Connect Beyond

SentinelOne™

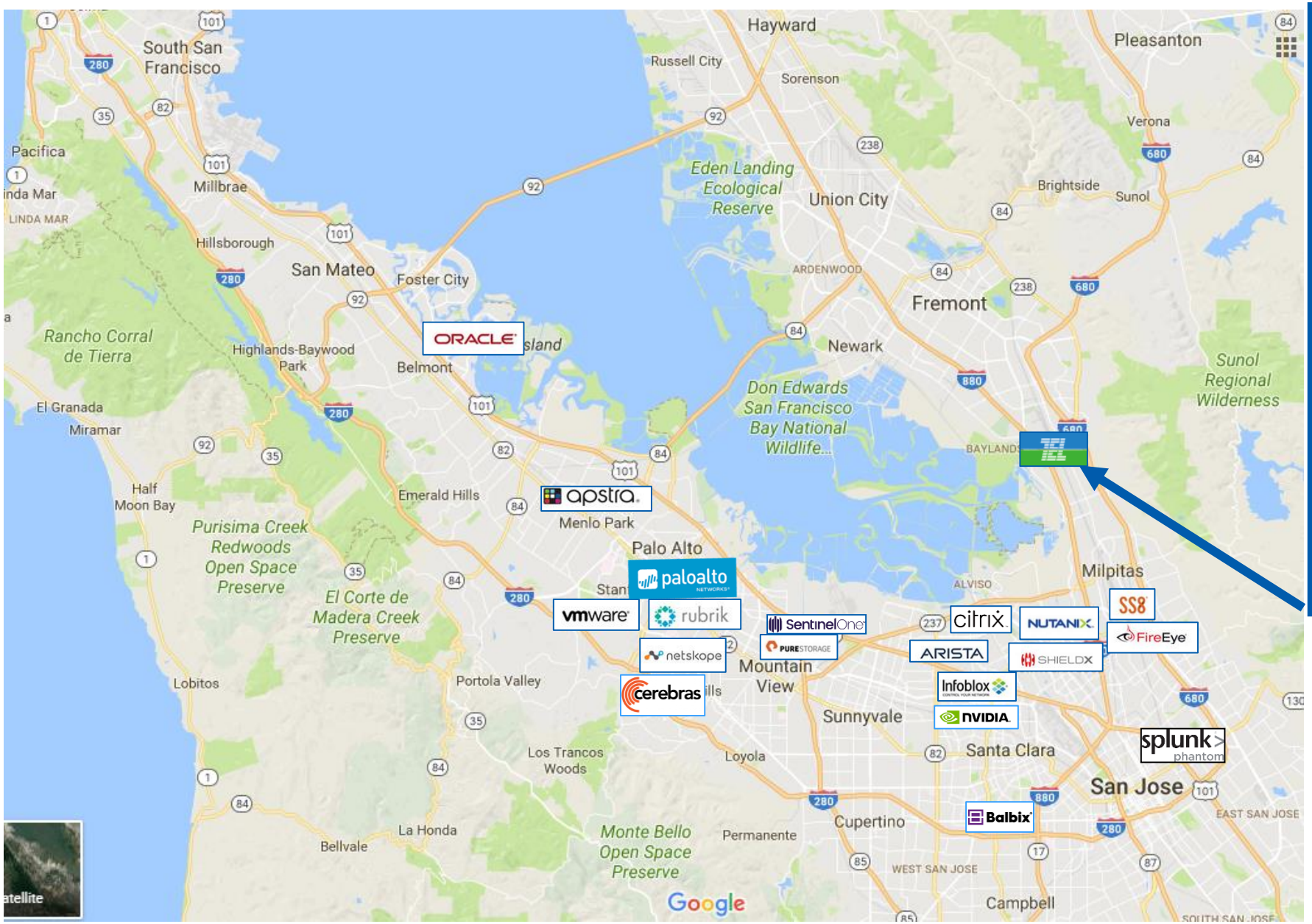
The Border2020

2020年12月

東京エレクトロン デバイス株式会社
クラウド技術部サイバーセキュリティ技術グループ
三吉 徹

TED? / Why SentinelOne??

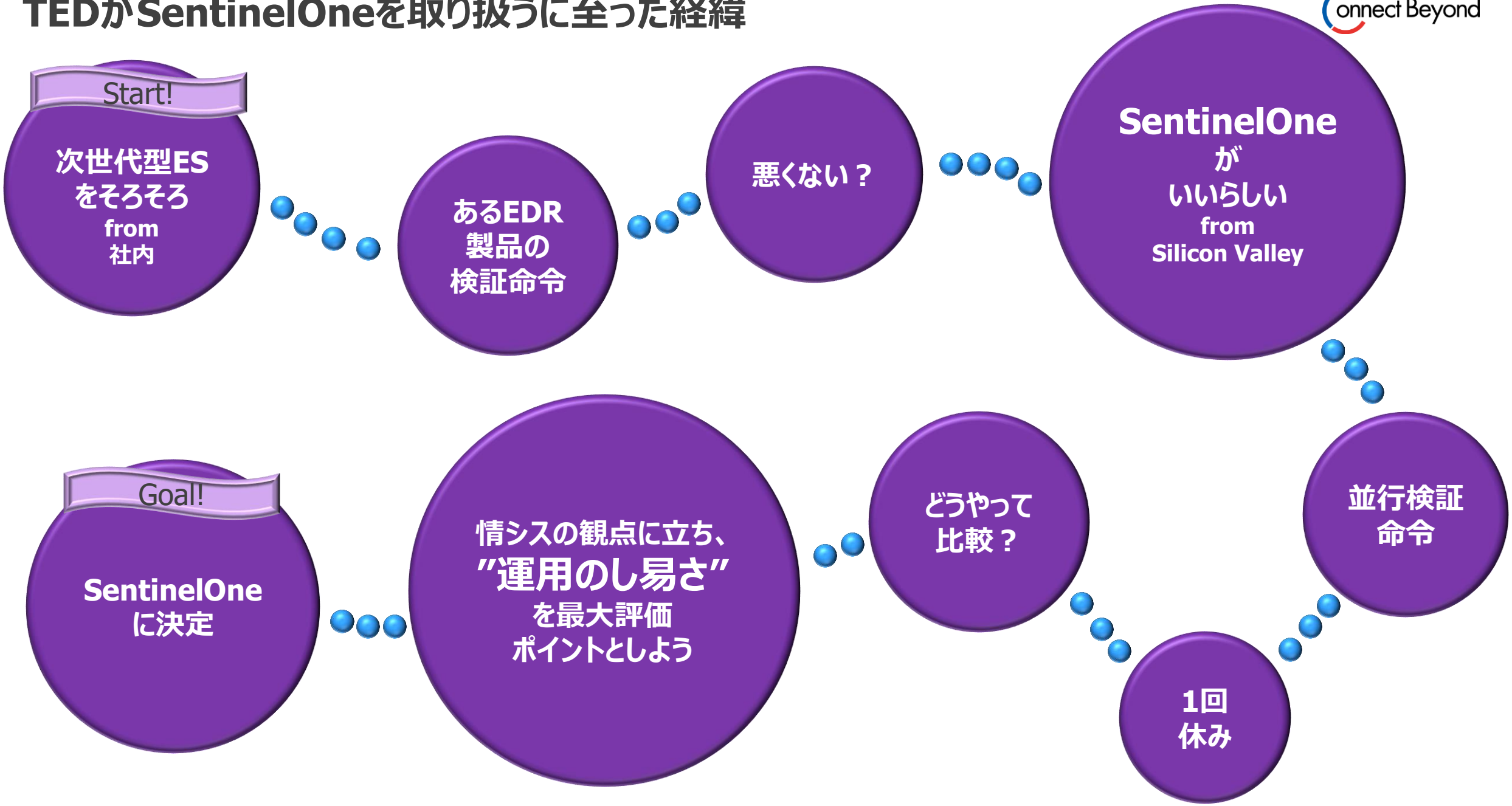
Tokyo Electron Device Americaにて情報収集



- 設立： 2016年4月1日
- 所在地： Fremont, CA
- 従業員数： 9名
- 資本金： $300,000

東京エレクトロン デバイス

TEDがSentinelOneを取り扱うに至った経緯



TEDがSentinelOneを取り扱う決め手になった要因

EPP/EDRが1エージェント

EDRの”R”-Responseが自動対応

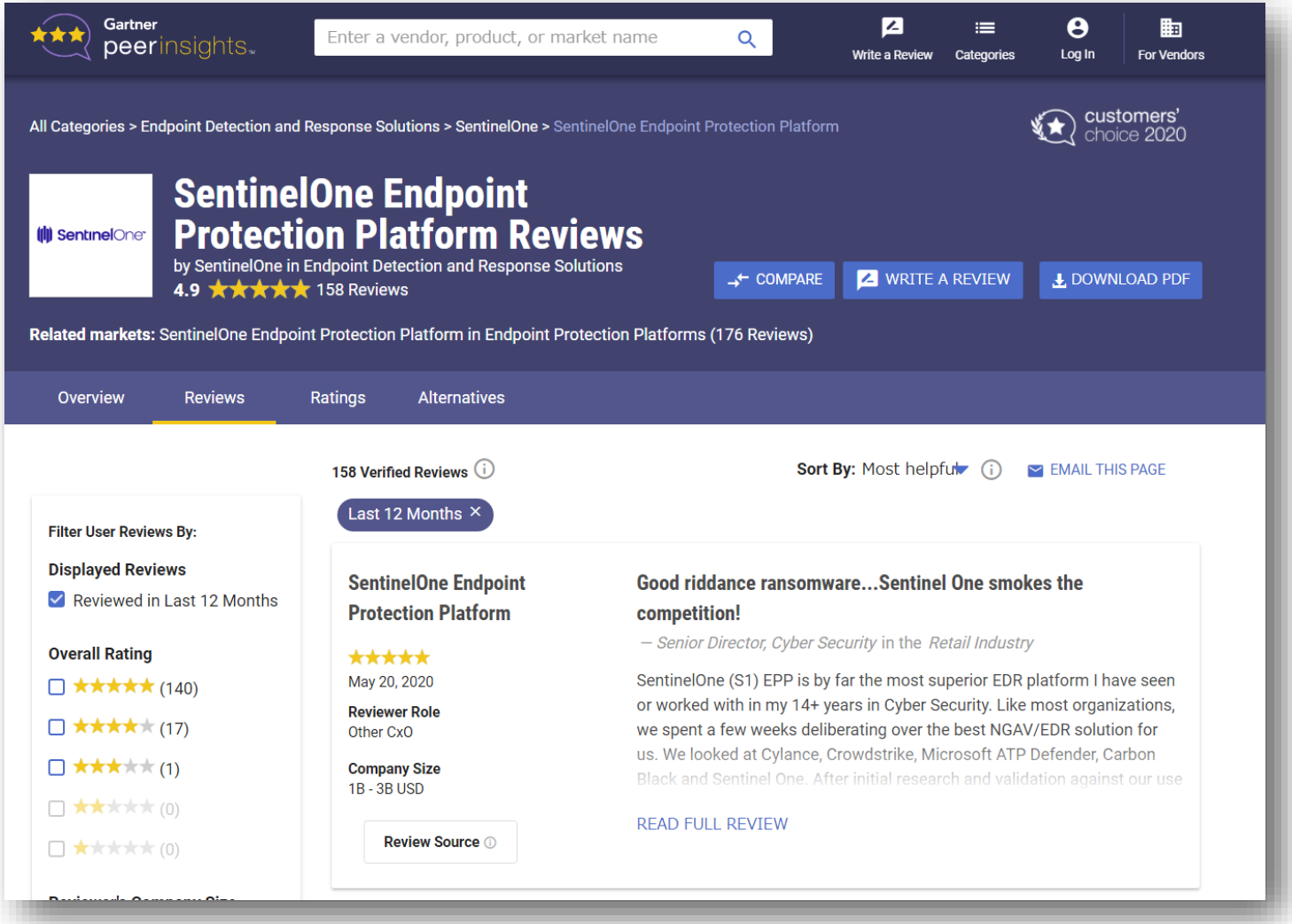
多彩な”R”の実装-Remediate/Rollback/Research

考えるプロセスを”極小化”出来るソリューション ＝ 運用が楽に違いない、という確信

SentinelOneに対する第三者評価

Gartner peer insights

"(SentinelOne) gives them the ability to do actual Security work instead of Administering an AV product for 90% of the time."

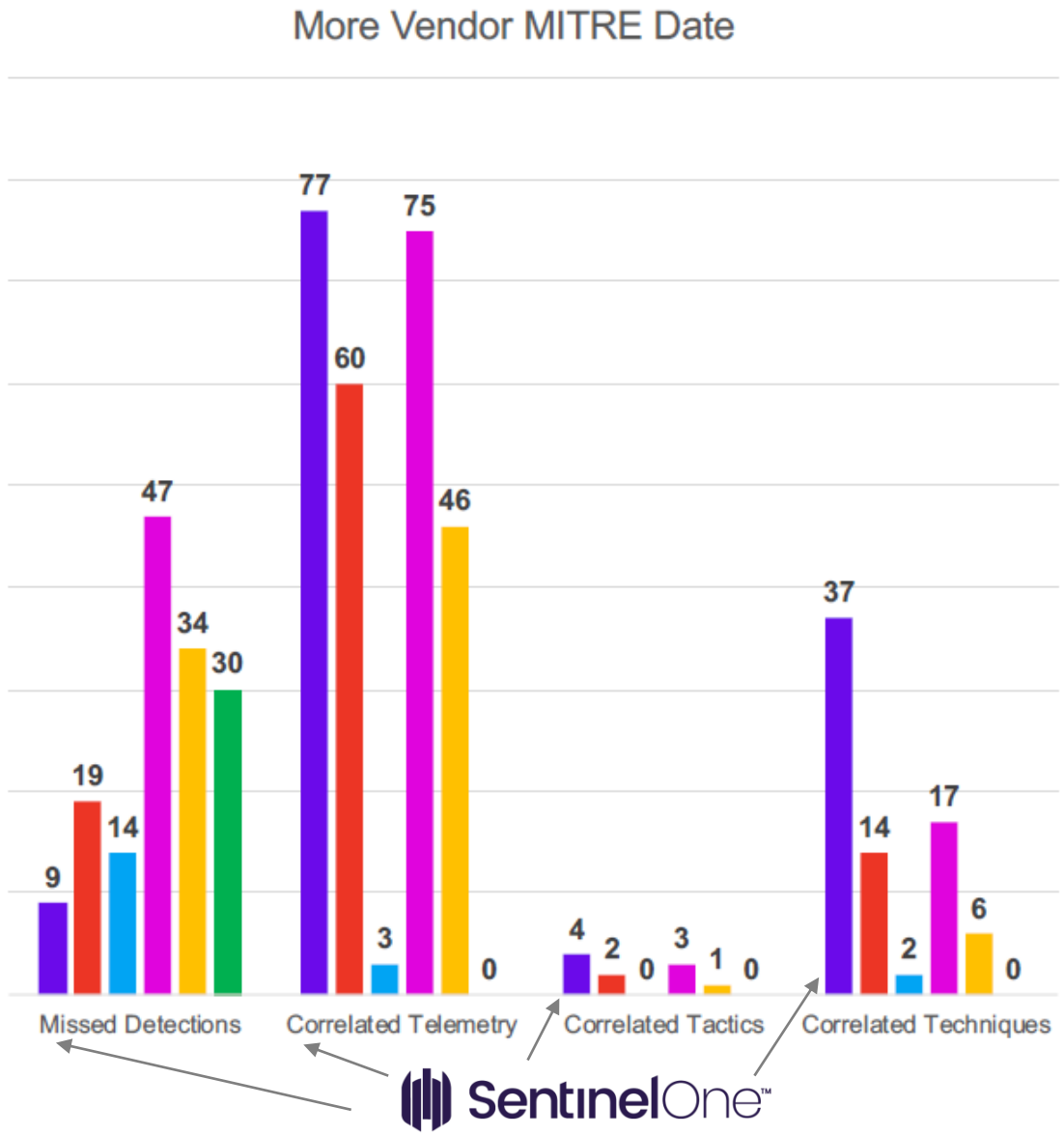


運用負荷軽減に関するコメントが多数見受けられる

引用元：https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions/vendor/sentinelone/product/sentinelone-endpoint-protection-platform/reviews

MITRE ATT&CK Evaluations

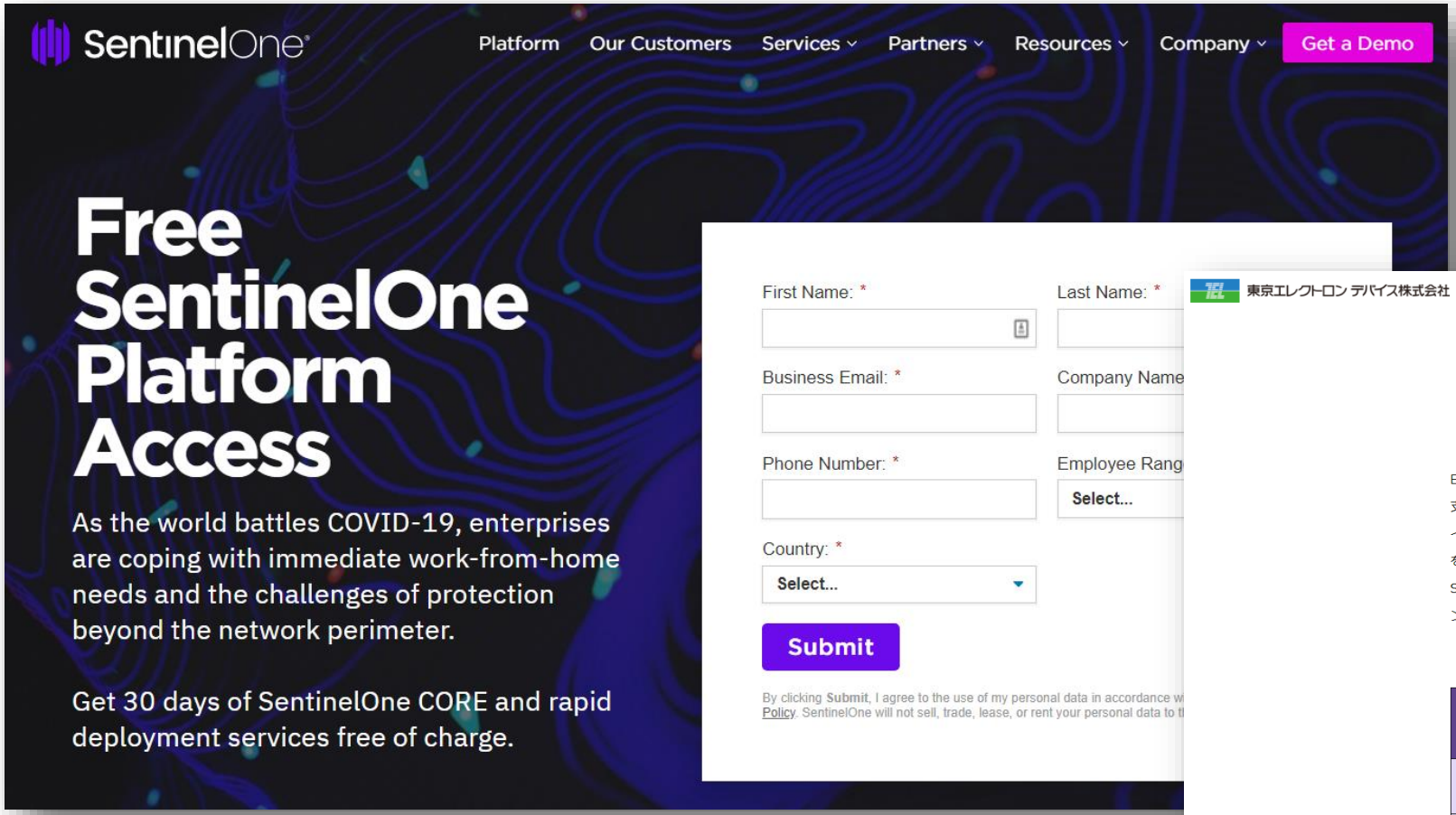
- ✓ APT29(別名:The Dukes)の攻撃手法をエミュレートしてEPP/EDR製品をテスト
- ✓ SentinelOneが最も詳細に検知
  - ✓ Missed→未検知数(9)
  - ✓ Telemetry→痕跡のログ保存(77)
  - ✓ Tactics→検知理由として攻撃フェーズを表示(4)
  - ✓ Techniques→検知理由として攻撃フェーズ並びに攻撃手法を表示(37)
- ✓ 運用に叶っていることが客観的にも証明

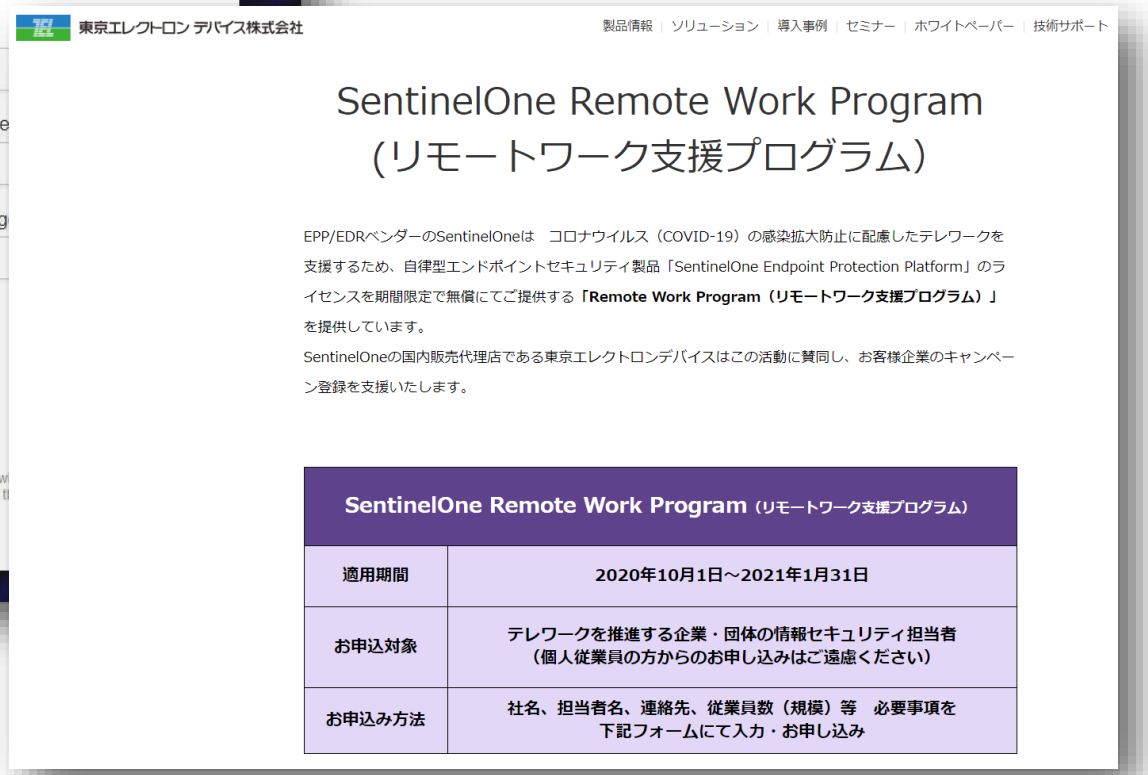


引用元：SentinelOne社資料 “MITRE ATT&CK Round 2 - SentinelOne results v2.1.pdf”

運用に関するエピソード

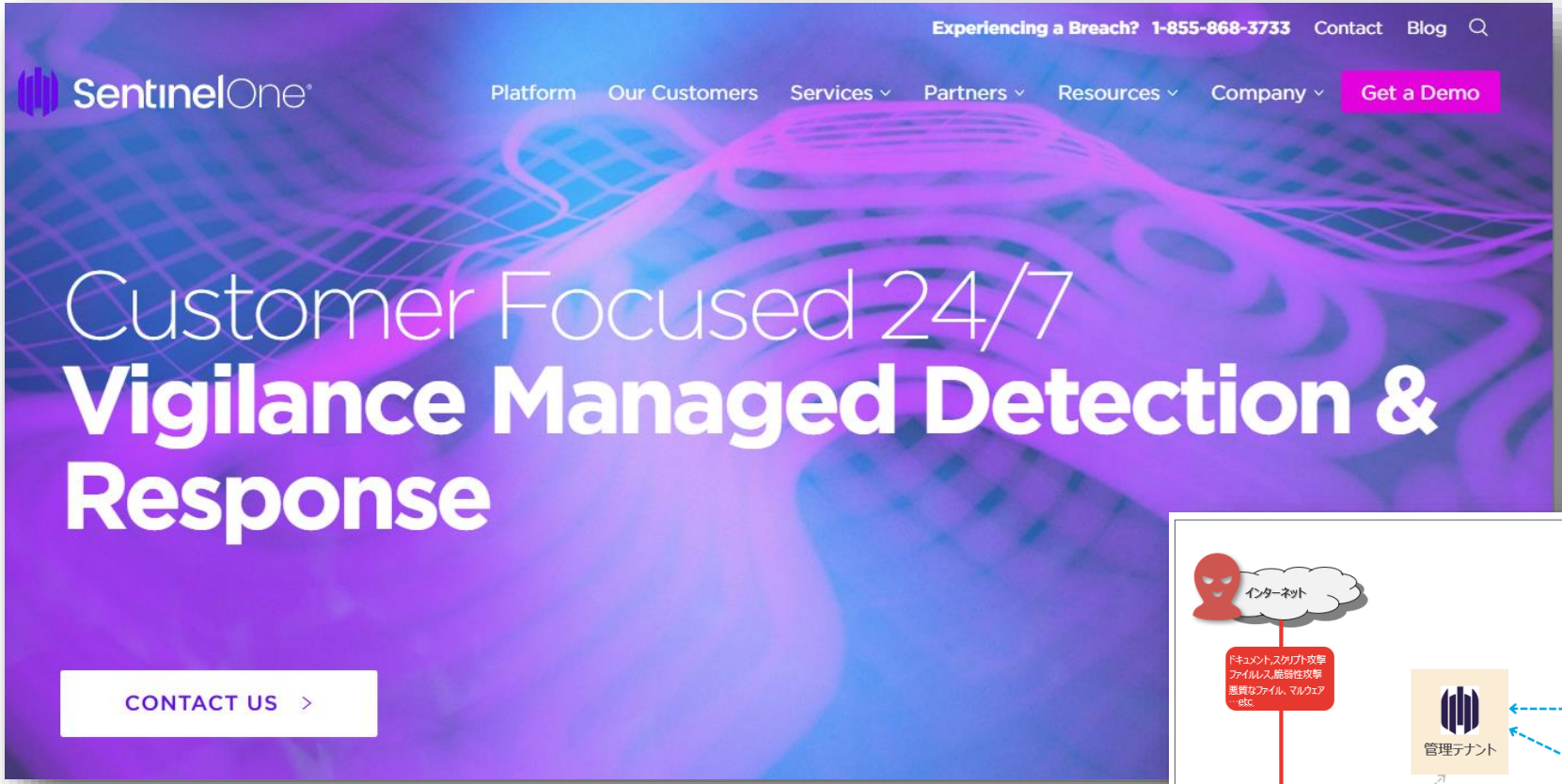
COVID-19無償キャンペーン

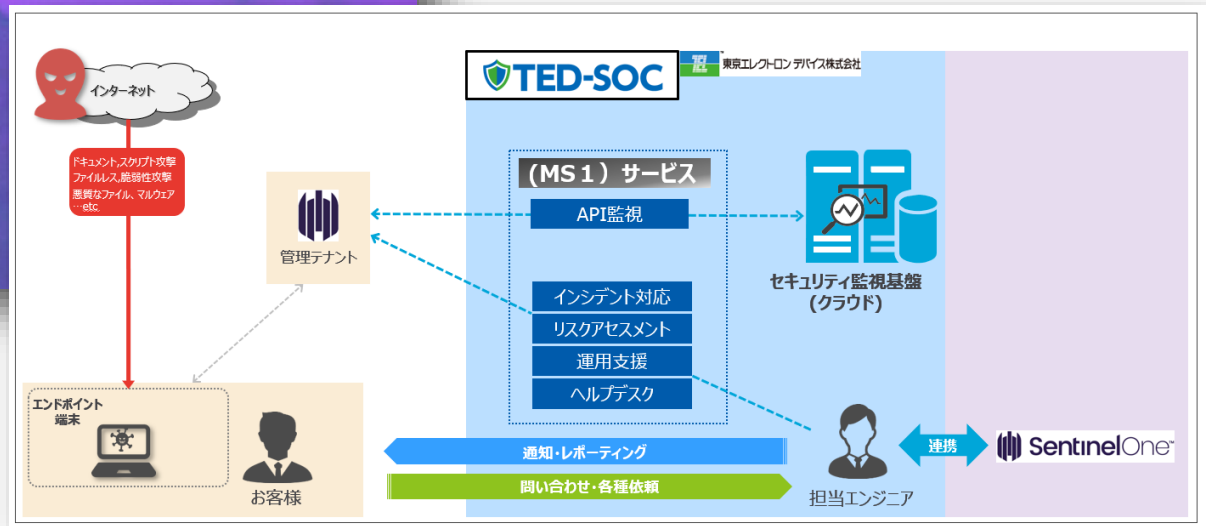




素早く展開出来、必ずしもSOCを必要としないSentinelOneならではのキャンペーン

SOC-MDR(Managed Detection & Response)の採用率





SOC採用率はWorldwideで10%弱、Japanで21%。他は全て自社運用

クララオンライン様へのご紹介に際して

クララオンライン様導入に際してのご支援(1)-検体提供

"Good PoC is Good Deal.
Let's use real malware!"

JARED PHIPPS
VP Worldwide Sales Engineering
ex US Air Force - MITRE

実際に存在するマルウェアファイルを検査検体としてご提供

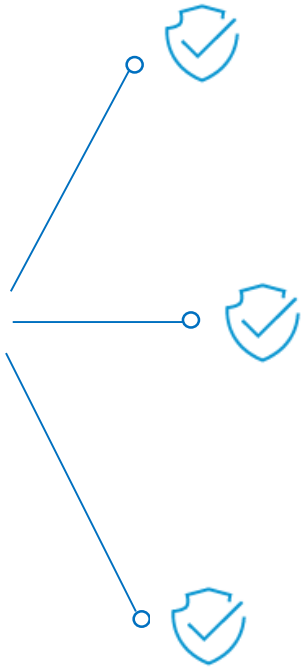
クララオンライン様へのご支援(2)評価項目表のご提供

■SentinelOne PoC 実施項目一覧表

9	静的検知/防御	シグネチャマッチングによる既知のマルウェアファイルの検知、隔離ができる
10		ファイル構造解析によるマルウェアファイルの実行前検知、隔離ができる
11		端末がオフライン状態の場合も、シグネチャマッチング・ファイル構造解析による マルウェアファイルの検知、隔離ができる
12	動的検知/防御	動的解析エンジンにより、悪意ある挙動(Powershellによるファイルレス攻撃など)の 検知、防御ができる
13		端末がオフライン状態の場合も、動的解析エンジンにより悪意ある挙動の 検知、防御ができる
14	軽減	管理画面より、端末のネットワーク隔離ができる
15		マルウェア検知時に、感染端末をポリシーにて自動的に隔離処理ができる
16		隔離したファイルに対して、隔離解除やダウンロード操作ができる
17		ハッシュ値を利用したブラックリスト登録ができる
18		静的エンジンに対するホワイトリスト登録ができる (ハッシュ、証明書、拡張子)
19		動的エンジンに対するホワイトリスト登録ができる (パス指定、ブラウザ)
20	修復	マルウェア感染時に一時作成されたファイル、改変されたレジストリキー等を元の状態に 修復できる
21		ランサムウェアに暗号化された感染端末内のファイルを復旧できる
22		管理画面より、隔離していた端末のネットワーク復帰ができる
23		実行されたコマンドラインの内容が確認できる
24		別プロセスへのインジェクション状況の確認ができる
25		プロセスが実行したディスク、レジストリ上の書き込み/読み込みの確認ができる
26		プロセスが実行したネットワークオペレーション（DNS、IPアドレス）の確認ができる
27		静的エンジンでの検知理由が確認ができる

運用面を重視したPoC評価項目のご提示

クララオンライン様ご採用に際しての印象深いこと



ロジカルな選定プロセス→迅速な意思決定

企業風土さえも評価対象-カルチャーフィット

全てリモート(非対面)で完遂-製品紹介からPoC、ご発注まで

今後の展開 with クララオンライン様

今後の展開 - SentinelOne +

CLARA ONLINE

東京エレクトロン デバイス

- Withコロナ/Afterコロナ- リモートワークへの訴求
- 一人情シスのお客様(特にSMB)へ寄り添う
- 来年もTheBorderに参加！？
- SentinelOneに続く新規ソリューションのご提案・協業

Connect Beyond

共に創る 新たな価値を

東京エレクトロン デバイス