Anti-Virus, EUBA, NextGen A/V, Endpoint/User Threat and Anomaly Detection

No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
1.1	**Next Gen A/V Requirements**			
1.2	- detect and prevent fileless malware	Functional		
1.3	- be able to scan script files on Windows\Linux\Mac	Functional		
1.4	- be able to analyze .net payloads and provide prevention against them	Functional		
1.5	- prevent known malware	Functional		
1.6	- prevent unknown malware	Functional		
1.7	- have a low false positive rate	Functional		
1.8	Prevention controls for attack surface reduction	Functional		
1.9	Prevention controls for At Rest (pre-execution) prevention and on-execution prevention on Windows\Linux\Mac	Functional		
1.10	- have ML NGAV on Windows\Linux\Mac	Functional		
1.11	- be able to scan files at rest periodically	Functional		
1.12	- be able to scan non-executable files (documents, general file formats) on Windows\Linux\Mac	Functional		
1.13	Prevention controls for memory exploitation (e.g. 0-day exploits)	Functional		
1.14	Prevention controls for behavior prevention	Functional		
1.15	Prevention for malicious downloads	Functional		
1.16	Prevent execution of selective processes	Functional		
1.17	- be able to detect lateral movement (e.g. PtH, Remote scheduled task creation, etc.)	Functional		
1.18	- support custom detection for user provided TTPs and IOCs	Functional		
1.19	- be able to detect memory-based defense evasion techniques (e.g. floating code)	Functional		
1.20	- have ability to make high fidelity detections based on loss-less large data analysis	Functional		
1.21	Prevention, detection, visibility across Windows, Mac, Linux	Functional		
1.22	- prevent an attempted copy of known signature ransomware	Functional		
1.23	prevent known ransomware from running	Functional		
1.24	Behavioral ransomware prevention for unknown ransomware strains	Functional		
1.25	- be able to analyze and correlate telemetry from the Identity and Access Management control, and enable detection and investigation of identity compromise indicators (suspicious use of identity, multiple failed authentication attempts, MFA bypass attempts etc.)	Functional		

No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
1.26	Detection of authentication brute force attempts	Functional		
1.27	Detection of authentication attempts from malicious sources by threat intel (e.g. Okta Threat-Insight)	Functional		
1.28	Detection of authentication attempts to suspicious web applications using single sign on credentials	Functional		
1.29	- be able to analyze and correlate telemetry from the email and productivity suite logs, and enable detection and investigation of email compromise indicators (phishing, account compromise, etc.)	Functional		
1.30	Detection of malicious email attachment indicators	Functional		
1.31	Detection of suspicious login attempts to an email inbox	Functional		
1.32	Detection of email forwarding to an external domain	Functional		
1.33	Detection of an identity compromise following a successful phishing	Functional		
1.34	Detection of data collection \ exfiltration by a compromised identity	Functional		
1.35	- score endpoint and non endpoint detections based on their severity \ criticality	Functional		
1.36	- be able to correlate events from multiple endpoint and non endpoint controls into a single detection	Functional		
1.37	- execute the remediation package on the endpoint	Functional		
1.38	- have the ability to isolate the machine from the network	Functional		
1.39	- have the ability to use Remote Shell	Functional		
1.40	Download a specific file from UI	Functional		
1.41	Solution provides a method to search across the entire environment with YARA rules or some similar method	Functional		
1.42	Solution provides consolidated, automatically prescribed remediation / containment procedures	Functional		
1.43	Ease of use for incident investigation workflows	Functional		
1.44	All EDR & EPP telemetry is proactively collected in near real time (no user interaction required for all data types)	Functional		
1.45	Correlation of any asset type to identity and activity (e.g. correlate endpoint telemetry across the entire enterprise)	Functional		
1.46	- list all processes, services, drivers, and auto-runs on all machines	Functional		
1.47	- show the command line execution used to run a process	Functional		
1.48	- show all network connections that a process makes	Functional		
1.49	- show DNS queries that a process makes	Functional		
1.50	- permit a search for an executable by file name or file hash	Functional		
1.51	- permit the download of an executed file off the endpoint	Functional		

No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
1.52	- execute file search and/or YARA search	Functional		
1.53	- list all ports an endpoint, or process on that endpoint listening	Functional		
1.54	- be able to provide telemetry for all connections made by all processes without limitation	Functional		
1.55	Collect a wide breadth of data types	Functional		
1.56	- provide complete access to all collected data (both alerts and telemetry) without requiring the use of any external system	Functional		
1.57	- offer long-term retention without requiring the use of any external system	Functional		
1.58	- provide complete access to data without requiring proficiency in any query language	Functional		
1.59	- enable API-driven hunting and investigation activities	Functional		
1.60	- enable Endpoint Controls	Functional		
1.61	- enable device control	Functional		
1.62	- enable firewall control	Functional		
1.63	- enable visibility into the full disk encryption status	Functional		
1.64	Solution increases efficacy of detection and prevention capabilities	Functional		
1.65	- condense alerts based on TTP to single incident	Functional		
1.66	- group all assets and identities in alerts	Functional		
1.67	- consolidate root cause data (show suspicions and evidence, show parent\grandparent and child attack tree)	Functional		
1.68	- provide rapid access to complete endpoint activity before and after specific point in time	Functional		
1.69	- provide Long term attack consolidation	Functional		
1.70	Long term timeline generation	Functional		
1.71	Consolidate recurrence of TTPs into the incident timeline	Functional		
1.72	- allow for timeline filtering within consolidated incidents	Functional		
1.73	User interface contains who\what\how\where\when in a single screen	Functional		
1.74	Complete attack tree view for every malicious and non-malicious process	Functional		
1.75	Solution console is easy to use	Functional		
1.76	Solution addresses analysts’ alert fatigue	Functional		
1.77	Solution is easy to learn and reduces onboarding overhead	Functional		
1.78	Solution's alerts and data can be accurately mapped to MITRE ATT&CK framework	Functional		
1.79	Telemetry availability in less than 2 min	Functional		
1.80	Detection alerting in less than 2 min	Functional		

No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
1.81	Solution should classify raw data based on maliciousness	Functional		
1.82	For all data collected, enrichment will be present and easy to understand. This will include benign data enrichment	Functional		
1.83	Correlation at the enterprise level	Functional		
1.84	IOC tuning capabilities (EX: hash, domain, IP) for exceptions	Functional		
1.85	Comprehensive behavioral tuning capabilities (EX: TTPs) for exceptions	Functional		
1.86	IOC tuning capabilities (EX: hash, domain, IP) for detections	Functional		
1.87	Comprehensive behavioral rule writing capabilities (EX: TTPs) for detections	Functional		
1.88	Endpoint agent registers as an AV with Windows Security Center	Functional		
1.89	Ability to discover domain-registered endpoints that are not managed	Functional		
1.90	True GDPR and Region-based deployments	Functional		
1.91	Platform has strong ROI and low TCO	Functional		
1.92	- install sensor without requiring the endpoint machine to restart	Functional		
1.93	- be able to install the sensor transparently to the end user with no visual prompts	Functional		
1.94	Solution sensor must require less than 5% of memory at all times	Functional		
1.95	- allow all software on user machine to continue to work with no impact	Functional		
1.96	- allow opening documents or other machine related tasks to remain unchanged	Functional		
1.97	- enable easy administration through a centralized console	Functional		
1.98	Platform must allow for RBAC / Federated Access	Functional		
1.99	Solution does not require restart on deployment, on initial install, or on upgrade	Functional		
1.100	- have ability to allow-list custom behaviors on endpoints	Functional		
1.101	- allow for sensors to be grouped together for purpose of policy assignment or other management tasks	Functional		
1.102	Solution will enable installation of sensors to groups in a predictable fashion	Functional		
1.103	- allow for installation of sensors via scripting and RMM solutions	Functional		
1.104	Platform must be able to configure exceptions for endpoint controls in policies and by groups	Functional		
1.105	- have NGAV on Windows 7 and greater	Functional		
1.106	Support for MacOs	Functional		
1.107	Support for Linux	Functional		

No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
1.108	Solution will have the ability to enhance other tools with correlated endpoint data (e.g. SIEM, Syslog)	Functional		
1.109	Solution will have an open and Flexible API and data export	Functional		
1.110	Solution can support orchestration workflows with SOAR, Ticketing (e.g. ServiceNow), or other platforms	Functional		
1.111	- provide critical response in 30 minutes or less	Functional		
1.112	- be able to provide remediation actions including machine isolation and process killing	Functional		
1.113	- provide proactive threat hunting	Functional		

Associated Security Operations Center and Assisted Response Capability

No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
2.1	• 24x7 threat hunting to detect and contain threats before they disrupt your operations or cause supply chain disruptions.	Non-Functional		
2.2	• Customizable compliance reporting to assure regulatory compliance and for supply chain due diligence purposes.	Functional		
2.3	• User & Entity Behavior Analytics (UEBA) helped determine and account for system's normal behavior pattern, and identify anomalies.	Functional		
2.4	• Complete security and analytics provided for the firm's large enterprise networks.	Functional		
2.5	• 24x7 Security Operations Center (SOC) services supported the firm during their investigations	Non-Functional		
2.6	Mix of human, automated and autonomous response	Non-Functional		
2.7	**Threat Intelligence Questions**			
2.8	Describe in detail your standard workflow for generating and leveraging threat intelligence within your proposed services.	Non-Functional		
2.9	Describe how the overall ingestion, analysis and production of threat intelligence is performed by your service using the TIP.	Non-Functional		
2.10	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		
2.11	How would you provide access into your managed TIP?			

No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
	Vulnerability Management Questions			

No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
3.1	Describe your detailed vulnerability scanning and notification processes for ad hoc and scheduled scans.	Non-Functional		
3.2	Describe your processes for tracking vulnerabilities to [Client] assets over time.	Functional		
3.3	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		
3.4	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		
3.5	How do you propose to work with [Client] to ensure that the platform includes or excludes our assets as appropriate?	Functional		
3.6	Describe your process for improving vulnerability management through this platform.	Functional		
	How does your solution help manage/implement:			
3.7	Attack Surface Management	Functional		
3.8	Insider Threat	Functional		
3.9	Posture Reporting and Benchmarks	Functional		
3.10	Policy violations and misconfigurations	Functional		
3.11	Forensics	Functional		
3.12	Analytics	Functional		
3.13	SOAR	Functional		
3.14	Threat Hunting	Functional		
3.15	Extended Detection	Functional		
3.16	Threat Detection	Functional		
3.17	Does your solution have out of the box and ad hoc compliance reports (FISMA)?	Functional		
No.	**Key Requirements**	**Functional / Non-Functional**	**Yes / No / Partial**	**Comments**
	Email Protections			
4.1	Does your Platform implement Email threat hunting?	Functional		
4.2	Does your platform delete email based on a filter language?	Functional		
4.3	Does it help threat hunt within email systems or O365?	Functional		
4.4	Can a sender be blocked globally from a central console	Functional		
4.5	Suspicious URL?	Functional		
4.6	Links to fake login page?	Functional		

No.	Key Requirements	Functional / Non-Functional	Yes / No / Partial	Comments
4.7	Malicious attachment?	Functional		
4.8	Spoofing your CEO?	Functional		
4.9	Suspicious Email?	Functional		
4.10	Unusual but benign?	Functional		
4.11	A never-before-seen attack?	Functional		