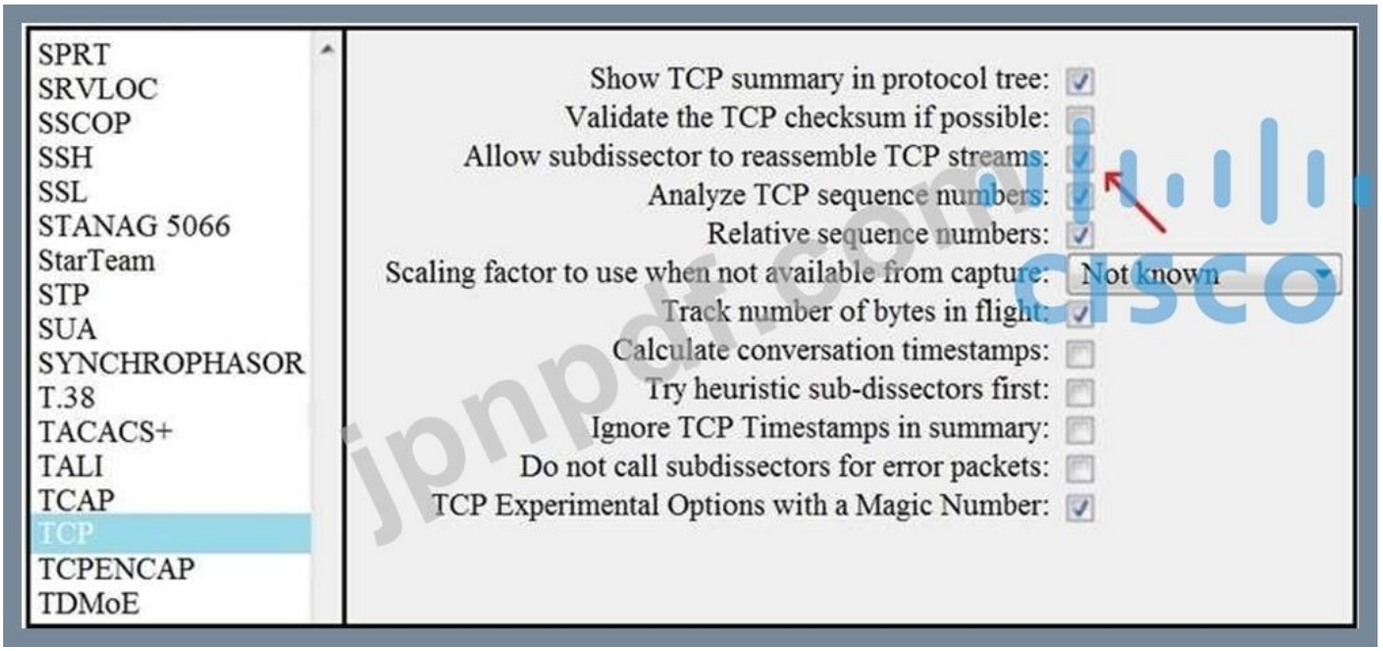
Cisco.200-201.v2023-02-14.q145

試験コード:	200-201
試験名称:	Understanding Cisco Cybersecurity Operations Fundamentals
認定資格:	Cisco
無料問題数:	145
バージョン:	v2023-02-14
アクセス数:	1162
ページビュー数:	1450
https://www.jpnpdf.com/Cisco.200-201.v2023-02-14.q145-mondaishu.html	

最新問題: **1**
攻撃者は、2 人のユーザー間で交換されるネットワーク トラフィックをどのように観察しますか?
A. 中間者
B. コマンド注入
C. サービス拒否
D. ポートスキャン
Answer: A (メーッセージを残す**)**

最新問題: **2**



展示を参照してください。"サブディセクタが TCP ストリームを再構築することを許可する"機能が有効になっている場合、どのような結果が期待されますか?
A. パケット キャプチャからファイルを抽出する

B. TCP サブディセクタを挿入
C. TCP ストリームを無効にする
D. アンフラグメント TCP
Answer: (解答を表示する**)**

最新問題**: 3**
展示を参照してください。

5 タプルの一部である表の 2 つの要素はどれですか? (2つ選んでください。)
A. イニシエータ IP
B. イニシエーター ユーザー
C. ソース ポート
D. 入力セキュリティ ゾーン
E. 最初のパケット
Answer: (解答を表示する**)**

最新問題**: 4**
不正アクセスから保護する必要がある個人を特定できる情報とは?
A. 生年月日
B. 運転免許証番号
C. 性別
D. 郵便番号
Answer: B (メーッセージを残す**)**

最新問題**: 5**
エージェントレス保護と比較した場合、エージェントベースの保護にはどのような利点がありますか?
A. 維持費が安くなる
B. 集中型プラットフォームを提供します
C. すべてのトラフィックをローカルで収集して検出します
D. 多数のデバイスを同時に管理します
Answer: C (メーッセージを残す**)**

ホスト ベースのウイルス対策保護は、エージェント ベースとも呼ばれます。エージェントベースのウイルス対策は、保護されたすべてのマシンで実行されます。エージェントレスのウイルス対策保護は、集中型システムからホストでスキャンを実行します。エージェントレス システムは、複数の OS インスタンスがホスト上で同時に実行される仮想化環境で一般的になっています。仮想化された各システムで実行されているエージェント ベースのウイルス対策は、システム リソースの深刻な浪費になる可能性があります。仮想ホストのエージェントレス アンチウイルスには、仮想ホストで最適化されたスキャン タスクを実行する特別なセキュリティ仮想アプライアンスの使用が含まれます。この例は、VMware の vShield です。

最新問題: **6**
ファイアウォールでディープ パケット インスペクションが調査されるのはどのレイヤーですか?
A. インターネット
B. 輸送
C. データリンク
D. アプリケーション
Answer: (解答を表示する**)**

最新問題: **7**
サンドボックス分析ツールで悪意のあるファイルを特定しました。他のホストによるこのファイルの追加のダウンロードを検索するために必要な分析からのファイル情報はどれですか?
A. ファイル名
B. ファイルの種類
C. ファイルのハッシュ値
D. ファイルサイズ
Answer: C (メーッセージを残す**)**

最新問題: **8**
展示を参照してください。
IP アドレスが 172.18.104.139 のサーバーについて、出力は何を示していますか?
A. サーバーの実行中のプロセス
B. FTP サーバーのポートを開く
C. Web サーバーのポートを開く
D. メールサーバーのポートを開く
Answer: (解答を表示する**)**

最新問題: **9**
エンジニアは、人事部から送信元アドレスが HRjacobm@companycom のフィッシング メールを大量に受け取りました。
このシナリオにおける攻撃者は何ですか?
A. 送信者

B. 受信機
C. フィッシングメール
D. 人事
Answer: (解答を表示する**)**

最新問題**: 10**
エンジニアは、既知の TOR 出口ノードを持つトラフィックがネットワーク上で発生したというセキュリティ アラートを受け取ります。
このトラフィックの影響は?
A. 感染後に通信するランサムウェア
B. データ流出
C. 著作権のあるコンテンツをダウンロードしているユーザー
D. ファイアウォールのユーザー回避
Answer: D (メーッセージを残す**)**

最新問題**: 11**
ユーザーが悪意のある添付ファイルを受信しましたが、実行しませんでした。侵入を分類するカテゴリはどれですか?
A. インストール
B. 武器化
C. 偵察
D. 配送
Answer: D (メーッセージを残す**)**

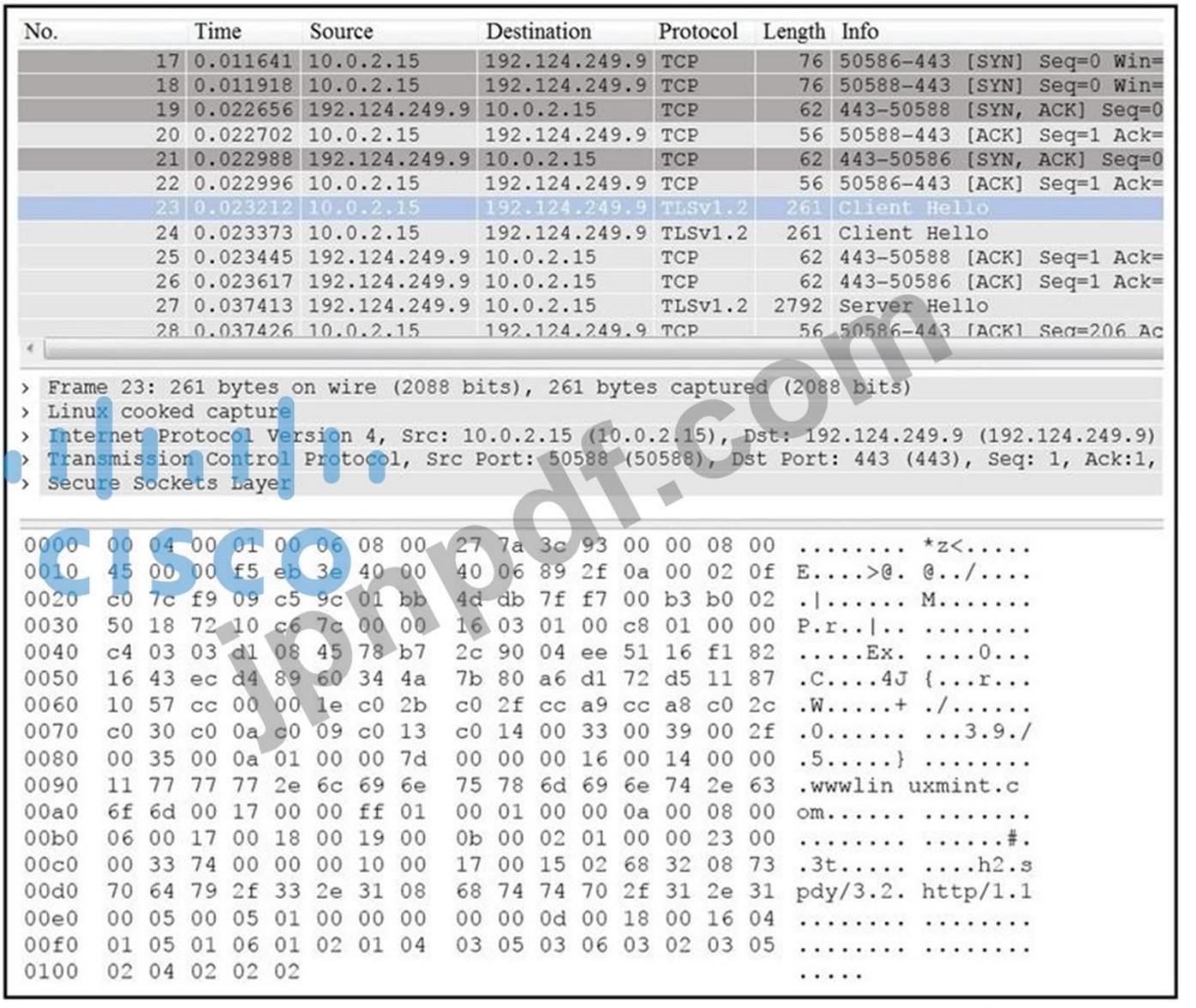
最新問題**: 12**
統計的検出はルールベースの検出とどう違うのですか?
A. 一定期間にわたる正当なデータ。事前定義された一連のルールに基づいて統計的検出が機能します。
B. ルールベースの検出にはイベントの評価が含まれ、統計的検出には評価された一連のイベントが機能することが必要です。
C. 統計的検出にはイベントの評価が含まれ、ルールベースの検出では、評価された一連のイベントが機能する必要があります。
D. 統計的検出により正当なデータが時間の経過とともに定義され、ルールベースの検出が定義済みの一連のルールに基づいて機能します。
Answer: D (メーッセージを残す**)**

最新問題**: 13**
ネットワークのプロファイリングに使用される 2 つの要素はどれですか? 2つ選んでください。)
A. セッション期間
B. 総スループット

C. 実行中のプロセス
D. リスニング ポート
E. OS フィンガープリント
Answer: A,B (メーッセージを残す**)**
説明
ネットワーク プロファイルには、次のような重要な要素を含める必要があります。
総スループット - 特定の送信元から特定の送信先に一定時間内に渡されるデータの量 セッション期間 - データ フローの確立から終了までの時間 使用ポート - 利用可能な TCP または UDP プロセスのリスト重要な資産のアドレス空間 - 重要なシステムまたはデータの IP アドレスまたは論理的な場所 プロファイリング データは、システムが収集したデータであり、これらのデータはインシデント対応とインシデントの検出に役立ちますクリティカル アセット アドレス スペース ホスト プロファイリング = リッスン ポート、ログイン アカウント、実行中のプロセス、実行中のタスク、アプリケーション

最新問題**: 14**
インライン トラフィック調査とトラフィック ミラーリングの違いは何ですか?
A. インライン インスペクションは、元のトラフィック データ フローに作用します。
B. トラフィック ミラーリングは、ライブ トラフィックをブロック用のツールに渡します。
C. トラフィック ミラーリングは、分析と軽減のためにライブ トラフィックを検査します。
D. インライン トラフィックは、分析とセキュリティのためにパケットをコピーします
Answer: A (メーッセージを残す**)**
説明
インライン トラフィック インテロゲーションは、リアルタイムでトラフィックを分析し、特定のトラフィックの転送を防止する機能を備えています トラフィック ミラーリングは、ライブ トラフィックを通過させず、代わりに 1 つまたは複数の送信元ポートからトラフィックをコピーし、コピーしたトラフィックを分析のために 1 つまたは複数の宛先に送信しますネットワーク アナライザまたはその他の監視デバイスによって

最新問題**: 15**
展示を参照してください。



No.	Time	Source	Destination	Protocol	Length	Info
17	0.011641	10.0.2.15	192.124.249.9	TCP	76	50586-443 [SYN] Seq=0 Win=
18	0.011918	10.0.2.15	192.124.249.9	TCP	76	50588-443 [SYN] Seq=0 Win=
19	0.022656	192.124.249.9	10.0.2.15	TCP	62	443-50588 [SYN, ACK] Seq=0
20	0.022702	10.0.2.15	192.124.249.9	TCP	56	50588-443 [ACK] Seq=1 Ack=
21	0.022988	192.124.249.9	10.0.2.15	TCP	62	443-50586 [SYN, ACK] Seq=0
22	0.022996	10.0.2.15	192.124.249.9	TCP	56	50586-443 [ACK] Seq=1 Ack=
23	0.023212	10.0.2.15	192.124.249.9	TLSv1.2	261	Client Hello
24	0.023373	10.0.2.15	192.124.249.9	TLSv1.2	261	Client Hello
25	0.023445	192.124.249.9	10.0.2.15	TCP	62	443-50588 [ACK] Seq=1 Ack=
26	0.023617	192.124.249.9	10.0.2.15	TCP	62	443-50586 [ACK] Seq=1 Ack=
27	0.037413	192.124.249.9	10.0.2.15	TLSv1.2	2792	Server Hello
28	0.037426	10.0.2.15	192.124.249.9	TCP	56	50586-443 [ACK] Seq=206 Ac

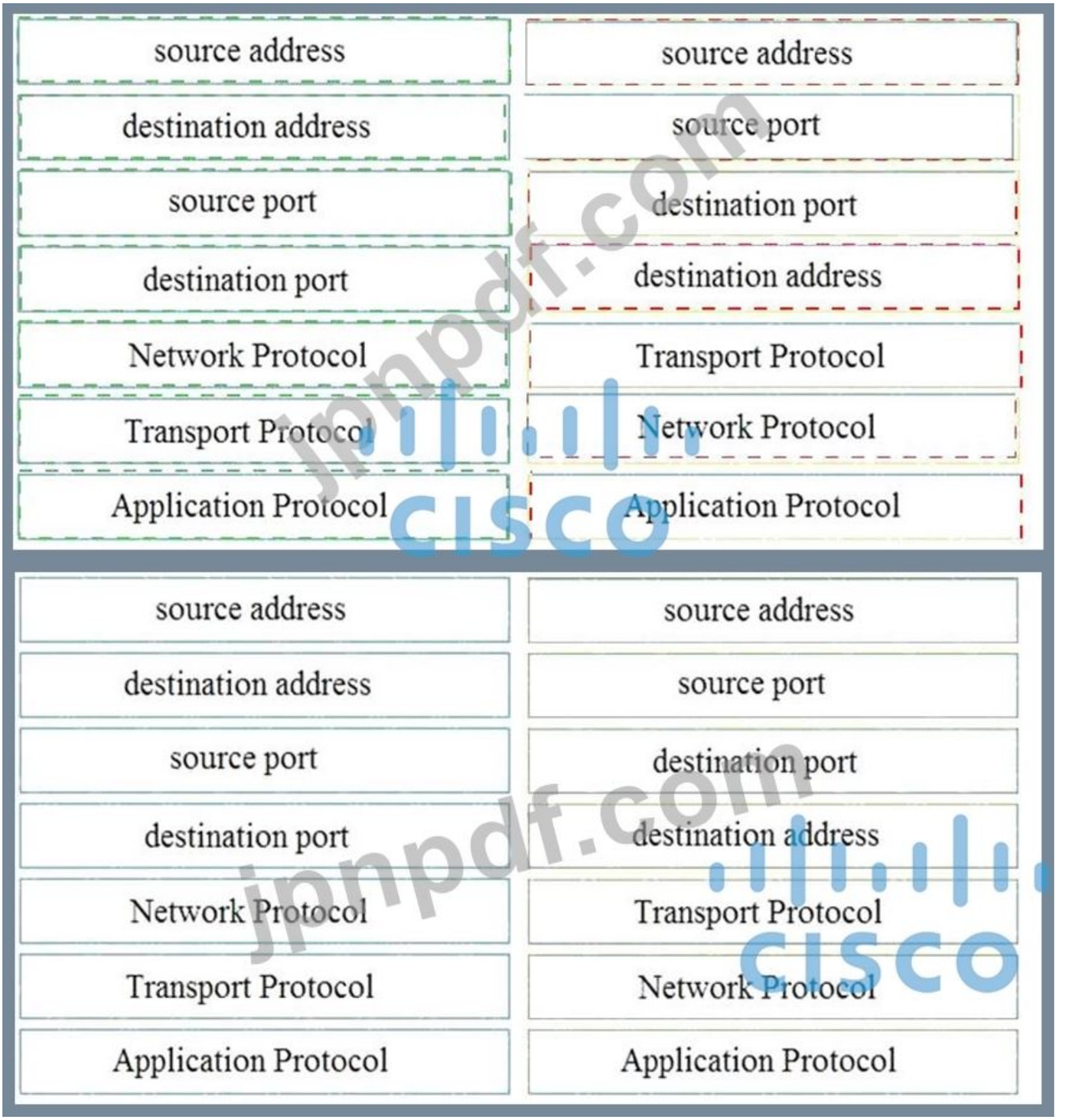
```
> Frame 23: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)
> Linux cooked capture
> Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.249.9)
> Transmission Control Protocol, Src Port: 50588 (50588), Dst Port: 443 (443), Seq: 1, Ack:1,
> Secure Sockets Layer
```

```
0000  00 04 00 01 00 06 08 00  27 7a 3c 93 00 00 08 00  ........ *z<.....
0010  45 00 00 f5 eb 3e 40 00  40 06 89 2f 0a 00 02 0f  E....>@. @../....
0020  c0 7c f9 09 c5 9c 01 bb  4d db 7f f7 00 b3 b0 02  .|...... M.......
0030  50 18 72 10 c6 7c 00 00  16 03 01 00 c8 01 00 00  P.r..|.. ........
0040  c4 03 03 d1 08 45 78 b7  2c 90 04 ee 51 16 f1 82  .....Ex. ....0...
0050  16 43 ec d4 89 60 34 4a  7b 80 a6 d1 72 d5 11 87  .C....4J {...r...
0060  10 57 cc 00 00 1e c0 2b  c0 2f cc a9 cc a8 c0 2c  .W.....+ ./......
0070  c0 30 c0 0a c0 09 c0 13  c0 14 00 33 00 39 00 2f  .0...... ...3.9./
0080  00 35 00 0a 01 00 00 7d  00 00 00 16 00 14 00 00  .5.....} ........
0090  11 77 77 77 2e 6c 69 6e  75 78 6d 69 6e 74 2e 63  .wwwlin uxmint.c
00a0  6f 6d 00 17 00 00 ff 01  00 01 00 00 0a 00 08 00  om...... ........
00b0  06 00 17 00 18 00 19 00  0b 00 02 01 00 00 23 00  ........ ......#.
00c0  00 33 74 00 00 00 10 00  17 00 15 02 68 32 08 73  .3t..... ....h2.s
00d0  70 64 79 2f 33 2e 31 08  68 74 74 70 2f 31 2e 31  pdy/3.2. http/1.1
00e0  00 05 00 05 01 00 00 00  00 00 0d 00 18 00 16 04  ........ ........
00f0  01 05 01 06 01 02 01 04  03 05 03 06 03 02 03 05  ........ ........
0100  02 04 02 02 02                                    .....
```

要素名を左側から右側の PCAP ファイルの正しい部分にドラッグ アンド ドロップします。

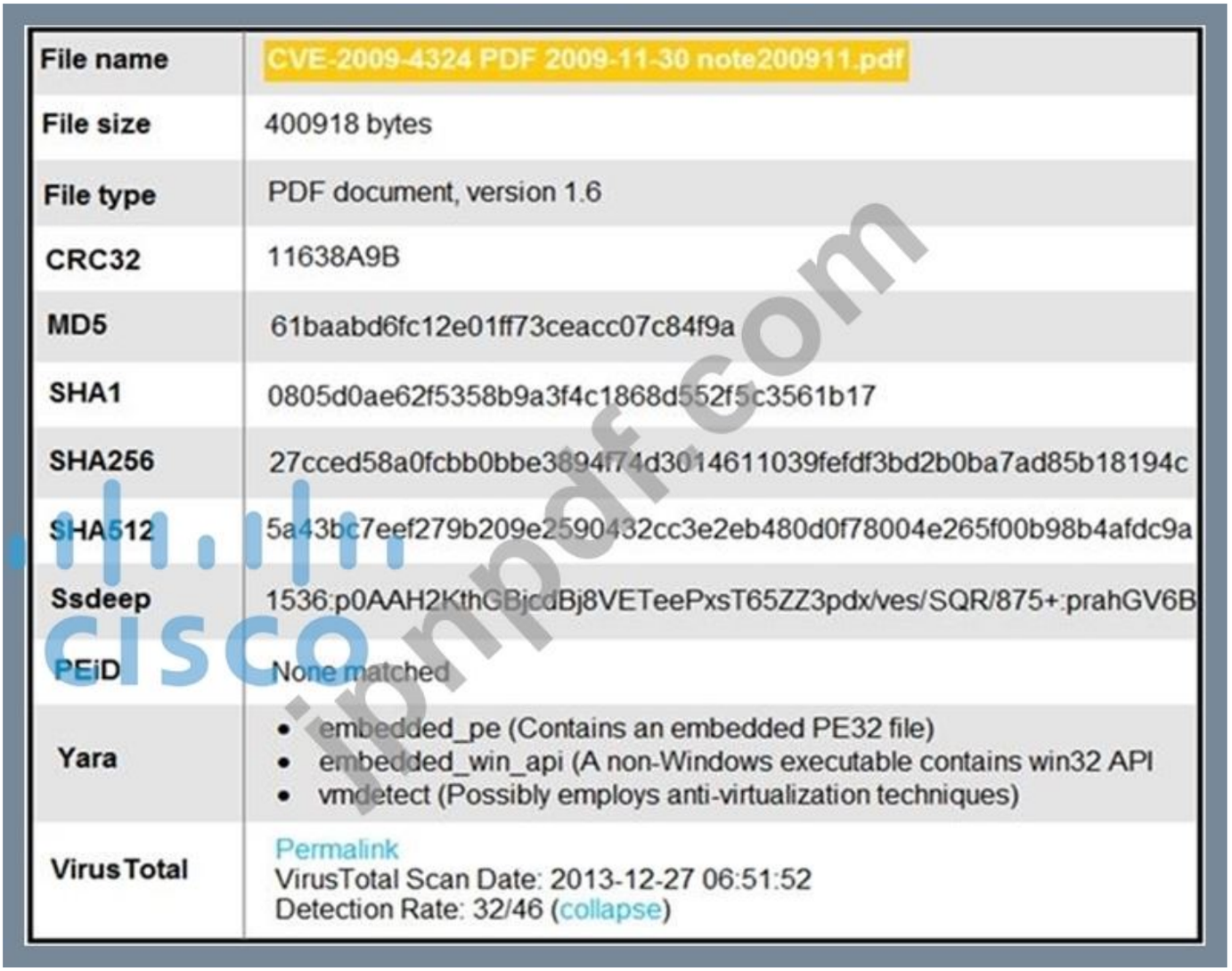
source address	10.0.2.15
destination address	50588
source port	443
destination port	192.124.249.9
Network Protocol	Transmission Control Protocol
Transport Protocol	Internet Protocol v4
Application Protocol	Transport Layer Security v1.2

Answer:



最新問題: **16**

展示を参照してください。



File name	CVE-2009-4324 PDF 2009-11-30 note200911.pdf
File size	400918 bytes
File type	PDF document, version 1.6
CRC32	11638A9B
MD5	61baabd6fc12e01ff73ceacc07c84f9a
SHA1	0805d0ae62f5358b9a3f4c1868d552f5c3561b17
SHA256	27cced58a0fcbb0bbe3894f74d3014611039fefdf3bd2b0ba7ad85b18194c
SHA512	5a43bc7eef279b209e2590432cc3e2eb480d0f78004e265f00b98b4afdc9a
Ssdeep	1536:p0AAH2KthGBjcdBj8VETeePxsT65ZZ3pdx/ves/SQR/875+:prahGV6B
PEiD	None matched
Yara	• embedded_pe (Contains an embedded PE32 file) • embedded_win_api (A non-Windows executable contains win32 API • vmdetect (Possibly employs anti-virtualization techniques)
VirusTotal	Permalink VirusTotal Scan Date: 2013-12-27 06:51:52 Detection Rate: 32/46 (collapse)

エンジニアは、電子メールからダウンロードされた PDF ファイルについて、この Cuckoo Sandbox レポートを分析しています。
このファイルの状態は？

A. ファイルは PEiD 脅威シグネチャと一致しましたが、シグネチャ リストが最新であるため、疑わしい機能は識別されません。

B. ファイルには Windows 32 実行可能ファイルが埋め込まれており、Yara フィールドには詳細な分析のために疑わしい機能がリストされています。

C. ファイルには Windows 以外の実行可能ファイルが埋め込まれていますが、疑わしい機能は識別されません。

D. ファイルには実行可能ファイルが埋め込まれており、詳細な分析のために PEiD 脅威シグネチャと一致しました。

Answer: (解答を表示する**)**

最新問題: **17**
エンジニアは、リモート サーバーが正常なセッションを確立できないという 2 つのサーバー間の接続の問題に対処しています。最初のチェックでは、最初の SYN を送信してセッションを確立しているときに、リモート サーバーが SYN-ACK を受信していないことが示されています。この問題の原因は何ですか?
A. 不正な TCP ハンドシェイク
B. snaplen 構成が正しくありません
C. UDP ハンドシェイクが正しくありません
D. OSI 構成が正しくありません
Answer: A (メーッセージを残す**)**

最新問題: **18**
エンジニアは、TCP 帯域幅の使用状況、応答時間、および遅延を可視化し、詳細なパケット検査と組み合わせて、ネットワーク トラフィック フローによって未知のソフトウェアを特定する必要があります。エンジニアがこの目標を達成するために使用すべき Cisco Application Visibility and Control の 2 つの機能はどれですか? (2つ選んでください。)
A. トラフィック フィルタリング
B. 管理と報告
C. アダプティブ AVC
D. 指標の収集とエクスポート
E. アプリケーションの認識
Answer: B,E (メーッセージを残す**)**

最新問題: **19**
システム管理者は、特定のレジストリ情報が正確であることを確認しています。
HKEY_LOCAL_MACHINE ハイブに含まれる構成情報の種類はどれですか?
A. ファイル拡張子の関連付け
B. システムのハードウェア、ソフトウェア、およびセキュリティの設定
C. 現在ログインしているユーザー (フォルダーとコントロール パネルの設定を含む)
D. ビジュアル設定を含む、システム上のすべてのユーザー
Answer: B (メーッセージを残す**)**
説明
https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users

最新問題: **20**

展示を参照してください。

No.	Time	Source	Destination	Protocol	Length	Info
1878	6.473353	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14404 Ack=2987 Win=65535 Len=0
1986	6.736855	173.37.145.84	10.0.2.15	HTTP	245	HTTP/1.1 304 Not Modified
1987	6.736873	10.0.2.15	173.37.145.84	TCP	56	49522→80 [ACK] Seq=2987 Ack=14593 Win=59640 Len=0
2317	7.245088	10.0.2.15	173.37.145.84	TCP	2976	[TCP segment of a reassembled PDU]
2318	7.245192	10.0.2.15	173.37.145.84	HTTP	1020	GET /web/fw/i/ntpagetag.gif?js=1&ts=1476292607552.286&tc
2321	7.246633	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=4447 Win=65535 Len=0
2322	7.246640	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=5907 Win=65535 Len=0
2323	7.246642	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=6871 Win=65535 Len=0
2542	7.512750	173.37.145.84	10.0.2.15	HTTP	442	HTTP/1.1 200 OK (GIF89a)
2543	7.512781	10.0.2.15	173.37.145.84	TCP	56	49522→80 [ACK] Seq=6871 Ack=14979 Win=62480 Len=0

Wireshark 内で抽出可能なファイルを含むパケットはどれですか?

A. 2318

B. 1986年

C. 2542

D. 2317

Answer: C (メーッセージを残す**)**

最新問題**: 21**

```
# nmap -sV 172.18.104.139

Starting Nmap 7.01 ( https://nmap.org ) at 2020-03-07 11:36 EST
Nmap scan report for 172.18.104.139
Host is up (0.000018s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
25/tcp  open  smtp     Postfix smtpd
110/tcp open  pop3     Dovecot pop3d
143/tcp open  imap     Dovecot imapd
Service Info: Host:   172.18.108.139; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

展示を参照してください。IP アドレスが 172.18.104.139 のサーバーについて、出力は何を示していますか?

A. Web サーバーのポートを開く

B. FTP サーバーのポートを開く

C. メールサーバーのポートを開く

D. サーバーの実行中のプロセス

Answer: (解答を表示する**)**

セクション: セキュリティ監視

最新問題**: 22**

```
GET /item.php?id=34' or sleep(10)
```

展示を参照してください。この要求は、データベースによって駆動される Web アプリケーションサーバーに送信されました。

どのタイプの Web サーバー攻撃が代表されますか?

A. パラメータ操作

B. ヒープ メモリの破損

C. コマンドインジェクション
D. ブラインド SQL インジェクション
Answer: D (メーッセージを残す**)**
セクション: ホストベースの分析

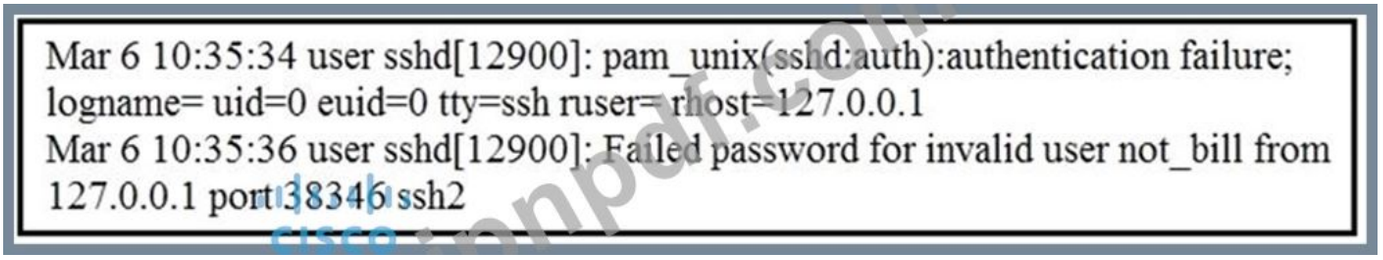
最新問題**: 23**
ソーシャル エンジニアリング攻撃の説明は何ですか?
A. 他人宛の貴重な注文を誤って受け取り、故意に隠したもの
B. 新製品を宣伝するために意図的に間違った受取人に送られたパッケージ
C. ユーザーをだまして機密データを提供させるための無料音楽ダウンロードの偽のオファー
D. 期日とカウンターが記載された、世界中のさまざまな休暇に関する直前のお得な情報を提供するメール
Answer: (解答を表示する**)**

最新問題**: 24**
アナリストは、インターネット上のコマンド アンド コントロール サーバーと通信しているように見えるネットワーク内のホストを調査しています。このパケット キャプチャを収集した後、アナリストは、通信に使用された手法とペイロードを特定できません。

攻撃者が使用している難読化手法はどれですか?
A. Base64 エンコーディング

B. TLS 暗号化
C. SHA-256 ハッシュ
D. ROT13 暗号化
Answer: B (メーッセージを残す)
説明
ROT13 は弱い暗号化と見なされ、TLS (HTTPS:443) では使用されません。ソース：
https://en.wikipedia.org/wiki/ROT13

最新問題: **25**
展示を参照してください。



この出力はどの Linux ログ ファイルにありますか?
A. var/log/var.log
B. /var/log/auth.log
C. /var/log/dmesg
D. /var/log/authorization.log
Answer: B (メーッセージを残す)

最新問題: **26**
脆弱性管理フレームワークの目的は何ですか?
A. ネットワーク上で脆弱性スキャンを実行します
B. 報告された脆弱性のリストを管理します
C. ソース コードの脆弱性を検出して削除します。
D. システムの脆弱性を特定、削除、軽減する
Answer: D (メーッセージを残す)

最新問題: **27**
NetFlow はトラフィック ミラーリングとどう違うのですか?
A. NetFlow はメタデータを収集し、トラフィック ミラーリングはデータを複製します。
B. トラフィック ミラーリングはスイッチのパフォーマンスに影響しますが、NetFlow は影響しません。
C. NetFlow は、トラフィック ミラーリングよりも多くのデータを生成します。
D. トラフィック ミラーリングは、NetFlow よりも運用コストが低くなります。
Answer: A (メーッセージを残す)

最新問題: **28**

IP アドレス 192.168.20.232 を取得するには、どの正規表現が必要ですか?
A. ^ (?:[0-9]f1,3}\.){1,4}
B. ^ (?:[0-9]{1,3}\.)'
C. ^ ([0-9]-{3})
D. ^ (?:[0-9]{1,3}\.){3}[0-9]{1,3}
Answer: D (メーッセージを残す**)**

最新問題**: 29**
RC4 のようなストリーム暗号が同じ鍵で 2 回使用された場合、ネットワークはどの攻撃に対して脆弱ですか?
A. 偽造攻撃
B. 平文のみの攻撃
C. 暗号文のみの攻撃
D. 中間攻撃
Answer: (解答を表示する**)**
解説 -参考：

最新問題**: 30**
インライン トラフィック インテロゲーション (TAPS) とトラフィック ミラーリング (SPAN) の違いは何ですか?
A. SPAN ポートは物理層エラーを除外するため、一部のタイプの分析がより困難になり、TAPS は物理エラーを含むすべてのパケットを受信します。
B. SPAN はより効率的なトラフィック分析を行い、TAPS はミラーリングによる遅延のためにかなり遅くなります。
C. TAPS は完全性を維持するためにトラフィックを複製し、SPAN は他の分析ツールに送信する前にパケットを変更します。
D. トラフィック ミラーリングが追加のタグをデータに適用し、SPAN が整合性を変更せず、全二重ネットワークを提供するため、TAPS の問い合わせはより複雑になります。
Answer: A (メーッセージを残す**)**

最新問題**: 31**
あるエンジニアが、重要なサーバーのパフォーマンス低下に影響するアラートを受け取りました。分析の結果、CPU とメモリの負荷が高いことがわかりました。このリソースの使用状況を調査するためにエンジニアが取るべき次のステップは何ですか?
A. ƀs -m」を実行してデーモンの既存の状態をキャプチャし、必要なプロセスをマップしてギャップを見つけます。
B. "ps -d" を実行して、高負荷プロセスの優先度の状態を下げ、リソースの枯渇を回避します。
C. "ps -ef" を実行して、大量のリソースを消費しているプロセスを把握します。
D. "ps -u" を実行して、サーバーに高い負荷を与えた追加プロセスを誰が実行したかを調べます。
Answer: A (メーッセージを残す**)**

最新問題: **32**
侵入者が悪意のある活動を試み、ユーザーと電子メールを交換し、電子メール配布リストなどの企業情報を受け取りました。侵入者は、ユーザーに電子メール内のリンクを使用するように求めました。fink が起動すると、マシンに感染し、侵入者は企業ネットワークにアクセスできました。侵入者が使用したテスト方法は?
A. ソーシャル エンジニアリング
B. 盗聴
C. おんぶ
D. 共連れ
Answer: (解答を表示する**)**
セクション: セキュリティ監視

最新問題: **33**
攻撃面と攻撃ベクトルの違いは何ですか?
A. 攻撃ベクトルは悪用される可能性のあるコンポーネントと一致し、攻撃面は悪用の潜在的なパスを分類します
B. 攻撃面は、攻撃に対して脆弱な部分を特定し、攻撃ベクトルは、それらの部分に対して実行可能な攻撃を指定します。
C. 攻撃ベクトルは攻撃の潜在的な結果を認識し、攻撃面は攻撃の方法を選択しています。
D. 攻撃面は外部の脆弱性を緩和し、攻撃ベクトルは緩和技術と考えられる回避策を特定します。
Answer: B (メーッセージを残す**)**

最新問題: **34**
シグネチャベースの検出と動作ベースの検出の違いは何ですか?
A. シグネチャ ベースでは、攻撃に関連する可能性のある動作を特定します。動作ベースでは、アラートの前に照合する定義済みの一連のルールがあります。
B. 動作ベースでは、攻撃に関連する可能性のある動作を特定します。一方、シグネチャ ベースでは、アラートの前に照合する定義済みの一連のルールがあります。
C. 動作ベースでは既知の脆弱性データベースを使用しますが、シグネチャ ベースでは既存のデータをインテリジェントに要約します。

D. シグネチャ ベースでは既知の脆弱性データベースが使用され、動作ベースでは既存のデータがインテリジェントに要約されます。
Answer: B (メーッセージを残す**)**
説明
特定のタイプの攻撃に関連するパターンを検索する代わりに、動作ベースの IDS ソリューションは、攻撃に関連する可能性のある動作を監視し、ネットワークが危険にさらされる前に悪意のあるアクションを特定して緩和する可能性を高めます。
https://accedian.com/blog/what-is-the-difference-between-signature-based-and-behavior-based-ids/

最新問題**: 35**
エンジニアは、ネットワーク システムを構成して、コマンド アンド コントロール通信を検出する必要があります。これには、入口と出口の境界トラフィックを解読し、ネットワーク セキュリティ デバイスが悪意のあるアウトバウンド通信を検出できるようにする必要があります。タスクを達成するためにどのテクノロジを使用する必要がありますか?
A. 暗号スイート
B. デジタル証明書
C. 署名
D. 静的 IP アドレス
Answer: B (メーッセージを残す**)**

最新問題**: 36**
SOC 環境における脆弱性管理指標とは?
A. 単一要素認証
B. インターネットに公開されているデバイス
C. コード署名の実施
D. フル アセット スキャン
Answer: (解答を表示する**)**

最新問題**: 37**
エンジニアが Wireshark でトラフィックをフィルタリングして、インターネットのないワークステーションとサーバー間の LAN 10.11.xx のトラフィックのみを表示することで PCAP ファイルをさらに分析できるようにするフィルターはどれですか?
A. ip.src=10.11.0.0/16 および ip.dst=10.11.0.0/16
B. src==10.11.0.0/16 および dst==10.11.0.0/16
C. src=10.11.0.0/16 および dst=10.11.0.0/16
D. ip.src==10.11.0.0/16 および ip.dst==10.11.0.0/16
Answer: D (メーッセージを残す**)**

最新問題**: 38**

脅威とリスクの違いは何ですか？
A. 脅威は、システムの弱点を利用できる潜在的な危険を表します。
B. リスクは、システム内の既知および特定された損失または危険を表します
C. リスクは、システム内の不確実性との意図的でない相互作用を表します
D. 脅威は、物理的または論理的に攻撃または侵害にさらされている状態を表します。
Answer: A (メーッセージを残す**)**
説明
脅威とは、資産に対する潜在的な危険です。脆弱性が存在するが、まだ悪用されていない場合、またはさらに重要なことに、まだ公に知られていない場合、脅威は潜在的であり、まだ認識されていません。

最新問題: **39**
展示を参照してください。

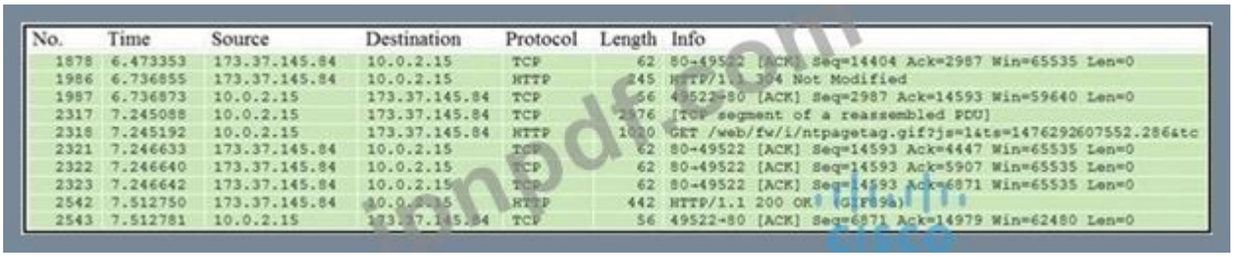
```
Nov 30 17:48:43 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
Nov 30 17:48:44 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:48 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:48 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:48 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:49 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:59 ip-172-31-27-153 sshd[23013]: Invalid user password from 218.26.11.11
Nov 30 17:48:59 ip-172-31-27-153 sshd[23013]: Invalid user password from 218.26.11.11
```

セキュリティ アナリストは、未知の IP アドレスからの異常なアクティビティを調査しています。このファイルはどのタイプの証拠ですか?
A. 最良の証拠
B. 直接証拠
C. 裏付けとなる証拠
D. 間接証拠
Answer: (解答を表示する**)**

最新問題: **40**
データベースからの情報の読み取り、書き込み、または消去に使用される脆弱性の種類はどれですか?
A. SQL インジェクション
B. クロスサイト リクエスト フォージェリ
C. クロスサイト スクリプティング

D. バッファ オーバーフロー
Answer: A (メーッセージを残す**)**

最新問題**: 41**
展示を参照してください。



No.	Time	Source	Destination	Protocol	Length	Info
1878	6.473353	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14404 Ack=2987 Win=65535 Len=0
1986	6.736855	173.37.145.84	10.0.2.15	HTTP	245	HTTP/1.1 304 Not Modified
1987	6.736873	10.0.2.15	173.37.145.84	TCP	56	49522→80 [ACK] Seq=2987 Ack=14593 Win=59640 Len=0
2317	7.245088	10.0.2.15	173.37.145.84	TCP	2976	[TCP segment of a reassembled PDU]
2318	7.245192	10.0.2.15	173.37.145.84	HTTP	1020	GET /web/fw/i/ntpagetag.gif?js=1&ts=1476292607552.286&tc
2321	7.246633	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=4447 Win=65535 Len=0
2322	7.246640	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=5907 Win=65535 Len=0
2323	7.246642	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=6871 Win=65535 Len=0
2542	7.512750	173.37.145.84	10.0.2.15	HTTP	442	HTTP/1.1 200 OK (GIF89a)
2543	7.512781	10.0.2.15	173.37.145.84	TCP	56	49522→80 [ACK] Seq=6871 Ack=14979 Win=62480 Len=0

Wireshark 内で抽出可能なファイルを含むパケットはどれですか?
A. 2317
B. 1986年
C. 2542
D. 2318
Answer: (解答を表示する**)**

最新問題**: 42**
脆弱性管理とは？
A. 侵入ポイントの明確化と絞り込みに重点を置いたセキュリティの実践。
B. 脅威を認識するのではなく、アクションを実行するセキュリティ プラクティス。
C. 既存の弱点を特定して修正するプロセス。
D. サービスの中断から回復し、ビジネスに不可欠なアプリケーションを復元するプロセス
Answer: (解答を表示する**)**

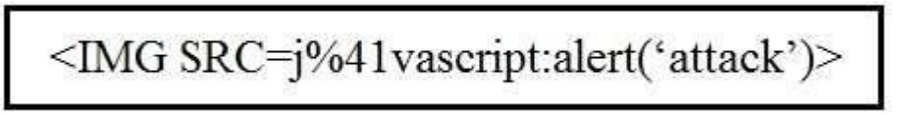
最新問題**: 43**
正当なトラフィックをブロックしてネットワーク トラフィックに影響を与えるシグネチャはどれですか?
A. 偽陰性
B. 偽陽性
C. 真陰性
D. 真陽性
Answer: B (メーッセージを残す**)**

最新問題**: 44**
情報セキュリティの目的の 1 つは、情報とシステムの CIA を保護することです。
この文脈でCIAは何を意味しますか？
A. 機密性、アイデンティティ、および承認
B. 機密性、完全性、および承認
C. 機密性、アイデンティティ、および可用性

D. 機密性、完全性、および可用性
Answer: (解答を表示する**)**
セクション: セキュリティの概念

最新問題**: 45**
セキュリティ エンジニアは、会社のすべての企業 PC に対して、企業全体のホスト/エンドポイント テクノロジを展開します。経営陣はエンジニアに、すべての PC で選択した一連のアプリケーションをブロックするように要求します。
このタスクを達成するには、どのテクノロジを使用する必要がありますか?
A. ウイルス対策/スパイウェア対策ソフトウェア
B. アプリケーションのホワイトリスト/ブラックリスト
C. ホストベースの IDS
D. ネットワーク NGFW
Answer: B (メーッセージを残す**)**

最新問題**: 46**

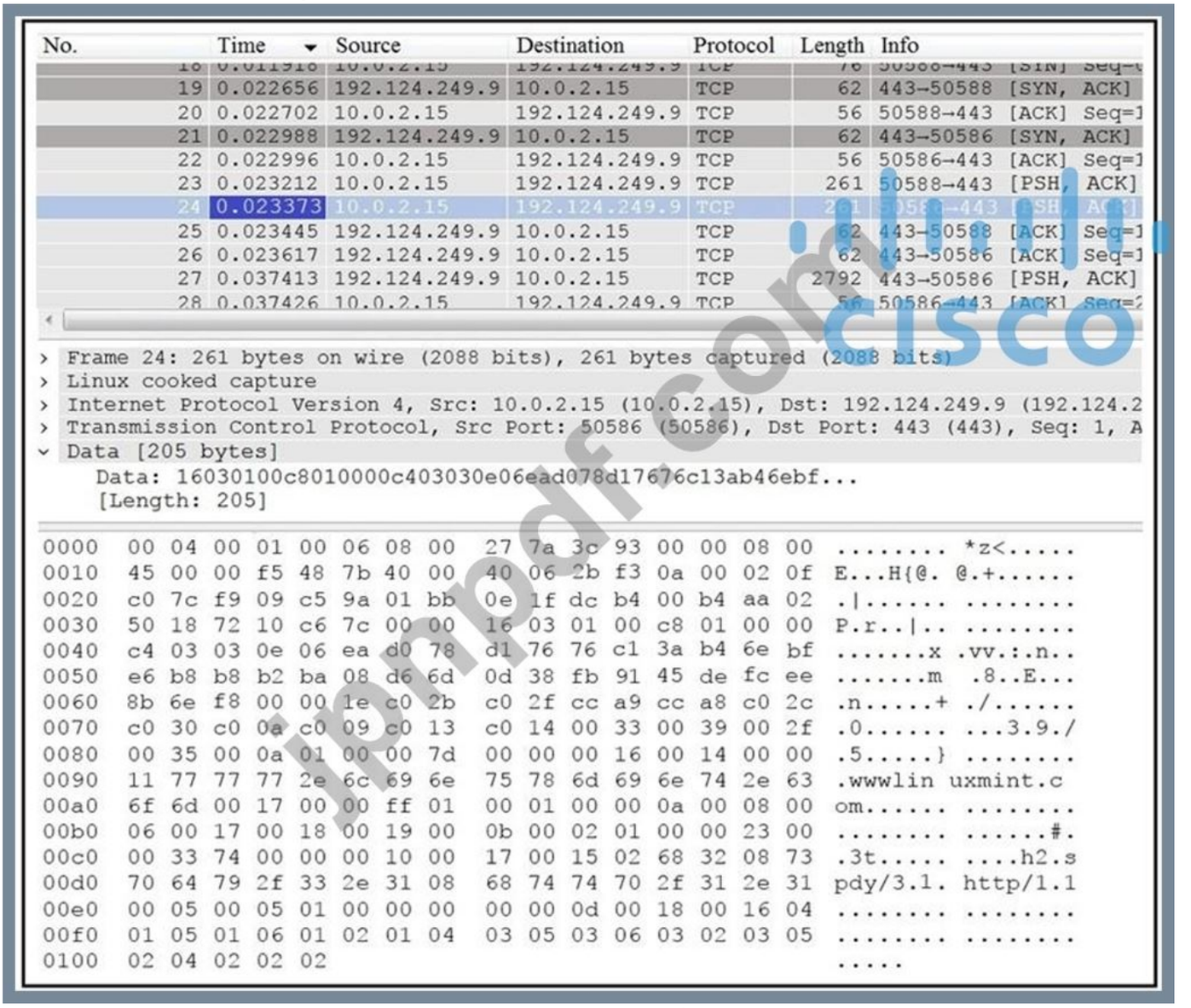


展示を参照してください。この文字列にはどのような攻撃方法が描かれていますか?
A. サービス拒否
B. クロスサイト スクリプティング
C. 中間者
D. SQL インジェクション
Answer: B (メーッセージを残す**)**

最新問題**: 47**
アナリストは、ホストで攻撃が成功したことを示すアラートをデスクトップ コンピューターで受け取りました。
調査の結果、アナリストは、攻撃中に緩和アクションが実行されなかったことを発見しました。この不一致の理由は何ですか?
A. コンピュータには HIDS がインストールされています。
B. コンピュータには HIPS がインストールされています。

C. コンピュータには NIPS がインストールされています。
D. コンピュータには NIDS がインストールされています。
Answer: (解答を表示する**)**

最新問題**: 48**
展示を参照してください。



この PCAP ファイルに含まれているアプリケーション プロトコルはどれですか?
A. HTTP
B. TLS
C. TCP
D. SSH
Answer: A (メーッセージを残す**)**

最新問題**: 49**
ネットワークのプロファイリングに使用される 2 つの要素はどれですか? 2つ選んでください。)
A. リスニング ポート

B. 全体の合計
C. セッション時間
D. OS フィンガープリント
E. 実行中のプロセス
Answer: A,D (メーッセージを残す**)**

最新問題**: 50**
Syslog 収集ソフトウェアがサーバーにインストールされている ログ格納用に、FAT タイプのパーティションを持つディスクが使用されている エンジニアは、4 GB のタイル サイズを超えるとログ ファイルが破損していると判断しました。問題を解決するアクションはどれですか?
A. FAT32 を使用して、4 GB の制限を超えます。
B. 最大 16 TB のファイルを保持できるため、Ext4 パーティションを使用します。
C. ログ ファイルの格納に NTFS パーティションを使用する
D. 既存のパーティションにスペースを追加し、保持期間を下げます。
Answer: C (メーッセージを残す**)**

最新問題**: 51**
従業員が仕事を遂行するために必要なリソースのみにアクセスできるようにする慣行は何ですか?
A. 最小権限の原則
B. 組織分離
C. 職務の分離
D. 原理を知る必要がある
Answer: A (メーッセージを残す**)**
セクション: セキュリティの概念

最新問題**: 52**
あるアナリストは、人事部門のサーバーの 1 つで処理能力が低下したというチケットを受け取りました。同じ日に、エンジニアはウイルス対策ソフトウェアが無効になっていることに気付きましたが、それがいつ、なぜ発生したのかを特定できませんでした。NIST インシデント処理ガイドによると、この調査の次のフェーズは何ですか?
A. 根絶
B. 検出
C. 分析
D. 回復
Answer: (解答を表示する**)**

最新問題**: 53**
最初の証拠から生じる理論または仮説を支持するのは、どのタイプの証拠ですか?
A. 裏付けあり

B. 確率的
C. 最高
D. 間接
Answer: A (メーッセージを残す**)**

最新問題**: 54**
事前に承認された一連のアプリケーションのみをシステム上で実行できるようにするセキュリティ テクノロジはどれですか?
A. アプリケーションレベルのブラックリスト
B. ホストベースの IPS
C. アプリケーションレベルのホワイトリスト
D. ウイルス対策
Answer: C (メーッセージを残す**)**
セクション: ホストベースの分析

最新問題**: 55**
ユーザー インタラクションはどのイベントですか?
A. ファイルの読み取りと書き込みの許可
B. 悪意のあるファイルを開く
C. リモート コードの実行
D. ルート アクセス権の取得
Answer: B (メーッセージを残す**)**

最新問題**: 56**
HTTP ヘッダー、Uniform Resource Identifier、および SSL セッション ID 属性に基づいてルーティングを決定するソリューションを実装するには、どのテクノロジを使用する必要がありますか?
A. AWS
B. IIS
C. ロードバランサー
D. プロキシ サーバー
Answer: (解答を表示する**)**
説明
負荷分散: HTTP(S) 負荷分散は、負荷分散の最も古い形式の 1 つです。この形式の負荷分散は第 7 層に依存しています。つまり、アプリケーション層で動作します。これにより、HTTP ヘッダー、Uniform Resource Identifier、SSL セッション ID、HTML フォーム データなどの属性に基づいてルーティングを決定できます。
ロード バランシングは、7 層の Open System Interconnection (OSI) モデルの第 4 層から第 7 層に適用されます。その機能は次のとおりです。L4。ネットワーク データおよびトランスポート層プロトコル (IP アドレスや TCP ポートなど) に基づいてトラフィックを誘導します。L7. ロード

バランシングにコンテンツ スイッチングを追加し、HTTP ヘッダー、Uniform Resource Identifier、SSL セッション ID、HTML フォーム データなどの特性に応じてルーティングを決定できるようにします。
GSLB。Global Server Load Balancing は、L4 および L7 機能を異なるサイトのサーバーに拡張します

最新問題: **57**
サンドボックスプロセス間通信サービスとは？
A. プロセス間のアクティビティの調整を可能にするインターフェイスのコレクション。
B. インターフェイス上でアクティブ化され、ポート間通信を可能にするネットワーク サービスの集合。
C. サンドボックス間の通信を可能にするホスト サービスのコレクション。
D. サンドボックス間の通信を防止するサンドボックス内のルールの集まり。
Answer: D (メーッセージを残す**)**

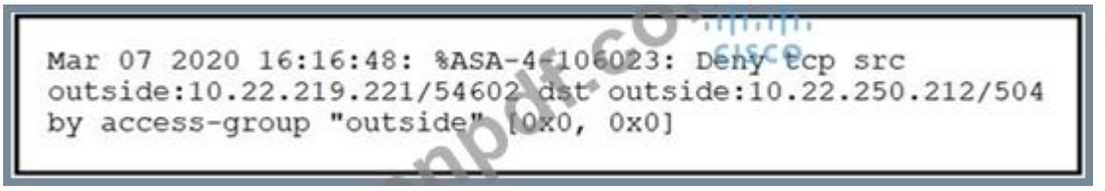
最新問題: **58**
アナリストは SIEM プラットフォームを使用しており、Cisco デバイスからカスタム プロパティを抽出し、 File: Clean」というフレーズをキャプチャする必要があります。アナリストはどの正規表現をインポートする必要がありますか?
A. ファイル: クリーン
B. ^ファイル: クリーン$
C. ファイル: クリーン (.*)
D. ^親ファイルの消去$
Answer: A (メーッセージを残す**)**

最新問題: **59**
2 つのソーシャル エンジニアリング手法とは? 2つ選んでください。）
A. DDoS 攻撃
B. ファーミング
C. 権限昇格
D. フィッシング
E. 中間者
Answer: B,D (メーッセージを残す**)**

最新問題: **60**
重要なタスクを実行するために複数の人員を必要とするセキュリティ原則はどれですか?
A. 最小権限
B. 知っておく必要があります
C. 職務の分離
D. デューデリジェンス

Answer: C (メーッセージを残す)
セクション: セキュリティの概念

最新問題: **61**
展示を参照してください。



このログを生成するテクノロジーはどれですか?
A. ファイアウォール
B. ネットフロー
C. IDS
D. ウェブ プロキシ
Answer: A (メーッセージを残す)

最新問題: **62**
ホスト ポートスキャンをブロックするユーティリティはどれですか?
A. HIDS
B. サンドボックス化
C. ホストベースのファイアウォール
D. マルウェア対策
Answer: (解答を表示する)

最新問題: **63**
アナリストは、正当なセキュリティ アラートが却下されたことを発見しました。このネットワーク トラフィックへの影響を引き起こしたシグニチャはどれですか?
A. 真陰性
B. 偽陰性
C. 偽陽性
D. 真陽性
Answer: B (メーッセージを残す)
説明

偽陰性は、セキュリティ システム (通常は WAF) が脅威を識別できない場合に発生します。それは
脅威が存在する場合でも、 否定的な」結果 (脅威が観察されていないことを意味します)。

最新問題: **64**
フォレンジック プロセスのどの段階で、収集されたデータから情報を抽出するためにツールや技術が使用されますか?
A. 調査
B. コレクション
C. 検査
D. レポート
Answer: (解答を表示する**)**

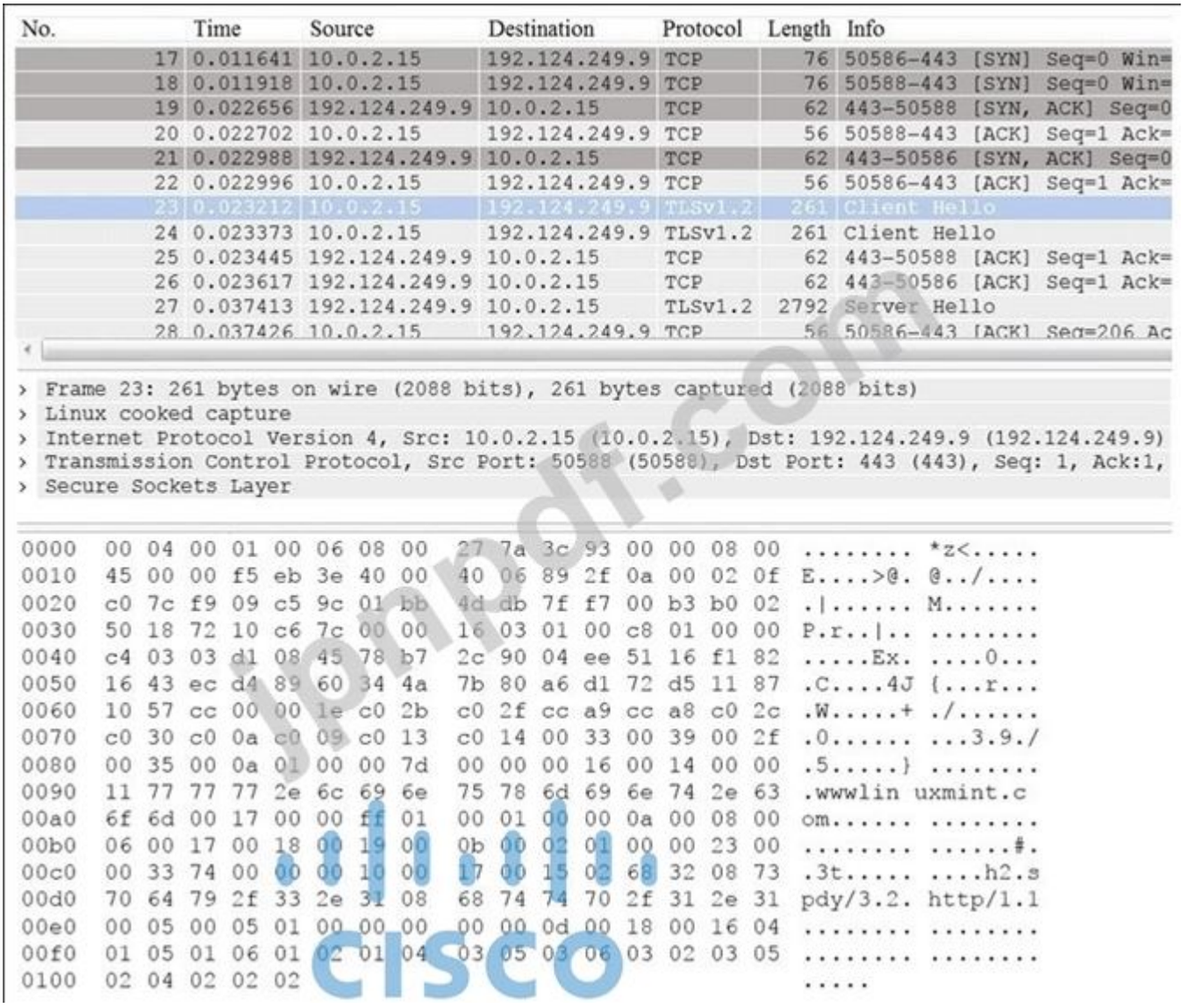
最新問題: **65**
インライン トラフィック調査とトラフィック ミラーリングの違いは何ですか?
A. インライン インスペクションは、元のトラフィック データ フローに作用します。
B. トラフィック ミラーリングは、ライブ トラフィックをブロック用のツールに渡します。
C. トラフィック ミラーリングは、分析と軽減のためにライブ トラフィックを検査します。
D. インライン トラフィックは、分析とセキュリティのためにパケットをコピーします
Answer: B (メーッセージを残す**)**
セクション: ネットワーク侵入分析

最新問題: **66**
ターゲット Web アプリケーション サーバーは root ユーザーとして実行されており、コマンド インジェクションに対して脆弱です。成功した攻撃の結果として正しいのはどれですか?
A. 権限昇格
B. クロスサイト スクリプティング
C. バッファ オーバーフロー
D. クロスサイト スクリプティング リクエスト フォージェリ
Answer: D (メーッセージを残す**)**

最新問題: **67**
ソーシャル エンジニアリング攻撃の例は何ですか?
A. 部門の毎週の WebEx ミーティングへの招待状を受け取る
B. 連絡先情報を更新するために、人事部から安全な Web サイトへのアクセスを要求する電子メールを受信する
C. 同じ会社の誰かから特徴のない添付ファイルが付いた見知らぬ人からの予期しない電子メールの受信
D. アカウントのパスワードを変更する方法を知っている管理者に口頭で要求を送信する
Answer: (解答を表示する**)**

最新問題: **68**
改ざんされたディスク イメージと改ざんされていないディスク イメージがセキュリティ インシデントに与える影響の 2 つの違いは何ですか? 2つ選んでください。)
A. セキュリティ調査プロセスで改ざんされていないイメージが使用されます
B. 改ざんされた画像は、セキュリティ調査プロセスで使用されます
C. 保存されたハッシュと計算されたハッシュが一致する場合、画像は改ざんされています
D. 改ざんされた画像は、インシデントの回復プロセスで使用されます
E. 保存されたハッシュと計算されたハッシュが一致する場合、画像は改ざんされていません
Answer: B,E (メーッセージを残す**)**
セクション: ホストベースの分析

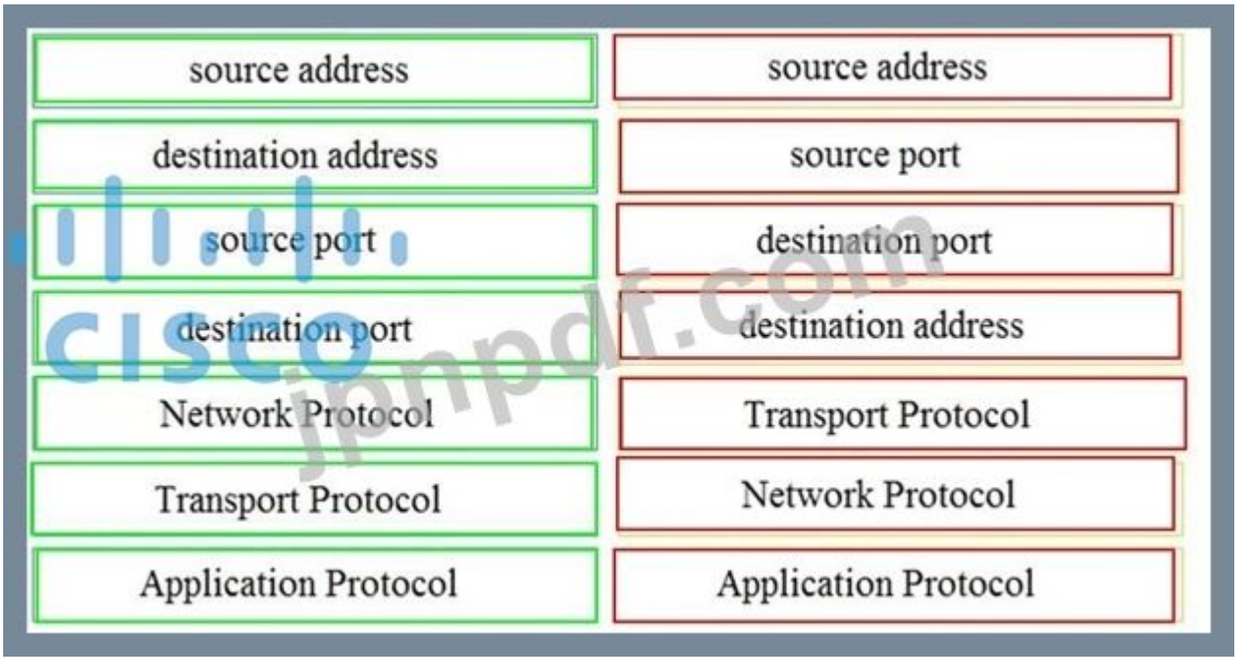
最新問題: **69**
展示を参照してください。



要素名を左側から右側の PCAP ファイルの正しい部分にドラッグ アンド ドロップします。

source address	10.0.2.15
destination address	50588
source port	443
destination port	192.124.249.9
Network Protocol	Transmission Control Protocol
Transport Protocol	Internet Protocol v4
Application Protocol	Transport Layer Security v1.2

Answer:



最新問題: **70**

アナリストは SIEM プラットフォームを使用しており、Cisco デバイスからカスタム プロパティを抽出し、File: Clean」というフレーズをキャプチャする必要があります。アナリストはどの正規表現をインポートする必要がありますか?

A. ^親ファイルの消去$

B. ^ファイル: クリーン$

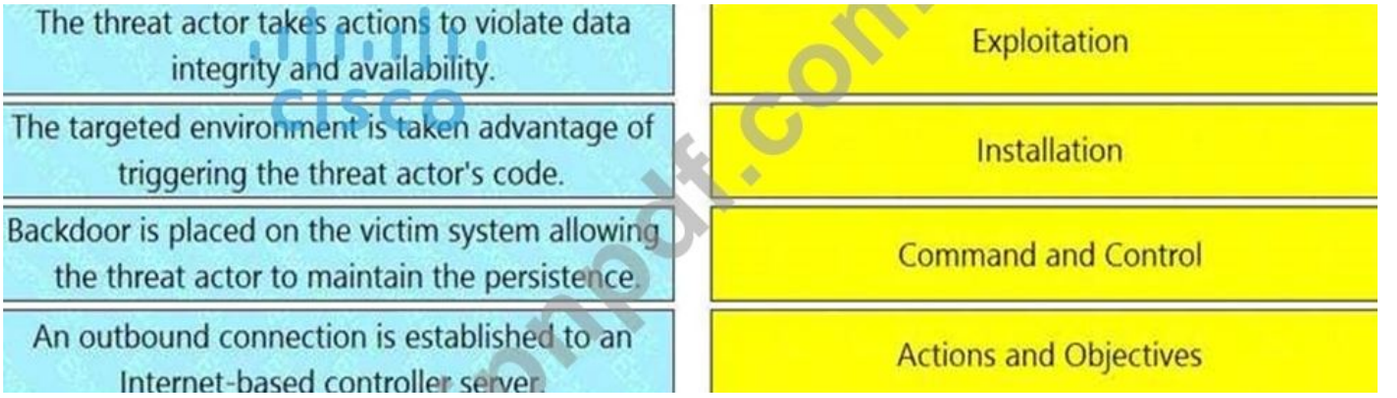
C. ファイル: クリーン

D. ファイル: クリーン (.*)

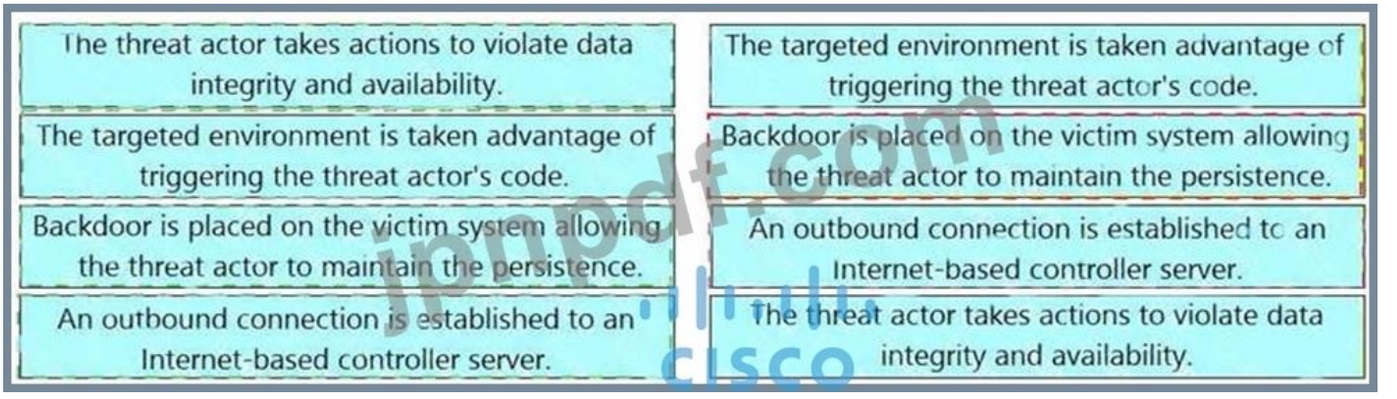
Answer: A (メーッセージを残す**)**

最新問題: **71**

定義を左側から右側のフェーズにドラッグ アンド ドロップして、サイバー キル チェーン モデルに従って侵入イベントを分類します。



Answer:



説明

悪用 - 攻撃者のコードをトリガーするために、標的の環境が利用されます。インストール - バックドアが被害者のシステムに配置され、攻撃者が持続性を維持できるようにします。

コマンド アンド コントロール - インターネット ベースのコントローラー サーバーへのアウトバウンド接続が確立されます。

アクションと目的 - 攻撃者は、データの整合性と可用性を侵害するアクションを実行します

最新問題: **72**

HTTPS トラフィックの監視が困難な理由は何ですか?

A. 暗号化

B. パケット ヘッダー サイズ

C. 署名検出時間

D. SSL インターセプト

Answer: A (メーッセージを残す**)**

最新問題: **73**

フォレンジックで使用されているブラウザの種類を識別するために使用される HTTP ヘッダー フィールドはどれですか?

A. リファラー

B. ユーザーエージェント

C. 受け入れる言語

D. ホスト

Answer: B (メーッセージを残す)

最新問題: **74**

展示を参照してください。

5 タプルの一部である表の 2 つの要素はどれですか? (2つ選んでください。)

A. ソース ポート

B. イニシエーター ユーザー

C. イニシエータ IP

D. 入力セキュリティ ゾーン

E. 最初のパケット

Answer: (解答を表示する)

最新問題: **75**

展示を参照してください。

展示の中で何が起きているのか?

A. XML 外部エンティティ攻撃

B. クロスサイト スクリプティング攻撃

C. 通常の GET リクエスト

D. 安全でない逆シリアル化

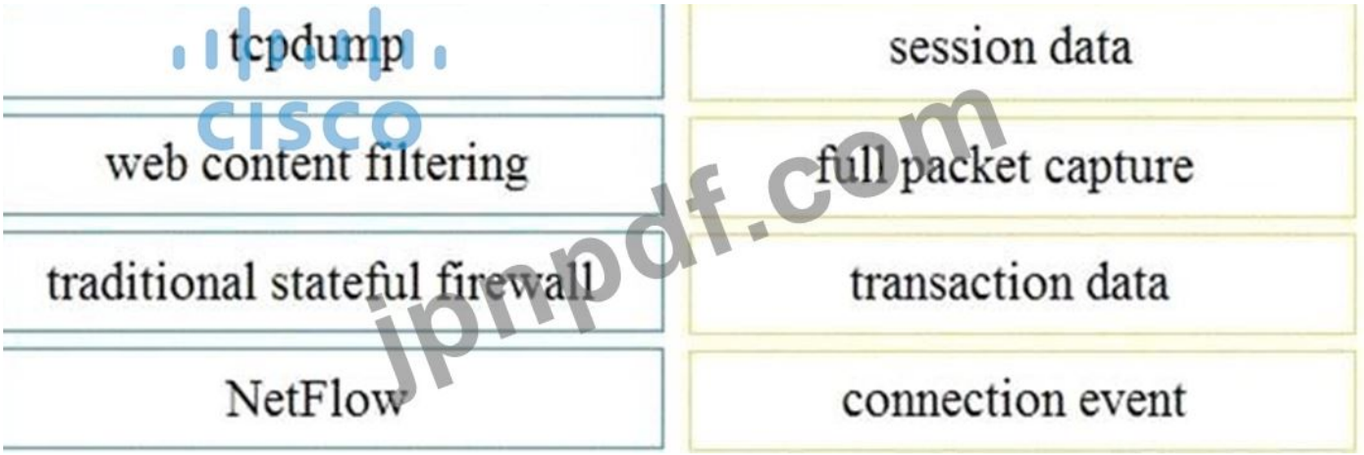
Answer: A (メーッセージを残す)

最新問題: **76**
展示を参照してください。

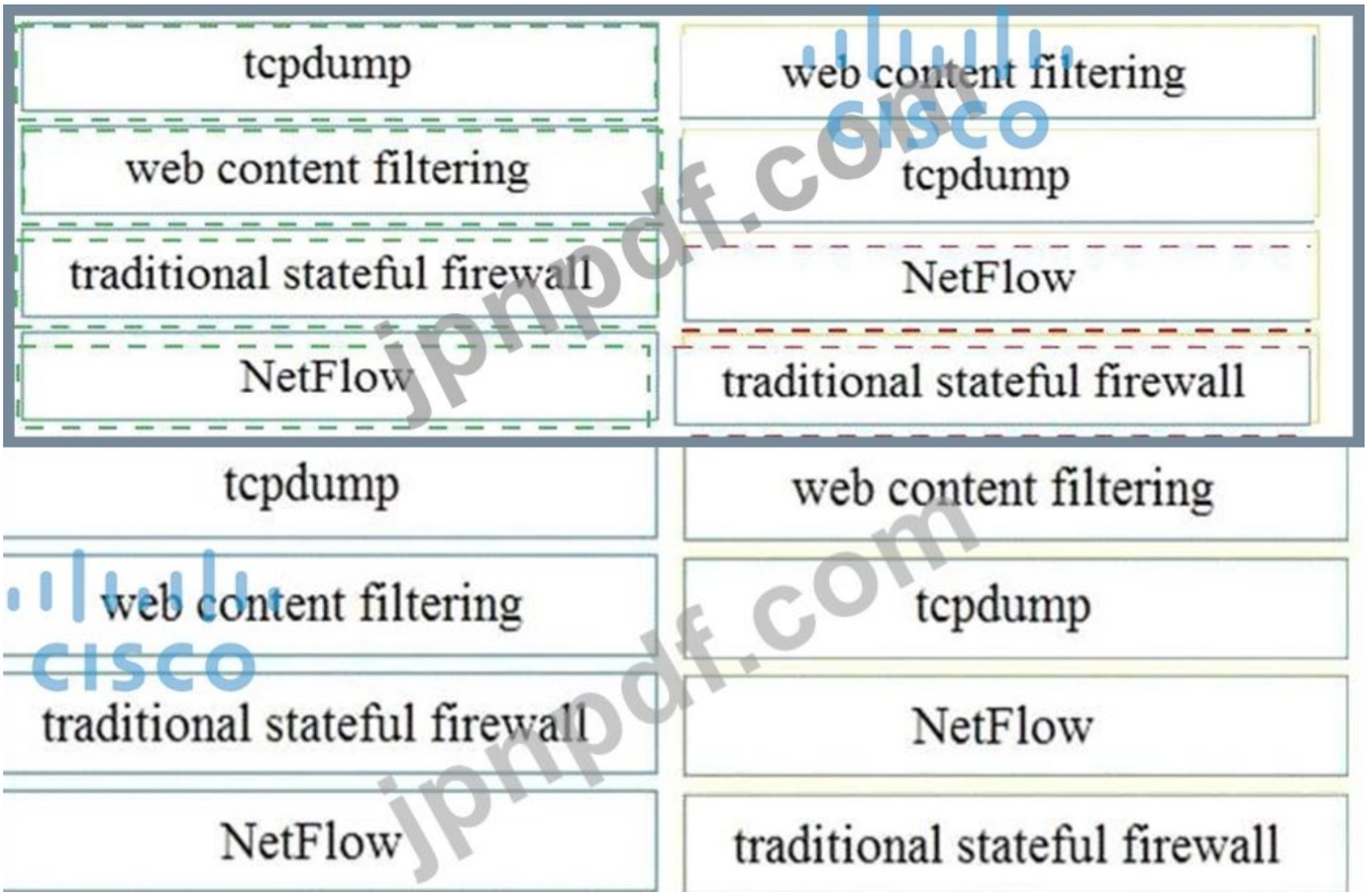
Employee Name	Role
Employee 1	Chief Accountant
Employee 2	Head of Managed Cyber Security Services
Employee 3	System Administration
Employee 4	Security Operation Center Analyst
Employee 5	Head of Network & Security Infrastructure Services
Employee 6	Financial Manager
Employee 7	Technical Director

会社のワークステーションが侵害された場合、どの利害関係者が関与する必要がありますか?
A. 従業員 4、従業員 6、従業員 7
B. 従業員 2、従業員 3、従業員 4、従業員 5
C. 従業員 1、従業員 2、従業員 4、従業員 5
D. 従業員 1 従業員 2、従業員 3、従業員 4、従業員 5、従業員 7
Answer: (解答を表示する**)**

最新問題: **77**
左側のテクノロジを、右側のテクノロジが提供するデータ型にドラッグ アンド ドロップします。



Answer:



最新問題: **78**
調査で帰属に必要な情報はどれですか?
A. 802.1x RADIUS 認証のパスと失敗のログ
B. 脅威アクターの既知の動作
C. ソース RFC 1918 IP アドレスを示すプロキシ ログ
D. インターネットから許可された RDP
Answer: B (メーッセージを残す**)**

最新問題: **79**
バッファ オーバーフロー攻撃とは?

A. メモリ バッファ レジスタからのデータのフェッチ
B. 新しいコマンドを既存のバッファに挿入する
C. 定義済みの量のメモリを過負荷にしています
D. プロセス内のバッファの抑制
Answer: C (メーッセージを残す**)**

最新問題**: 80**
IPv4 プロトコル ヘッダーから収集される情報はどれですか? (2つ選んでください。)
A. トラフィックの宛先となる UDP ポート
B. トラフィックの送信元の TCP ポート
C. パケットの送信元 IP アドレス
D. パケットの宛先 IP アドレス
E. トラフィックの送信元の UDP ポート
Answer: C,D (メーッセージを残す**)**
セクション: ネットワーク侵入分析

最新問題**: 81**
SOC アナリストが、特定のセッションを識別している Linux システムに関連するインシデントを調査しています。
アクティブなプログラムを追跡する識別子はどれですか?
A. アプリケーション識別番号
B. アクティブなプロセス識別番号
C. ランタイム識別番号
D. プロセス識別番号
Answer: D (メーッセージを残す**)**
セクション: ホストベースの分析

最新問題**: 82**
TLS ハンドシェイクのネゴシエーション フェーズでクライアントがサーバーに送信する情報を識別するリストはどれですか?
A. ClientStart、サポートする TLS バージョン、サポートする暗号スイート、および推奨される圧縮方法
B. ClientHello、サポートする TLS バージョン、サポートする暗号スイート、および推奨される圧縮方法
C. ClientStart、ClientKeyExchange、サポートする暗号スイート、および推奨される圧縮方法
D. ClientHello、ClientKeyExchange、サポートする暗号スイート、および推奨される圧縮方法
Answer: B (メーッセージを残す**)**

最新問題**: 83**
NetFlow はトラフィック ミラーリングとどう違うのですか?

A. NetFlow がメタデータを収集し、トラフィック ミラーリング クローン データ
B. トラフィック ミラーリングはスイッチのパフォーマンスに影響を与えますが、NetFlow は影響しません。
C. トラフィック ミラーリングは、NetFlow よりも運用コストが低くなります。
D. NetFlow は、トラフィック ミラーリングよりも多くのデータを生成します
Answer: A (メーッセージを残す**)**
セクション: セキュリティ監視

最新問題**: 84**
エージェントレス保護と比較した場合、エージェントベースの保護にはどのような利点がありますか?
A. 集中型プラットフォームを提供します
B. 多数のデバイスを同時に管理します
C. 維持費を下げる
D. すべてのトラフィックをローカルで収集して検出します
Answer: A (メーッセージを残す**)**

最新問題**: 85**
アナリストは、正当なセキュリティ アラートが却下されたことを発見しました。
このネットワーク トラフィックへの影響を引き起こしたシグニチャはどれですか?
A. 真陰性
B. 偽陰性
C. 偽陽性
D. 真陽性
Answer: B (メーッセージを残す**)**
セクション: ネットワーク侵入分析

最新問題**: 86**
スイッチド ネットワーク上のトラフィックを傍受する攻撃方法はどれですか?
A. サービス拒否
B. ARP キャッシュ ポイズニング
C. DHCP スヌーピング
D. コマンド アンド コントロール
Answer: (解答を表示する**)**
攻撃者が 2 つのデバイスの ARP キャッシュを攻撃者のネットワーク インターフェイス カード (NIC) の MAC アドレスでポイズニングすると、ARP ベースの MITM 攻撃が実行されます。ARP キャッシュが正常にポイズニングされると、被害者の各デバイスは、他のデバイスとの通信時にすべてのパケットを攻撃者に送信し、攻撃者を 2 つの被害者デバイス間の通信パスの途中に配置します。これにより、攻撃者は被害者のデバイス間のすべての通信を簡単に監視できます。その目

的は、2 つの被害者デバイス間で渡される情報を傍受して表示し、2 つの被害者デバイス間にセッションとトラフィックを導入する可能性があることです。

最新問題: **87**
ユーザーは、「r405-report2609-empl094.exe」という名前の電子メールの添付ファイルを受け取りましたが、実行しませんでした。このタイプのイベントには、サイバー キル チェーンのどのカテゴリを割り当てる必要がありますか?
A. 武器化
B. インストール
C. 配送
D. 偵察
Answer: B (メーッセージを残す**)**

最新問題: **88**
組織内で特定の役割を実行するために必要な権限のみを従業員に付与する慣行は何ですか?
A. デューデリジェンス
B. 最小権限
C. 整合性検証
D. 知っておく必要があります
Answer: (解答を表示する**)**

最新問題: **89**
PII データの不適切な使用または開示に関連するカテゴリはどれですか?
A. 合法
B. コンプライアンス
C. 規制
D. 契約上の
Answer: (解答を表示する**)**

最新問題: **90**
展示を参照してください。

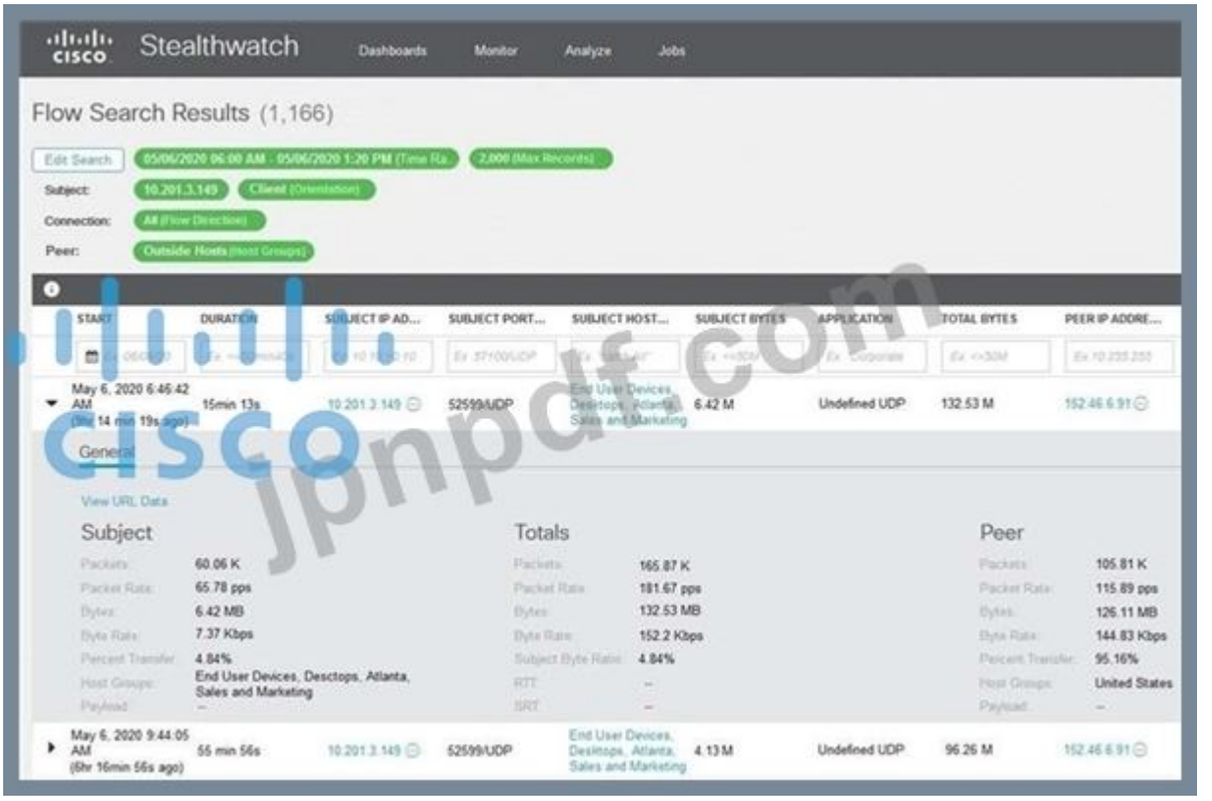
```
$ cuckoo submit --machine cuckoo1 /path/to/binary
```

どのイベントが発生していますか?
A. 悪意のあるバイナリが含まれているかどうかを確認するために、URL が評価されています。
B. VM cuckoo1 で実行するためにバイナリが送信されています。
C. VM cuckoo1 上のバイナリが評価のために送信されています
D. 「submit」という名前のバイナリが VM cuckoo1 で実行されています。
Answer: (解答を表示する**)**

最新問題: **91**
調査におけるサイバー アトリビューション アイデンティティとは?
A. 攻撃の原因
B. 攻撃の攻撃者
C. 悪用された脆弱性
D. 攻撃の悪用
Answer: B (メーッセージを残す**)**

最新問題: **92**
ローカル システムの動作とローカル ネットワーク アクセスを監視して、セキュリティ ポリシーに違反していないかどうかを監視するシステムはどれですか?
A. ホストベースの侵入検知
B. システムベースのサンドボックス
C. ホストベースのファイアウォール
D. ウイルス対策
Answer: (解答を表示する**)**
HIDS は、コンピューティング システムの内部だけでなく、ネットワーク インターフェイス上のネットワーク パケットも監視できます。ホストベースのファイアウォールは、単一のホスト上で実行されるソフトウェアの一部であり、そのホストのみの着信および発信ネットワーク アクティビティを制限できます。

最新問題: **93**



展示を参照してください。この Stealthwatch ダッシュボードで特定された潜在的な脅威は何ですか?

A. ホスト 10.201.3.149 は、TCP/443 を使用して 152.46.6.91 にデータを送信しています。

B. ホスト 152.46.6.91 は、データ転送のウォッチリストの国として識別されています。

C. 152.46.6.149 へのトラフィックは、高度なネットワーク制御ポリシーによって拒否されています。

D. ホスト 10.201.3.149 は、ホスト 152.46.6.91 に送信されるデータのほぼ 19 倍のデータを受信しています。

Answer: D (メーッセージを残す)

セクション: ホストベースの分析

最新問題: **94**

脆弱性と脅威の関係は?

A. 脅威は、脆弱性によって引き起こされる潜在的な損失の計算です

B. 脆弱性は、脅威によって引き起こされる潜在的な損失の計算です

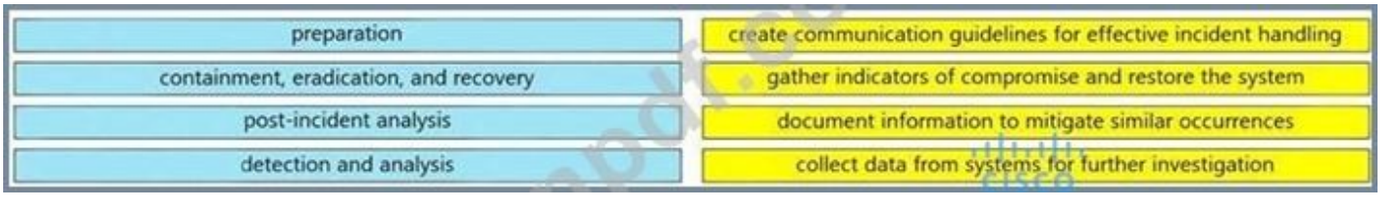
C. 脆弱性を悪用する脅威

D. 脆弱性が脅威を悪用する

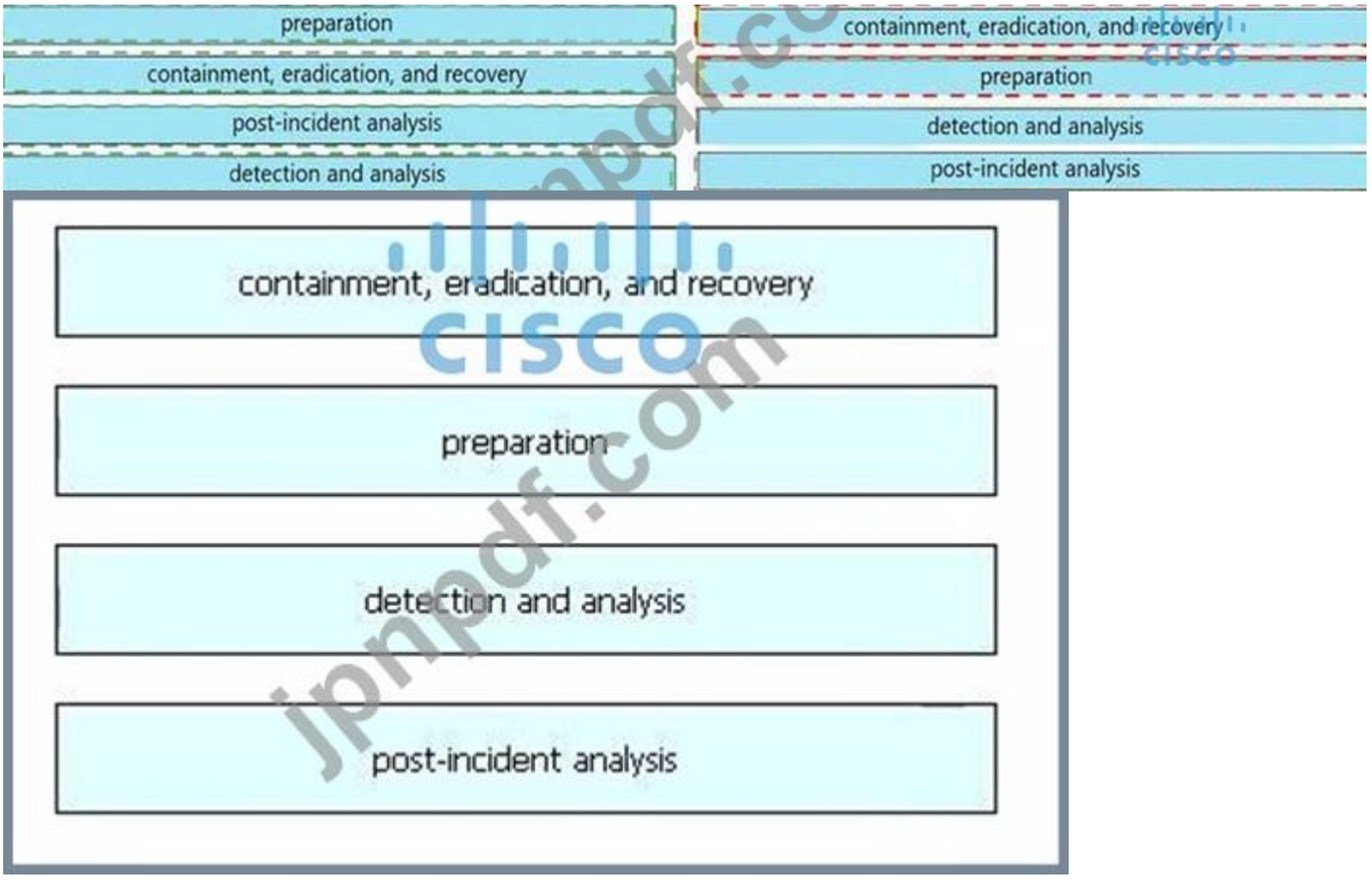
Answer: C (メーッセージを残す)

最新問題: **95**

要素を左側からドラッグ アンド ドロップして、右側のインシデント処理の正しい順序にします。



Answer:



最新問題: **96**

ある企業が IIS 7 を使用して自社の Web サーバーで侵害に遭遇しました 7 5 調査中に、エンジニアは、攻撃者が TLS 1 2 を使用して安全な通信でデータを読み取って変更し、接続を輸出グレードの暗号化にダウングレードして機密情報を傍受したことを発見しました。エンジニアは、将来的に同様のインシデントを軽減し、クライアントとサーバーが常に最も安全なプロトコル バージョンと暗号化パラメーターとネゴシエートするようにする必要があります。エンジニアはどのアクションを推奨しますか?

A. TLS v1 3 にアップグレードします。

B. 最新の IIS バージョンをインストールします。

C. TLS 1.1 にダウングレードします。

D. 侵入検知システムを導入する

Answer: (解答を表示する**)**

最新問題: **97**

展示を参照してください。

```
192.168.10.10 – – [01/Dec/2020:11:12:22 -0200] "GET /icons/powered_by_rh.png HTT
P/1.1" 200 1213 "http://192.168.0.102/" "Mozilla/5.0 (X11; U; Linux x86_64; en-U
S; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 – – [01/Dec/2020:11:13:15 -0200] "GET /favicon.ico HTTP/1.1" 404 2
88 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12) Gecko/2009070812
Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 – – [01/Dec/2020:11:14:22 -0200] "GET /%27%27;!–%22%3CXSS%3E=&{()
} HTTP/1.1" 404 310 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12)
Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
```

展示の中で何が起きているのか?

A. 通常の GET リクエスト

B. クロスサイト スクリプティング攻撃

C. XML 外部エンティティ攻撃

D. 安全でない逆シリアル化

Answer: A (メーッセージを残す**)**

最新問題**: 98**

展示を参照してください。

この Stealthwatch ダッシュボードで特定された潜在的な脅威は何ですか?

A. ネットワーク上のホストが別の内部ホストに DDoS 攻撃を送信しています。

B. ホスト 10.201.3.149 でポリシー違反が発生しています。

C. ホスト 10.10.101.24 でポリシー違反が発生しています。

D. アクティブなデータ流出アラートが 2 つあります。

Answer: D (メーッセージを残す**)**

最新問題**: 99**

```
10.44.101.23 - - [20/Nov/2017:14:18:06 -0500] "GET / HTTP/1.1"
200 1254 "-" "Mozilla/5.0(X11; Ubuntu; Linux x86_64; rv:54.0)
Gecko/20100101 Firefox/54.0"
```

展示を参照してください。メッセージは何を示していますか?

A. Mosaic の Web ブラウザからアクセスしようとしました

B. パスワードファイルを取得するためのアクセス試行が成功しました
C. Web サイトのルートを取得するためのアクセス試行が成功しました
D. パスワード ファイルを取得するためのアクセス試行が拒否されました
Answer: C (メーッセージを残す**)**
セクション: ホストベースの分析

最新問題**: 100**
ディープ パケット インスペクションとステートフル インスペクションの違いは何ですか?
A. ディープ パケット インスペクションによりレイヤー 7 の可視性が可能になり、ステートフル インスペクションによりレイヤー 4 の可視性が可能になります。
B. ディープ パケット インスペクションは、レイヤー 4 のステートフル インスペクションよりも安全です。
C. ステートフル インスペクションは、レイヤ 7 のディープ パケット インスペクションよりも安全です。
D. ステートフル インスペクションはレイヤ 4 でコンテンツを検証し、ディープ パケット インスペクションはレイヤで接続を検証します。
7。
Answer: A (メーッセージを残す**)**

最新問題**: 101**
Web アプリケーションとの間で送受信されるすべてのメッセージの整合性と信頼性を保証するセキュリティ テクノロジはどれですか?
A. VPN
B. トンネリング
C. SSL証明書
D. ハイパーテキスト転送プロトコル
Answer: C (メーッセージを残す**)**

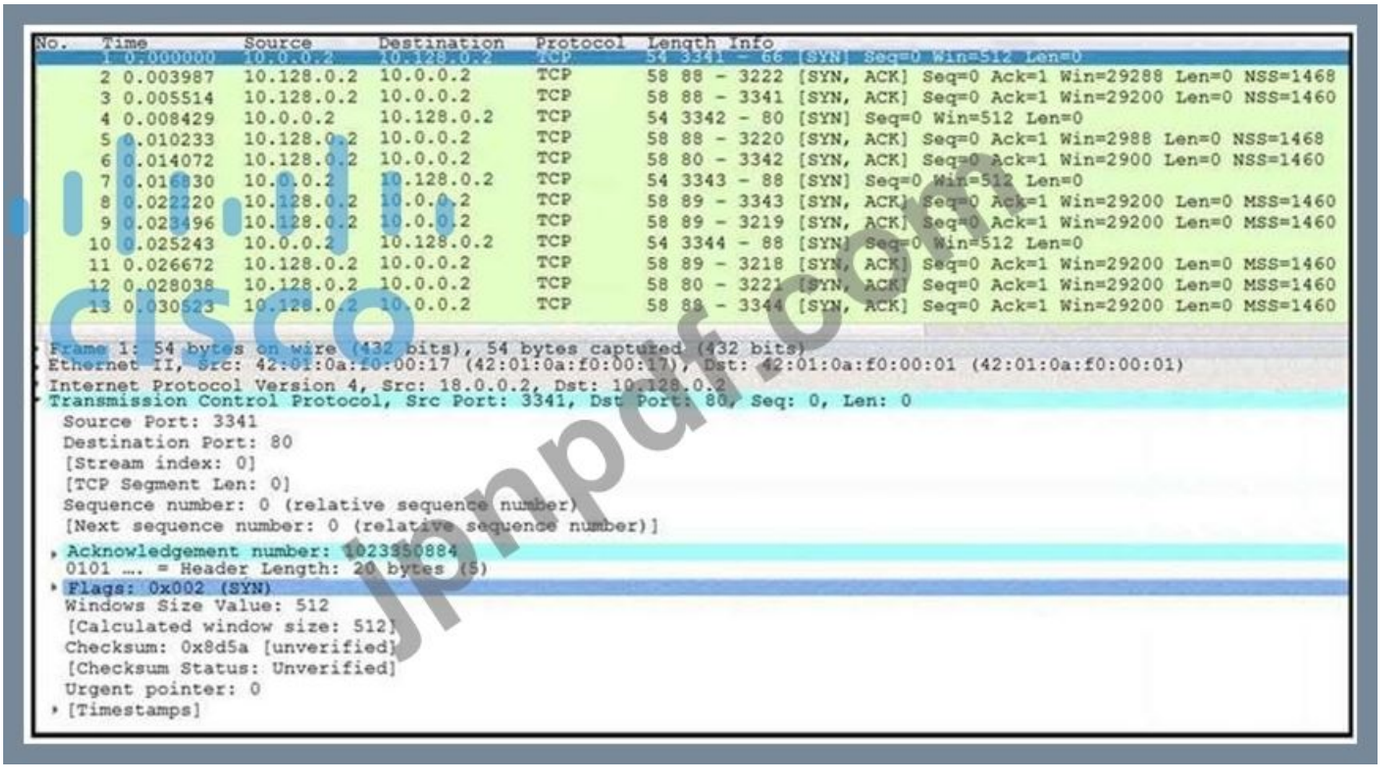
最新問題**: 102**
暗号化がセキュリティ監視にとって難しいのはなぜですか?
A. 攻撃者は暗号化を回避および難読化の手段として使用します。
B. 暗号分析は、VPN トンネルを監視するために攻撃者によって使用されます。
C. 暗号化により、CPU による追加の処理要件が導入されます。
D. 暗号化により、分析および保存するパケット サイズが大きくなります。
Answer: A (メーッセージを残す**)**

最新問題**: 103**
脆弱性とリスクの違いは何ですか?
A. リスクはエクスプロイトが適用される潜在的な脅威であり、脆弱性は脅威そのものを表します。

B. リスクは攻撃者がネットワークに侵入するために使用する潜在的な脅威であり、脆弱性はエクスプロイトです。
C. 脆弱性は潜在的な悪意のあるエントリ ポイントの合計であり、リスクは不正なエントリ自体の可能性を表します。
D. 脆弱性は、悪用される可能性があるセキュリティの欠陥を表し、リスクはそれが引き起こす可能性のある潜在的な損害です。
Answer: (解答を表示する**)**

最新問題**: 104**
セッション データをリアルタイムで表示できるツールはどれですか?
A. トラフィックダンプ
B. トラフィックショー
C. tcpdstat
D. tcptrace
Answer: D (メーッセージを残す**)**

最新問題**: 105**



展示を参照してください。このネットワーク トラフィックで何が発生していますか?
A. 複数の送信元から単一の宛先 IP に向けて送信される SYN パケットの割合が高い
B. 単一の送信元 IP から複数の宛先 IP に向けて送信される SYN パケットの割合が高い
C. 単一のソース IP から複数の宛先 IP への ACK パケットのフラッド
D. 単一の送信元 IP から単一の宛先 IP への SYN パケットのフラッド
Answer: D (メーッセージを残す**)**
セクション: セキュリティ監視

最新問題: **106**
エンジニアがコンプライアンス チームと協力して、ネットワークを通過するデータを特定しています。分析中、エンジニアはコンプライアンス チームに、外部ペンメーター データ フローにレコード、書き込み、およびアートワークが含まれていることを通知します。内部の分離されたネットワーク フローには、性別による顧客の選択、住所、および年齢による製品の好みが含まれます。エンジニアは、保護されたデータを特定する必要があります。どの 2 種類のデータを特定する必要がありますか?」2つ選んでください。）
A. PII
B. ファイ
C. 著作権
D. PCI
E. SOX
Answer: A,B (メーッセージを残す**)**

最新問題: **107**
アナリストは、パケット キャプチャ データを表示しているときに、IP ヘッダーを変更することにより、1 つの IP が複数のデバイスのトラフィックを送受信していることを確認します。
この動作を可能にするテクノロジーはどれですか?
A. トル
B. NAT
C. カプセル化
D. トンネリング
Answer: B (メーッセージを残す**)**

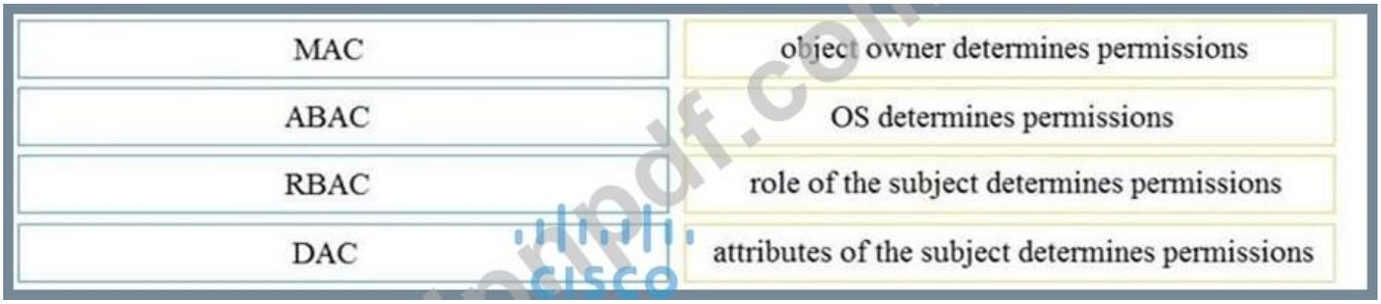
最新問題: **108**
不正アクセスから保護する必要がある個人を特定できる情報とは?
A. 生年月日
B. 運転免許証番号
C. 性別
D. 郵便番号
Answer: B (メーッセージを残す**)**

セクション: セキュリティ ポリシーと手順

最新問題: **109**
正当なユーザーが一貫して容易にアクセスできるデータの概念を説明するものは何ですか?
A. アクセシビリティ
B. 在庫状況
C. 守秘義務
D. 完全性
Answer: B (メーッセージを残す**)**

最新問題: **110**
エンジニアは、既知の TOR 出口ノードを持つトラフィックがネットワーク上で発生したというセキュリティ アラートを受け取ります。
このトラフィックの影響は?
A. 感染後に通信するランサムウェア
B. 著作権のあるコンテンツをダウンロードしているユーザー
C. データの流出
D. ファイアウォールのユーザー回避
Answer: D (メーッセージを残す**)**
セクション: セキュリティ監視

最新問題: **111**
アクセス制御モデルを左側から右側の正しい説明にドラッグアンドドロップします。



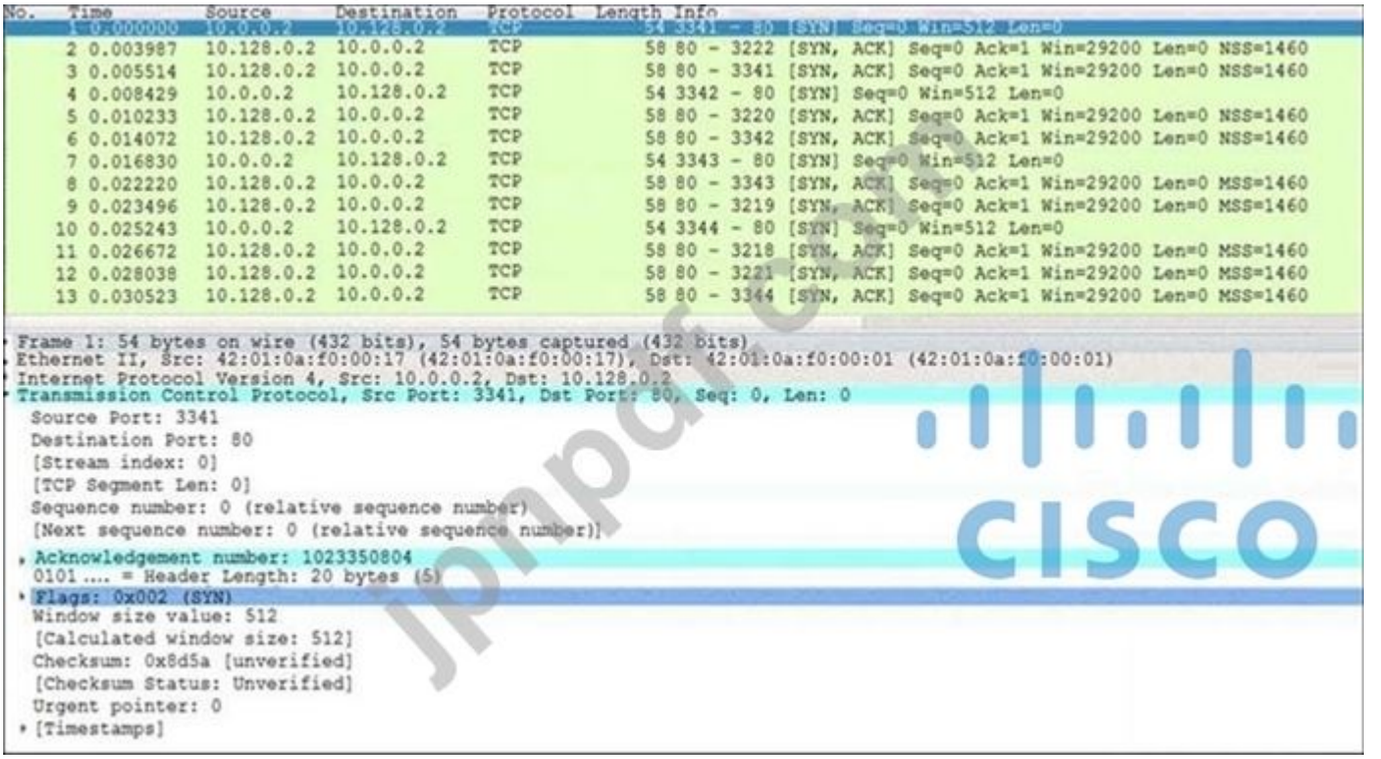
Answer:

最新問題: **112**
脅威とリスクの違いは何ですか？
A. 脅威は、システムの弱点を利用できる潜在的な危険を表します。
B. リスクは、システム内の既知および特定された損失または危険を表します

C. リスクは、システム内の不確実性との意図的でない相互作用を表します
D. 脅威は、物理的または論理的に攻撃または侵害にさらされている状態を表します。
Answer: (解答を表示する**)**
脅威とは、資産に対する潜在的な危険です。脆弱性が存在するが、まだ悪用されていない場合、またはさらに重要なことに、まだ公に知られていない場合、脅威は潜在的であり、まだ認識されていません。

最新問題**: 113**
セキュリティ エンジニアは、同じデータ センター内のファイルが競合他社に転送されたのと同じ日に撮影されたデータ センターに入る容疑者のビデオを持っています。
これはどのような証拠ですか？
A. 最良の証拠
B. 一応の証拠
C. 間接証拠
D. 物的証拠
Answer: C (メーッセージを残す**)**
セクション: ホストベースの分析

最新問題**: 114**
展示を参照してください。



このネットワーク トラフィックで何が発生していますか?
A. 単一の送信元 IP から複数の宛先 IP への ACK パケットのフラッド。
B. 単一の送信元 IP から複数の宛先 IP に向けて送信される ACK パケットの割合が高い。
C. 複数の送信元から 1 つの宛先 IP に向けて送信される SYN パケットの割合が高い。

D. 単一の送信元 IP から単一の宛先 IP への SYN パケットのフラッド。
Answer: D (メーッセージを残す**)**

最新問題**: 115**
開発者は、必要な結果を得るためにプロセスを作成できる Linux ツールを使用してプロジェクトに取り組んでいます。
※処理に失敗した場合はマイナス値を返します。
※処理が成功した場合、子プロセスに0値を返し、親プロセスにプロセスIDを送信します。
この操作の結果、どのコンポーネントが生成されますか?
A. CPU セットを管理するためのマクロ
B. ファイル パス名の親ディレクトリ名
C. プロセス生成スケジュール
D. 親プロセスによって作成された新しいプロセス
Answer: (解答を表示する**)**

最新問題**: 116**
Windows システムのイベントがログ メッセージにイベント コード 4625 を表示する原因は何ですか?
A. 特権ユーザーがシステムに正常にログインしました
B. 誰かがネットワーク上でブルート フォース攻撃を試みています
C. 別のデバイスがシステムへの root アクセス権を取得しています
D. システムが XSS 攻撃を検出しました
Answer: B (メーッセージを残す**)**

最新問題**: 117**
エンジニアは、プロキシ サーバーからログを取得し、受信したデータに従って実際のイベントを生成する必要があります。
このタスクを達成するために、エンジニアはどのテクノロジを使用する必要がありますか?
A. ステルスウォッチ
B. Web セキュリティ アプライアンス
C. 火力
D. E メール セキュリティ アプライアンス
Answer: A (メーッセージを残す**)**

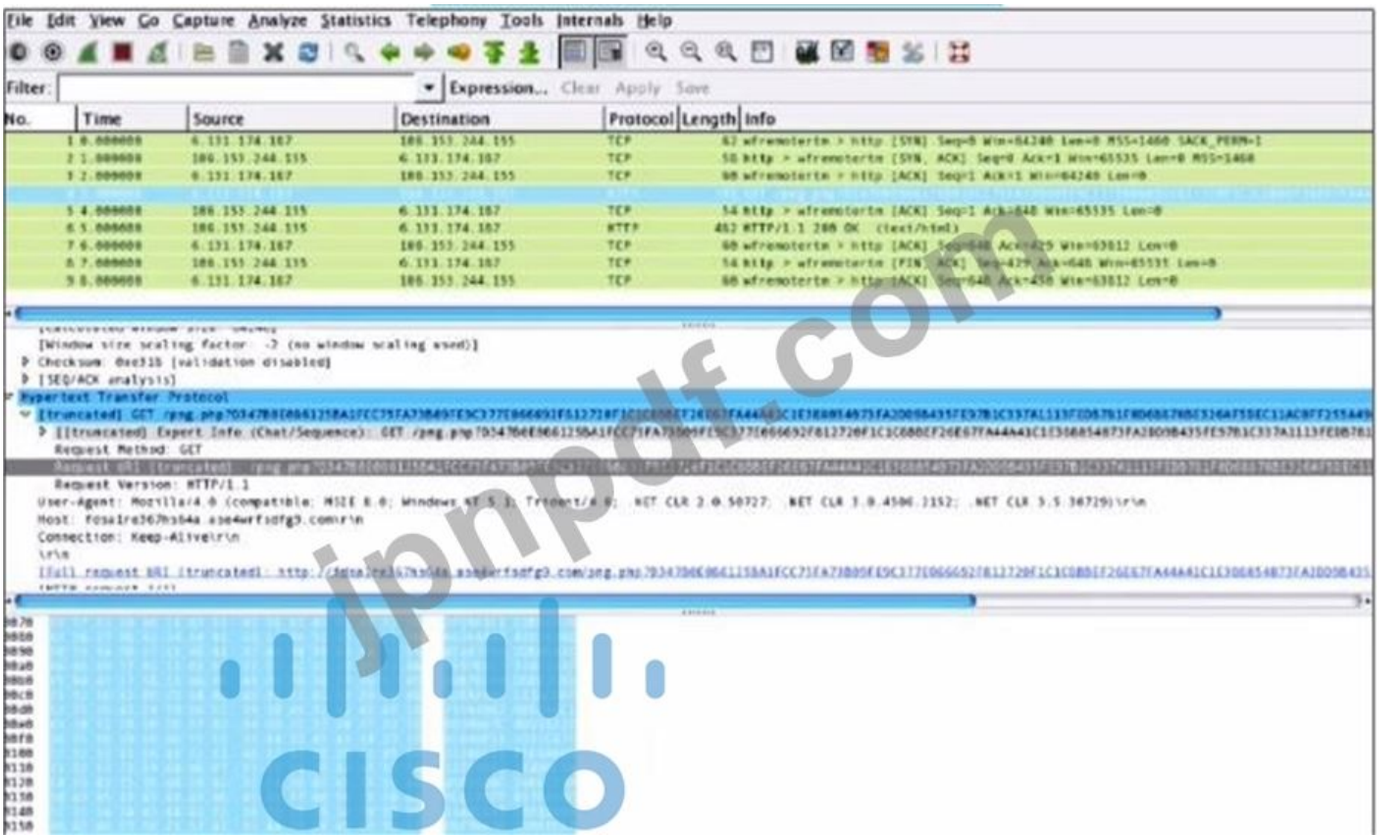
最新問題**: 118**
調査員は、CDFS 形式で保存されている ISO ファイルのコピーを調べています。このファイルはどのような種類の証拠ですか?
A. Mac ベースのシステムを使用してコピーされた CD からのデータ
B. Linux システムを使用してコピーされた CD からのデータ
C. Windows システムを使用してコピーされた DVD からのデータ

D. Windows でコピーした CD のデータ
Answer: B (メーッセージを残す**)**
説明
CDfs は、Unix ライクなオペレーティング システム用の仮想ファイル システムです。コンパクト ディスクのデータおよびオーディオ トラックへのアクセスを提供します。CDfs ドライバーがコンパクト ディスクをマウントすると、各トラックがファイルとして表されます。これは、「すべてがファイルである」という Unix の規則と一致しています。ソース:
https://en.wikipedia.org/wiki/CDfs

最新問題**: 119**
フル パケット キャプチャの 2 つの特徴は何ですか? (2つ選んでください。)
A. 生データから断片化されたトラフィックを再構築します。
B. ネットワーク トランザクションの履歴記録を提供します。
C. セキュリティとパフォーマンスの問題の原因をトラブルシューティングします。
D. ネットワーク ループと衝突ドメインの特定。
E. 一般的なハードウェア障害を検出し、障害のある資産を特定します。
Answer: A,B (メーッセージを残す**)**

最新問題**: 120**
組織は最近、既知のハクティビスト グループによるオンラインの脅威に対応して、セキュリティ スタンスを調整しました。
NIST SP800-61 で呼び出される初期イベントは何ですか?
A. オンライン攻撃
B. トリガー
C. 扇動者
D. 前駆体
Answer: (解答を表示する**)**

最新問題**: 121**
展示を参照してください。



この PCAP ファイルには何が表示されますか?

A. ユーザーエージェントは Mozilla/5.0 です。

B. HTTP GET はエンコードされます。

C. プロトコルは TCP です。

D. タイムスタンプがエラーで表示されます。

Answer: (解答を表示する**)**

最新問題**: 122**

SIEM と SOAR の違いは何ですか?

A. SOAR はセキュリティ アラートを予測して防止し、SIEM は攻撃パターンをチェックして緩和策を適用します。

B. SIEM はセキュリティ アラートを予測して防止し、SOAR は攻撃パターンをチェックして緩和策を適用します。

C. SIEM の主な機能は異常を収集して検出することですが、SOAR はセキュリティ オペレーションの自動化と対応に重点を置いています。

D. SOAR の主な機能は異常の収集と検出ですが、SIEM はセキュリティ オペレーションの自動化と対応に重点を置いています。
Answer: D (メーッセージを残す**)**

最新問題**: 123**
ユーザーが悪意のある添付ファイルを受け取りましたが、実行しませんでした。
侵入を分類するカテゴリはどれですか?
A. 武器化
B. 偵察
C. インストール
D. 配送
Answer: D (メーッセージを残す**)**
セクション: セキュリティの概念

最新問題**: 124**
定義を左側から右側のフェーズにドラッグ アンド ドロップして、サイバー キル チェーン モデルに従って侵入イベントを分類します。

Answer:

説明
配信: このステップでは、武器をターゲットに送信します。
兵器化: このステップでは、侵入者はターゲットの脆弱性を悪用するために、ウイルスやワームなどのマルウェア兵器を作成します。攻撃者のターゲットと目的に応じて、このマルウェアは検出されていない新しい脆弱性 (ゼロデイ エクスプロイトとも呼ばれる) を悪用したり、さまざまな脆弱性の組み合わせに焦点を合わせたりすることができます。

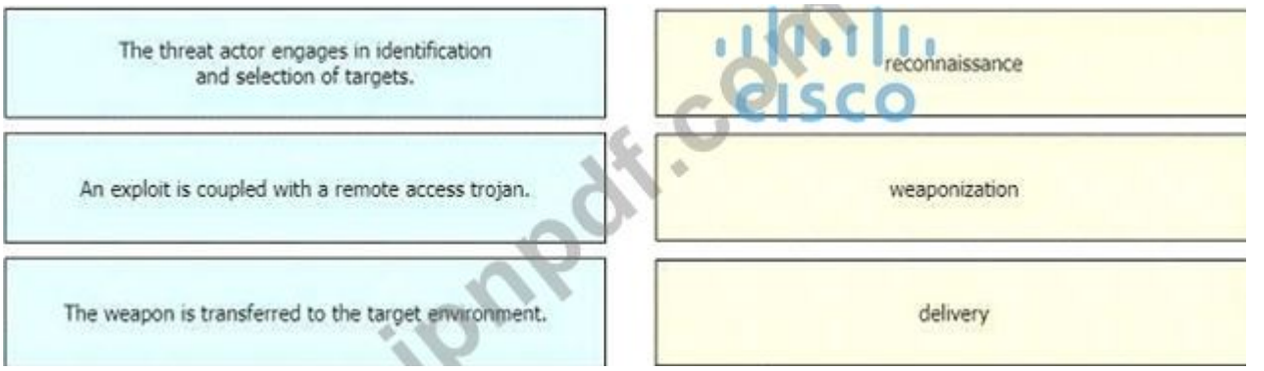
偵察: このステップでは、攻撃者/侵入者がターゲットを選択します。次に、このターゲットについて詳細な調査を行い、悪用される可能性のある脆弱性を特定します。

最新問題: **125**
セキュリティ アナリストは、ネットワークで使用するアプローチを決定するためにインライン トラフィック調査とトラフィック タップを比較する際に何を考慮する必要がありますか?
A. 質問をタップすると、トラフィックを分析するために信号が別のポートに複製されます
B. インライン調査は悪意のあるトラフィックを検出しますが、トラフィックをブロックしません
C. インライン調査により、トラフィックのコピーを表示して、トラフィックがセキュリティ ポリシーに準拠していることを確認できます
D. 調査をタップすることで、悪意のあるトラフィックを検出してブロックします
Answer: (解答を表示する**)**

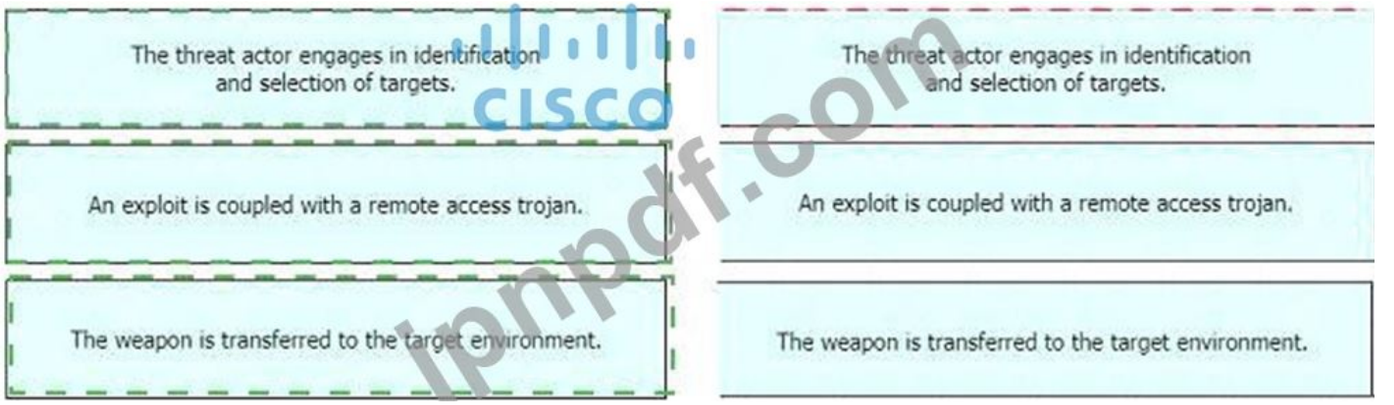
最新問題: **126**
セキュリティ アナリストは、着信トラフィックの急増に気づき、未知の送信者からの未知のパケットを検出します。さらに調査した結果、アナリストは、顧客が会社のサーバーにアクセスできないと主張していることを知りました。NIST SP800-61 によると、インシデント対応プロセスのどのフェーズがアナリスト?
A. 検出と分析
B. 事件後の活動
C. 準備
D. 封じ込め、根絶、回復
Answer: D (メーッセージを残す**)**

最新問題: **127**
バッファ オーバーフロー攻撃を防ぐアクションはどれですか?
A. 入力サニタイズ
B. Web ベースのアプリケーションを使用する
C. Linux オペレーティング システムを使用する場合
D. 変数のランダム化
Answer: (解答を表示する**)**

最新問題: **128**
定義を左側から右側のフェーズにドラッグ アンド ドロップして、サイバー キル チェーン モデルに従って侵入イベントを分類します。



Answer:



説明

配信: このステップでは、武器をターゲットに送信します。

兵器化: このステップでは、侵入者はターゲットの脆弱性を悪用するために、ウイルスやワームなどのマルウェア兵器を作成します。攻撃者のターゲットと目的に応じて、このマルウェアは検出されていない新しい脆弱性 (ゼロデイ エクスプロイトとも呼ばれる) を悪用したり、さまざまな脆弱性の組み合わせに焦点を合わせたりすることができます。

偵察: このステップでは、攻撃者/侵入者がターゲットを選択します。次に、このターゲットについて詳細な調査を行い、悪用される可能性のある脆弱性を特定します。

最新問題: **129**

展示を参照してください。

Severity	Date	Time	Sig ID	Source IP	Source Port	Dest IP	Dest Port	Description
6	Jan 15 2020	05:15:22	33883	62.5.22.54	22557	198.168.5.22	53	*

どのタイプのログが表示されますか?

A. プロキシ

B. ネットフロー

C. IDS

D. システム

Answer: D (メーッセージを残す**)**

最新問題: **130**

攻撃の影響を受けるすべてのホストを特定することが含まれるインシデント対応ステップはどれですか?
A. 検出と分析
B. 事件後の活動
C. 準備
D. 封じ込め、根絶、回復
Answer: (解答を表示する**)**
説明
3.3.3 攻撃ホストの特定 インシデントの処理中に、システム所有者や他のユーザーは、攻撃ホストを特定したい、または特定する必要がある場合があります。この情報は重要である可能性がありますが、インシデント対応担当者は通常、封じ込め、根絶、および回復に集中する必要があります。
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf インシデント対応の対応フェーズまたは封じ込めは、インシデント対応チームが影響を受けるシステムとのやり取りを開始し、試みを開始するポイントです。事件の結果としてこれ以上の被害が発生しないように。

最新問題**: 131**
侵入検知システムが多数のソースから異常に大量のスキャンを受信し始めた場合に示される回避技術はどれですか?
A. 資源枯渇
B. トンネリング
C. タイミングアタック
D. トラフィックの断片化
Answer: (解答を表示する**)**

最新問題**: 132**
Linux および Mac OS X オペレーティング システムを使用するオープンソースのパケット キャプチャ ツールはどれですか?
A. ネットスカウト
B. tcpdump
C. netsh
D. ソーラーウィンズ
Answer: B (メーッセージを残す**)**

最新問題**: 133**
セキュリティ エンジニアは、同じデータ センター内のファイルが競合他社に転送されたのと同じ日に撮影されたデータ センターに入る容疑者のビデオを持っています。
これはどのような証拠ですか？
A. 最良の証拠
B. 物的証拠
C. 一応の証拠

D. 間接証拠
Answer: (解答を表示する**)**

最新問題**: 134**
ビジネス サービスに影響を与える可能性のあるセキュリティ インシデントが発生しました。誰が攻撃を実行しますか?
A. マルウェア作成者
B. 攻撃者
C. バグ賞金稼ぎ
D. 直接の競合他社
Answer: A (メーッセージを残す**)**

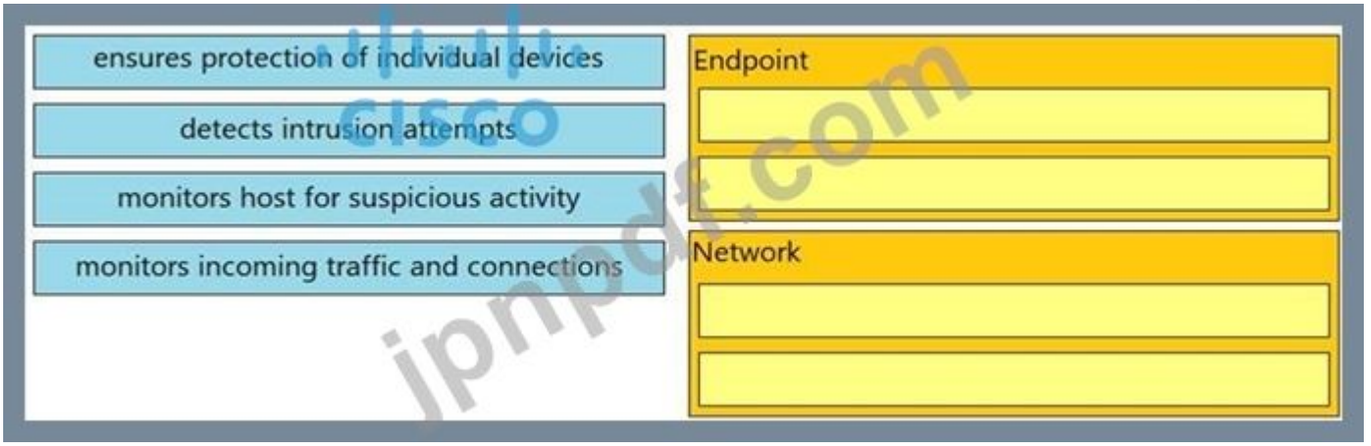
最新問題**: 135**
データの整合性を向上させるために IPS イベントを削除するときに使用されるプロセスはどれですか?
A. データの可用性
B. データの正規化
C. データ署名
D. データ保護
Answer: B (メーッセージを残す**)**

最新問題**: 136**
サイバー属性は調査で何を特定しますか?
A. 攻撃の原因
B. 攻撃の悪用
C. 攻撃の攻撃者
D. 悪用された脆弱性
Answer: C (メーッセージを残す**)**

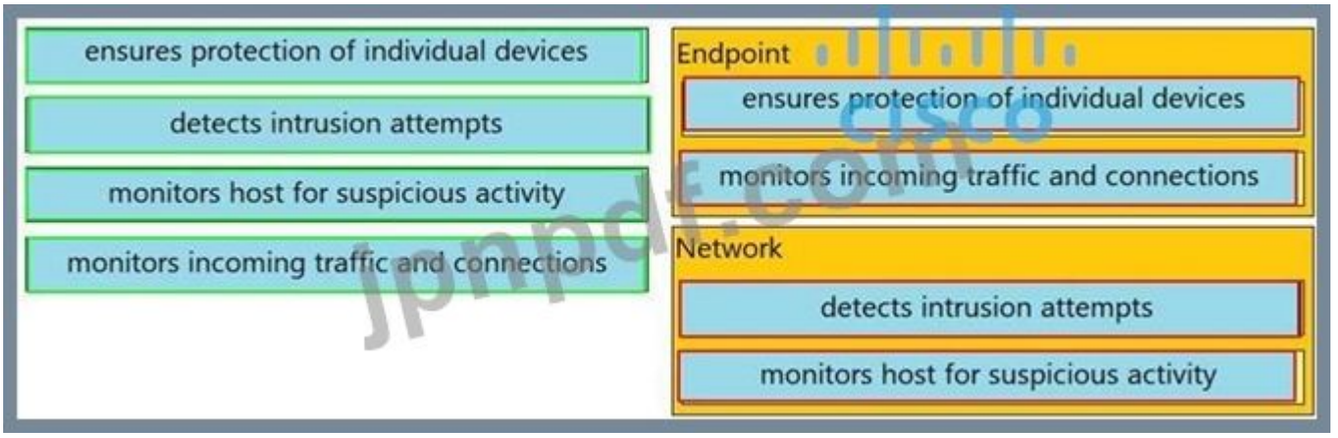
最新問題**: 137**
IPv4 プロトコル ヘッダーから収集される情報はどれですか? (2つ選んでください。)
A. トラフィックの送信元の TCP ポート

B. トラフィックの送信元の UDP ポート
C. パケットの送信元 IP アドレス
D. パケットの宛先 IP アドレス
E. トラフィックの宛先となる UDP ポート
Answer: C,D (メーッセージを残す**)**

最新問題**: 138**
左側の用途を右側のセキュリティ システムの種類にドラッグ アンド ドロップします。



Answer:

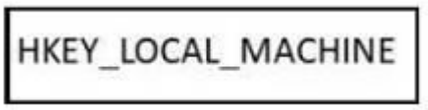


最新問題**: 139**
行動検出と比較した場合のルールベースの検出の違いは何ですか?
A. 行動システムは特定の攻撃シグネチャに一致するシーケンスを見つけますが、ルールベースは潜在的な攻撃を識別します。
B. ルールベースの検出では、特定の種類の攻撃に関連するパターンを検索しますが、動作による検出ではシグネチャごとに識別します。
C. ルールベースのシステムでは、新しいデータでは変化しないパターンが確立されていますが、動作は変化します。
D. 行動システムは何百人ものユーザーから事前に定義されたパターンですが、ルールベースはシグネチャを使用して潜在的に異常なパターンにのみフラグを立てます。
Answer: A (メーッセージを残す**)**

最新問題: **140**
正当なトラフィックをブロックしてネットワーク トラフィックに影響を与えるシグネチャはどれですか?
A. 偽陰性
B. 真陽性
C. 真陰性
D. 偽陽性
Answer: (解答を表示する**)**
セクション: ネットワーク侵入分析

最新問題: **141**
攻撃の影響を受けるすべてのホストを特定することが含まれるインシデント対応ステップはどれですか?
A. 検出と分析
B. 事件後の活動
C. 準備
D. 封じ込め、根絶、回復
Answer: (解答を表示する**)**
セクション: セキュリティ ポリシーと手順

最新問題: **142**
展示を参照してください。



この展示品で識別可能なコンポーネントはどれですか?
A. ローカル マシン上の信頼されたルート証明書ストア
B. Windows PowerShell 動詞
C. Windows レジストリ ハイブ
D. Windows サービス マネージャーのローカル サービス
Answer: C (メーッセージを残す**)**
説明
https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-hives
https://ldapwiki.com/wiki/HKEY_LOCAL_MACHINE#:~:text=HKEY_LOCAL_MACHINE%20Windows%20

最新問題: **143**
ツールを使用して元のデータとコピーされたデータのメッセージ ダイジェストを計算し、ダイジェストの類似性を比較する検証の種類はどれですか?
A. データ保存

B. 揮発性データ収集
C. データの整合性
D. 証拠収集順序
Answer: C (メーッセージを残す**)**

最新問題**: 144**

```
$ cuckoo submit --machine cuckoo1 /path/to/binary
```

展示を参照してください。どのイベントが発生していますか?
A. 「submit」という名前のバイナリが VM cuckoo1 で実行されています。
B. 悪意のあるバイナリが含まれているかどうかを確認するために、URL が評価されています。
C. VM cuckoo1 で実行するためにバイナリが送信されています。
D. VM cuckoo1 上のバイナリが評価のために送信されています。
Answer: (解答を表示する**)**

最新問題**: 145**
展示を参照してください。

```
GET /item.php?id=34' or sleep(10)
```

この要求は、データベースによって駆動される Web アプリケーション サーバーに送信されました。どのタイプの Web サーバー攻撃が代表されますか?
A. コマンド注入
B. ブラインド SQL インジェクション
C. パラメータ操作
D. ヒープ メモリの破損
Answer: B (メーッセージを残す**)**