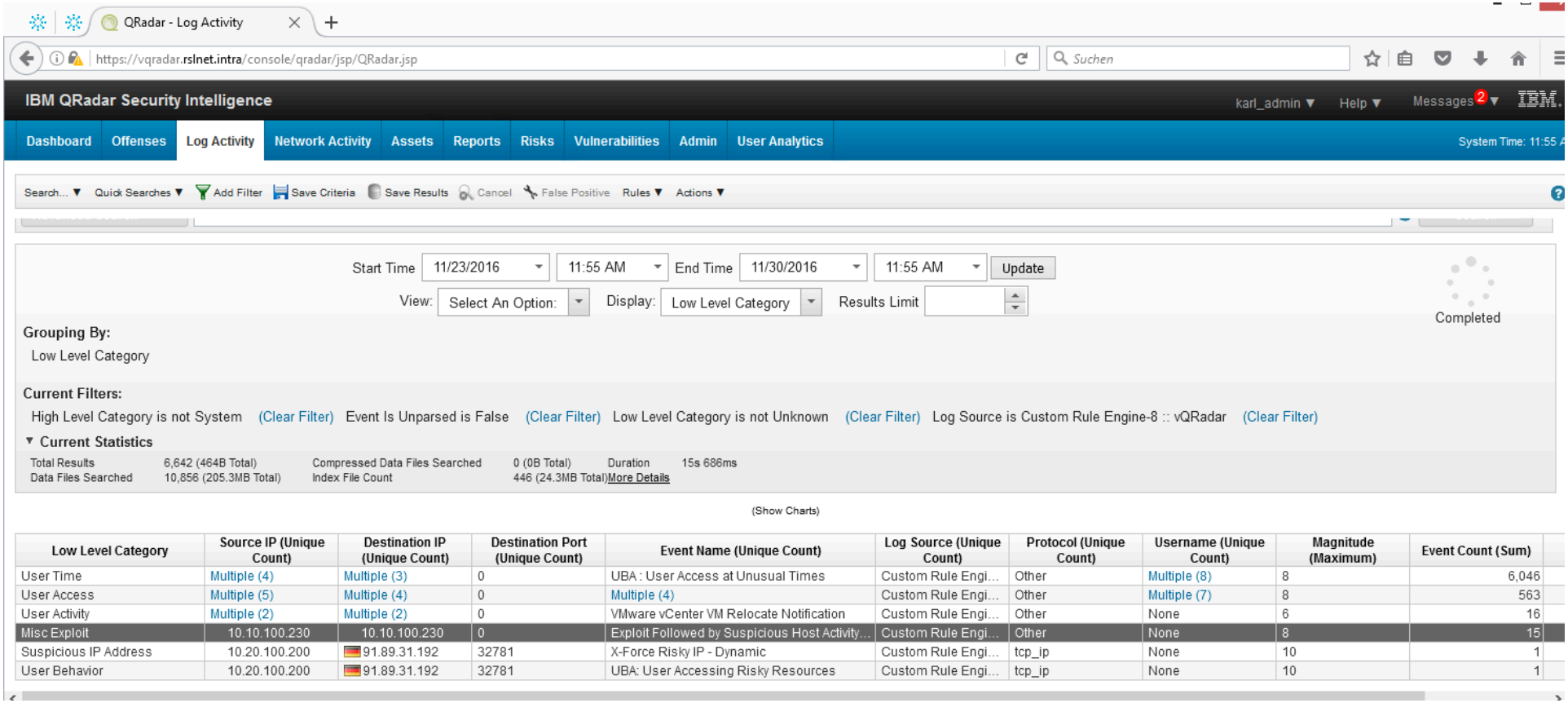
# QRadar hacks

## false alarm

**Karl Jaeger**

Pro4bizz GmbH
https://www.pro4bizz.de
karl.jaeger@pro4bizz.de
0721-909 81 720

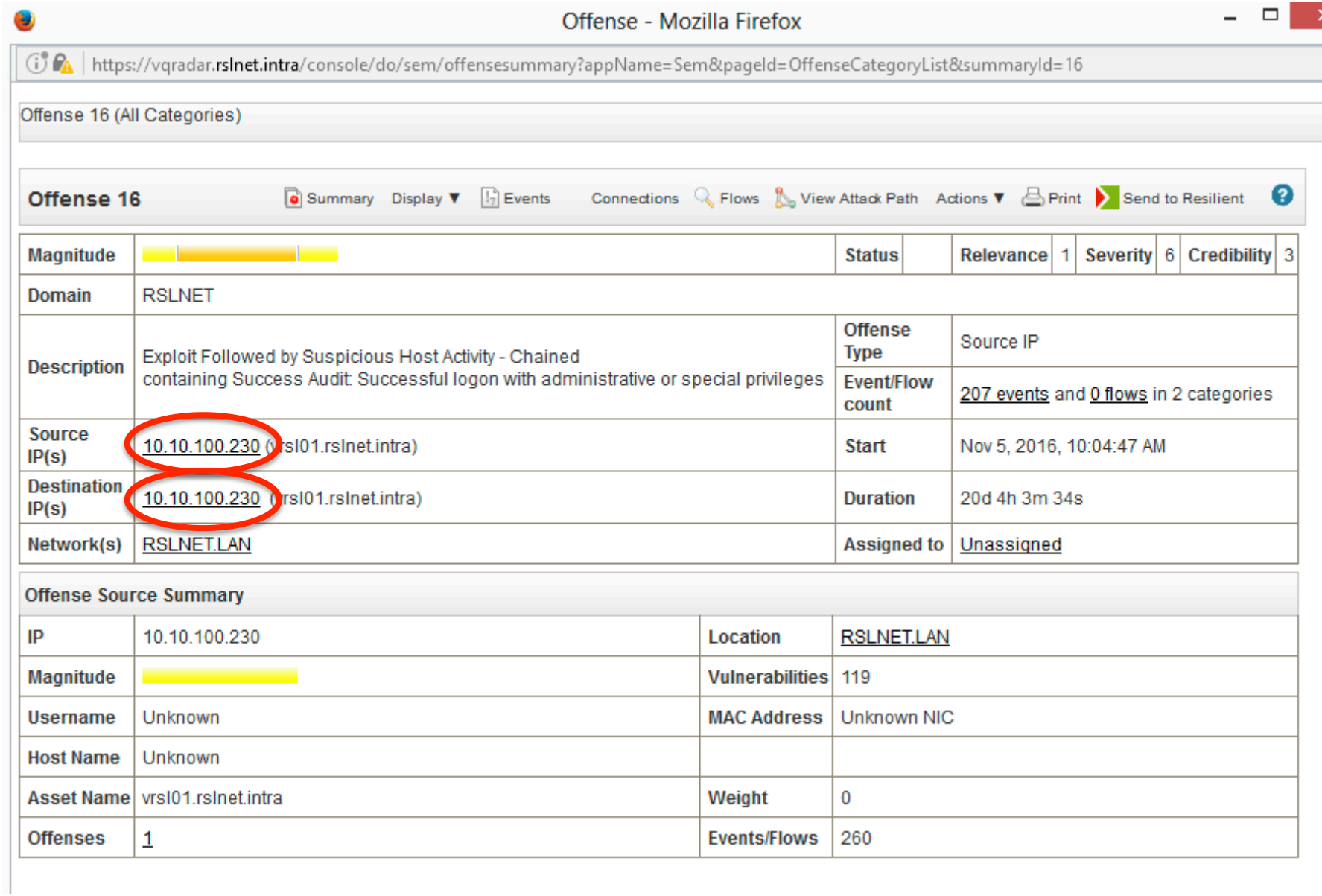
zu viele offenses – was nun?



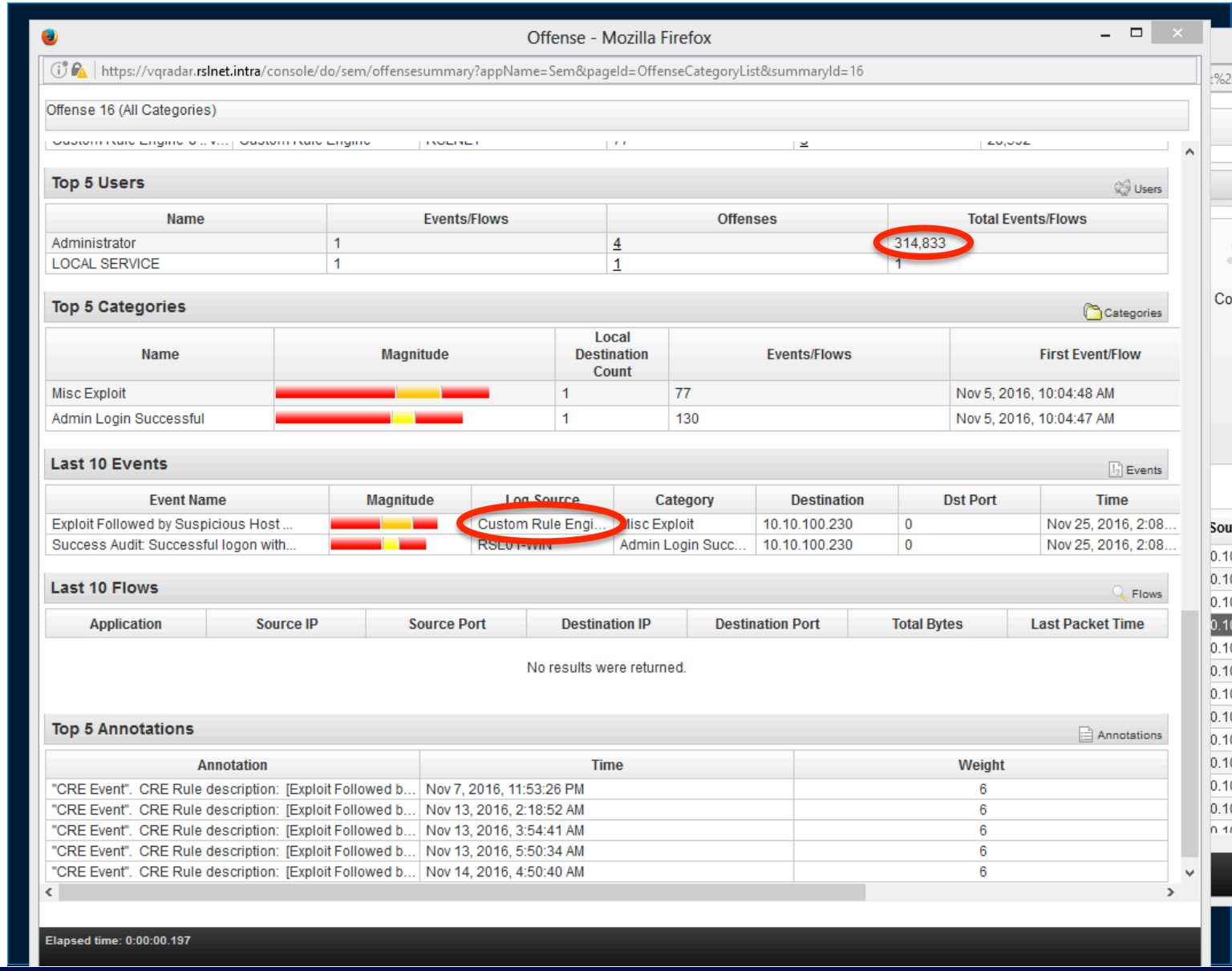

| Low Level Category | Source IP (Unique Count) | Destination IP (Unique Count) | Destination Port (Unique Count) | Event Name (Unique Count) | Log Source (Unique Count) | Protocol (Unique Count) | Username (Unique Count) | Magnitude (Maximum) | Event Count (Sum) |
|---|---|---|---|---|---|---|---|---|---|
| User Time | Multiple (4) | Multiple (3) | 0 | UBA : User Access at Unusual Times | Custom Rule Engi... | Other | Multiple (8) | 8 | 6,046 |
| User Access | Multiple (5) | Multiple (4) | 0 | Multiple (4) | Custom Rule Engi... | Other | Multiple (7) | 8 | 563 |
| User Activity | Multiple (2) | Multiple (2) | 0 | VMware vCenter VM Relocate Notification | Custom Rule Engi... | Other | None | 6 | 16 |
| Misc Exploit | 10.10.100.230 | 10.10.100.230 | 0 | Exploit Followed by Suspicious Host Activity... | Custom Rule Engi... | Other | None | 8 | 15 |
| Suspicious IP Address | 10.20.100.200 | 91.89.31.192 | 32781 | X-Force Risky IP - Dynamic | Custom Rule Engi... | tcp_ip | None | 10 | 1 |
| User Behavior | 10.20.100.200 | 91.89.31.192 | 32781 | UBA: User Accessing Risky Resources | Custom Rule Engi... | tcp_ip | None | 10 | 1 |

false alarm vs. false positive

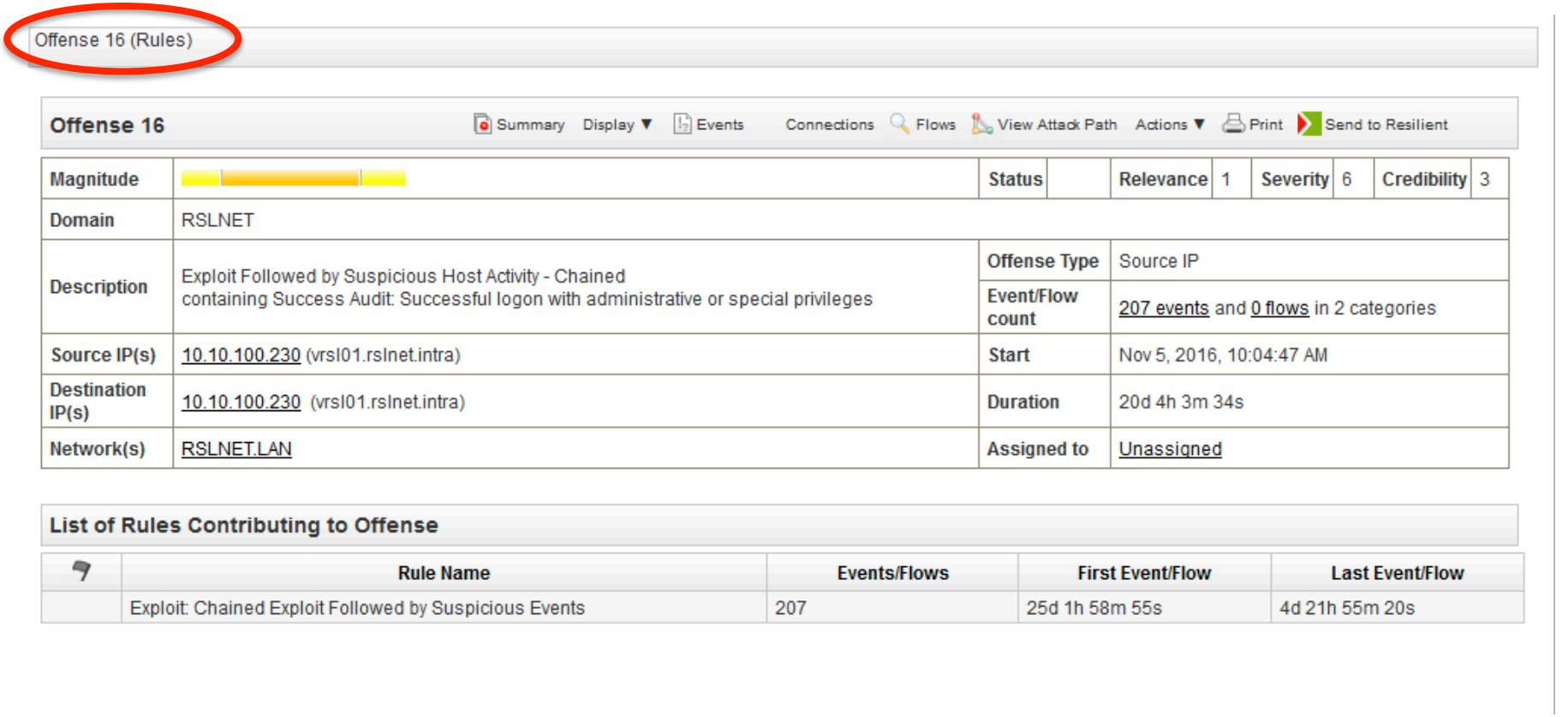
wieso?
weshalb?
warum?
woher?



Summary lesen!!!
top5 users
top5 categories
last 10 events
top5 annotations



## triggering rule



Offense 16 (Rules)

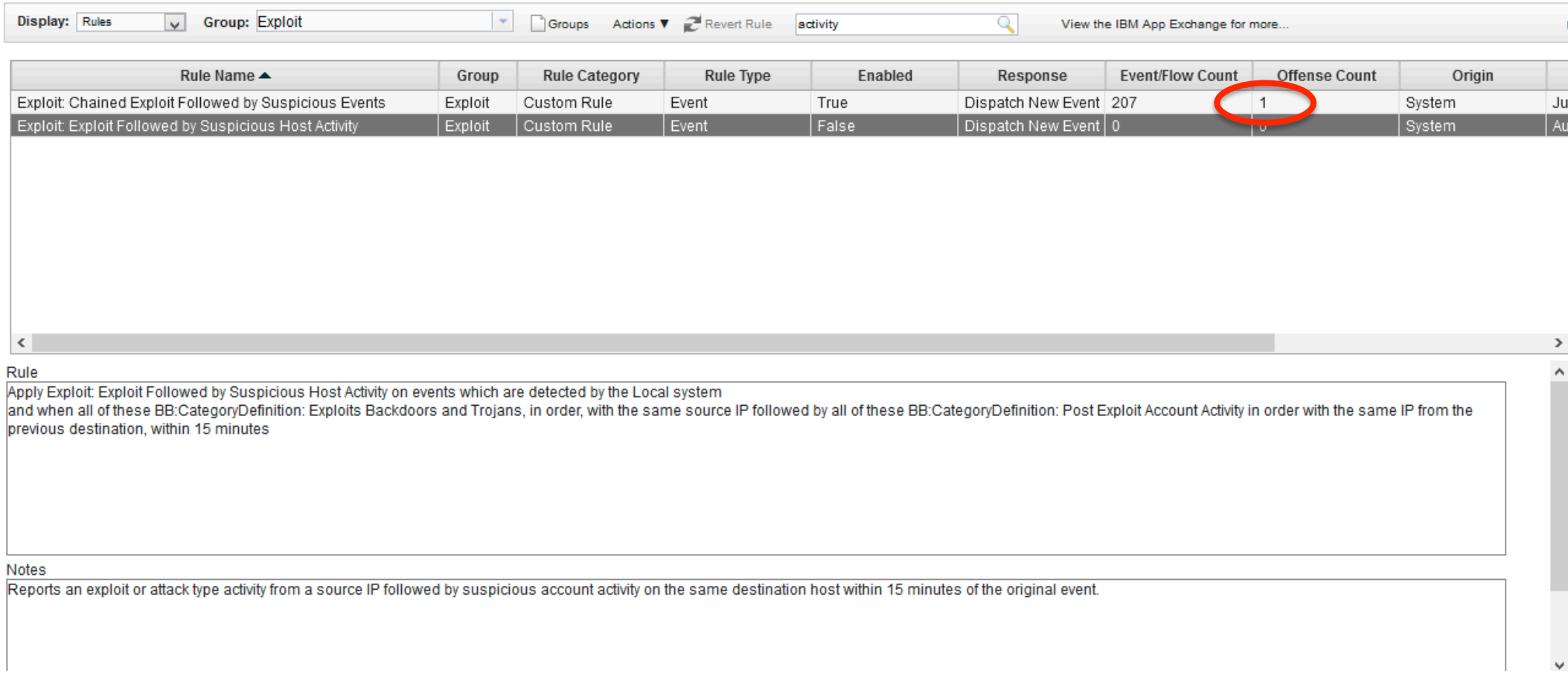
**Offense 16** Summary | Display ▼ | Events | Connections | Flows | View Attack Path | Actions ▼ | Print | Send to Resilient

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Magnitude** | | **Status** | | **Relevance** | 1 | **Severity** | 6 | **Credibility** | 3 |
| **Domain** | RSLNET | | | | | | | | |
| **Description** | Exploit Followed by Suspicious Host Activity - Chained<br>containing Success Audit: Successful logon with administrative or special privileges | **Offense Type** | Source IP | | | | | | |
| | | **Event/Flow count** | 207 events and 0 flows in 2 categories | | | | | | |
| **Source IP(s)** | 10.10.100.230 (vrsl01.rslnet.intra) | **Start** | Nov 5, 2016, 10:04:47 AM | | | | | | |
| **Destination IP(s)** | 10.10.100.230 (vrsl01.rslnet.intra) | **Duration** | 20d 4h 3m 34s | | | | | | |
| **Network(s)** | RSLNET.LAN | **Assigned to** | Unassigned | | | | | | |

**List of Rules Contributing to Offense**

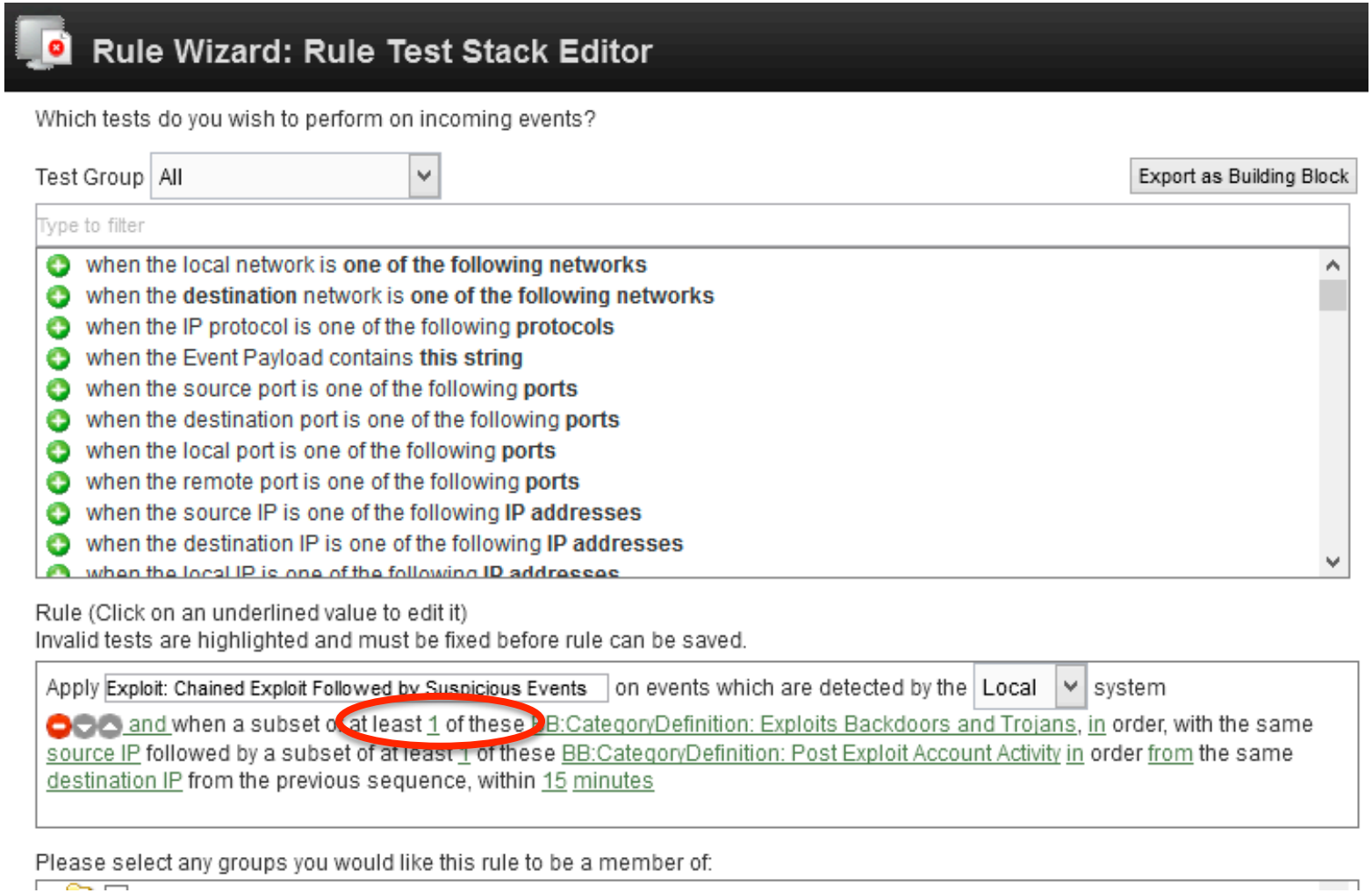
| | Rule Name | Events/Flows | First Event/Flow | Last Event/Flow |
|---|---|---|---|---|
| | Exploit: Chained Exploit Followed by Suspicious Events | 207 | 25d 1h 58m 55s | 4d 21h 55m 20s |

rules chaining



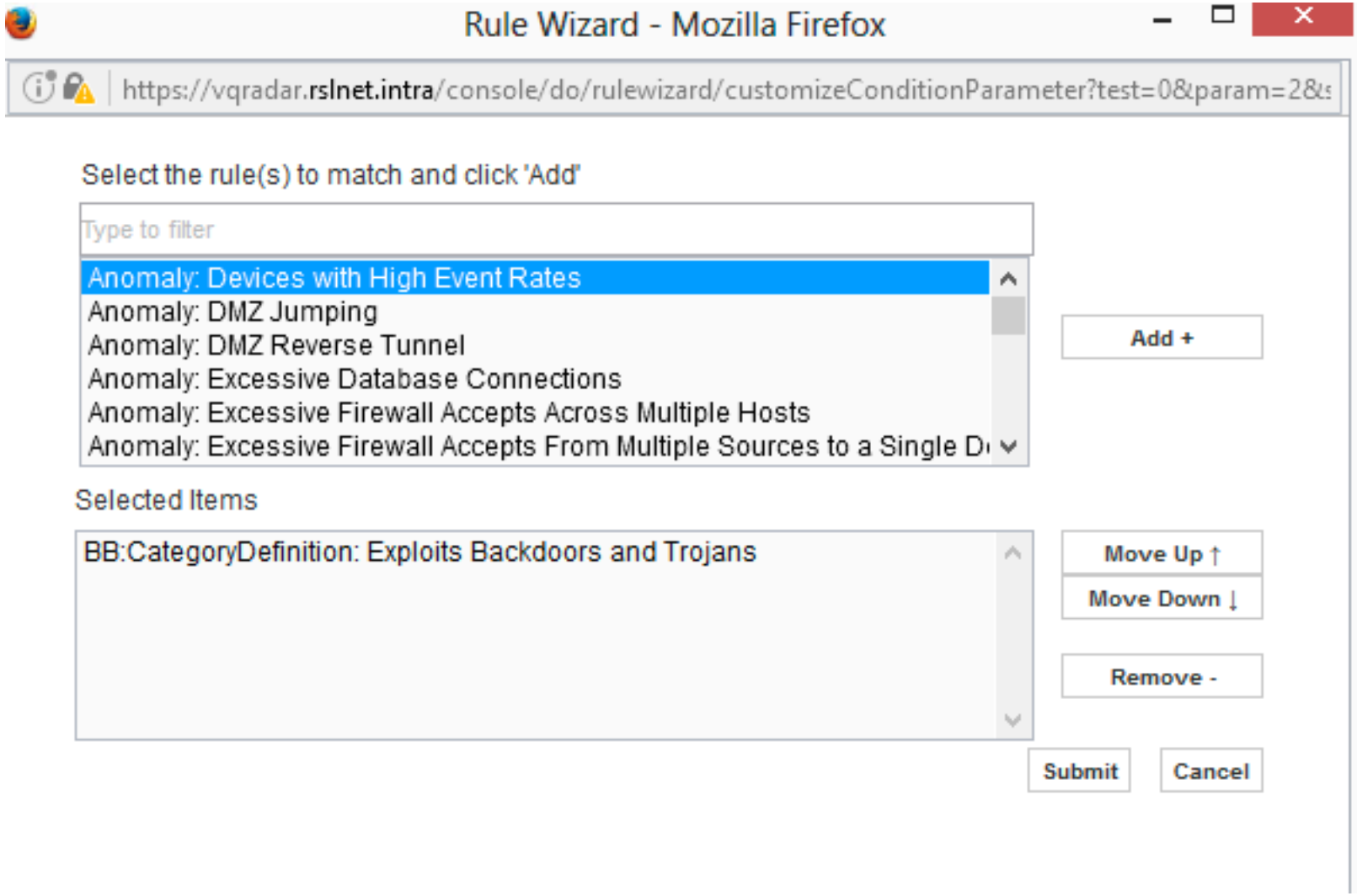
rule wizard

contains 2 BBs!

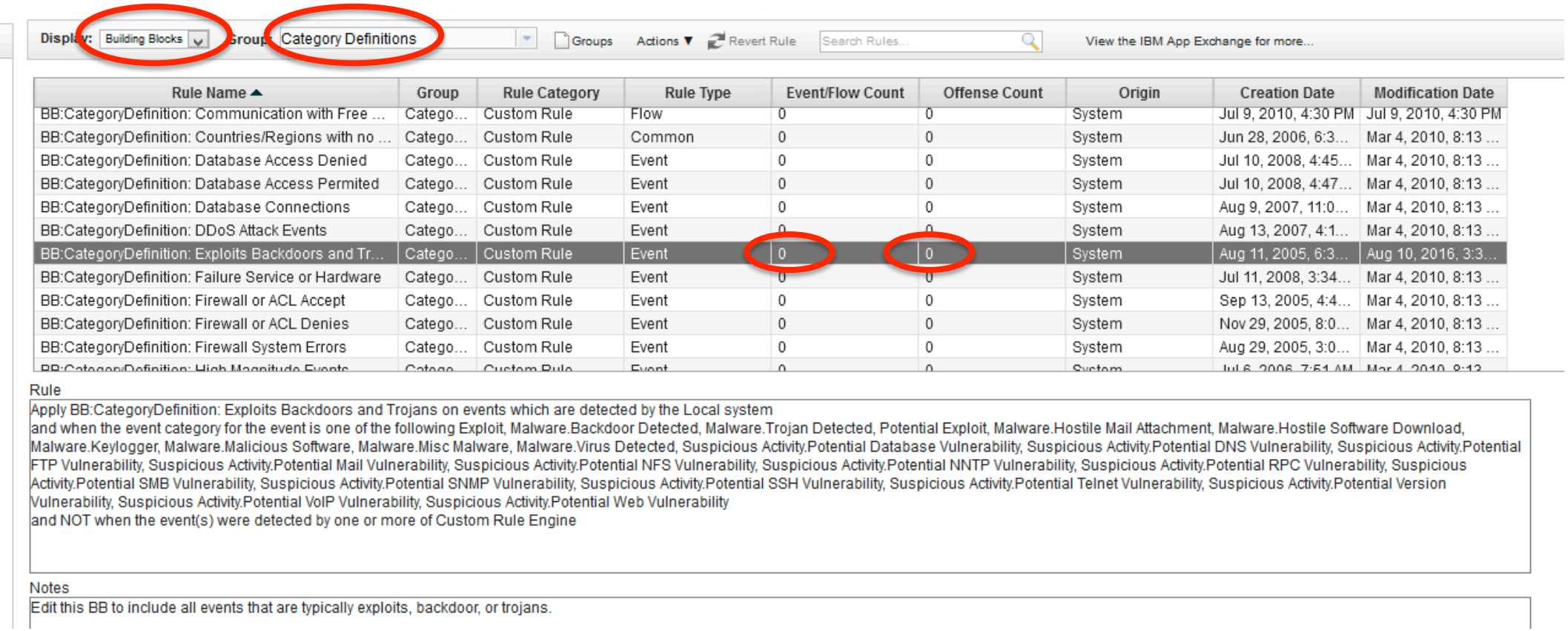


analyze BBs

no drilldown!



# BB search – no match



pro4bizz
protect.your.business

# BB trigger based on event category – match!

Display: Building Blocks | Group: Rule and Building Block Groups | Groups | Actions | Revert Rule | Search Rules... | View the IBM App Exchange for more...

| Rule Name | Group | Rule Category | Rule Type | Event/Flow Count | Offense Count | Origin | Creation Date | Modification Date |
|---|---|---|---|---|---|---|---|---|
| BB:CategoryDefinition: Mail Policy Violation | Catego... | Custom Rule | Event | 0 | 0 | System | Jan 6, 2006, 3:27 ... | Mar 4, 2010, 8:13 ... |
| BB:CategoryDefinition: Malware Annoyances | Catego... | Custom Rule | Event | 0 | 0 | System | Apr 12, 2006, 5:3... | Mar 4, 2010, 8:13 ... |
| BB:CategoryDefinition: Network DoS Attack | Catego... | Custom Rule | Event | 0 | 0 | System | Jan 2, 2007, 5:14 ... | Mar 4, 2010, 8:13 ... |
| BB:CategoryDefinition: Off Hours | | Custom Rule | Common | 0 | 0 | System | Aug 10, 2010, 3:1... | Aug 10, 2010, 3:1... |
| BB:CategoryDefinition: Policy Events | Catego... | Custom Rule | Event | 0 | 0 | System | Sep 29, 2005, 5:3... | Mar 4, 2010, 8:13 ... |
| BB:CategoryDefinition: Post DMZ Jump | Catego... | Custom Rule | Common | 0 | 0 | System | Oct 21, 2008, 3:1... | Mar 4, 2010, 8:13 ... |
| BB:CategoryDefinition: Post Exploit Account Activity | Catego... | Custom Rule | Event | 0 | 0 | System | Aug 9, 2007, 10:4... | Mar 4, 2010, 8:13 ... |
| BB:CategoryDefinition: Pre DMZ Jump | Catego... | Custom Rule | Common | 0 | 0 | System | Oct 21, 2008, 3:1... | Mar 4, 2010, 8:13 ... |
| BB:CategoryDefinition: Pre Reverse DMZ Jump | Catego... | Custom Rule | Common | 0 | 0 | System | Oct 21, 2008, 3:2... | Mar 4, 2010, 8:13 ... |
| BB:CategoryDefinition: Privileged Activity : UBA | | Custom Rule | Event | 0 | 0 | System | May 11, 2016, 7:2... | Aug 10, 2016, 3:1... |
| BB:CategoryDefinition: Privileged Escalation Failed | | Custom Rule | Event | 0 | 0 | System | Aug 10, 2010, 3:4... | Aug 10, 2010, 3:4... |

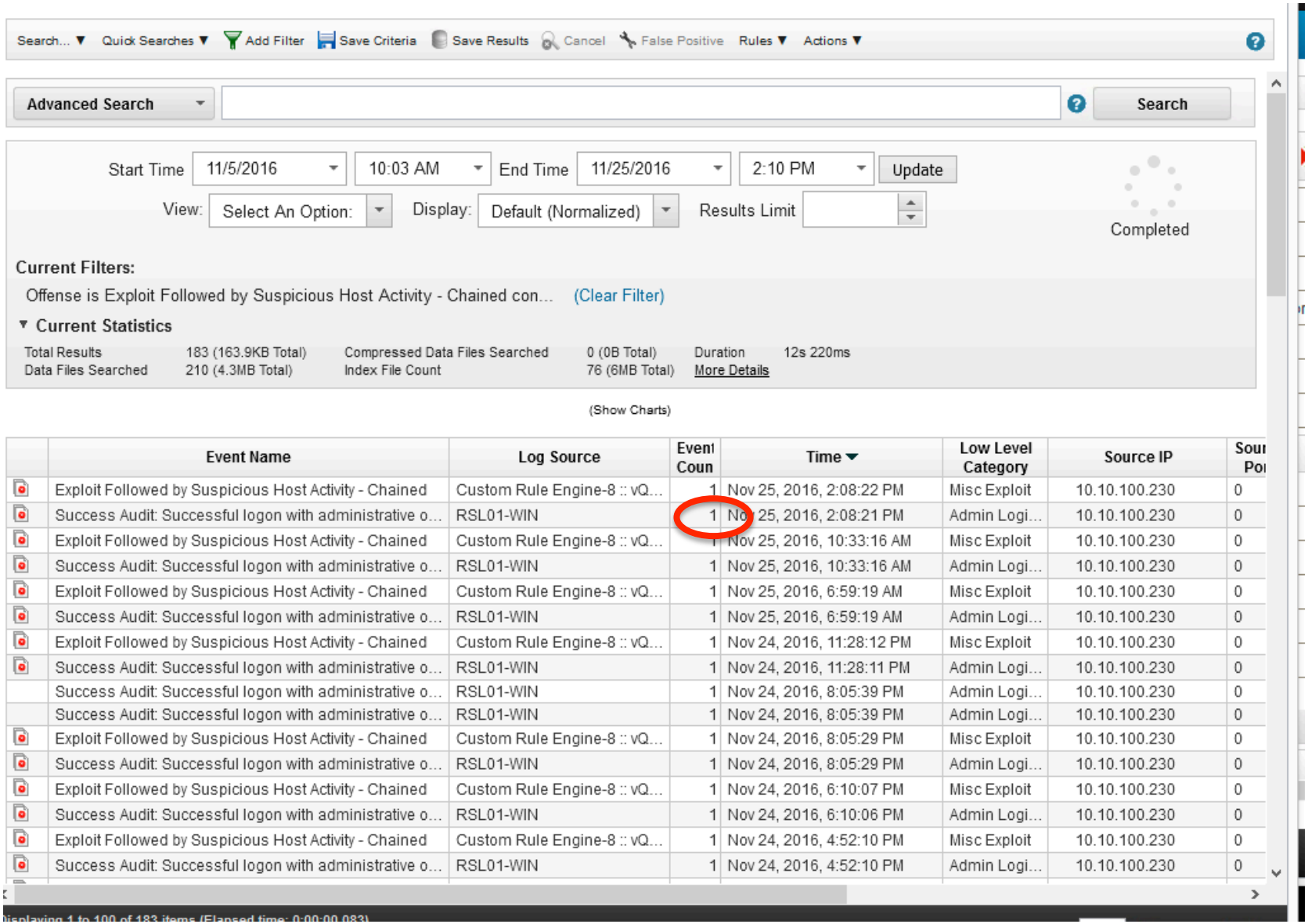
Rule

Apply BB:CategoryDefinition: Post Exploit Account Activity on events which are detected by the Local system
and when the event category for the event is one of the following Authentication.Admin Login Successful, Authentication.Auth Server Login Succeeded, Authentication.Computer Account Added, Authentication.Computer Account Changed, Authentication.Computer Account Removed, Authentication.FTP Login Succeeded, Authentication.General Authentication Successful, Authentication.Group Added, Authentication.Group Changed, Authentication.Group Member Added, Authentication.Group Member Removed, Authentication.Group Removed, Authentication.Host Login Succeeded, Authentication.Login with username/password defaults successful, Authentication.Mail Service Login Succeeded, Authentication.Misc Login Succeeded, Authentication.Password Change Succeeded, Authentication.Policy Added, Authentication.Policy Change, Authentication.Privilege Escalation Succeeded, Authentication.Remote Access Login Succeeded, Authentication.Samba Login Succeeded, Authentication.SSH Login Succeeded, Authentication.Suspicious Password, Authentication.Suspicious Username, Authentication.System Security Access Granted, Authentication.System Security Access Removed, Authentication.Telnet Login Succeeded, Authentication.Trusted Domain Added, Authentication.Trusted Domain Removed, Authentication.User Account Added, Authentication.User Account Changed, Authentication.User Account Removed, Authentication.User Right Assigned, Authentication.User Right Removed, Authentication.VoIP Login Succeeded, Authentication.Web Service Login Succeeded

Notes

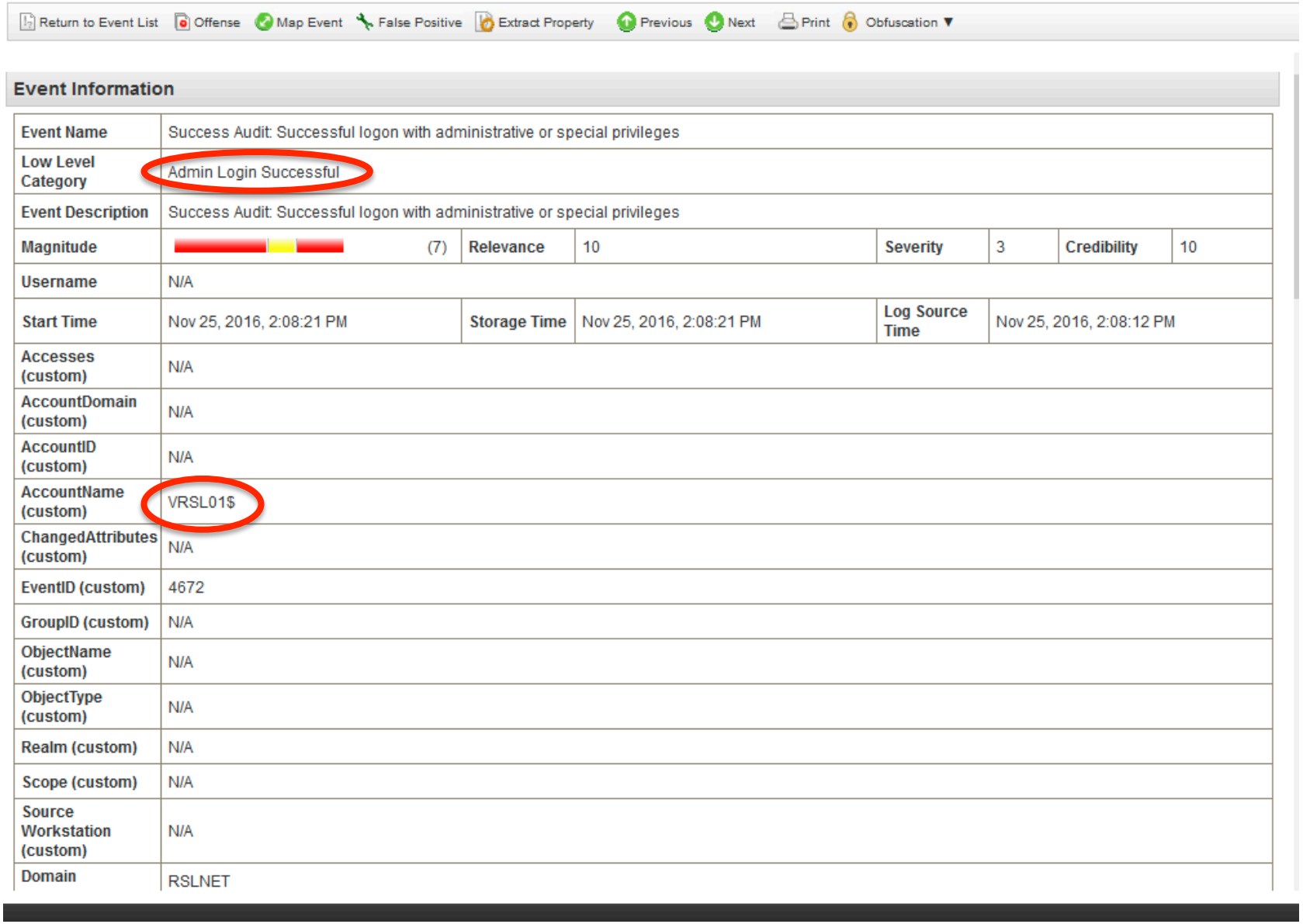
This Building Block identifies events that generally happen after an exploit.

## event search drill down




| Event Name | Log Source | Event Coun | Time | Low Level Category | Source IP | Sour Por |
|---|---|---|---|---|---|---|
| Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQ... | 1 | Nov 25, 2016, 2:08:22 PM | Misc Exploit | 10.10.100.230 | 0 |
| Success Audit: Successful logon with administrative o... | RSL01-WIN | 1 | Nov 25, 2016, 2:08:21 PM | Admin Logi... | 10.10.100.230 | 0 |
| Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQ... | 1 | Nov 25, 2016, 10:33:16 AM | Misc Exploit | 10.10.100.230 | 0 |
| Success Audit: Successful logon with administrative o... | RSL01-WIN | 1 | Nov 25, 2016, 10:33:16 AM | Admin Logi... | 10.10.100.230 | 0 |
| Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQ... | 1 | Nov 25, 2016, 6:59:19 AM | Misc Exploit | 10.10.100.230 | 0 |
| Success Audit: Successful logon with administrative o... | RSL01-WIN | 1 | Nov 25, 2016, 6:59:19 AM | Admin Logi... | 10.10.100.230 | 0 |
| Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQ... | 1 | Nov 24, 2016, 11:28:12 PM | Misc Exploit | 10.10.100.230 | 0 |
| Success Audit: Successful logon with administrative o... | RSL01-WIN | 1 | Nov 24, 2016, 11:28:11 PM | Admin Logi... | 10.10.100.230 | 0 |
| Success Audit: Successful logon with administrative o... | RSL01-WIN | 1 | Nov 24, 2016, 8:05:39 PM | Admin Logi... | 10.10.100.230 | 0 |
| Success Audit: Successful logon with administrative o... | RSL01-WIN | 1 | Nov 24, 2016, 8:05:39 PM | Admin Logi... | 10.10.100.230 | 0 |
| Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQ... | 1 | Nov 24, 2016, 8:05:29 PM | Misc Exploit | 10.10.100.230 | 0 |
| Success Audit: Successful logon with administrative o... | RSL01-WIN | 1 | Nov 24, 2016, 8:05:29 PM | Admin Logi... | 10.10.100.230 | 0 |
| Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQ... | 1 | Nov 24, 2016, 6:10:07 PM | Misc Exploit | 10.10.100.230 | 0 |
| Success Audit: Successful logon with administrative o... | RSL01-WIN | 1 | Nov 24, 2016, 6:10:06 PM | Admin Logi... | 10.10.100.230 | 0 |
| Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQ... | 1 | Nov 24, 2016, 4:52:10 PM | Misc Exploit | 10.10.100.230 | 0 |
| Success Audit: Successful logon with administrative o... | RSL01-WIN | 1 | Nov 24, 2016, 4:52:10 PM | Admin Logi... | 10.10.100.230 | 0 |

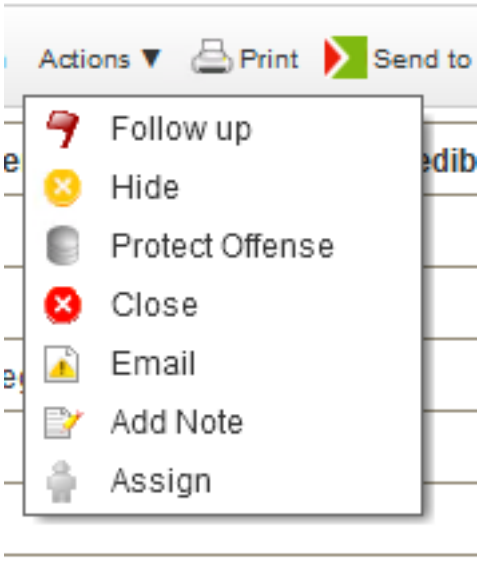
system account!



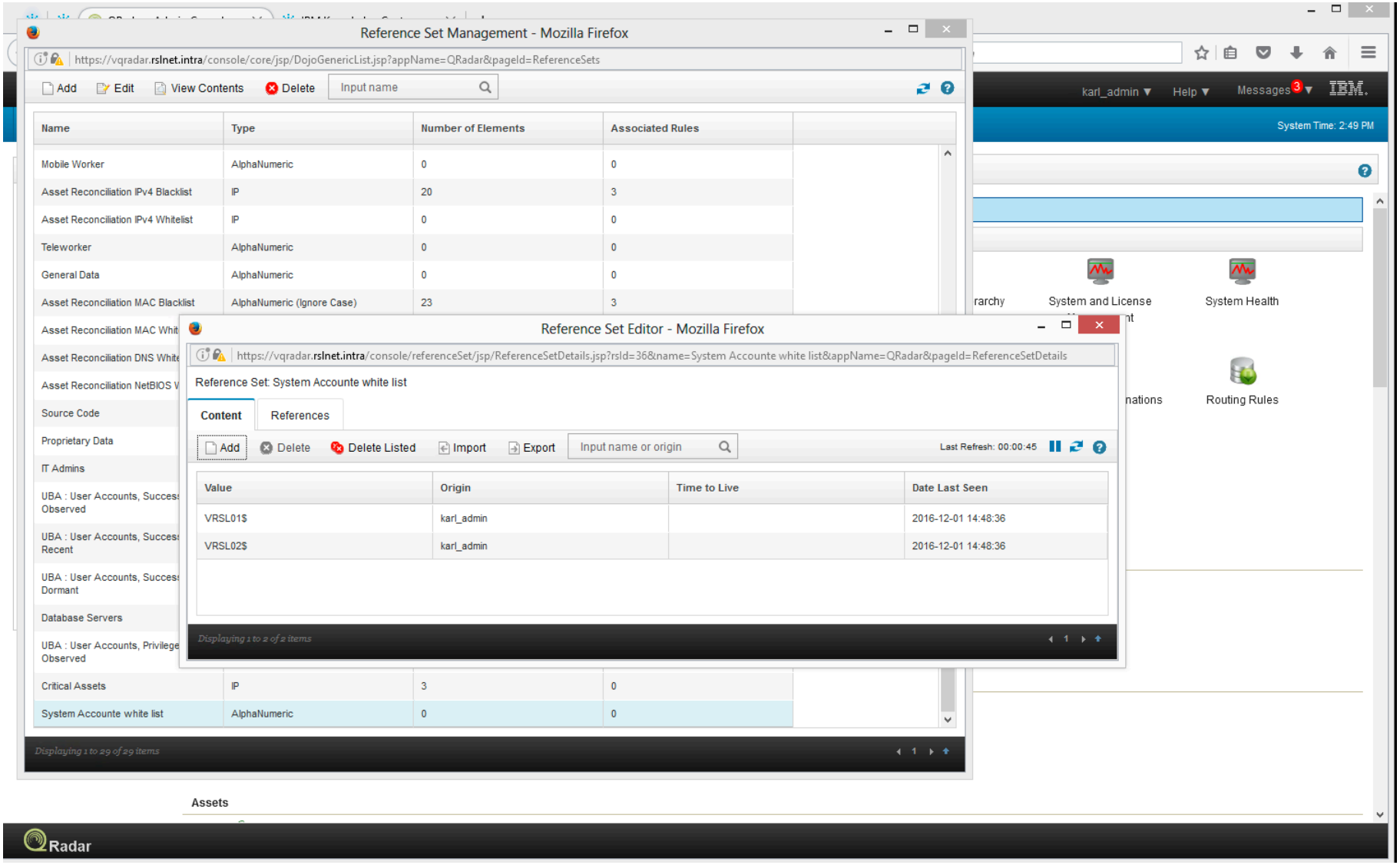

**Event Information**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Event Name** | Success Audit: Successful logon with administrative or special privileges | | | | | | |
| **Low Level Category** | Admin Login Successful | | | | | | |
| **Event Description** | Success Audit: Successful logon with administrative or special privileges | | | | | | |
| **Magnitude** | (7) | **Relevance** | 10 | **Severity** | 3 | **Credibility** | 10 |
| **Username** | N/A | | | | | | |
| **Start Time** | Nov 25, 2016, 2:08:21 PM | **Storage Time** | Nov 25, 2016, 2:08:21 PM | **Log Source Time** | Nov 25, 2016, 2:08:12 PM | | |
| **Accesses (custom)** | N/A | | | | | | |
| **AccountDomain (custom)** | N/A | | | | | | |
| **AccountID (custom)** | N/A | | | | | | |
| **AccountName (custom)** | VRSL01$ | | | | | | |
| **ChangedAttributes (custom)** | N/A | | | | | | |
| **EventID (custom)** | 4672 | | | | | | |
| **GroupID (custom)** | N/A | | | | | | |
| **ObjectName (custom)** | N/A | | | | | | |
| **ObjectType (custom)** | N/A | | | | | | |
| **Realm (custom)** | N/A | | | | | | |
| **Scope (custom)** | N/A | | | | | | |
| **Source Workstation (custom)** | N/A | | | | | | |
| **Domain** | RSLNET | | | | | | |

tuning
hide offense!

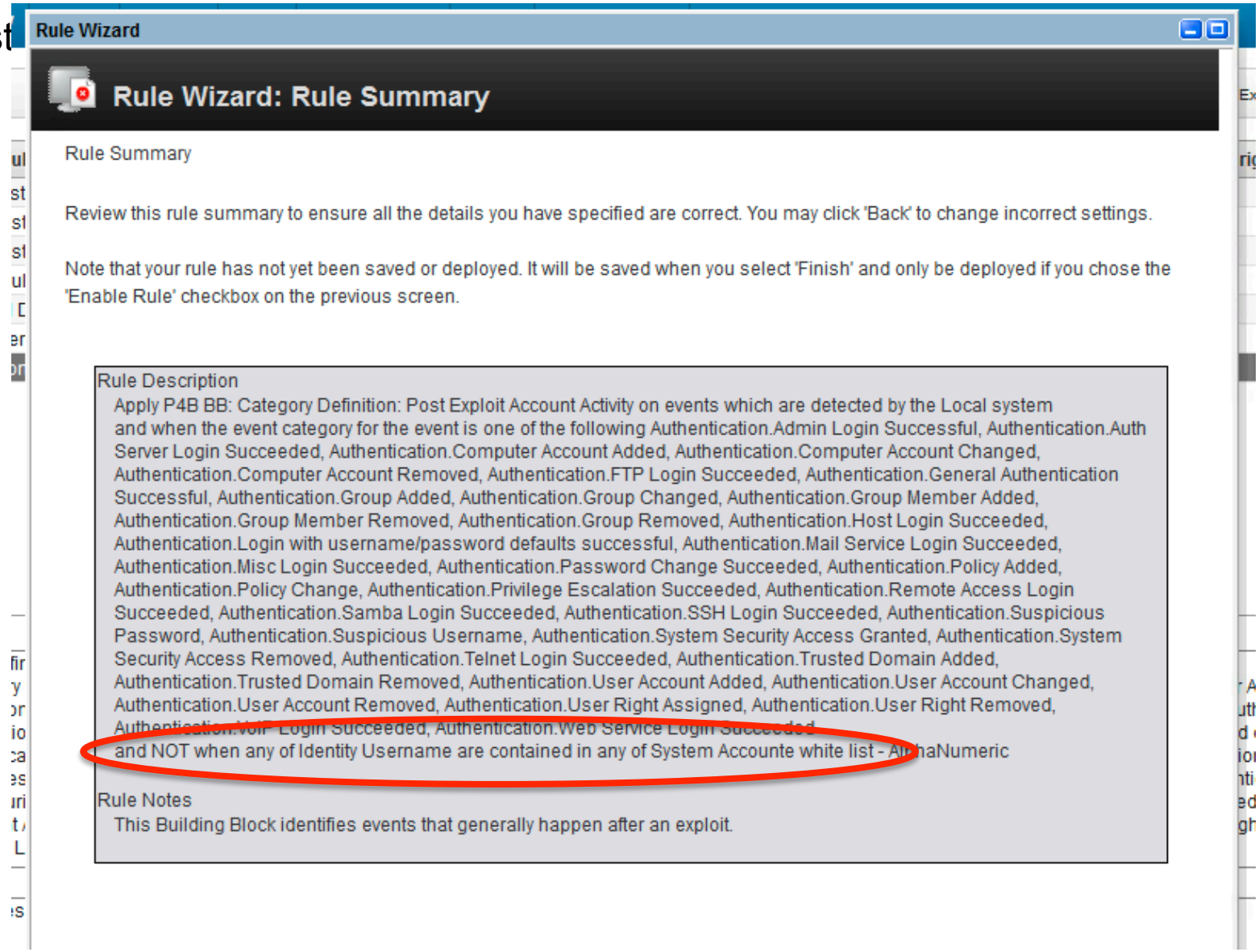


## tuning - add to reference set

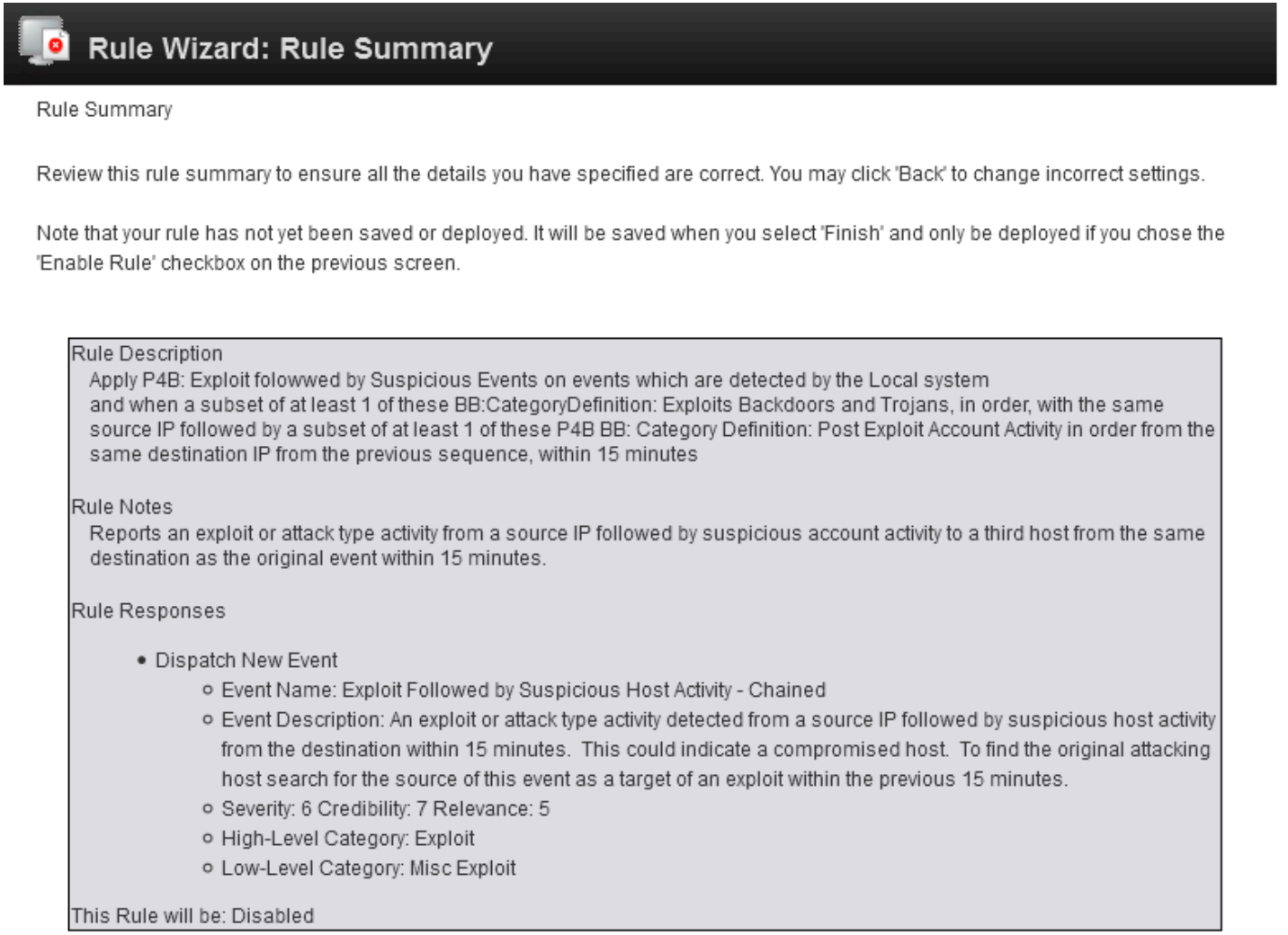


tuning – modify BB

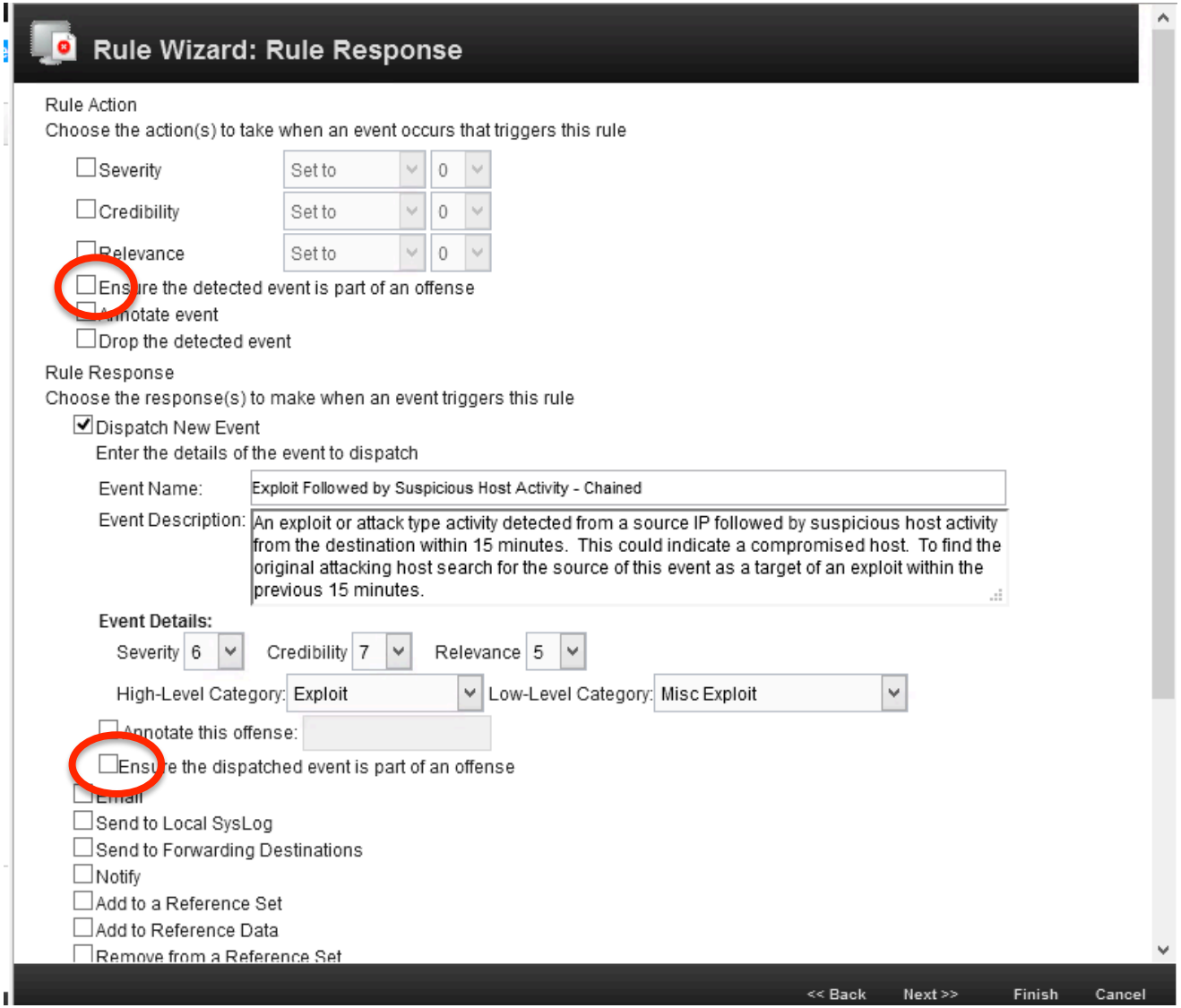
check auf white list



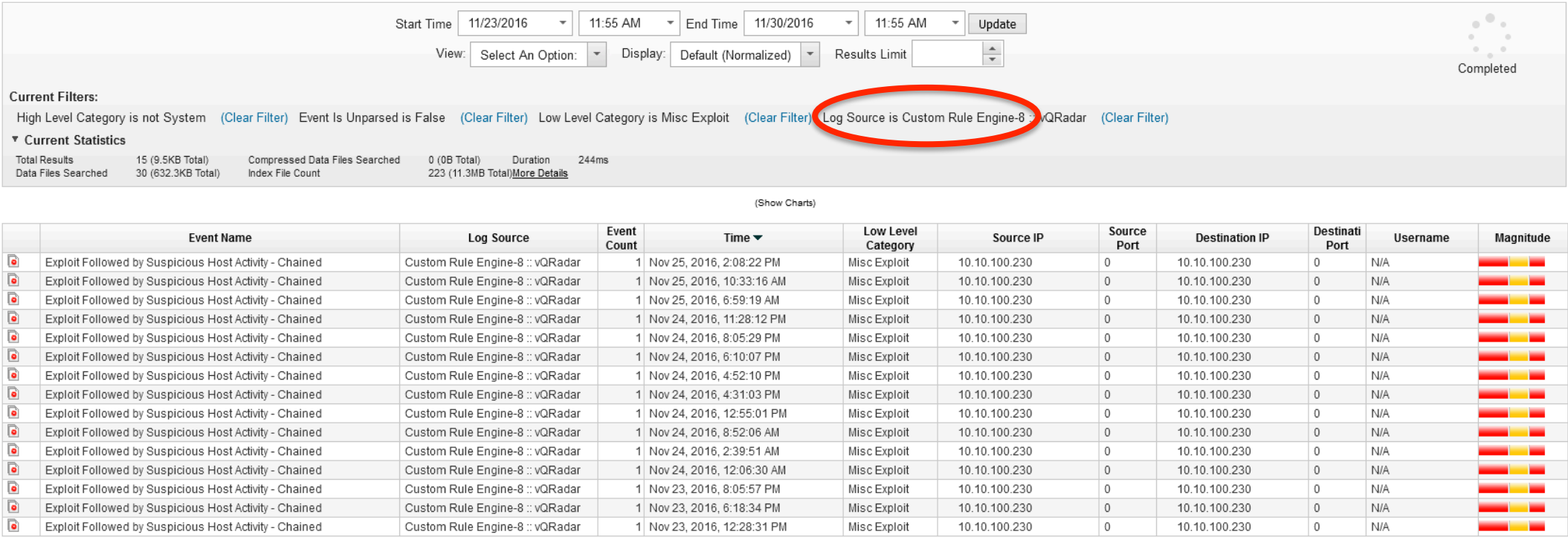
tuning – modify rule
ersetze BB in rule



tuning – remove offense from rule
no offense
no false negative
no cry ☺



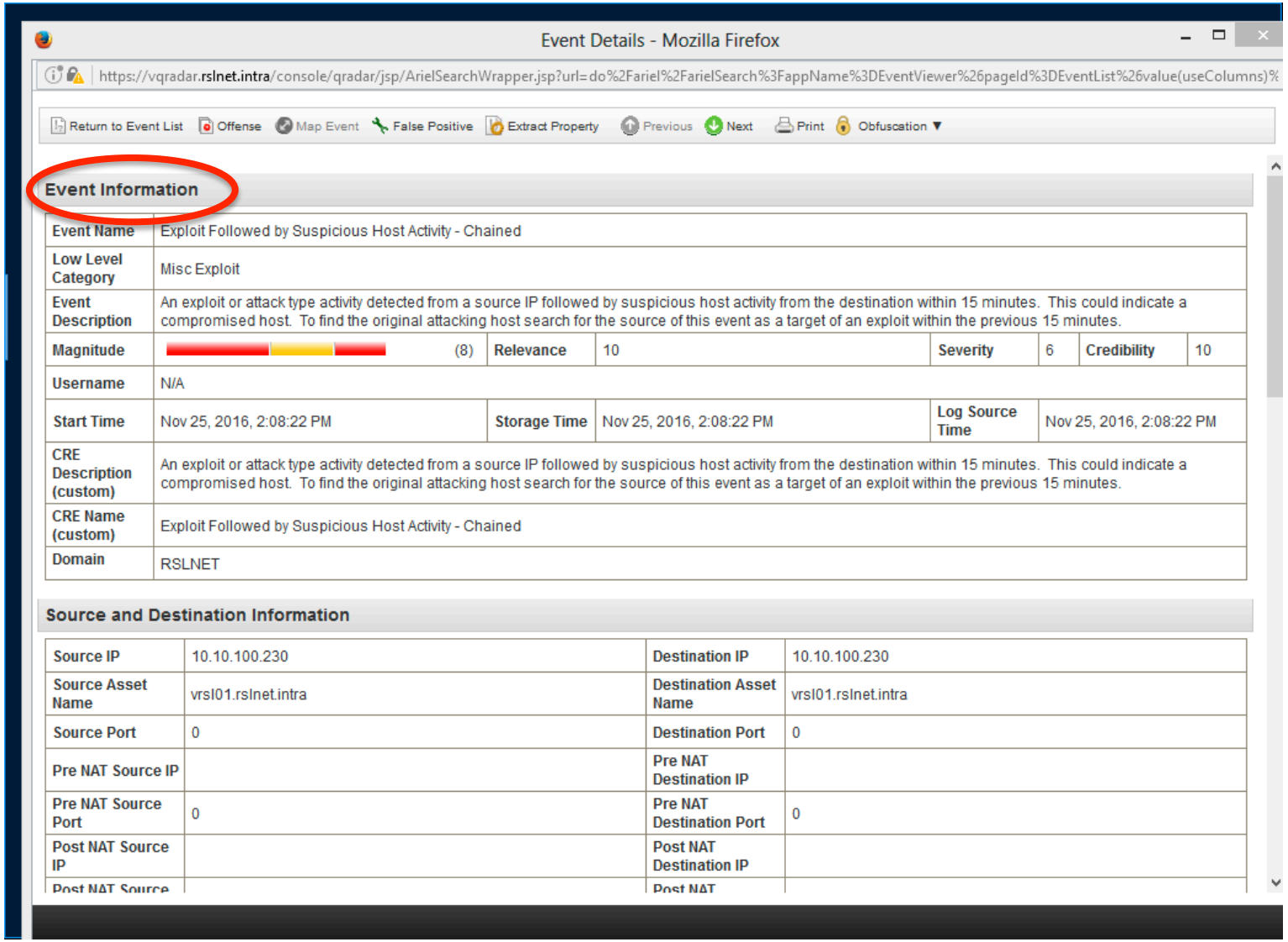
# Tipps: CRE search




| | Event Name | Log Source | Event Count | Time | Low Level Category | Source IP | Source Port | Destination IP | Destinati Port | Username | Magnitude |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQRadar | 1 | Nov 25, 2016, 2:08:22 PM | Misc Exploit | 10.10.100.230 | 0 | 10.10.100.230 | 0 | N/A | |
| | Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQRadar | 1 | Nov 25, 2016, 10:33:16 AM | Misc Exploit | 10.10.100.230 | 0 | 10.10.100.230 | 0 | N/A | |
| | Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQRadar | 1 | Nov 25, 2016, 6:59:19 AM | Misc Exploit | 10.10.100.230 | 0 | 10.10.100.230 | 0 | N/A | |
| | Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQRadar | 1 | Nov 24, 2016, 11:28:12 PM | Misc Exploit | 10.10.100.230 | 0 | 10.10.100.230 | 0 | N/A | |
| | Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQRadar | 1 | Nov 24, 2016, 8:05:29 PM | Misc Exploit | 10.10.100.230 | 0 | 10.10.100.230 | 0 | N/A | |
| | Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQRadar | 1 | Nov 24, 2016, 6:10:07 PM | Misc Exploit | 10.10.100.230 | 0 | 10.10.100.230 | 0 | N/A | |
| | Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQRadar | 1 | Nov 24, 2016, 4:52:10 PM | Misc Exploit | 10.10.100.230 | 0 | 10.10.100.230 | 0 | N/A | |
| | Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQRadar | 1 | Nov 24, 2016, 4:31:03 PM | Misc Exploit | 10.10.100.230 | 0 | 10.10.100.230 | 0 | N/A | |
| | Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQRadar | 1 | Nov 24, 2016, 12:55:01 PM | Misc Exploit | 10.10.100.230 | 0 | 10.10.100.230 | 0 | N/A | |
| | Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQRadar | 1 | Nov 24, 2016, 8:52:06 AM | Misc Exploit | 10.10.100.230 | 0 | 10.10.100.230 | 0 | N/A | |
| | Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQRadar | 1 | Nov 24, 2016, 2:39:51 AM | Misc Exploit | 10.10.100.230 | 0 | 10.10.100.230 | 0 | N/A | |
| | Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQRadar | 1 | Nov 24, 2016, 12:06:30 AM | Misc Exploit | 10.10.100.230 | 0 | 10.10.100.230 | 0 | N/A | |
| | Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQRadar | 1 | Nov 23, 2016, 8:05:57 PM | Misc Exploit | 10.10.100.230 | 0 | 10.10.100.230 | 0 | N/A | |
| | Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQRadar | 1 | Nov 23, 2016, 6:18:34 PM | Misc Exploit | 10.10.100.230 | 0 | 10.10.100.230 | 0 | N/A | |
| | Exploit Followed by Suspicious Host Activity - Chained | Custom Rule Engine-8 :: vQRadar | 1 | Nov 23, 2016, 12:28:31 PM | Misc Exploit | 10.10.100.230 | 0 | 10.10.100.230 | 0 | N/A | |

# Tipp: zero offense rule vs. CRE event

custom CRE event triggers
no false alarm



Tipps: beteiligte BBs prüfen und ggfs. anpassen

- network
- white list
- black list

| Rule Name ▲ | Group | Rule Category | Rule Type | Event/Flow Count | Offense Count | Origin | Creation Date | Modification Date |
|---|---|---|---|---|---|---|---|---|
| BB:BehaviorDefinition: Compromise Activities | Catego... | Custom Rule | Event | 0 | 0 | System | Jul 11, 2008, 2:44... | Mar 4, 2010, 8:13 ... |
| BB:CategoryDefinition: Exploits Backdoors and Trojans | Catego... | Custom Rule | Event | 0 | 0 | System | Aug 11, 2005, 6:3... | Aug 10, 2016, 3:3... |
| BB:CategoryDefinition: Policy Events | Catego... | Custom Rule | Event | 0 | 0 | System | Sep 29, 2005, 5:3... | Mar 4, 2010, 8:13 ... |
| BB:CategoryDefinition: Post Exploit Account Activity | Catego... | Custom Rule | Event | 0 | 0 | System | Aug 9, 2007, 10:4... | Mar 4, 2010, 8:13 ... |
| BB:CategoryDefinition: Privileged Activity : UBA | | Custom Rule | Event | 0 | 0 | System | May 11, 2016, 7:2... | Aug 10, 2016, 3:1... |
| BB:CategoryDefinition: Recon Event Categories | Catego... | Custom Rule | Event | 0 | 0 | System | May 6, 2010, 3:17 ... | May 6, 2010, 3:17 ... |
| BB:CategoryDefinition: Recon Events | Catego... | Custom Rule | Common | 0 | 0 | System | Aug 11, 2005, 1:3... | Mar 4, 2010, 8:13 ... |
| BB:CategoryDefinition: Recon Flows | Catego... | Custom Rule | Flow | 0 | 0 | System | May 6, 2010, 3:17 ... | May 6, 2010, 3:19 ... |
| BB:CategoryDefinition: Suspicious Event Categories | Catego... | Custom Rule | Event | 0 | 0 | System | May 6, 2010, 3:14 ... | May 6, 2010, 3:14 ... |
| BB:CategoryDefinition: Suspicious Events | Catego... | Custom Rule | Common | 0 | 0 | System | Aug 29, 2005, 2:4... | Mar 4, 2010, 8:13 ... |
| BB:CategoryDefinition: Suspicious Flows | Catego... | Custom Rule | Flow | 0 | 0 | System | May 6, 2010, 2:32 ... | May 6, 2010, 3:26 ... |

Rule

Apply BB:CategoryDefinition: Suspicious Event Categories on events which are detected by the Local system
and when the event category for the event is one of the following Suspicious Activity, Potential Exploit, Access.ACL Deny, Access.Firewall Deny, Access.IPS Deny, Access.No Translation Group Found, Flow.Empty Packet Flows, Flow.High number of Empty Packet Flows, Flow.High number of Unidirectional Flows, Flow.High number of Unidirectional ICMP Flows, Flow.High number of Unidirectional TCP Flows, Flow.Low number of Empty Packet Flows, Flow.Low number of Unidirectional Flows, Flow.Low number of Unidirectional ICMP Flows, Flow.Low number of Unidirectional TCP Flows, Flow.Medium number of Empty Packet Flows, Flow.Medium number of Unidirectional Flows, Flow.Medium number of Unidirectional ICMP Flows, Flow.Medium number of Unidirectional TCP Flows, Flow.Suspicious Flow, Flow.Suspicious ICMP Flow, Flow.Suspicious TCP Flow, Flow.Suspicious UDP Flow, Flow.Unidirectional Flow, Flow.Unidirectional ICMP Flow, Flow.Unidirectional TCP Flow, Authentication.Admin Login Failure, Authentication.Auth Server Login Failed, Authentication.FTP Login Failed, Authentication.General Authentication Failed, Authentication.Host Login Failed, Authentication.Login with username/password defaults failed, Authentication.Mail Service Login Failed, Authentication.Misc Login Failed, Authentication.Privilege Escalation Failed, Authentication.Remote Access Login Failed, Authentication.Samba Login Failed, Authentication.SSH Login Failed, Authentication.Suspicious Password, Authentication.Suspicious Username, Authentication.Telnet Login Failed, Authentication.Web Service Login Failed

Notes

Edit this BB to include all events that indicate suspicious activity.