Requirement Category	ID	Requirement Topic	Requirement Description	Response (for Custom Development indicate impacts for support and updates)	Current Capability or Configurable Item	Future Release	Custom Development	Not Available	Indicate Module or Product Offering Associated to Requirement and Pricing.
Technology Features	A-1	Collection/Aggregation /Normalization (CAN)	*Indicate whether your solution supports the following CAN capabilities and describe your specific capability in that area:*						
Technology Features	A-2	Collection/Aggregation /Normalization (CAN)	o Net flow data / data sources						
Technology Features	A-3	Collection/Aggregation /Normalization (CAN)	o Identity data / data sources						
Technology Features	A-4	Collection/Aggregation /Normalization (CAN)	o Application-specific data / data sources						
Technology Features	A-5	Collection/Aggregation /Normalization (CAN)	o Database-specific data / data sources						
Technology Features	A-6	Collection/Aggregation /Normalization (CAN)	o Configuration data / data sources						
Technology Features	A-7	Collection/Aggregation /Normalization (CAN)	o File integrity data / data sources						
Technology Features	A-8	Collection/Aggregation /Normalization (CAN)	o Non log infrastructure information						
Technology Features	A-9	Collection/Aggregation /Normalization (CAN)	o Full packet capture						
Technology Features	A-10	Collection/Aggregation /Normalization (CAN)	o IPv6 source support						
Technology Features	A-11	Collection/Aggregation /Normalization (CAN)	o Cloud environment information						
Technology Features	C-1	Correlation	*Indicate whether your solution supports the following correlation capabilities and describe your specific capability in that area:*						
Technology Features	C-2	Correlation	o Correlation according to canned policies.						
Technology Features	C-3	Correlation	o Correlation according to user-defined policies.						
Technology Features	C-4	Correlation	o Correlation according to adaptive/heuristic policies.						
Technology Features	C-5	Correlation	o Correlation according to behavior-based.						
Technology Features	C-6	Correlation	o Correlation according to Big Data analytics or machine learning functionality						
Technology Features	C-7	Correlation	o Indicate whether correlations are performed on solution itself or performed by an integrated separate platform.						
Technology Features	C-8	Correlation	o Indicate whether correlations can include host/asset criticality information to enable prioritization						
Technology Features	C-9	Correlation	o Indicate whether there is scoring based on correlation patterns						
Technology Features	D-1	Forensic Analysis	*Indicate whether your solution supports the following forensic analysis capabilities and describe your specific capability in that area:*						
Technology Features	D-2	Forensic Analysis	o Custom querying.						
Technology Features	D-3	Forensic Analysis	o Data drill-down.						
Technology Features	D-4	Forensic Analysis	o Data export of relevant forensic analysis data with data preservation.						
Technology Features	D-5	Forensic Analysis	o Parsing of IAM and application data						
Technology Features	D-6	Forensic Analysis	o Support for ad hoc queries for incident investigation with ability to query both normalized data and original data collected						
Technology Features	D-7	Forensic Analysis	o Event session reconstruction to present the raw data is an understandable way						
Technology Features	E-1	Data Management and Security	*Describe the security capabilities inherent within your solution. Address the following:*						
Technology Features	E-2	Data Management and Security	o Role-based access control to the solution as a whole.						
Technology Features	E-3	Data Management and Security	o Role-based access control to specific capabilities, functions and/or data repositories within the solution.						
Technology Features	E-4	Data Management and Security	o Encryption of all data within remote collectors/aggregators/analyzers, where such devices are part of your solution.						
Technology Features	E-5	Data Management and Security	o Encryption of all data within local collectors/aggregators/analyzers.						

Technology Features	E-6	Data Management and Security	o Encryption of all communications between collection point and storage repositories.
Technology Features	E-7	Data Management and Security	o Single sign-on with Active Directory and/or Azure Active Directory.
Technology Features	E-8	Data Management and Security	*Describe the data retention capabilities inherent within your solution. Address the following:*
Technology Features	E-9	Data Management and Security	o Indicate whether your solution allows for hierarchical storage management such that active data can be retained for real-time investigation and historical data can be retained for as required investigation.
Technology Features	E-10	Data Management and Security	o Where the capability exists, indicate the volume of active data that can be stored within the system (expressed in correlated events) for real-time access.
Technology Features	E-11	Data Management and Security	o Where the capability exists, indicate the volume of historical data that can be stored within the system (expressed in correlated events) for as required access.
Technology Features	E-12	Data Management and Security	o Indicate the ability, if it exists, to provide for extended storage of log files beyond capability of SIEM appliance (LAN, NAS, SAN, etc.).
Technology Features	E-13	Data Management and Security	o Indicate the ability, if it exits, for the creation of automated policies for moving data logs to secondary storage.
Technology Features	E-14	Data Management and Security	o Indicate the ability, if it exists, to query against both the primary and secondary storage of the SIEM.
Technology Features	E-15	Data Management and Security	o Indicate the data compression ratio.
Technology Features	E-16	Data Management and Security	o Indicate the capability, if it exists, to perform data access monitoring of the SIEM itself (integration with database audit and protection products, DLP, or FIM).
Technology Features	F-1	Threat Intelligence Feed	*Describe the integration capabilities of your solution and a separated threat intelligence feed platform, either provided by your threat intelligence-based platform or a third-party platform, inherent within your solution.*
Technology Features	F-2	Threat Intelligence Feed	*List what threat intelligence feeds your SIEM product can integrate with.*
Technology Features	F-3	Threat Intelligence Feed	*Describe the updating schedule of the related threat intelligence feeds and how this can be customized by the user.*
Technology Features	F-4	Threat Intelligence Feed	*Describe what formats and uses an integrated threat intelligence feed supports:*
Technology Features	F-5	Threat Intelligence Feed	o Update watch lists
Technology Features	F-6	Threat Intelligence Feed	o Update reporting
Technology Features	F-7	Threat Intelligence Feed	o Update alerting
Technology Features	F-8	Threat Intelligence Feed	o Update filtering
Technology Features	F-9	Threat Intelligence Feed	o Update rules
Technology Features	F-10	Threat Intelligence Feed	o Update querying
Technology Features	G-1	Incident Management	*Describe your solutions ability to detect incidents or breaches and provide management capabilities to enable a streamlined process from detection to remediation of an incident.*
Technology Features	G-2	Incident Management	○ Indicate the ability to generate an incident and triage this incident into prioritized rankings in order to provide the most important areas of work for administrators.
Technology Features	G-3	Incident Management	○ Indicate the ability to integrate with enterprise workflow systems.
Technology Features	G-4	Incident Management	○ Indicate the ability to integrate with early breach detection solutions in order to gain better incident detection.
Technology Features	H-1	Remediation	*Describe your solution's inherent ability to provide bi-directional communication with network and security devices to enable remediation in face of defined incidents.*
Technology Features	H-2	Remediation	○ Indicate where the capabilities exist for the creation of remediation activities defined by administrators.

Technology Features	H-3	Remediation	o Indicate where the capabilities exist for the implementation of approval of workflow with hierarchy of approval when remediating activities.
Technology Features	H-4	Remediation	o Indicate the ability to generate automated remediation policies.
Technology Features	H-5	Remediation	o Indicate the ability to integrate with security technologies and non-security solutions for remediation actions.
Technology Features	I-1	Big Data Analytics	*Describe the ability for the solution to integrate with purpose-built big data repositories.*
Technology Features	I-2	Big Data Analytics	*Describe the ability for the solution to integrate with purpose built big data security analytics.*
Technology Features	J-1	Alarming and Alerting	*Describe the process by which the command console can be configured to issue alarms and alerts. Detail the different alarming/alerting mechanisms that can be configured and the manner in which those alarming/alerting mechanisms are configured.*
Technology Features	J-2	Alarming and Alerting	*Indicate whether your solution can integrate with third-party ticketing and workflow systems, and where integration is possible, indicate with which platforms your solution integrates, and describe the integration process.*
Technology Features	K-1	Auditing and Reporting	*Describe the auditing and reporting capabilities for captured logs. Address whether standard report templates exist, whether they must be constructed, or whether the system supports ad hoc reporting only. Where standard templates exist, indicate what types of reports they represent and in all cases indicate what types of information can be presented in reports. Specify if specific compliances mandates can be reported against.*
Technology Features	K-2	Auditing and Reporting	*Indicate whether your solution can integrate with third-party reporting solutions, and where integration is possible. Indicate with which platforms your solution integrates and describe the integration process.*
Architecture	L-1	Deployment	*Indicate which of the following deployment modes your solution supports. Indicate if your solution works optimally in one mode versus another:*
Architecture	L-2	Deployment	o Fully centralized (central collection, central analysis & alerting).
Architecture	L-3	Deployment	o Partially distributed (distributed collection, central analysis & alerting).
Architecture	L-4	Deployment	o Fully distributed (distributed collection, distributed analysis & alerting).
Architecture	L-5	Deployment	o Hybrid (central and distributed collection, central and distributed analysis & reporting).
Architecture	L-6	Deployment	o Hosted (off-premise collection, analysis, and alerting).
Architecture	L-7	Deployment	*Indicate which of the following platforms your solution uses for delivery. Indicate if your solution works optimally on one platform versus another:*
Architecture	L-8	Deployment	o Appliance-based (appliances for collection and analysis & alerting).
Architecture	L-9	Deployment	o Software-based (licensed software for collection and analysis & alerting).
Architecture	L-10	Deployment	o Virtual machine-based (virtual appliances for collection and analysis & alerting).
Architecture	L-11	Deployment	o Hybrid (any combination of the three platforms).
Architecture	L-12	Deployment	o If your solution is appliance-based, indicate any internal redundancy/resiliency capabilities (e.g. internally redundant hardware) and external redundancy/resiliency capabilities (e.g. failover devices) that are part of, or can be made part of, your solution.
Architecture	L-13	Deployment	o If your solution is software-based, indicate whether licensing is periodic or perpetual, and whether it is deployment, seat, or named-user based.
Architecture	L-14	Deployment	*Indicate if your solution can be deployed as:*
Architecture	L-15	Deployment	o A hierarchy of SIEM servers as tiers of systems that aggregate, correlate and store data.

Architecture	L-16	Deployment	o As a segmented server functions so that specialized servers are dedicated to collection, correlation, storage, reporting and display.
Architecture	L-17	Deployment	o A combination of a hierarchy and segmented servers.
Architecture	L-18	Deployment	*Indicate whether your solution is offered as a Managed Security Service, and if so, the terms and costs associated with the services provided. As well indicate any third-party Managed Security Service Provider (MSSP) Integration capabilities.*
Architecture	L-19	Deployment	*Please list any MSSP you have formal partnerships with*
Architecture	L-20	Deployment	*Please list any MSSP you do not have a formal partnership with, but can offer a managed security service of your SIEM solutions.*
Architecture	M-1	Required Infrastructure/Licenses	*Based on the provided enterprise description, indicate how many collectors/aggregators/analyzers and what type (if your solution is based on point capability solutions) will be required for optimal levels of network protection; provide justification for that number of devices/licenses. Where multiple devices/licenses are required, indicate which model is necessary in each specific case and provide justification for that model of device/license.*
Architecture	M-2	Required Infrastructure/Licenses	*If you are a networking infrastructure vendor, include any embedded or native sensors within your supported infrastructure that are used / can be used for log collection.*
Architecture	N-1	Required Supporting Devices	*Indicate whether your solution requires a separate and dedicated management device/license. If a separate and dedicated management device/license is not required, but one is available, indicate the management enhancements provided by this device/license.*
Architecture	N-2	Required Supporting Devices	*Indicate whether your solution requires a separate and dedicated reporting device/license. If a separate and dedicated reporting device/license is not required, but one is available, indicate the reporting enhancements provided by this device/license.*
Architecture	O-1	System Scalability	*Indicate the degree to which your solution(s) can be scaled. Indicate both the degree to which an individual collector/aggregator/analyzer can be scaled (that is, have its performance increased/enhanced without being replaced), as well as the degree to which the system as a whole can be scaled (that is, the number of individual collectors/aggregators/analyzers that can be effectively managed via the management interface).*
Architecture	P-1	Other System Integration	*Indicate which type(s) (if any) of the following enterprise solutions your solution(s) can integrate with:*
Architecture	P-2	Other System Integration	o Security solutions:
Architecture	P-3	Other System Integration	Perimeter anti-malware solutions
Architecture	P-4	Other System Integration	Firewall/UTM solutions
Architecture	P-5	Other System Integration	Intrusion detection/prevention solutions
Architecture	P-6	Other System Integration	o Network devices:
Architecture	P-7	Other System Integration	Core switches
Architecture	P-8	Other System Integration	Distribution switches
Architecture	P-9	Other System Integration	Routers
Architecture	P-10	Other System Integration	o Servers:
Architecture	P-11	Other System Integration	Application servers
Architecture	P-12	Other System Integration	Database servers
Architecture	P-13	Other System Integration	Web servers
Architecture	P-14	Other System Integration	Communications servers (email, unified communications, etc.)

Support	Q-1	Customer Support	*Do you provide toll-free customer support 24 hours a day, seven days a week? Please specify all paid and unpaid support options.*
Support	R-1	Geographic and Language Support	*Do you provide support in specify location (e.g. North America, EMEA, APAC, and Latin America) and specify language (e.g. English, Spanish, Mandarin)?*
Support	S-1	User Manuals	*Do you provide a complete set of user manuals (either in hardcopy, softcopy, or via a searchable software interface) for all software applications to document and explain system features and functions?*
Support	T-1	Training	*Describe the type of training provided to administrators. Specify whether training is available direct from the vendor or provided through a partner.*
Support	V-1	Software Updates	*Do you provide future software releases and updates to all applications as part of regular software maintenance fees?*
Support	V-2	Software Updates	*For on premise solutions, please specify the software update process, typical time between releases and end-of-life schedules.*
Support	V-3	Software Updates	*For off-premise and appliance solutions, please specify the standard update cycle.*
Support	W-1	Technical Documentation	*Do you provide technical documentation for support staff including system overviews, design, flowcharts, and file layouts?*
Support	X-1	Performance monitoring (if applicable)	*Do you provide remote software monitoring to identify anomalies and provide automatic upgrades?*
Support	Y-1	Implementation & Configuration	*Describe the process by which collector/aggregator/analyzer devices/licenses for your solution are deployed. Include any tasks that must be performed on systems or devices already deployed (e.g. network configuration and third-party integration).*
Support	Y-2	Implementation & Configuration	*Describe the process by which the management devices/licenses for your solution are deployed. Include any tasks that must be performed on systems or devices already deployed (such as network configuration and third-party solution integration).*
Support	Y-3	Implementation & Configuration	*Describe the process by which the reporting devices/licenses for your solution are deployed. Include any tasks that must be performed on systems or devices already deployed (such as network configuration and third-party solution integration).*
Support	Y-4	Implementation & Configuration	*Describe the process by which the command console(s) for your solution(s) is initially configured. Include the creation of administrative accounts, key databases, audit and reporting functions, policy creation, etc.*
Support	Z-1	On-going Operations	*Describe the process by which the initial configuration of your solution is performed. Include the implementation of any signature database(s), the creation of any rules, and the configuration of any and all settings required for optimal operations.*
Support	Z-2	On-going Operations	*Describe the process by which the initial configuration of your solution is updated and maintained. Include the update of any signature database(s), the update and/or modification of any rules, etc.*
Support	Z-3	On-going Operations	*Describe the processes by which the command console can be backed up. Address whether the back-up process in any way compromises operations and/or security.*