■「EDRを利用したSOCサービスの設計、構築、導入及び運用保守業務」仕様書に関する問い合わせへの回答

令和5年(2023年)8月8日

仕様書に対して、問い合わせがあった内容について以下のとおり回答します。

札幌市デジタル戦略推進局情報システム部

項番	仕様書該当箇所	質問	回答
1	EDR要求機能一覧 No.13 以下に記載するOSに対応すること。 ・マルチセッション版のWindows10 Enterprise (64bit) ・マルチセッション版のWindows11 Enterprise (64bit)	マルチセッション版のWindowsと記載されておりますが、一つのVMインスタンスに対して複数ユーザがログインする形を想定されておりますでしょうか？ 弊社ご提案を想定しているソリューションでは、センサーはVMインスタンスごとにインストールされるため、アラート検知後に隔離対処を実施した場合は、VMインスタンスに接続するすべてのユーザすに影響が及びます。 本対応は許容いただけますでしょうか。	マルチセッション版のWindowsに関しては、ご認識のとおりです。 隔離対処時にVMインスタンスに接続する全てのユーザに影響が出てしまうことについては、許容いたします。
2	SOCサービス要求機能一覧 No.5 最低限必要な4つの内容を設けることができる機能を有すること。 Lv4：早期対応が必要 Lv3：攻撃が成功した可能性が高い Lv2：攻撃につながる可能性が低い Lv1：攻撃とはいえないが留意すべき事項	質問回答（令和5年7月26日掲載）に記載がございました以下内容についてご確認させてください。 --- インシデントレベル4と3は包括せずに、「SOCサービス要求機能一覧」No.4、5で示す4段階以上のインシデントレベルを設定いただきますようお願いいたします。 --- インシデントレベルの区分の内容を記載頂いておりますが、 4つ以上の段階の定義に関する対処方針は、別途運用設計等で検討する理解でよろしいでしょうか。 弊社ご提案を想定しているソリューションでは、Lv4(緊急)の場合の対処はただちに隔離実行が行われ、Lv3（警戒)については、隔離解除ではなくアラートに関連付けられたプロセスとすべての子プロセスを停止します。この対処方針で許容頂けますでしょうか。	4つ以上の段階の定義に関する対処方針は、別途運用設計等で検討させていただきます。 なお、仕様書付属文書「SOCサービス要求機能一覧」NO.10についても満たすことができる運用としていただき、仮にLv3のインシデントであっても隔離措置が適切な場合は、隔離措置する運用を想定しております。
3	SOCサービス要求機能一覧 No.10 判定されたインシデントレベルに応じて、脅威（検体）や被疑端末の隔離措置ができること。また、隔離実行の判断は本市ではせず、インシデントレベルに応じて隔離を行い、誤検知だった場合は隔離解除できること。	判定されたインシデントレベルに応じて、脅威（検体）や被疑端末の隔離措置ができること。また、隔離実行の判断は本市ではせず、インシデントレベルに応じて隔離を行い、誤検知だった場合は隔離解除できること。 との記載がございますが、「隔離解除」については、本市様にてご判断頂く認識でよろしいでしょうか。	ご認識のとおりです。
4	別紙１ 要件定義書 (15) 保守 ウ 保守対象 本業務で監視対象としている端末やそれらに付随するソフトウェアおよび機器類全般とする。	保守対象として、監視対象としている端末やそれらに付随するソフトウェアおよび機器類全般とする。 との記載がございますが、本調達対象においては、AVDおよびNEWSネット端末の保守は含まず、AVDおよびNEWSネット端末に導入されるEDRに関するソフトウェアを対象とする認識でよろしいでしょうか。	ご認識のとおりです。
5	別紙１ 要件定義書 (11) 移行 ア 共通	導入対象となる端末にて、既存で使用されているアンチウイルスソフトの製品名をご教示お願いいたします。 既存のEPP/NGEPP製品によっては、今回導入対象のEPP/NGEPPとの置き換えが必要となりますことをご理解頂きたくよろしくお願い致します。	導入対象となる端末は、新規で構築/調達するものとなりますので、既存のEPP製品はございません。
6	別紙１ 要件定義書 (14) 運用 （ウ）ログ管理 ②受託者は、保存対象ログの取り出しについて、本市担当者から依頼・指示を受けた場合は、速やかに対応すること。	貴市担当者から保存対象のログの取り出しについて依頼、指示を受けた場合の対応につきまして、 対象のログは、インシデント情報のログでよろしいでしょうか。	仕様書付属文書「EDR要求機能一覧」NO.32に記載されているものとなります。
7	(15) 保守 エ 保守業務 (ア) インシデント対応、隔離、隔離解除 ① 重要なインシデントが発生していると判断した場合、内容の決定から 60分以内を原則とし、本市運用管理者へ報告すること。	重大なインシデントが発生していると判断した場合、内容の決定から60分以内を原則とし、本市運管理者へ報告すること。 とございますが、「60分以内」は、重大なインシデント発生を本市運用管理者様へ報告する初報時間との理解でよろしいでしょうか。	ご認識のとおりです。
8	別紙１ 要件定義書 (14) 運用 (エ) 変更管理 ①共通 ・ 受託者は、インシデント発生時の影響の最小化において必須である、検知、通知、調査、対応、復旧のサービスを提供し、影響範囲調査・対応開始を起点とし、 翌営業日以内を原則とし、本市管理者へ報告すること。	インシデント発生時の影響の最小化において必須である「復旧のサービス」につきましては、EDR機能として提供可能な対応との理解でよろしいでしょうか。（例：隔離解除対応）	仕様書付属文書「SOCサービス要求機能一覧」NO.10の記載のとおり、復旧については、以下の運用・保守業務を受託した事業者に対して、インシデントレベルや内容に応じて、作業を支援をしていただくこととなります。 ・「クラウド型仮想デスクトップ」上で実行される「デスクトップおよびアプリの仮想化サービス（Azure Virtual Desktop）」 ・NEWSネットへある程度の期間をかけて段階的に移行する業務用FAT端末