2022 年 7 月 4 日

報道関係各位

GMO サイバーセキュリティ by イエラエ株式会社

「GMO サイバーセキュリティ侵入テスト」において『レッドチーム演習』を提供開始

～疑似的なサイバー攻撃により、企業・組織のサイバー防衛レベルの確認やサイバー防衛チームの実践的トレーニングが可能に～

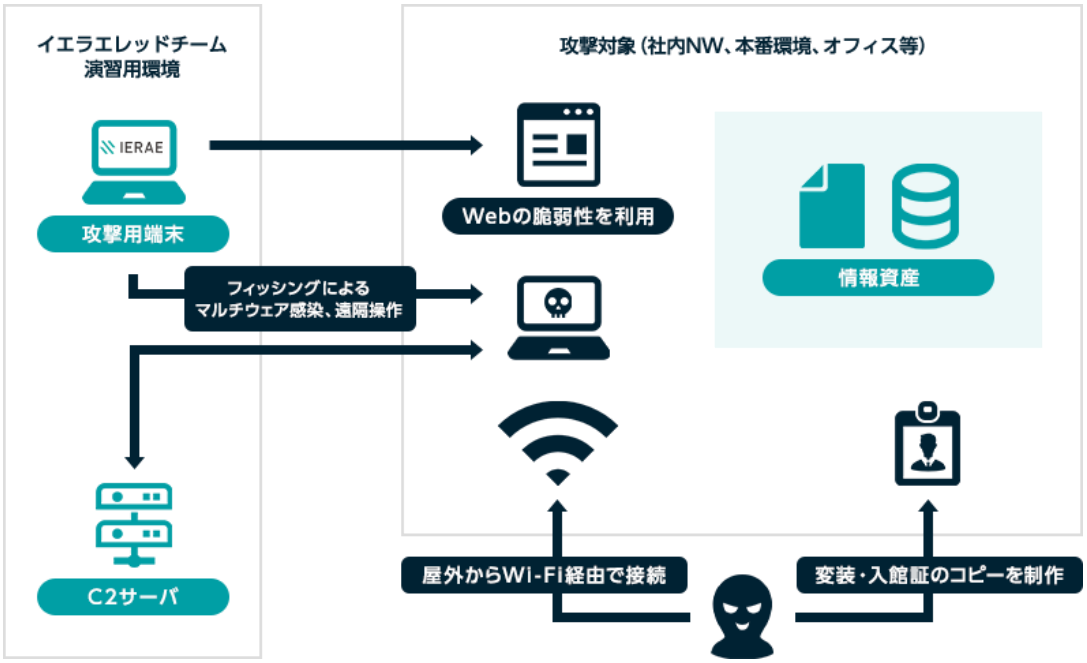
GMO インターネットグループでサイバーセキュリティ関連事業を展開する GMO サイバーセキュリティ by イエラエ株式会社（代表取締役 CEO：牧田 誠　旧称：イエラエセキュリティ　以下、GMO サイバーセキュリティ by イエラエ）は、本日 2022 年 7 月 4 日（月）より、ホワイトハッカーによるサイバーセキュリティ診断サービス「GMO サイバーセキュリティ侵入テスト」において新メニュー『レッドチーム演習』の提供を開始します。

【『レッドチーム演習』とは】（URL：https://gmo-cybersecurity.com/service/redteam）

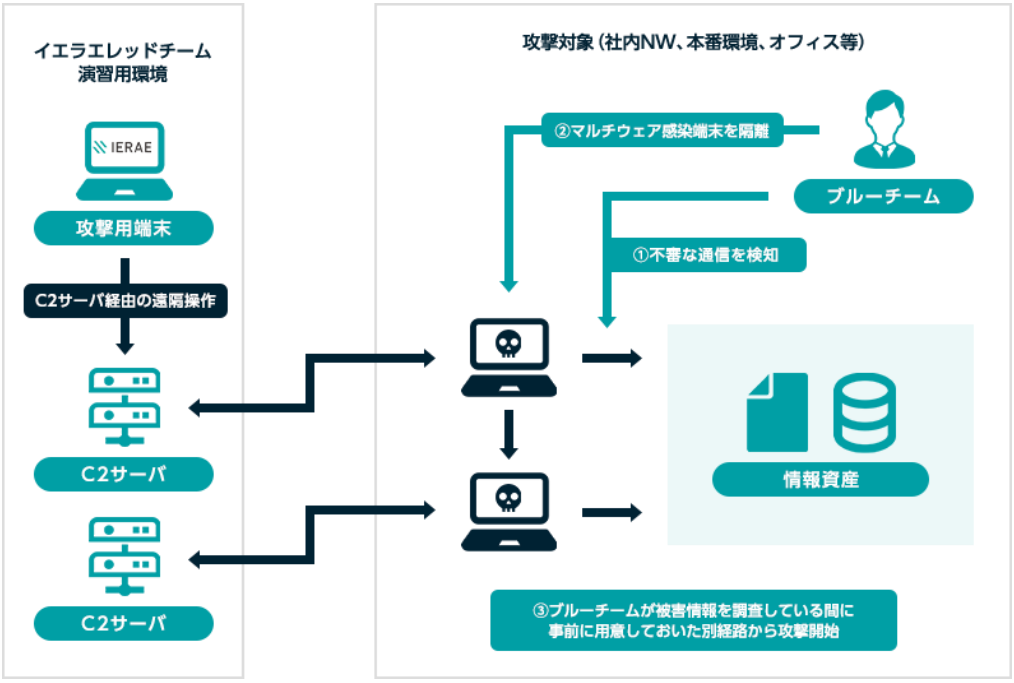
依頼元の組織全体に対して、GMO サイバーセキュリティ by イエラエに所属するホワイトハッカーが疑似的なサイバー攻撃を行うことにより、企業・組織のサイバー防衛レベルの確認やサイバー防衛チームの実践的トレーニングを行うサービスです。

『レッドチーム演習』では、GMO サイバーセキュリティ by イエラエのホワイトハッカーが、実際の攻撃者を想定したサイバー攻撃を行う「レッドチーム」、依頼元企業のサイバー防衛担当者が、レッドチームによるサイバー攻撃を検知しブロックする「ブルーチーム」となり、演習形式でサイバー攻撃対応を行います。演習中は、依頼元企業の一部の関係者により組織された「ホワイトチーム」が演習状況を監視・調整し、演習後の評価も行います。

<レッドチームによる様々な手法を利用した攻撃>



<ブルーチームによるサイバー防衛をかわし、攻撃を継続するレッドチーム>



■『レッドチーム演習』の 2 つの特徴

(1)攻撃シナリオを環境ごとに設定

レッドチームは組織内の異なる環境ごとに攻撃シナリオを作成し、様々な手法でサイバー攻撃を実施します。そのため、運用や設計における不備から物理的なリスクの利用など、多角的な視点の攻撃を実施可能です。

(2)高度なサイバー攻撃を受けた場合の対応について訓練が可能

レッドチームは、ブルーチームが検知できない高度なサイバー攻撃を行います。検知された場合も攻撃手法を切り替えたり、攻撃を永続化したりすることで攻撃の継続が可能です。そのため、ブルーチームは実際にサイバー攻撃を受けた場合と同様にスピード感を持って正確に被害範囲を把握し対処することが求められます。

■ペネトレーションテストと『レッドチーム演習』の違い

事前に取り決めたスコープやシナリオに沿った形で進行するペネトレーションテスト（侵入テスト）と異なり、『レッドチーム演習』では組織全体が攻撃（診断）対象となるのに加え、本物のサイバー攻撃と同様に実際のインシデント相当の対応が求められるのが大きな特徴となっています。SOC や CSIRT 等の体制強化や組織全体のセキュリティレベル確認に最適な内容です。

	ペネトレーションテスト	レッドチーム演習
事前通知	事前にSOCやCSIRTに通知 検知発生時の対応も取り決める	ごく一部の関係者のみに共有
スコープ (テスト範囲)	事前に関係者間で協議し、 定義された範囲、シナリオに基き ゴール達成リスクを評価する	組織全体がスコープ ゴール達成にとって有益なものは全て攻撃対象になりえる 例：フィッシング、Web、無線AP、物理的侵入、漏洩情報の悪用
検知発生時の対応	事前に取り決めた対応に従う	本物の攻撃同様に 被害状況の調査や感染端末の隔離を リアルタイムで実施する

【提供開始の背景】

サイバー攻撃の高度化・巧妙化や攻撃対象の多様化を背景に、企業や組織におけるサイバー防衛体制構築の必要性は日々高まっています。

GMO サイバーセキュリティ by イエラエでは、ホワイトハッカーによるサイバーセキュリティ診断サービス「GMO サイバーセキュリティ侵入テスト」において特定の製品やシステムを対象として、ホワイトハッカーが疑似的なサイバー攻撃を行うことでリスク評価を行うペネトレーションテスト（侵入テスト）を提供しており、幅広い業界に対する多数の実施実績を持ち、国内企業のセキュリティレベル向上に寄与してまいりました。この度、サイバー防衛力のさらなる向上とサイバー防衛体制構築を望む企業のご要望に応えるべく、「レッドチーム演習」の提供を開始することといたしました。

■GMO サイバーセキュリティ by イエラエの確かな技術力

・**国内外の CTF（※1）において受賞実績**を持つ技術力の高いホワイトハッカー（セキュリティエンジニア）が在籍

・ペネトレーションテストにおいて **90%以上の侵入成功率**（※2）

・ペネトレーションテストの際に、企業が利用する他社製**システム・サービスの脆弱性を半年間で 16 件発見**（※3）

・**幅広い業界におけるペネトレーションテスト実施・リピート実績**を持ち、各業界特有の知見・ノウハウも蓄積

【業界例】金融機関、製造業（自動車等）、ゲーム、IT（暗号資産／SaaS／アプリ／セキュリティ等）など

（※1）2018 年 Car Hacking Village DEFCON 26:世界 1 位 / 2018 年 Positive Hack Day：2 位 / 2018 年 S4 CTF：世界 3 位 / 2017 年 Practical CAN bus hacking CTF：国内 1 位

（※2）2018 年 3 月-2021 年 10 月ペネトレーションテスト診断 114 件の実績値（金融 38 件 その他 76 件）。ゴール達成に加えて、不正侵入、サーバー乗っ取り、機密情報の奪取につながる脆弱性の検出を含む。

（※3）2021 年 12 月～2022 年 6 月までの半年間で発行された CVE を集計。ペネトレーションテスト中に発見した脆弱性を含む。

URL：https://gmo-cybersecurity.com/cve/

【「GMO サイバーセキュリティ侵入テスト」について】

（URL: https://gmo-cybersecurity.com/service/pentest/）

GMO サイバーセキュリティ by イエラエのホワイトハッカーによるサイバーセキュリティ診断サービスです。企業・組織のサイバー防衛レベル・体制にあわせて、以下のメニューより診断方法をお選びいただくことが可能です。

■ペネトレーションテスト（侵入テスト）

標的に対して様々なシナリオに沿った疑似的なサイバー攻撃を行うことでリスク評価

＜シナリオ例＞

- **標的型攻撃**：独自開発の疑似マルウェアを用いた外部からの攻撃者を想定したペネトレーションテスト
- **OSINT**：社外に公開されたデジタル資産の調査・分析
- **物理環境**：物理環境（Wi-Fi や社員証の偽造など）に対する攻撃を想定したペネトレーションテスト
- **Web ペネトレーションテスト**：Web アプリケーションを対象としたペネトレーションテスト
- **調査特化型**：運用中・運用予定のシステムや製品に対するペネトレーションテスト

■レッドチーム演習

演習形式での実践的なサイバー攻撃対応訓練・リスク評価

【GMO サイバーセキュリティ by イエラエについて】（URL:https://gmo-cybersecurity.com/）

「誰もが犠牲にならない社会」をミッションに掲げ、国内最大規模のホワイトハッカーを組織するサイバーセキュリティのプロフェッショナルカンパニーです。Web アプリケーションやスマホアプリ、企業の基幹システムなどに対するサイバー攻撃に対する高度なセキュリティ対策を提供し、持続可能な事業継続をサポートしています。国内各業界に対する技術支援をより加速すべく、2022 年 4 月には銀行向けのサイバーセキュリティ総合対策パッケージ「GMO サイバーセキュリティ for 銀行」（URL：https://gmo-cybersecurity.com/lp/for-bank/）の提供を開始するなど、業界特化型の技術支援の取組も強化しています。

加えて、事業を担うエンジニアが世界一働きやすい職場となるべく取組を進めており、2021 年には「ホワイト企業プラチナ認定」を取得しています。

■在籍エンジニアが発信するサイバーセキュリティの最新情報はこちらから

https://gmo-cybersecurity.com/blog/

以上

【報道関係お問い合わせ先】

●GMO サイバーセキュリティ by イエラエ株式会社
事業推進部　帰山
TEL：03-6276-6045　E-mail：info@ierae.co.jp

●GMO インターネット株式会社
グループコミュニケーション部広報担当 寺山
TEL：03-5456-2695　E-mail：pr@gmo.jp

【サービスに関するお問い合わせ先】

●GMO サイバーセキュリティ by イエラエ株式会社
事業推進部　営業チーム
TEL：03-6276-6045　E-mail：info@ierae.co.jp

【GMO サイバーセキュリティ by イエラエ株式会社】（URL: https://gmo-cybersecurity.com/ ）

会　　社　　名	GMO サイバーセキュリティ by イエラエ株式会社

所　　在　　地	東京都渋谷区桜丘町 26 番 1 号　セルリアンタワー
代　　表　　者	代表取締役 CEO　牧田　誠
事　業　内　容	■Web アプリ及びスマホアプリ脆弱性診断　■ペネトレーションテスト ■不正利用(チート)診断　■IoT 脆弱性診断 ■自動車脆弱性診断　■フォレンジック調査 ■CSIRT 支援　■クラウドセキュリティ診断 ■クラウドセキュリティ・アドバイザリー
資　　本　　金	8,000 万円

【GMO インターネット株式会社】（URL：https://www.gmo.jp/ ）

会　　社　　名	GMO インターネット株式会社　（東証プライム　証券コード：9449）
所　　在　　地	東京都渋谷区桜丘町 26 番 1 号　セルリアンタワー
代　　表　　者	代表取締役グループ代表　熊谷　正寿
事　業　内　容	■インターネットインフラ事業　■インターネット広告・メディア事業 ■インターネット金融事業　■暗号資産事業
資　　本　　金	50 億円