サンプル

(相手先企業名) 御中

たよれーる らくらくNGAV for Deep Instinct 2023年度7月度　レポート

株式会社 大塚商会 たよれーるコンタクトセンター
2023/08/xx

サンプル

1. 概要

1.1. デバイス関連

1.1.1. 検知モードPCの台数

(検知モードとなっているデバイスの台数を過去3カ月にわたり、OS別に記載しています。)

		2023年		
		5月	6月	7月
デバイス種別	Windows	16	18	19
	Mac OS	-	-	-
	Linux	-	-	-
	Chrome OS	-	-	-
	モバイル	-	-	-

1.1.2. 隔離モードPCの台数

(隔離モードとなっているデバイスの台数を過去3カ月に渡り、OS別に記載しています。)

		2023年		
		5月	6月	7月
デバイス種別	Windows	0	0	0
	Mac OS	-	-	-
	Linux	-	-	-
	Chrome OS	-	-	-
	モバイル	-	-	-

1.2. ポリシー別のデバイス数

(各ポリシー別のデバイス数を過去3カ月に渡り、OS別に記載しています。)

		2023年		
		5月	6月	7月
デバイス種別	Windows Default Policy	0	17	17
	macOS Default Policy	-	1	1
	Linux Default Policy	-	0	0
	Android Default Policy	-	1	1
	Chrome OS Default Policy	-	0	0
	iOS Default Policy	-	0	0

1.2.1. 検知モードのポリシー別のデバイス数

(検知モードとなっているデバイスを検知モードポリシー別に、過去3カ月にわたり記載しています。)

		2023年		
		5月	6月	7月
デバイス種別	Windows Default Policy	0	17	17
	macOS Default Policy	-	1	1
	Linux Default Policy	-	0	0
	Android Default Policy	-	1	1
	Chrome OS Default Policy	-	0	0
	iOS Default Policy	-	0	0

サンプル

1.3.　デバイス別検知リスク数TOP10

（当月のデバイス別の検知数Top10を、過去3カ月の同デバイスの検知数と共に記載しています。
際立って検知数が多いデバイスについては、何らかの異常が疑われるため、該当デバイスの
正常性について精査されることを強く推奨いたします。）

		統計月		
		5月	6月	7月
デバイス名	DESKTOP-JRTA0AE	0	0	9
	LAPTOP-HJVUJ48I	0	0	1
	DESKTOP-M1R9SHV	0	0	0
	DESKTOP-COR22B5	0	0	0
	LAPTOP-6HDFCP9G	0	0	0
	DESKTOP-LS3C6DN	0	0	0
	DESKTOP-9P17IK9	0	0	0
	DELL-2	0	0	0
	Google_sdk_gphone64_x86_64	0	0	0
	DELL-1	0	0	0

2.　検知統計

2.1.　検知イベントTOP10

（当月の検知イベントごとのTop10を、過去3カ月の同イベントの検知数と共に記載しています。）

		統計月		
		5月	6月	7月
検知イベント	C:¥Windows¥System32¥rundll32.exe	0	0	0
	C:¥Users¥dac¥Desktop¥static¥*	0	0	0
	C:¥ProgramData¥Dell¥SARemediation¥SystemRepair¥Snapshots¥Backup¥*	0	0	0
	C:¥Program Files¥Microsoft Office¥Updates¥Download¥PackageFiles¥*	0	0	0
	C:¥Program Files¥Common Files¥Microsoft Shared¥ClickToRun¥Updates¥*¥*	0	0	0
	C:¥Program Files (x86)¥XMind¥plugins¥*.tmp	0	0	0
	C:¥Program Files¥PuTTY¥putty.exe	0	0	0
	¥apps¥bin¥osri¥audit¥*.zip	0	0	0
	C:¥Windows¥SysWOW64¥WindowsPowerShell¥v1.0¥powershell.exe	0	0	0
	C:¥Program Files¥Oracle¥VirtualBox¥VBoxHeadless.exe	0	0	0

3.　Executive Summary Report

3.1.　Executive Summary Report

※別紙を参照ください。

サンプル

4. Appendix1

4.1. 検知ポリシーになっているデバイス一覧

(検知ポリシーとなっているデバイスの一覧を記載しています。意図せずに検知ポリシーとなっている
デバイスについては、早期に隔離ポリシーに移行することを強く推奨いたします。)

		デバイス名
デバイスグループ	Android Default Group	Google_sdk_gphone64_x86_64
	Windows Default Group	DELL-2
		LAPTOP-HJVUJ48I
		DESKTOP-COR22B5
		DESKTOP-JRTA0AE
		DESKTOP-LS3C6DN
		LAPTOP-6HDFCP9G
		DESKTOP-M1R9SHV
		DESKTOP-COR22B5
		LAPTOP-HJVUJ48I
		DESKTOP-L1281Q3
		DELL-2
		DESKTOP-EHG63QR
		DESKTOP-ASD0NRR
	macOS Default Group	DACのMacBook Pro
	tytest group	DESKTOP-9P17IK9

サンプル

5. Appendix2

4.2 用語集

用語	意味
検知モード	外部脅威に対する防御は行わず検知のみ行うポリシー設定となります。 脅威に対して危険な状態ですので、早期の隔離モードへの移行を推奨します。
隔離モード	外部脅威に対する防御を行うポリシー設定となります。 脅威に対して防御が行われる状態ですので、原則本モードでの運用を推奨します。
xx Default Policy	DeepInstinctにて、各OSごとに用意されているデフォルトのポリシーとなります。 検知モード状態となりますので、早期の隔離モードへの移行を推奨いたします。
イベント	DeepInstinctで検知された各種のアラートを「イベント」と称します。 アラートにまで満たない動きについては「疑わしいイベント」と称されています。
重大度	各イベント/疑わしいイベントの重大性を段階的に示しています。 深刻度順に「Very High」「High」「Moderate」「Low」の4段階となっています。
D-Client	エンドポイント防御のためにデバイスにインストールされるクライアントソフトウェアを意味します。
ポリシー	脅威に対する検知・防御を行うための設定の一覧となります。 設定したポリシーをデバイスが含まれるグループに紐づけることにより、グループ内のデバイスは、設定したポリシーに沿った検知・防御が行われることとなります。
グループ	デバイスの特定条件による集合体を意味します。 デバイスをグループに参加させるには手動での対応の他、タグやOS、IPアドレス等一定の条件により自動でグループに参加させることも可能となっています。
静的検知	一般的なアンチウイルスに近い、ファイルスキャンによる検知となります。 後述の動的検知に比べ一般的に誤検知等が少なく、運用負荷が低いものとなります。 また、静的なファイル自体の安全性をレピュテーションサイト等で確認可能です。
動的検知	前述の静的検知とは異なり、ファイル自体の安全性ではなく、危険な振る舞いを監視し、脅威と考えられるものである場合に検知・防御する仕組みとなります。 静的検知とは異なり特定のファイルに起因するものではないことから、ファイル自体がレピュテーションサイトで安全であっても脅威でないと断言できないことが特色の一つと言えます。

6. 問い合わせ先

本レポートに関するお問い合わせ、及び設定変更依頼については以下までお願いいたします。

株式会社 大塚商会 たよれーるコンタクトセンター
らくらくNGAV for Deep Instinct 担当
対応時間：　　平日 9 時00分～17時30分
メールアドレス：　　tayoreru-soc@con.daj.co.jp