No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
1. Monitoring and Control				
No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
1.1	The solution must support file integrity monitoring.	Functional		
1.2	The solution must provide a risk rating or vulnerability rating for each asset and user.	Functional		
1.3	The solution must maintain an accurate asset inventory.	Functional		
1.4	The solution must provide log collection and retention.	Functional		
1.4.a	The solution includes 13 months of log retention at the quoted price.	Functional		
1.5	The solution must include threat hunting.	Functional		
1.5.a	Proactive, vendor initiated threat hunting	Functional		
1.5.b	On-demand, customer requested threat hunting	Functional		
1.5.c	On-demand, customer initiated threat hunting	Functional		
1.6	The solution must support the discovery of exposed attack surfaces.	Functional		
1.6.a	Memory monitoring	Functional		
1.6.b	User account monitoring (login attempts)	Functional		
1.6.c	Network traffic behavioral analysis	Functional		
1.7	The solution must identify gaps in coverage for one or more frameworks (NIST CSF, MITRE ATT&CK, etc.).	Functional		
1.8	The solution must provide discovery and monitoring of medical, OT, and IoT devices.	Functional		
1.9	The solution must provide monitoring of BYOD and rogue devices.	Functional		
1.10	The solution must provide device isolation and remediation assistance.	Functional		
			Section 1 Score	Perfect Score is: 398
2. Prevention and Detection				
No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
2.1	Does the solution have email filtering capabilities? If so, please describe the filtering provided by the solution.	Functional		

2.2	Does the solution have web filtering capabilities? If so, please describe the filtering provided by the solution.	Functional		
2.3	Does the solution have endpoint detection and response (EDR) capabilities? If so, please describe.	Functional		
2.4	Does the solution have network detection and response (NDR) capabilities? If so, please describe.	Functional		
2.5	Does the solution provide extended detection and response (XDR) capabilities? If so, please describe.	Functional		
2.6	Does the solution provide intrusion prevention capabilities? If so, please describe.	Functional		
2.7	Does the solution have Active Directory protection capabilities? If so, please describe.	Functional		
2.8	Does the solution have data protection capabilities? If so, please describe.	Functional		
2.9	Does the solution provide endpoint antivirus protection? If so, please describe.	Functional		
2.10	The solution must identify malicious files and prevent them from execution, including viruses, trojans, ransomware, spyware, cryptominers and any other malware type.	Functional		
2.10.a	Signature-based malware protection	Functional		
2.10.b	Static analysis (for example: machine learning)	Functional		
2.10.c	Dynamic analysis (for example: real time sandbox)	Functional		
2.10.d	Cyber threat intelligence	Functional		
2.10.e	Virus Total	Functional		
2.11	The solution must identify malicious behavior of executed files, running processes, registry modifications, and memory access, and terminate them at runtime, or raise an alert (fileless, macros, PowerShell, WMI etc.).	Functional		
2.11.a	Memory access monitoring	Functional		
2.11.b	Process behavioral analysis (heuristics)	Functional		
2.11.c	High similarity (for example: fuzzy hashing)	Functional		
2.11.d	Threat intelligence	Functional		

2.12	The solution must support the creation of rules to exclude specific addresses, imp ranges, domains, and URLs.	Functional		
2.13	The solution must identify and block privilege escalation attacks.	Functional		
2.14	The solution must identify and block reconnaissance attacks (scanning).	Functional		
2.15	The solution must identify, and block credential theft attempts form either memory (credential dump, brute force, etc.) or network traffic (ARP spoofing, DNS responder, etc.).	Functional		
2.15.a	Memory monitoring	Functional		
2.15.b	User account monitoring (login attempts)	Functional		
2.15.c	Network traffic behavioral analysis	Functional		
2.16	The solution must identify and block/alert on lateral movement (SMB relay, pass the hash, etc.).	Functional		
2.16.a	Network traffic monitoring	Functional		
2.16.b	Deception via fake nodes	Functional		
2.16.c	Deception via fake user accounts	Functional		
2.16.d	Deception via fake network connections	Functional		
2.17	The solution must identify user account malicious behavior.	Functional		
2.17.a	User activity policies (policy violation)	Functional		
2.17.b	User account baseline (behavioral analysis, anomaly detection, etc.)	Functional		
2.17.c	User account compromise (deep web monitoring)	Functional		
2.18	The solution must identify malicious interaction with data files.	Functional		
2.19	The solution must identify data exfiltration via legitimate protocols (DNS tunneling, icmp tunneling, https, etc.)	Functional		
2.19.a	Network traffic monitoring	Functional		
2.19.b	File access monitoring	Functional		
2.20	The solution must identify and block usage of common attack tools (Metasploit, Empire, Cobalt etc.).	Functional		
2.21	The solution must have a mechanism to prevent access and manipulation by unauthorized users and processes (tamper protection).	Functional		
			Section 1 Score	Perfect Score is: 730

3. Investigation and Response

No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
3.1	Does the solution have management portal access based on user role and requirements (RBAC)?	Functional		
3.2	Does the solution provide guidance based on the MITRE ATT&CK framework?	Functional		
3.3	Does the solution provide detailed remediation advice?	Functional		
3.4	Does the solution provide remediation services?	Non-Functional		
3.5	Does the solution provide incident response services at no additional cost?	Non-Functional		
3.6	Does the solution provide service level agreements (SLAs) and compensation for failing to meet SLAs? Describe.	Non-Functional		
3.7	Does the solution provide a financial guarantee in the event of a breach?	Non-Functional		
			Section 3 Score	Perfect Score is: 126

4. Infrastructure

No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
4.1	Does the solution integrate with Ivanti for automatic service desk ticket generation?	Functional		
4.2	Does the solution integrate with any other common IT tools or software? If so, please describe.	Functional		
4.3	Does the solution run without the need for any special appliances or hardware?	Functional		
4.4	Does the solution provide full capabilities without the need of any EDR or agents from a third party?	Functional		
4.5	Does the solution provide full capabilities without the need for any special software (such as Java)?	Functional		
4.6	Does the solution rely on any threat intelligence feed from a third party?	Functional		
4.7	Does the solution provide vulnerability management services?	Non-Functional		
4.8	Does the solution provide patch management services?	Non-Functional		
4.8	Does the solution have a defined frequency of updates and patches? If so, please describe.	Functional		

4.9	Does the solution integrate with on-premises Active Directory?	Functional		
4.10	Does the solution integrate with ADFS?	Functional		
4.11	Does the solution integrate with SAML 2.0?	Functional		
			Section 4 Score	Perfect Score is: 130

5. Operation

No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
5.1	The solution must have co-management capabilities.	Functional		
5.2	The solution must include a dedicated, named, contact or concierge.	Functional		
5.3	The solution must have the ability to enable and disable desired types of notifications.	Functional		
5.4	The solution must have the ability to specify alert exclusions for selected objects.	Functional		
5.5	The solution must have the ability to rate the severity of security alerts.	Functional		
5.6	The solution must provide a central collection and processing of alerts in real-time.	Functional		
5.7	The solution must have the ability to block access to the program settings for end users.	Functional		
5.8	The solution must provide a central distribution of updates without need of user intervention and of restarting the endpoint or server.	Functional		
5.9	The solution must have the ability to specify a schedule for downloading updates, including the ability to disable automatic updates.	Functional		
5.10	The solution must assign a risk score to all objects within the protected environment.	Functional		
5.11	The solution must support the logging of events, alerts, and updates.	Functional		
5.12	The solution must support integration with email infrastructure to send alerts to designated staff.	Functional		
5.13	The solution must support integration with common SIEM products.	Functional		
5.14	The solution must provide standardized and customizable reports.	Functional		
5.15	The solution must provide regulatory compliance reports for HIPAA and PCI	Functional		

5.14	The solution must provide operations from two or more geographically diverse Security Operations Centers.	Functional		
			Section 5 Score	Perfect Score is: 286

6. Extended Capabilities

No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
6.1	• 24x7 threat hunting to detect and contain threats before they disrupt your operations or cause supply chain disruptions.	Non-Functional		
6.2	• Customizable compliance reporting to assure regulatory compliance and for supply chain due diligence purposes.	Functional		
6.3	• User & Entity Behavior Analytics (UEBA) helped determine and account for system’s normal behavior pattern, and identify anomalies.	Functional		
6.4	• Complete security and analytics provided for the firm’s large enterprise networks.	Functional		
6.5	• 24x7 Security Operations Center (SOC) services supported the firm during their investigations	Non-Functional		
6.6	Mix of human, automated and autonomous response	Non-Functional		
6.7	**Threat Intelligence Questions**			
6.8	Describe in detail your standard workflow for generating and leveraging threat intelligence within your proposed services.	Non-Functional		
6.9	Describe how the overall ingestion, analysis and production of threat intelligence is performed by your service using the TIP.	Non-Functional		
6.10	Does your managed TIP ingest both industry standard formats and unstructured data? Provide examples of threat intelligence and enrichment data managed through your platform.	Non-Functional		
6.11	How would you provide access into your managed TIP?			

7. Vulnerability Management Questions

No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
7.1	Describe your detailed vulnerability scanning and notification processes for ad hoc and scheduled scans.	Non-Functional		

7.2	Describe your processes for tracking vulnerabilities to [Client] assets over time.	Functional		
7.3	Describe your solution’s asset discovery and scanning capabilities, with and without credentials on target systems. What are the limitations of credential-less scanning?	Functional		
7.4	How does your solution identify changes since a previous scan against the target system? How does your solution help to identify unexpected changes to targeted assets?	Functional		
7.5	How do you propose to work with [Client] to ensure that the platform includes or excludes our assets as appropriate?	Functional		
7.6	Describe your process for improving vulnerability management through this platform.	Functional		

8. Dashboard, Reporting and Case Management Questions

No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
8.1	Describe the standard dashboards and reports that can be generated on your solution and viewed/downloaded by authorized [Client] personnel. How do you manage requests for custom dashboards or reporting?	Non-Functional		
8.2	Describe how case management is used to support your standard incident management process including post-incident reviews/reporting.	Non-Functional		
8.3	Describe the reporting provided by your managed security services. What reports are provided and at what frequency? Do you also provide ad hoc or self-service reporting?	Non-Functional		
8.4	How will you provide reports that you generate? (e.g. via a customer portal, email, etc.)	Non-Functional		
8.5	What are the key service level parameters with respect to service management that you measure, track and report on?	Non-Functional		
	Key Requirements			
8.6	• OEM platform independent	Non-Functional		
8.7	• Scalable architecture across plants	Non-Functional		
8.8	• Robust asset management across OS, networking and embedded devices	Functional		
8.9	• Single interface across endpoints	Functional		
8.10	• Event logging, correlation and storage	Functional		
8.11	• Patch management	Functional		

8.12	• Backup and restore management	Functional		
8.13	• Strong ICS-experienced support	Functional		
8.14				
8.15	complete automated inventory,	Functional		
8.16	endpoint asset management,	Functional		
8.17	context to assets in order to facilitate and verify the use of compensating controls, and the remediation of issues after they are detected.	Functional		
8.18	1. Speed/cost/network efficiency of assessment visibility vs. network taps or calls to devices	Functional		
8.19	2. Deeper endpoint risk assessment visibility with IT-like endpoint management capabilities built safe for OT (including netflow, syslog, and machine learning)	Functional		
8.20	3. Faster time to remediation with integration risk remediation actions	Functional		
8.21	4. Lower cost OT systems management with integrated, single dashboard view	Functional		
8.22	5. Greater levels of support with in-houses dedicated team of ICS engineers, not just cyber people	Functional		

9. IT-OT Converged Functions

No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
	Practical Results / Output			
9.1	• Affordable, small footprint install	Non-Functional		
9.2	• OT-safe inventory, including embedded assets	Functional		
9.3	• OT-specific context of the asset	Functional		
9.4	• All known vulnerability or risk markers	Functional		
9.5	• Ability to remediate (patch or compensating controls)	Functional		
9.6	• OT oversight on actions	Functional		
9.7	• Contained ecosystem for reporting	Functional		
9.8	• Real-time updates	Functional		
9.9	• Scalable (no use of WMI), near real-time data	Functional		
9.10	• User-friendly, dynamic, navigable filterable dashboards to contextualize and direct remediation. Unlimited filters to see data exactly how you want.	Functional		
9.11	Identifies assets with a passive and active option	Functional		

9.12	Defending Against Industrial Ransomware	Functional		
9.13	Complementing OEM Solutions	Functional		
9.14	Illuminating IT/OT Convergence	Functional		
9.15	Passive Asset ID, Active Option	Functional		
9.16	Cyber AI Analyst: Augmenting the Human	Non-Functional		

10. Centralized Email Protections

No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
	Email Protections			
10.1	Does your Platform implement Email threat hunting?	Functional		
10.2	Does your platform delete email based on a filter language?	Functional		
10.3	Does it help threat hunt within email systems or O365?	Functional		
10.4	Can a sender be blocked globally from a central console	Functional		
10.5	Suspicious URL?	Functional		
10.6	Links to fake login page?	Functional		
10.7	Malicious attachment?	Functional		
10.8	Spoofing your CEO?	Functional		
10.9	Suspicious Email?	Functional		
10.10	Unusual but benign?	Functional		
10.11	A never-before-seen attack?	Functional		