LAMPIRAN A

SPESIFIKASI TEKNIKAL

SEBUTHARGA BIL. 14/2019 :

PEROLEHAN SISTEM *ENDPOINT SECURITY THREAT PROTECTION*

BIL	BUTIR-BUTIR KERJA	PEMATUHAN (Sila √ atau x)	CATATAN *
1. Dashboard			
1.1	The console must provides a comprehensive visual representation of the threat activity in network, endpoint, and email environment. The widgets on the Dashboard must show the current patterns in threat detections.	☐	
1.2	The Dashboard must contains at least the following widgets: • The Event Activity widget provides information about the malicious files that were detected in network, endpoint, and email environments. This widget displays information from the Network, Endpoint, and Email widgets, which you can select individually to view additional information about each of those control points. • The Endpoint Event Activity widget provides information about both malicious files and suspicious files that were detected on your endpoints. Malicious files are the files that were blocked based on their detection as known threats. Suspicious files are the files that were flagged based on their reputation score but were otherwise undetected as malicious. Suspicious files may be benign but may be worth investigating. • The Email Event Activity widget provides information about malicious the files that were detected in email traffic from the endpoints in your environment. Malicious files are the files that were blocked based on their detection as known threats.	☐ ☐ ☐	

BIL	BUTIR-BUTIR KERJA	PEMATUHAN (Sila √ atau x)	CATATAN *
	• The Endpoints widget provides you with the following information about the endpoints in your environment: - Actively Infected Endpoints: The number of endpoints detected malicious activity in the last 96 hours. - Active Endpoint: The number of endpoints detected active in the last 96 hours. • The New and Unknown Threats widget lists the number of files that were detected as threats within the environment	☐ ☐	
2. Incidents			
2.1	Please explain on how the solution provides information on events, incidents, and entities	☐	
2.2	Please provide and explain the following items from the solution: - • How does the solution creates and prioritises incidents? • How to identify threats in the organisation with the proposed solution • Please explain on how does it analyzing the process behaviors that occurred on endpoints • Elaborate on the isolating breached endpoints and also deleting files from endpoints • Elaborate on the blacklisting and whitelisting suspicious domains, URLs, and IP addresses • Reporting false positive and false negative file convictions	☐ ☐ ☐ ☐ ☐ ☐	

BIL	BUTIR-BUTIR KERJA	PEMATUHAN (Sila √ atau x)	CATATAN *
	• Eloborate how cloud based sandboxing helps to detect malicious behavior and zero-day threats • Please explain on your recovery best practices	☐ ☐	
3. Policy			
3.1	Please explain on how the solution works on Blacklist and Whitelist	☐	
3.2	What are the Supported policy types and match values	☐	
3.3	Elaborate about importing and exporting policies	☐	
4. Logs			
4.1	Viewing the status of actions taken on entities in the Actions log	☐	
4.2	Viewing endpoint activities in the System Activity log	☐	
4.3	Does your solution able to exports logs to a .csv file	☐	
5. Reports			
5.1	Please elaborate on the Reports capability	☐	
5.2	Elaborate on the scheduling reports and the Purging of Reports	☐	
5.3	Elaborate on the Executive Report and also how can customer can use the Executive Report	☐	
5.4	Elaborate on the Incident Details Report	☐	
6. Capability			
6.1	The solution must have at least these Core Capabilities : • Support Windows, Linux, iOS & Android operating system for 400 endpoint devices in SME Corp. Headquarters & 12 States Offices (refer to SME Corp. Malaysia official website www.smecorp.gov.my for full addresses) • Antivirus - Scans for and eradicates malware that arrives on a system. Must support Windows, Linux, iOS & Android operating system	☐ ☐	

BIL	BUTIR-BUTIR KERJA	PEMATUHAN (Sila √ atau x)	CATATAN *
	• Firewall and intrusion prevention - Blocks malware before it spreads to the machine and controls traffic. • Application and device control - Controls file, registry, and device access and behavior; also offers whitelisting and blacklisting. • Power Eraser - An aggressive tool, which can be triggered remotely, to address advanced persistent threats and remedy tenacious malware. • Host integrity - Ensures endpoints are protected and compliant by enforcing policies, detecting unauthorized changes, and conducting damage assessments; it can also isolate a managed system that does not meet company requirements. • System lockdown - Allows whitelisted applications (known to be good) to run or blocks blacklisted applications (known to be bad) from running.	☐ ☐ ☐ ☐ ☐	
6.2	The solution also provides some OR all advanced capabilities as follows : • Global Intelligence Network - The world's largest civilian threat intelligence network collects data from millions of attack sensors; that data is analyzed by more than a thousand highly skilled threat researchers to provide unique visibility into threats. • Reputation Analysis - Determines safety of files and websites using artificial intelligence techniques in the cloud and powered by the GIN. • Emulator - Uses a lightweight sandbox to detect polymorphic malware hidden by custom packers. • Intelligent threat cloud - Rapid scan capabilities using advanced techniques such	☐ ☐ ☐ ☐	

BIL	BUTIR-BUTIR KERJA	PEMATUHAN (Sila √ atau x)	CATATAN *
	as pipelining, trust propagation, and batched queries able to avoid unnecessary to download all signature definitions to the endpoint to maintain a high level of effectiveness. Only the newest threat information is downloaded. • Roaming client visibility - Receives critical events from clients that are off the corporate network. • Suspicious file detection - Enables IT security teams to tune the level of detection and blocking separately to optimize protection and gain enhanced visibility into suspicious files for each customer environment.	☐ ☐	
6.3	Application isolation: • Hardens endpoints by isolating suspicious or malicious apps into 'jail mode' to prevent the execution of privileged operations including downloading executable files, writing to the registry, and more. • Maximizes security efficacy by complementing critical hardening technology with prevention capabilities. • Strengthens protections by shielding productivity tools and other known good applications from vulnerability exploits.	☐ ☐ ☐	
6.4	Application control: • Delivers fixed-function device lock-down by enforcing default-deny to applications and restricting updates to those defined as trusted. • Offers restricted execution of unauthorized apps for standard endpoints by governing the 'allow' list of approved apps for additional flexibility. • Easily extends the use of unapproved applications when deemed safe while alerting administrators of potential risks posed by application drift.	☐ ☐ ☐	

BIL	BUTIR-BUTIR KERJA	PEMATUHAN (Sila √ atau x)	CATATAN *
	• Maximizes security efficacy by complementing critical hardening technology with prevention capabilities.	☐	
6.5	Endpoint Detection and Response: • Detects and exposes - Reduces time to breach discovery and quickly exposes scope. • Investigates and contains - Increases incident responder productivity and ensures threat containment. • Resolves - Rapidly fixes endpoints and ensures threat does not return. • Enhances Security Investments - Takes advantage of prebuilt integrations and public APIs.	☐ ☐ ☐ ☐	
6.6	Mobile capabilities: Offers add-on defenses that deliver dynamic protection that complements endpoint security to address attack vectors for modern devices and user behavior for Windows, Linux, IOS and Android devices	☐	
6.7	Simplified management: Cloud-based management console for endpoint security - able to deliver accurate, intelligent, and faster insights with AI-guided security management from a single console.	☐	
6.8	Cyber Defense Manager: • Full cloud console - Manages complete endpoint security from a single cloud console to reduce endpoint security management complexity. • Single agent • AI-guided security management	☐ ☐ ☐	

BIL	BUTIR-BUTIR KERJA	PEMATUHAN (Sila √ atau x)	CATATAN *
	• Autonomous security management - Learns from administrators or the organization or community to continuously assess and strengthen security posture.	☐	
	• Simplified workflows - Uses simplified workflows with context-aware recommendations to eliminate routine tasks and enhance endpoint security decisions.	☐	

* sila nyatakan di ruangan ini jika terdapat maklumat tambahan berkaitan tawaran yang dikemukakan atau kemukakan kertas cadangan tambahan jika ruang tidak mencukupi

Saya / Kami memperakui maklumat yang diberikan adalah benar.

.....

Nama :

Jawatan :

Tarikh :

Cop Syarikat :