Q0001

脅威インテリジェンス・攻撃分析
タグ：サイバーキルチェーン
用語：サイバーキルチェーンの確認ポイント1：攻撃を偵察から目的達成までの段階で整理するモデル

次の説明に最も合う用語はどれか。攻撃を偵察から目的達成までの段階で整理するモデル

A. MITRE ATT&CK
B. OSINT
C. サイバーキルチェーン
D. フィッシング分析

答え・解説

Q0001 正答：C. サイバーキルチェーン

解説：サイバーキルチェーンは、攻撃を偵察から目的達成までの段階で整理するモデル。ほかの選択肢は目的又は適用場面が異なる。

Q0002

脅威インテリジェンス・攻撃分析
タグ：サイバーキルチェーン
用語：サイバーキルチェーンの確認ポイント2：攻撃を偵察から目的達成までの段階で整理するモデル

サイバーキルチェーンの説明として最も適切なものはどれか。

A. 実際の攻撃者の戦術と技術を体系化した知識ベース
B. 公開情報から必要な情報を収集・分析する活動
C. 送信元、URL、ヘッダ、添付、誘導内容などを調べる活動
D. 攻撃を偵察から目的達成までの段階で整理するモデル

答え・解説

Q0002 正答：D. 攻撃を偵察から目的達成までの段階で整理するモデル

解説：サイバーキルチェーンの要点は「攻撃を偵察から目的達成までの段階で整理するモデル」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0003

脅威インテリジェンス・攻撃分析
タグ：サイバーキルチェーン
用語：サイバーキルチェーンの確認ポイント3：攻撃を偵察から目的達成までの段階で整理するモデル

用語と説明の組合せとして適切なものはどれか。論点は「サイバーキルチェーン」である。

A. サイバーキルチェーン：攻撃を偵察から目的達成までの段階で整理するモデル
B. MITRE ATT&CK：攻撃を偵察から目的達成までの段階で整理するモデル
C. OSINT：攻撃を偵察から目的達成までの段階で整理するモデル
D. フィッシング分析：攻撃を偵察から目的達成までの段階で整理するモデル

答え・解説

Q0003 正答：A. サイバーキルチェーン：攻撃を偵察から目的達成までの段階で整理するモデル

解説：正しい組合せは「サイバーキルチェーン：攻撃を偵察から目的達成までの段階で整理するモデル」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0004

脅威インテリジェンス・攻撃分析
タグ：サイバーキルチェーン
用語：サイバーキルチェーンの確認ポイント4：攻撃を偵察から目的達成までの段階で整理するモデル

「サイバーキルチェーン」は、攻撃を偵察から目的達成までの段階で整理するモデル。

A. ○
B. ×

答え・解説

Q0004 正答：○

解説：正しい。サイバーキルチェーンは攻撃を偵察から目的達成までの段階で整理するモデル。実務では対象、目的、前提条件を併せて確認する。

Q0005

脅威インテリジェンス・攻撃分析
タグ：サイバーキルチェーン
用語：サイバーキルチェーンの確認ポイント5：攻撃を偵察から目的達成までの段階で整理するモデル

組織が「攻撃を偵察から目的達成までの段階で整理するモデル」ために採用すべき概念又は仕組みはどれか。

A. MITRE ATT&CK
B. OSINT
C. サイバーキルチェーン
D. フィッシング分析

答え・解説

Q0005 正答：C. サイバーキルチェーン
解説：この目的に対応するのはサイバーキルチェーンである。攻撃を偵察から目的達成までの段階で整理するモデルという機能・考え方を持つためである。

Q0006

脅威インテリジェンス・攻撃分析
タグ：サイバーキルチェーン
用語：サイバーキルチェーンの確認ポイント6：攻撃を偵察から目的達成までの段階で整理するモデル

「サイバーキルチェーン」について、誤解を避けるための説明として最も適切なものはどれか。

A. 送信元、URL、ヘッダ、添付、誘導内容などを調べる活動
B. 公開情報から必要な情報を収集・分析する活動
C. 実際の攻撃者の戦術と技術を体系化した知識ベース
D. 攻撃を偵察から目的達成までの段階で整理するモデル

答え・解説

Q0006 正答：D. 攻撃を偵察から目的達成までの段階で整理するモデル
解説：サイバーキルチェーンは攻撃を偵察から目的達成までの段階で整理するモデル。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0007

脅威インテリジェンス・攻撃分析
タグ：サイバーキルチェーン
用語：サイバーキルチェーンの確認ポイント7：攻撃を偵察から目的達成までの段階で整理するモデル

「サイバーキルチェーン」は、実際の攻撃者の戦術と技術を体系化した知識ベース。

A. ○
B. ×

答え・解説

Q0007 正答：×

解説：誤り。記述はMITRE ATT&CKの説明である。サイバーキルチェーンは攻撃を偵察から目的達成までの段階で整理するモデル。

Q0008

脅威インテリジェンス・攻撃分析
タグ：サイバーキルチェーン
用語：サイバーキルチェーンの確認ポイント8：攻撃を偵察から目的達成までの段階で整理するモデル

次の状況で中心となる論点はどれか。「攻撃を偵察から目的達成までの段階で整理するモデル」ことが求められている。

A. OSINT
B. サイバーキルチェーン
C. フィッシング分析
D. MITRE ATT&CK

答え・解説

Q0008 正答：B. サイバーキルチェーン

解説：中心となる論点はサイバーキルチェーンである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0009

脅威インテリジェンス・攻撃分析
タグ：サイバーキルチェーン
用語：サイバーキルチェーンの確認ポイント9：攻撃を偵察から目的達成までの段階で整理するモデル

「攻撃を偵察から目的達成までの段階で整理するモデル」という特徴を持つものを選べ。

A. フィッシング分析
B. OSINT
C. サイバーキルチェーン
D. MITRE ATT&CK

答え・解説

Q0009 正答：C. サイバーキルチェーン
解説：サイバーキルチェーンが該当する。定義は攻撃を偵察から目的達成までの段階で整理するモデルであり、他の候補とは機能が異なる。

Q0010

脅威インテリジェンス・攻撃分析
タグ：MITRE ATT&CK
用語：MITRE ATT&CKの確認ポイント1：実際の攻撃者の戦術と技術を体系化した知識ベース

次の説明に最も合う用語はどれか。実際の攻撃者の戦術と技術を体系化した知識ベース

A. TTP
B. STIX
C. C2通信
D. MITRE ATT&CK

答え・解説

Q0010 正答：D. MITRE ATT&CK
解説：MITRE ATT&CKは、実際の攻撃者の戦術と技術を体系化した知識ベース。ほかの選択肢は目的又は適用場面が異なる。

Q0011

脅威インテリジェンス・攻撃分析
タグ：MITRE ATT&CK
用語：MITRE ATT&CKの確認ポイント2：実際の攻撃者の戦術と技術を体系化した知識ベース

MITRE ATT&CKの説明として最も適切なものはどれか。

A. 実際の攻撃者の戦術と技術を体系化した知識ベース
B. 攻撃者の戦術・技術・手順をまとめた行動特性
C. サイバー脅威情報を構造化して表現する仕様
D. 攻撃者が侵害端末へ指令を送り結果を受け取る通信

答え・解説

Q0011 正答：A. 実際の攻撃者の戦術と技術を体系化した知識ベース

解説：MITRE ATT&CKの要点は「実際の攻撃者の戦術と技術を体系化した知識ベース」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0012

脅威インテリジェンス・攻撃分析
タグ：MITRE ATT&CK
用語：MITRE ATT&CKの確認ポイント3：実際の攻撃者の戦術と技術を体系化した知識ベース

用語と説明の組合せとして適切なものはどれか。論点は「MITRE ATT&CK」である。

A. TTP：実際の攻撃者の戦術と技術を体系化した知識ベース
B. MITRE ATT&CK：実際の攻撃者の戦術と技術を体系化した知識ベース
C. STIX：実際の攻撃者の戦術と技術を体系化した知識ベース
D. C2通信：実際の攻撃者の戦術と技術を体系化した知識ベース

答え・解説

Q0012 正答：B. MITRE ATT&CK：実際の攻撃者の戦術と技術を体系化した知識ベース

解説：正しい組合せは「MITRE ATT&CK：実際の攻撃者の戦術と技術を体系化した知識ベース」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0013

脅威インテリジェンス・攻撃分析
タグ：MITRE ATT&CK
用語：MITRE ATT&CKの確認ポイント4：実際の攻撃者の戦術と技術を体系化した知識ベース

「MITRE ATT&CK」は、実際の攻撃者の戦術と技術を体系化した知識ベース。

A. ○
B. ×

答え・解説

Q0013 正答：○

解説：正しい。MITRE ATT&CKは実際の攻撃者の戦術と技術を体系化した知識ベース。実務では対象、目的、前提条件を併せて確認する。

Q0014

脅威インテリジェンス・攻撃分析
タグ：MITRE ATT&CK
用語：MITRE ATT&CKの確認ポイント5：実際の攻撃者の戦術と技術を体系化した知識ベース

組織が「実際の攻撃者の戦術と技術を体系化した知識ベース」ために採用すべき概念又は仕組みはどれか。

A. TTP
B. STIX
C. C2通信
D. MITRE ATT&CK

答え・解説

Q0014 正答：D. MITRE ATT&CK

解説：この目的に対応するのはMITRE ATT&CKである。実際の攻撃者の戦術と技術を体系化した知識ベースという機能・考え方を持つためである。

Q0015

脅威インテリジェンス・攻撃分析
タグ：MITRE ATT&CK
用語：MITRE ATT&CKの確認ポイント6：実際の攻撃者の戦術と技術を体系化した知識ベース

「MITRE ATT&CK」について、誤解を避けるための説明として最も適切なものはどれか。

A. 実際の攻撃者の戦術と技術を体系化した知識ベース
B. 攻撃者が侵害端末へ指令を送り結果を受け取る通信
C. サイバー脅威情報を構造化して表現する仕様
D. 攻撃者の戦術・技術・手順をまとめた行動特性

答え・解説

Q0015 正答：A. 実際の攻撃者の戦術と技術を体系化した知識ベース

解説：MITRE ATT&CKは実際の攻撃者の戦術と技術を体系化した知識ベース。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0016

脅威インテリジェンス・攻撃分析
タグ：MITRE ATT&CK
用語：MITRE ATT&CKの確認ポイント7：実際の攻撃者の戦術と技術を体系化した知識ベース

「MITRE ATT&CK」は、攻撃者の戦術・技術・手順をまとめた行動特性。

A. ○
B. ×

答え・解説

Q0016 正答：×

解説：誤り。記述はTTPの説明である。MITRE ATT&CKは実際の攻撃者の戦術と技術を体系化した知識ベース。

Q0017

脅威インテリジェンス・攻撃分析
タグ：MITRE ATT&CK
用語：MITRE ATT&CKの確認ポイント8：実際の攻撃者の戦術と技術を体系化した知識ベース

次の状況で中心となる論点はどれか。「実際の攻撃者の戦術と技術を体系化した知識ベース」ことが求められている。

A. STIX
B. C2通信
C. MITRE ATT&CK
D. TTP

答え・解説

Q0017 正答：C. MITRE ATT&CK

解説：中心となる論点はMITRE ATT&CKである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0018

脅威インテリジェンス・攻撃分析
タグ：MITRE ATT&CK
用語：MITRE ATT&CKの確認ポイント9：実際の攻撃者の戦術と技術を体系化した知識ベース

「実際の攻撃者の戦術と技術を体系化した知識ベース」という特徴を持つものを選べ。

A. C2通信
B. STIX
C. TTP
D. MITRE ATT&CK

答え・解説

Q0018 正答：D. MITRE ATT&CK

解説：MITRE ATT&CKが該当する。定義は実際の攻撃者の戦術と技術を体系化した知識ベースであり、他の候補とは機能が異なる。

Q0019

脅威インテリジェンス・攻撃分析
タグ：TTP
用語：TTPの確認ポイント1：攻撃者の戦術・技術・手順をまとめた行動特性

次の説明に最も合う用語はどれか。攻撃者の戦術・技術・手順をまとめた行動特性

A. TTP
B. OSINT
C. TAXII
D. ラテラルムーブメント

答え・解説

Q0019 正答：A. TTP

解説：TTPは、攻撃者の戦術・技術・手順をまとめた行動特性。ほかの選択肢は目的又は適用場面が異なる。

Q0020

脅威インテリジェンス・攻撃分析
タグ：TTP
用語：TTPの確認ポイント2：攻撃者の戦術・技術・手順をまとめた行動特性

TTPの説明として最も適切なものはどれか。

A. 公開情報から必要な情報を収集・分析する活動
B. 攻撃者の戦術・技術・手順をまとめた行動特性
C. 脅威情報をサービス間で交換するための通信仕様
D. 侵入後に組織内の別端末やアカウントへ横展開する行動

答え・解説

Q0020 正答：B. 攻撃者の戦術・技術・手順をまとめた行動特性

解説：TTPの要点は「攻撃者の戦術・技術・手順をまとめた行動特性」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0021

脅威インテリジェンス・攻撃分析
タグ：TTP
用語：TTPの確認ポイント3：攻撃者の戦術・技術・手順をまとめた行動特性

用語と説明の組合せとして適切なものはどれか。論点は「TTP」である。

A. OSINT：攻撃者の戦術・技術・手順をまとめた行動特性
B. TAXII：攻撃者の戦術・技術・手順をまとめた行動特性
C. TTP：攻撃者の戦術・技術・手順をまとめた行動特性
D. ラテラルムーブメント：攻撃者の戦術・技術・手順をまとめた行動特性

答え・解説

Q0021 正答：C. TTP：攻撃者の戦術・技術・手順をまとめた行動特性

解説：正しい組合せは「TTP：攻撃者の戦術・技術・手順をまとめた行動特性」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0022

脅威インテリジェンス・攻撃分析
タグ：TTP
用語：TTPの確認ポイント4：攻撃者の戦術・技術・手順をまとめた行動特性

「TTP」は、攻撃者の戦術・技術・手順をまとめた行動特性。

A. ○
B. ×

答え・解説

Q0022 正答：○

解説：正しい。TTPは攻撃者の戦術・技術・手順をまとめた行動特性。実務では対象、目的、前提条件を併せて確認する。

Q0023

脅威インテリジェンス・攻撃分析
タグ：TTP
用語：TTPの確認ポイント5：攻撃者の戦術・技術・手順をまとめた行動特性

組織が「攻撃者の戦術・技術・手順をまとめた行動特性」ために採用すべき概念又は仕組みはどれか。

A. TTP
B. OSINT
C. TAXII
D. ラテラルムーブメント

答え・解説

Q0023 正答：A. TTP

解説：この目的に対応するのはTTPである。攻撃者の戦術・技術・手順をまとめた行動特性という機能・考え方を持つためである。

Q0024

脅威インテリジェンス・攻撃分析
タグ：TTP
用語：TTPの確認ポイント6：攻撃者の戦術・技術・手順をまとめた行動特性

「TTP」について、誤解を避けるための説明として最も適切なものはどれか。

A. 侵入後に組織内の別端末やアカウントへ横展開する行動
B. 攻撃者の戦術・技術・手順をまとめた行動特性
C. 脅威情報をサービス間で交換するための通信仕様
D. 公開情報から必要な情報を収集・分析する活動

答え・解説

Q0024 正答：B. 攻撃者の戦術・技術・手順をまとめた行動特性

解説：TTPは攻撃者の戦術・技術・手順をまとめた行動特性。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0025

脅威インテリジェンス・攻撃分析
タグ：TTP
用語：TTPの確認ポイント7：攻撃者の戦術・技術・手順をまとめた行動特性
「TTP」は、公開情報から必要な情報を収集・分析する活動。

A. ○
B. ×

答え・解説

Q0025 正答：×
解説：誤り。記述はOSINTの説明である。TTPは攻撃者の戦術・技術・手順をまとめた行動特性。

Q0026

脅威インテリジェンス・攻撃分析
タグ：TTP
用語：TTPの確認ポイント8：攻撃者の戦術・技術・手順をまとめた行動特性
次の状況で中心となる論点はどれか。「攻撃者の戦術・技術・手順をまとめた行動特性」ことが求められている。

A. TAXII
B. ラテラルムーブメント
C. OSINT
D. TTP

答え・解説

Q0026 正答：D. TTP
解説：中心となる論点はTTPである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0027

脅威インテリジェンス・攻撃分析
タグ：TTP
用語：TTPの確認ポイント9：攻撃者の戦術・技術・手順をまとめた行動特性
「攻撃者の戦術・技術・手順をまとめた行動特性」という特徴を持つものを選べ。

A. TTP
B. ラテラルムーブメント
C. TAXII
D. OSINT

答え・解説

Q0027 正答：A. TTP
解説：TTPが該当する。定義は攻撃者の戦術・技術・手順をまとめた行動特性であり、他の候補とは機能が異なる。

Q0028

脅威インテリジェンス・攻撃分析
タグ：OSINT
用語：OSINTの確認ポイント1：公開情報から必要な情報を収集・分析する活動
次の説明に最も合う用語はどれか。公開情報から必要な情報を収集・分析する活動

A. STIX
B. OSINT
C. マルウェアサンドボックス
D. サイバーキルチェーン

答え・解説

Q0028 正答：B. OSINT
解説：OSINTは、公開情報から必要な情報を収集・分析する活動。ほかの選択肢は目的又は適用場面が異なる。

Q0029

脅威インテリジェンス・攻撃分析
タグ：OSINT
用語：OSINTの確認ポイント2：公開情報から必要な情報を収集・分析する活動

OSINTの説明として最も適切なものはどれか。

A. サイバー脅威情報を構造化して表現する仕様
B. 隔離環境で不審ファイルを実行し挙動を観察する仕組み
C. 公開情報から必要な情報を収集・分析する活動
D. 攻撃を偵察から目的達成までの段階で整理するモデル

答え・解説

Q0029 正答：C. 公開情報から必要な情報を収集・分析する活動

解説：OSINTの要点は「公開情報から必要な情報を収集・分析する活動」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0030

脅威インテリジェンス・攻撃分析
タグ：OSINT
用語：OSINTの確認ポイント3：公開情報から必要な情報を収集・分析する活動

用語と説明の組合せとして適切なものはどれか。論点は「OSINT」である。

A. STIX：公開情報から必要な情報を収集・分析する活動
B. マルウェアサンドボックス：公開情報から必要な情報を収集・分析する活動
C. サイバーキルチェーン：公開情報から必要な情報を収集・分析する活動
D. OSINT：公開情報から必要な情報を収集・分析する活動

答え・解説

Q0030 正答：D. OSINT：公開情報から必要な情報を収集・分析する活動

解説：正しい組合せは「OSINT：公開情報から必要な情報を収集・分析する活動」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0031

脅威インテリジェンス・攻撃分析
タグ：OSINT
用語：OSINTの確認ポイント4：公開情報から必要な情報を収集・分析する活動
「OSINT」は、公開情報から必要な情報を収集・分析する活動。

A. ○
B. ×

答え・解説

Q0031 正答：○
解説：正しい。OSINTは公開情報から必要な情報を収集・分析する活動。実務では対象、目的、前提条件を併せて確認する。

Q0032

脅威インテリジェンス・攻撃分析
タグ：OSINT
用語：OSINTの確認ポイント5：公開情報から必要な情報を収集・分析する活動
組織が「公開情報から必要な情報を収集・分析する活動」ために採用すべき概念又は仕組みはどれか。

A. STIX
B. OSINT
C. マルウェアサンドボックス
D. サイバーキルチェーン

答え・解説

Q0032 正答：B. OSINT
解説：この目的に対応するのはOSINTである。公開情報から必要な情報を収集・分析する活動という機能・考え方を持つためである。

Q0033

脅威インテリジェンス・攻撃分析
タグ：OSINT
用語：OSINTの確認ポイント6：公開情報から必要な情報を収集・分析する活動

「OSINT」について、誤解を避けるための説明として最も適切なものはどれか。

A. 攻撃を偵察から目的達成までの段階で整理するモデル
B. 隔離環境で不審ファイルを実行し挙動を観察する仕組み
C. 公開情報から必要な情報を収集・分析する活動
D. サイバー脅威情報を構造化して表現する仕様

答え・解説

Q0033 正答：C. 公開情報から必要な情報を収集・分析する活動

解説：OSINTは公開情報から必要な情報を収集・分析する活動。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0034

脅威インテリジェンス・攻撃分析
タグ：OSINT
用語：OSINTの確認ポイント7：公開情報から必要な情報を収集・分析する活動

「OSINT」は、サイバー脅威情報を構造化して表現する仕様。

A. ○
B. ×

答え・解説

Q0034 正答：×

解説：誤り。記述はSTIXの説明である。OSINTは公開情報から必要な情報を収集・分析する活動。

Q0035

脅威インテリジェンス・攻撃分析
タグ：OSINT
用語：OSINTの確認ポイント8：公開情報から必要な情報を収集・分析する活動
次の状況で中心となる論点はどれか。「公開情報から必要な情報を収集・分析する活動」ことが求められている。

A. OSINT
B. マルウェアサンドボックス
C. サイバーキルチェーン
D. STIX

答え・解説

Q0035 正答：A. OSINT
解説：中心となる論点はOSINTである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0036

脅威インテリジェンス・攻撃分析
タグ：OSINT
用語：OSINTの確認ポイント9：公開情報から必要な情報を収集・分析する活動
「公開情報から必要な情報を収集・分析する活動」という特徴を持つものを選べ。

A. サイバーキルチェーン
B. OSINT
C. マルウェアサンドボックス
D. STIX

答え・解説

Q0036 正答：B. OSINT
解説：OSINTが該当する。定義は公開情報から必要な情報を収集・分析する活動であり、他の候補とは機能が異なる。

Q0037

脅威インテリジェンス・攻撃分析
タグ：STIX
用語：STIXの確認ポイント1：サイバー脅威情報を構造化して表現する仕様

次の説明に最も合う用語はどれか。サイバー脅威情報を構造化して表現する仕様

A. TAXII
B. フィッシング分析
C. STIX
D. MITRE ATT&CK

答え・解説

Q0037 正答：C. STIX

解説：STIXは、サイバー脅威情報を構造化して表現する仕様。ほかの選択肢は目的又は適用場面が異なる。

Q0038

脅威インテリジェンス・攻撃分析
タグ：STIX
用語：STIXの確認ポイント2：サイバー脅威情報を構造化して表現する仕様

STIXの説明として最も適切なものはどれか。

A. 脅威情報をサービス間で交換するための通信仕様
B. 送信元、URL、ヘッダ、添付、誘導内容などを調べる活動
C. 実際の攻撃者の戦術と技術を体系化した知識ベース
D. サイバー脅威情報を構造化して表現する仕様

答え・解説

Q0038 正答：D. サイバー脅威情報を構造化して表現する仕様

解説：STIXの要点は「サイバー脅威情報を構造化して表現する仕様」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0039

脅威インテリジェンス・攻撃分析
タグ：STIX
用語：STIXの確認ポイント3：サイバー脅威情報を構造化して表現する仕様

用語と説明の組合せとして適切なものはどれか。論点は「STIX」である。

A. STIX：サイバー脅威情報を構造化して表現する仕様
B. TAXII：サイバー脅威情報を構造化して表現する仕様
C. フィッシング分析：サイバー脅威情報を構造化して表現する仕様
D. MITRE ATT&CK：サイバー脅威情報を構造化して表現する仕様

答え・解説

Q0039 正答：A. STIX：サイバー脅威情報を構造化して表現する仕様

解説：正しい組合せは「STIX：サイバー脅威情報を構造化して表現する仕様」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0040

脅威インテリジェンス・攻撃分析
タグ：STIX
用語：STIXの確認ポイント4：サイバー脅威情報を構造化して表現する仕様

「STIX」は、サイバー脅威情報を構造化して表現する仕様。

A. ○
B. ×

答え・解説

Q0040 正答：○

解説：正しい。STIXはサイバー脅威情報を構造化して表現する仕様。実務では対象、目的、前提条件を併せて確認する。

Q0041

脅威インテリジェンス・攻撃分析
タグ：STIX
用語：STIXの確認ポイント5：サイバー脅威情報を構造化して表現する仕様

組織が「サイバー脅威情報を構造化して表現する仕様」ために採用すべき概念又は仕組みはどれか。

A. TAXII
B. フィッシング分析
C. STIX
D. MITRE ATT&CK

答え・解説

Q0041 正答：C. STIX
解説：この目的に対応するのはSTIXである。サイバー脅威情報を構造化して表現する仕様という機能・考え方を持つためである。

Q0042

脅威インテリジェンス・攻撃分析
タグ：STIX
用語：STIXの確認ポイント6：サイバー脅威情報を構造化して表現する仕様

「STIX」について、誤解を避けるための説明として最も適切なものはどれか。

A. 実際の攻撃者の戦術と技術を体系化した知識ベース
B. 送信元、URL、ヘッダ、添付、誘導内容などを調べる活動
C. 脅威情報をサービス間で交換するための通信仕様
D. サイバー脅威情報を構造化して表現する仕様

答え・解説

Q0042 正答：D. サイバー脅威情報を構造化して表現する仕様
解説：STIXはサイバー脅威情報を構造化して表現する仕様。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0043

脅威インテリジェンス・攻撃分析
タグ：STIX
用語：STIXの確認ポイント7：サイバー脅威情報を構造化して表現する仕様

「STIX」は、脅威情報をサービス間で交換するための通信仕様。

A. ○
B. ×

答え・解説

Q0043 正答：×

解説：誤り。記述はTAXIIの説明である。STIXはサイバー脅威情報を構造化して表現する仕様。

Q0044

脅威インテリジェンス・攻撃分析
タグ：STIX
用語：STIXの確認ポイント8：サイバー脅威情報を構造化して表現する仕様

次の状況で中心となる論点はどれか。「サイバー脅威情報を構造化して表現する仕様」ことが求められている。

A. フィッシング分析
B. STIX
C. MITRE ATT&CK
D. TAXII

答え・解説

Q0044 正答：B. STIX

解説：中心となる論点はSTIXである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0045

脅威インテリジェンス・攻撃分析
タグ：STIX
用語：STIXの確認ポイント9：サイバー脅威情報を構造化して表現する仕様

「サイバー脅威情報を構造化して表現する仕様」という特徴を持つものを選べ。

A. MITRE ATT&CK
B. フィッシング分析
C. STIX
D. TAXII

答え・解説

Q0045 正答：C. STIX

解説：STIXが該当する。定義はサイバー脅威情報を構造化して表現する仕様であり、他の候補とは機能が異なる。

Q0046

脅威インテリジェンス・攻撃分析
タグ：TAXII
用語：TAXIIの確認ポイント1：脅威情報をサービス間で交換するための通信仕様

次の説明に最も合う用語はどれか。脅威情報をサービス間で交換するための通信仕様

A. マルウェアサンドボックス
B. C2通信
C. TTP
D. TAXII

答え・解説

Q0046 正答：D. TAXII

解説：TAXIIは、脅威情報をサービス間で交換するための通信仕様。ほかの選択肢は目的又は適用場面が異なる。

Q0047

脅威インテリジェンス・攻撃分析
タグ：TAXII
用語：TAXIIの確認ポイント2：脅威情報をサービス間で交換するための通信仕様

TAXIIの説明として最も適切なものはどれか。

A. 脅威情報をサービス間で交換するための通信仕様
B. 隔離環境で不審ファイルを実行し挙動を観察する仕組み
C. 攻撃者が侵害端末へ指令を送り結果を受け取る通信
D. 攻撃者の戦術・技術・手順をまとめた行動特性

答え・解説

Q0047 正答：A. 脅威情報をサービス間で交換するための通信仕様

解説：TAXIIの要点は「脅威情報をサービス間で交換するための通信仕様」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0048

脅威インテリジェンス・攻撃分析
タグ：TAXII
用語：TAXIIの確認ポイント3：脅威情報をサービス間で交換するための通信仕様

用語と説明の組合せとして適切なものはどれか。論点は「TAXII」である。

A. マルウェアサンドボックス：脅威情報をサービス間で交換するための通信仕様
B. TAXII：脅威情報をサービス間で交換するための通信仕様
C. C2通信：脅威情報をサービス間で交換するための通信仕様
D. TTP：脅威情報をサービス間で交換するための通信仕様

答え・解説

Q0048 正答：B. TAXII：脅威情報をサービス間で交換するための通信仕様

解説：正しい組合せは「TAXII：脅威情報をサービス間で交換するための通信仕様」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0049

脅威インテリジェンス・攻撃分析
タグ：TAXII
用語：TAXIIの確認ポイント4：脅威情報をサービス間で交換するための通信仕様

「TAXII」は、脅威情報をサービス間で交換するための通信仕様。

A. ○
B. ×

答え・解説

Q0049 正答：○

解説：正しい。TAXIIは脅威情報をサービス間で交換するための通信仕様。実務では対象、目的、前提条件を併せて確認する。

Q0050

脅威インテリジェンス・攻撃分析
タグ：TAXII
用語：TAXIIの確認ポイント5：脅威情報をサービス間で交換するための通信仕様

組織が「脅威情報をサービス間で交換するための通信仕様」ために採用すべき概念又は仕組みはどれか。

A. マルウェアサンドボックス
B. C2通信
C. TTP
D. TAXII

答え・解説

Q0050 正答：D. TAXII

解説：この目的に対応するのはTAXIIである。脅威情報をサービス間で交換するための通信仕様という機能・考え方を持つためである。

Q0051

脅威インテリジェンス・攻撃分析
タグ：TAXII
用語：TAXIIの確認ポイント6：脅威情報をサービス間で交換するための通信仕様

「TAXII」について、誤解を避けるための説明として最も適切なものはどれか。

A. 脅威情報をサービス間で交換するための通信仕様
B. 攻撃者の戦術・技術・手順をまとめた行動特性
C. 攻撃者が侵害端末へ指令を送り結果を受け取る通信
D. 隔離環境で不審ファイルを実行し挙動を観察する仕組み

答え・解説

Q0051 正答：A. 脅威情報をサービス間で交換するための通信仕様
解説：TAXIIは脅威情報をサービス間で交換するための通信仕様。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0052

脅威インテリジェンス・攻撃分析
タグ：TAXII
用語：TAXIIの確認ポイント7：脅威情報をサービス間で交換するための通信仕様

「TAXII」は、隔離環境で不審ファイルを実行し挙動を観察する仕組み。

A. ○
B. ×

答え・解説

Q0052 正答：×
解説：誤り。記述はマルウェアサンドボックスの説明である。TAXIIは脅威情報をサービス間で交換するための通信仕様。

Q0053

脅威インテリジェンス・攻撃分析
タグ：TAXII
用語：TAXIIの確認ポイント8：脅威情報をサービス間で交換するための通信仕様

次の状況で中心となる論点はどれか。「脅威情報をサービス間で交換するための通信仕様」ことが求められている。

A. C2通信
B. TTP
C. TAXII
D. マルウェアサンドボックス

答え・解説

Q0053 正答：C. TAXII
解説：中心となる論点はTAXIIである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0054

脅威インテリジェンス・攻撃分析
タグ：TAXII
用語：TAXIIの確認ポイント9：脅威情報をサービス間で交換するための通信仕様

「脅威情報をサービス間で交換するための通信仕様」という特徴を持つものを選べ。

A. TTP
B. C2通信
C. マルウェアサンドボックス
D. TAXII

答え・解説

Q0054 正答：D. TAXII
解説：TAXIIが該当する。定義は脅威情報をサービス間で交換するための通信仕様であり、他の候補とは機能が異なる。

Q0055

脅威インテリジェンス・攻撃分析
タグ：マルウェアサンドボックス
用語：マルウェアサンドボックスの確認ポイント1：隔離環境で不審ファイルを実行し挙動を観察する仕組み

次の説明に最も合う用語はどれか。隔離環境で不審ファイルを実行し挙動を観察する仕組み

A. マルウェアサンドボックス
B. フィッシング分析
C. ラテラルムーブメント
D. OSINT

答え・解説

Q0055 正答：A. マルウェアサンドボックス

解説：マルウェアサンドボックスは、隔離環境で不審ファイルを実行し挙動を観察する仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0056

脅威インテリジェンス・攻撃分析
タグ：マルウェアサンドボックス
用語：マルウェアサンドボックスの確認ポイント2：隔離環境で不審ファイルを実行し挙動を観察する仕組み

マルウェアサンドボックスの説明として最も適切なものはどれか。

A. 送信元、URL、ヘッダ、添付、誘導内容などを調べる活動
B. 隔離環境で不審ファイルを実行し挙動を観察する仕組み
C. 侵入後に組織内の別端末やアカウントへ横展開する行動
D. 公開情報から必要な情報を収集・分析する活動

答え・解説

Q0056 正答：B. 隔離環境で不審ファイルを実行し挙動を観察する仕組み

解説：マルウェアサンドボックスの要点は「隔離環境で不審ファイルを実行し挙動を観察する仕組み」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0057

脅威インテリジェンス・攻撃分析
タグ：マルウェアサンドボックス
用語：マルウェアサンドボックスの確認ポイント3：隔離環境で不審ファイルを実行し挙動を観察する仕組み

用語と説明の組合せとして適切なものはどれか。論点は「マルウェアサンドボックス」である。

A. フィッシング分析：隔離環境で不審ファイルを実行し挙動を観察する仕組み
B. ラテラルムーブメント：隔離環境で不審ファイルを実行し挙動を観察する仕組み
C. マルウェアサンドボックス：隔離環境で不審ファイルを実行し挙動を観察する仕組み
D. OSINT：隔離環境で不審ファイルを実行し挙動を観察する仕組み

答え・解説

Q0057 正答：C. マルウェアサンドボックス：隔離環境で不審ファイルを実行し挙動を観察する仕組み

解説：正しい組合せは「マルウェアサンドボックス：隔離環境で不審ファイルを実行し挙動を観察する仕組み」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0058

脅威インテリジェンス・攻撃分析
タグ：マルウェアサンドボックス
用語：マルウェアサンドボックスの確認ポイント4：隔離環境で不審ファイルを実行し挙動を観察する仕組み

「マルウェアサンドボックス」は、隔離環境で不審ファイルを実行し挙動を観察する仕組み。

A. ○
B. ×

答え・解説

Q0058 正答：○

解説：正しい。マルウェアサンドボックスは隔離環境で不審ファイルを実行し挙動を観察する仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0059

脅威インテリジェンス・攻撃分析
タグ：マルウェアサンドボックス
用語：マルウェアサンドボックスの確認ポイント5：隔離環境で不審ファイルを実行し挙動を観察する仕組み

組織が「隔離環境で不審ファイルを実行し挙動を観察する仕組み」ために採用すべき概念又は仕組みはどれか。

A. マルウェアサンドボックス
B. フィッシング分析
C. ラテラルムーブメント
D. OSINT

答え・解説

Q0059 正答：A. マルウェアサンドボックス
解説：この目的に対応するのはマルウェアサンドボックスである。隔離環境で不審ファイルを実行し挙動を観察する仕組みという機能・考え方を持つためである。

Q0060

脅威インテリジェンス・攻撃分析
タグ：マルウェアサンドボックス
用語：マルウェアサンドボックスの確認ポイント6：隔離環境で不審ファイルを実行し挙動を観察する仕組み

「マルウェアサンドボックス」について、誤解を避けるための説明として最も適切なものはどれか。

A. 公開情報から必要な情報を収集・分析する活動
B. 隔離環境で不審ファイルを実行し挙動を観察する仕組み
C. 侵入後に組織内の別端末やアカウントへ横展開する行動
D. 送信元、URL、ヘッダ、添付、誘導内容などを調べる活動

答え・解説

Q0060 正答：B. 隔離環境で不審ファイルを実行し挙動を観察する仕組み
解説：マルウェアサンドボックスは隔離環境で不審ファイルを実行し挙動を観察する仕組み。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0061

脅威インテリジェンス・攻撃分析
タグ：マルウェアサンドボックス
用語：マルウェアサンドボックスの確認ポイント7：隔離環境で不審ファイルを実行し挙動を観察する仕組み
「マルウェアサンドボックス」は、送信元、URL、ヘッダ、添付、誘導内容などを調べる活動。
A. ○
B. ×

答え・解説

Q0061 正答：×
解説：誤り。記述はフィッシング分析の説明である。マルウェアサンドボックスは隔離環境で不審ファイルを実行し挙動を観察する仕組み。

Q0062

脅威インテリジェンス・攻撃分析
タグ：マルウェアサンドボックス
用語：マルウェアサンドボックスの確認ポイント8：隔離環境で不審ファイルを実行し挙動を観察する仕組み
次の状況で中心となる論点はどれか。「隔離環境で不審ファイルを実行し挙動を観察する仕組み」ことが求められている。
A. ラテラルムーブメント
B. OSINT
C. フィッシング分析
D. マルウェアサンドボックス

答え・解説

Q0062 正答：D. マルウェアサンドボックス
解説：中心となる論点はマルウェアサンドボックスである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0063

脅威インテリジェンス・攻撃分析
タグ：マルウェアサンドボックス
用語：マルウェアサンドボックスの確認ポイント9：隔離環境で不審ファイルを実行し挙動を観察する仕組み

「隔離環境で不審ファイルを実行し挙動を観察する仕組み」という特徴を持つものを選べ。

A. マルウェアサンドボックス
B. OSINT
C. ラテラルムーブメント
D. フィッシング分析

答え・解説

Q0063 正答：A. マルウェアサンドボックス

解説：マルウェアサンドボックスが該当する。定義は隔離環境で不審ファイルを実行し挙動を観察する仕組みであり、他の候補とは機能が異なる。

Q0064

脅威インテリジェンス・攻撃分析
タグ：フィッシング分析
用語：フィッシング分析の確認ポイント1：送信元、URL、ヘッダ、添付、誘導内容などを調べる活動

次の説明に最も合う用語はどれか。送信元、URL、ヘッダ、添付、誘導内容などを調べる活動

A. C2通信
B. フィッシング分析
C. サイバーキルチェーン
D. STIX

答え・解説

Q0064 正答：B. フィッシング分析

解説：フィッシング分析は、送信元、URL、ヘッダ、添付、誘導内容などを調べる活動。ほかの選択肢は目的又は適用場面が異なる。

Q0065

脅威インテリジェンス・攻撃分析
タグ：フィッシング分析
用語：フィッシング分析の確認ポイント2：送信元、URL、ヘッダ、添付、誘導内容などを調べる活動

フィッシング分析の説明として最も適切なものはどれか。

A. 攻撃者が侵害端末へ指令を送り結果を受け取る通信
B. 攻撃を偵察から目的達成までの段階で整理するモデル
C. 送信元、URL、ヘッダ、添付、誘導内容などを調べる活動
D. サイバー脅威情報を構造化して表現する仕様

答え・解説

Q0065 正答：C. 送信元、URL、ヘッダ、添付、誘導内容などを調べる活動

解説：フィッシング分析の要点は「送信元、URL、ヘッダ、添付、誘導内容などを調べる活動」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0066

脅威インテリジェンス・攻撃分析
タグ：フィッシング分析
用語：フィッシング分析の確認ポイント3：送信元、URL、ヘッダ、添付、誘導内容などを調べる活動

用語と説明の組合せとして適切なものはどれか。論点は「フィッシング分析」である。

A. C2通信：送信元、URL、ヘッダ、添付、誘導内容などを調べる活動
B. サイバーキルチェーン：送信元、URL、ヘッダ、添付、誘導内容などを調べる活動
C. STIX：送信元、URL、ヘッダ、添付、誘導内容などを調べる活動
D. フィッシング分析：送信元、URL、ヘッダ、添付、誘導内容などを調べる活動

答え・解説

Q0066 正答：D. フィッシング分析：送信元、URL、ヘッダ、添付、誘導内容などを調べる活動

解説：正しい組合せは「フィッシング分析：送信元、URL、ヘッダ、添付、誘導内容などを調べる活動」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0067

脅威インテリジェンス・攻撃分析
タグ：フィッシング分析
用語：フィッシング分析の確認ポイント4：送信元、URL、ヘッダ、添付、誘導内容などを調べる活動

「フィッシング分析」は、送信元、URL、ヘッダ、添付、誘導内容などを調べる活動。

A. ○
B. ×

答え・解説

Q0067 正答：○

解説：正しい。フィッシング分析は送信元、URL、ヘッダ、添付、誘導内容などを調べる活動。実務では対象、目的、前提条件を併せて確認する。

Q0068

脅威インテリジェンス・攻撃分析
タグ：フィッシング分析
用語：フィッシング分析の確認ポイント5：送信元、URL、ヘッダ、添付、誘導内容などを調べる活動

組織が「送信元、URL、ヘッダ、添付、誘導内容などを調べる活動」ために採用すべき概念又は仕組みはどれか。

A. C2通信
B. フィッシング分析
C. サイバーキルチェーン
D. STIX

答え・解説

Q0068 正答：B. フィッシング分析

解説：この目的に対応するのはフィッシング分析である。送信元、URL、ヘッダ、添付、誘導内容などを調べる活動という機能・考え方を持つためである。

Q0069

脅威インテリジェンス・攻撃分析
タグ：フィッシング分析
用語：フィッシング分析の確認ポイント6：送信元、URL、ヘッダ、添付、誘導内容などを調べる活動

「フィッシング分析」について、誤解を避けるための説明として最も適切なものはどれか。

A. サイバー脅威情報を構造化して表現する仕様
B. 攻撃を偵察から目的達成までの段階で整理するモデル
C. 送信元、URL、ヘッダ、添付、誘導内容などを調べる活動
D. 攻撃者が侵害端末へ指令を送り結果を受け取る通信

答え・解説

Q0069 正答：C. 送信元、URL、ヘッダ、添付、誘導内容などを調べる活動
解説：フィッシング分析は送信元、URL、ヘッダ、添付、誘導内容などを調べる活動。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0070

脅威インテリジェンス・攻撃分析
タグ：フィッシング分析
用語：フィッシング分析の確認ポイント7：送信元、URL、ヘッダ、添付、誘導内容などを調べる活動

「フィッシング分析」は、攻撃者が侵害端末へ指令を送り結果を受け取る通信。

A. ○
B. ×

答え・解説

Q0070 正答：×
解説：誤り。記述はC2通信の説明である。フィッシング分析は送信元、URL、ヘッダ、添付、誘導内容などを調べる活動。

Q0071

脅威インテリジェンス・攻撃分析
タグ：フィッシング分析
用語：フィッシング分析の確認ポイント8：送信元、URL、ヘッダ、添付、誘導内容などを調べる活動

次の状況で中心となる論点はどれか。「送信元、URL、ヘッダ、添付、誘導内容などを調べる活動」ことが求められている。

A. フィッシング分析
B. サイバーキルチェーン
C. STIX
D. C2通信

答え・解説

Q0071 正答：A. フィッシング分析

解説：中心となる論点はフィッシング分析である。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0072

脅威インテリジェンス・攻撃分析
タグ：フィッシング分析
用語：フィッシング分析の確認ポイント9：送信元、URL、ヘッダ、添付、誘導内容などを調べる活動

「送信元、URL、ヘッダ、添付、誘導内容などを調べる活動」という特徴を持つものを選べ。

A. STIX
B. フィッシング分析
C. サイバーキルチェーン
D. C2通信

答え・解説

Q0072 正答：B. フィッシング分析

解説：フィッシング分析が該当する。定義は送信元、URL、ヘッダ、添付、誘導内容などを調べる活動であり、他の候補とは機能が異なる。

Q0073

脅威インテリジェンス・攻撃分析
タグ：C2通信
用語：C2通信の確認ポイント1：攻撃者が侵害端末へ指令を送り結果を受け取る通信

次の説明に最も合う用語はどれか。攻撃者が侵害端末へ指令を送り結果を受け取る通信

A. ラテラルムーブメント
B. MITRE ATT&CK
C. C2通信
D. TAXII

答え・解説

Q0073 正答：C. C2通信

解説：C2通信は、攻撃者が侵害端末へ指令を送り結果を受け取る通信。ほかの選択肢は目的又は適用場面が異なる。

Q0074

脅威インテリジェンス・攻撃分析
タグ：C2通信
用語：C2通信の確認ポイント2：攻撃者が侵害端末へ指令を送り結果を受け取る通信

C2通信の説明として最も適切なものはどれか。

A. 侵入後に組織内の別端末やアカウントへ横展開する行動
B. 実際の攻撃者の戦術と技術を体系化した知識ベース
C. 脅威情報をサービス間で交換するための通信仕様
D. 攻撃者が侵害端末へ指令を送り結果を受け取る通信

答え・解説

Q0074 正答：D. 攻撃者が侵害端末へ指令を送り結果を受け取る通信

解説：C2通信の要点は「攻撃者が侵害端末へ指令を送り結果を受け取る通信」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0075

脅威インテリジェンス・攻撃分析
タグ：C2通信
用語：C2通信の確認ポイント3：攻撃者が侵害端末へ指令を送り結果を受け取る通信
用語と説明の組合せとして適切なものはどれか。論点は「C2通信」である。

A. C2通信：攻撃者が侵害端末へ指令を送り結果を受け取る通信
B. ラテラルムーブメント：攻撃者が侵害端末へ指令を送り結果を受け取る通信
C. MITRE ATT&CK：攻撃者が侵害端末へ指令を送り結果を受け取る通信
D. TAXII：攻撃者が侵害端末へ指令を送り結果を受け取る通信

答え・解説

Q0075 正答：A. C2通信：攻撃者が侵害端末へ指令を送り結果を受け取る通信
解説：正しい組合せは「C2通信：攻撃者が侵害端末へ指令を送り結果を受け取る通信」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0076

脅威インテリジェンス・攻撃分析
タグ：C2通信
用語：C2通信の確認ポイント4：攻撃者が侵害端末へ指令を送り結果を受け取る通信
「C2通信」は、攻撃者が侵害端末へ指令を送り結果を受け取る通信。

A. ○
B. ×

答え・解説

Q0076 正答：○
解説：正しい。C2通信は攻撃者が侵害端末へ指令を送り結果を受け取る通信。実務では対象、目的、前提条件を併せて確認する。

Q0077

脅威インテリジェンス・攻撃分析
タグ：C2通信
用語：C2通信の確認ポイント5：攻撃者が侵害端末へ指令を送り結果を受け取る通信
組織が「攻撃者が侵害端末へ指令を送り結果を受け取る通信」ために採用すべき概念又は仕組みはどれか。

A. ラテラルムーブメント
B. MITRE ATT&CK
C. C2通信
D. TAXII

答え・解説

Q0077 正答：C. C2通信
解説：この目的に対応するのはC2通信である。攻撃者が侵害端末へ指令を送り結果を受け取る通信という機能・考え方を持つためである。

Q0078

脅威インテリジェンス・攻撃分析
タグ：C2通信
用語：C2通信の確認ポイント6：攻撃者が侵害端末へ指令を送り結果を受け取る通信
「C2通信」について、誤解を避けるための説明として最も適切なものはどれか。

A. 脅威情報をサービス間で交換するための通信仕様
B. 実際の攻撃者の戦術と技術を体系化した知識ベース
C. 侵入後に組織内の別端末やアカウントへ横展開する行動
D. 攻撃者が侵害端末へ指令を送り結果を受け取る通信

答え・解説

Q0078 正答：D. 攻撃者が侵害端末へ指令を送り結果を受け取る通信
解説：C2通信は攻撃者が侵害端末へ指令を送り結果を受け取る通信。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0079

脅威インテリジェンス・攻撃分析
タグ：C2通信
用語：C2通信の確認ポイント7：攻撃者が侵害端末へ指令を送り結果を受け取る通信
「C2通信」は、侵入後に組織内の別端末やアカウントへ横展開する行動。

A. ○
B. ×

答え・解説

Q0079 正答：×
解説：誤り。記述はラテラルムーブメントの説明である。C2通信は攻撃者が侵害端末へ指令を送り結果を受け取る通信。

Q0080

脅威インテリジェンス・攻撃分析
タグ：C2通信
用語：C2通信の確認ポイント8：攻撃者が侵害端末へ指令を送り結果を受け取る通信
次の状況で中心となる論点はどれか。「攻撃者が侵害端末へ指令を送り結果を受け取る通信」ことが求められている。

A. MITRE ATT&CK
B. C2通信
C. TAXII
D. ラテラルムーブメント

答え・解説

Q0080 正答：B. C2通信
解説：中心となる論点はC2通信である。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0081

脅威インテリジェンス・攻撃分析
タグ：C2通信
用語：C2通信の確認ポイント9：攻撃者が侵害端末へ指令を送り結果を受け取る通信
「攻撃者が侵害端末へ指令を送り結果を受け取る通信」という特徴を持つものを選べ。

A. TAXII
B. MITRE ATT&CK
C. C2通信
D. ラテラルムーブメント

答え・解説

Q0081 正答：C. C2通信
解説：C2通信が該当する。定義は攻撃者が侵害端末へ指令を送り結果を受け取る通信であり、他の候補とは機能が異なる。

Q0082

脅威インテリジェンス・攻撃分析
タグ：ラテラルムーブメント
用語：ラテラルムーブメントの確認ポイント1：侵入後に組織内の別端末やアカウントへ横展開する行動
次の説明に最も合う用語はどれか。侵入後に組織内の別端末やアカウントへ横展開する行動

A. サイバーキルチェーン
B. TTP
C. マルウェアサンドボックス
D. ラテラルムーブメント

答え・解説

Q0082 正答：D. ラテラルムーブメント
解説：ラテラルムーブメントは、侵入後に組織内の別端末やアカウントへ横展開する行動。ほかの選択肢は目的又は適用場面が異なる。

Q0083

脅威インテリジェンス・攻撃分析
タグ：ラテラルムーブメント
用語：ラテラルムーブメントの確認ポイント2：侵入後に組織内の別端末やアカウントへ横展開する行動

ラテラルムーブメントの説明として最も適切なものはどれか。

A. 侵入後に組織内の別端末やアカウントへ横展開する行動
B. 攻撃を偵察から目的達成までの段階で整理するモデル
C. 攻撃者の戦術・技術・手順をまとめた行動特性
D. 隔離環境で不審ファイルを実行し挙動を観察する仕組み

答え・解説

Q0083 正答：A. 侵入後に組織内の別端末やアカウントへ横展開する行動

解説：ラテラルムーブメントの要点は「侵入後に組織内の別端末やアカウントへ横展開する行動」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0084

脅威インテリジェンス・攻撃分析
タグ：ラテラルムーブメント
用語：ラテラルムーブメントの確認ポイント3：侵入後に組織内の別端末やアカウントへ横展開する行動

用語と説明の組合せとして適切なものはどれか。論点は「ラテラルムーブメント」である。

A. サイバーキルチェーン：侵入後に組織内の別端末やアカウントへ横展開する行動
B. ラテラルムーブメント：侵入後に組織内の別端末やアカウントへ横展開する行動
C. TTP：侵入後に組織内の別端末やアカウントへ横展開する行動
D. マルウェアサンドボックス：侵入後に組織内の別端末やアカウントへ横展開する行動

答え・解説

Q0084 正答：B. ラテラルムーブメント：侵入後に組織内の別端末やアカウントへ横展開する行動

解説：正しい組合せは「ラテラルムーブメント：侵入後に組織内の別端末やアカウントへ横展開する行動」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0085

脅威インテリジェンス・攻撃分析
タグ：ラテラルムーブメント
用語：ラテラルムーブメントの確認ポイント4：侵入後に組織内の別端末やアカウントへ横展開する行動

「ラテラルムーブメント」は、侵入後に組織内の別端末やアカウントへ横展開する行動。

A. ○
B. ×

答え・解説

Q0085 正答：○

解説：正しい。ラテラルムーブメントは侵入後に組織内の別端末やアカウントへ横展開する行動。実務では対象、目的、前提条件を併せて確認する。

Q0086

脅威インテリジェンス・攻撃分析
タグ：ラテラルムーブメント
用語：ラテラルムーブメントの確認ポイント5：侵入後に組織内の別端末やアカウントへ横展開する行動

組織が「侵入後に組織内の別端末やアカウントへ横展開する行動」ために採用すべき概念又は仕組みはどれか。

A. サイバーキルチェーン
B. TTP
C. マルウェアサンドボックス
D. ラテラルムーブメント

答え・解説

Q0086 正答：D. ラテラルムーブメント

解説：この目的に対応するのはラテラルムーブメントである。侵入後に組織内の別端末やアカウントへ横展開する行動という機能・考え方を持つためである。

Q0087

脅威インテリジェンス・攻撃分析
タグ：ラテラルムーブメント
用語：ラテラルムーブメントの確認ポイント6：侵入後に組織内の別端末やアカウントへ横展開する行動

「ラテラルムーブメント」について、誤解を避けるための説明として最も適切なものはどれか。

A. 侵入後に組織内の別端末やアカウントへ横展開する行動
B. 隔離環境で不審ファイルを実行し挙動を観察する仕組み
C. 攻撃者の戦術・技術・手順をまとめた行動特性
D. 攻撃を偵察から目的達成までの段階で整理するモデル

答え・解説

Q0087 正答：A. 侵入後に組織内の別端末やアカウントへ横展開する行動

解説：ラテラルムーブメントは侵入後に組織内の別端末やアカウントへ横展開する行動。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0088

脅威インテリジェンス・攻撃分析
タグ：ラテラルムーブメント
用語：ラテラルムーブメントの確認ポイント7：侵入後に組織内の別端末やアカウントへ横展開する行動

「ラテラルムーブメント」は、攻撃を偵察から目的達成までの段階で整理するモデル。

A. ○
B. ×

答え・解説

Q0088 正答：×

解説：誤り。記述はサイバーキルチェーンの説明である。ラテラルムーブメントは侵入後に組織内の別端末やアカウントへ横展開する行動。

Q0089

脅威インテリジェンス・攻撃分析
タグ：ラテラルムーブメント
用語：ラテラルムーブメントの確認ポイント8：侵入後に組織内の別端末やアカウントへ横展開する行動

次の状況で中心となる論点はどれか。「侵入後に組織内の別端末やアカウントへ横展開する行動」ことが求められている。

A. TTP
B. マルウェアサンドボックス
C. ラテラルムーブメント
D. サイバーキルチェーン

答え・解説

Q0089 正答：C. ラテラルムーブメント

解説：中心となる論点はラテラルムーブメントである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0090

脅威インテリジェンス・攻撃分析
タグ：ラテラルムーブメント
用語：ラテラルムーブメントの確認ポイント9：侵入後に組織内の別端末やアカウントへ横展開する行動

「侵入後に組織内の別端末やアカウントへ横展開する行動」という特徴を持つものを選べ。

A. マルウェアサンドボックス
B. TTP
C. サイバーキルチェーン
D. ラテラルムーブメント

答え・解説

Q0090 正答：D. ラテラルムーブメント

解説：ラテラルムーブメントが該当する。定義は侵入後に組織内の別端末やアカウントへ横展開する行動であり、他の候補とは機能が異なる。