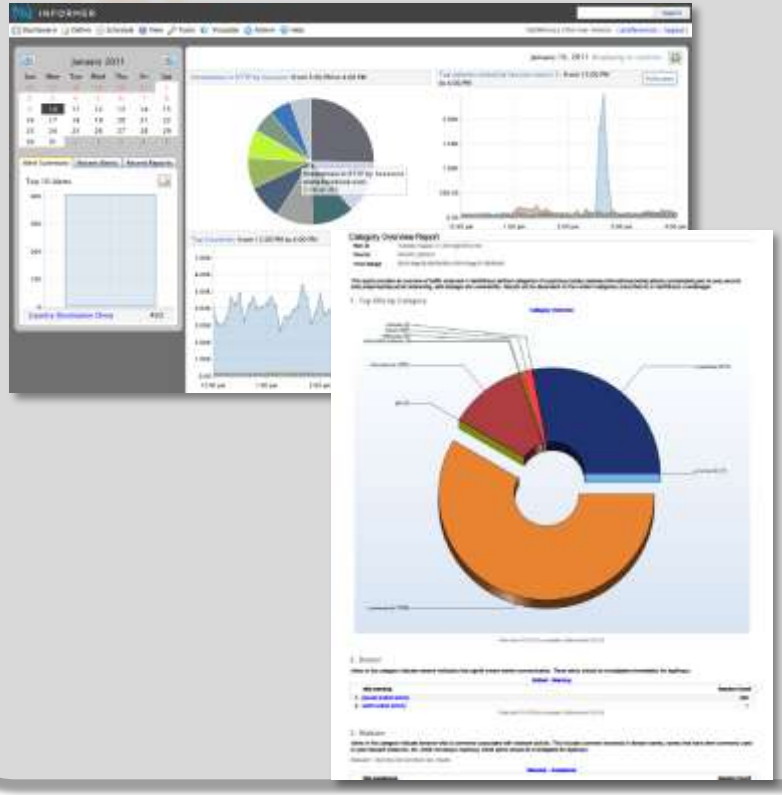
Getting Answers to the Toughest New Questions

Investigator

- Interactive data-driven session analysis of layer 2-7 content
- Award-winning, patented, port agnostic session analysis
- Infinite free-form analysis paths and content /context investigation points
- Data presented as the user experienced (Web, Voice, Files, Emails, Chats, etc.)
- Supports massive data-sets
  - Instantly navigate terabytes of data - analysis that once took days, now takes minutes
- Freeware version used by over 50,000 security experts worldwide

Automated Analysis, Reporting and Alerting

Informer



- Flexible dashboard, chart and summary displays for unified view of threat vectors
- Automated answers to any question:
  - Network Security
  - Security / HR
  - Legal / R&D / Compliance
  - I/T Operations
- HTML, CSV and PDF report formats included
- Supports CEF, SNMP, syslog, SMTP data push for full integration in SIEM

A New Way to Look at Information

Visualize

- Revolutionary visual interface to content on the network
  - Extracts and interactively presents images, files, objects, audio, and voice for analysis
  - Supports multi-touch, drilling, timeline and automatic “play” browsing
  - Rapid review and triage of content

Automated Malware Analysis and Prioritization

Spectrum

- Identify the widest spectrum of malware-based attacks
  - Gain insight into attacks missed by both traditional and modern approaches to malware protection
- Analyze attacks by utilizing a wide spectrum of investigation techniques
  - Combine four distinct investigation techniques
  - Automatically answer thousands of questions about the behavior of files
- Increase the speed and accuracy of investigations

NetWitness Live – How It Works

- NetWitness partners with the most trusted and reliable content providers in the security community, including our own research team
- Content Management System (CMS) is a cloud based environment aggregating and consolidating only the more pertinent information
- LiveManager's configurable dashboard enables a user to easily manage their content, subscriptions and search priorities
- Content can be automatically pushed into your NetWitness infrastructure

DEMO

Example: SpearPhish Attack

How Do You Cope With New Threats?

Subject: DPRK has carried out nuclear missile attack on Japan

Office of the Director of National Intelligence
INTELLIGENCE BULLETIN
UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U//FOUO) DPRK has carried out nuclear missile attack on Japan

05 March 2010

(U//FOUO) Prepared by Defense Intelligence Agency

(U//FOUO) Today, March 05, 2010 at 01.41 AM local time (UTC/GMT -5 hours), US seismographic stations recorded seismic activity in the area of Okinawa Island (Japan). According to National Geospatial-Intelligence Agency, Democratic People's Republic of Korea has carried out an average range missile attack with use of nuclear warhead. The explosion caused severe destructions in the northern part of the Okinawa island. Casualties among the personnel of the US military base are being estimated at the moment.

(U//FOUO) In connection with the occurred events, it is necessary for the personnel of the services listed below to be ready for immediate mobilization:

CENTRAL INTELLIGENCE AGENCY
Phone: (703) 482-0623

DEFENSE INTELLIGENCE AGENCY
Phone: (202) 231-8601
Email: DIA-PAO@dia.mil

DEPARTMENT OF ENERGY:
OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE
Phone: 1-202-586-5000
Email: The.Secretary@hq.doe.gov

DEPARTMENT OF HOMELAND SECURITY:
OFFICE OF INTELLIGENCE AND ANALYSIS
Phone: (202) 282-8000

DEPARTMENT OF STATE:
BUREAU OF INTELLIGENCE AND RESEARCH
Phone: (202) 647-4000

DEPARTMENT OF THE TREASURY:
OFFICE OF INTELLIGENCE AND ANALYSIS
Phone: (202) 622-2000

DRUG ENFORCEMENT ADMINISTRATION:
OFFICE OF NATIONAL SECURITY INTELLIGENCE
Phone: (202) 307-1000

FEDERAL BUREAU OF INVESTIGATION
NATIONAL SECURITY BRANCH
Phone: (202) 324-3000

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
Phone: (703) 755-5900

NATIONAL RECONNAISSANCE OFFICE
Phone: (703) 808-1198

NATIONAL SECURITY AGENCY
Phone: 1-800-688-6115
Email: NIASC@nsa.gov

UNITED STATES AIR FORCE
Phone: (251) 441-6215/6211

UNITED STATES ARMY
Phone: 1-888-550-2769

UNITED STATES COAST GUARD
Phone: (202) 372-2100

UNITED STATES MARINE CORPS
Phone: (202) 372-4411

UNITED STATES NAVY
Phone: (202) 372-2020

(U//FOUO) Additional information can be found in the following report:

http://dnicenter.com/docs/report.zip

Office of the Director of National Intelligence
Washington, D.C. 20511

End-user behavior, lack of visibility, and network realities create a gap

RSA

EMC²

Zero-Day : Your A/V security has failed

- You can't rely only upon preventative tools
- Only 1 of 42 AV vendors identified the file as malicious on 03.05.2010 (virustotal.com)
- AV disabled by overwriting the host file, vendor updates routed to 127.0.0.1
- Result: if AV didn't pick up the malware initially, it never will

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
127.0.0.1 downloads-eu1.kaspersky-labs.com
127.0.0.1 downloads2.kaspersky-labs.com
127.0.0.1 downloads4.kaspersky-labs.com
127.0.0.1 downloads1.kaspersky-labs.com
127.0.0.1 downloads-us1.kaspersky-labs.com
127.0.0.1 rads.mcafee.com
127.0.0.1 liveupdate.symanteclive update.com
127.0.0.1 liveupdate.symantec.com
127.0.0.1 liveupdate.symantec.d4p.net
127.0.0.1 update.symantec.com
```

File **report.exe** received on **2010.03.05 14:01:07 (UTC)**
Current status: **finished**
Result: **1/42 (2.38%)**

Compact | Print results

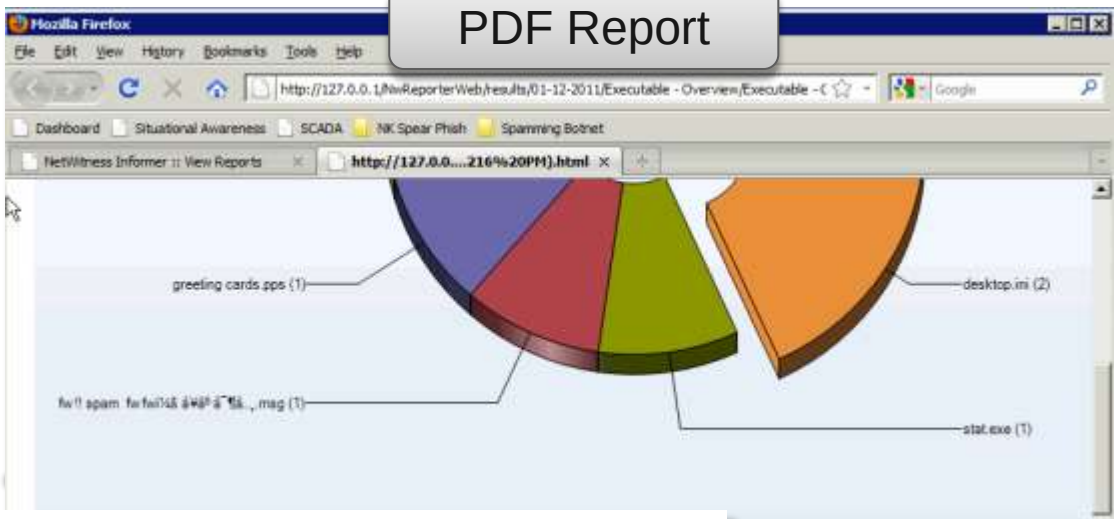
Antivirus	Version	Last Update	Result
a-squared	4.5.0.50	2010.03.05	-
AhnLab-V3	5.0.0.2	2010.03.05	-
AntiVir	8.2.1.180	2010.03.05	-
Antiy-AVL	2.0.3.7	2010.03.05	-
Authentium	5.2.0.5	2010.03.05	-
Avast	4.8.1351.0	2010.03.05	-
Avast5	5.0.332.0	2010.03.05	-
AVG	9.0.0.730	2010.03.05	-
BitDefender	7.2	2010.03.05	-
CAT-QuickHeal	10.00	2010.03.05	-
ClamAV	0.96.0.0-git	2010.03.05	-
Comodo	4091	2010.02.28	-
DrWeb	5.0.1.12222	2010.03.05	-
eSafe	7.0.17.0	2010.03.04	-
eTrust-Vet	35.2.7341	2010.03.05	-
F-Prot	4.5.1.85	2010.03.04	-
F-Secure	9.0.15370.0	2010.03.05	-
Fortinet	4.0.14.0	2010.03.04	-
GData			
Ikarus			
Jiangmin			
K7AntiVirus			
Kaspersky			
McAfee			
McAfee+Artemis			
McAfee-GW-Edition			
Microsoft			
NOD32	4918	2010.03.05	-
Norman	6.04.08	2010.03.05	-
nProtect	2009.1.8.0	2010.03.05	-

Let's take a look at how your world looks with NetWitness…

Informer – Your Automated Analyst

Informer uses NetWitness infrastructure to produce unique security reports and alerts – in this case intersecting multiple content-based indicators to escalate a potential incident

PDF Report



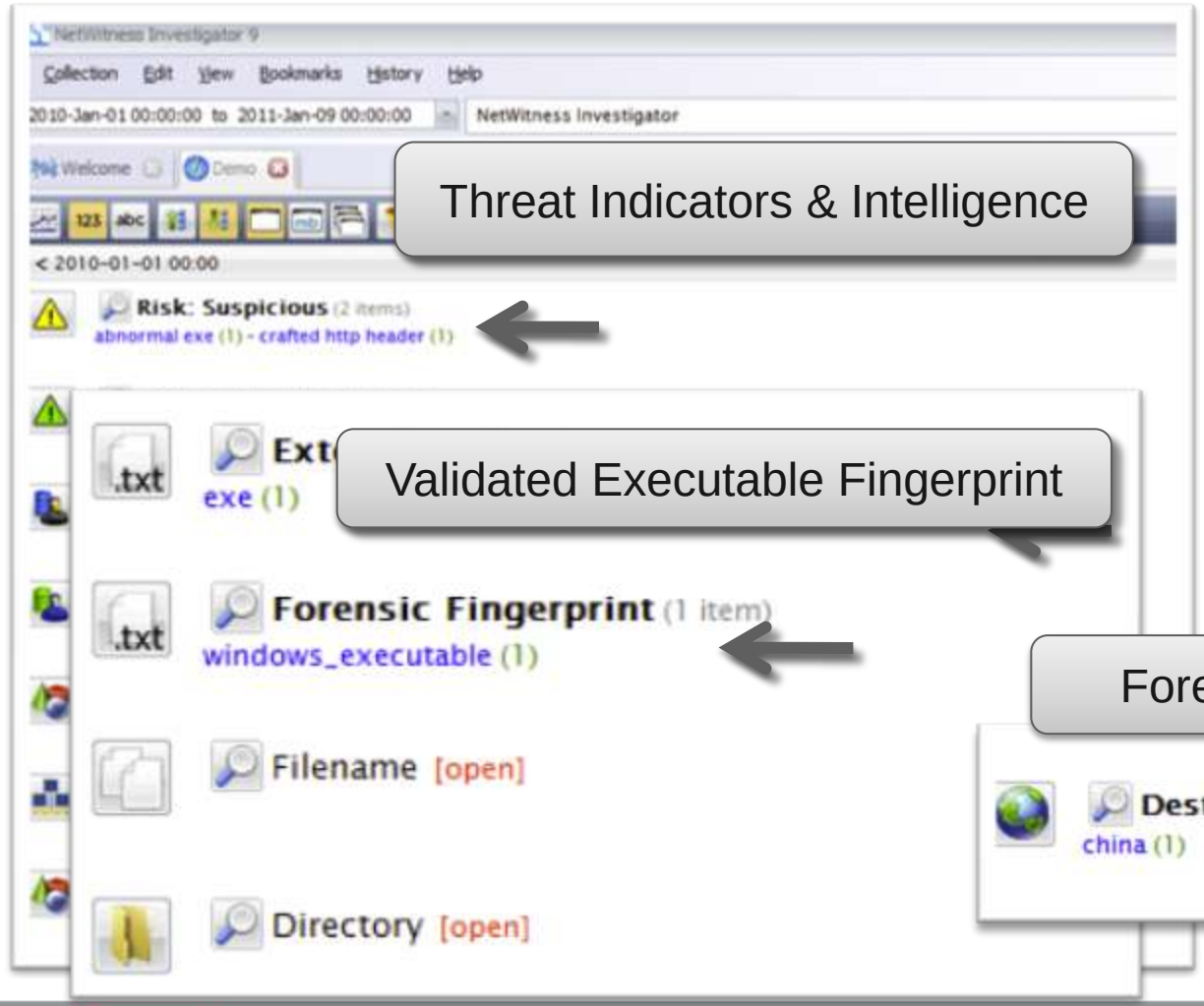
Executables from blacklisted hosts - All

filename
1. stat.exe
1. risk.suspicious abnormal exe
2. risk.suspicious crafted http header
1. threat.source malwaredomainlist-domain
2. threat.source zeustracker-domain
3. threat.source netwitness
4. threat.source malwaredomains.com
1. ip.src 192.168.0.32
1. ip.dst 115.100.250.105
1. org.dst beijing yiliyou date co.,ltd.
1. alias.host updatekernel.com

Rule took 0:0:0.406 to complete. (Actions took 0:0:5.359)

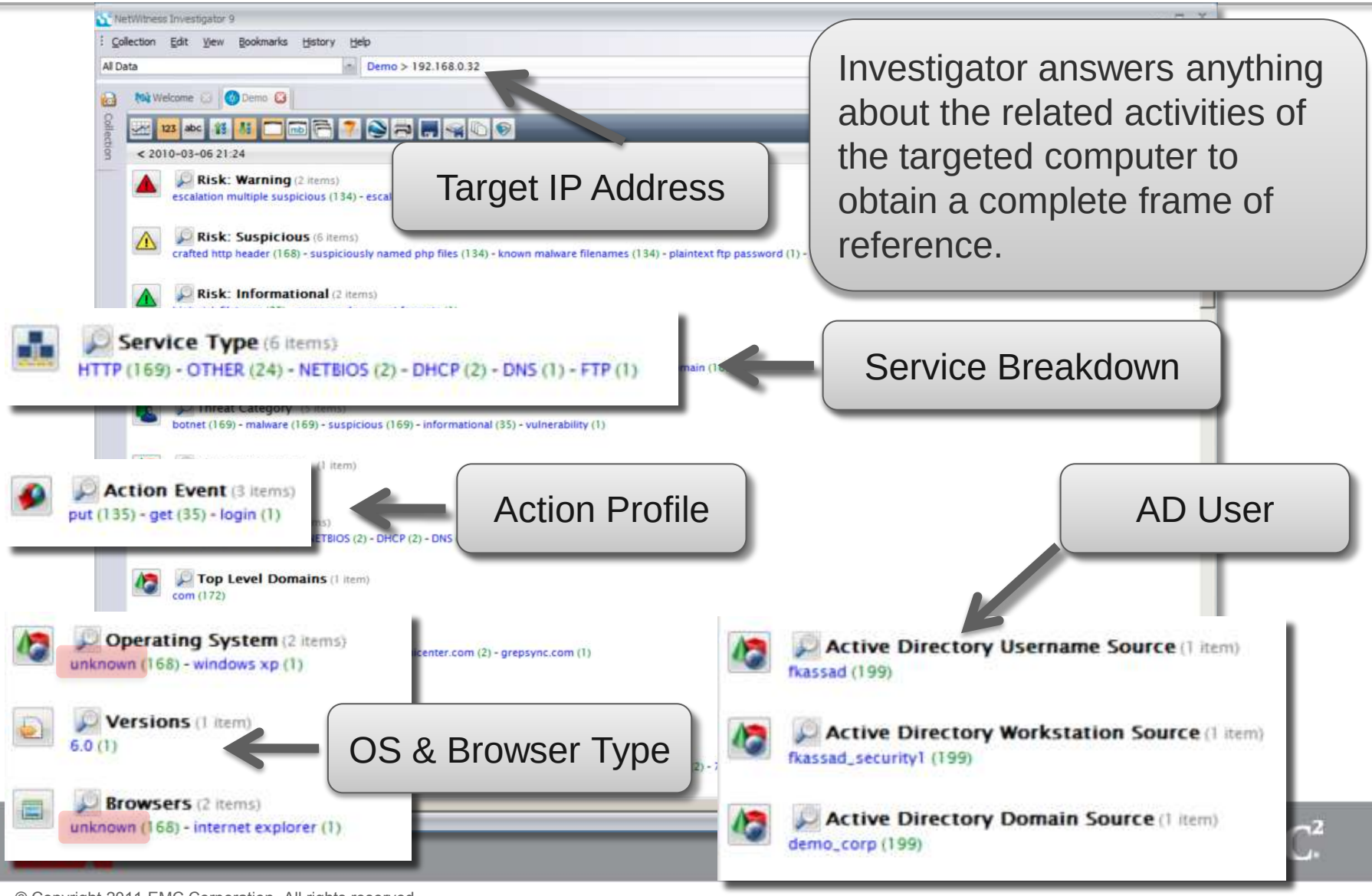
-Abnormal EXE structure
-Global Security Intelligence
-Crafted header
-Foreign Country

Precise Detail and Context with Investigator™

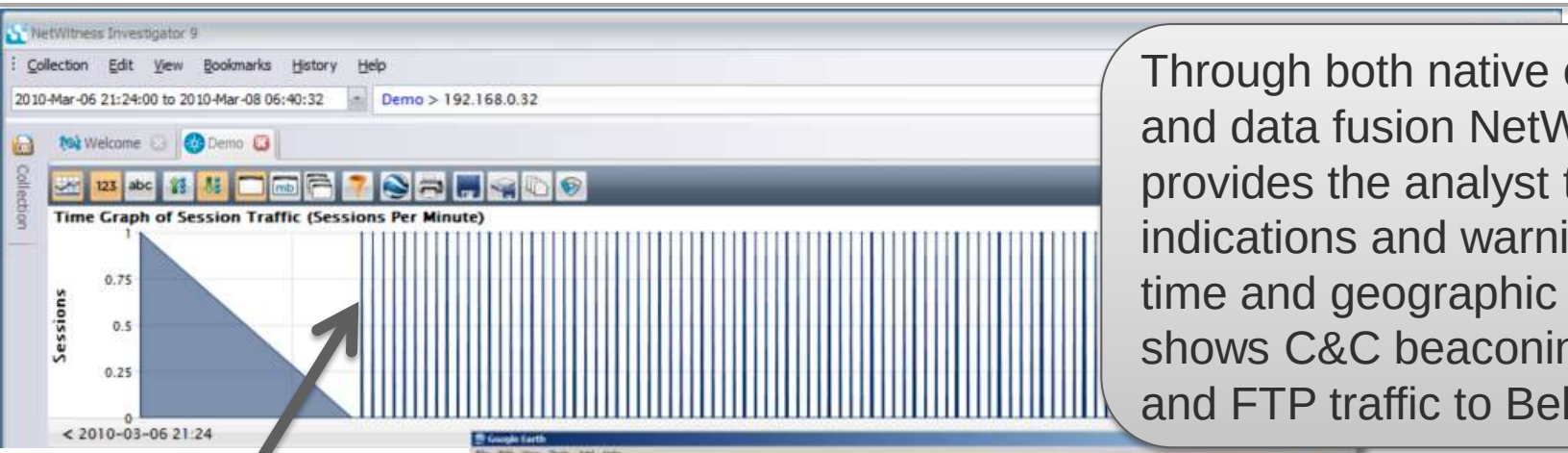


Investigator provides precise detail about the suspect event – in this case specific, concerning and compounding network behavior involving multiple characteristics

Precise Detail and Context with Investigator



Deeper Visibility and Layers of Discovery

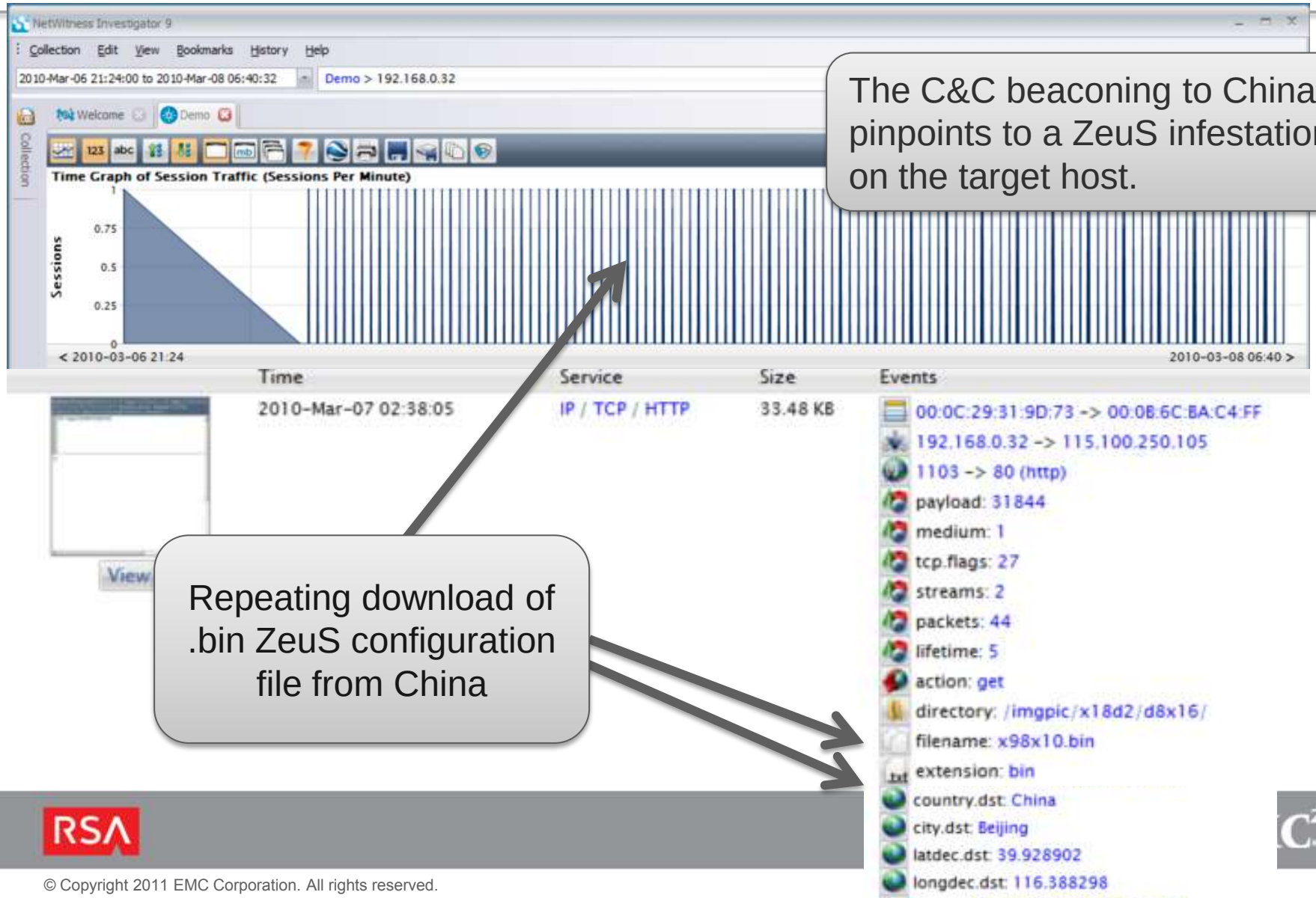


Through both native capabilities and data fusion NetWitness provides the analyst the most indications and warnings, e.g.: time and geographic rendering shows C&C beaconing to China and FTP traffic to Belarus.

High volume (red) beacon traffic to server in China, 115.100.250.105

FTP Traffic to a server in Belarus, 86.57.246.177

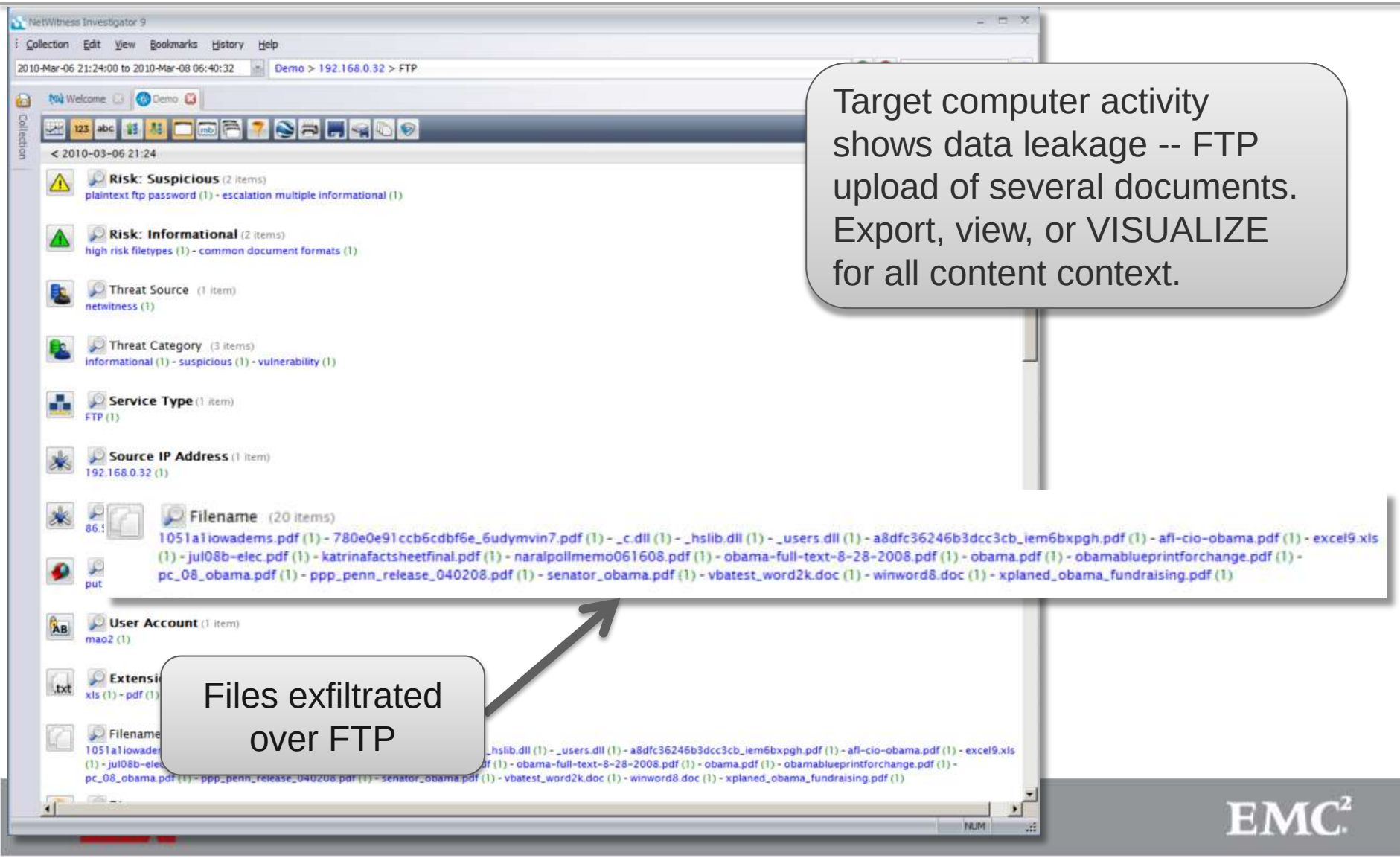
Unparalleled Analytics and Precision



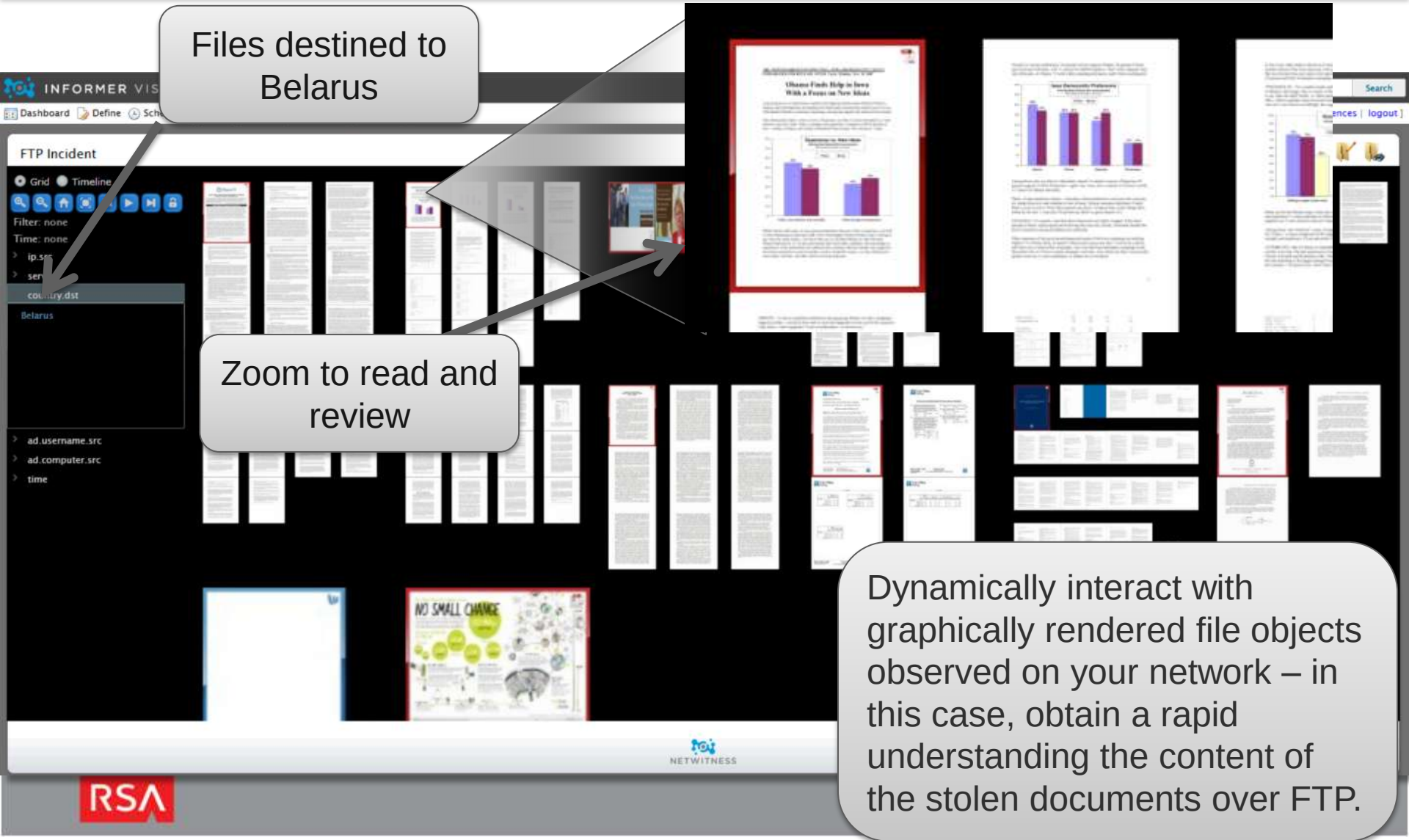
The C&C beaconing to China pinpoints to a ZeuS infestation, on the target host.

Repeating download of .bin ZeuS configuration file from China

Every New Question Yields An Accurate Answer

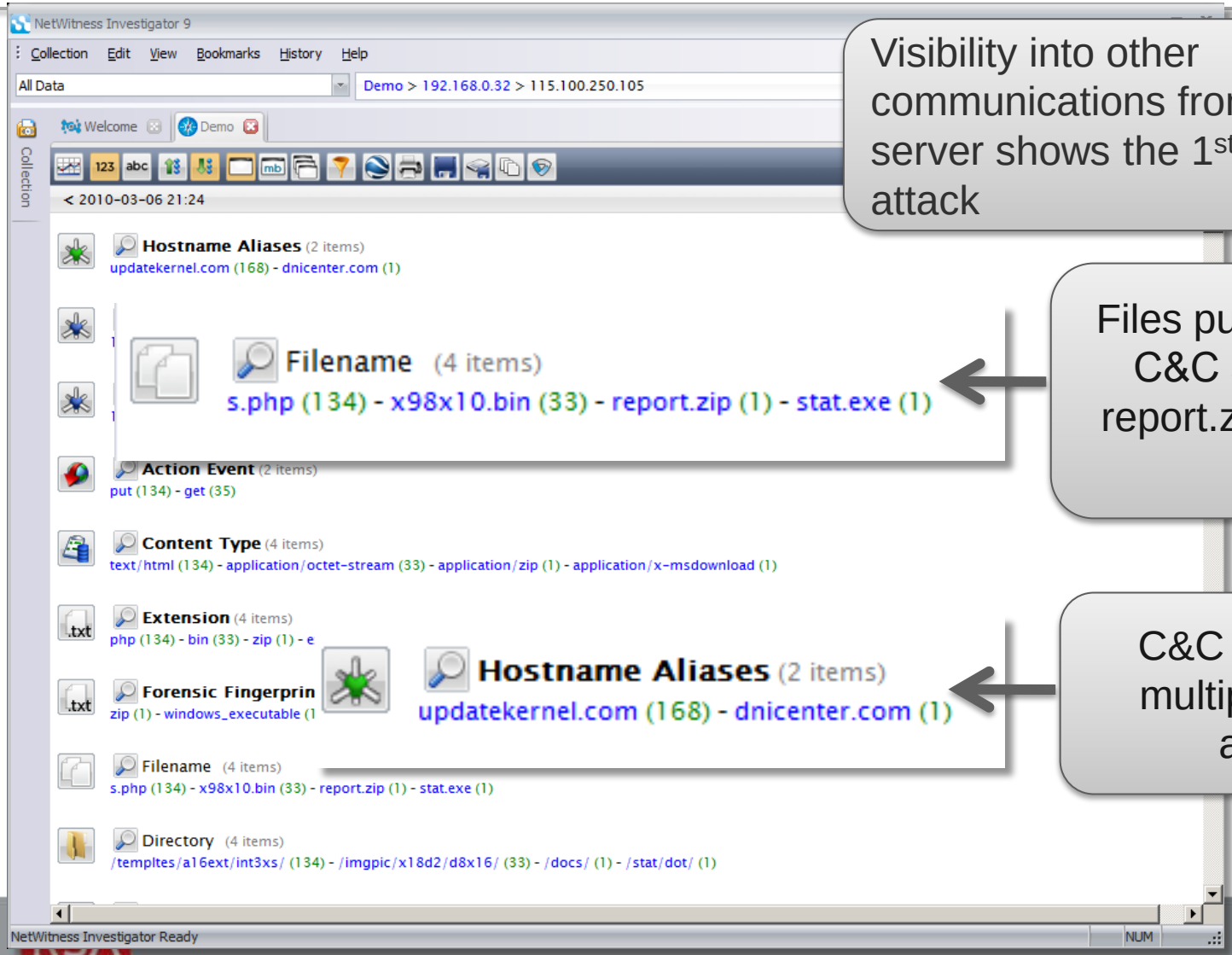


Visualize – Interact with Your Information



Dynamically interact with graphically rendered file objects observed on your network – in this case, obtain a rapid understanding the content of the stolen documents over FTP.

Exposing Patient Zero / Finding Root Cause



Visibility into other communications from the C&C server shows the 1st stage of the attack

Files pulled from the C&C server… is report.zip anywhere else?

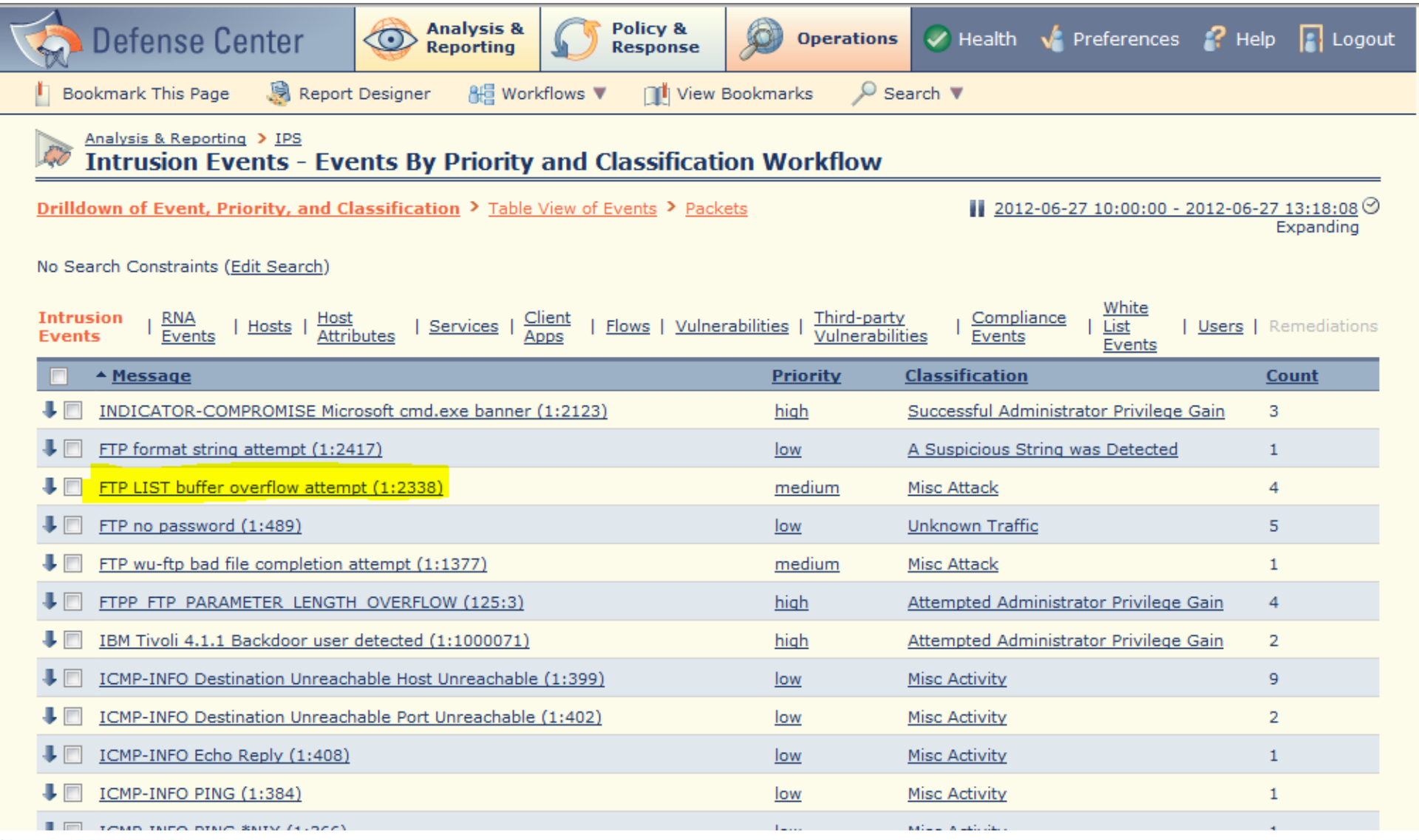
C&C server has multiple domain aliases

Demonstration Recap

- The Issue
  - You need to know what is happening on your network and get answers about anything at any time
- Series of Unfortunate Events
  - User receives a well crafted spear-phish that bypasses all process and technology defenses
  - User downloads and executes a zip file from a site in China
  - Once executed, the victim's machine becomes a member of a ZeuS botnet.
  - The ZeuS botnet begins beaconing to establish command and control with the botnet operator
  - Botnet operator commands the new zombie to download and execute second-stage malware
  - This second-stage malware successfully FTPs documents from the victim computer to a server in Belarus.
- Only NetWitness can:
  - Provide pervasive network visibility into the content of all network traffic and context of all network behavior
  - Deliver precise and actionable real-time intelligence that fuses your organization's information with the knowledge of the global security community
  - Get you answers to any security question on a single enterprise network monitoring platform

What about logs?

Sourcefire: list of events

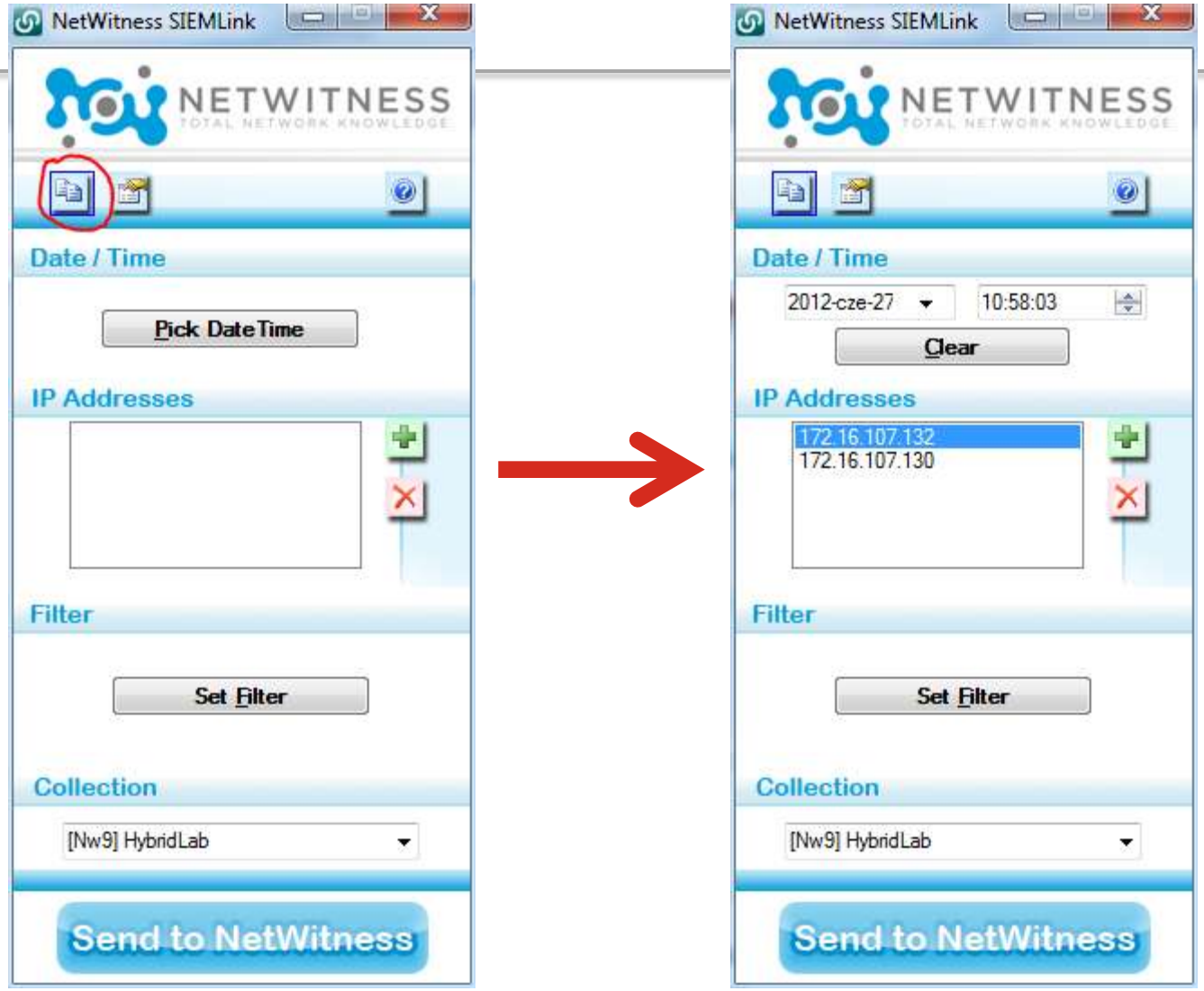


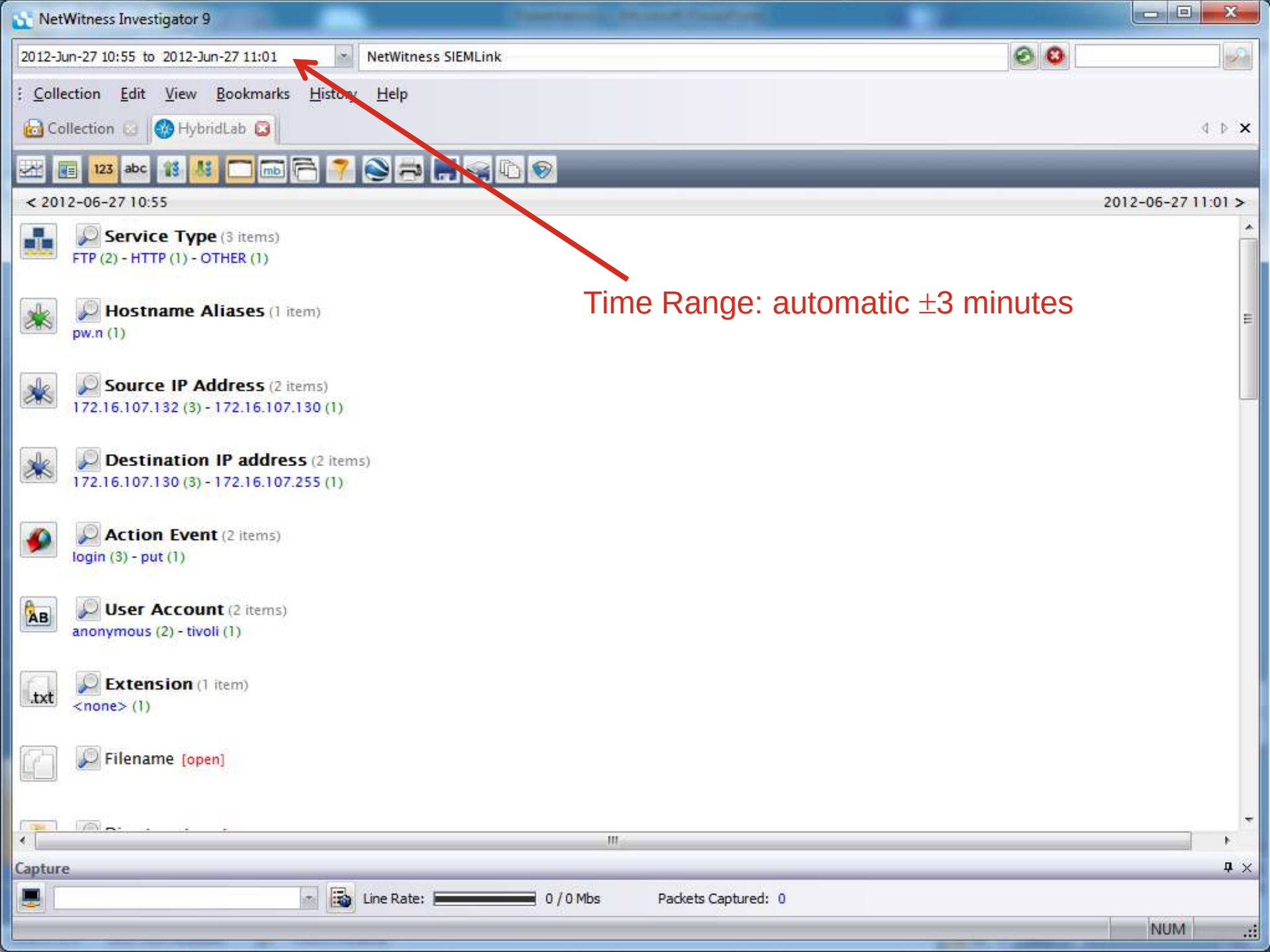
Message	Priority	Classification	Count
INDICATOR-COMPROMISE Microsoft cmd.exe banner (1:2123)	high	Successful Administrator Privilege Gain	3
FTP format string attempt (1:2417)	low	A Suspicious String was Detected	1
FTP LIST buffer overflow attempt (1:2338)	medium	Misc Attack	4
FTP no password (1:489)	low	Unknown Traffic	5
FTP wu-ftp bad file completion attempt (1:1377)	medium	Misc Attack	1
FTPP_FTP_PARAMETER_LENGTH_OVERFLOW (125:3)	high	Attempted Administrator Privilege Gain	4
IBM Tivoli 4.1.1 Backdoor user detected (1:1000071)	high	Attempted Administrator Privilege Gain	2
ICMP-INFO Destination Unreachable Host Unreachable (1:399)	low	Misc Activity	9
ICMP-INFO Destination Unreachable Port Unreachable (1:402)	low	Misc Activity	2
ICMP-INFO Echo Reply (1:408)	low	Misc Activity	1
ICMP-INFO PING (1:384)	low	Misc Activity	1

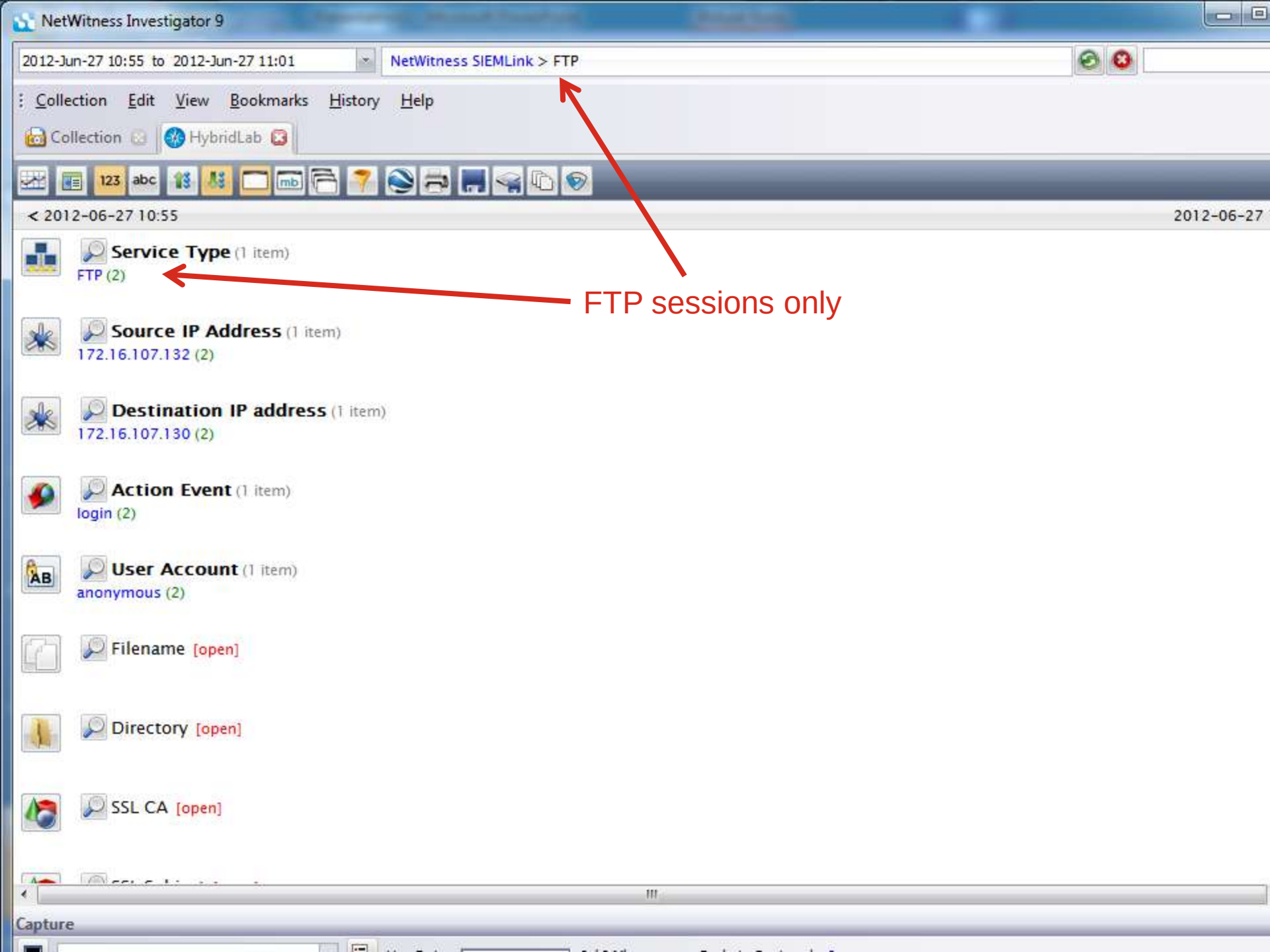
Sourcefire: event details

(Ctrl+C on details containing Date, Source IP and Destination IP)

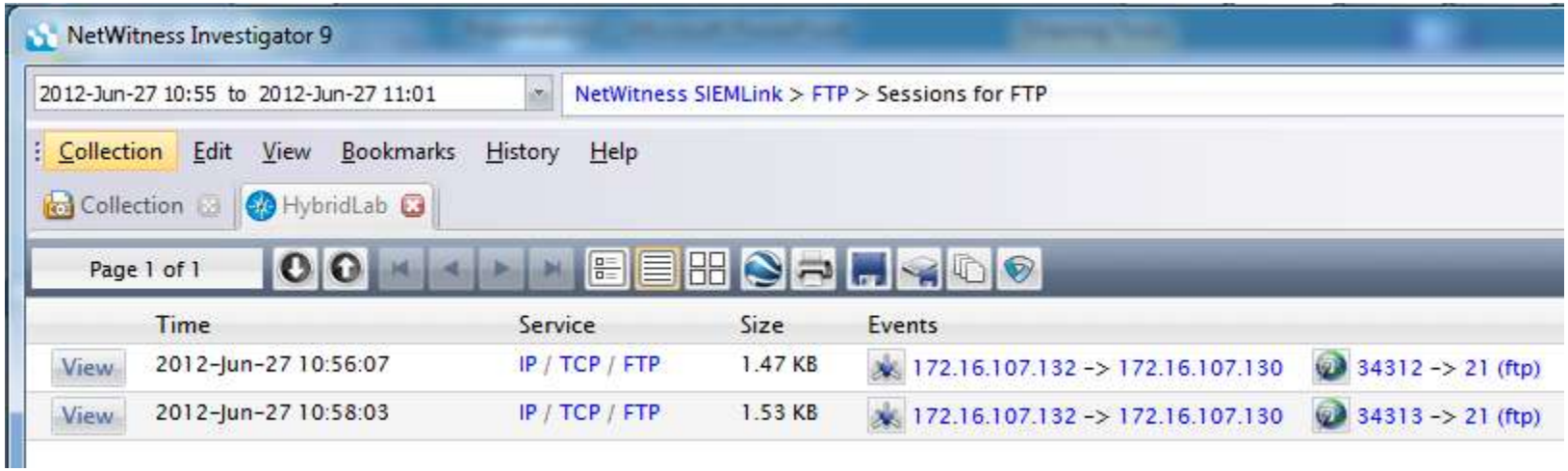
RSA SIEMLink - clipboard integration



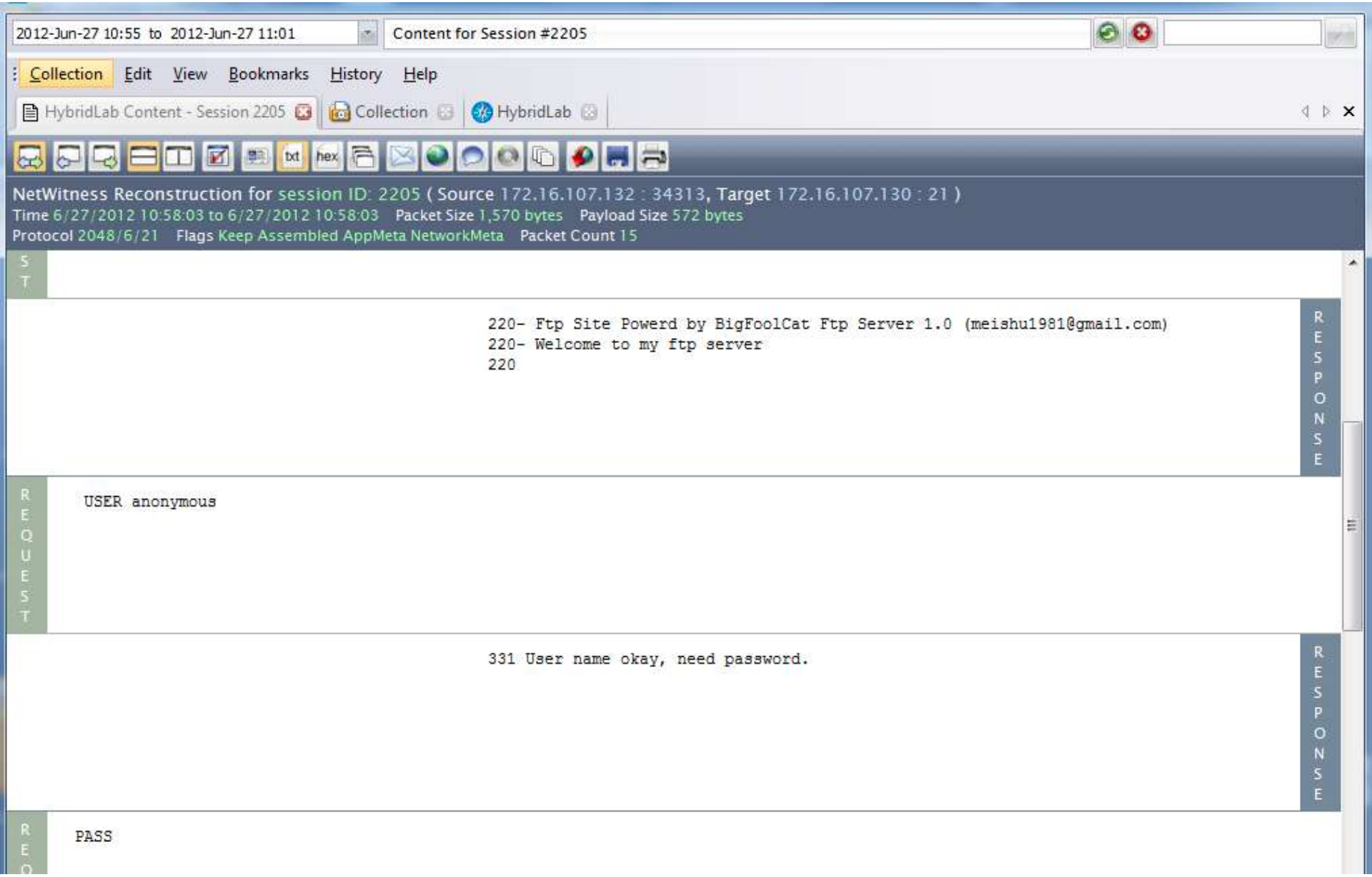

NetWitness Investigator 9
2012-Jun-27 10:55 to 2012-Jun-27 11:01
NetWitness SIEMLink
Collection Edit View Bookmarks History Help
Collection
HybridLab
< 2012-06-27 10:55
2012-06-27 11:01 >
Service Type (3 items)
FTP (2) - HTTP (1) - OTHER (1)
Hostname Aliases (1 item)
pw.n (1)
Source IP Address (2 items)
172.16.107.132 (3) - 172.16.107.130 (1)
Destination IP address (2 items)
172.16.107.130 (3) - 172.16.107.255 (1)
Action Event (2 items)
login (3) - put (1)
User Account (2 items)
anonymous (2) - tivoli (1)
Extension (1 item)
<none> (1)
Filename [open]
Time Range: automatic ±3 minutes
Capture
Line Rate: 0 / 0 Mbs
Packets Captured: 0
NUM


NetWitness Investigator 9
2012-Jun-27 10:55 to 2012-Jun-27 11:01
NetWitness SIEMLink > FTP
Collection Edit View Bookmarks History Help
Collection
HybridLab
< 2012-06-27 10:55
2012-06-27
Service Type (1 item)
FTP (2)
Source IP Address (1 item)
172.16.107.132 (2)
Destination IP address (1 item)
172.16.107.130 (2)
Action Event (1 item)
login (2)
User Account (1 item)
anonymous (2)
Filename [open]
Directory [open]
SSL CA [open]
FTP sessions only
Capture

NetWitness: view sessions



NetWitness: beginning of session



Session View: exploit

REQUEST

```
PASS
```

RESPONSE

```
230- anonymous
230- Ftp server have run for 0h-1m-22s
230 anonymous logged in.
```

REQUEST

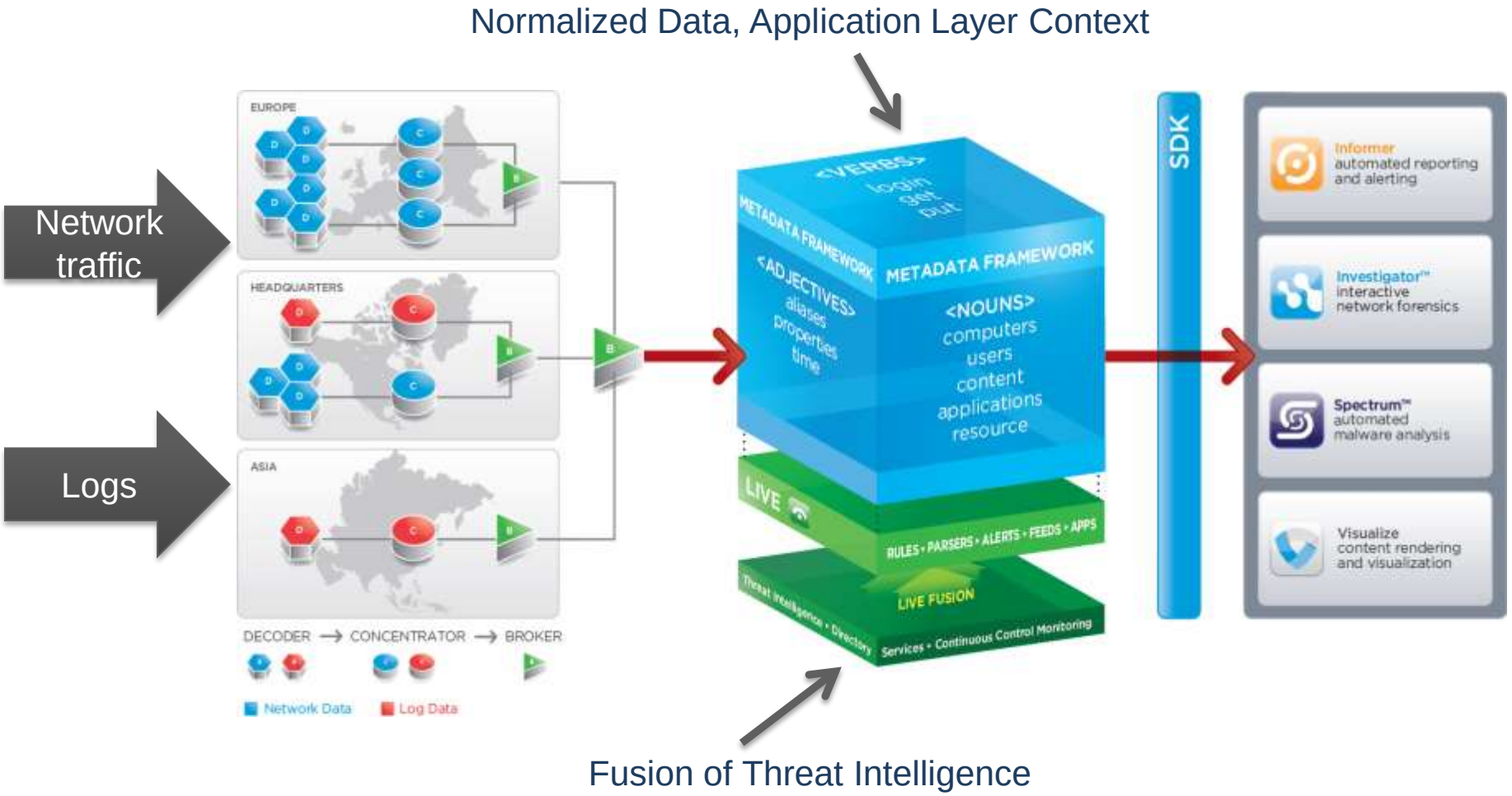

```
LIST □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□3B□□□□□□t$□[□s□□5`□□□□□□]q`趆%□>Ie□□□맑□?]□)
c□□a□□□D1□□t□m□w,,□□d□P□?.□c□~뷩4□c□□a<iD□v□□>uPmuMlc□9뷷□끙□ic5□`趆□ ћ띥k
uN0□E□d□ ؤ□b□b□□X□□MTV@□□A@□□P□□[□□□□□GTt$□□F□□P□□Z□□R□□E@□□X□□F□□A□Ↄ□GTt$□□5`
□□□|
```


RESPONSE

```
150 Opening ASCII mode data connection
```

RSA EMC²

Why not enrich packet based data with log data? That leads to Security Analytics



Example:
Advanced Threat Detection & Analysis

Navigate to "Malicious Code"

- Top Events View
- DoS & Network modifications may be expected, but Malicious Code? 3rd & 4th highest?

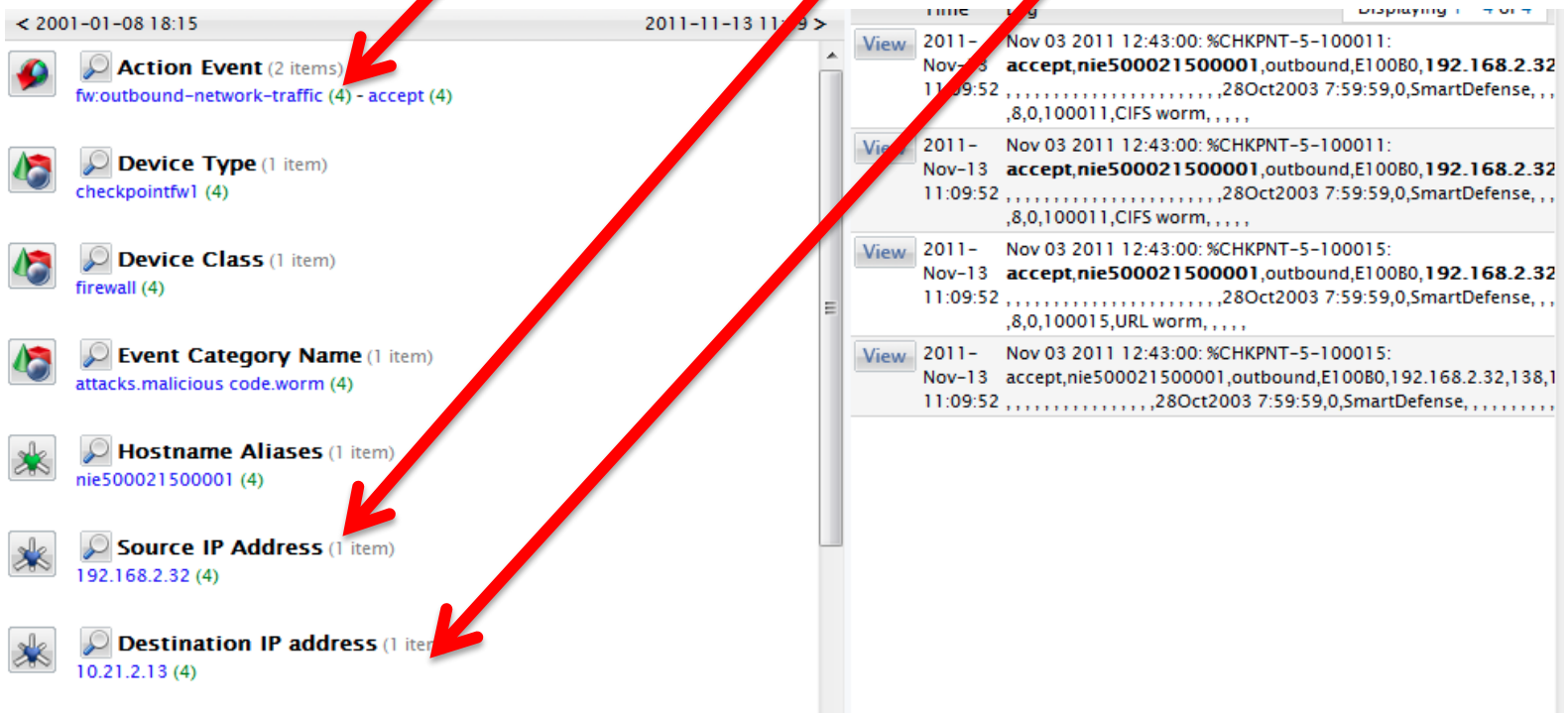
Advanced Threat Detection & Analysis

Navigate to "Firewall"

Malicious Code event was based on IDS and Firewall logs

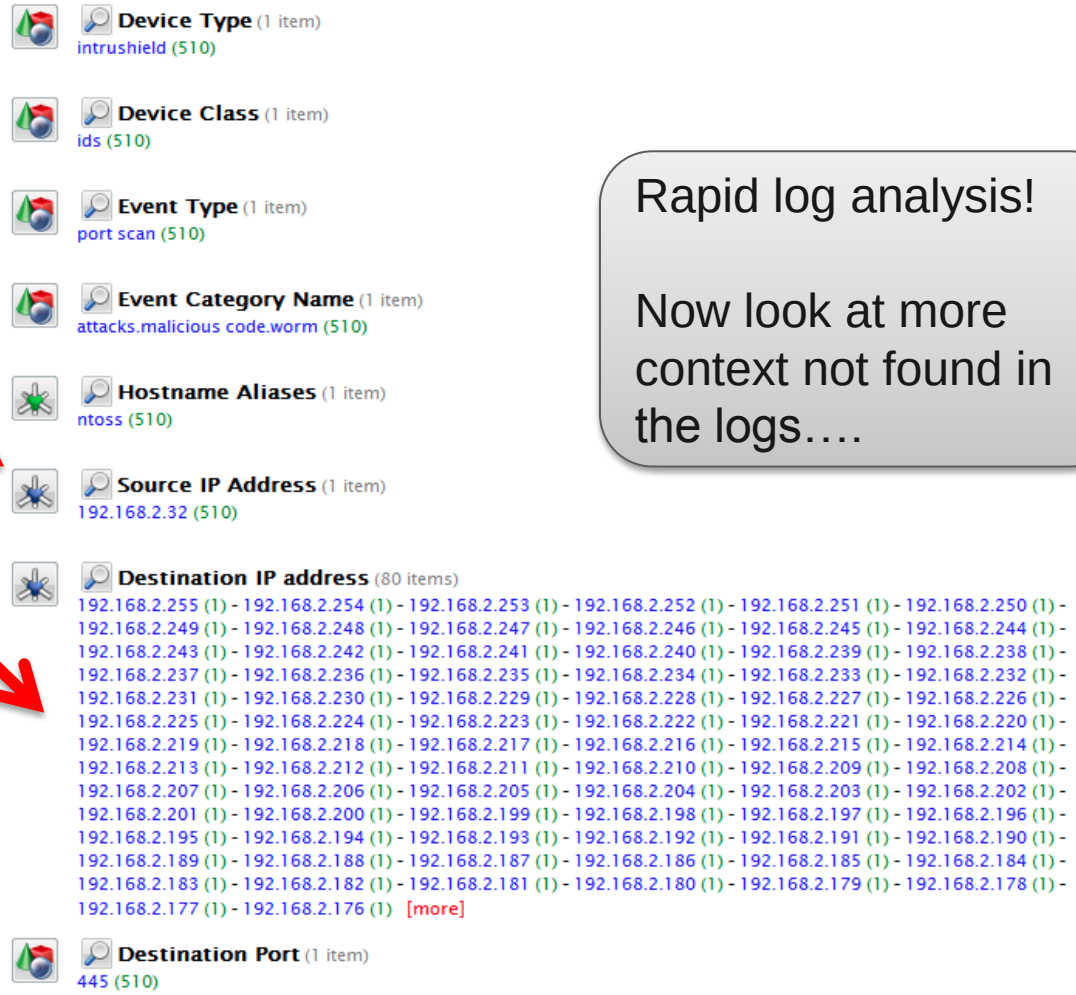
Advanced Threat Detection & Analysis

Firewall logs show outbound traffic from 192.168.2.32 that was not blocked. Destination IP likely a proxy/gateway



Advanced Threat Detection & Analysis

Source IP performing scans, flagged by IDS



Rapid log analysis!

Now look at more context not found in the logs….

Advanced Threat Detection & Analysis

Risk: Warning (2 items)
escalation multiple suspicious (1) - abnormal exe (1)

Risk: Suspicious (3 items)
watchlist tld (1) - escalation multiple informational (1) - crafted http header (1)

Risk: Informational (1 item)
common document formats (1)

Service Type (1 item)
HTTP (40)

Action Event (1 item)
get (40)

Hostname Aliases (1 item)
moisha.cn (1)

Source IP Address (1 item)
192.168.2.32 (40)

Destination IP address (2 items)
192.168.2.129 (39) - 58.65.239.28 (1)

TCP Destination Port (2 items)
2869 (39) - 80 (http) (1)

Content Type (2 items)
text/html (39) - text/plain (1)

Extension (2 items)
<none> (39) - txt (1)

Forensic Fingerpri
windows_executable (1)

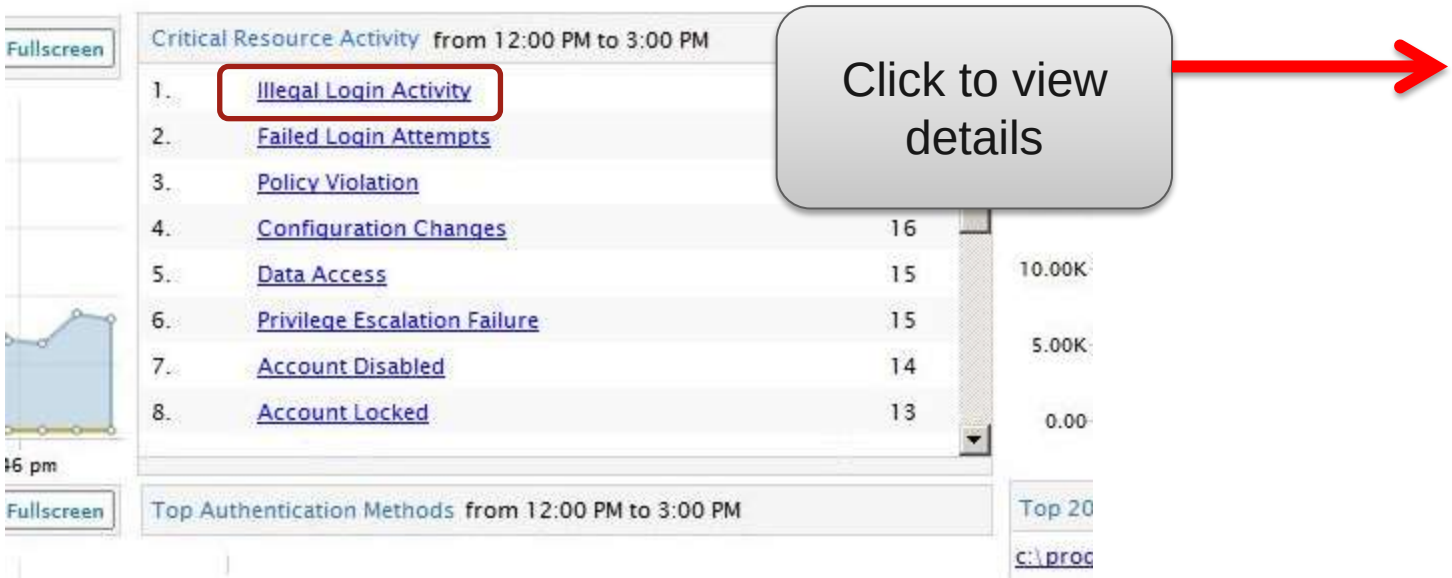
Deeper network analysis shows multiple malicious indicators sourced from 192.168.2.32:

- Beaconing activity
- Abnormal exe triggers
- Crafted HTTP header
- Http over non-standard ports

Total context. More than just a scan... Abnormal exe download, and beaconing trojan

Example:

Illegal Login – False Positive Resolution, Threat Analysis



- Dashboard shows “Illegal Login Activity” for a ‘Critical Resource’
  - Login and privilege escalation logs fused with internal feeds provides an optic into high-value targets

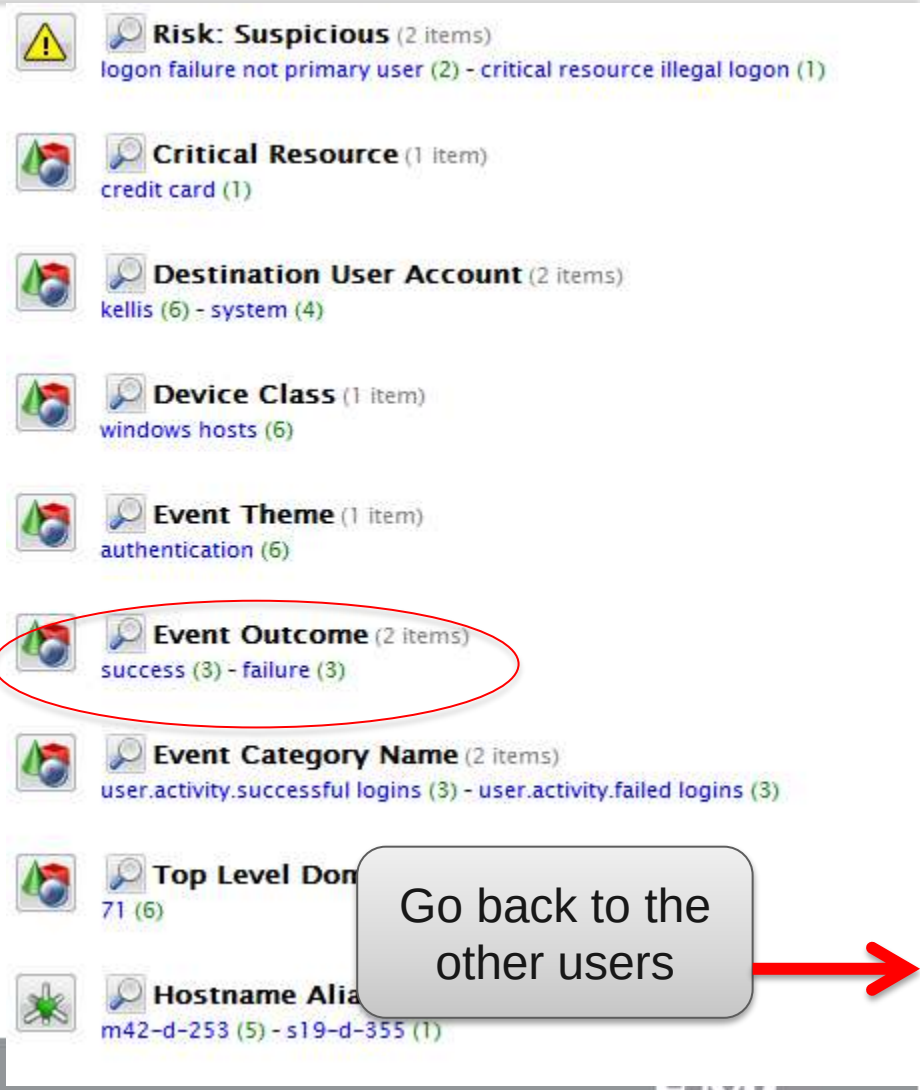
Illegal Login – False Positive Resolution, Threat Analysis

Detail shows 3 user accounts and 2 hosts subject to this categorization

Click user "kellis"

Illegal Login – False Positive Resolution, Threat Analysis

- Pivot shows an equal number of login success and failures between two computers.
- In all likelihood this user has mistyped their password on a few occasions.
- FALSE POSITIVE

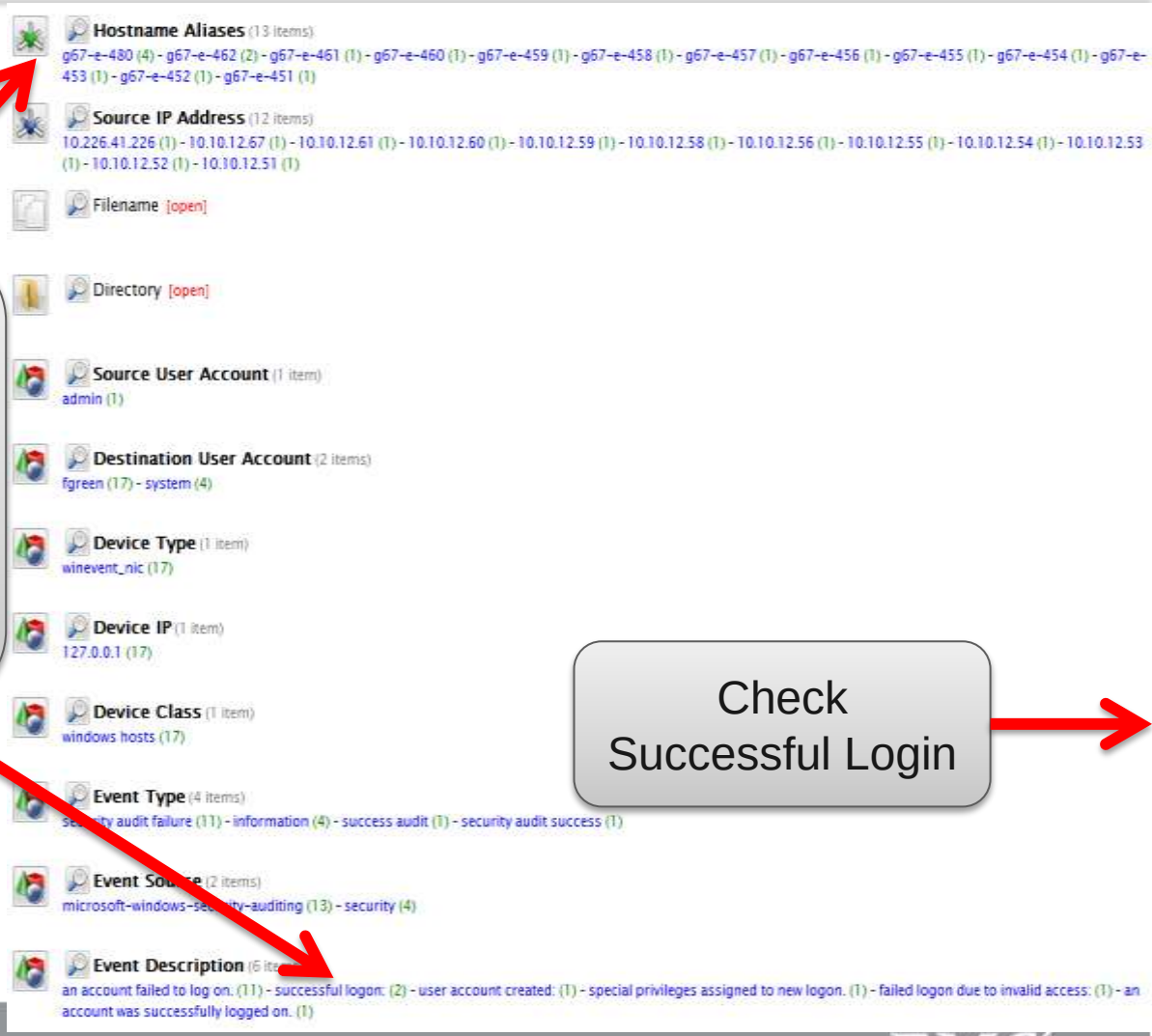


Illegal Login – False Positive Resolution, Threat Analysis

Click user "fgreen"

Illegal Login – False Positive Resolution, Threat Analysis

…LOGS…
- Multiple involved hosts and IPs indicate “probe” activity
- Event Description shows failed logins and privilege escalation
- Likely successful compromise



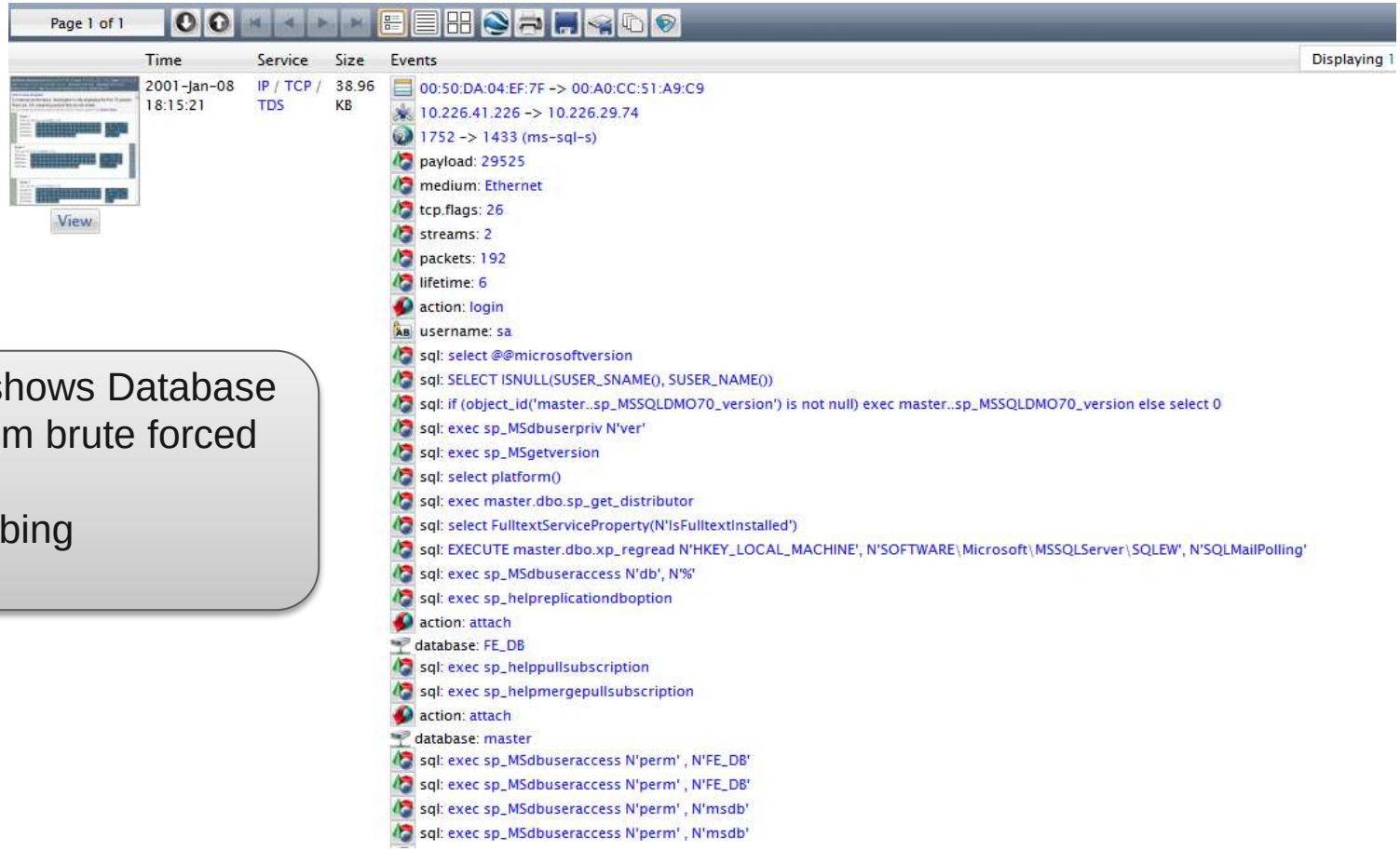
Check Successful Login

Illegal Login – False Positive Resolution, Threat Analysis

…Network data… Successful login IP shows additional network activity to include SMB, RDP and TDS activity --- typically indicates advanced threat lateral movement inside an enterprise

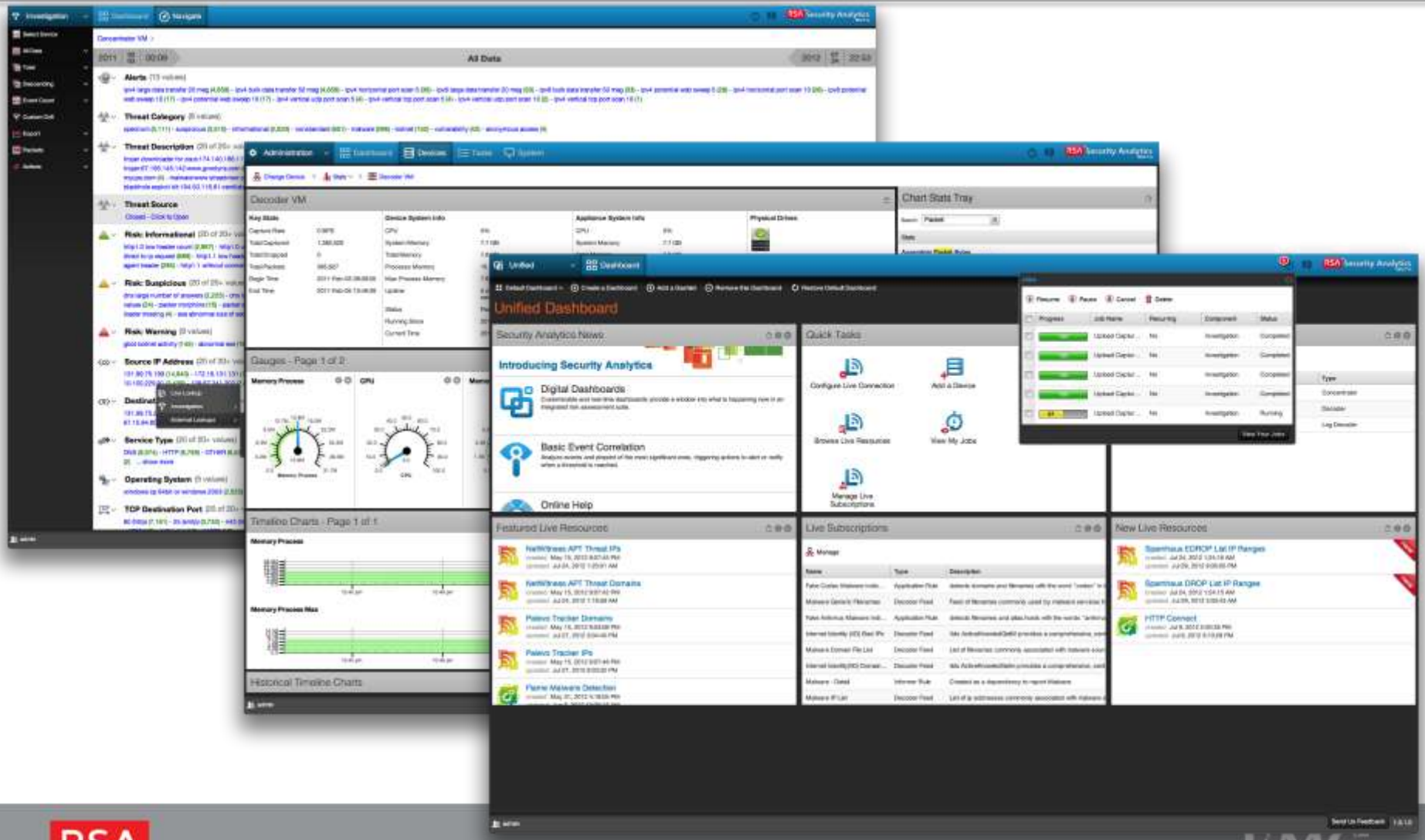
Content visibility

Illegal Login – False Positive Resolution, Threat Analysis



TDS activity shows Database interaction from brute forced device, SQL execution/probing

Introducing RSA Security Analytics



THANK YOU