Discontinued Content

In an ongoing effort to provide the best user experience, RSA periodically discontinues content (such as rules and reports). This is to keep pace with the ever evolving threat landscape, and to ensure our customers are not overwhelmed with stale information and ‘alert fatigue’. By tailoring content to current threats, we can help keep the systems performing efficiently. In addition, this is part of an effort to refocus to more threat- and data-driven approaches to detection.

Note:	All Flex parsers are discontinued. For replacements, see **Mapping of Flex to Lua Parsers**.

Some reasons that a piece of content is discontinued:

- Replaced by better, newer content
- Offered little or no value
- Threats that are no longer relevant

Note:	Discontinued content still appears. In RSA NetWitness Platform, there is a checkbox to show discontinued content. With discontinued content there just won’t be any updates, and users won’t see these items when they search in Live.

RSA Application Rules

Name	Title	Description	Notes
nw02605	adware client	Detects known malware with a client header of "downloadmr"	This is an out-dated threat and detection method, thus no longer relevant.
nw132520	APT Domain Intelligence	Helper Rule for domain and IP list that were identified as possibly harboring APT.	The domains have expired, and the IP addresses have not been used in any recent campaigns.
nw45080	carberp botnet activity	Detects known Carberp botnet activity	The botnet is no longer active, and the indicators in this rule have gotten stale.
nw30025	Console Gaming	Detects user-agent strings associated with the Xbox, Playstation and Wii gaming consoles.	Provides very little enterprise security value.
nw45645	CryptoLocker Beaconing	Detects traffic indicative of the beaconing activity of the Russian CryptoLocker ransom-ware variants.	Returned too many false positives to be useful.
nw10001	custom router firmware admin page	Detects connections to SOHO routers that have been upgraded using DD-WRT or Tomato firmware. This allows enhanced functionality from a home internet connection and is often a precursor or indicator for tunneling activity.	Description does not match what the rule detects. Additionally, the rule is dependent upon technology not updated since 2013.
nw00025	Direct to IP HTTP Request	session with an HTTP request directly to an IP address with no corresponding alias.host meta.	Replaced by logic in the HTTP Lua parser.
nw30045	Escalation - Multiple Blacklist Feed Hits	Creates alert in **risk.warning** if a single session triggers 3 or more NetWitness Live feeds hits.	Provides very little enterprise security value.
nw30035	Escalation - Multiple Informational	Creates a **risk.suspicious** alert if 3 or more risk.info alerts exist in a single session.	Provides very little enterprise security value.
nw30040	Escalation - Multiple Suspicious	Creates alert in **risk.warning** if 3 or more **risk.suspicious** alerts exist in a single session.	Provides very little enterprise security value.
nw100005	Facebook Login	Identifies logins to Facebook.	Facebook works on full SSL now, so this rule never fires.
nw100010	Facebook Profile	Identifies visits to Facebook profile pages	Facebook works on full SSL now, so this rule never fires.

nw20045	Fake Antivirus Malware Indicators	Detects filenames and alias.hosts with the words **antivirus**, **scan**, or **protect** in them. If filenames are detected, they are tied to a forensic, executable fingerprint.	This rule generated thousands of false positives, and depended upon a discontinued flex parser.
nw20040	Fake Codec Malware Indicators	detects domains and filenames with the word \codec\ in them.	Excessively noisy.
nw110140	jRAT Download	Detects an internal network session download of jRAT. A network parser that supports population of meta keys of "action" and "filename" is required. Examples of such network parsers are HTTP, FTP, IRC and NFS.	There is no longer active support for this rule, and thus it will never trigger.
nw110055	Large Outbound Session to File Upload Sites	"Detects an Outbound session where the data size is greater than 5 MB, and the destination is identified by the File Upload Sites feed.	Relies on File Upload Sites feed, which is being deprecated due to the large number and distributed nature of cloud storage services.
nw30020	loopback Traffic	Detects references to 127.0.0.0/8 in sessions.	Discontinued to reduce negative indicators.
nw90006	NJRAT Acquisition	10.4 and higher. Detects web traffic from an internal IP address to the following URL: **http://ge.tt/85SH60t/v/0**.	There is no longer active support for this rule, and thus it will never trigger.
NWFL_AuthFailure	NWFL_account:auth-failure	NWFL App Rule to support Informer Reports.	This rule was never released to Live.
nw02635	php botnet beaconing w	Detects botnet beaconing with w=188 in the query string.	This rule has never provided any value.
nw02575	php put with 40x error	Detects PHP puts that create 4 series errors. This may indicate suspicious or botnet check-in traffic.	This rule has never provided any value. Further, a similar detection exists in HTTP_lua.
nw02595	potential Chinese malware installer	Detects when an HTTP transaction has a client header that begins "agent". This has been observed by RSA Research in malware incidents.	Stale and outdated TTP associated with malware.
nw20055	Potential Exploit Payload Delivery	Detects forensic file type content being delivered via a suspicious filename as identified by suspicious filename feeds.	This is an outdated TTP associated with Exploit Kits no longer found in the wild.
nw110080	Remote Control Client Download	Detects remote client file downloads by looking for the file name and extension within the filename meta key. Use of an HTTP network parser is required.	There is no longer active support for this rule, and thus it will never trigger.
nw70005	Skype Login	Detects a Skype client checking for software updates.	Logins are now encrypted, so this rule is no longer valid.
nw20115	Small Executable From Black listed Host	Detects a small executable from a host on a NetWitness Live Blacklist.	Superseded by nw20065 (High Risk File From Blacklisted Host).
nw02610	suspicious client contains	Detects suspicious clients (my toolbar, winhttprequest).	Outdated signatures for clients no longer found in the wild.
nw02570	suspicious server banner	Detects certain server banners that are suspicious in nature.	Outdated signatures for servers no longer found in the wild.
nw02630	tax document in attachment	Detects attachments with the word tax in the filename.	Prone to too many false positives creating increased noise in the product.
nw02590	udp 16464 beaconing	Detects UDP beaconing on port 16464. This has been observed by RSA Research in malware-related check-in traffic	Limited number of Zero Access instances found in the wild
nw60160	Unknown Service Telnet Port	Detects an unidentified service over a port typically used for telnet traffic.	Duplicate of Unknown Service Over Telnet Port.
nw10005	wikileaks domain hit	Hits or DNS lookups of domains known to be Wikileaks mirrors, compiled from the mirror list at wikileaks.ch	Stale information based on the feed at wikileaks.ch that no longer exists.
nw110020	Wikileaks Email Submission	Detects emails being sent to the Wikileaks domain, sun- shinepress.org.	Due to the decentralized nature of Wikileaks and their use of TOR for submissions this

			rule is no longer valid.
nw30060	Windows NTLM Network Logon Successful	Indicates a possible pass-the-hash attack on Windows systems configured to use the NTLM authentication protocol. This rule does not apply to systems which use the Kerberos authentication protocol. The rule reduces false positives for anonymous logons and eliminates all DC or machine logons by removing any usernames that end in a $. It is recommended to exclude the domain that the Domain Controller is responsible within the rule logic.	An improved application rule for Pass the Hash has been created. This rule is very similar, and has been discontinued.
nw40005	Zeus Bot- net Activity	10.4 or higher. Alerts if a session contains a ZeuS tracker feed hit and a post to a PHP page on port 80.	Uses unsupported feeds in addition to looking for an outdated indicator, leading to little analytic value.
app00001	zusy_botnet	Detects the beaconing activity of the Zusy botnet.	An abandoned malware family. The last infection in the wild was last spotted 2 years ago.

RSA ESA (Event Stream Analysis) Rules

Name	Description	Notes
Active Directory Policy Modified	An Active Directory service object was changed—created, deleted, modified, or moved— in a Windows-based Active Directory system.	This rule triggers false positives when non-security related configuration changes are made.
Adapter Entered Promiscuous Mode	10.4 or higher. Detects when packet meta has a source country not equal to the home country, followed by a log event indicating the interface entered promiscuous mode. The packet destination IP address must match the device IP address of the log event. Both the home country and time range parameters are configurable.	This rule would only trigger under ideal circumstances that were highly unlikely in the wild. They were removed in favor of making the system more efficient.
Adapter in Promiscuous mode after Multiple login attempts	Five or more consecutive failed root login events followed by a successful login event from the same user and, then, the adapter goes into promiscuous mode within a time window of 5 minutes. The time window is configurable.	This rule would only trigger under ideal circumstances that were highly unlikely in the wild. They were removed in favor of making the system more efficient.
Adapter in Promiscuous mode after User Creation and Login	Adapter goes into promiscuous mode after the same user has been created and logged on within 5 minutes. The time window is configurable.	This rule would only trigger under ideal circumstances that were highly unlikely in the wild. They were removed in favor of making the system more efficient.
Attempted Identity Abuse via Excessive Login Failures	Detects identity abuse when there are multiple failed logins from the same user to multiple destinations.	This rule is superseded by esa000111, **Logins Across Multiple Servers**.
Brute Force Login From Same Source	Detects more than 10 failed login attempts from the same host within a five-minute time period.	Replaced by Multiple Failed Logins Followed by Successful Login rule
Brute Force Login To Same Destination	Detects more than 10 failed login attempts to the same destination within a five-minute time period.	Replaced by Multiple Failed Logins Followed by Successful Login rule
Consecutive Login without Logout	Detects consecutive logins by the same user to the same system without a logout.	This rule creates a large number of false positives because, a user can be disconnected from the network without any log notifications or events.
Cybergate RAT Download	Detects an internal network session download of CyberGate RAT.	Replaced by an application rule.
Detection of High Volume of TCP Resets using Netflow	Detects a high volume of TCP resets in a given time frame. TCP resets are detected via tcp flags captured from Network Flows. TCP Reset is detected when tcp_flags(tcp_flags_seen) = 4 (RST) or 20 (RST+ACK).	Never functioned as designed.
Direct Login By A Guest Account	Detects a successful interactive logon or a successful remote interactive logon to a guest account on a Microsoft Windows host.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1).

		The new rule is supported in RSA NetWitness version 11.1 and higher.
Direct Login to an Administrative Account	Detects a successful interactive or remote interactive logon using an administrative account for Windows. The list of administrative accounts is configurable.	This rule was merged into the **Direct Login to Watchlist Account** ESA rule.
DNS Lookups from the Same Host	Detects 50 DNS lookups in 60 seconds from the same IP source. Both the time window and the number of lookups are configurable.	Provides no operational security value, as it just finds all DNS activity from client machines.
DoS Logged and Service Shutdown	By default, detects 2 DoS log events to a host, followed by a service on the Windows host shutting down within 5 minutes.	Replaced during consolidation of the various Web DoS rules.
Excessive Denied Inbound Traffic Followed by Permit by Source IP	Detects when 10 or more consecutive inbound network communication denies are followed by a permit from the same source IP address within a five-minute time period.	Provides little or no enterprise security value.
Failed logins Followed By Successful Login and a Password Change	Detects five or more failed logins for a user, followed by a successful login and a password change within a five-minute time period.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
File Transfer Using Non Standard Port	Detects when a file is transferred using a non-standard TCP destination port. Both the list of file extensions and list of standard TCP ports are configurable.	Does not solve a correlation-required use case, and adds to confusion and noise in customer environments.
HTTP Get Flood	Detects when successful HTTP connections send GET requests, which result in at least 1,000 packets sent to the same destination IP address within 60 seconds.	Replaced during consolidation of the various Web DoS rules.
HTTP Outbound Traffic to Multiple Destinations From Single Source	HTTP outbound traffic to 50 unique destination IPs from a single source IP within 60 seconds. Outbound traffic is defined as that which does not have a private reserved address.	Provides little or no enterprise security value.
Insider Threat Mass Audit Clearing	Detects when the same user logs on multiple times to multiple Windows machines, then clears the audit log on each machine within a configurable time frame.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
jRAT Download	Detects an internal network session download of jRAT.	Replaced by an application rule.
krbtgt Account Modified on Domain Controller	Detects modification to the krbtgt account on a domain controller.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
Lateral Movement Suspected Windows	Detects within a Windows environment a sequence of events in which an executable is copied to a file share, the executable is used to create a new service and the service is started within 5 minutes. The sequence of events may indicate an attacker moving laterally by executing a backdoor on a victim machine from an already compromised system.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
Logins across multiple servers	Detects logins from the same user across 3 or more separate servers within 5 minutes.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
Logins by same user to multiple servers	Identifies a user that attempts to log in to multiple hosts within one minute.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1).

		The new rule is supported in RSA NetWitness version 11.1 and higher.
Low Orbit on Cannon DoS Tool Download	Detects Low Orbit Ion Cannon DoS tool download from sourceforge.net.	The rule logic was ineffective, and the threat is no longer relevant.
Malware Domains feed hit followed by an ECAT alert	Triggered when the same host registers a hit against a Malware Domains feed and then generates an ECAT alert.	The feed upon which this rule depended has been discontinued.
Multi Service Connection Attempts Log	Detects multiple failed connection attempts from a single source to multiple common service ports within a five-minute time period.	Functionality overlaps with Port Scanning rules.
Multi Service Connection Attempts Pckt	Detects an IP address that attempts to connect to four or more of the listed ports on a destination within a five minute period. This indicates service reconnaissance on the destination IP.	Functionality overlaps with Port Scanning rules.
Multiple Account Lockouts From Same or Different Users	Detects multiple account lockouts reported for a single or multiple users within a time period of 10 minutes.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
Multiple Failed logins Followed By Successful Login	Multiple failed logons followed by a successful logon by the same user within 5 minutes.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
Multiple Failed Logins from Multiple Diff Sources to Same Dest	Detects log events that contain multiple failed logins from a single user from multiple different sources to same destination within 3600 seconds.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
Multiple Failed Logins from Multiple Users to Same Destination	Detects log events that contain multiple failed logins from multiple different users from the same source to the same destination in 180 seconds.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
Multiple Failed Logins from Same User Originating from Different Countries	Multiple failed logins from the same user, originating from multiple different countries. IP addresses are used to indicate that the attempted logins originated from different countries.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
Multiple Failed Privilege Escalations by Same User	Fires after a user account fails privilege escalation 3 times within a 5 minute period. Both the time window and the number of privilege escalation failures are configurable.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
Multiple Login Failures by Administrators to Domain Controller	This rule is triggered when a user enters Administrator credentials to log on to a domain controller and fails multiple times within a certain number of minutes. The default is 3 failures within 3 minutes.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
Multiple Login Failures by Guest to Domain Controller	This rule is triggered when a user enters Guest credentials to log on to a domain controller and fails multiple times within a certain number of minutes. The default is 3 failures within 3 minutes.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
Multiple Logs from a MsgID Set with Same SourceIP and DestinationIP	Detects when multiple log events from the specified list of message IDs with Same Source IP and Destination IP take place in the specified time period.	Provided little or no security value.

Multiple Successful Logins from Multiple Diff Src to Diff Dest	Detects log events that contain multiple successful logins from a single user from multiple different sources to multiple different destinations in 180 seconds.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
Multiple Successful Logins from Multiple Diff Src to Same Dest	Detects log events that contain multiple successful logins from a single user from multiple different sources to same destination in 3600 seconds.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
Multiple Unique Logs from Msg ID Set with Same Source IP and Destination IP	Multiple unique log events from group of message IDs (each log has to have a unique message ID among the specified set of IDs) with same source IP and destination IP that take place within given time window.	This rule provides no operational security value.
Non DNS Traffic on UDP Port 53 Containing Executable	Detects non-DNS traffic over TCP or UDP destination port 53 containing an executable. You can configure the list of executable file extensions and ports for DNS traffic.	Replaced by an application rule.
Non HTTP Traffic on TCP Port 80 Containing Executable	Detects non-HTTP traffic on TCP destination port 80 containing an executable. You can configure the list of executable file extensions and TCP port for HTTP traffic.	Replaced by an application rule.
Non SMTP Traffic on TCP Port 25 Containing Executable	Detects non-SMTP traffic on TCP destination port 25 containing an executable file. You can configure the list of executable file extensions and TCP port for SMTP traffic.	Replaced by an application rule.
Port Scan Horizontal Log	Alerts when log events contain 200 unique IP destinations with the same source IP and destination port within 60 seconds, indicating a horizontal port scan. Both the time window and number of unique IP destinations are configurable.	Replaced by Port Scan Horizontal, which merges the Logs rule and the Packets rule.
Port Scan Horizontal Packet	Alerts when network sessions contain 40 unique IP destinations with the same source IP and destination port within 180 seconds, indicating a horizontal port scan. The time window, destination port range and number of unique IP destinations are configurable.	Replaced by Port Scan Horizontal, which merges the Logs rule and the Packets rule.
Port Scan Messages Log	Detects log events that contain 20 messages indicating a port scan within 300 seconds from the same source IP.	Replaced by Horizontal Port Scan rule.
Privilege Escalation Detected	Detects an escalation in privileges for a Windows user or group.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
Privilege User Account Password Change	Detects a logged modification of an administrative account password.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
RIG Decimal IP Campaign	This rule indicates the presence of decimal-IP (i.e. an IP address expressed in decimal format) redirectors in use with RIG Exploit Kit (EK) operations.	Functionality was added to RIG Exploit Kit ESA rule, making this rule unnecessary.

Suspicious Privileged User Access Activity	Triggers when a privileged user account is observed logging into 3 or more unique hosts within 5 minutes.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
System Configuration Changes By a Non Administrative User	Detects modification of a system configuration by a non-administrative user.	Not working as designed.
UDP DoS Tool Use Detection	Detects when at least 100 UDP packets per second are sent from the same source IP address to the same destination IP address.	Replaced during consolidation of the various Web DoS rules.
User Account Created Logged in and Deleted Within an Hour	Detects when a user account is created, and then gets deleted within one hour.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
User added to admin group same user login OR same user su sudo	Detects when a user is upgraded to one of the admin groups (custom list of groups) and the same user logs in or performs a sudo operation.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
User added to Administrative Group + SIGHUP detected within 5 minutes	Detects when a user is upgraded to one of the admin groups (custom list of groups) and a SIGHUP is detected on a service on the same device.ip. This rule is specific to Unix devices.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
WebSploit Tool Download	Detects WebSploit tool download from sourceforge.net.	The rule no longer triggers, as the content it was referencing was retired.
Windows Suspicious Admin Activity: Audit Log Cleared	Detects when a user account is created, added to the Administrators group, and the audit logs are cleared within a five-minute period.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
Windows Suspicious Admin Activity: Firewall Service Stopped	Detects when a user account is created, added to the Administrators group, and the firewall is stopped within a five-minute time period.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
Windows Suspicious Admin Activity: Network Share Created	Detects when a user account is created, added to the Administrators group, and a network share is created within a five-minute time period.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.
Windows Suspicious Admin Activity: Shared Object Accessed	Detects a when a Windows user account is created, a shared object is accessed, and the account is deleted within a five-minute time period.	Replaced with a rule of the same name due to integration of a Context Hub list into the rule logic (new feature for version 11.1). The new rule is supported in RSA NetWitness version 11.1 and higher.

RSA Feeds

The following feeds are being discontinued because RSA Research is no longer supporting them. Instead, they are focused on emerging, sophisticated threats around the globe.

Name	Description	Notes

Arin Net Destination ASNs	Identifies the country in which a specific destination ASN resides, as identified by Arin Net.	MaxMind is no longer supporting this content.
Arin Net Source ASNs	Identifies the country in which a specific source ASN resides, as identified by Arin Net.	MaxMind is no longer supporting this content.
ASN Info Pack	Provides additional meta information for AS Networks, Organization names, Country codes, and country names as sourced from MaxMind and ArinNet.	MaxMind is no longer supporting this content.
File Upload Sites	Creates meta when hits to known online file storage sites are detected.	Due to the distributed and constantly evolving infrastructure of cloud services, it is not beneficial to track all systems by their FQDNs.
High Risk File	Detects high-risk file types by extension.	Prone to false positives due to attackers mimicking legitimate download behaviors.
Hijacked	Hijacked IP list source from **www.bluetack.co.uk**.	Outdated list of IP addresses that is are longer publicly updated and provided to the community.
hunting	The Hunting feed can be deployed to provide a baseline response framework that allows analysts to investigate collections with a modular approach to response.	Replaced by the Investigation Feed.
IDefense Threat Indicators Domains	Verisign idefense security intelligence services gives information security executives access to accurate and actionable cyber-intelligence related to vulnerabilities, malicious code, and global threats 24 hours a day, 7 days a week.	This feed is no longer available nor updated, due to an expired partnership with IDefense.
Malware Domains	List of domains commonly associated with malware sourced from **www.malwaredomains.com**.	RSA no longer licenses this feed.
MaxMind ASN	List of AS Networks associated with IP address ranges regularly updated and sourced from MaxMind.	MaxMind is no longer supporting this content.
NetWitness Fraud Intelligence powered by Verisign	Verisign idefense security intelligence services gives information security executives access to accurate and actionable cyber-intelligence related to vulnerabilities, malicious code, and global threats 24 hours a day, 7 days a week.	This feed has been incorporated into the existing RSA Research feed.
Palevo Tracker Domains	Palevo Tracker offers three different blocklists, used to block the access to well known Palevo botnet Command & Control botnets.	The Palevo tracker feeds are no longer being updated by the community; the threat has diminished, and this content provides no operational security value.
Palevo Tracker IPs		
RSA FirstWatch APT Attachments	Contains attachments that are known to be associated with APTs.	Due to rapid evolution of attacker TTP, these indicators were too varied to provide much operational value.
RSA FirstWatch Criminal Socks User IPs	Contains IPs that have been observed using criminal anonymization services.	The malware that this project leveraged has since gone dormant, and the data it provided has outlived its usefulness.
RSA FirstWatch Criminal VPN Entry Domains	Contains domains that represent known VPN entry nodes for criminal anonymization services.	The feeds associated with VPN IPs (RSA FirstWatch Criminal VPN Entry/Exit IPs) provide more value than the domain related ones. The only time the domain feeds would fire are on DNS lookup vs. the actual VPN traffic.
RSA FirstWatch Criminal VPN Exit Domains	Contains domains that represent known VPN exit nodes for criminal anonymization services.	
RSA FirstWatch Exploit Domains	Contains Domains that are known to be associated with malware delivery.	Duplication of effort and value of the RSA Fraud Action Domain feed.
RSA FirstWatch Exploit IPs	Contains IPs that are known to be associated with malware delivery.	
RSA FirstWatch IP Reputation	Contains IP that are known to be compromised.	

RSA FirstWatch Insider Threat Domains	Contains domains known to be associated with insider threats.	Due to the distributed nature of cloud services and the number of new file sharing services that continue to appear this feed provided more noise than analytical value.
RSA FirstWatch Insider Threat IPs	Contains IPs known to be associated with insider threats.	
SpyEye Domain Tracker	SpyEye domain tracker is a list of spyeye (also known as zbot, prg, wsnpoem, gorhax and kneber) command & control domain names. SpyEye tracker has tracked more than 2,800 malicious spyeye c&c servers. SpyEye is spread mainly through drive-by downloads and phishing schemes.	The SpyEye tracker feeds are no longer being updated by the community; the threat has diminished, and this content provides no operational security value.
SpyEye Tracker		
SRI Attackers	Contains malicious ip addresses sourced from **www.sri.com**.	A change in licensing prevents RSA from redistributing the data feed
SSH IP Blacklist	The SSH blacklist, contains IP addresses of hosts which tried to bruteforce into any of currently 10 hosts (all running OpenBSD, FreeBSD or Linux) using the SSH protocol. The hosts are located in Germany, the United States, and Australia, and are setup to report and log those attempts to a central database.	The website that hosts this material has posted a notice that they will no longer be providing updates.
Tor Nodes	Contains IPs that are listed as active nodes in the Tor network.	This list contains all Tor nodes, and because other services are often hosted on the same IP address as the Tor node, this leads to false positives.
url-shortening-services.zip	Detects hits to known URL-shortening services.	Due to their adoption across social media and within organizations, this feed has limited analytic value due to increased noise.
WikiLeaks Domains	Wikileaks domain mirrors.	Wikileaks has adopted a TOR as a method of distribution instead of a wide network of WWW mirrors.
Zeus Domain Tracker	Zeus domain tracker is a list of zeus (also known as **zbot**, **prg**, **wsnpoem**, **gorhax** and **kneber**) command & control domain names. Zeus tracker has tracked more than 2,800 malicious zeus C&C servers. Zeus is spread mainly through drive-by downloads and phishing schemes.	The ZeuS feed is sporadically updated by the community, and the updates are prone to false positives because updates have shifted towards compromised sites rather than core ZeuS infrastructure.
Zeus Tracker	Zeus tracker is a list of IP addresses of zeus servers (hosts) around the world.	

RSA Lua Parsers

Name	Description	Notes
AIM_lua	OSCAR protocol used by AIM (AOL Instant Messenger) and ICQ, and AIM-express web client.	As of December 15, 2017, AOL Instant Messenger products and services have been shut down and no longer work.
BITS	Identifies Microsoft BITS Protocol.	BITS was added to HTTP_lua, making the standalone BITS parser redundant. BITS parsing in HTTP_lua is also much more complete than it was in the standalone parser.

RSA Flex Parsers

All Flex parsers are discontinued. For replacements, see **Mapping of Flex to Lua Parsers**.

RSA System Parsers

Name	Description	Notes
AIM	AOL Instant Messenger	These native parsers were removed from Decoders because they no longer provide value.
LotusNotes	Lotus Notes Mail Protocol	
MSN	Microsoft Instant Messenger	
Net2Phone	Net2Phone Protocol	
SAMETIME	Lotus Notes Sametime Instant Messenger Protocol	
WEBMAIL	Webmail via HTTP	
YCHAT	Yahoo! Web Chat Protocol	
YMSG	Yahoo Messenger	

RSA Security Analytics List

One list is being discontinued: **admin users**. This is a duplicate of the **Administrative Users** list.

RSA NetWitness Reports

The following reports and report templates are discontinued.

Name	Description	Notes
Access to Compliance Data - Detail	Compliance Report Template- Access to Compliance Data - Detail	The individual compliance reports have been superseded by the “Core Compliance” reports. The new reports allow customers to look in fewer places for the same information.
Access to Compliance Data - Top 25	Compliance Report Template- Access to Compliance Data - Top 25	
Account Management	Compliance Report Template- Account Management	
Accounts Created	Compliance Report Template- Accounts Created	
Accounts Deleted	Compliance Report Template- Accounts Deleted	
Accounts Disabled	Compliance Report Template- Accounts Disabled	
Accounts Modified	Compliance Report Template- Accounts Modified	
Admin Access to Compliance Systems - Detail	Compliance Report Template- Admin Access to Compliance Systems - Detail	
Admin Access to Compliance Systems - Top 25	Compliance Report Template- Admin Access to Compliance Systems - Top 25	
Antivirus Signature Update	Compliance Report Template- Antivirus Signature Update	
Botnet Activity	Use this report to get the various Botnets activity within the network.	A more comprehensive Malware Activity report has replaced this and includes results for botnets as well as crimeware, apt, command and control and more.
Change in Audit Settings	Compliance Report Template- Change in Audit Settings	The individual compliance reports have been superseded by the “Core Compliance” reports. The new reports allow customers to look in fewer places for the same information.
Encryption Failures	Compliance Report Template- Encryption Failures	
Escalation of Privileges - Detail	Compliance Report Template- Escalation of Privileges - Detail	

Escalation of Privileges - Top 25	Compliance Report Template- Escalation of Privileges - Top 25	
Failed Escalation of Privileges - Detail	Compliance Report Template- Failed Escalation of Privileges - Detail	
Failed Escalation of Privileges - Top 25	Compliance Report Template- Failed Escalation of Privileges - Top 25	
Failed Remote Access - Detail	Compliance Report Template- Failed Remote Access - Detail	
Failed Remote Access - Top 25	Compliance Report Template- Failed Remote Access - Top 25	
Firewall Configuration Changes	Compliance Report Template- Firewall Configuration Changes	
Firmware Changes Wireless Devices	Compliance Report Template- Firmware Changes Wireless Devices	
Group Management	Compliance Report Template- Group Management	
Key Generation and Changes	Compliance Report Template- Key Generation and Changes	
Logon Failures - Detail	Compliance Report Template- Logon Failures - Detail	
Logon Failures - Top 25	Compliance Report Template- Logon Failures - Top 25	
NetWitness Incident Management	The report displays a summary and detailed view of the incidents and alerts generated using NetWitness Respond.	This report has been renamed to **NetWitness Respond**.
Password Change on Privileged Account	Displays instances of privileged account passwords being changed. It includes a list that may be customized to include the privileged user accounts in your network environment. To use the report, create and populate the report list with user accounts as noted in the dependencies.	Prone to excessive noise depending on environment configuration. It's also a direct mapping of functionality that exists in the product.
Password Changes - Detail	Compliance Report Template- Password Changes - Detail	The individual compliance reports have been superseded by the "Core Compliance" reports. The new reports allow customers to look in fewer places for the same information.
Password Changes - Top 25	Compliance Report Template- Password Changes - Top 25	
Router Configuration Changes	Compliance Report Template- Router Configuration Changes	
Successful Remote Access - Detail	Compliance Report Template- Successful Remote Access - Detail	
Successful Remote Access - Top 25	Compliance Report Template- Successful Remote Access - Top 25	
Successful Use of Encryption	Compliance Report Template- Successful Use of Encryption	
System Clock Synchronization	Compliance Report Template- System Clock Synchronization	
Scanning Activity	Reports vertical and horizontal port scans for both IPv4 and IPv6 addresses across network sessions.	Dependent upon discontinued Correlation Rules.
Security Analytics Administration Report	Gives a summary and detail view of the NetWitness Administration - Audit events report.	Renamed to **NetWitness Administration Report**
Top 10 Risk Suspicious	Summarizes Top 10 Risk Suspicious by Source, Destination and Session Size.	Duplicate of the **All Risk Suspicious** report.
Top 10 Risk Warning	Summarizes Top 10 Risk Warning by Source, Destination and Session Size.	Duplicate of the **All Risk Warning** report.

User Access Revoked	Compliance Report Template- User Access Revoked	The individual compliance reports have been superseded by the “Core Compliance” reports. The new reports allow customers to look in fewer places for the same information.
User Access to Compliance Systems - Detail	Compliance Report Template- User Access to Compliance Systems - Detail	
User Access To Compliance Systems - Top 25	Compliance Report Template- User Access To Compliance Systems - Top 25	
User Session Terminated - Top 25	Compliance Report Template- User Session Terminated - Top 25	

RSA NetWitness Rules

Name	Details	Notes
Botnet Activity	Fires when any one or more of 128 different Botnets have been detected.	A more comprehensive Malware Activity rule has replaced this.
IPv4 Horizontal Port Scans	Fires when either IPv4 Horizontal Port Scan 5, IPv4 Potential Web Sweep 10 or IPv4 Potential DB Server Sweep 5 has been generated within the report date range across network sessions.	Dependent upon discontinued Correlation Rules.
IPv4 Vertical Port Scans	Fires when either IPv4 Vertical TCP Port Scan 5 or IPv4 Vertical UDP Port Scan 5 has been generated within the report date range across network sessions.	Dependent upon discontinued Correlation Rules.
IPv6 Horizontal Port Scans	Fires when either IPv6 Horizontal Port Scan 5, IPv6 Potential Web Sweep 10 or IPv6 Potential DB Server Sweep 5 has been generated within the report date range across network sessions.	Dependent upon discontinued Correlation Rules.
IPv6 Vertical Port Scans	Fires when either IPv6 Vertical TCP Port Scan 5 or IPv6 Vertical UDP Port Scan has been generated within the report date range across network sessions.	Dependent upon discontinued Correlation Rules.
Large Outbound Connections to 3rd Party Sites	Summarizes sessions that have a session size of 5 MB or greater. These sessions are indicative of a large file transfer from RFC 1918 to 3rd party Storage sites, identified by the File Upload Sites feed.	Relies on File Upload Sites feed that is being deprecated.
NetWitness Incident Management - Alert Details	This rule provides a detailed list of the alerts generated using NetWitness Respond.	This rule has been renamed to **NetWitness Respond - Alert Details**.
NetWitness Incident Management - Alert Summary	The rule displays a summary view of the alerts generated using NetWitness Respond.	This rule has been renamed to **NetWitness Respond - Alert Summary**.
NetWitness Incident Management - Incident Summary	This rule displays a summary view of the incidents generated using NetWitness Respond.	This rule has been renamed to **NetWitness Respond - Incident Summary**.
Security Analytics Administration - Events Classification Summary	Provides a summary of event types and sub types with its count and the last time the event occurred.	Renamed to replace "Security Analytics" with "NetWitness" to reflect the name change of the product suite.
Security Analytics Administration - Hosts and Events Summary	Provides a summary of all the events that occurred under each host along with its count.	Renamed to replace "Security Analytics" with "NetWitness" to reflect the name change of the product suite.
Security Analytics Administration - User Activity by Source IP Summary	Provides a break-down of the user activity for each user along with its Source Address, Count and the last time the event occurred.	Renamed to replace "Security Analytics" with "NetWitness" to reflect the name change of the product suite.
Security Analytics Administration - User Authentication Attempt Details	Provides a detailed list of authentication (success and failures) with Source IP address, Hostname, time and so on.	Renamed to replace "Security Analytics" with "NetWitness" to reflect the name change of the product suite.
Security Analytics Administration - User Authentication Failure Details	Provides a detailed list of authentication failures with Hostname, Source IP address, time and so on.	Renamed to replace "Security Analytics" with "NetWitness" to reflect the name change of the product suite.
Security Analytics Administration - User Authentication Failure Reason Summary	Provides a break-down of the reasons for authentication failures for each user along with its occurrence count and last time the event occurred.	Renamed to replace "Security Analytics" with "NetWitness" to reflect the name change of the product suite.
Top 10 Risk Suspicious by Destination IP	Aggregates sessions by **risk.suspicious** and displays the top ten results by **ip.dst** in descending order.	Duplicate functionality to the **All Risk Suspicious** rule.
Top 10 Risk Suspicious by Source IP	Aggregates sessions by **risk.suspicious** and displays the top ten results by **ip.dst** in descending order.	
Top 10 Risk Suspicious by Session Size	Aggregates sessions by **risk.suspicious** and displays the top ten results by session size in descending order.	

Top 10 Risk Warning by Destination IP	Aggregates sessions by **risk.warning** and displays the top ten results by **ip.dst** in descending order.	Duplicate functionality to the **All Risk Warning** rule.
Top 10 Risk Warning by Source IP	Aggregates sessions by **risk.warning** and displays the top ten results by **ip.dst** in descending order.	
Top 10 Risk Warning by Session Size	Aggregates sessions by **risk.warning** and displays the top ten results by session size in descending order.	
Windows Automated Explicit Logon	Indicative of possible lateral movement on Windows systems	Dependent upon discontinued Correlation Rules.

RSA Correlation Rules (Discontinued)

All Correlation Rules have been discontinued, due to them having little investigative value and limited correlation options.

Display Name	Description
IPV4 Potential DB Server Sweep	Detects when Packet or Log Decoder receives sessions from a unique, source IPV4 address that connects to five or more unique destination IPV4 addresses on destination ports 1433 (MSSQL), 1521 (Oracle), and 3306 (mysql) within one minute. This rule should be deployed on Concentrator, as it examines both Log and Packet metadata. The rule uses **ip.dstport** for logs and **tcp.dstport** for packets. For IP addresses, the rule examines **ip.src** and **ip.dst** metadata.
IPV6 Potential DB Server Sweep	Detects when Packet or Log Decoder receives sessions from a unique source IPV6 address that connects to five or more unique destination IPV6 addresses on destination ports 1433 (MSSQL), 1521 (Oracle), and 3306 (mysql) within one minute. This rule should be deployed on Concentrator, as it examines both Log and Packet metadata. The rule uses **ip.dstport** for logs and **tcp.dstport** for packets. For IP addresses, the rule examines **ipv6.src** and **ipv6.dst** metadata.
IPv4 Horizontal Port Scan 5	Detects when a unique IPv4 source address communicates with five or more unique IP destination addresses within one minute, across network sessions.
IPv6 Horizontal Port Scan 5	Detects when a unique IPv6 source address communicates with five or more unique IP destination addresses, within one minute across network sessions.
IPv4 Vertical TCP Port Scan 5	Detects when a unique combination of IPv4 source and destination addresses communicate over five or more unique TCP ports within one minute, across network sessions.
IPv4 Vertical UDP Port Scan 5	Detects when a unique combination of IPv4 source and destination addresses communicate over five or more unique UDP ports within one minute, across network sessions.
IPv6 Vertical TCP Port Scan 5	Detects when a unique combination of IPv6 source and destination addresses communicate over five or more unique TCP ports within one minute across network sessions.
IPv6 Vertical UDP Port Scan 5	Detects when a unique combination of IPv6 source and destination addresses communicate over five or more unique UDP ports within one minute, across network sessions.
IPv4 Potential Web Sweep 10	Detects when a unique IPv4 source address communicates over ten or more unique IP destination addresses over port 80, within one minute.
IPv6 Potential Web Sweep 10	Detects when a unique IPv6 source address communicates over ten or more unique IP destination addresses over port 80, within one minute.
IPv4 Bulk Data Transfer 20 Mb	Detects events when the amount of data transferred between Source-Destination IPV4 pairs is more than 20 MB of data, within 5 minutes.

IPV6 Bulk Data Transfer 20 Mb	Detects events when the amount of data transferred between Source-Destination IPV6 pairs is more than 20 MB of data, within 5 minutes.
IPv4 Bulk Data Transfer 50 Mb	Detects events when the amount of data transferred between Source-Destination IPV4 pairs is more than 50 MB of data, within 5 minutes.
IPV6 Bulk Data Transfer 50 Mb	Detects events when the amount of data transferred between Source-Destination IPV6 pairs is more than 50 MB of data, within 5 minutes.
Windows Automated Explicit Logon	Detects automated logons attempted to the same destination using explicit credentials. This rule only applies when an atypical process, **0x4** (system), **cscript.exe** (to Remote) or **svchost.exe** (to Remote), is reported within the event. In order to import and deploy the rule, the custom meta key **event.computer** must be added.