# Getting Ahead of Targeted Attacks Using Big Data and Intelligence Driven Security

**Eddie Schwartz**
RSA, The Security Division of EMC

TH-2004

Advanced

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

# Agenda

- Security Today and the Threat Landscape
- The Rise of Big Data and Intelligence-Driven Security
- Two Simple Case Studies
- Questions

# Security Today

# Security Today

- Over reliance on perimeter security and “pre-breach tooling” is a failing strategy
- Far too much focus on ISO27001 and compliance versus adversaries, material assets, and real pain points
- Cyber security needs an overhaul…

# Organizations Do Not Understand Their Adversaries

NATION STATE ACTORS

### Nation states

Government, defense industrial base, IP rich organizations

CRIMINALS

### Petty criminals

Unsophisticated

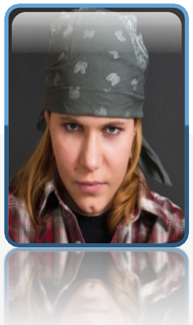
### Organized crime

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

NON-STATE ACTORS

### Insiders

Various reasons, including collaboration



### Cyber-terrorists / Hacktivists

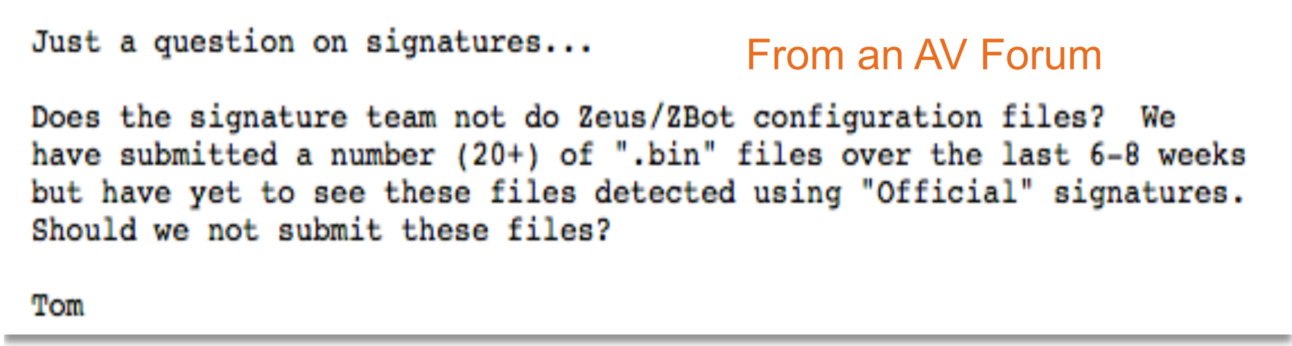
Political targets of opportunity, mass disruption

# Why is Prevention Inadequate as a Security Strategy?

Goal– Prevent or limit unauthorized connections in and out of the network

Reality – Adversaries' malware use "allowed paths" (DNS, HTTP, SMTP, etc) for C&C and data exfiltration channels from inside your network

Current AV and IPS are focused on vulnerabilities, are signature-based, require constant updates to remain useful. Due to malware production levels, these signatures lag from days to weeks

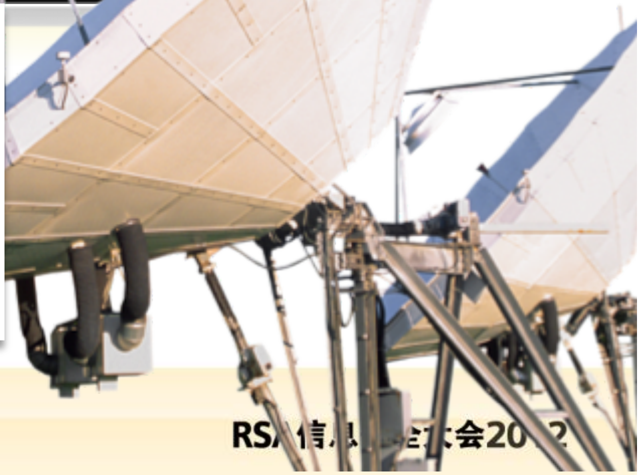


From an AV Forum

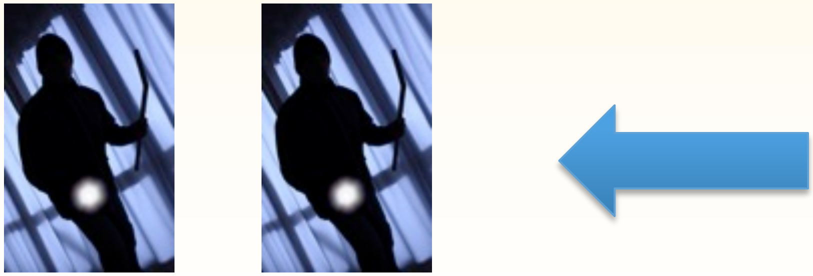
Just a question on signatures...

Does the signature team not do Zeus/ZBot configuration files? We have submitted a number (20+) of ".bin" files over the last 6-8 weeks but have yet to see these files detected using "Official" signatures. Should we not submit these files?

Tom

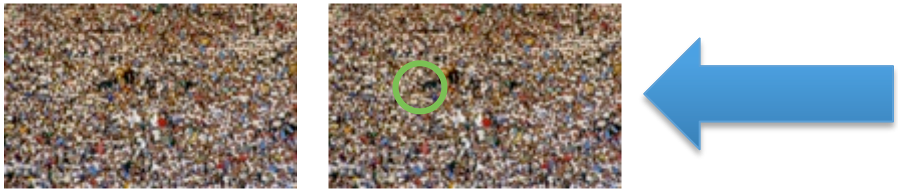


# Separating "Bad" from "Good" is an Increasingly Difficult Problem



= BAD

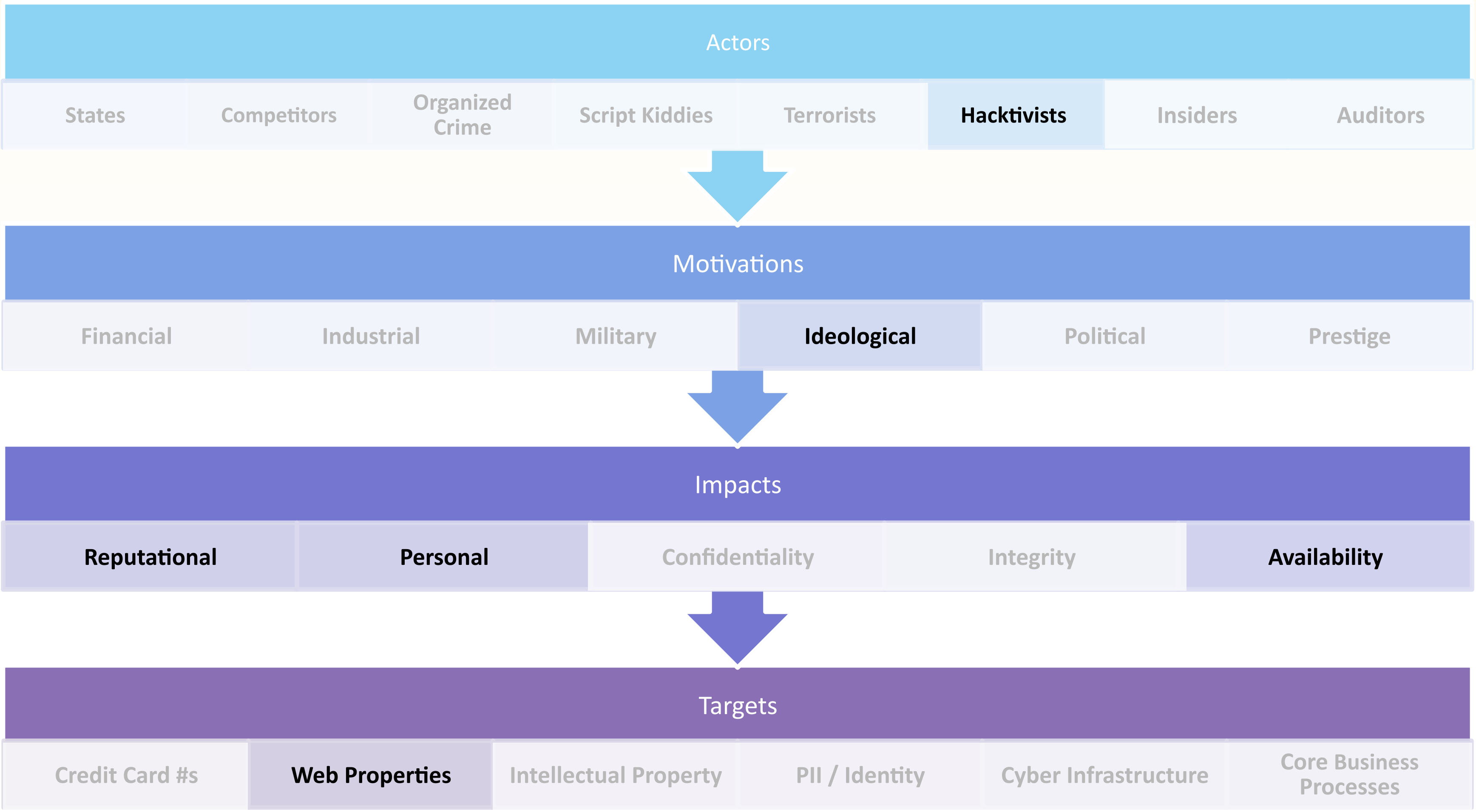
- Understand what "bad" looks like and look for similarities
  - Antivirus
  - Intrusion Prevention Systems
  - Thresholds exceeded



= BAD

- Understand what "good" looks like and look for meaningful differences
  - Network analysis and baselining
  - Anomaly detection
  - Predictive failure analysis

# Creating a Threat Model



Actors

States | Competitors | Organized Crime | Script Kiddies | Terrorists | **Hacktivists** | Insiders | Auditors

Motivations

Financial | Industrial | Military | **Ideological** | Political | Prestige

Impacts

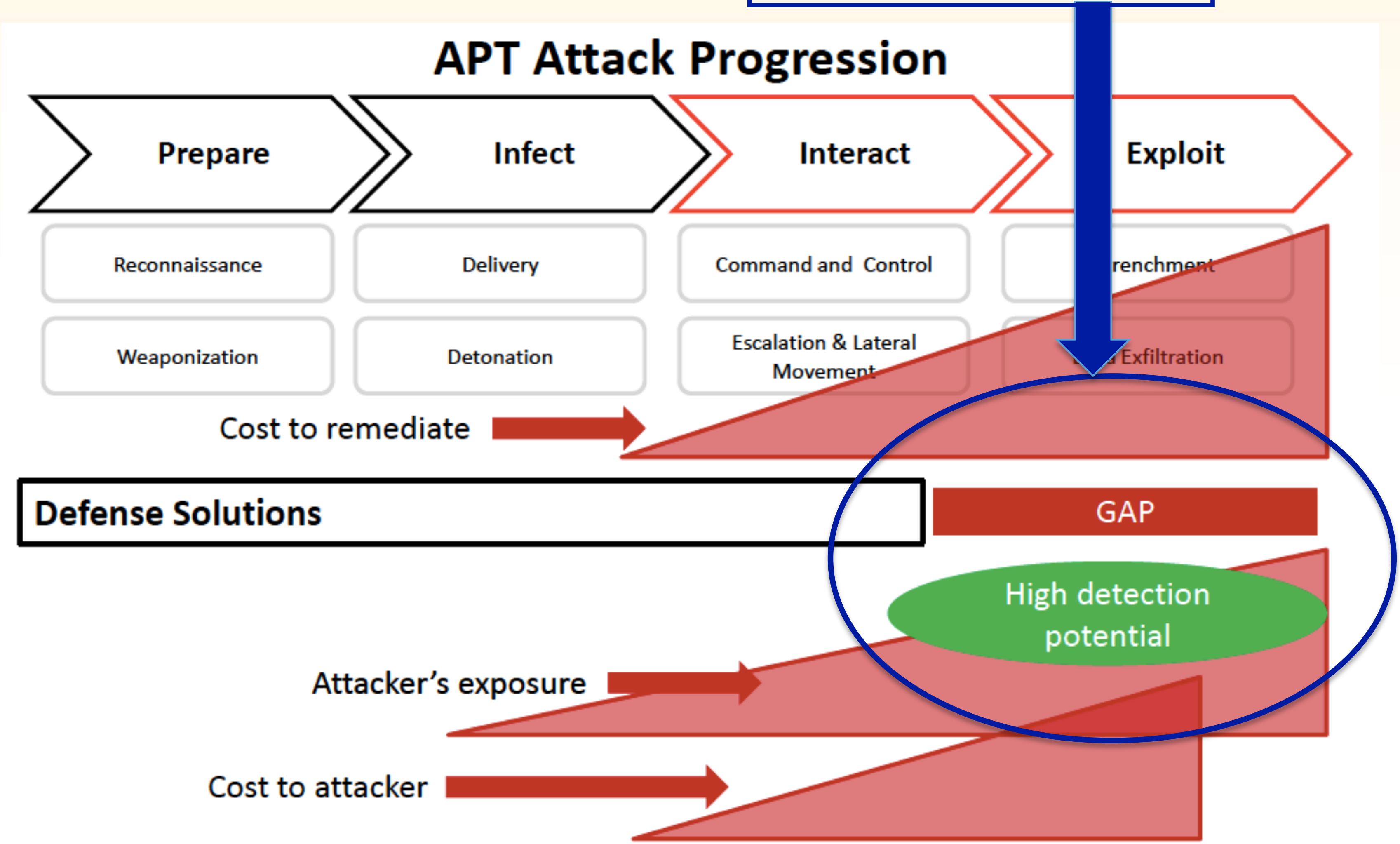
**Reputational** | **Personal** | Confidentiality | Integrity | **Availability**

Targets

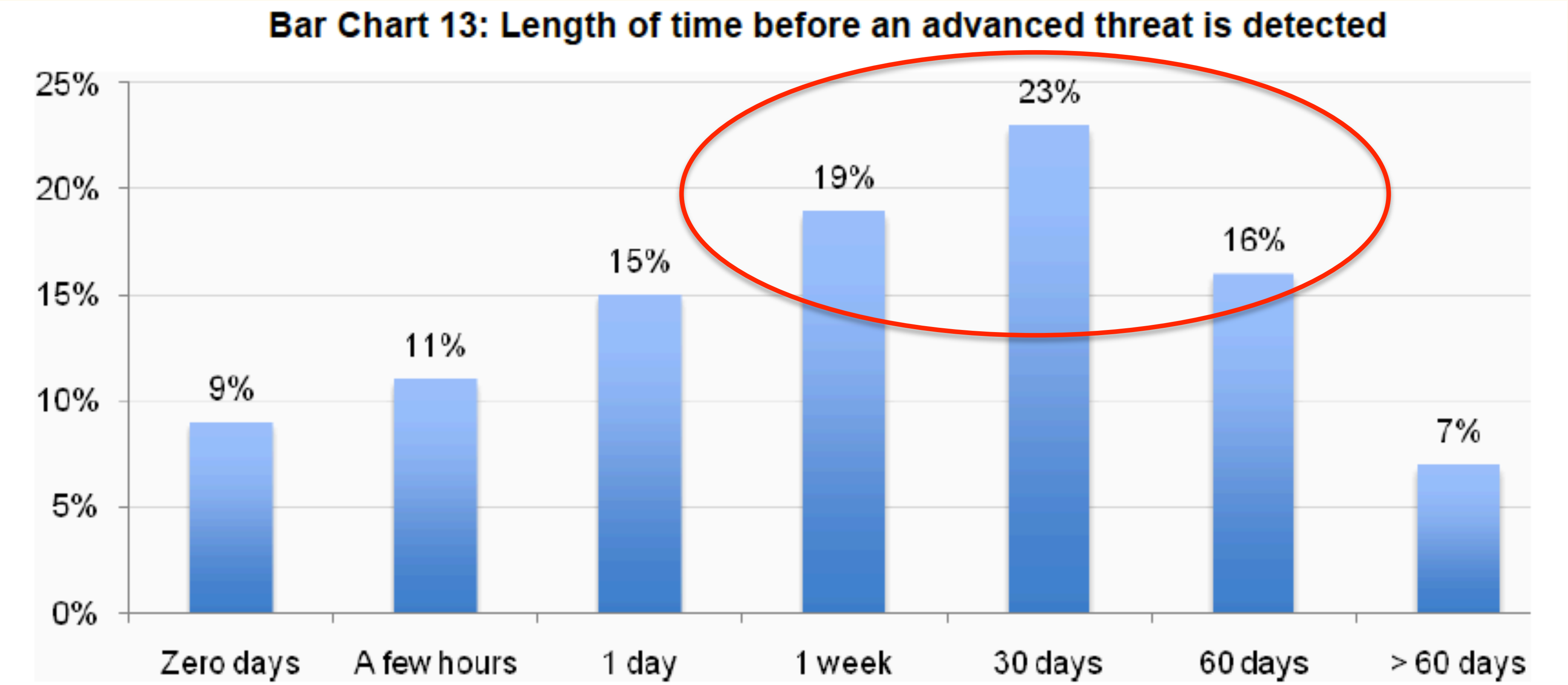
Credit Card #s | **Web Properties** | Intellectual Property | PII / Identity | Cyber Infrastructure | Core Business Processes

# Attacker “Free Time”

What level of resources belongs RIGHT HERE??



# Time to Detect – Not So Good..



Source: Ponemon Institute

# The Rise of Big Data and Security Intelligence

# What Is Big Data?

- “Big data is a term applied to data sets whose size is beyond the ability of commonly used software tools to capture, manage, and process within a tolerable elapsed time.” – Wikipedia
- “Data growth challenges are three-dimensional, increasing volume (amount of data), velocity (speed of data in/out), and variety (range of data types, sources).” – Analyst Report
- “44 percent of large organizations collect at least 1 terabyte of log files per month. 11 percent say that they capture more than 10 terabytes a month.” - ESG Research

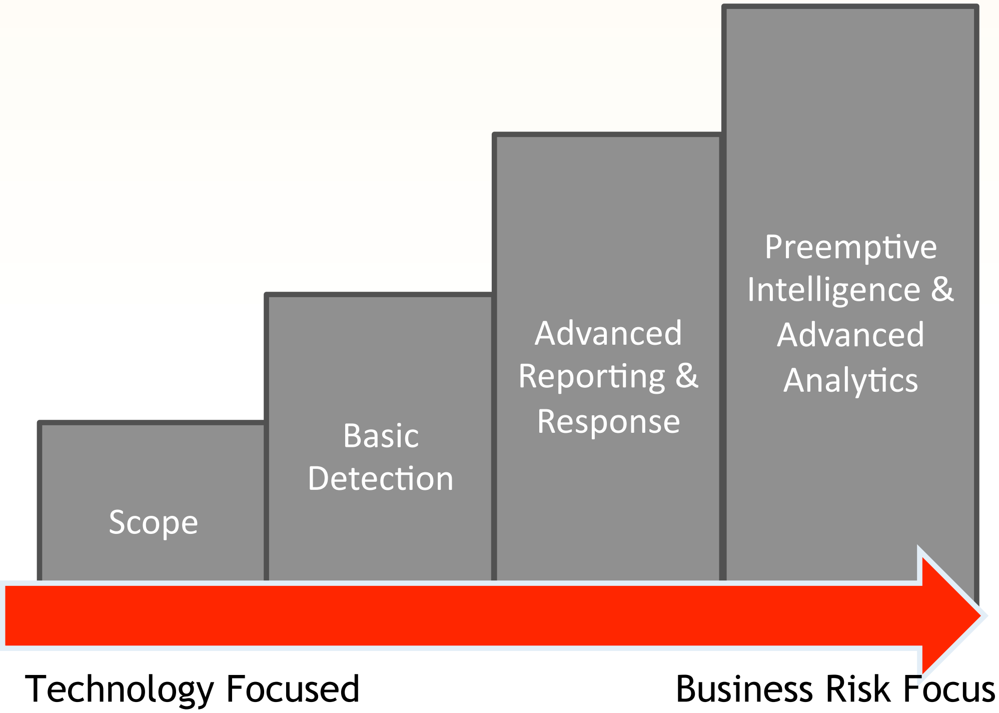
## Data Challenges for Security Operations

- Data Volume
  - Reducing data “noise”
- Accessibility
  - Centralization is not feasible
- Latency
  - How current is the data relative to problem at hand
- Retention
  - How much needs to be online versus in other methods (archival)
- Disjoint Sources
  - Incorporating context data
- Data Analysis (most important)
  - Query in real time

# Security Analyst Obstacles to Big Data Adoption

- Lack of Context
  - Gaining insight from data outside the system
- Vague Unstructured Data
  - Need familiar normalized data language
- System Data Reduction
  - Trying to filter “unimportant” data
- Automating Daily Tasks
  - Perform job functions still leaving time for new analysis

# So What is the Journey to a More Advanced Security Operations Approach?


Scope
Basic Detection
Advanced Reporting & Response
Preemptive Intelligence & Advanced Analytics
Technology Focused
Business Risk Focus

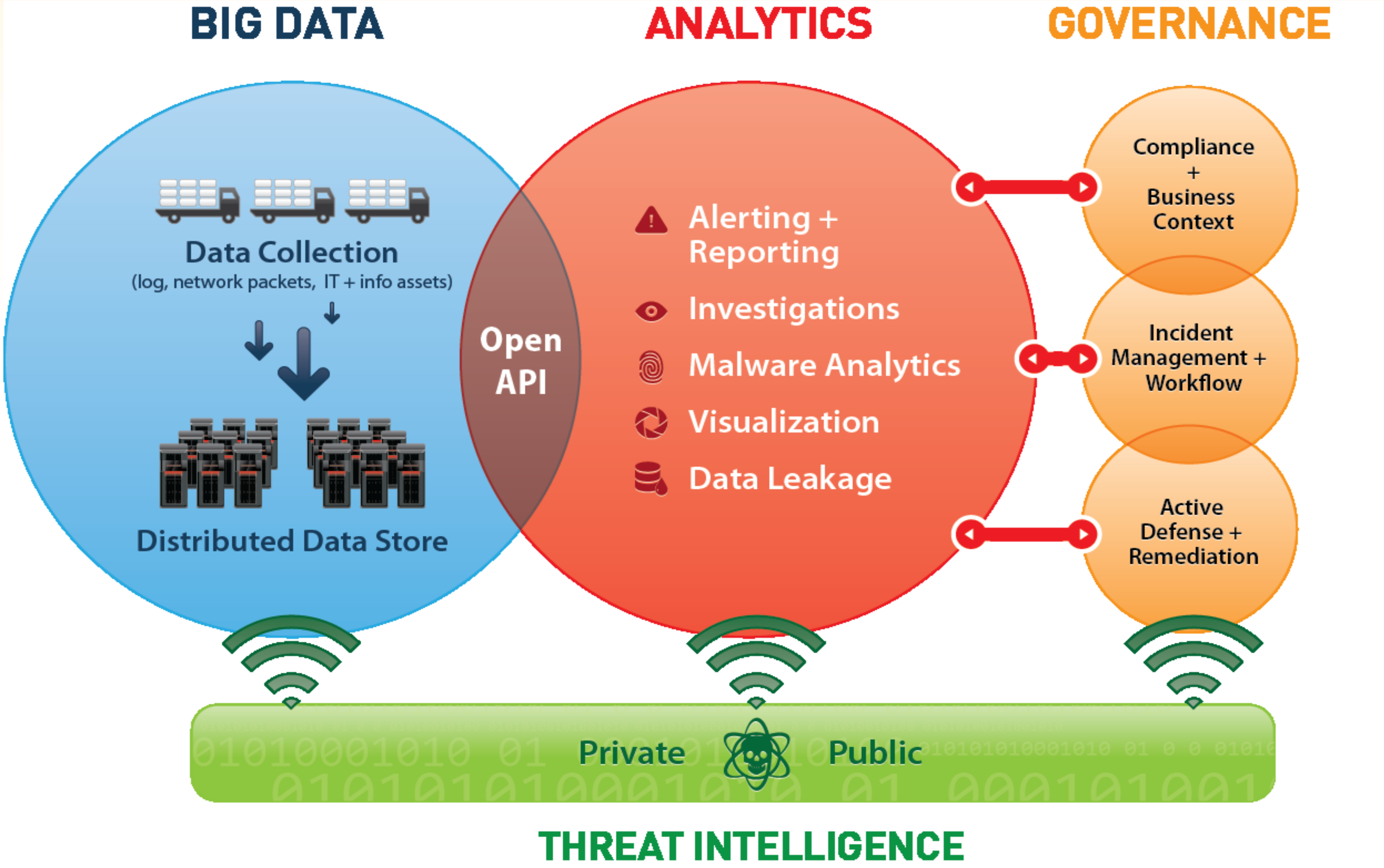
# Establish a Big Data Architecture Philosophy

- Leave Your Data Where It Is
  - Distributed data model
  - Centralization too inefficient
  - Eliminate data duplication
  - Save network bandwidth
- Provide Data To The People That Need It
  - Hierarchical data model
  - Accessibility
  - Query speeds
- Leverage Context Data
  - More context equals greater understanding

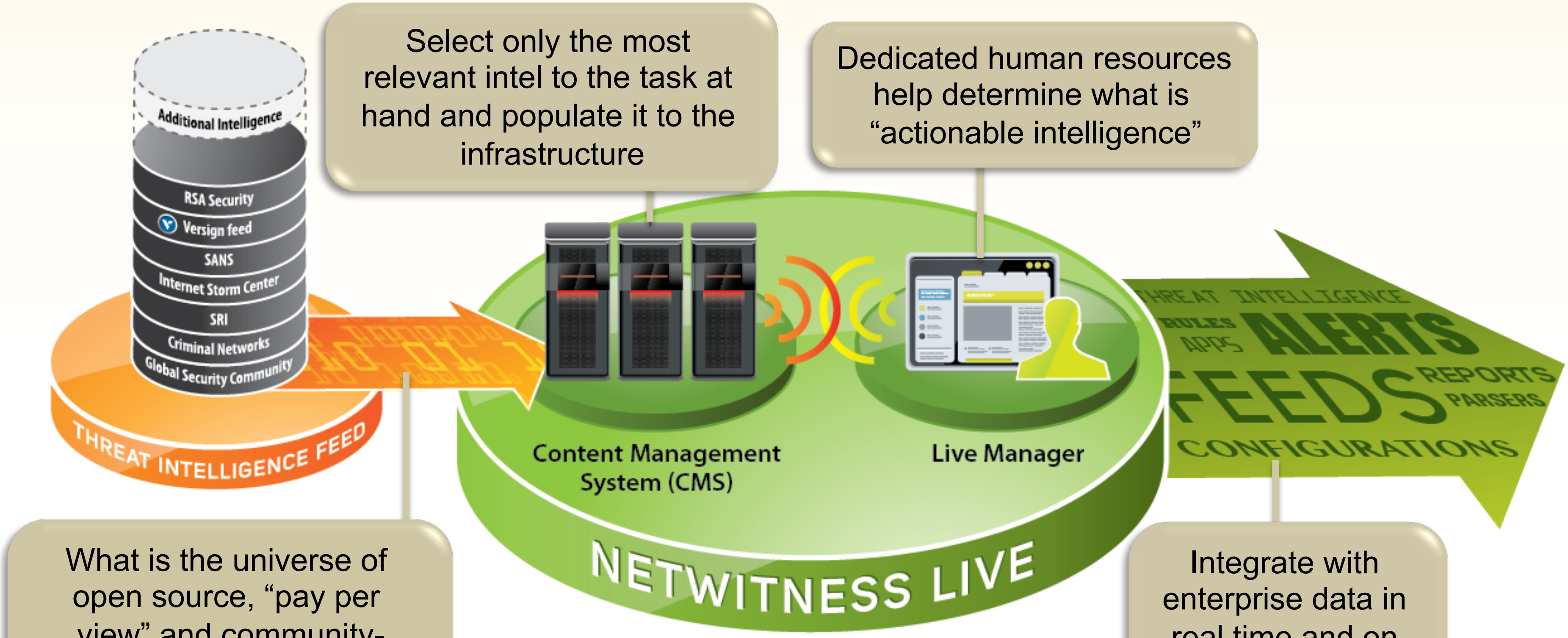
# Establish a Big Data Analysis Philosophy

- "Pre-mine" Data Intelligence
  - Add value (analytics and enrich) at time of capture
  - Quickly analyze important data
- Empower Ad Hoc Analysis
  - Don't "process" at the expense of the needle in the haystack
  - Enable "reduction analysis"
- Separate Functions with Differing Needs
  - Think in terms of best use of technology and temporal planes – what is each of these for you?
  - Complex Event Processing
  - Archiving
  - Real-time
  - Compliance

# Big Data + Intelligence – the Big Picture



# Fusion of Big Data with Threat Intelligence



Select only the most relevant intel to the task at hand and populate it to the infrastructure

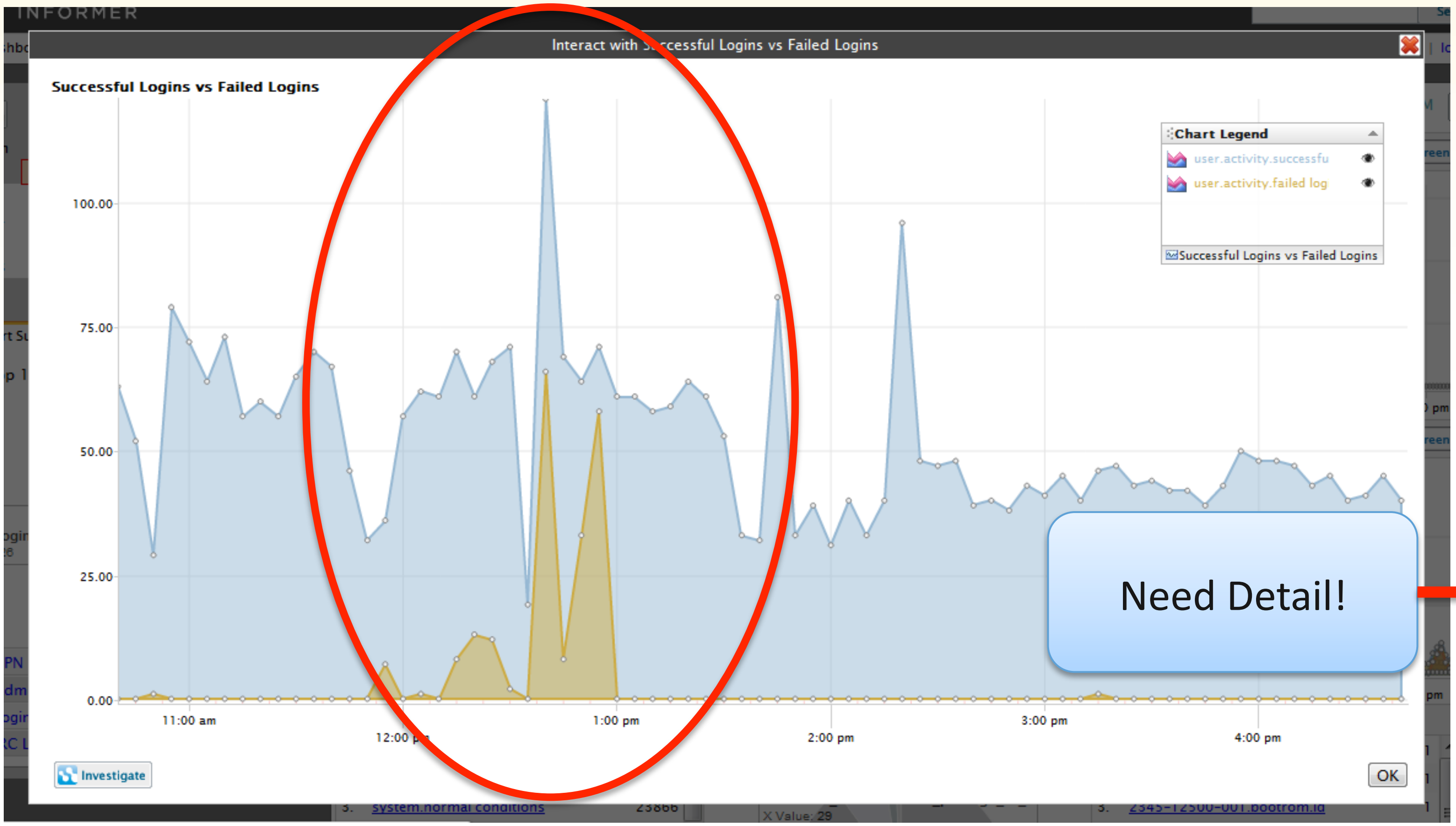
Dedicated human resources help determine what is “actionable intelligence”

What is the universe of open source, “pay per view” and community-based intelligence that can be gathered?

Integrate with enterprise data in real time and on other temporal planes

# Two Small Case Studies

# Full Packet and Log Overlay



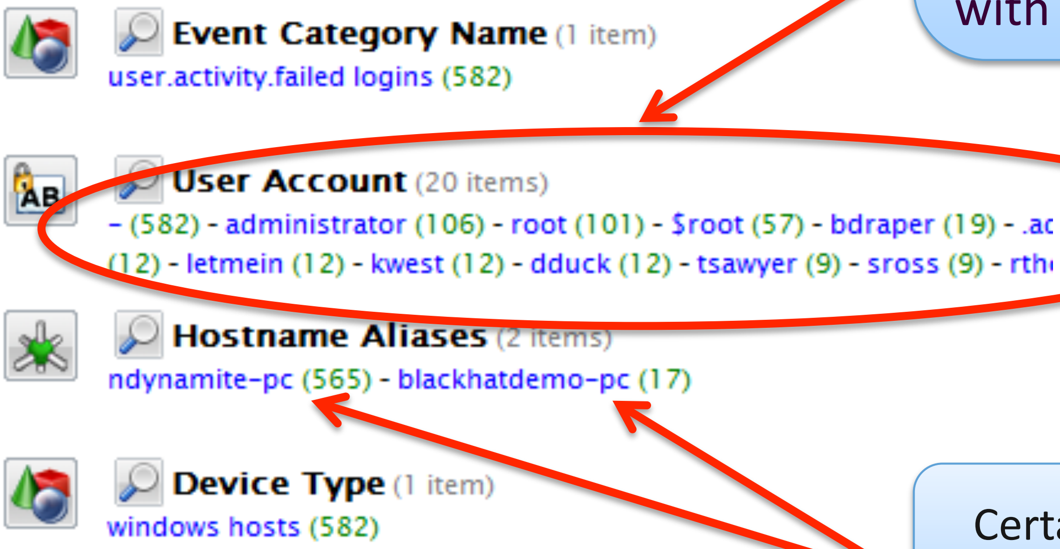
Need Detail!

Login charts show activity associated with successful and unsuccessful login attempts.

# Immediate understanding of a potential "owned" machine

Pivoting from the report based on a log entry 'failed logins'

Full packet sessions also show all user accounts and hostnames associated with the activity.



**Event Category Name** (1 item)

user.activity.failed logins (582)

**User Account** (20 items)

- (582) - administrator (106) - root (101) - $root (57) - bdraper (19) - .ac
(12) - letmein (12) - kwest (12) - dduck (12) - tsawyer (9) - sross (9) - rth

**Hostname Aliases** (2 items)

ndynamite-pc (565) - blackhatdemo-pc (17)

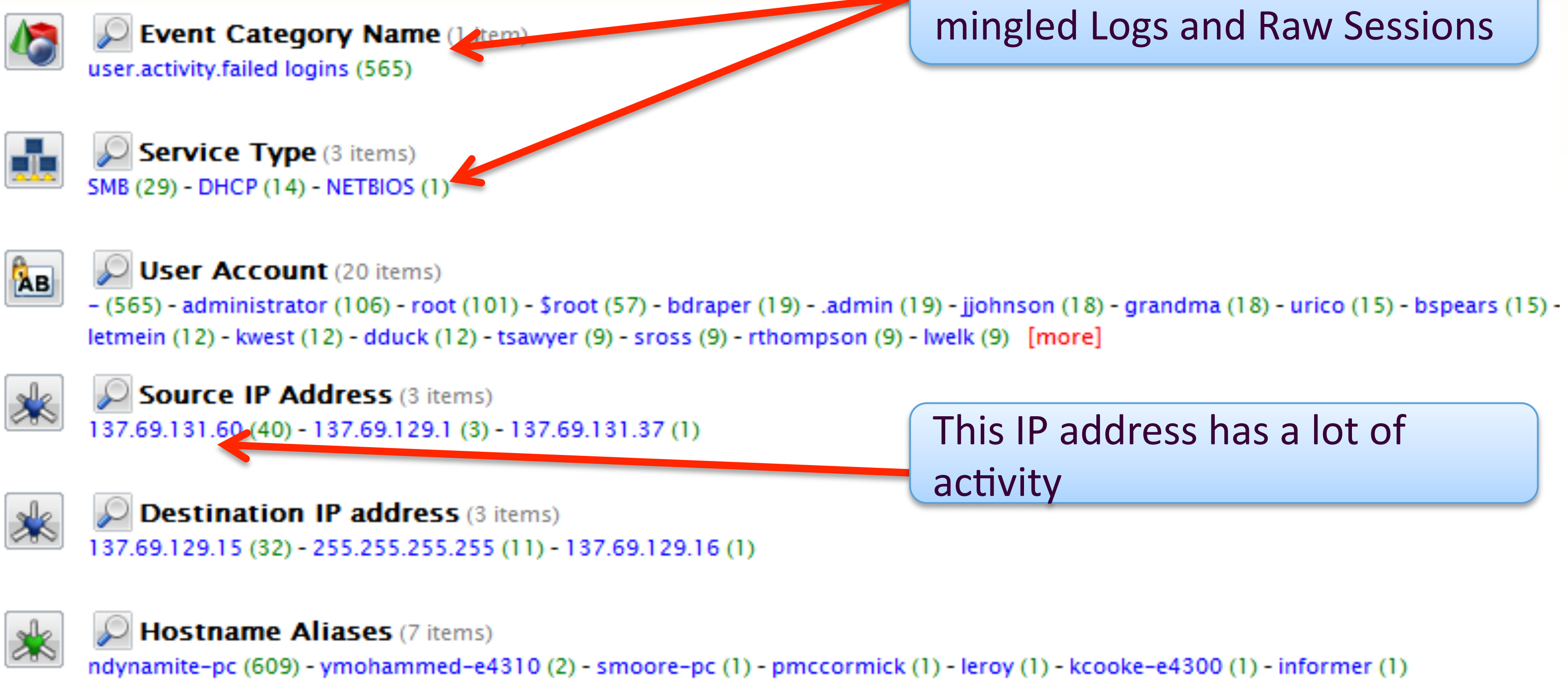
**Device Type** (1 item)

windows hosts (582)

Certain hostnames has more activity than others

# Pivoting on “ndynamite-pc”

Again we see the “big data” co-mingled Logs and Raw Sessions



**Event Category Name** (1 item)
user.activity.failed logins (565)

**Service Type** (3 items)
SMB (29) - DHCP (14) - NETBIOS (1)

**User Account** (20 items)
– (565) - administrator (106) - root (101) - $root (57) - bdraper (19) - .admin (19) - jjohnson (18) - grandma (18) - urico (15) - bspears (15) - letmein (12) - kwest (12) - dduck (12) - tsawyer (9) - sross (9) - rthompson (9) - lwelk (9) [more]

**Source IP Address** (3 items)
137.69.131.60 (40) - 137.69.129.1 (3) - 137.69.131.37 (1)

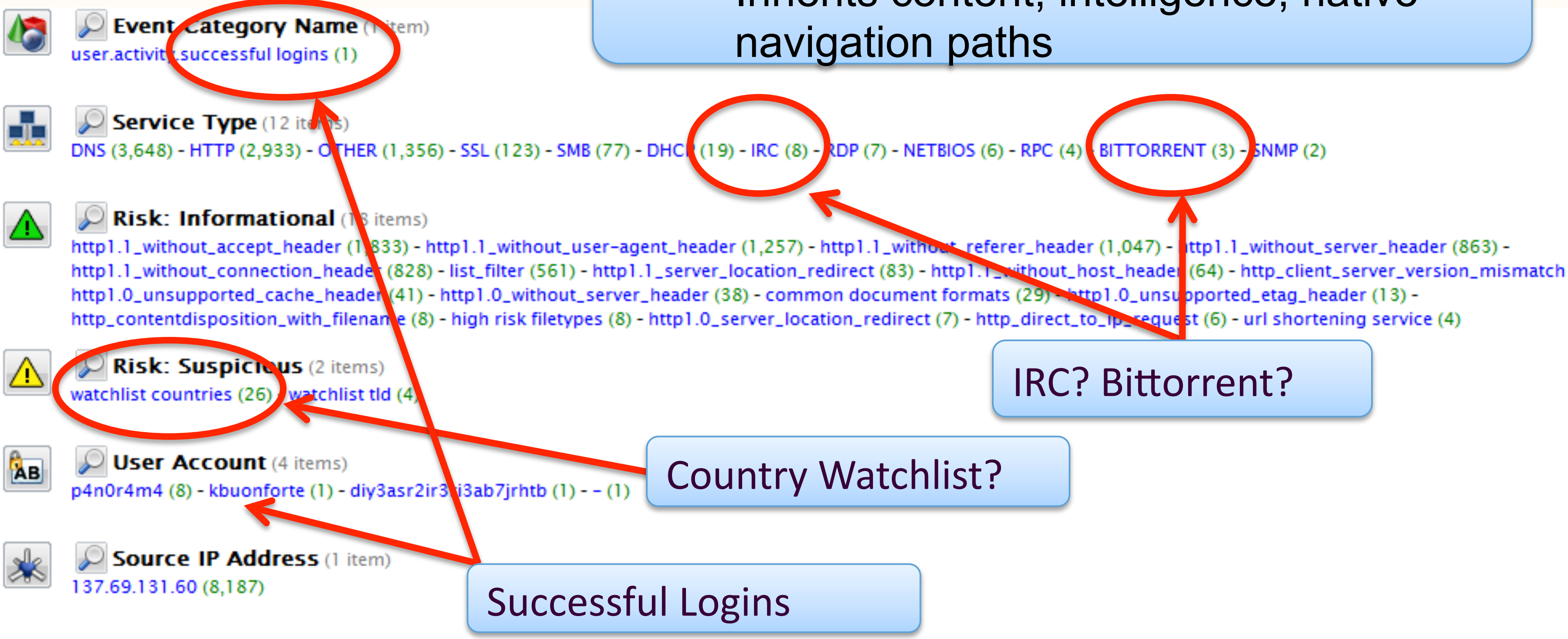
**Destination IP address** (3 items)
137.69.129.15 (32) - 255.255.255.255 (11) - 137.69.129.16 (1)

**Hostname Aliases** (7 items)
ndynamite-pc (609) - ymohammed-e4310 (2) - smoore-pc (1) - pmccormick (1) - leroy (1) - kcooke-e4300 (1) - informer (1)

This IP address has a lot of activity

# Pivot based on IP address 137.69.131.60

- Profile all activity for IP Address
  - Inherits content, intelligence, native navigation paths



**Event Category Name** (1 item)
user.activity.successful logins (1)

**Service Type** (12 items)
DNS (3,648) - HTTP (2,933) - OTHER (1,356) - SSL (123) - SMB (77) - DHCP (19) - IRC (8) - RDP (7) - NETBIOS (6) - RPC (4) - BITTORRENT (3) - SNMP (2)

**Risk: Informational** (18 items)
http1.1_without_accept_header (1,833) - http1.1_without_user-agent_header (1,257) - http1.1_without_referer_header (1,047) - http1.1_without_server_header (863) - http1.1_without_connection_header (828) - list_filter (561) - http1.1_server_location_redirect (83) - http1.1_without_host_header (64) - http_client_server_version_mismatch http1.0_unsupported_cache_header (41) - http1.0_without_server_header (38) - common document formats (29) - http1.0_unsupported_etag_header (13) - http_contentdisposition_with_filename (8) - high risk filetypes (8) - http1.0_server_location_redirect (7) - http_direct_to_ip_request (6) - url shortening service (4)

**Risk: Suspicious** (2 items)
watchlist countries (26) - watchlist tld (4)

**User Account** (4 items)
p4n0r4m4 (8) - kbuonforte (1) - diy3asr2ir3 i3ab7jrhtb (1) - - (1)

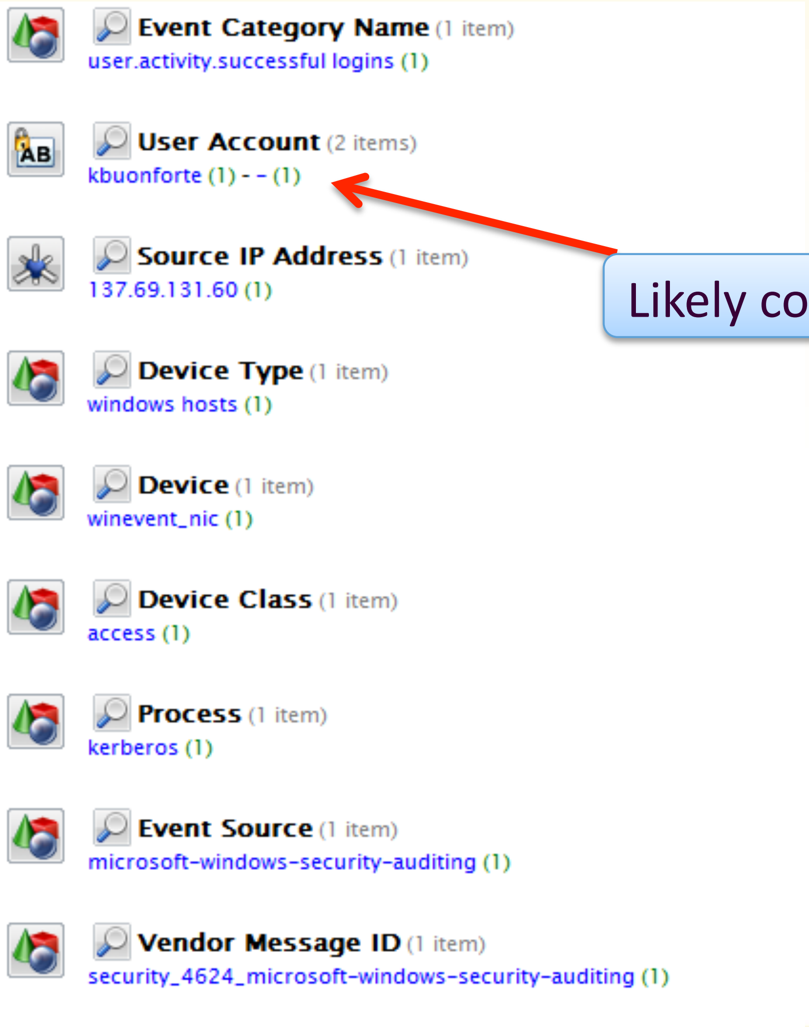
**Source IP Address** (1 item)
137.69.131.60 (8,187)

IRC? Bittorrent?

Country Watchlist?

Successful Logins

# Log Event for Successful Login Entry



**Event Category Name** (1 item)
user.activity.successful logins (1)

**User Account** (2 items)
kbuonforte (1) - - (1)

**Source IP Address** (1 item)
137.69.131.60 (1)

**Device Type** (1 item)
windows hosts (1)

**Device** (1 item)
winevent_nic (1)

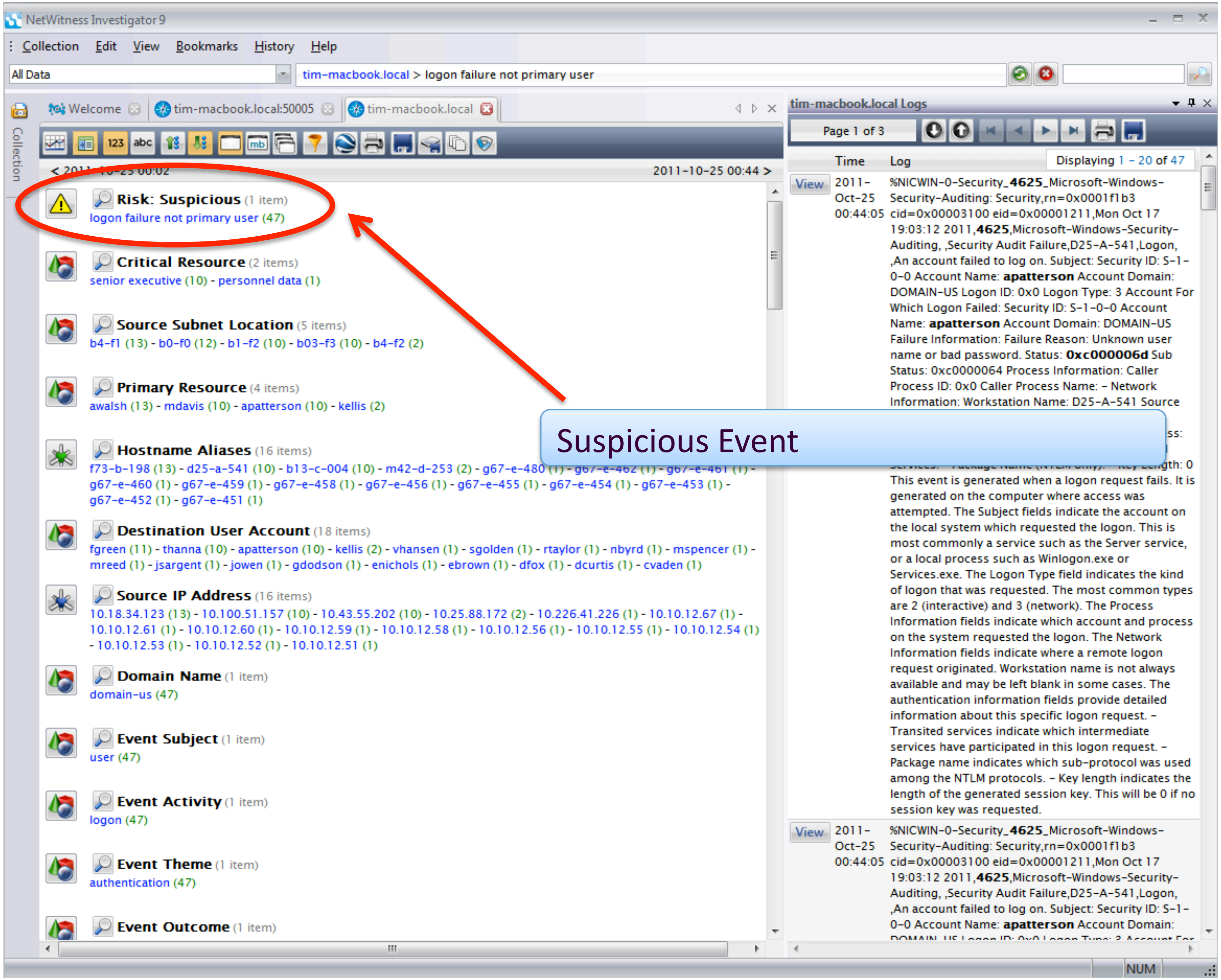
**Device Class** (1 item)
access (1)

**Process** (1 item)
kerberos (1)

**Event Source** (1 item)
microsoft-windows-security-auditing (1)

**Vendor Message ID** (1 item)
security_4624_microsoft-windows-security-auditing (1)

Likely compromised ID



tim-macbook.local > logon failure not primary user

< 2011-10-25 00:02 2011-10-25 00:44 >

**Risk: Suspicious** (1 item)
logon failure not primary user (47)

**Critical Resource** (2 items)
senior executive (10) - personnel data (1)

**Source Subnet Location** (5 items)
b4-f1 (13) - b0-f0 (12) - b1-f2 (10) - b03-f3 (10) - b4-f2 (2)

**Primary Resource** (4 items)
awalsh (13) - mdavis (10) - apatterson (10) - kellis (2)

**Hostname Aliases** (16 items)
f73-b-198 (13) - d25-a-541 (10) - b13-c-004 (10) - m42-d-253 (2) - g67-e-480 (1) - g67-e-462 (1) - g67-e-461 (1) - g67-e-460 (1) - g67-e-459 (1) - g67-e-458 (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)

**Destination User Account** (18 items)
fgreen (11) - thanna (10) - apatterson (10) - kellis (2) - vhansen (1) - sgolden (1) - rtaylor (1) - nbyrd (1) - mspencer (1) - mreed (1) - jsargent (1) - jowen (1) - gdodson (1) - enichols (1) - ebrown (1) - dfox (1) - dcurtis (1) - cvaden (1)

**Source IP Address** (16 items)
10.18.34.123 (13) - 10.100.51.157 (10) - 10.43.55.202 (10) - 10.25.88.172 (2) - 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)

**Domain Name** (1 item)
domain-us (47)

**Event Subject** (1 item)
user (47)

**Event Activity** (1 item)
logon (47)

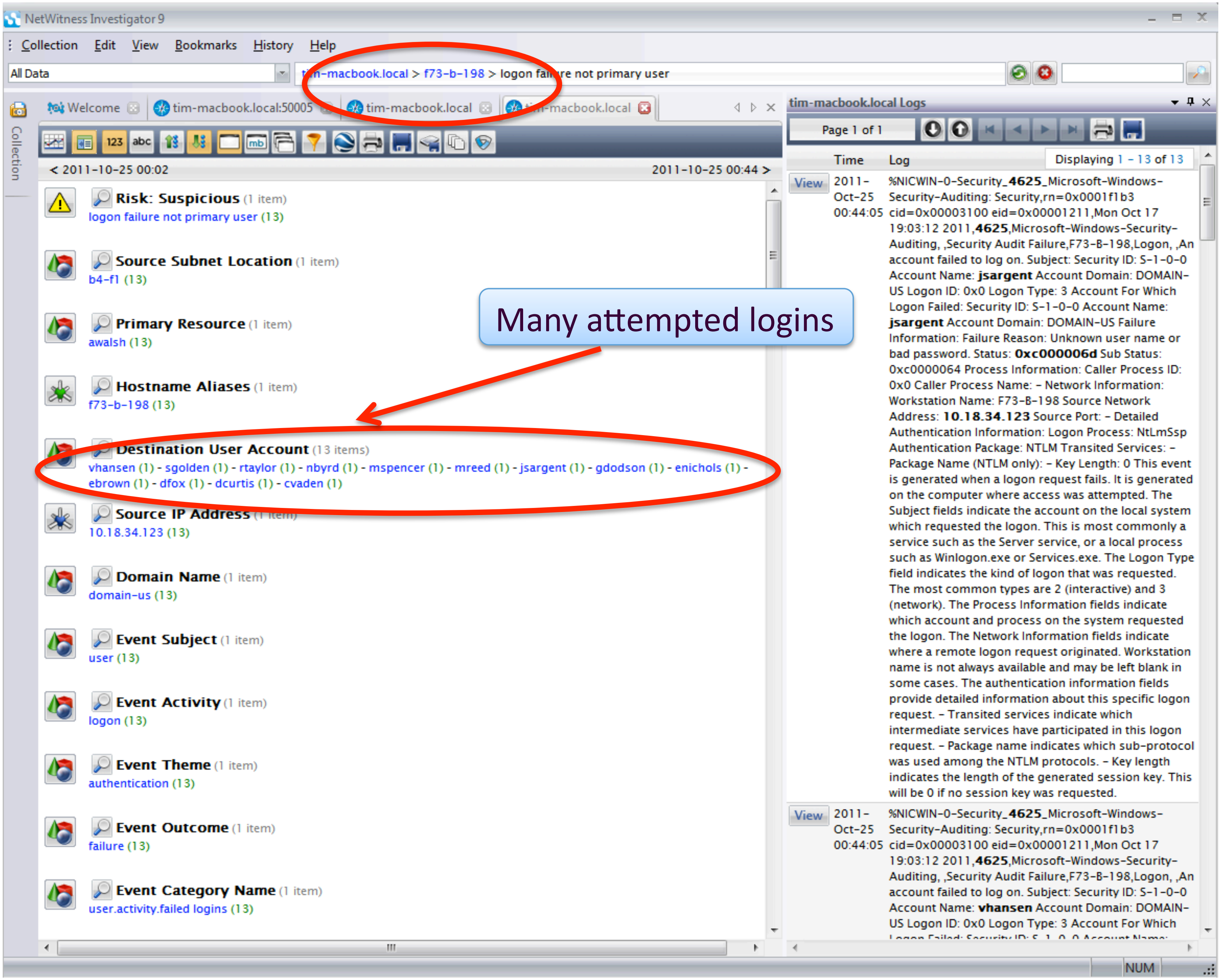
**Event Theme** (1 item)
authentication (47)

**Event Outcome** (1 item)

| | Time | Log |
|---|---|---|
| View | 2011-Oct-25 00:44:05 | %NICWIN-0-Security_**4625**_Microsoft-Windows-Security-Auditing: Security,rn=0x0001f1b3 cid=0x00003100 eid=0x00001211,Mon Oct 17 19:03:12 2011,**4625**,Microsoft-Windows-Security-Auditing, ,Security Audit Failure,D25-A-541,Logon, ,An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: **apatterson** Account Domain: DOMAIN-US Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: **apatterson** Account Domain: DOMAIN-US Failure Information: Failure Reason: Unknown user name or bad password. Status: **0xc000006d** Sub Status: 0xc0000064 Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: D25-A-541 Source ss: Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| View | 2011-Oct-25 00:44:05 | %NICWIN-0-Security_**4625**_Microsoft-Windows-Security-Auditing: Security,rn=0x0001f1b3 cid=0x00003100 eid=0x00001211,Mon Oct 17 19:03:12 2011,**4625**,Microsoft-Windows-Security-Auditing, ,Security Audit Failure,D25-A-541,Logon, ,An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: **apatterson** Account Domain: DOMAIN-US Logon ID: 0x0 Logon Type: 3 Account For |

Displaying 1 - 20 of 47

Suspicious Event



Many attempted logins

< 2011-10-25 00:02 2011-10-25 00:44 >

**Risk: Suspicious** (1 item)
logon failure not primary user (13)

**Source Subnet Location** (1 item)
b4-f1 (13)

**Primary Resource** (1 item)
awalsh (13)

**Hostname Aliases** (1 item)
f73-b-198 (13)

**Destination User Account** (13 items)
vhansen (1) - sgolden (1) - rtaylor (1) - nbyrd (1) - mspencer (1) - mreed (1) - jsargent (1) - gdodson (1) - enichols (1) - ebrown (1) - dfox (1) - dcurtis (1) - cvaden (1)

**Source IP Address** (1 item)
10.18.34.123 (13)

**Domain Name** (1 item)
domain-us (13)

**Event Subject** (1 item)
user (13)

**Event Activity** (1 item)
logon (13)

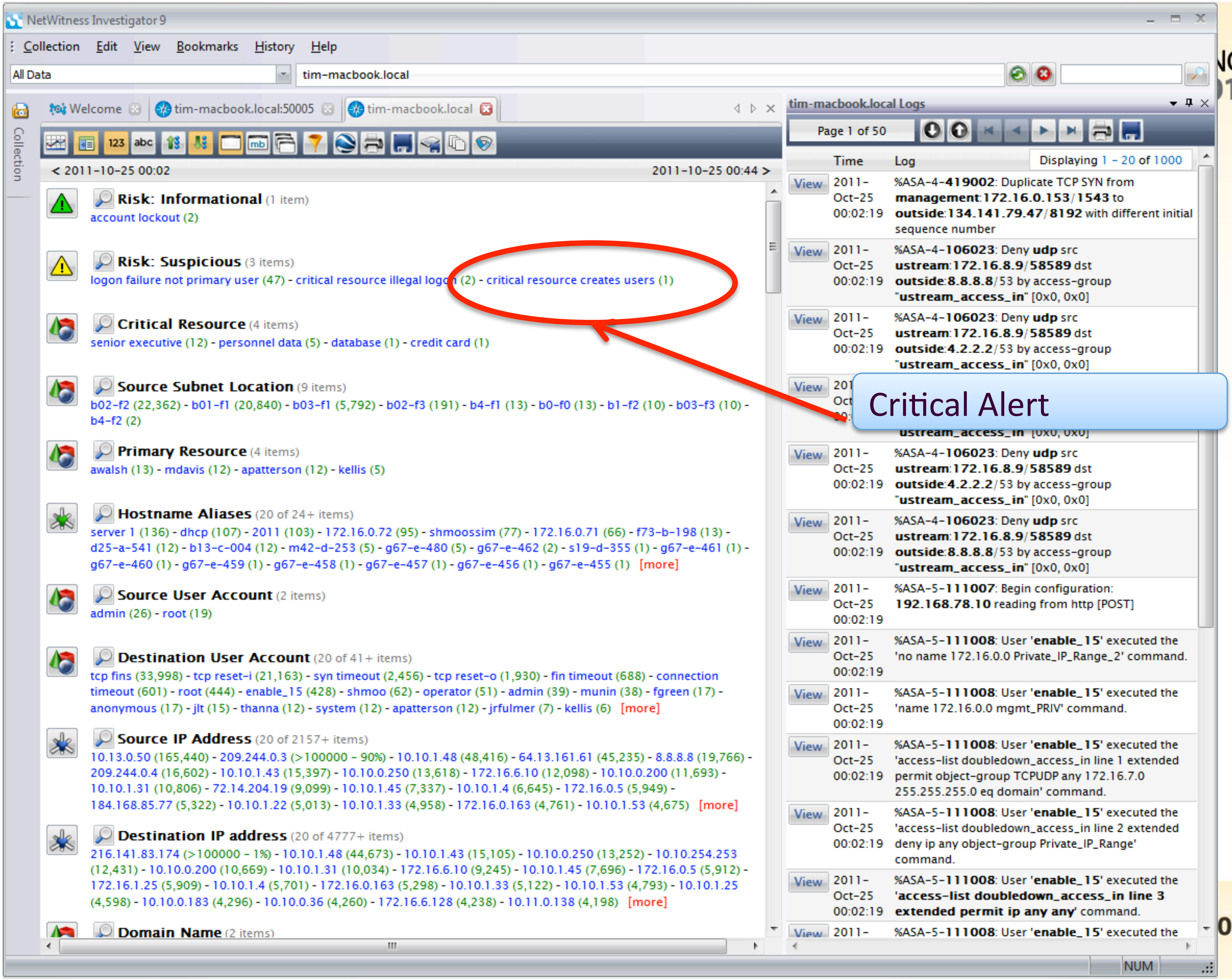
**Event Theme** (1 item)
authentication (13)

**Event Outcome** (1 item)
failure (13)

**Event Category Name** (1 item)
user.activity.failed logins (13)

| | Time | Log |
|---|---|---|
| View | 2011-Oct-25 00:44:05 | %NICWIN-0-Security_**4625**_Microsoft-Windows-Security-Auditing: Security,rn=0x0001f1b3 cid=0x00003100 eid=0x00001211,Mon Oct 17 19:03:12 2011,**4625**,Microsoft-Windows-Security-Auditing, ,Security Audit Failure,F73-B-198,Logon, ,An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: **jsargent** Account Domain: DOMAIN-US Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: **jsargent** Account Domain: DOMAIN-US Failure Information: Failure Reason: Unknown user name or bad password. Status: **0xc000006d** Sub Status: 0xc0000064 Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: F73-B-198 Source Network Address: **10.18.34.123** Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| View | 2011-Oct-25 00:44:05 | %NICWIN-0-Security_**4625**_Microsoft-Windows-Security-Auditing: Security,rn=0x0001f1b3 cid=0x00003100 eid=0x00001211,Mon Oct 17 19:03:12 2011,**4625**,Microsoft-Windows-Security-Auditing, ,Security Audit Failure,F73-B-198,Logon, ,An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: **vhansen** Account Domain: DOMAIN-US Logon ID: 0x0 Logon Type: 3 Account For Which |

Displaying 1 - 13 of 13



**Risk: Informational** (1 item)
account lockout (2)

**Risk: Suspicious** (3 items)
logon failure not primary user (47) - critical resource illegal logon (2) - critical resource creates users (1)

**Critical Resource** (4 items)
senior executive (12) - personnel data (5) - database (1) - credit card (1)

**Source Subnet Location** (9 items)
b02-f2 (22,362) - b01-f1 (20,840) - b03-f1 (5,792) - b02-f3 (191) - b4-f1 (13) - b0-f0 (13) - b1-f2 (10) - b03-f3 (10) - b4-f2 (2)

**Primary Resource** (4 items)
awalsh (13) - mdavis (12) - apatterson (12) - kellis (5)

**Hostname Aliases** (20 of 24+ items)
server 1 (136) - dhcp (107) - 2011 (103) - 172.16.0.72 (95) - shmoossim (77) - 172.16.0.71 (66) - f73-b-198 (13) - d25-a-541 (12) - b13-c-004 (12) - m42-d-253 (5) - g67-e-480 (5) - g67-e-462 (2) - s19-d-355 (1) - 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) [more]

**Source User Account** (2 items)
admin (26) - root (19)

**Destination User Account** (20 of 41+ items)
tcp fins (33,998) - tcp reset-i (21,163) - syn timeout (2,456) - tcp reset-o (1,930) - fin timeout (688) - connection timeout (601) - root (444) - enable_15 (428) - shmoo (62) - operator (51) - admin (39) - munin (38) - fgreen (17) - anonymous (17) - jlt (15) - thanna (12) - system (12) - apatterson (12) - jrfulmer (7) - kellis (6) [more]

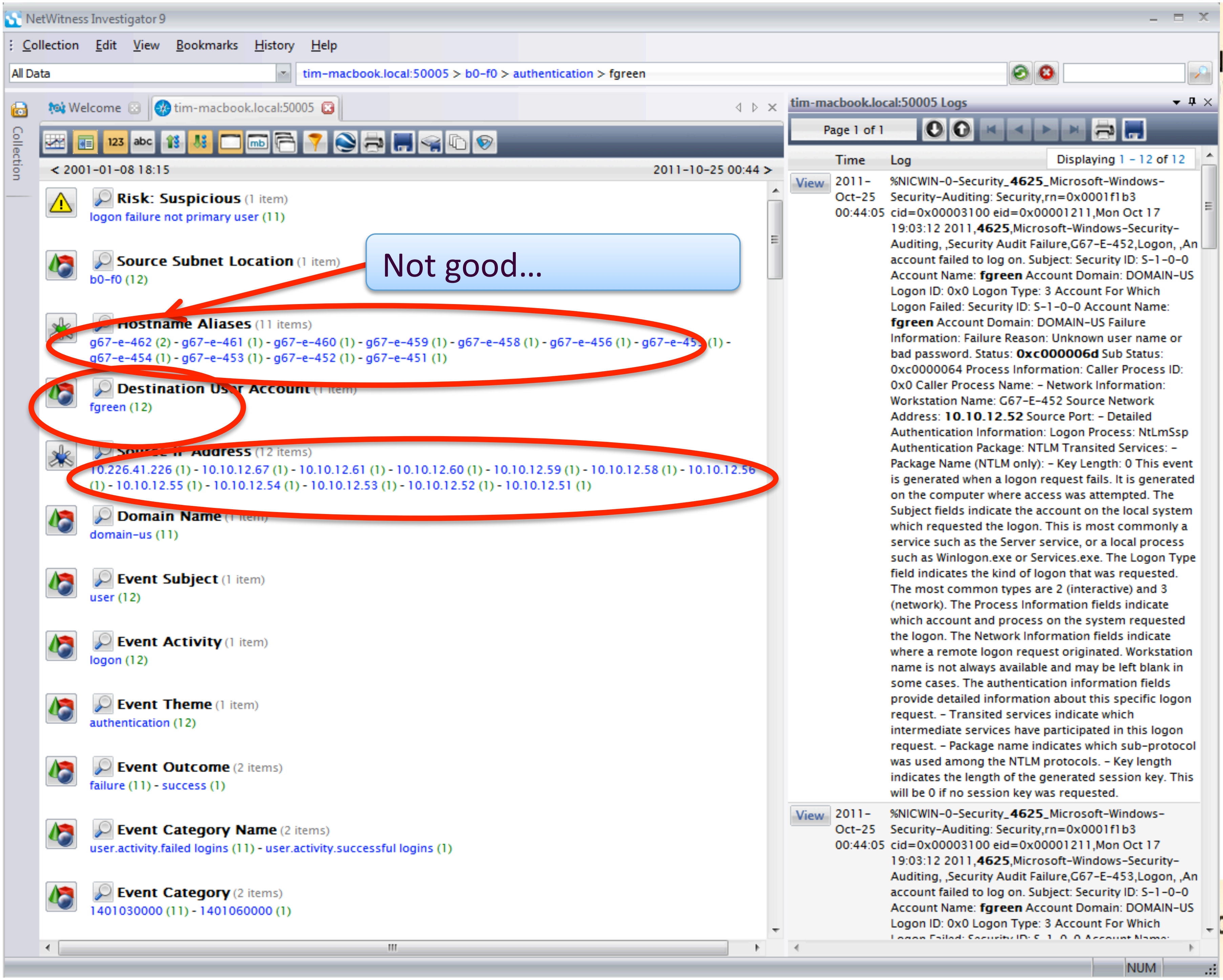
**Source IP Address** (20 of 2157+ items)
10.13.0.50 (165,440) - 209.244.0.3 (>100000 - 90%) - 10.10.1.48 (48,416) - 64.13.161.61 (45,235) - 8.8.8.8 (19,766) - 209.244.0.4 (16,602) - 10.10.1.43 (15,397) - 10.10.0.250 (13,618) - 172.16.6.10 (12,098) - 10.10.0.200 (11,693) - 10.10.1.31 (10,806) - 72.14.204.19 (9,099) - 10.10.1.45 (7,337) - 10.10.1.4 (6,645) - 172.16.0.5 (5,949) - 184.168.85.77 (5,322) - 10.10.1.22 (5,013) - 10.10.1.33 (4,958) - 172.16.0.163 (4,761) - 10.10.1.53 (4,675) [more]

**Destination IP address** (20 of 4777+ items)
216.141.83.174 (>100000 - 1%) - 10.10.1.48 (44,673) - 10.10.1.43 (15,105) - 10.10.0.250 (13,252) - 10.10.254.253 (12,431) - 10.10.0.200 (10,669) - 10.10.1.31 (10,034) - 172.16.6.10 (9,245) - 10.10.1.45 (7,696) - 172.16.0.5 (5,912) - 172.16.1.25 (5,909) - 10.10.1.4 (5,701) - 172.16.0.163 (5,298) - 10.10.1.33 (5,122) - 10.10.1.53 (4,793) - 10.10.1.25 (4,598) - 10.10.0.183 (4,296) - 10.10.0.36 (4,260) - 172.16.6.128 (4,238) - 10.11.0.138 (4,198) [more]

**Domain Name** (2 items)

```
     Time          Log                                              Displaying 1 - 20 of 1000
View 2011-Oct-25   %ASA-4-419002: Duplicate TCP SYN from management:172.16.0.153/1543 to
     00:02:19      outside:134.141.79.47/8192 with different initial sequence number
View 2011-Oct-25   %ASA-4-106023: Deny udp src ustream:172.16.8.9/58589 dst
     00:02:19      outside:8.8.8.8/53 by access-group "ustream_access_in" [0x0, 0x0]
View 2011-Oct-25   %ASA-4-106023: Deny udp src ustream:172.16.8.9/58589 dst
     00:02:19      outside:4.2.2.2/53 by access-group "ustream_access_in" [0x0, 0x0]
View 201 Oct                                    ustream_access_in" [0x0, 0x0]
View 2011-Oct-25   %ASA-4-106023: Deny udp src ustream:172.16.8.9/58589 dst
     00:02:19      outside:4.2.2.2/53 by access-group "ustream_access_in" [0x0, 0x0]
View 2011-Oct-25   %ASA-4-106023: Deny udp src ustream:172.16.8.9/58589 dst
     00:02:19      outside:8.8.8.8/53 by access-group "ustream_access_in" [0x0, 0x0]
View 2011-Oct-25   %ASA-5-111007: Begin configuration: 192.168.78.10 reading from http [POST]
     00:02:19
View 2011-Oct-25   %ASA-5-111008: User 'enable_15' executed the 'no name 172.16.0.0 Private_IP_Range_2' command.
     00:02:19
View 2011-Oct-25   %ASA-5-111008: User 'enable_15' executed the 'name 172.16.0.0 mgmt_PRIV' command.
     00:02:19
View 2011-Oct-25   %ASA-5-111008: User 'enable_15' executed the 'access-list doubledown_access_in line 1 extended
     00:02:19      permit object-group TCPUDP any 172.16.7.0 255.255.255.0 eq domain' command.
View 2011-Oct-25   %ASA-5-111008: User 'enable_15' executed the 'access-list doubledown_access_in line 2 extended
     00:02:19      deny ip any object-group Private_IP_Range' command.
View 2011-Oct-25   %ASA-5-111008: User 'enable_15' executed the 'access-list doubledown_access_in line 3
     00:02:19      extended permit ip any any' command.
View 2011-         %ASA-5-111008: User 'enable_15' executed the
```

Critical Alert


NetWitness Investigator 9
Collection Edit View Bookmarks History Help
All Data
tim-macbook.local:50005 > b0-f0 > authentication > fgreen
Welcome
tim-macbook.local:50005
123 abc
< 2001-01-08 18:15
2011-10-25 00:44 >
tim-macbook.local:50005 Logs
Page 1 of 1
Time Log
Displaying 1 - 12 of 12
View
NUM

Not good…

**Risk: Suspicious** (1 item)
logon failure not primary user (11)

**Source Subnet Location** (1 item)
b0-f0 (12)

**Hostname Aliases** (11 items)
g67-e-462 (2) - g67-e-461 (1) - g67-e-460 (1) - g67-e-459 (1) - g67-e-458 (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)

**Destination User Account** (1 item)
fgreen (12)

**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)

**Domain Name** (1 item)
domain-us (11)

**Event Subject** (1 item)
user (12)

**Event Activity** (1 item)
logon (12)

**Event Theme** (1 item)
authentication (12)

**Event Outcome** (2 items)
failure (11) - success (1)

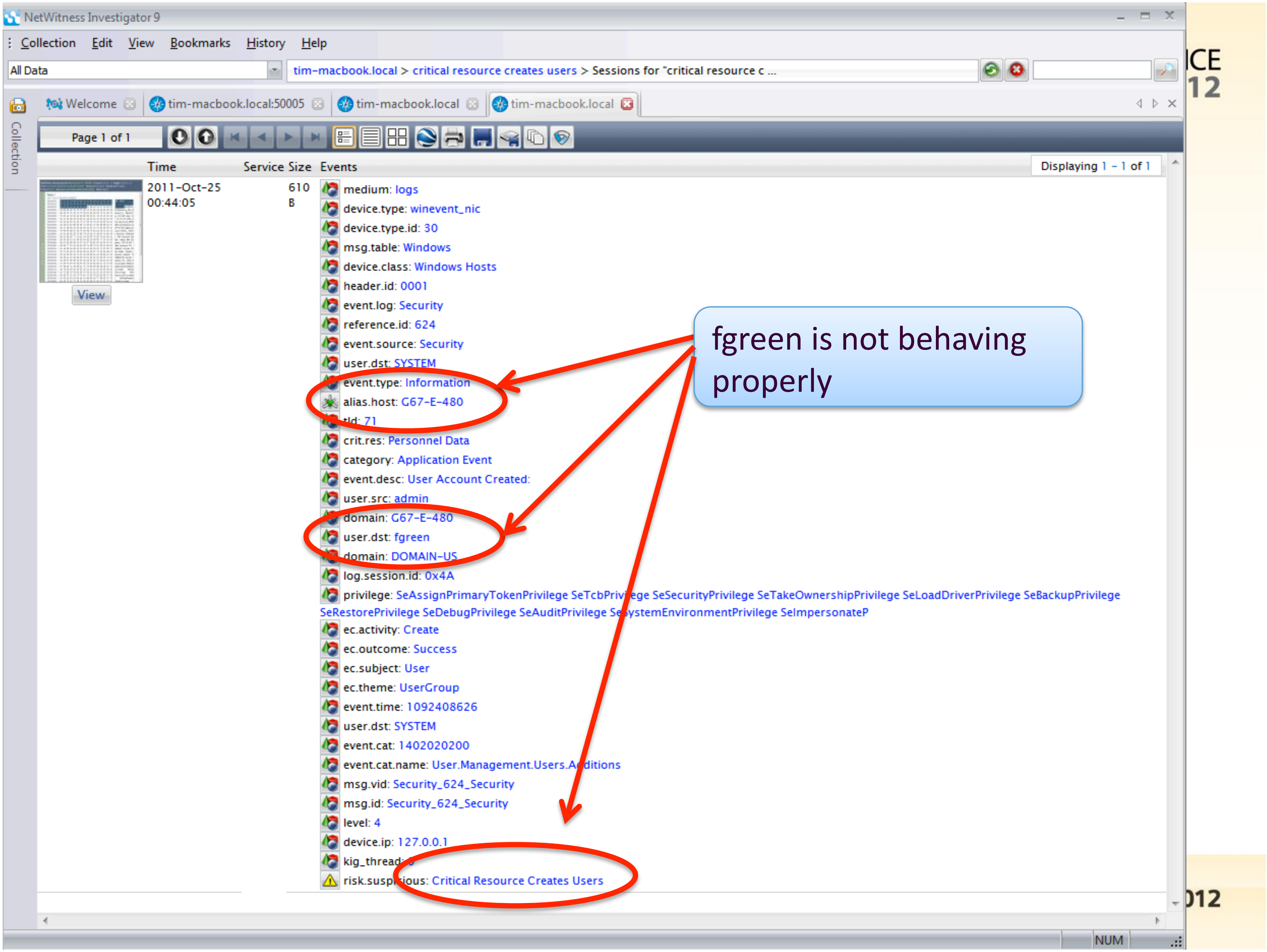
**Event Category Name** (2 items)
user.activity.failed logins (11) - user.activity.successful logins (1)

**Event Category** (2 items)
1401030000 (11) - 1401060000 (1)

```
2011-Oct-25 00:44:05
%NICWIN-0-Security_4625_Microsoft-Windows-Security-Auditing: Security,rn=0x0001f1b3 cid=0x00003100 eid=0x00001211,Mon Oct 17 19:03:12 2011,4625,Microsoft-Windows-Security-Auditing, ,Security Audit Failure,G67-E-452,Logon, ,An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: fgreen Account Domain: DOMAIN-US Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: fgreen Account Domain: DOMAIN-US Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xc000006d Sub Status: 0xc0000064 Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: G67-E-452 Source Network Address: 10.10.12.52 Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

2011-Oct-25 00:44:05
%NICWIN-0-Security_4625_Microsoft-Windows-Security-Auditing: Security,rn=0x0001f1b3 cid=0x00003100 eid=0x00001211,Mon Oct 17 19:03:12 2011,4625,Microsoft-Windows-Security-Auditing, ,Security Audit Failure,G67-E-453,Logon, ,An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: fgreen Account Domain: DOMAIN-US Logon ID: 0x0 Logon Type: 3 Account For Which
```

ICE
12
012


NetWitness Investigator 9
Collection Edit View Bookmarks History Help
All Data
tim-macbook.local > critical resource creates users > Sessions for "critical resource c ...
Welcome
tim-macbook.local:50005
tim-macbook.local
tim-macbook.local
Collection
Page 1 of 1
Displaying 1 - 1 of 1
View
NUM
ICE
12
012

| Time | Service | Size |
|---|---|---|
| 2011-Oct-25 00:44:05 | | 610 B |

```
Events
medium: logs
device.type: winevent_nic
device.type.id: 30
msg.table: Windows
device.class: Windows Hosts
header.id: 0001
event.log: Security
reference.id: 624
event.source: Security
user.dst: SYSTEM
event.type: Information
alias.host: G67-E-480
tld: 71
crit.res: Personnel Data
category: Application Event
event.desc: User Account Created:
user.src: admin
domain: G67-E-480
user.dst: fgreen
domain: DOMAIN-US
log.session.id: 0x4A
privilege: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege
SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonateP
ec.activity: Create
ec.outcome: Success
ec.subject: User
ec.theme: UserGroup
event.time: 1092408626
user.dst: SYSTEM
event.cat: 1402020200
event.cat.name: User.Management.Users.Additions
msg.vid: Security_624_Security
msg.id: Security_624_Security
level: 4
device.ip: 127.0.0.1
kig_thread: 0
risk.suspicious: Critical Resource Creates Users
```

fgreen is not behaving properly

# Summary Take Away Ideas

- Prevention is impossible – think about reallocation of resources (financial, human, operational) - You need to think differently about preventive and detective approaches.
- Focus on the adversary and your most important material assets
- Security is a big data problem – you need to have more data, better analytics and be focusing on intelligence-driven operations
- This work requires a change to the way you do things - You can't buy a turnkey solution to do it all for you – but there are some good tools out there (hint, hint)
- You should NOT be repeating the same processes to find the same old things – why waste your time?
- New intelligence is used to automate finding those [now] known threats in the future (which is not investigative or detective at that point).
- If you don't think differently about security management, you will fail

# Q&A

RSA®

# Thank You

eddie.schwartz@rsa.com
Twitter: @eddieschwartz
http://www.rsa.com

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012