使用大数据和情报驱动安全性防御有针对性的攻击

Eddie Schwartz

EMC 的安全产品分公司 RSA

专题会议 ID：TH-2004

专题会议分类：高级

RSACONFERENCE
CHINA 2012
RSA信息安全大会2012

议程

- 当今的安全和威胁形势
- 大数据和情报驱动安全性的兴起
- 两个简单的案例研究
- 问题

当今的安全形势

当今的安全形势

- 过于依赖外围安全性和“违规前检查工具”是失败的策略
- 与对手、材料资产和真实难题相比，过多关注 ISO27001 和法规遵从性
- 网络安全需要全面检查...

组织不了解其对手

国家行动者

国家

政府、国防工业基地、
IP 丰富的组织

犯罪分子

小规模犯罪分子

不复杂

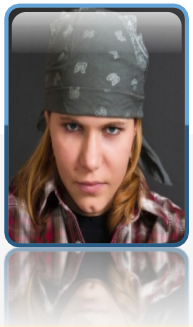
有组织的犯罪

有组织的、复杂的供应链
（PII、财务服务、零售）

非国家行动者

内部人员

各种原因，包括协作



网络恐怖分子/
黑客活动家

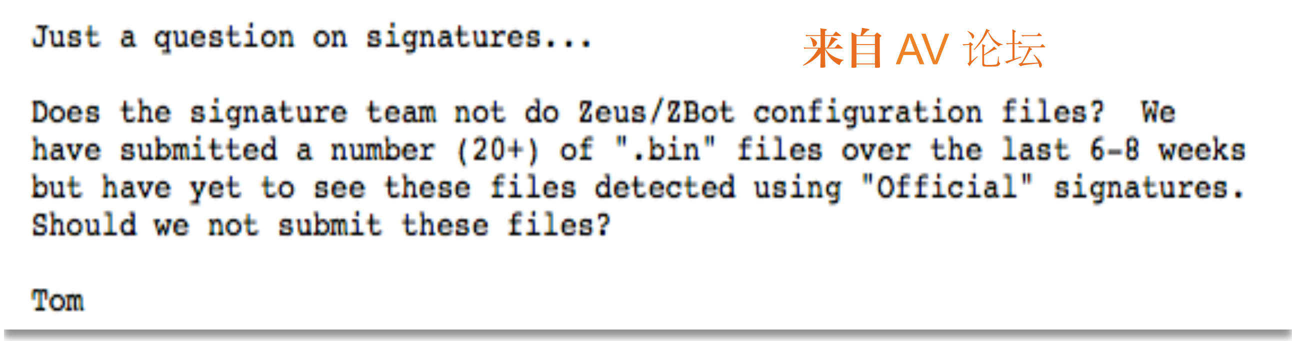
政治机会目标，大规模破坏

为什么预防作为安全策略是远远不够的？

目标 – 阻止或限制进出网络的未授权连接

现实情况 – 对手的恶意软件使用“允许的路径”（DNS、HTTP、SMTP 等）作为您网络中的 C&C 和数据外泄通道

当前 AV 和 IPS 关注的是漏洞，基于签名，并且需要不断更新才能发挥作用。由于恶意软件生产级别的原因，这些签名会滞后数天至数周

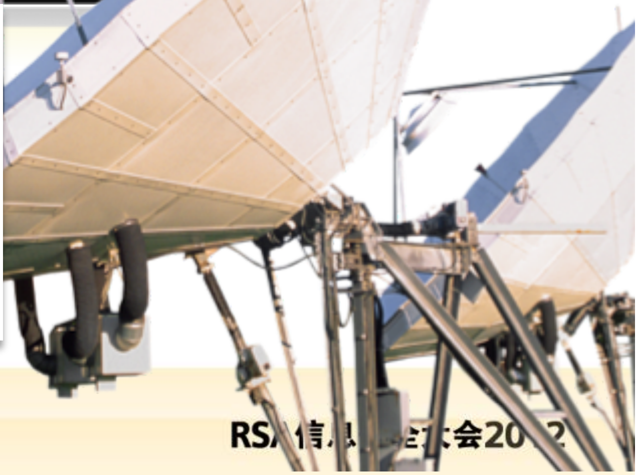


来自 AV 论坛

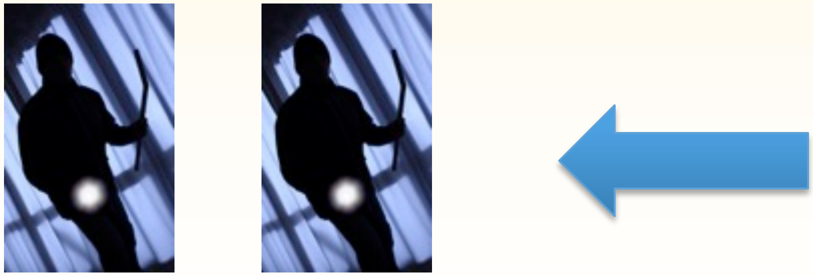
Just a question on signatures...

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

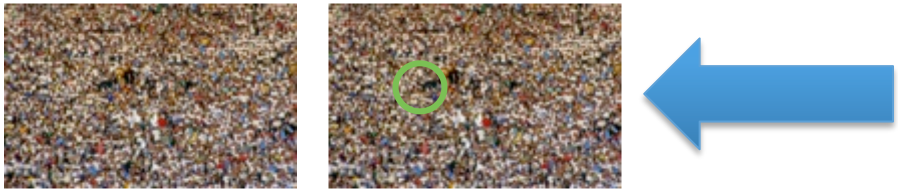


将“坏的”与“好的”区分开变得越来越难



= 坏的

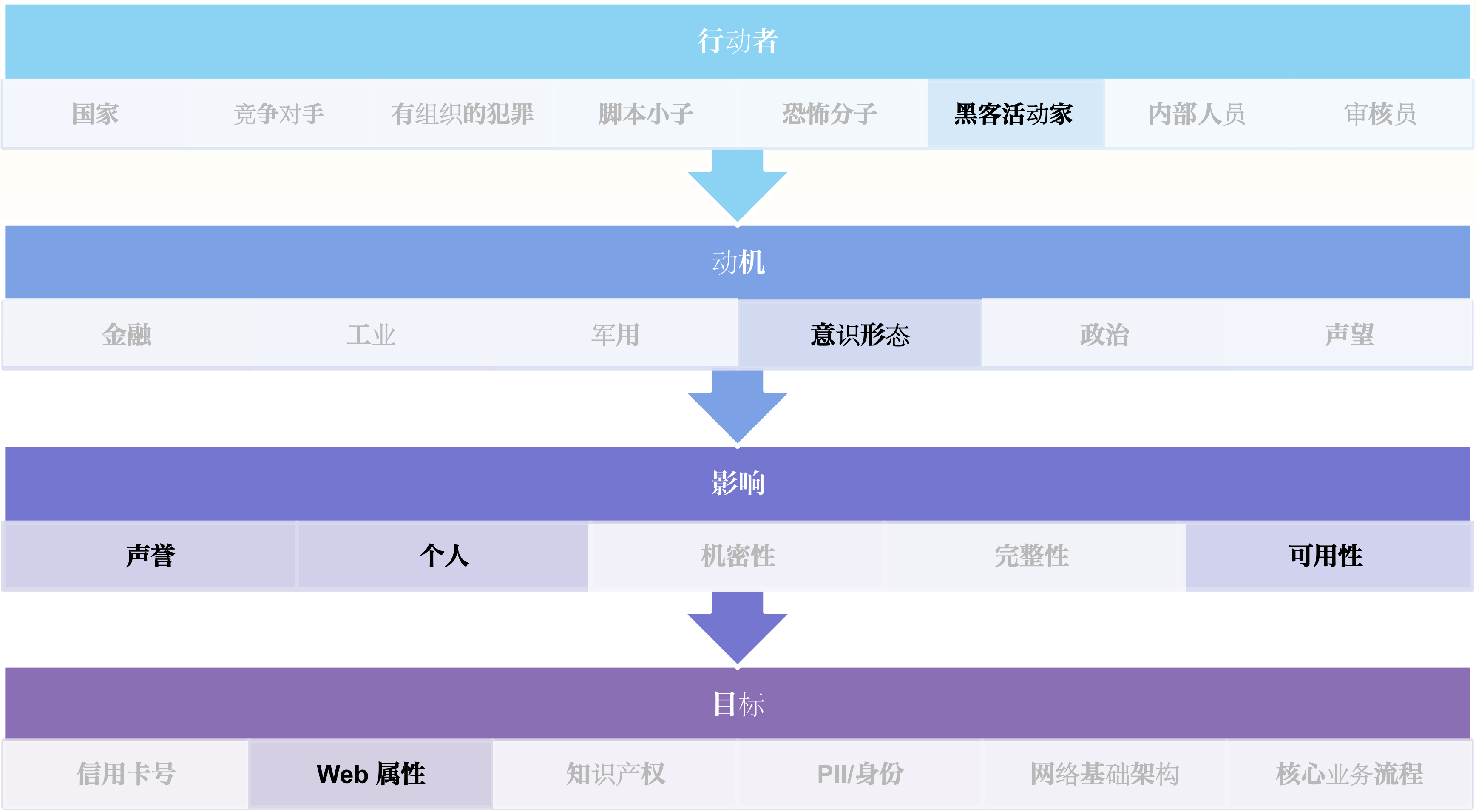
- 了解“坏的”看起来是什么样子的并查找类似的内容
  - 防病毒
  - 入侵防御系统
  - 超过了阈值



= 坏的

- 了解“好的”看起来是什么样子的并查找有意义的区别
  - 网络分析和基准衡量
  - 异常检测
  - 预测失败分析

创建威胁模型



行动者

国家 | 竞争对手 | 有组织的犯罪 | 脚本小子 | 恐怖分子 | **黑客活动家** | 内部人员 | 审核员

动机

金融 | 工业 | 军用 | **意识形态** | 政治 | 声望

影响

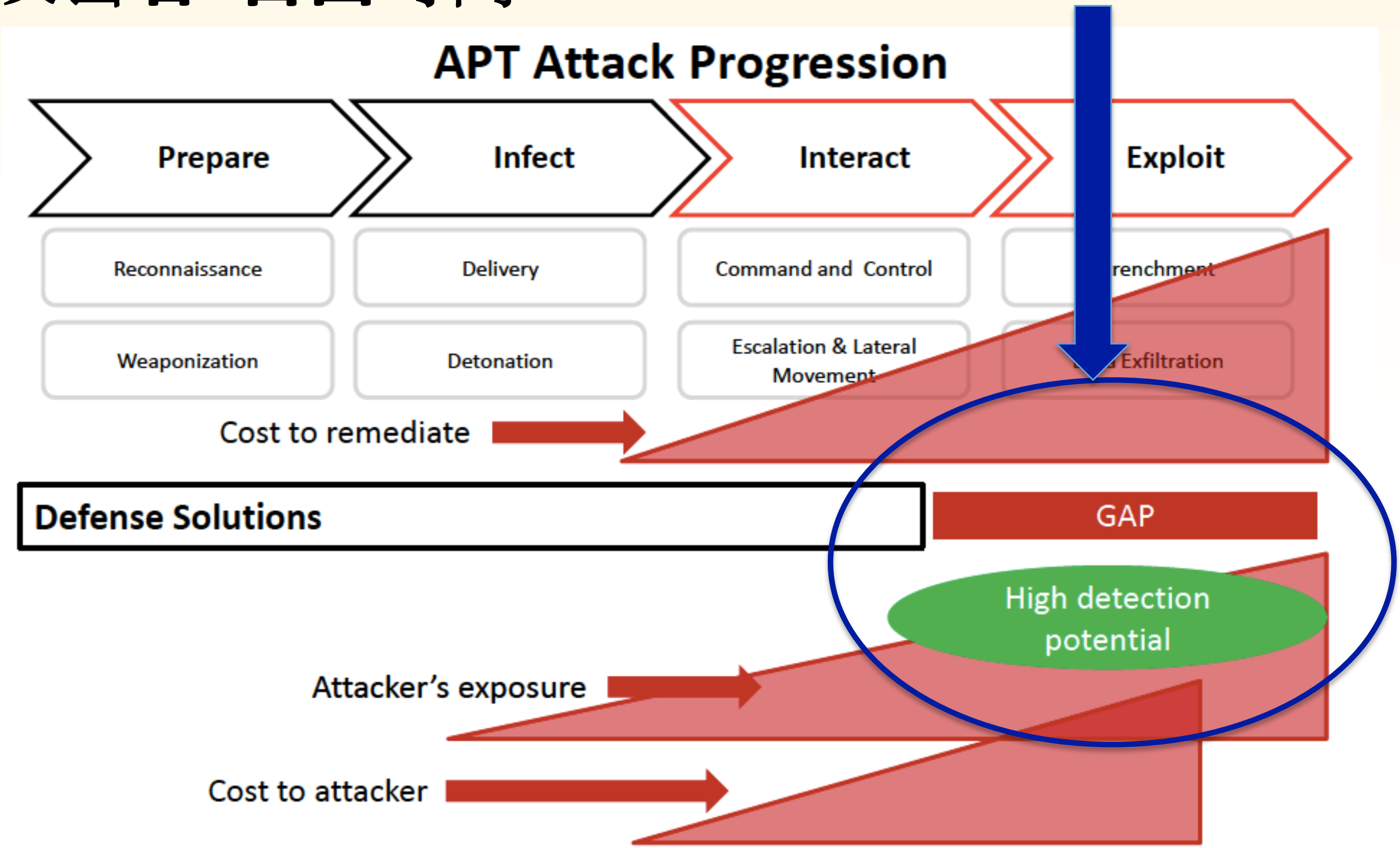
声誉 | **个人** | 机密性 | 完整性 | **可用性**

目标

信用卡号 | **Web 属性** | 知识产权 | PII/身份 | 网络基础架构 | 核心业务流程

攻击者“自由时间”

什么级别的资源正好位于这里？



APT Attack Progression

Prepare

Infect

Interact

Exploit

Reconnaissance

Delivery

Command and Control

renchment

Weaponization

Detonation

Escalation & Lateral Movement

Exfiltration

Cost to remediate

Defense Solutions

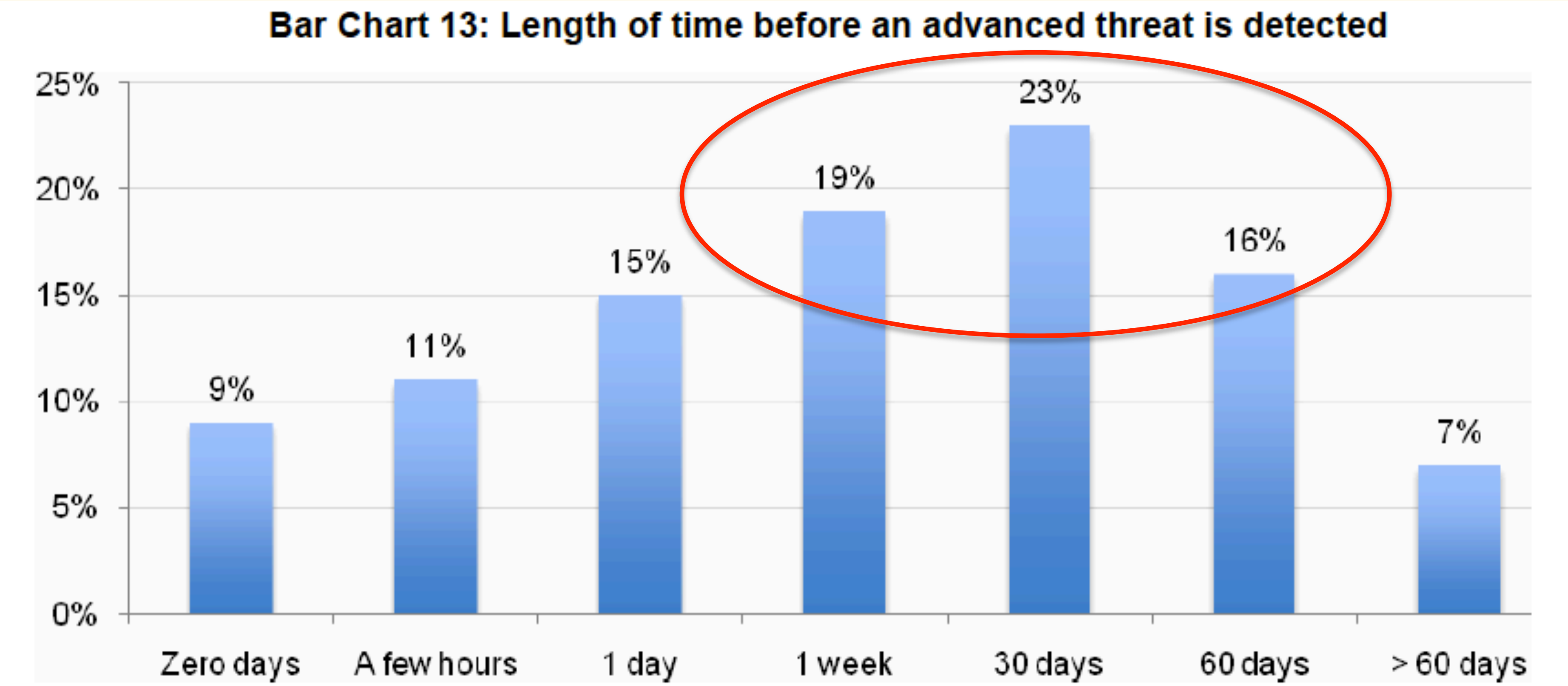
GAP

High detection potential

Attacker’s exposure

Cost to attacker

检测时间 – 不太好..



来源：Ponemon Institute

大数据和安全情报的兴起

什么是大数据？

- “大数据是指常用软件工具无法在可容忍的时间内捕获、管理和处理其大小的数据集。”– 维基百科
- “数据增长挑战是三维的，数量（数据量）、速度（数据输入/输出速度）和多样性（数据类型范围、来源）都在增加。”– 分析报告
- “44% 的大型组织每月至少收集 1 TB 的日志文件。11% 的大型组织说他们每月捕获的数据超过 10 TB。”– ESG Research

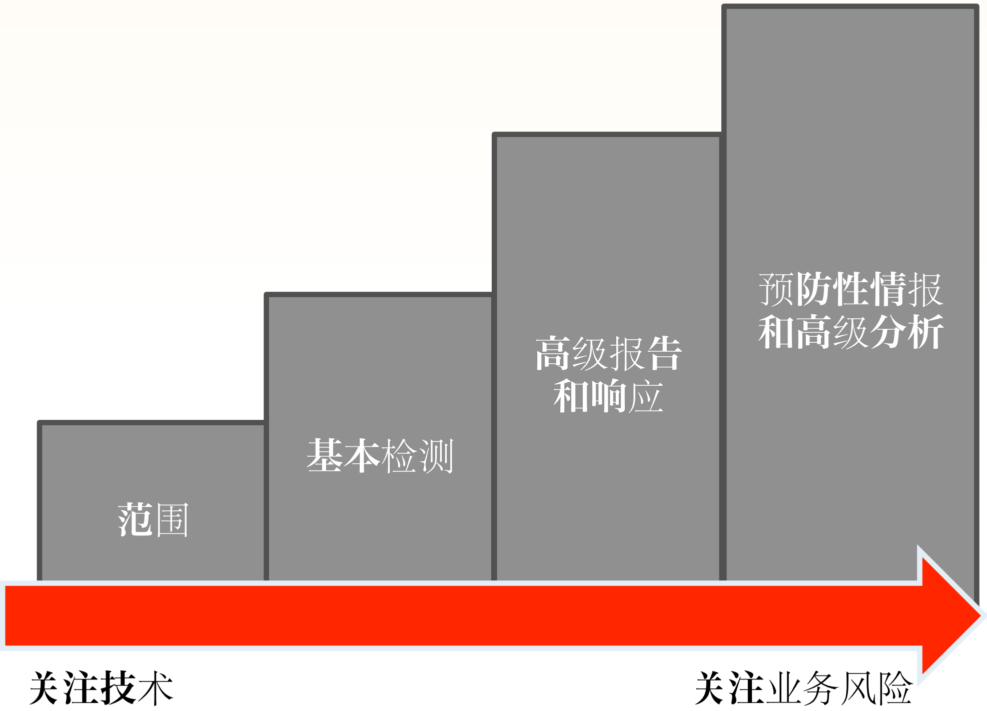
安全操作的数据挑战

- 数据量
  - 减少数据“干扰”
- 可访问性
  - 集中化不可行
- 滞后时间
  - 数据相对于手头问题来说有多新
- 保留
  - 与其他方法（归档）相比，多少数据需要联机
- 非连续源
  - 合并上下文数据
- 数据分析（最重要）
  - 实时查询

安全分析师采用大数据的障碍

- 缺乏上下文
  - 从系统外部的数据获得见解
- 模糊的非结构化数据
  - 需要熟悉的标准化数据语言
- 系统数据减少
  - 尝试筛选“不重要的”数据
- 自动化日常任务
  - 履行工作职能，同时仍有时间进行新的分析

通往更先进的安全操作方法的进程是什么？



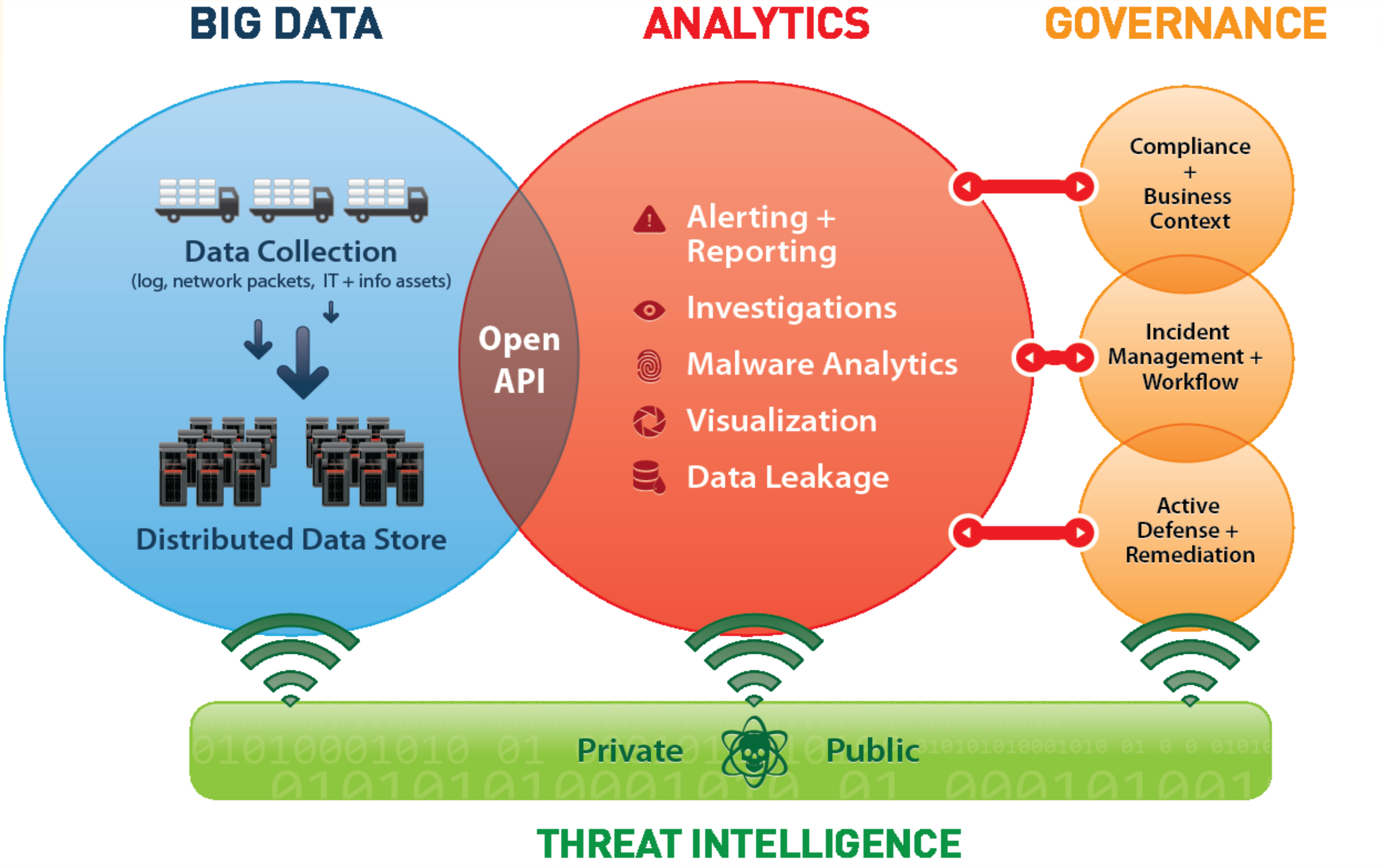
建立大数据体系结构理念

- 将您的数据留在原处
  - 分布式数据模型
  - 集中化效率太低
  - 消除数据重复
  - 节省网络带宽
- 将数据提供给需要它的人
  - 分层数据模型
  - 可访问性
  - 查询速度
- 利用上下文数据
  - 上下文越多，了解越深

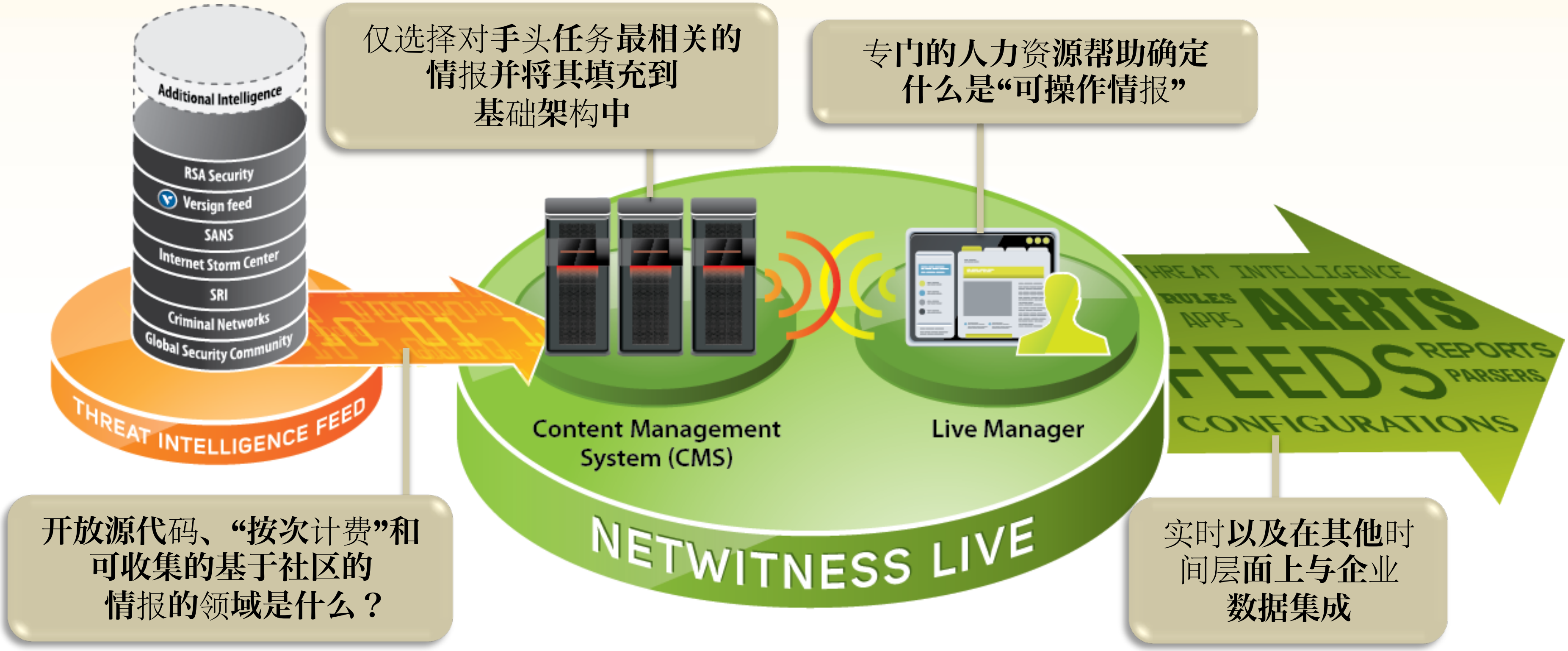
建立大数据分析理念

- “预挖掘”数据情报
  - 在捕获时增添价值（分析和扩充）
  - 快速分析重要数据
- 实现专门分析
  - 不要大海捞针般地进行处理
  - 允许“简化分析”
- 将具有不同需要的职能部门区分开
  - 从技术和时间层面的最佳用法角度进行考虑 – 对您来说，各个最佳用法是什么？
  - 复杂的事件处理
  - 归档
  - 实时
  - 法规遵从性

大数据 + 情报 – 重要特性


BIG DATA
ANALYTICS
GOVERNANCE
Data Collection
(log, network packets, IT + info assets)
Distributed Data Store
Open API
Alerting + Reporting
Investigations
Malware Analytics
Visualization
Data Leakage
Compliance + Business Context
Incident Management + Workflow
Active Defense + Remediation
Private
Public
THREAT INTELLIGENCE

大数据与威胁情报的融合



仅选择对手头任务最相关的情报并将其填充到基础架构中

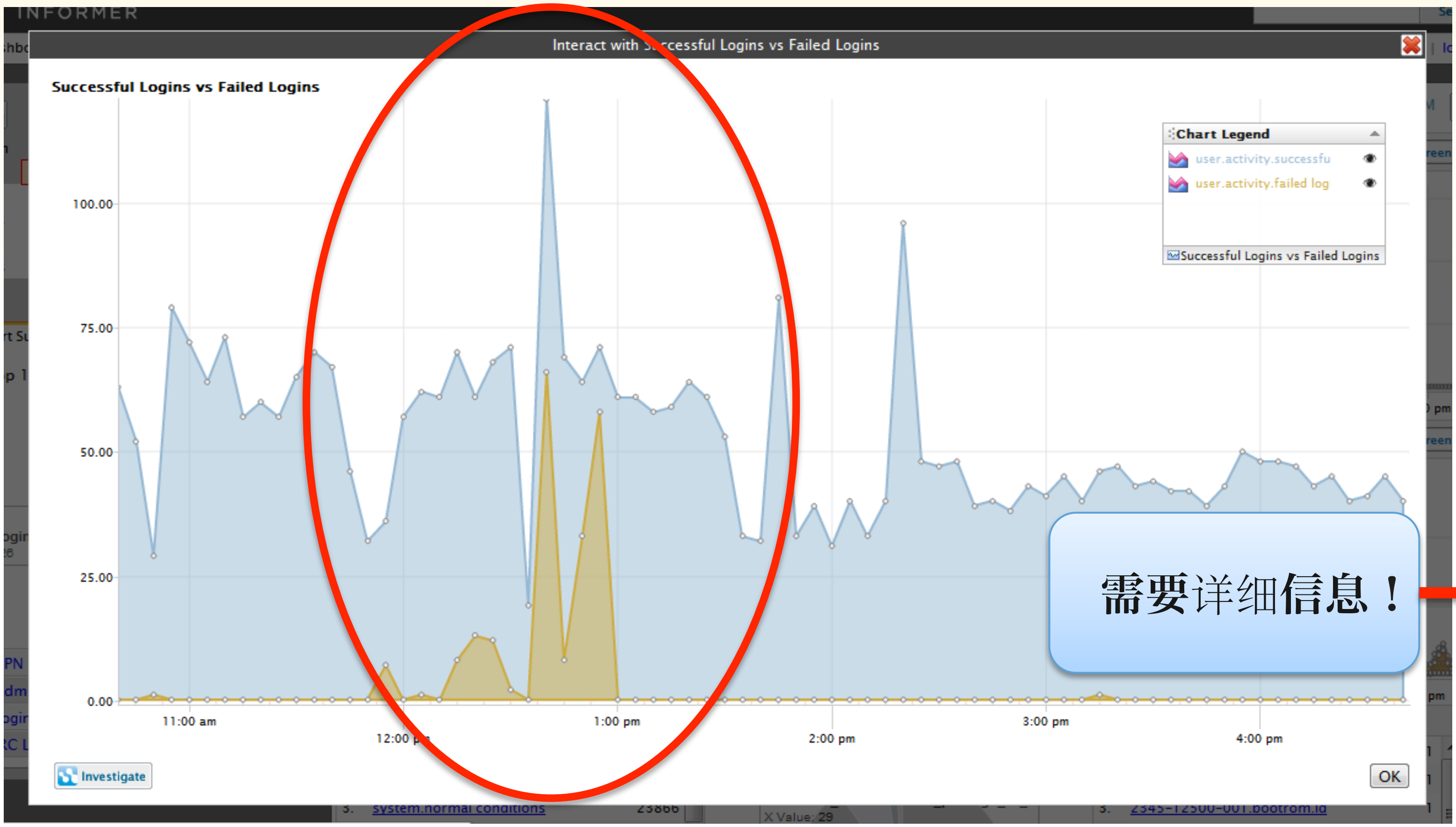
专门的人力资源帮助确定什么是“可操作情报”

开放源代码、“按次计费”和可收集的基于社区的情报的领域是什么？

实时以及在其他时间层面上与企业数据集成

两个简单的案例研究

完整数据包和日志覆盖



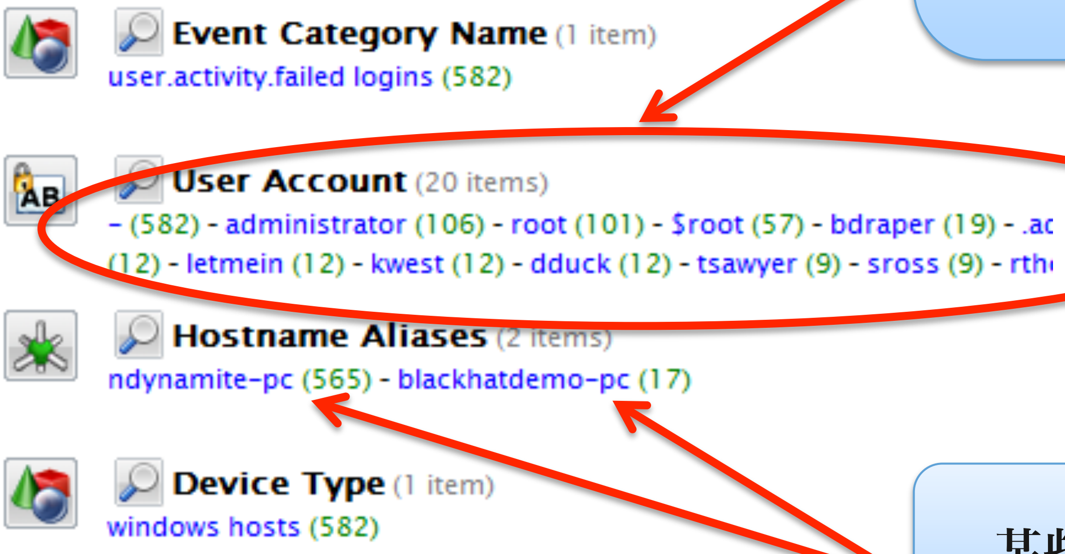
需要详细信息！

登录图表显示与成功和失败的登录尝试关联的活动。

即时了解可能“拥有的”机器

从基于日志条目“failed logins”的报告进行透视

完整数据包会话还显示与活动关联的所有用户帐户和主机名



Event Category Name (1 item)
user.activity.failed logins (582)

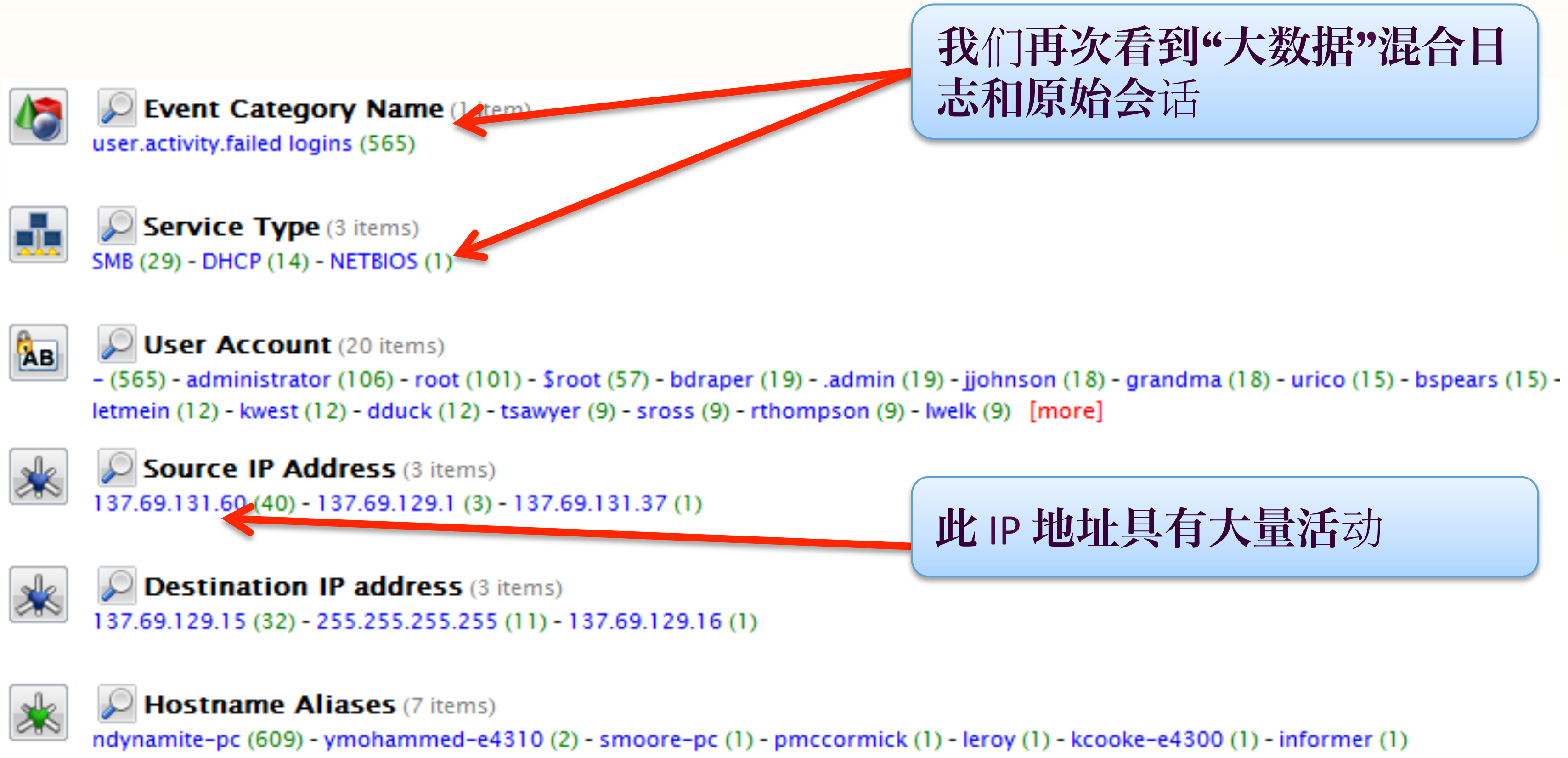
User Account (20 items)
– (582) - administrator (106) - root (101) - $root (57) - bdraper (19) - .ac
(12) - letmein (12) - kwest (12) - dduck (12) - tsawyer (9) - sross (9) - rth

Hostname Aliases (2 items)
ndynamite-pc (565) - blackhatdemo-pc (17)

Device Type (1 item)
windows hosts (582)

某些主机名的活动比其他主机名的多

对“ndynamite-pc”进行透视



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)

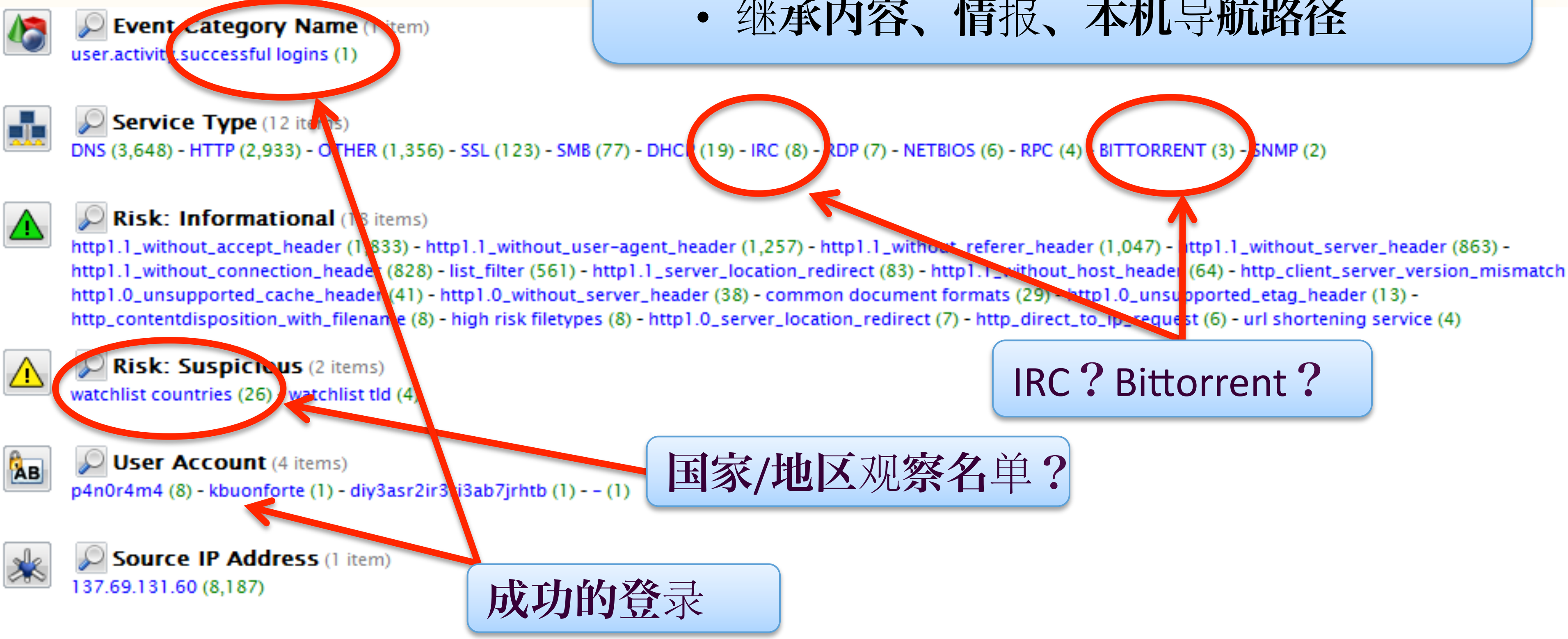
Hostname Aliases (7 items)
ndynamite-pc (609) - ymohammed-e4310 (2) - smoore-pc (1) - pmccormick (1) - leroy (1) - kcooke-e4300 (1) - informer (1)

我们再次看到“大数据”混合日志和原始会话

此 IP 地址具有大量活动

基于 IP 地址 137.69.131.60 的透视

- 分析 IP 地址的所有活动
  - 继承内容、情报、本机导航路径



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) - diy3asr2ir3ri3ab7jrhtb (1) - – (1)

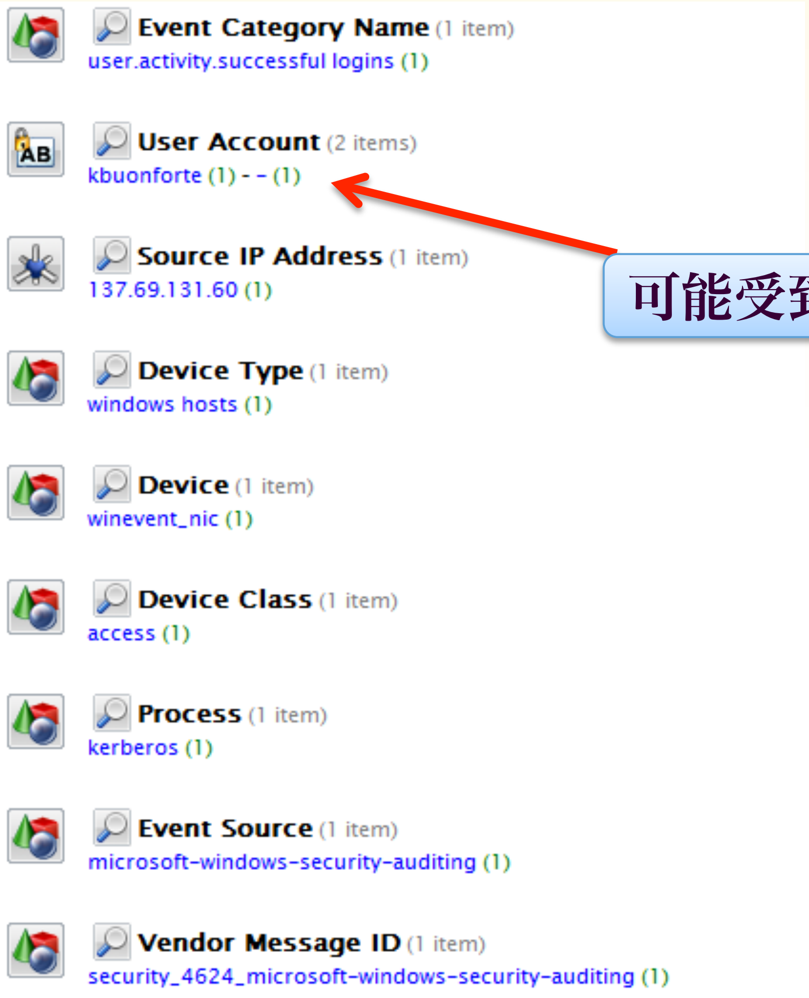
Source IP Address (1 item)
137.69.131.60 (8,187)

IRC？Bittorrent？

国家/地区观察名单？

成功的登录

成功的登录条目的日志事件



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)

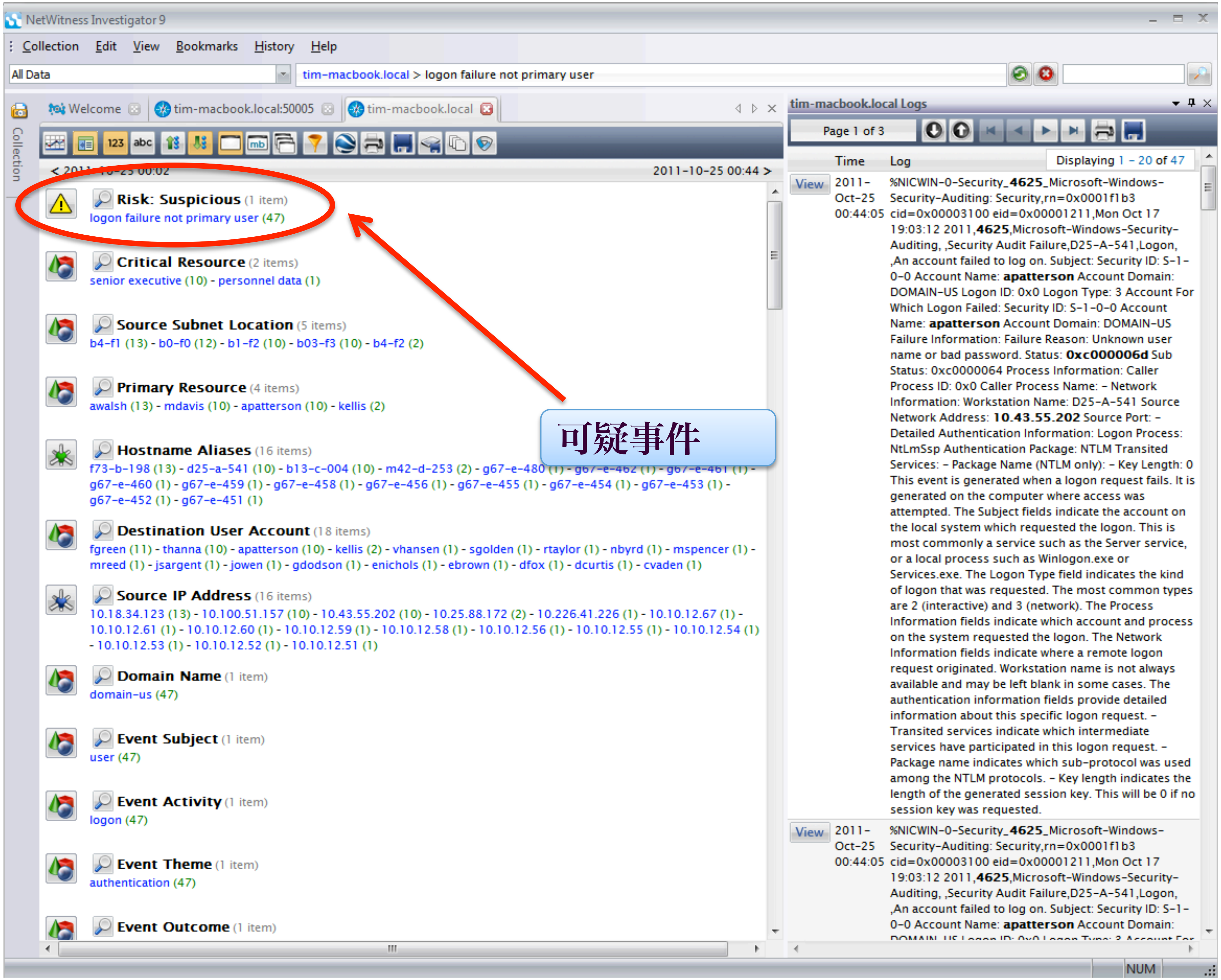
Device Class (1 item)
access (1)

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)

可能受到攻击的 ID



可疑事件

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)

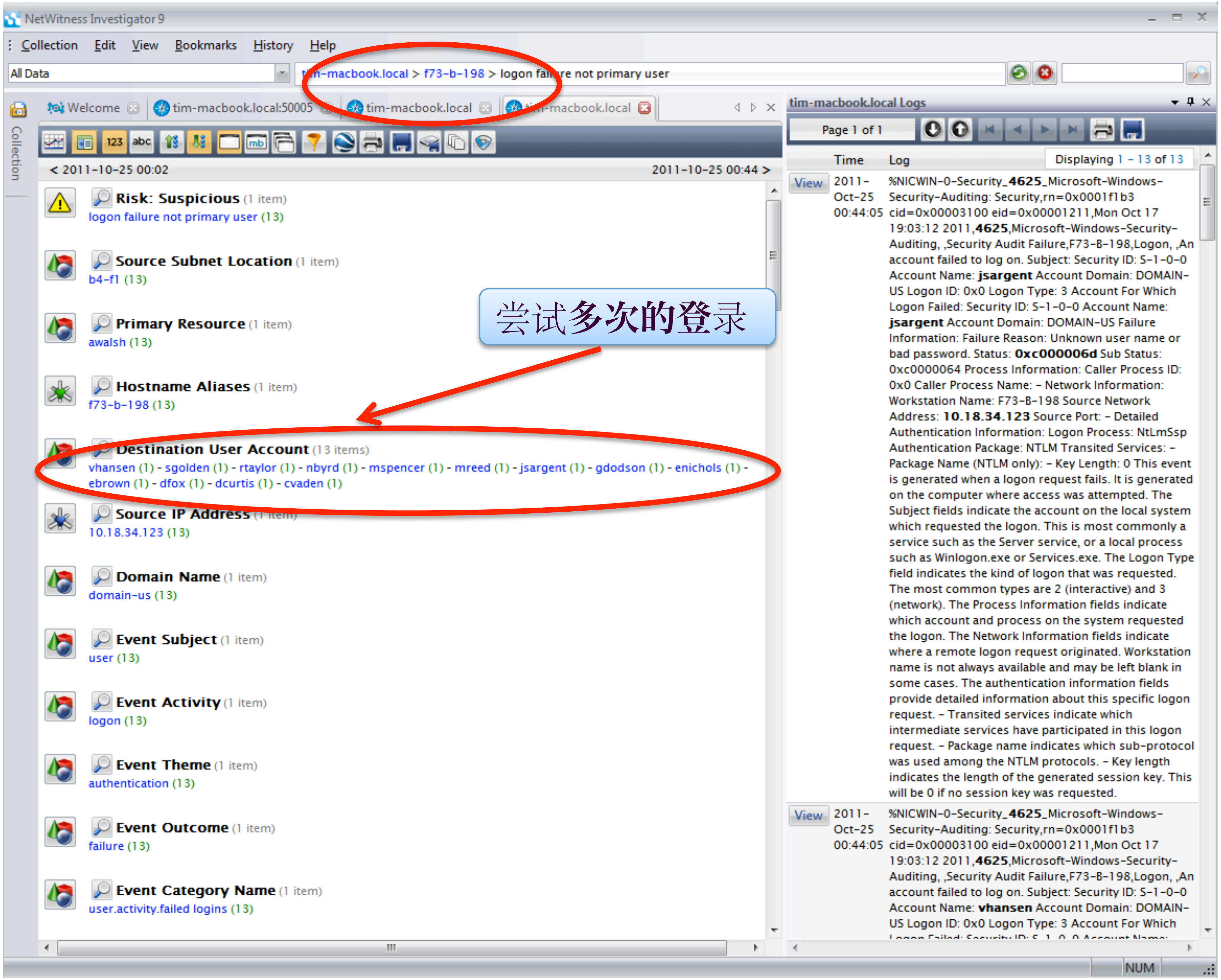
Event Subject (1 item)
user (47)

Event Activity (1 item)
logon (47)

Event Theme (1 item)
authentication (47)

Event Outcome (1 item)

```
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 Network Address: 10.43.55.202 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,D25-A-541,Logon, ,An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: apatterson Account Domain:
```



tim-macbook.local > f73-b-198 > logon failure not primary user

< 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)

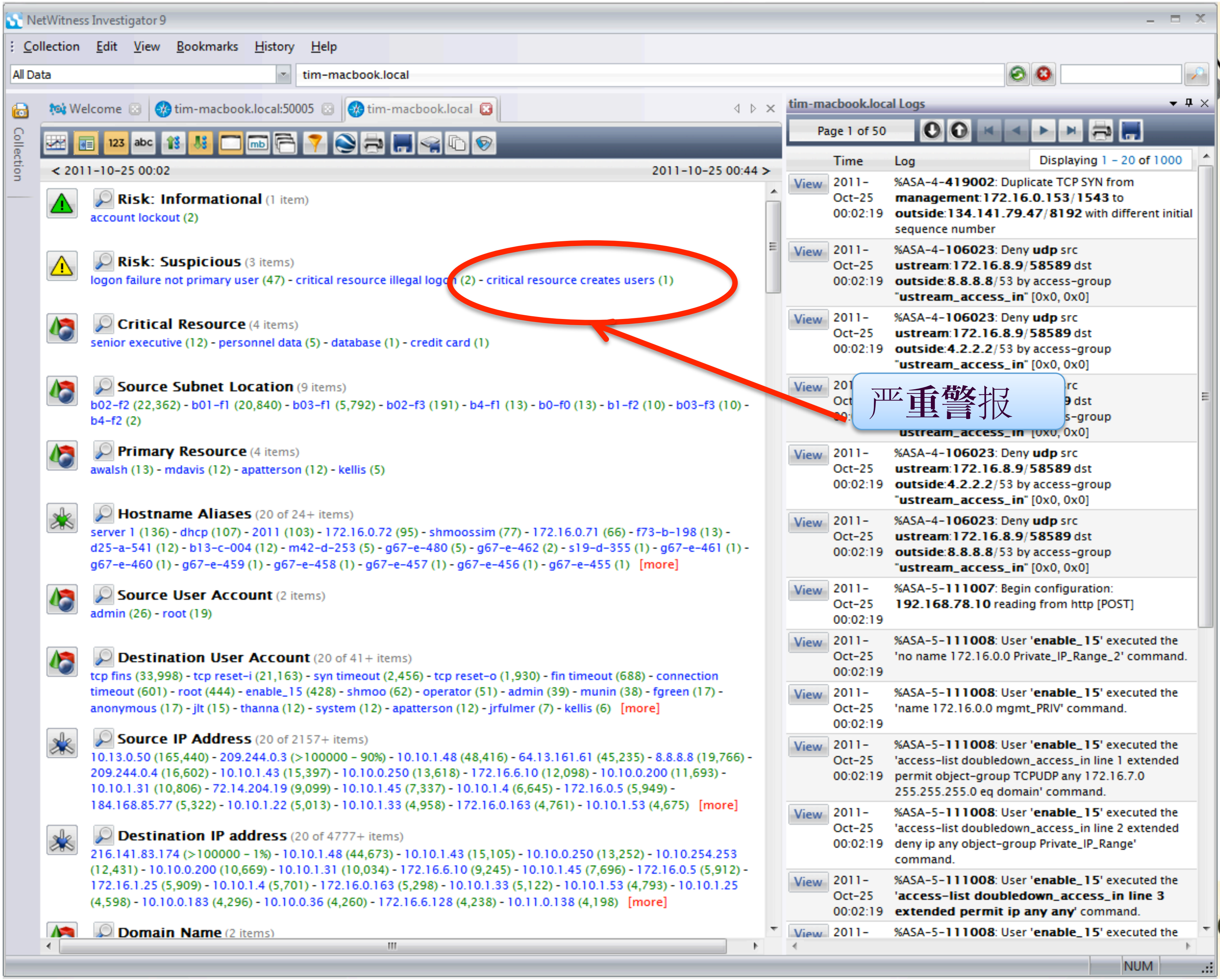
Event Outcome (1 item)
failure (13)

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

尝试多次的登录

Time | Log | Displaying 1 - 13 of 13

```
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
```



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

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]

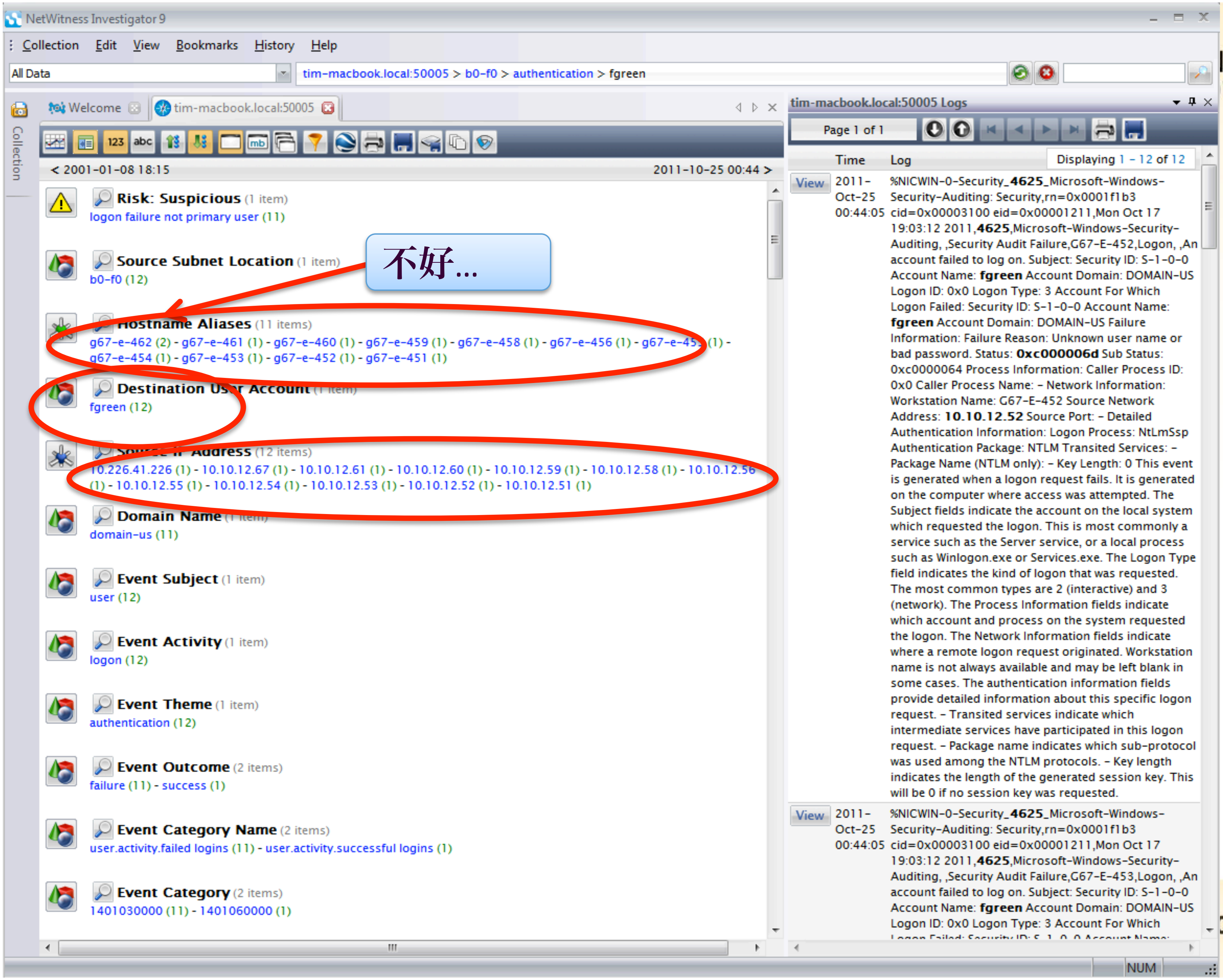
Destination IP address (20 of 4777+ items)
216.141.83.174 (>100000 - 1%) - 10.10.1.48 (44,673) - 10.10.1.43 (15,105) - 10.10.0.250 (13,252) - 10.10.254.253 (12,431) - 10.10.0.200 (10,669) - 10.10.1.31 (10,034) - 172.16.6.10 (9,245) - 10.10.1.45 (7,696) - 172.16.0.5 (5,912) - 172.16.1.25 (5,909) - 10.10.1.4 (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-      %ASA-4-419002: Duplicate TCP SYN from
      Oct-25     management:172.16.0.153/1543 to
      00:02:19   outside:134.141.79.47/8192 with different initial
                 sequence number
View  2011-      %ASA-4-106023: Deny udp src
      Oct-25     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-      %ASA-4-106023: Deny udp src
      Oct-25     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                                  rc
      Oct                                  9 dst
                                           s-group
                 ustream_access_in" [0x0, 0x0]
View  2011-      %ASA-4-106023: Deny udp src
      Oct-25     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-      %ASA-4-106023: Deny udp src
      Oct-25     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-      %ASA-5-111007: Begin configuration:
      Oct-25     192.168.78.10 reading from http [POST]
      00:02:19
View  2011-      %ASA-5-111008: User 'enable_15' executed the
      Oct-25     'no name 172.16.0.0 Private_IP_Range_2' command.
      00:02:19
View  2011-      %ASA-5-111008: User 'enable_15' executed the
      Oct-25     'name 172.16.0.0 mgmt_PRIV' command.
      00:02:19
View  2011-      %ASA-5-111008: User 'enable_15' executed the
      Oct-25     '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-      %ASA-5-111008: User 'enable_15' executed the
      Oct-25     'access-list doubledown_access_in line 2 extended
      00:02:19   deny ip any object-group Private_IP_Range'
                 command.
View  2011-      %ASA-5-111008: User 'enable_15' executed the
      Oct-25     '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
```

NCE
012

012



tim-macbook.local:50005 > b0-f0 > authentication > fgreen

< 2001-01-08 18:15 2011-10-25 00:44 >

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)

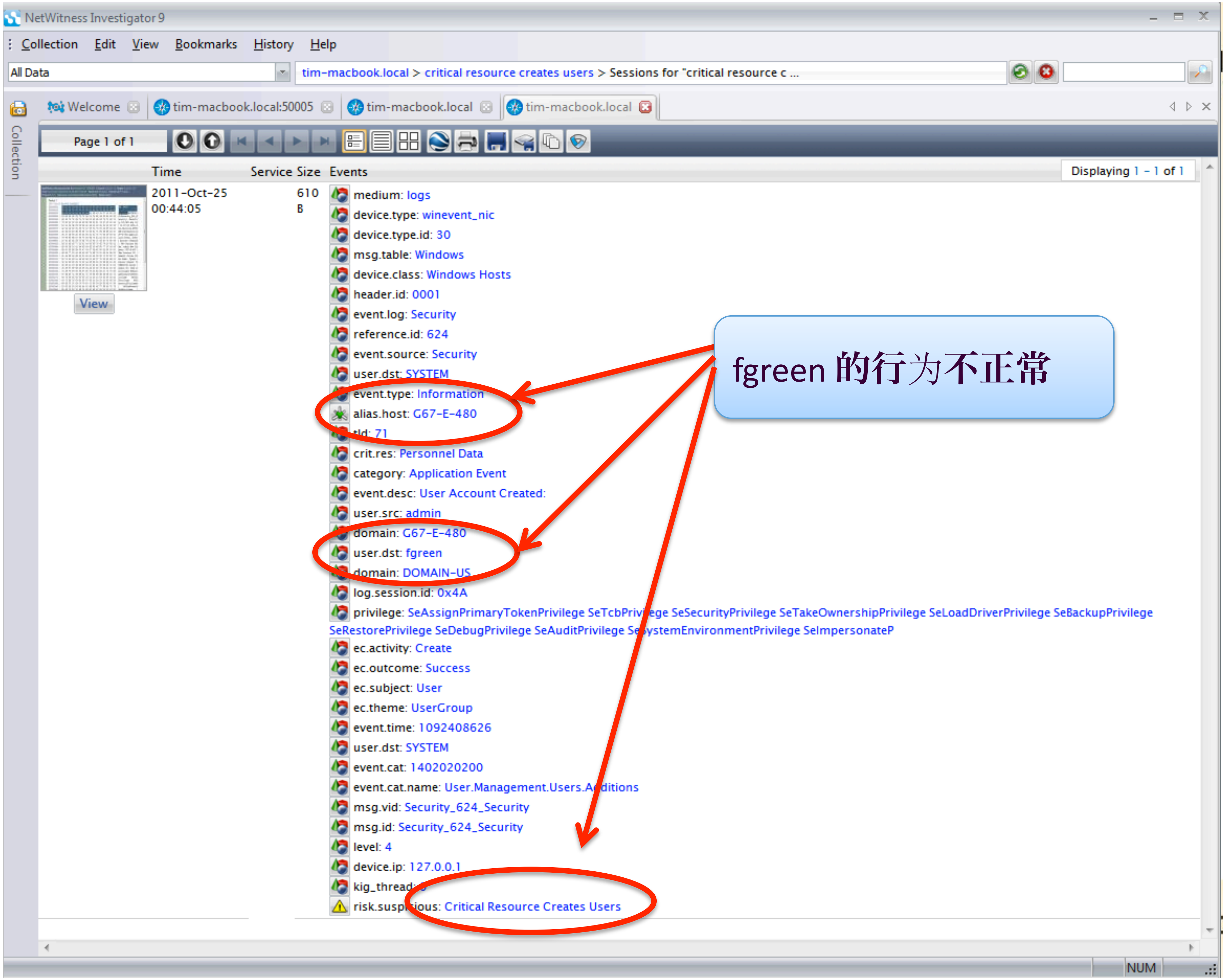
Event Category (2 items)
1401030000 (11) - 1401060000 (1)

不好...

Page 1 of 1

Displaying 1 - 12 of 12

```
      Time       Log
View  2011-      %NICWIN-0-Security_4625_Microsoft-Windows-
      Oct-25     Security-Auditing: Security,rn=0x0001f1b3
      00:44:05   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.
View  2011-      %NICWIN-0-Security_4625_Microsoft-Windows-
      Oct-25     Security-Auditing: Security,rn=0x0001f1b3
      00:44:05   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
```


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
Time Service Size Events
Displaying 1 - 1 of 1
View
NUM

2011-Oct-25 00:44:05 610 B

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 的行为不正常

摘要关键讯息

- 预防是不可能的 – 考虑重新分配资源（财务、人力、运营）– 您需要从不同的思路思考预防和检测方法。
- 关注对手和您最重要的材料资产。
- 安全性是一个大数据问题 – 您需要具有更多数据、更好的分析，并且关注情报驱动的操作。
- 此工作需要改变您做事的方式 – 您无法购买一种全包式解决方案替您完成一切 – 但确实有一些不错的工具（提示）。
- 您不应重复相同的过程来查找相同的旧内容 – 为什么要浪费时间？
- 新情报用于以后自动查找那些 [现在] 已知的威胁（届时将不可调查或不可检测）。
- 如果您不从不同的思路思考安全管理，您将会失败。

问题解答

RSA®

谢谢大家！

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

RSACONFERENCE
CHINA 2012
RSA信息安全大会2012