ID	Category	Description	Yes / No / Partial	Score	Comments
1.00	SIEM ABILITIES (Security information and event management)				
1.01	Inputs & Access Controls	What types of inputs/devices can the tool accept? e.g. NetFlow, Syslog, SNMP, Windows, Linux, Applications(AV and Websense) How does the system collect data from proprietary or legacy event sources? How do you provide software based deployments with centralized management? How does the tool leverage Windows Unified Connector? How does the system recognize privileged users?			
1.02	Normalization/Categorization	How do you pre-normalize the data before its written to a database? How many dimensions are categorized? (i.e. device type, behavior, outcome, etc.)			
1.03	Proactive alerting and monitoring	Besides reactive monitoring what can the tool tell us about network activity in real time? 1) How do you provide geo-IP lookup, port to application mapping, model mapping, and custom field mapping pre-correlation? 2) Global threats and how are we prepared? 3) What services or capabilities does the vendor provide for incident analysis or investigation?			
1.04	Transactional Assurance/Audit & Accountability	How do you guarantee event integrity, confidentiality, and availability? (i.e. how does the system monitor and alert when original event source stops sending log data)			
1.05	Full Text Search	How does your tool index both deconstruct and structure data? How many events per second can the tool return search results?			
1.06	Centralized Log Storage	How many TB's of log data can be stored locally? How does it use classification of data to segregate security, compliance, IT operations, etc?			
1.07	Linear Scalability	How many events per second can a single appliance scale to? How do you search across multiple peers without first having to centralize and index data store?			
1.08	Threat Evaluation	How do you correlate against past activities related to the target or reference the targets current vulnerabilities? How does your tool handle rule creation?			
1.09	Notification and Workflow	What is your process framework for integrating security monitoring and investigations into existing workflow procedures? What type of visual accounting do you provide for showing the complete attack life cycle of a threat?			
1.10	Threat/Incident Response	How do you trigger scripts or execute integration with third party solutions to quarantine or block nefarious activity in real-time?			
1.11	Reputation Correlation	How does your tool detect threats early? (zero day attacks) How does your tool monitor and protect the reputation of a company's website, assets, and partners not found in a bad reputation list?			
1.12	Compliance Automation	How does your tool provide real time alerts and reports for compliance regulations such as NIST?			
1.13	Pattern Detection	How does your tool detect low-and-slow attacks that are not easily recognized by pre-existing thresholds?			
2.00	APPLICATION PROTECTION				
2.01	Vulnerability Scans	How do you provide Static binary and byte code analysis reviews of compiled code, libraries and third party plug-in's rather than source code? Do you reverse engineer software for binary analysis? How do you provide dynamic scans for applications in production?			
2.02	Integration	How do you integrate with IPS, WAF, or SIEM? Do you support netflow, syslog?			
2.03	Automated Tool	What automated tools do you use for scans and how do you scrub out false positives?			
3.00	REPORTING				
3.01	Top X Reports	Please provide information on this solution's ability to create "Top X" reports.			
3.02	Drill Down	Does this solution have the ability to drill into actual log sources that generated reporting?			

ID	Category	Description	Yes / No / Partial	Score	Comments
3.03	Accuracy	How do you verify the solution is providing accurate reporting that is reliable and runs in a timely fashion			
3.04	Report Saving	Does this solution have the ability to create and save reports in a flexible/free form manner (such as search x device for y string/IP/name/port etc.)			
3.05	Executive Reporting	Does the solution provide executive reports that are meaningful and do not need to be explained			
3.06	Timing	Are metrics available for time to generate statistics or reports based on the number of log entries?			
3.07	Samples	Are sample reports available for review?			
4.00	COMPLIANCE				
4.01	Vulnerability Scanning	Can this solution provide internal and external vulnerability scanning?			
4.02	NIST	How many security controls from NIST 800-53/82 does this solution address and which ones?			
4.03	PCI Experience	What experience do you have around PCI. How would you rate your overall competency in this space?			
4.04	Reporting	What are your reporting and technical abilities surrounding NIST & PCI?			
5.00	CAPACITY				
5.01	Logs	How long is log information available for analysis (13 months should be adequate)? Are older logs archived? If so, what is the process and time requirements to access them?			
6.00	EASE OF USE				
6.01	GUI	Does the tool have a GUI that is simple, fast, and easy to use?			
6.02	Web Based	Does the tool run in a web browser without having to load a client?			
6.03	Tool Complexity	Is the tool intuitive to use? Would other team members not familiar with network security be able to log into the tool and use it with little training?			
#REF!	Basic Tool Use	What is the approximate time required to learn basic GUI interface and develop custom reports?			
7.00	SYSTEM SECURITY				
7.01	Protecting Data (systems and communications)	How would you protect ARRC data from unauthorized access? 1) From outside intrusion? 2) Firewalls in use? 3) Proactive intrusion detection? 4) How are you alerted? 5) Proactive intrusion testing? 6) Internal threats?			
7.02	Physical Protections	What physical protections are in place to secure data center servers?			
7.03	Monitoring	What type of security monitoring do you do?			
7.04	Log Review	What type of security log reviews do you do?			
7.05	Anti-Virus	Describe your anti-virus/spyware/malware systems			
8.00	SYSTEM STABILITY AND SUPPORT				
8.01	Maintenance & Support Model	Describe your maintenance and support model			
8.02	SLA Details	What is your typical SLA response time?			
8.03	System Response Times	What are the system response times you support?			

ID	Category	Description	Yes / No / Partial	Score	Comments
8.04	**Support Response Times**	What are the support response times (24/7, 8/5) you support?			
8.05	**Escalation**	What is your escalation path?			
8.06	**Online / Offline**	What online / offline support options do you offer for your system?			
8.07	**System Releases**	How many releases of the software have occurred? (version X.x)			
8.08	**System Release Communications**	How are they communicated?			
8.09	**System Release Implementations**	How are they implemented?			
8.10	**3 - 5 year Product Strategy**	Please describe your product strategy looking out 3 - 5 years			
8.11	**Max # of Concurrent Users**	What is the maximum # of simultaneous users?			
8.12	**Patch Strategy**	Describe your patching strategy			
8.13	**Warranty**	Describe your solution warranty coverage: 1) Duration? 2) What's covered? 3) Other useful information?			
9.00	**SYSTEM STABILITY AND SUPPORT**				
9.01	**Uptime Assurance**	Describe how your system strategy provides maximum uptime (24/7) for ARRC businesses			
9.02	**Downtime Communications**	How do you communicate downtime (planned and unplanned) and maintenance windows?			
9.03	**Proactive Monitoring**	How do you proactively monitor your system for unplanned downtime?			
9.04	**Required Downtime**	Is there any "required" system downtime?			
9.05	**HW/SW Maintenance Protocol**	Outline how hardware and software maintenance will be carried out without loss of service			
9.06	**Backup / Recover Measures**	What data backup and recovery measures do you have in place?			
9.07	**DR Strategy**	Describe your disaster recovery strategy			
9.08	**Issue/Bug Reporting**	What is your process for reporting bugs, issues and services requests?			
9.09	**Recent Uptime**	What has your system uptime been over the last 24 months?			
10.00	**DEVELOPMENT STRATEGY**				
10.01	**SDLC & Change Control**	Describe your SDLC and change control procedures?			
10.02	**QA / Testing Risk Assessment**	Describe your software QA/testing processes?			
10.03	**Update / Release Schedule**	Do you have a standard update release schedule?			
10.04	**Technical Documentation**	Describe your technical systems documentation? Where is it located? 1) Installation Guide 2) Systems Guide 3) Maintenance Guide 4) Etc.			