Use cases – RSA Netwitness Suite

Category	Sub Category	Use Case	Log Source	RSA Supported
Business Use Cases				
Access/Authentication	Identity Management	Monitor for use of disabled usernames	Active Directory , Databases, Applications, Web Proxy, HR data	Integrating Windows AD and monitoring for event ID's for User login attempts and correlating with Status of user in AD
	Password Guessing	Possible successful brute force attack detected	All event sources	OOB
		Possible successful brute force attack detected on critical devices/servers	Critical devices and servers	Criticality context to be incorporated using Feed integration from secops EM
	Enterprise Services Access Management	Increase in failed domain admin account logins detected	All event sources	User activity Trend Dashboard monitoring for User login activity
	Perimeter & Network Security	Increase in failed remote login attempts detected	windows, Unix, Firewalls, IDS & IPS, Access controls & VPN.	User activity Trend Dashboard monitoring for User login activity
	Enterprise Services Access Management	Unusual number of failed/successful vendor/default user login attempts	All Network, Host, Server & Security devices	User activity Trend Dashboard monitoring/Alerting for Privilege User login activity
	Perimeter & Network Security	Password change on a known privileged account detected	All windows, Unix, VPN, Database, Firewall & FIM.	Provilege account monitoring Alert/Dasboard/Chart
Audit Trail	System Health	Tampering of system audit logs detected	All event sources	Integration of SA Audit logs with decoder for monitoring user audit activity
Policy violation	Physical Security	Employee absenteeism – Badge sharing detection	Physical Access logs & AD logs	Integration of HID Access Card DB and AD last login details with Feeds from Leave Management system to monitor employee movements and access requests
		attendance policy violation	VPN, My Time Application & Physical Access logs	Time from Access Control time tracker and matching with HID Access intime and out time for employee work hours policy monitoring
	Enterprise Services Access Management	Password Sharing – Policy access violation	All event sources	Same User login from different machines or locations in a specific time

				or any such attempts being made more than once
	Enterprise Windows account Management	Unauthorized use of service account	Windows OS	Monitoring service accounts monitoring
		RDP attempts from local admin account	Windows OS	Monitoring remote Desktop port usage and identifying any such attempts by providing Dashboard or report for such admin activities
	Network Security	Server access from unauthorized IP Address	Firewall logs	
		Internet access by unauthorized server	Internet Firewall, Proxy	List of such users to be provided for Web activity monitoring
		Policy Violation - Internet access from authorized server	Internet Firewall, Proxy	Proxy policy violation reorts user wise
		Reverse Proxy bypass - Application accesed externally	Internet Firewalls	Any access requests to Web servers or applications not published to external internet
		Insecure application access - non https	Firewall logs	Non standard port using known service, like FTP over http protocol
Operational / Functional	System Health	Device Stopped Sending logs	Proposed solution logs	Health and wellness built in system
		Log source stopped sending logs after reboot	All event sources	Health and wellness built in system
		Disk Array capacity approaching threshold	Proposed solution logs	Health and wellness built in system
		Possible system instability state detected	All event sources	Health and wellness built in system
		System shutdown	Proposed solution logs	Health and wellness built in system
		Backup and recovery: failed	Proposed solution logs	Health and wellness built in system
		Backup and recovery: cancelled	Proposed solution logs	Health and wellness built in system
	Perimeter & Network Security	Network performance degradation detected	All router, switch & firewalls.	Nusing netflows we can having session monitoring to detect any deviations in usage
	System metrics	Windows service state change	Windows OS	Monitoring windows Event logs
		Successful or Failed Installation/	Proposed solution logs	Enable windows logging for auditing with file audits

		Updating any package		and folder audits in addition to Application, Security and system logs
		EPS Warning – EPS approaching limit	Proposed solution logs	On Screen Nag screens and notifications can be configured for such monitoring
		Log Source added/deleted	Proposed solution logs	Built in system to notify on any new integrations
		User added to "remote user group" AD group	Active Directory	AD user activity log monitoring
		User added as part of "domain administrator" & "local administrator" group	Active Directory	AD user activity log monitoring
		New windows service installation	Windows OS	Windows system and appliaction security logs
		User added to VPN administrative group	Active Directory	VPN service and activity log monitoring
Integrity	Integrity Monitoring	Changes to databases holding customer data by unauthorized users	Database System Logs	DB Fine Grain Auditing
	Perimeter & Network Security	Configuration change on network & security device intercepted	IDS, IPS, Firewall & VPN.	Configuration Changes on assets listed to be monitored for any deviations
		Host checker configuration changed on VPN device	VPN device logs	Monitor any changes on VPN device Host checker service on clients through Windows application logs or host checker logs
Privilege Access	Enterprise Services Access Management	Elevation of account privilege followed by restoration of previous state within a period of 24 hrs.	All event sources	Privilege user monitoring
		Revocation of user privileges detected	All windows, Unix, Firewall, IDS & Network Configuration Management Solution.	Changes in privilege access
Usage Activity	Data transfer	Large files transfer to 3rd Party Sites	All Firewall & Web proxy	Using netflows and logs correlation session size through FTP uploads or any such transfers on other protocols to be monitored

	Perimeter & Network Security	Monitoring over ports not permitted by policy on Internet-facing firewalls, non-compliant traffic activity.	All Internet facing Firewalls	Using Watchlist of such ports we can monitor traffic of such users and report or alert on same
		Use of clear-text confidential information detected	IDS, IPS, Web logs, Mail server logs, Database, Unix & Windows	Using Network session Clear text confidential information can be detected
		Excessive inbound denied connections	Firewall logs	Trend report on session and flow including firewall logs to identify what content and date is being transmitted in sessions
		Increase in file transfer activity using instant messaging detected	All IDS, IPS, Router & Firewall.	Monitor IM traffic for any kind of file sharing activities
		Active syn flood attack detected by network & security devices	This rule works with all IDS, IPS, and Firewall	OOB
		Possible arp poisoning or spoofing activity detected	All IDS, IPS, Firewalls, Switch & Unix	OOB
		Remote data harvesting	VPN device logs	VPN user activity monitoring
		High Volume of TCP Resets	All firewalls	OOB and customizable
Threat Intelligence	Perimeter & Network Security	Communication between internal hosts and known malware distribution site	All IDS, IPS, Firewalls, web proxy & Threat Intelligence feed	OOB. Monitoring using threat intelligence feeds
		A connection from a server with a known spam sending host	All IDS, IPS, Firewalls & Threat Intelligence feed	OOB. Monitoring using threat intelligence feeds
Malicious Activity Monitoring	Perimeter & Network Security	Increase in peer to peer traffic detected	IDS, IPS, Firewall & VPN	Monitor Peer to peer protocols, networks and hosts
	Network Security	Unintended download of computer software from internet	Web Proxy solution	Using packets any downloads can be monitored and reported out for any such anomalies
		Successful backdoor attack	All IDS, IPS, Firewalls & Antivirus	Based on the analyis and fusing threat intelligence feeds backdoor activity can be tracked. Also any such patterns can be

				customized
		Worm propagation in the internal network	All IDS, IPS & Firewalls	Similar worm alerts triggered over Lan /WAN using netflows can be monitored using lateral movements
		SQL injection attack detection	Web server logs	OOB pattern available
		Attack exploiting Microsoft Directory service vulnerability detected	All IDS/IPS	MDS monitoring, with IPS signature trigger and corrleating with Vulnerability CVE ID for correlation
		Streaming Media detected	All Firewall ,Web proxy & IDS/IPS	Using packet and netflow such downloading activities can be monitored
		Possible intruder trying to gain unauthorized access to network	All IDS, IPS, Firewalls, VPN & Threat Intelligence feed	Using Threat feeds we can detect any communication to known malwares or spam hosts including blackisted IP's
		Successful Connections after Denied Attempts from same external source	All firewalls & IDS /IPS	OOB can be customized
		Aggressive database scan	All firewalls	OOB monitoring on DB ports
		Virus deletions failed on system	Antivirus System	Monitoring Antivirus Client side scan Actions
		System getting infected by same virus	Antivirus System	Report on Virus actions and alerts by using lookup and add function against unique Virusname and Hostname/IP
		High number of Denial of Service (DoS) attack detected	All IDS, IPS & firewall.	OOB
		Vulnerability correlation alerts	Vulnerability Data, IPS/IDS	IPS alarms to be correlated with Vulnerability scan results for achieveing vulnerabiliuty based correlations
		Malicious Activity - VPN access	Active Directory	Any activity / actions notified by system evaluated by Threat feeds on VPN System
		Malicious Activity - Deviation of network	Network Monitoring tool	Trend report on bandwidth utilization over a period of

		utilization of resources		time or against a threshold
Processes/services	Active Directory	Active directory schema change	Window Security Event Logs	AD change logs
		Active directory policy modified	Window Security Event Logs	GPO policy change notifications
	Microsoft Exchange	Increase in the number of non-delivery report messages collected from Microsoft Exchange	Window Event Logs	Monitor the Mail notifications and report on NDR status for each source and recipient malboxes
	System Health	Patch & update failures	Patch Management Server	Use patch management server logs to see patch status and any Actions based on patch deployment jobs
Attack Life Cycle based Use Cases				
Initial Recon	Port Scan from outside	Horizontal port Scan	Internet Facing Firewalls	OOB
		Horizontal port scan on well known vulnerable ports	Internet Facing Firewalls	OOB
		Horizontal port scan on critical assets (PDMZ)	Internet Facing Firewalls	OOB
		Horizontal port scan on existing vulnerable ports on critical assets (PDMZ)	Internet Facing Firewalls, Vulnerability Management Reports	OOB
		Vertical Port Scan	Internet Facing Firewalls	OOB
		Vertical port scan on well known vulnerable ports	Internet Facing Firewalls	OOB
		Vertical port scan on critical assets (PDMZ)	Internet Facing Firewalls	OOB
		Vertical port scan on existing vulnerable ports on critical assets (PDMZ)	Internet Facing Firewalls	OOB
		IDS/IPS port scan on well known vulnerable ports	Internet IPS/IDS	OOB
		IDS/IPS port scan on critical assets (PDMZ)	Internet IPS/IDS	OOB
		IDS/IPS port scan on well known	Internet IPS/IDS	OOB

		vulnerable ports		
	Vulnerability Scan from outside	Vulnerability Scan	Internet - Firewalls and IDS/IPS	OOB
		Vulnerability Scan on critical assets	Internet - Firewalls and IDS/IPS, Server HIDS/HIPS	Using Criticality context to identify the Port scan on vulnerable ports
	Communication traffic that is from an unusual geo location source.	Communication traffic observed from an unusual geo location source.	Internet - Firewalls and IPS/IDS, VPN Devices	Can use data from FW, IPS & IDS and use GeoIP enrichment to identify any communication to or from unusual Geo's
	Communication traffic that is known to be from bad or blacklisted source host addresses.	Communication traffic observed from bad or blacklisted source host addresses.	Firewalls, IPS/IDS, VPN	Can use data from FW, IPS & IDS and use Threat intelligence to identify any communication to or from unusual Geo's
	Slow Scans	Slow Horizontal Scan	Internet - Firewalls and IDS/IPS	Using logs and Packets with threat intelligence to detect any beaconing traffic
		Slow Vertical Scan	Internet - Firewalls and IDS/IPS	Using logs and Packets with threat intelligence to detect any beaconing traffic
		Slow Box Scan (Combination of horizontal and Vertical Scan)	Internet - Firewalls and IDS/IPS	Using logs and Packets with threat intelligence to detect any beaconing traffic
Initial Compromise	Spear phishing	Malware downloaded	AV	Using Packet capture to analyse the downloaded file for malicious content
	Weaponized document	Malware downloaded	AV	Using Packet capture to analyse the downloaded file for malicious content
	Watering Hole attack	Malware downloaded	proxy	Using Packet capture to analyse the downloaded file for malicious content
	System Exploit	C&C communication attempts	Proxy/Firewall Threat feed	Using Threat intelligence identify known CnC communication attempts
Establish Foothold	install backdoor malware	Malware has been installed	AV	The installation of package can be identified by system logs but the actual Endpoint forensics can be achieved from Endpoint solution ECAT. Without endpoint forensics we cannot confirm the installed software is malicious or not unless

				Threat feeds already have the data
	create command and control infrastructure	C&C communication denied by firewall/proxy.	Firewalls/Proxy - Threat Feed	Using Threat intelligence identify known CnC communication attempts
		Successful C&C communication	Firewalls/Proxy - Threat Feed	Using Threat intelligence identify known CnC communication attempts
	install keyloggers	Unauthorized software installed - Key loggers.	AV	The installation of package can be identified by system logs but the actual Endpoint forensics can be achieved from Endpoint solution ECAT. Without endpoint forensics we cannot confirm the installed software is malicious or not unless Threat feeds already have the data
	Dump password hashes	Privilege escalation alerts	Windows OS	Any privilege escalations monitored for changes
		Unauthorized software installed - password hash dumping tool.	AV / EDR	The installation of package can be identified by system logs but the actual Endpoint forensics can be achieved from Endpoint solution ECAT. Without endpoint forensics we cannot confirm the installed software is malicious or not unless Threat feeds already have the data
	Rootkits	Successful Privilege escalation alerts	Windows OS	The installation of package can be identified by system logs but the actual Endpoint forensics can be achieved from Endpoint solution ECAT. Without endpoint forensics we cannot confirm the installed software is malicious or not unless Threat feeds already have the data

		Rootkits installed	AV	The installation of package can be identified by system logs but the actual Endpoint forensics can be achieved from Endpoint solution ECAT. Without endpoint forensics we cannot confirm the installed software is malicious or not unless Threat feeds already have the data
Escalate Privileges	Retrieve password hashes	Password hash transport detected	NIDS/NIPS(Signature to capture NTLM password hash in clear text)	Using Parser for content analysis packet capture can detect the cleartext transport of hashes or other data
	traffic sniffing	Network adaptor going in promiscus mode (white list for apps like Symantec HIDS)	Windows/UnixOS	OOB
	keylogging	Unauthorized software installed - Key loggers.	AV	The installation of package can be identified by system logs but the actual Endpoint forensics can be achieved from Endpoint solution ECAT. Without endpoint forensics we cannot confirm the installed software is malicious or not unless Threat feeds already have the data
Internal Recon	Gather system information, network information, hardware info	Inside - Horizontal port Scan	Firewalls, IPS/IDS	OOB
		Inside - Horizontal port scan on well known vulnerable ports		OOB
		Inside - Horizontal port scan on critical assets (PDMZ)		OOB
		Inside - Horizontal port scan on existing vulnerable ports on critical assets (PDMZ)		OOB
		Inside - Vertical Port Scan		OOB
		Inside - Vertical port scan on well known		OOB

		vulnerable ports		
		Inside - Vertical port scan on critical assets		OOB
		Inside - Vertical port scan on existing vulnerable ports on critical assets		OOB
		Inside - HIDS/HIPS port scan on well known vulnerable ports		OOB
		Inside - HIDS/HIPS port scan on critical assets		OOB
		Inside - HIDS/HIPS port scan on well known vulnerable ports		OOB
		Inside - Vulnerability Scan		OOB
		Inside - Vulnerability Scan on critical assets		OOB
		Inside - ARP broadcast Detected		Using Netflow or Packet capture
	Looks at files and documents, explore file shares	Work station to work station communication	Windows OS, SEPM	Internal communication monitoring user to user VLAN

		User behavior anomaly detected		The solution proposed is based around the RSA Security Analytics platform. This can collect logs as well as network packet data to give much greater visibility into the risk that the organization may be exposed to. By combining not just the log data collected from the devices within the infrastructure but also identifying anomalies within the network traffic as well as using 3rd party feeds from industry authoritative sources it is possible to identify if your organization is under attack, exposed to the new and emerging threats as well as identifying if the organization has already been compromised. This can be implemented in a phased approach, initially focusing on log data, eventually moving towards a more pervasive view with the implementation of packet capture.At the log collection level RSA can use techniques such as base lining of events across devices as well as advanced correlation so that an organization can be alerted to an event that falls outside of normal day to day activity. This can help provide insight into anomalies and areas of concern that the security analyst may need to be aware of. These can be as simple as multiple failed logins across a number of different devices, to more complicated scenarios such as unusual activity seen in web logs from a certain username combined with

				escalation of privileges from that user and then failed an successful logins to resources holding sensitive data that may in some circumstances indicate a breach of the network.In terms of packet data there are a number of techniques and applications available to help an organization get deep visibility into the health of the network.Metadata is assigned to the packets that are collected to make the data much easier to search through as well as much more humanly readable. The data that is collected can also be referenced against live feeds from various authoritative sources to further enrich your data and provide intelligence around the latest threats as well as blacklisted IPs, known bad websites etc. This enables automated alerting and reporting against the threats that the organization is exposed to. These alerts and reports are presented on a dashboard. The alerts and reports can be customized to provide intelligence relevant to the organization.Another component of the solution is the malware analysis tool that will evaluate the threat posed by any executable seen within the organization. This is done using a variety of techniques such as static file analysis, sandboxing, next generation analysis, referencing it against community information as

				well as allowing the organization to see if their antivirus or in fact any antivirus vendor would have flagged this as malicious. This tool is especially useful when looking for 0 day malware that signatures alone would not have spotted.
Move Laterally	Use of psexec, scheduled tasks (at command), WMI	capture schedule tasks with taskname "At<number>g" event ID 602,4698.	windows OS	Using Event ID's can be achieved from windows sytem event logs
		psexec:- monitor event log service install 4697 with service name psexesvc	windows OS	Using Event ID's can be achieved from windows sytem event logs
	Use of valid credentials over SMB or RDP	Anomaly detection using event logs	User behavior analysis	Internal communication monitoring for user behaviour changes like multiple login fails and succeffull logins frequently
		Desktop to Desktop communication observed	SEPM/HIDS (personal firewall)	Internal communication monitoring for user behaviour changes like multiple login fails and succeffull logins frequently

Maintain Presence	Backdoor malware	Malware has been installed	Application whitelisting, AV, Anti Malware solution	The installation of package can be identified by system logs but the actual Endpoint forensics can be achieved from Endpoint solution ECAT. Without endpoint forensics we cannot confirm the installed software is malicious or not unless Threat feeds already have the data
	VPN access	Detailed analysis of host check failure alerts	VPN device	Trend report on Host checker status of VPN clients
		Anomaly detection for VPN users (user profiling)	User behavior analysis	Baselining of VPN users access requests to monitor any behavioural changes or deviations
		Executable detected in http/https traffic	NIDS/NIPS	Using Packet capture files detected as non-standard service over standard protocol
	password encoded zip or RAR files	Password encoded Outbound file transfer detected	NIDS, proxy DLP	Using Packet Capture identify zip and rara files.
	FTP	Detected File transfer over FTP (white list for FTP allowed Ips)	Firewalls	Whitelisting of key listed FTP sites
	smb	Connection established over port SMB ports (139, 445) towards known bad IP	Firewalls - threat feed	Using Threat intelligence and SMB ports to identify threats and SMB traffic within internal network