GENBU

あなたの会社の
セキュリティ
本当に大丈夫ですか?

GENBU ASM は、サイバー攻撃のリスクを可視化し、脆弱性を徹底診断。
最新のテクノロジーで、企業の安全を守ります。
サイバーセキュリティ診断なら、GENBU ASM

こんなお悩みにアプローチ!

- 膨大な数のIT資産を把握・管理する
- セキュリティ診断の手間を省く
- セキュリティ対策の負担を軽減

BEANS Communication

Cyber Security

アタックサーフェス診断サービス概要

① 外部公開資産の把握

インターネット上の情報からIT資産を自動探索し、未把握な資産やリスクの存在を明らかにします。

■ 対象とするインターネット上の情報(例):
IPアドレス、ドメイン、証明書、オープンポート、ソフトウェア、漏洩パスワード...等

＋

② リスクの可視化と対応優先度の決定

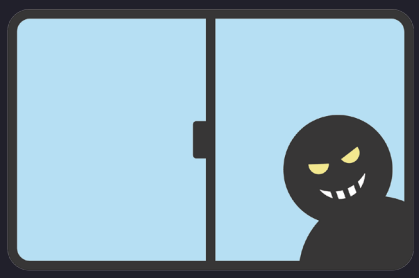
IT資産の脆弱性をOSINT技術※により分析することで、企業のリスクを可視化し、迅速な対処法を提示します。

緊急リスク　重大リスク　警告リスク

- 簡単に診断が可能
- サプライチェーン全体の調査が可能
- スピーディな診断
- 客観的なリスク評価

※OSINT技術により公開情報から脆弱性を調査するため、貴社システムへの影響無しで調査可能です。

サービスプラン



- 【イメージ例】家の外からカメラでチェックする
- 「窓が開いている」「鍵が壊れている」「フェンスが低くて侵入しやすい」など、ツールを使って明らかに見える脆弱性を発見！
- ただし、泥棒がどこから侵入するのか、どうやって攻撃するのかまでは詳しく調査不可

価格 ¥300,000(税抜)　**納期** 3～5営業日でレポート提出

サービス提供実績

アタックサーフェス診断に基づく侵入テストを実施

金融業(従業員数5,000人～)

半年間にわたりアタックサーフェスをモニタリングし、公開資産の脆弱性や漏洩情報を網羅的に調査。さらに、潜在的な侵入経路に対して侵入テストを実施し、リスクの可視化と対策を支援。

膨大なシステム数に対して効率的な診断を実現

インフラ業(従業員数1,000人～)

150以上のシステムを自社保有する組織に対し、外部からの侵入経路を網羅的に調査。サイバー攻撃のリスク評価を行い、対応優先度を明確化。

ボット感染の早期発見に成功

人材派遣業(従業員数100人～)

約1か月にわたるアタックサーフェス診断を通じ、システムの脆弱性や漏洩情報のリスクを特定。さらに、業務端末のボット感染を発見し、早期対策を提案。

BEANS Communication

株式会社BEANS COMMUNICATION
住所：〒150-0041 東京都渋谷区神南1丁目11-4 FPGリンクス神南5階
お問い合わせはこちら mail：y.ohashi@beanscommunication.com

HP