
RSA Security Analytics

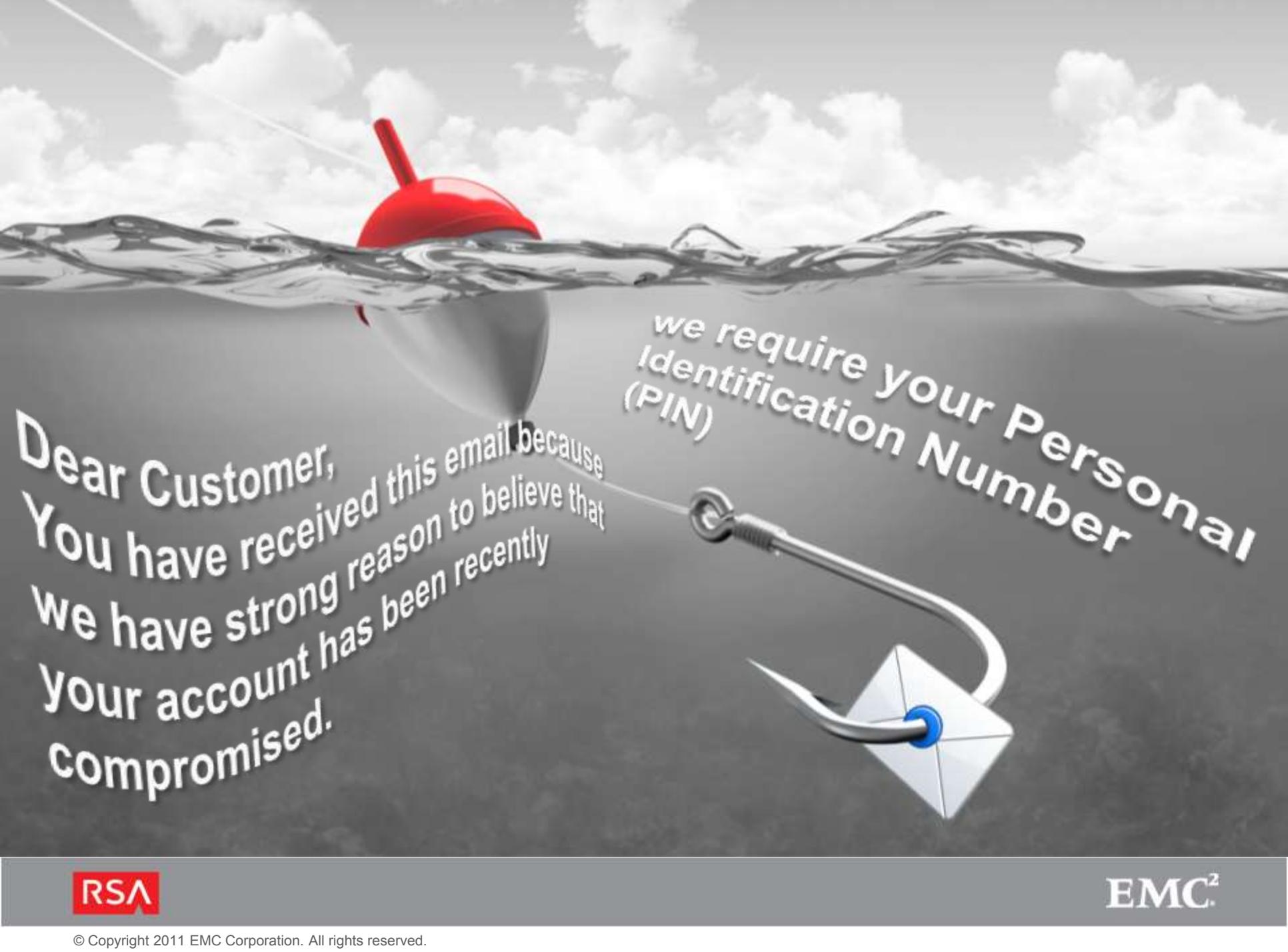
the complete approach to security monitoring
or how to approach advanced threats

Grzegorz Mucha
grzegorz.mucha@rsa.com



Advanced Threats





Dear Customer,
You have received this email because
we have strong reason to believe that
your account has been recently
compromised.

we require your Personal
Identification Number
(PIN)



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*

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

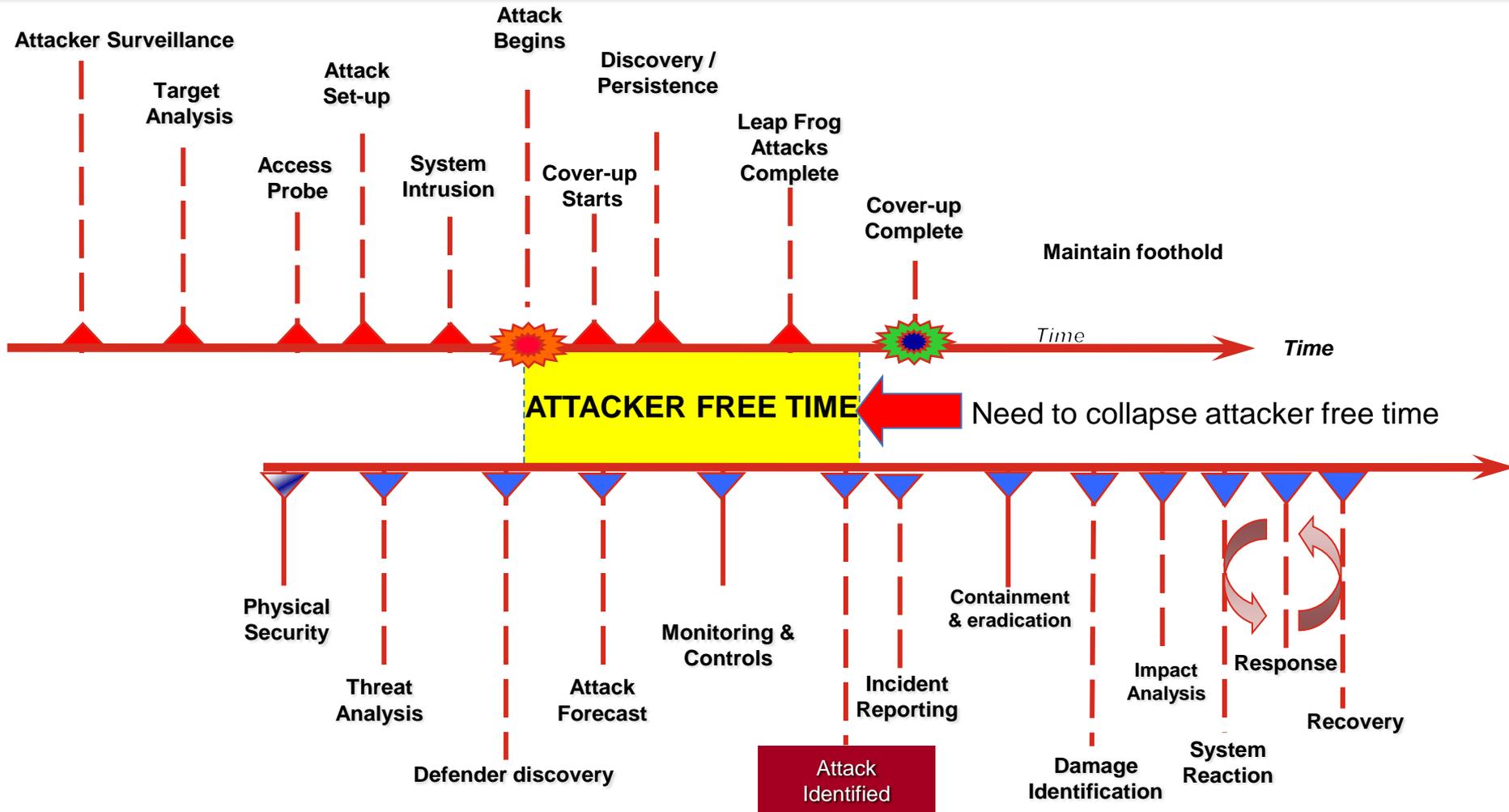


Characteristics of advanced threats



- 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



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

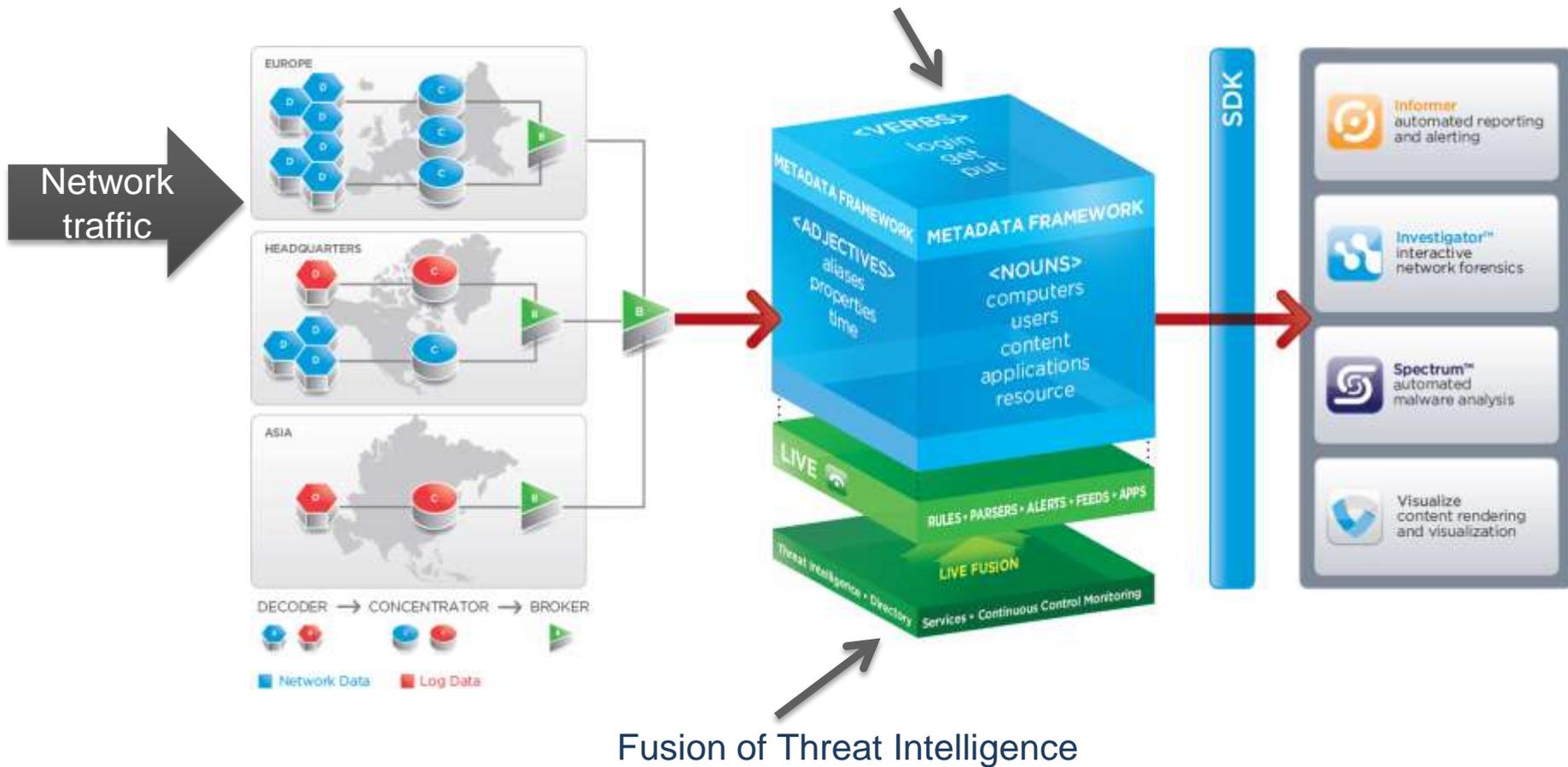
RSA NetWitness

gaining a total visibility of your
network traffic



Let's start with RSA NetWitness Network Monitoring Platform

Normalized Data, Application Layer Context



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



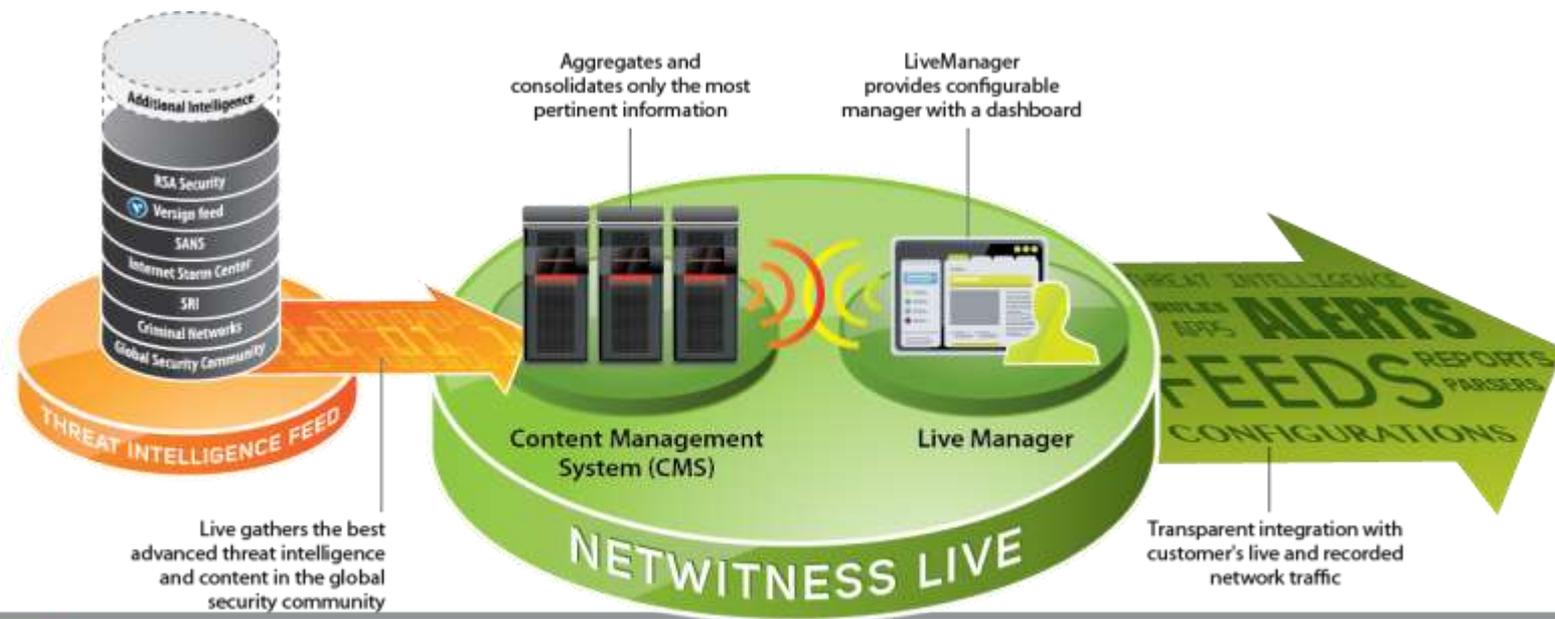
Spectrum



- 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

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.symantec-liveupdate.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	1.0		
NOD32	4918	2010.03.05	-
Norman	6.04.08	2010.03.05	-
nProtect	2009.1.8.0	2010.03.05	-

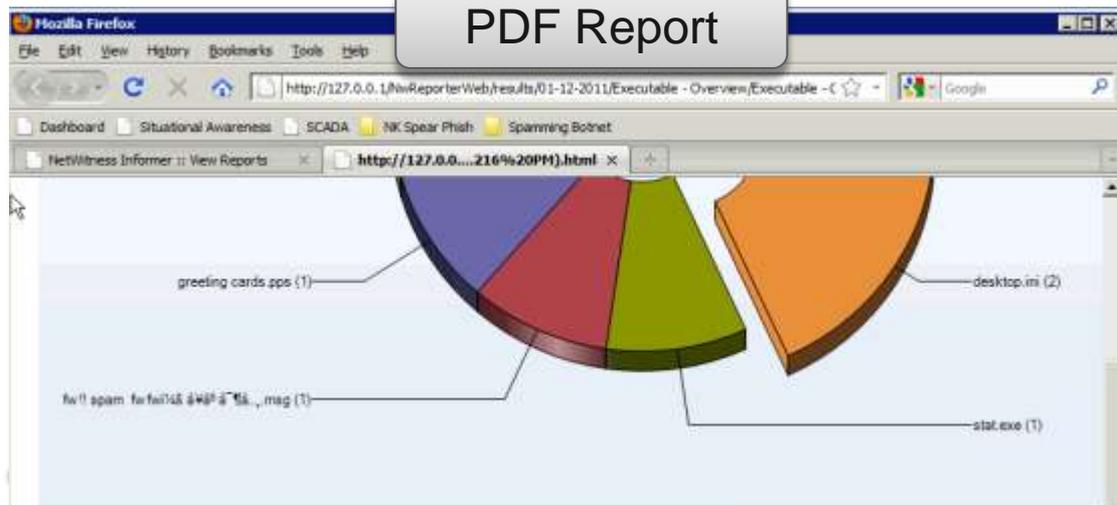
Let's take a look at how your world looks with NetWitness...



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 |

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

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





Precise Detail and Context with Investigator™

The screenshot shows the NetWitness Investigator 9 interface. At the top, there is a menu bar with 'Collection', 'Edit', 'View', 'Bookmarks', 'History', and 'Help'. Below the menu bar, a date range is set from '2010-Jan-01 00:00:00 to 2011-Jan-09 00:00:00'. A search bar contains the text 'NetWitness Investigator'. The main display area shows a search result for 'Risk: Suspicious (2 items)' with sub-items 'abnormal exe (1)' and 'crafted http header (1)'. Below this, there are several categories of results, each with a magnifying glass icon and a count: 'Ext exe (1)', 'Forensic Fingerprint (1 item) windows_executable (1)', 'Filename [open]', and 'Directory [open]'. Arrows point from callout boxes to these specific results.

Threat Indicators & Intelligence

Validated Executable Fingerprint

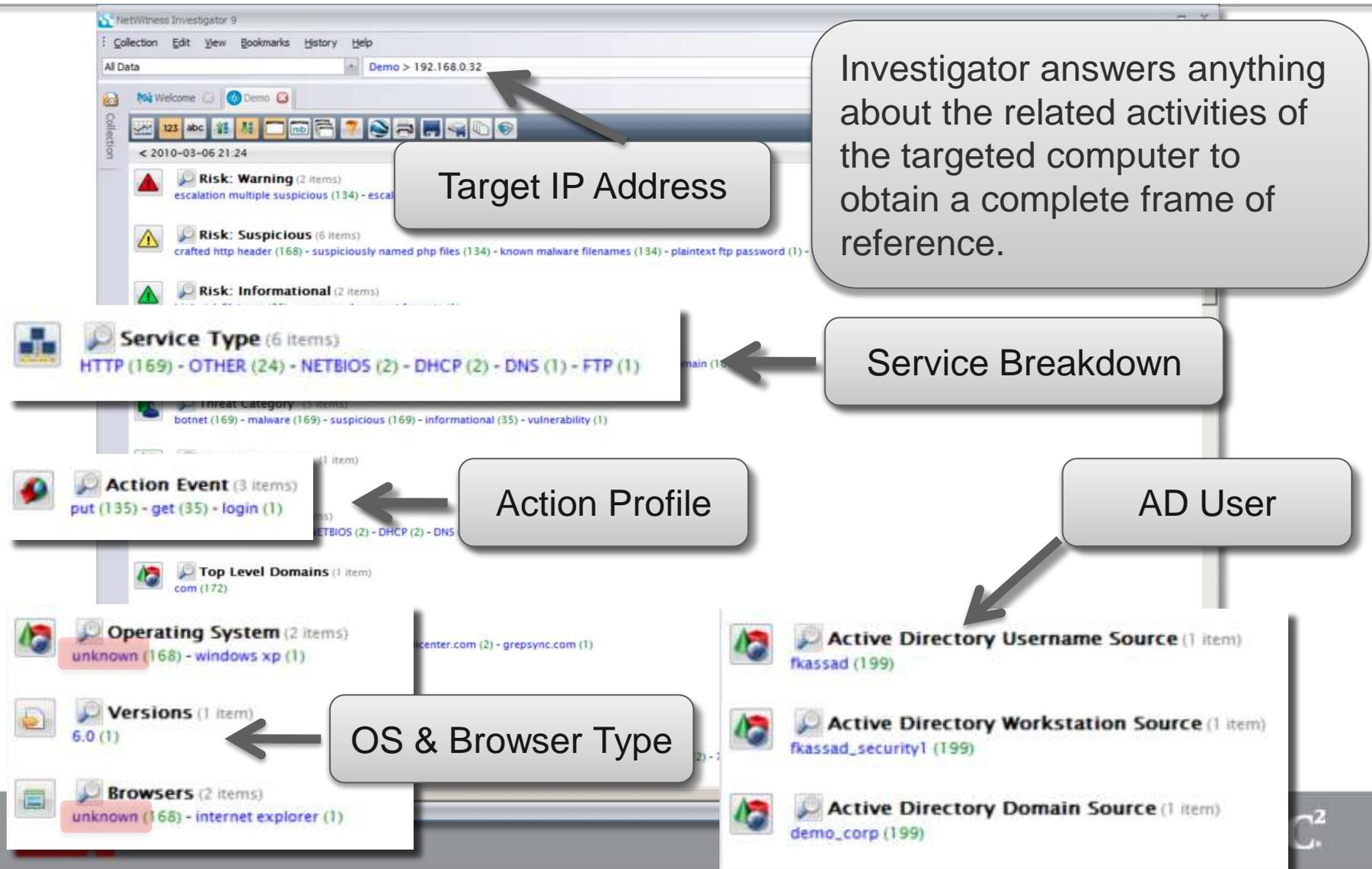
Foreign Country

Destination Country (1 item)
china (1)

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

Target computer activity shows data leakage -- FTP upload of several documents. Export, view, or VISUALIZE for all content context.

Files exfiltrated over FTP





Visualize – Interact with Your Information

The screenshot displays the Informer Vis interface. On the left, a sidebar titled "FTP Incident" shows a filter menu with "country.dst" selected and "Belarus" chosen. The main area is a grid of file objects. A callout box labeled "Files destined to Belarus" points to the filter. Another callout box labeled "Zoom to read and review" points to a document object. A large callout box on the right shows a zoomed-in view of a document titled "Obama Finds Edge in Iowa With a Focus on 'New Ideas'". The document contains a bar chart with the following data:

Category	Value 1	Value 2
Category 1	~85	~75
Category 2	~75	~65
Category 3	~65	~55
Category 4	~55	~45

Other visible elements include the "INFORMER VIS" header, "Dashboard Define Schedule" tabs, and a "Search" bar in the top right. The bottom of the interface features the "RSA" logo and "NETWITNESS" branding.

Files destined to Belarus

Zoom to read and review

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

NetWitness Investigator 9

Collection Edit View Bookmarks History Help

All Data Demo > 192.168.0.32 > 115.100.250.105

Collection

Welcome Demo

< 2010-03-06 21:24

- Hostname Aliases (2 items)
updatekernel.com (168) - dnicenter.com (1)
- Filename (4 items)
s.php (134) - x98x10.bin (33) - report.zip (1) - stat.exe (1)
- Action Event (2 items)
put (134) - get (35)
- Content Type (4 items)
text/html (134) - application/octet-stream (33) - application/zip (1) - application/x-msdownload (1)
- Extension (4 items)
php (134) - bin (33) - zip (1) - e
- Forensic Fingerprint (1)
zip (1) - windows_executable (1)
- Hostname Aliases (2 items)
updatekernel.com (168) - dnicenter.com (1)
- Filename (4 items)
s.php (134) - x98x10.bin (33) - report.zip (1) - stat.exe (1)
- Directory (4 items)
/templates/a16ext/int3xs/ (134) - /imgpic/x18d2/d8x16/ (33) - /docs/ (1) - /stat/dot/ (1)

NetWitness Investigator Ready

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

Analysis & Reporting > IPS
Intrusion Events - Events By Priority and Classification Workflow

[Drilldown of Event, Priority, and Classification](#) > [Table View of Events](#) > [Packets](#)

2012-06-27 10:00:00 - 2012-06-27 13:18:08 Expanding

No Search Constraints ([Edit Search](#))

Intrusion Events | [RNA Events](#) | [Hosts](#) | [Host Attributes](#) | [Services](#) | [Client Apps](#) | [Flows](#) | [Vulnerabilities](#) | [Third-party Vulnerabilities](#) | [Compliance Events](#) | [White List Events](#) | [Users](#) | [Remediations](#)

<input type="checkbox"/> ^ Message	Priority	Classification	Count
<input type="checkbox"/> INDICATOR-COMPROMISE Microsoft cmd.exe banner (1:2123)	high	Successful Administrator Privilege Gain	3
<input type="checkbox"/> FTP format string attempt (1:2417)	low	A Suspicious String was Detected	1
<input type="checkbox"/> FTP LIST buffer overflow attempt (1:2338)	medium	Misc Attack	4
<input type="checkbox"/> FTP no password (1:489)	low	Unknown Traffic	5
<input type="checkbox"/> FTP wu-ftp bad file completion attempt (1:1377)	medium	Misc Attack	1
<input type="checkbox"/> FTPP FTP_PARAMETER_LENGTH_OVERFLOW (125:3)	high	Attempted Administrator Privilege Gain	4
<input type="checkbox"/> IBM Tivoli 4.1.1 Backdoor user detected (1:1000071)	high	Attempted Administrator Privilege Gain	2
<input type="checkbox"/> ICMP-INFO Destination Unreachable Host Unreachable (1:399)	low	Misc Activity	9
<input type="checkbox"/> ICMP-INFO Destination Unreachable Port Unreachable (1:402)	low	Misc Activity	2
<input type="checkbox"/> ICMP-INFO Echo Reply (1:408)	low	Misc Activity	1
<input type="checkbox"/> ICMP-INFO PING (1:384)	low	Misc Activity	1
<input type="checkbox"/> ICMP-INFO PING #N/A (1:366)	low	Misc Activity	1

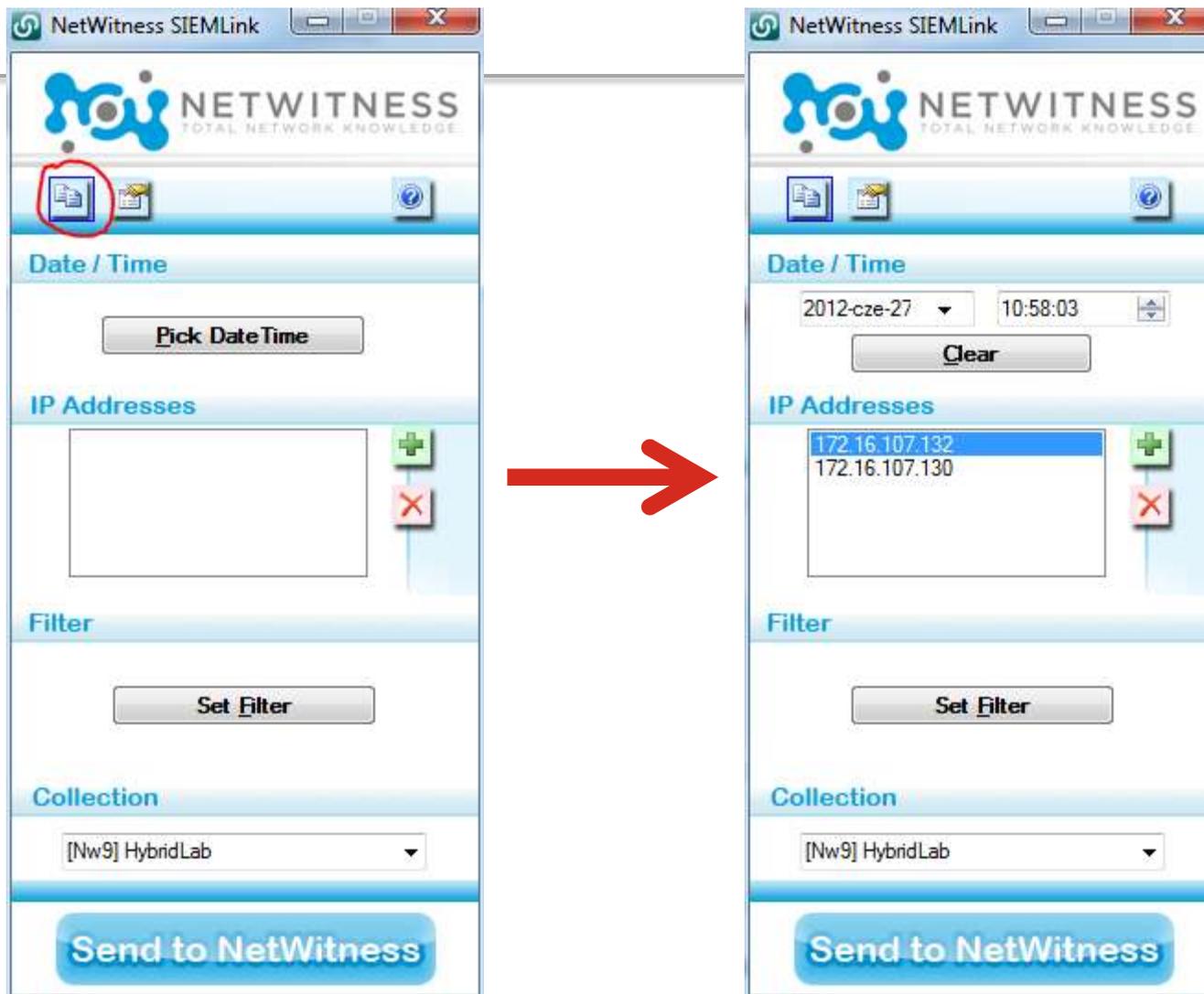
Sourcefire: event details

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

The screenshot displays the Sourcefire Defense Center interface. The top navigation bar includes sections for Defense Center, Analysis & Reporting, Policy & Response, Operations, Health, Preferences, and Help. Below this is a secondary bar with links for Bookmark This Page, Report Designer, Workflows, View Bookmarks, and Search. The main content area is titled "Intrusion Events - Events By Priority and Classification Workflow" and includes a breadcrumb trail: "Drilldown of Event, Priority, and Classification > Table View of Events > Packets". A search filter is set to "2012-06-27 10:00:00 - 2012-06-27 13:00:00" and is currently disabled. A navigation menu at the top of the table lists various event categories like RNA Events, Hosts, Host Attributes, Services, Client Apps, Flows, Vulnerabilities, etc. The table below shows a list of intrusion events with columns for Time, Priority, Impact Flag, Inline Result, Detection Engine, Protocol, Source IP, and Destination IP. Four events are listed, all with a medium priority and detected by the IPS DE / Sensor engine on 2012-06-27 between 10:49:27 and 10:58:03. The source and destination IP addresses for all events are 172.16.107.132 and 172.16.107.130.

<input type="checkbox"/>	<u>Time</u> <input type="checkbox"/>	<u>Priority</u> <input type="checkbox"/>	<u>Impact Flag</u> <input type="checkbox"/>	<u>Inline Result</u> <input type="checkbox"/>	<u>Detection Engine</u> <input type="checkbox"/>	<u>Protocol</u> <input type="checkbox"/>	<u>Source IP</u> <input type="checkbox"/>	<u>Destination IP</u> <input type="checkbox"/>
<input type="checkbox"/>	2012-06-27 10:49:27	medium			IPS DE / Sensor	tcp	172.16.107.132	172.16.107.130
<input type="checkbox"/>	2012-06-27 10:53:16	medium			IPS DE / Sensor	tcp	172.16.107.132	172.16.107.130
<input type="checkbox"/>	2012-06-27 10:56:07	medium			IPS DE / Sensor	tcp	172.16.107.132	172.16.107.130
<input type="checkbox"/>	2012-06-27 10:58:03	medium			IPS DE / Sensor	tcp	172.16.107.132	172.16.107.130

RSA SIEMLink - clipboard integration



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]

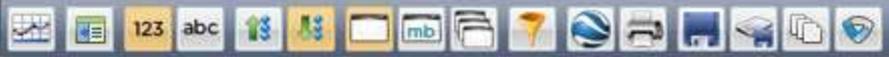
Time Range: automatic ± 3 minutes

Capture

Line Rate: 0 / 0 Mbs

Packets Captured: 0

NUM



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

NetWitness: view sessions

The screenshot displays the NetWitness Investigator 9 interface. The title bar reads "NetWitness Investigator 9". The main window shows a time range of "2012-Jun-27 10:55 to 2012-Jun-27 11:01" and a breadcrumb path: "NetWitness SIEMLink > FTP > Sessions for FTP". Below this is a menu bar with "Collection", "Edit", "View", "Bookmarks", "History", and "Help". The "Collection" menu is open, showing "Collection" and "HybridLab". A toolbar below the menu contains various icons for navigation and actions. The main content area is a table with the following data:

	Time	Service	Size	Events
View	2012-Jun-27 10:56:07	IP / TCP / FTP	1.47 KB	172.16.107.132 -> 172.16.107.130 34312 -> 21 (ftp)
View	2012-Jun-27 10:58:03	IP / TCP / FTP	1.53 KB	172.16.107.132 -> 172.16.107.130 34313 -> 21 (ftp)

NetWitness: beginning of session

2012-Jun-27 10:55 to 2012-Jun-27 11:01 Content for Session #2205

Collection Edit View Bookmarks History Help

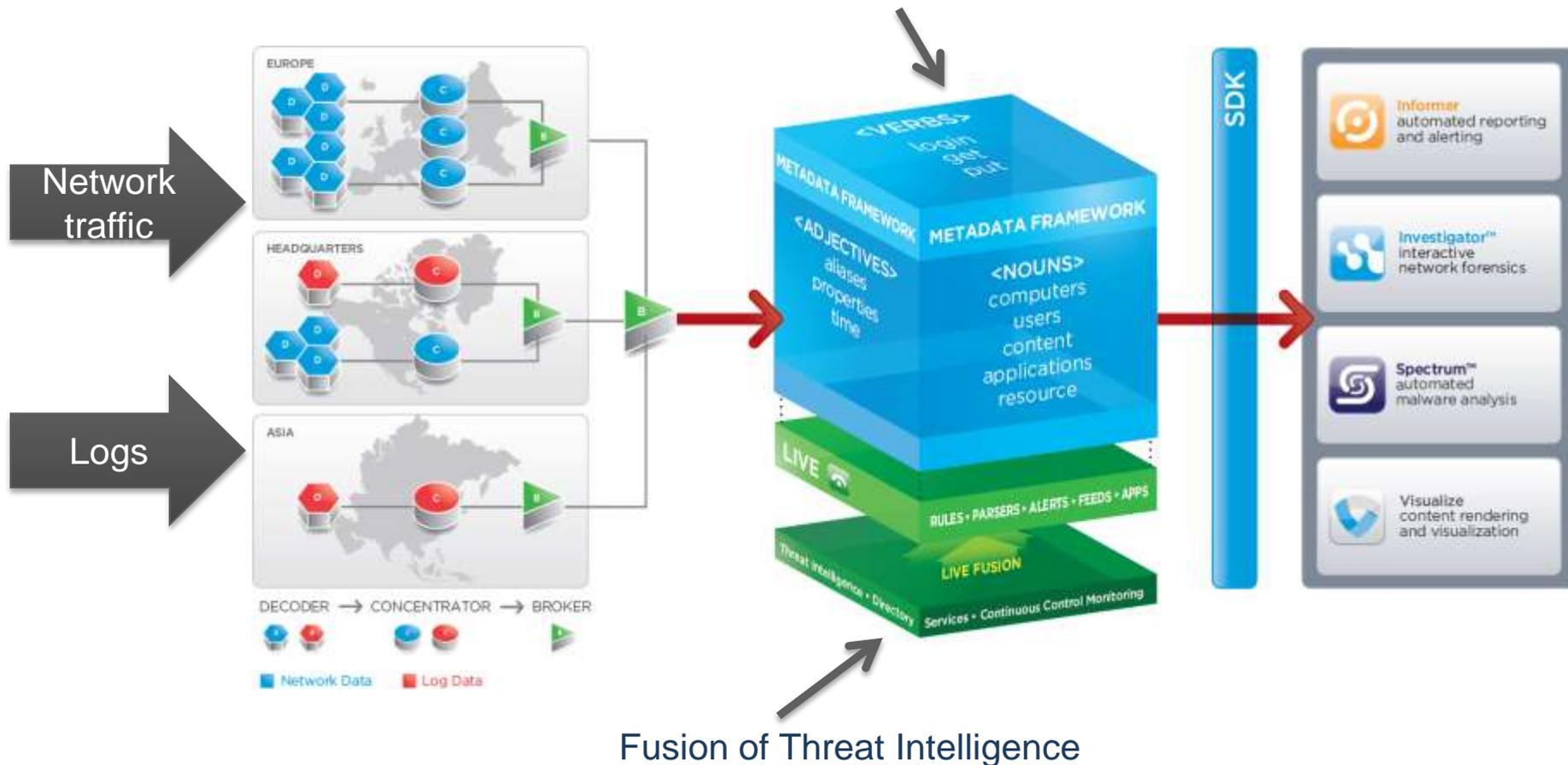
HybridLab Content - Session 2205 Collection HybridLab

NetWitness Reconstruction for session ID: 2205 (Source 172.16.107.132 : 34313, Target 172.16.107.130 : 21)
Time 6/27/2012 10:58:03 to 6/27/2012 10:58:03 Packet Size 1,570 bytes Payload Size 572 bytes
Protocol 2048/6/21 Flags Keep Assembled AppMeta NetworkMeta Packet Count 15

S	T
	220- Ftp Site Powerd by BigFoolCat Ftp Server 1.0 (meishu1981@gmail.com) 220- Welcome to my ftp server 220
R	USER anonymous
	331 User name okay, need password.
R	PASS

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

Normalized Data, Application Layer Context



Example: Advanced Threat Detection & Analysis

Rank	Event Name	Count
1.	Denial of Service	89
2.	Access.Modification.Network Based	64
3.	Malicious Code	30
4.	Malicious Code.Worm	39
5.	Access.Modification.Host Based.FTP	96
6.	Privilege Escalation Failure	44
7.	Account Disabled	40
8.	Account Locked	

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

Advanced Threat Detection & Analysis

Malicious Code event was based on IDS and Firewall logs

Navigate to
"Firewall"



-  **Device Type** (2 items)
intrushield (510) - checkpointfw1 (4)
-  **Device Class** (2 items)
ids (510) - firewall (4)
-  **Event Type** (1 item)
port scan (510)
-  **Event Category Name** (1 item)
attacks.malicious.code.worm (514)

Advanced Threat Detection & Analysis

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

The screenshot displays a firewall log analysis interface. On the left, a sidebar shows several filters: 'Action Event (2 items)' with 'fw:outbound-network-traffic (4) - accept (4)'; 'Device Type (1 item)' with 'checkpointfw1 (4)'; 'Device Class (1 item)' with 'firewall (4)'; 'Event Category Name (1 item)' with 'attacks.malicious code.worm (4)'; 'Hostname Aliases (1 item)' with 'nie500021500001 (4)'; 'Source IP Address (1 item)' with '192.168.2.32 (4)'; and 'Destination IP address (1 item)' with '10.21.2.13 (4)'. Red arrows point from the text box above to these filters. The main pane shows a log table with columns for 'Time' and 'Log'. The log entries are as follows:

Time	Log
2011-11-03 12:43:00	%CHKPNT-5-100011: accept,nie500021500001,outbound,E10080,192.168.2.32
2011-11-03 11:09:52,28Oct2003 7:59:59,0,SmartDefense,.....,8,0,100011,CIFS worm,.....
2011-11-03 12:43:00	%CHKPNT-5-100011: accept,nie500021500001,outbound,E10080,192.168.2.32
2011-11-03 11:09:52,28Oct2003 7:59:59,0,SmartDefense,.....,8,0,100011,CIFS worm,.....
2011-11-03 12:43:00	%CHKPNT-5-100015: accept,nie500021500001,outbound,E10080,192.168.2.32
2011-11-03 11:09:52,28Oct2003 7:59:59,0,SmartDefense,.....,8,0,100015,URL worm,.....
2011-11-03 12:43:00	%CHKPNT-5-100015: accept,nie500021500001,outbound,E10080,192.168.2.32,138,1
2011-11-03 11:09:52,28Oct2003 7:59:59,0,SmartDefense,.....

Advanced Threat Detection & Analysis

Device Type (1 item)
intrushield (510)

Device Class (1 item)
ids (510)

Event Type (1 item)
port scan (510)

Event Category Name (1 item)
attacks.malicious code.worm (510)

Hostname Aliases (1 item)
ntoss (510)

Source IP Address (1 item)
192.168.2.32 (510)

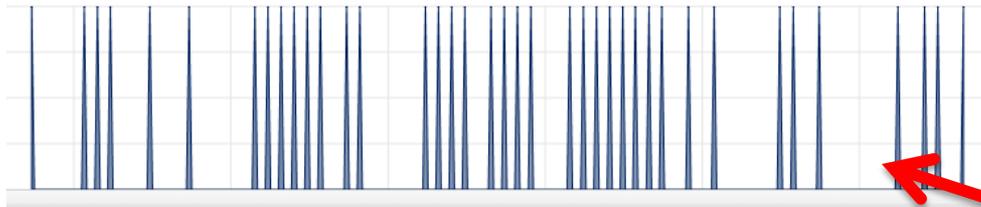
Destination IP address (80 items)
192.168.2.255 (1) - 192.168.2.254 (1) - 192.168.2.253 (1) - 192.168.2.252 (1) - 192.168.2.251 (1) - 192.168.2.250 (1) -
192.168.2.249 (1) - 192.168.2.248 (1) - 192.168.2.247 (1) - 192.168.2.246 (1) - 192.168.2.245 (1) - 192.168.2.244 (1) -
192.168.2.243 (1) - 192.168.2.242 (1) - 192.168.2.241 (1) - 192.168.2.240 (1) - 192.168.2.239 (1) - 192.168.2.238 (1) -
192.168.2.237 (1) - 192.168.2.236 (1) - 192.168.2.235 (1) - 192.168.2.234 (1) - 192.168.2.233 (1) - 192.168.2.232 (1) -
192.168.2.231 (1) - 192.168.2.230 (1) - 192.168.2.229 (1) - 192.168.2.228 (1) - 192.168.2.227 (1) - 192.168.2.226 (1) -
192.168.2.225 (1) - 192.168.2.224 (1) - 192.168.2.223 (1) - 192.168.2.222 (1) - 192.168.2.221 (1) - 192.168.2.220 (1) -
192.168.2.219 (1) - 192.168.2.218 (1) - 192.168.2.217 (1) - 192.168.2.216 (1) - 192.168.2.215 (1) - 192.168.2.214 (1) -
192.168.2.213 (1) - 192.168.2.212 (1) - 192.168.2.211 (1) - 192.168.2.210 (1) - 192.168.2.209 (1) - 192.168.2.208 (1) -
192.168.2.207 (1) - 192.168.2.206 (1) - 192.168.2.205 (1) - 192.168.2.204 (1) - 192.168.2.203 (1) - 192.168.2.202 (1) -
192.168.2.201 (1) - 192.168.2.200 (1) - 192.168.2.199 (1) - 192.168.2.198 (1) - 192.168.2.197 (1) - 192.168.2.196 (1) -
192.168.2.195 (1) - 192.168.2.194 (1) - 192.168.2.193 (1) - 192.168.2.192 (1) - 192.168.2.191 (1) - 192.168.2.190 (1) -
192.168.2.189 (1) - 192.168.2.188 (1) - 192.168.2.187 (1) - 192.168.2.186 (1) - 192.168.2.185 (1) - 192.168.2.184 (1) -
192.168.2.183 (1) - 192.168.2.182 (1) - 192.168.2.181 (1) - 192.168.2.180 (1) - 192.168.2.179 (1) - 192.168.2.178 (1) -
192.168.2.177 (1) - 192.168.2.176 (1) [more]

Destination Port (1 item)
445 (510)

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)

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

-  **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 Fingerprint**
windows_executable (1)

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

The screenshot displays a list of threat analysis categories with the following details:

- Risk: Suspicious** (1 item)
critical resource illegal logon (2)
- Critical Resource** (2 items)
database (1) - credit card (1)
- Threat Source** [open]
- Threat Category** [open]
- Threat Description** [open]
- Destination User Account** (3 items)
system (2) - kellis (1) - fgreen (1)
- Top Level Domains** (1 item)
71 (2)
- Hostname Aliases** (2 items)
s19-d-355 (1) - g67-e-457 (1)

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

The screenshot displays a list of pivots from a threat analysis tool. The pivots are:

- Risk: Suspicious** (2 items)
logon failure not primary user (2) - critical resource illegal logon (1)
- Critical Resource** (1 item)
credit card (1)
- Destination User Account** (2 items)
kellis (6) - system (4)
- Device Class** (1 item)
windows hosts (6)
- Event Theme** (1 item)
authentication (6)
- Event Outcome** (2 items)
success (3) - failure (3)
- Event Category Name** (2 items)
user.activity.successful logins (3) - user.activity.failed logins (3)
- Top Level Domain**
71 (6)
- Hostname Alias**
m42-d-253 (5) - s19-d-355 (1)

A red circle highlights the 'Event Outcome' pivot. A callout box with a red arrow points to the right, containing the text 'Go back to the other users'.

Illegal Login – False Positive Resolution, Threat Analysis

The screenshot displays a list of threat analysis categories with the following details:

- Risk: Suspicious** (1 item)
critical resource illegal logon (2)
- Critical Resource** (2 items)
database (1) - credit card (1)
- Threat Source** [open]
- Threat Category** [open]
- Threat Description** [open]
- Destination User Account** (3 items)
system (2) - kellis (1) - fgreen (1)
- Top Level Domains** (1 item)
71 (2)
- Hostname Aliases** (2 items)
s19-d-355 (1) - g67-e-457 (1)

The 'Destination User Account' category is circled in red. A callout box on the right contains the text 'Click user "fgreen"' with a red arrow pointing to the 'fgreen (1)' entry in the list.

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

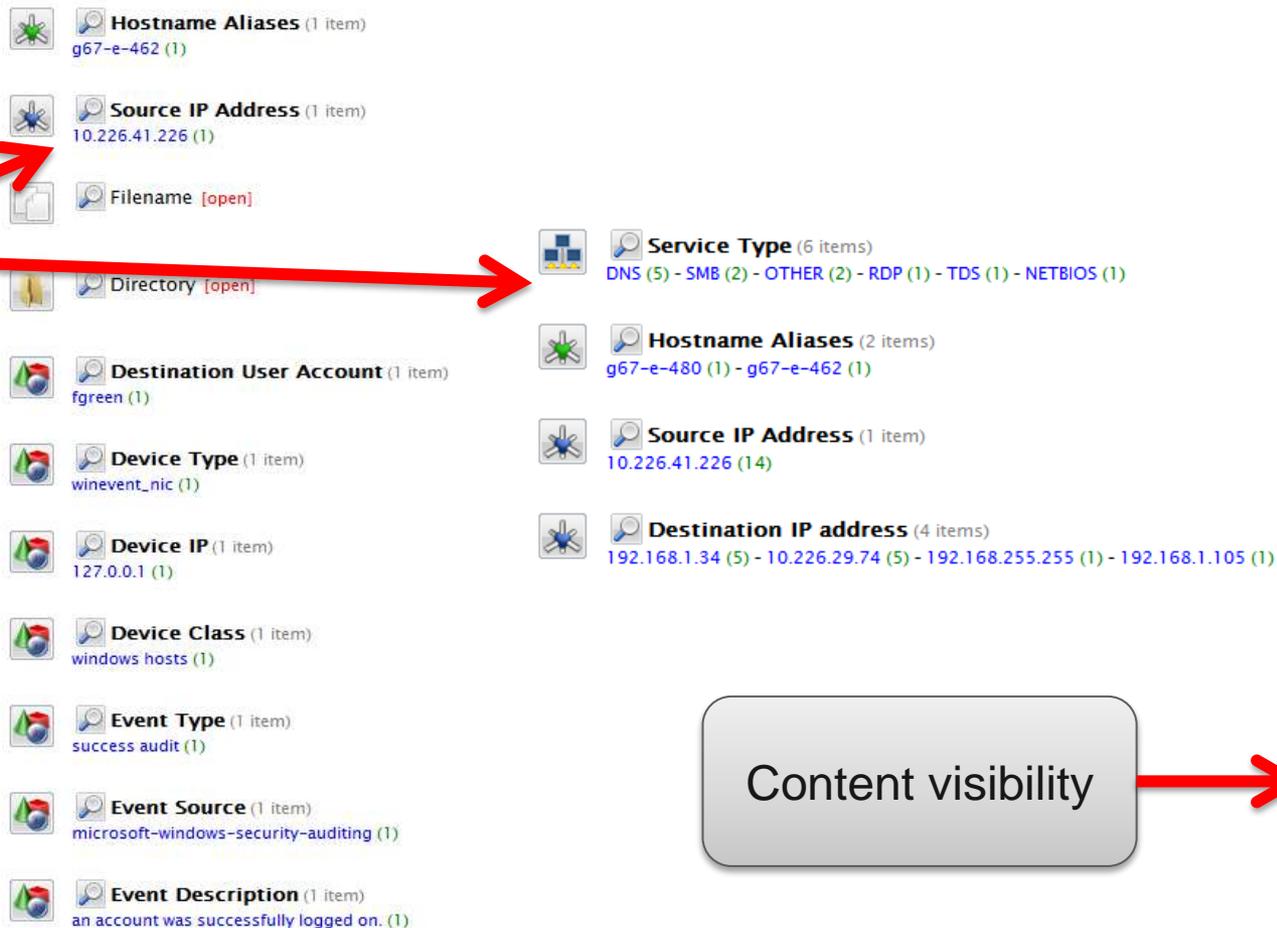
The screenshot displays a list of event categories and their associated counts:

- Hostname Aliases** (13 items): g67-e-480 (4) - g67-e-462 (2) - g67-e-461 (1) - g67-e-460 (1) - g67-e-459 (1) - g67-e-458 (1) - g67-e-457 (1) - g67-e-456 (1) - g67-e-455 (1) - g67-e-454 (1) - g67-e-453 (1) - g67-e-452 (1) - g67-e-451 (1)
- Source IP Address** (12 items): 10.226.41.226 (1) - 10.10.12.67 (1) - 10.10.12.61 (1) - 10.10.12.60 (1) - 10.10.12.59 (1) - 10.10.12.58 (1) - 10.10.12.56 (1) - 10.10.12.55 (1) - 10.10.12.54 (1) - 10.10.12.53 (1) - 10.10.12.52 (1) - 10.10.12.51 (1)
- Filename** [open]
- Directory** [open]
- Source User Account** (1 item): admin (1)
- Destination User Account** (2 items): fgreen (17) - system (4)
- Device Type** (1 item): winevent_nic (17)
- Device IP** (1 item): 127.0.0.1 (17)
- Device Class** (1 item): windows hosts (17)
- Event Type** (4 items): security audit failure (11) - information (4) - success audit (1) - security audit success (1)
- Event Source** (2 items): microsoft-windows-security-auditing (13) - security (4)
- Event Description** (6 items): an account failed to log on. (11) - successful logon. (2) - user account created. (1) - special privileges assigned to new logon. (1) - failed logon due to invalid access. (1) - an account was successfully logged on. (1)

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



Illegal Login – False Positive Resolution, Threat Analysis

Time	Service	Size	Events
2001-Jan-08 18:15:21	IP / TCP / TDS	38.96 KB	00:50:DA:04:EF:7F -> 00:A0:CC:51:A9:C9 10.226.41.226 -> 10.226.29.74 1752 -> 1433 (ms-sql-s) payload: 29525 medium: Ethernet tcp.flags: 26 streams: 2 packets: 192 lifetime: 6 action: login username: sa sql: select @@microsoftversion sql: SELECT ISNULL(SUSER_SNAME(), SUSER_NAME()) sql: if (object_id('master..sp_MSSQLDMO70_version') is not null) exec master..sp_MSSQLDMO70_version else select 0 sql: exec sp_MSdbuserpriv N'ver' sql: exec sp_MSgetversion sql: select platform() sql: exec master.dbo.sp_get_distributor sql: select FulltextServiceProperty(N'IsFulltextInstalled') sql: EXECUTE master.dbo.xp_regread N'HKEY_LOCAL_MACHINE', N'SOFTWARE\Microsoft\MSSQLServer\SQLLEW', N'SQLMailPolling' sql: exec sp_MSdbuseraccess N'db', N%' sql: exec sp_helpreplicationdboption action: attach database: FE_DB sql: exec sp_helppullsubscription sql: exec sp_helpmergepullsubscription action: attach database: master sql: exec sp_MSdbuseraccess N'perm', N'FE_DB' sql: exec sp_MSdbuseraccess N'perm', N'FE_DB' sql: exec sp_MSdbuseraccess N'perm', N'msdb' sql: exec sp_MSdbuseraccess N'perm', N'msdb'

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

Introducing RSA Security Analytics

The image displays a complex dashboard for RSA Security Analytics. The interface is divided into several sections:

- Alerts:** A list of alerts with details such as "Alerts (13 values)", "Threat Category (3 values)", "Threat Description (21 of 25)", and "Threat Source (3 values)".
- Device Information:** A section for "Decoder VM" showing system info like CPU (96%), Memory (1,380,028), and Disk (7.7 GB).
- Unified Dashboard:** A central dashboard with sections for "Security Analytics News", "Quick Tasks" (Configure Live Connection, Add a Device, Browse Live Resources, View My Jobs, Manage Live Subscriptions), "Featured Live Resources" (listing various threat feeds like "Network APT Threat IPs"), "Live Subscriptions", and "New Live Resources" (listing "Scamhaus EDROP List IP Ranges").
- Visualizations:** Includes "Gauges - Page 1 of 2" for Memory Process and CPU, "Timeline Charts - Page 1 of 1" for Memory Process Max, and "Historical Timeline Charts".
- Table:** A table on the right side of the Unified Dashboard with columns: Progress, Job Name, Pausing, Completed, Status, Type, Concentration, Stack, Log Details.



THANK YOU

