LOGPOINT

リリースノート(VA)

Rev.2.4

2023.03.31

ジュピターテクノロジー

目次

変更履歴

版	発行日	変更内容
Rev. 1.0	2021/10/11	新規作成
Rev. 1.1	2022/01/21	V6.12.2 対応
Rev. 2.0	2022/05/31	V7.0.2 対応
Rev. 2.1	2022/09/22	V7.1.0 対応
Rev. 2.2	2022/10/22	V7.1.1 対応
Rev. 2.3	2023/03/28	V7.1.2 対応

Rev. 2.4	2023/03/31	V7.1.3 対応

お問合せ先、およびカスタマーポータル

ジュピターテクノロジー株式会社（Jupiter Technology Corp.）

住所：　〒183-0023 東京都府中市宮町一丁目 40 番地 KDX 府中ビル 6F
URL：　https://www.jtc-i.co.jp/
電話番号：　042-358-1251
FAX 番号：　042-360-6221

ご購入のお問い合わせ：
　　お問い合わせフォーム　https://www.jtc-i.co.jp/contact/scontact.php
製品サポートのお問い合わせ：
　　カスタマーポータル　https://www.jtc-i.co.jp/support/customerportal/
評価版のダウンロード：
　　https://www.jtc-i.co.jp/support/download/

1. Logpoint Version 7.1.3

Logpoint v7.1.3 パッチ

■リリースの詳細

Release Date: 2022-12-11
Download: logpoint-7.1.3.pak
SHA256: b6f572e22c7641fd96bbdca603b541bcb30ac33e7c5062029c6f74cc77a73e77

■インストール要件

- インストールには、少なくとも / に 500MB および /opt に 5GB の空きディスク容量が必要です。

■注意事項

- Logpoint v7.1.3 パッチは、Logpoint v7.1.0, v7.1.1 および v7.1.2 にインストールできます。
- Logpoint v7.1.3 パッチは、以下と互換性があります。
  Logpoint Search Master (LPSM) v2.1.1
  Director Fabric v2.1.2
  Director Console v2.1.2

■バグ修正

内容	Issue ID
すべての既存の Logpoint ユーザーは、Logpoint v7.1.3 にアップグレードした後、SOAR 設定、プレイブック、およびケースに対する完全な権限を持つようになりました。	LP-50424

■既知の問題

内容	Issue ID
ユーザー名にスペースやその他の特殊文字が含まれている場合、ユーザーは Duo 認証を使用して Logpoint にログインできません。	LP-45294

toList　プロセスコマンドは、リストの有効期限切れ後、動的リストを最新の値に更新しません。	LP-46808
インポートされたアラートルールは、エクスポートされたシステムからのすべてのリポジトリ構成を保持します。	LP-48142
ウィジェットまたはアラートルールのクエリで使用される動的リストが更新された場合、更新されたリストの結果は過去の時間間隔に反映されません。	LP-46874
ダッシュボードとアラートでの遅延したログの問題。	LP-34682

■プラグイン

更新バンドルアプリケーション

アプリケーション	更新バージョン
Alert Rules	5.3.14
CIFS Fetcher	5.1.1
Cisco	5.2.0
CloudTrail	5.2.0
Crowdstrike	5.0.0
CSV Enrichment Source	5.2.0
Deny All WAF	5.2.0
Evaluation Process Plugin	5.0.0
Event Hubs	5.1.4
FortiGate	5.2.1
FSecure	5.1.0
GateWatcher	5.0.0
Office 365	5.3.0
PostFix	5.1.0
SOAR	1.1.0
Sophos	5.2.0
TrendMicro	5.1.0
Thycotic	5.0.0
Universal REST API Fetcher	1.0.1
Windows	5.4.6

2. Logpoint Version 7.1.2（JTC リリース見送り）

Logpoint v7.1.2 パッチ

■リリースの詳細

Release Date: 2022-11-28
Download: logpoint-7.1.2.pak
SHA256: 103a0ce7992cc01f7bf4fcdddacb4fd661df85e414f8a098643f43d06c336a93

■重要

以前の Logpoint リリースから v7.1.2 にアップグレードすると、デフォルトで設定されている権限が、以前に作成されたプレイブックの実行に影響を与える可能性があります。この問題は v7.1.3 で修正されました。

■インストール要件

・ インストールには、少なくとも / に 500MB および /opt に 5GB の空きディスク容量が必要です。

■注意事項

・ Logpoint v7.1.2 パッチは、Logpoint v7.1.0 および LogPoint v7.1.1 にインストールできます。
・ Logpoint v7.1.1 パッチは、以下と互換性があります。
LogPoint Search Master (LPSM) v2.1.1
Director Fabric v2.1.2
Director Console v2.1.2

■新機能および改善点

内容	Issue ID
SOAR Settings, Playbooks, Cases のユーザーアクセスを Permission Groups を使用して制御できるようになりました。詳細については、「ユーザーアカウント管理」ガイドの「権限グループ」(Permission Groups)を参照してください。 v7.1.2 へのアップグレード後は、カスタム権限グループの SOAR 権限を手動で追加する必要があります。	LP-46511

■バグ修正

内容	Issue ID
バッファーを有効にした Logpoint コレクターは、エンリッチされたログのみをメインの Logpoint に転送していました。	LP-48029
toTable プロセスコマンドで、ダイナミックテーブルの NULL フィールドが検索結果に入力されないという問題がありました。	LP-49001
localhost をデバイスとする linux デバイスグループを選択した場合、生 syslog フォワーダーを設定することができませんでした。	LP-47060
生 syslog フォワーダーにおいて、ユーザーがデバイス設定のデバイスグループを変更しても、その更新が保存されないことがありました。	LP-49709
受信者欄に複数の電話番号が記載されていても、SMS アラート通知が 1 つの電話番号にしか送信されませんでした。	LP-49878
UEBA Overall Risk のページに、UEBA エンティティの全体的なリスク状況が表示されていないケースがありました。	LP-49970

■脆弱性の修正

内容	Issue ID
cronjob ファイルのパーミッションに誤りがあると、li-admin ユーザーがそのファイルに書き込みできる可能性があります。	LP-48885

■既知の問題

内容	Issue ID
以前の Logpoint リリースから v7.1.2 にアップグレードすると、デフォルトで設定されている権限が、以前に作成されたプレイブックの実行に影響を与える可能性	LP-50424

内容	Issue ID
があります。	
極端に遅延したログがダッシュボードやアラートで表示されない問題があります。	LP-34682
ウィジェットやアラートルールのクエリで使用するダイナミックリストが更新された場合、更新されたリストの結果が過去の時間間隔に反映されません。	LP-46874
インポートされたアラートルールは、エクスポートされたシステムからすべてのレポ設定を引き継ぐ問題があります。	LP-48142

■プラグイン

更新バンドルアプリケーション

アプリケーション	更新バージョン
Alert Rules	5.3.14
CIFS Fetcher	5.1.1
CloudTrail	5.2.0
CSV Enrichment Source	5.2.0
Evaluation Process Plugin	5.0.0
Event Hubs	5.1.4
Office 365	5.3.0
SOAR	1.1.0
Sophos	5.2.0
Universal REST API Fetcher	1.0.1
Windows	5.4.6

新規バンドルアプリケーション

アプリケーション	バージョン
Crowdstrike	5.0.0
Thycotic	5.0.0

3. Logpoint Version 7.1.1（JTC リリース見送り）

Logpoint v7.1.1 パッチ

■リリースの詳細

Name:	Logpoint
Version:	7.1.1
Type:	FlexPatch
Severity	Optional
Dependency	7.1.0
Release Date:	2022-09-27
Download	logpoint-7.1.1.pak
SHA256:	852f55acfd96fd90e13f3e1d0f8f61f63cda794edff14a396094878293884f99

■インストール要件

- インストールには、少なくとも /に 500MB および/opt に 5GB の空きディスク容量が必要です。
- .pak ファイルをアップロードした後、Updates ページを更新すると、アップロードされたファイルが表示されます。

■注意事項

- Logpoint v7.1.1 パッチは、Logpoint v7.1.0 にインストールできます。
- Logpoint v7.1.1 パッチは、以下と互換性があります。

  LogPoint Search Master (LPSM) v2.1.1

  Director Fabric v2.1.1

  Director Console v2.1.1

■新機能および改善点

SMS アラート通知

内容	Issue ID
SMS(ショートメッセージ)アラートルール通知を設定できるようになりました。アラー	LP-47864

トルールがトリガーされると、Logpoint はーつまたは複数の電話番号に SMS 通知を送信します。 詳細については、「アラートとインシデント」ガイドの「SMS 通知の設定」を参照してください。	

その他の改善点

内容	Issue ID
Logpoint UEBA では、エンティティ選択時に User Principal Name (UPN) とユーザーエンティティを対応付けることもできるようになりました。	LP-48907

■バグ修正

内容	Issue ID
32KB を超えるフィールドサイズを持つログを受信したときに発生する例外により、インデックス作成サービスが再起動することがありました。適切な例外処理が実装され、このような場合に監査ログが生成されるようになりました。	LP-46844
インデックス分割の問題で、大きなキューがシステムに組み込まれていました。	LP-45211
生 syslog フォワーダーで構成されたシステムで、遅いネットワーク接続により、ログ収集パイプラインに大きなキューを作成することがありました。	LP-48260
分散 Logpoint セットアップの場合、リモート Logpoint のデバイス設定とリポジトリ設定にサーチヘッドからアクセスできませんでした。	LP-48537
SSL のバッファーサイズを超えるログを処理する際、SSL 接続セッションで接続が適切に終了しなかった場合、Syslog コレクターは最後のログイベントを収集しませんでした。	LP-48800
ユーザーは、特殊文字を含むパスワードを変更することができませんでした。	LP-49299
syslog_time と datetime デファイナーは、ログイベント内の曜日と月の間に余分な空白文字があるタイムスタンプを解析しませんでした。	LP-48429

■脆弱性の修正

内容	Issue ID
検索テンプレートにテンプレートインジェクションの脆弱性があり、テンプレートに不正な入力ができる可能性がありました。	LP-48882

■既知の問題

内容	Issue ID
大幅に遅延したログが、Logpoint のダッシュボードやアラートで表示されないことがあります。アラートとダッシュボードのエンジンはリアルタイムのログで動作するため、古いタイムスタンプのログが Logpoint に到着し、その監視時間間隔内の結果がすでに計算されている場合、そのログは表示されません。	LP-34682
ウィジェットまたはアラートルールのクエリで使用されている動的リストが更新されると、過去の時間間隔のエントリがリストに含まれません。	LP-46874
インポートされたアラートルールは、エクスポートしたシステムのすべてのレポジトリ設定を引き継ぎます。 回避策:インポートされたアラートルールのレポジトリを個別に、または一括して編集して設定することができます。	LP-48142

■プラグイン

以下のバンドルアプリケーションを更新しました。

アプリケーション	更新バージョン
SOAR	1.0.4
Alert Rules	5.3.12
Cisco	5.2.0
Deny All WAF	5.2.0
FortiGate	5.2.1
FSecure	5.1.0
PostFix	5.1.0
TrendMicro	5.1.0
Windows	5.4.5

新たに以下のアプリケーションをバンドルしました。

アプリケーション	バージョン
GateWatcher	5.0.0

4. LogPoint Version 7.1.0

■Release Date: 2022-07-26

■ダウンロード製品とチェックサム

製品	SHA256 チェックサム
LogPoint v7.1.0 OVA	c9be90294a4901984c95dc9706ddbe5663e2ca5e6d855475ede850b7ba1d3ec3
LogPoint v7.1.0 Hyper-V VHD	292a36e9fac4ae9c86369fb0aaff35456995f27350844f3f704caf488596fb69
LogPoint v7.1.0 AMI	LogPoint の AMI または Azure VHD を入手される場合は、弊社までご連絡ください。
LogPoint v7.1.0 Azure VHD	
logpoint_7.1.0.pak	da47fa93b0102de7c76d230b7c6446ec33264496bd49124028d18e3aa8eb44fb

■インストール要件

- パッチアップグレードには、/に最低 500MB、および/opt に最低 5GB の空きディスク容量が必要です。
- LogPoint AMI, OVA, VHD のデプロイ時には、150GB のディスク容量が必要です。

■注意事項

- LogPoint v7.1.0は、以下と互換性があります。
  LogPoint Search Master (LPSM) v2.1.0
  Director Fabric v2.1.0
  Director Console v2.1.0

LogPoint v7.1.0 パッチ

- LogPoint v7.1.0 パッチは、以下に対してインストールすることができます。
  LogPoint v7.0.0
  LogPoint v7.0.1
  LogPoint v7.0.2
- パッチアップグレードをスムーズに行うために、十分なシステムリソースを確保してください。
- 生 syslog フォワーダーのリモートターゲットがダウンしている場合、ログは一時的にシステムデータベースに保存されます。この場合、v7.1.0 へのアップグレードは、データベースの移行のために比較的時間がかかります。
- インストール後、システムが再起動します。

■新機能および改善事項

システムアップグレード

- LogPoint のベースオペレーティングシステムは、Ubuntu 20.04.4 にアップグレードされました。

ユニバーサル REST API フェッチャー

- LogPoint は、ユニバーサル REST API フェッチャー v1.0.0 をバンドルしています。詳細については、Universal REST API ガイドを参照してください。

UEBA

内容	Issue ID
UEBA 機能を有効にした場合、ナビゲーションバーから UEBA にアクセスできるようになりました。UEBA UI のルック&フィールが更新され、ユーザーエクスペリエンスが向上しました。[Overall Risk]ページで、以下のことができるようになりました。 ・ リスク上位 5 件とそのリスクスコアの表示 ・ 全体のリスクレベルとリスクの傾向、分析されたイベントと発見された異常の表示 さらに、[Explore]ページは、users、shares、servers、websites などの個別の[Entity]ページに置き換えられています。[Entity]ページでは、以下のことが可能です。 ・ [Matrix of Anomalies]チャートの閲覧	LP-45098

・ 各エンティティの詳細を表示 ・ 選択した時間範囲に基づくエンティティおよび異常のフィルタリング ・ 異常のリスクレベルに基づいた異常のフィルタリング ・ フィルタラベルに基づく異常のフィルタリング ・ 異常からのインシデントの作成 ・ 異常からの生イベントの検索 ・ エンティティの概要の表示 ・ レポートの生成 詳細については、UEBA Guide を参照してください。	
異常検知のデータソースとして SAP 認証を利用できるようになりました。詳しくは UEBA ガイドの[Data Sources for UEBA]をご覧ください。	LP-45447

SOAR

内容	Issue ID
SOAR UI のルック＆フィールを更新し、ユーザーエクスペリエンスを向上させました。 以下は、プレイブックの改善点です。 ・ プレイブックを追加する際に、[Add Action]ボタンにドラッグ＆ドロップのオプションが追加され、トリガーブロックの出力ノートをダブルクリックする方法を置き換えました。 ・ プレイブックによって自動的に作成されたケースを処理するために、[Edit Playbook Configuration]に SLA サポートを有効にする機能が追加され、[Reports]ページで SLA レポートが生成されるようになりました。 ・ プレイブックアクションタイプに[Description]フィールドが追加されました。 ・ プレイブックアクションタイプは、タイプによって色分けされるようになりました。 ・ 新規の[Export]ボタンをクリックして、プレイブックをエクスポートするようになりました。 プレイブックキャンバスビューに、新規に[Zoom In]、[Zoom Out]、[Fit Playbook to Canvas]ボタンが追加されました。 ・ プレイブックモニタリングページに新しい日付範囲ピッカーが追加され、ビュー内のプレイブックを日付によってフィルタリングすることができるようになりました。 ・ プレイブックモニタリングページに新規に更新ボタンが追加されました。 ・ [Automation Configuration]ページでは、オートメーションを追加する際	–

の[Triage]セクションが廃止されました。 ・ [Playbooks]ページの、エクスポート、クローン、および削除のアクションは、[Actions]列に移動されました。 ・ プレイブック一覧は、プレイブックの[Name]または[Category]に従ってソートすることができます。 以下は SOAR 設定の改善点です。 ・ 新しい部品アイコン ・ システムヘルスと実行追跡の追加 以下は、Cases ページの改善点です。 ・ [Run Playbooks]ボタンが[Cases Investigation]ページから個々のケースページに移動しました。 詳細については、Cases、Playbooks、SOAR Settings ガイドを参照してください。	

監査ログの強化

内容	Issue ID
以下のコンポーネントのアップデートに関する監査ログが強化され、previous_config と updated_config フィールドが含まれるようになりました。 ・ アラートルール ・ デバイスとそのコレクター、フェッチャー ・ 正規化パッケージと正規化ポリシー ・ ユーザー、ユーザーグループ、オブジェクトのパーミッション ・ レポジトリ、ルーティングポリシー、プロセシングポリシー ・ 一般設定、ロックアウトポリシー、NTP 設定 ・ マクロ 新しいフィールドが追加されたことで、システムの変更点を容易に把握することができるようになりました。	LP-44448, LP-46419, LP-28702

システム監視

内容	Issue ID
SNMP を使用して、マルチパスデバイスを持つシステムのすべての LUN のステータスを容易に監視できるようになりました。	LP-39224

新しい SNMP OID の一覧については、System Configuration ガイドの SNMP Monitoring を参照してください。	

アラートとインシデント

内容	Issue ID
LogPoint は、アラートルールをエクスポートする際に、.pak ファイルにアラートルールのレポジトリの設定を保存するようになりました。アラートルールをインポートする際、エクスポートされたアラートルールから、インポートしようとしているユーザーが利用できるレポジトリとその設定のみが選択されます。 詳細については、Alerts and Incidents ガイドの Importing Alert Rules を参照してください。	LP-41959
通知が有効なアラートルールは、[Actions]列に固定のベルアイコンが表示され、識別できるようになりました。詳細については、Alerts and Incidents ガイドの Setting UP Alert Notification を参照してください。	LP-44374

LogPoint Director

内容	Issue ID
LogPoint Director 設定に[SSH Settings]タブが追加されました。詳細は、Director Configuration ガイドの SSH Settings を参照してください。	COM-15868

その他の改善点

内容	Issue ID
検索テンプレート、レポートテンプレート、ダッシュボード、アラートルールを、空のユーザーグループとも共有できるようになりました。グループの共有権限は、ユーザーを追加または削除した場合に自動的に反映されます。	LP-44039
UI のルック&フィールが新しくなり、モダンな外見に加え、ユーザーエクスペリエンスの向上をもたらしました。 ・ [My Preferences]のレイアウトが更新され、ナビゲーションバーからアクセスできるようになりました。[User] > [My Preference]の順にクリックします。 ・ [Notifications]がナビゲーションバーに移動しました。また、[Notifications]ドロワーの UI も更新されました。 ・ LogPoint からログアウトするには、ナビゲーションバーで[User] >	LP-45754

[Logout]の順にクリックします。 ・ ナビゲーションバーに新しい[Help]メニューが追加されました。[Help]では、[Documentation]、[Help Center]、[Contact Support]、[Feedback]、[EULA]にアクセスできます。また、[Help]メニューの[About LogPoint]をクリックすると、使用中の LogPoint のバージョン情報を確認することができます。 ・ ナビゲーションバーから[My Saved Search]、[My Dashboard]、[My Search History]へのショートカットリンクが削除されました。ナビゲーションバーの時計は、[My Preferences]の[Date/Time Preference]に移動しました。	
mac_address と jdatetime の二つのデファイナーが追加されました。詳しくは Data Integration ガイドの List of Definers をご覧ください。	LP-43322
TCP と UDP の両モードで、生 syslog フォワーダーのパフォーマンスが向上しました。生 syslog フォワーダーでは、ログ転送速度が大幅に向上しました。	LP-42787
集計関数の検索結果の内部上限を 50 万件に引き上げました。これにより、LogPoint は非常に多くのログを処理することができ、より良い検索体験を提供します。	LP-13595
LogPoint は、SNMP 監視のための OID のリストを含む MIB ファイルを Help Center で提供するようにしました。	LP-10074
エンリッチメントデータベースからのデータ取得の実装を改善し、データの冗長性の低減、検索時間の改善、リソース消費量の削減を実現しました。	LP-40353
多くのレポジトリが存在するシステムにおいて、大規模なシステム更新やデータ処理に対応するため、最大許容プロセス数の上限を増加しました。 最大許容ユーザープロセス数は、システムによって動的に設定されます。しかし、ユーザーの要件に応じて変更することができます。	LP-45549

■バグ修正

検索と視覚化

内容	Issue ID
Single Aggregation with Grouping クエリが同じグルーピングパラメータで複数行の結果を返した場合、Sankey チャートはそのうちの 1 行の結果のみを表示していました。	LP-43405
並び替えコマンドを持たない検索クエリで大量の検索結果を処理すると、検索結	LP-13595

果に矛盾が生じることがありました。	
特定のタイムスタンプで受信したログは、ログを収集しているにもかかわらず、検索結果に表示されない場合がありました。	LP-43252
LogPoint で定義された正規表現 datetime_m デファイナーで norm on コマンドを使用すると、結果が表示されませんでした。	LP-43322
rex on コマンドでチャート集計を行うと、結果が表示されませんでした。	LP-46239
norm コマンドによるクエリを syslog_time デファイナーと共に使用すると、期待される値が抽出されないことがありました。	LP-46517
相関クエリの処理中にシステムが大量のメモリを確保し、処理を停止してもメモリが解放されないことがありました。	LP-45543, LP-45552

ログ収集

内容	Issue ID
syslog コレクターが UDP 経由でログを収集すると、大きなログの一部が欠けることがありました。大きなログに続く小さなログも消えることがありました。	LP-16579
syslog コレクターで、SSL 接続と TCP 接続から同時に受信したログを転送できないことがありました。	LP-41758
LogPoint がコレクターやフェッチャーから受け取った大きなログファイルを処理しなければならないとき、ログ収集が遅延することがありました。	LP-40498
ポート 514 の UDP 経由でログを収集する際、syslog コレクターがクラッシュすることがありました。	LP-39778
インデックス作成の際、インデックスのプロパティが正しくないためにシステム内に大きなキューが作成され、ログ収集に影響を与えることがありました。	LP-45211, LP-45876

生 syslog フォワーダー

内容	Issue ID
生 syslog フォワーダーを追加する際に、他の生 syslog フォワーダーで既に使用されているデバイスも選択できていました。現在、使用中のデバイスは非表示にするようにしました。	LP-37427
短時間に大量のログを生 syslog フォワーダーに送信する際に、システム内に大きなキューが作成され、メモリの使用量が多くなる問題が発生していました。	LP-42787, LP-42771, LP-42032

SOAR

内容	Issue ID

SOAR API のアクションは、デフォルトでは出力に rawResponse フィールドを提供していませんでした。	LSB-54
lp-incidents-dispatcher パーサーは、LogPoint SIEM for SOAR からのインシデントをパースしませんでした。	LSB-52
子プレイブックのステータスが Failed であっても、親プレイブックのステータスは常に Succeeded になっていました。	LSB-50

LogPoint OVA

内容	Issue ID
LogPoint OVA を基にしたシステムで、再起動するたびに、空でないマシン識別子に関する不要なエラーが表示される不具合を修正しました。	LP-44472

その他のバグ修正

内容	Issue ID
ブラウザの拡張機能で API リクエストを送信すると、UI 側でも API ユーザーが認証され、UI ユーザーがログアウトされてしまうことがありました。	LP-44326
バックアップ処理中の内部 CLI 引数の一部を監視ツールが表示できていました。	LP-44740
エンリッチメントサブスクライバーシステムで、LogPoint Sync が一部のエンリッチメントソースとポリシーをインポートできないことがありました。	LP-45243
一部の画面解像度では、[SMTP]メニューに[Test SMTP]ボタンが表示されないことがありました。	LP-44686
エンリッチメントデータベースが、設定されたフェッチ間隔通りに更新されない場合がありました。	LP-41652
検索テンプレートウィジェットで一度検索結果が表示されないと、パラメータを更新しても結果が表示されないままでした。この問題は、ユーザーがページを更新することで解決していました。	LP-47029
LogPoint で、検索クエリがキューに保持されているために、ダッシュボードへの入力、レポートの生成、アラートのトリガー、または検索結果の生成ができないことがありました。また、これが原因でメモリーリークが発生することもありました。	LP-43850

■脆弱性の修正

内容	Issue ID
カーネルに領域外メモリアクセスの欠陥があり、システムクラッシュや権限昇格を引き起こす可能性がありました。この脆弱性は、Linux カーネルを v5.4.0-105 に更新することで対処しました。	LP-46102

Apache commons-collections:commons-collections パッケージにデシリアライズの脆弱性があり、任意の Java コードが実行される可能性がありました。	LP-47204
nginx バージョン 0.6.x から 1.20.1 に、巧妙に作成した DNS 応答を使用して 1 バイトのメモリ上書きを引き起こす脆弱性があり、ワーカープロセスのクラッシュや任意のリモートコードの実行を引き起こす可能性がありました。	LP-44772
LDAP 認証使用時のログインの脆弱性により、ユーザー名フィールドで HTML や JavaScript のタグを使用される可能性がありました。	LP-47311

■既知の問題

内容	Issue ID
LogPoint に到着したログが大幅に遅延し、ダッシュボードやアラートに表示されないことがあります。アラートおよびダッシュボードエンジンはリアルタイムのログで動作するため、古いタイムスタンプのログが LogPoint に到着し、その時間間隔内の結果がすでに計算されている場合、そのログは表示されないためです。	LP-34682
ウィジェットやアラートルールのクエリで使用される動的リストが更新された場合、更新されたリストの結果が過去の時間間隔に対して反映されないという問題があります。	LP-46874
インポートされたアラートルールは、エクスポートされたシステムのすべてのレポジトリ設定を引き継ぎます。 回避策：インポートされたアラートルールのレポジトリを個別に、または一括して編集して設定することができます。	LP-48142
生 syslog フォワーダーで構築されたシステムでは、低速のネットワーク接続により、ログ収集パイプラインで LogPoint が大きなキューを生成する場合があります。この問題のトラブルシューティングについては、弊社サポートにお問い合わせください。	LP-48260

■非推奨の機能

現在の SNMP 監視用 OID は、将来のバージョンで非推奨となり、新しい OID に置き換えられる予定です。

■プラグイン

以下のバンドルアプリケーションを更新しました。

アプリケーション	更新バージョン
Experimental Median Quartile Quantile	5.0.0
GEOIP	5.1.0
Look Up Process	5.1.0
Mitre Dataset Updater	6.1.0
ODBC Fetcher	5.0.1
Threat Intelligence	6.1.0
UEBA PreConfiguration	5.0.2
Vulnerability Management	6.1.1
Alert Rules	5.3.9
Barracuda	5.3.0
Cisco	5.1.0
Citrix	5.2.0
Cylance	5.0.3
FortiGate	5.2.0
JSON Normalizer	5.1.0
McAfee EPO	5.1.0
Oracle	5.0.3
PaloAlto Network Firewall	5.3.0
PfSense Firewall	5.0.1
Sonicwall Firewall	5.1.0
Unix	5.2.1
UseCases	5.1.2
Windows	5.4.4

新たに以下のアプリケーションをバンドルしました。

アプリケーション	バージョン
AzureLogAnalytics	5.0.2
BoxAudit	5.1.1
CiscoAMP	5.2.0
CiscoUmbrella	5.2.0
Cloud Trail	5.0.2
CloudWatch	5.0.1
Duo Security	5.0.0
EventHubs	5.1.1

アプリケーション	バージョン
GSuite	6.0.0
Incapsula	6.0.0
LogPoint Agent Collector	5.2.2
MicrosoftDefenderATP	5.1.0
MysqlRDS	5.0.1
Office365	5.2.0
Salesforce	5.0.0
SymantecCloudSecurity	5.0.1
VeritasSaaSBackup	5.0.0
VirusTotal	5.0.0
VPCFlowLog	5.0.1
UEBA Analytics	5.1.0
Universal REST API Fetcher	1.0.0
WebSense	5.2.0

バンドルされているアプリケーションの詳細な一覧については、Install and Upgrade Guide の Bundled Applications の項を参照してください。

5. LogPoint Version 7.0.2

LogPoint v7.0.2 パッチ

■リリースの詳細

Name: LogPoint
Version: 7.0.2
Type: FlexPatch
Severity Optional
Dependency 7.0.0, 7.0.1
Release Date: 2022-03-31
Download LogPoint-7.0.2.pak
SHA256: 4bab86798163d96a732c31f0faeb271e36038283f751eabef774c9e37d98be7a

■インストール要件

・ インストールには、/および/opt に最低 500MB の空きディスク容量が必要です。

・ .pak ファイルをアップロードした後、Updates ページを更新すると、アップロードされたファイルが表示されます。

■注意事項

・ LogPoint v7.0.2 は、LogPoint v7.0.0, v7.0.1 にインストールできます。
・ LogPoint v7.0.2 は、以下と互換性があります。
LogPoint Search Master (LPSM) v2.0.0
Director Fabric v2.0.0
Director Console v2.0.0

■バグ修正

内容	Issue ID
FTP コレクターが複数の同時接続を処理する場合に、新しいリクエストを処理できない問題。	LP-45817

■脆弱性の修正

内容	Issue ID
OpenSSL に自己署名証明書を使用すると、証明書の解析中に無限ループが発生する脆弱性があり、サービス拒否につながる可能性がありました。	LP-46217

6. LogPoint Version 7.0.1（JTC リリース見送り）

LogPoint v7.0.1 パッチ

■リリースの詳細

Name: LogPoint
Version: 7.0.1
Type: FlexPatch
Severity Optional
Dependency 7.0.0
Release Date: 2022-03-09
Download LogPoint-7.0.1.pak
SHA256: 81dca84230c309fb080b163572ca6f6e916f50291780ef0832a01adf17246741

■インストール要件

- インストールには、/および/opt に最低 500MB の空きディスク容量が必要です。
- .pak ファイルをアップロードした後、Updates ページを更新すると、アップロードされたファイルが表示されます。

■注意事項

- LogPoint v7.0.1 パッチは、LogPoint v7.0.0 にインストールできます。
- LogPoint v7.0.1 パッチは、以下と互換性があります。
  LogPoint Search Master (LPSM) v2.0.0
  Director Fabric v2.0.0
  Director Console v2.0.0
- LogPoint v7.0.1 パッチは、LogPoint がリリースしているプラグインにのみ対応し、また v3.0.0 以降のプラグインにのみ対応しています。

■バグ修正

内容	Issue ID
timechart クエリに少なくとも一つのグルーピングパラメータを使用した場合、結果の最初の行の値が結果テーブル全体とチャートで繰り返された問題。	LP-45564
特定のフォーマットに一致するログファイルが、.CSV ファイルタイプであると誤って識別され、SCP Fetcher と FileSystem Collector によって廃棄される場合があるというログ収集の問題。	LP-44752

■脆弱性の修正

内容	Issue ID
policykit-1 にローカル権限昇格の脆弱性があり、攻撃者が環境変数を利用して root 権限を取得できる可能性がありました。	LP-45471
LogPoint は、ロギングに Log4j の代わりに Logback ライブラリを使用するようになりました。	LP-44894

7. LogPoint Version 7.0.0（JTC リリース見送り）

LogPoint v7.0.0 OVA

■リリースの詳細

Name:	LogPoint OVA
Version:	7.0.0
Type:	OVA
Release Date:	2022-02-28
Download	LogPoint-7.0.0.ova
SHA256:	84df1669ccb84244c53916de5e53b91c2c80eb24bd0bc8f2d875a66e935a8d88

■インストール要件

・インストールには、最低 150GB の空きディスク容量が必要です。

■注意事項

- LogPoint v7.0.0 OVA は、LogPoint v7.0.0 パッチの全機能を含んでいます。詳細は、「LogPoint v7.0.0 パッチ」のリリースノートを参照してください。
- LogPoint v7.0.0 OVA は、VMWare ESXi server v6.0 以降にインストールできます。
- LogPoint v7.0.0 OVA は、ext4 ファイルシステムをベースにしています。
- LogPoint v7.0.0 OVA は、Open VM tools を含んでいます。
- LogPoint v7.0.0 OVA は、以下と互換性があります。

  LogPoint Search Master (LPSM) v2.0.0

  Director Fabric v2.0.0

  Director Console v2.0.0

■改善内容

内容	Issue ID
LogPoint は、デフォルトで/, /boot, /opt, /opt/immune/app_store および /opt/immune/storage パーティションを単一の論理ボリュームとしてグループ化するようにしました。さらに、長期保存の要件に対応するために、パーティションのディスク容量を増加しました。	LP-33946
サポート接続がデフォルトで無効になりました。有効にするには、System Settings >> Support Connection に移動して設定します。	LP-41941
LogPoint のインストーラーは、インストール時にデフォルトで 8GB の専用スワップパーティションを構成するようになりました。スワップパーティションは RAW パーティションとなり、ファイルシステムは割り当てられません。	LP-43698, LP-45359

■バグ修正

内容	Issue ID
1 個の OVA からインストールされたすべての LogPoint インスタンスのマシン ID が	LP-43131

同じになっていました。各 LogPoint インストールの最初のブート時に一意のマシン ID が生成されるようになりました。	

LogPoint v7.0.0 Hyper-V VHD

■リリースの詳細

Name: LogPoint Hyper-V VHD
Version: 7.0.0
Type: VHD
Release Date: 2022-02-28
Download LogPoint-7.0.0.vhd
SHA256: 0454c04b8ec4775930e36cb58a11535791e24f291e5d03d5640dcf53f4ccc18f

■インストール要件

- インストールには、最低 150GB の空きディスク容量が必要です。

■注意事項

- LogPoint v7.0.0 Hyper-V VHD は、LogPoint v7.0.0 パッチの全機能を含んでいます。詳細は、「LogPoint v7.0.0 パッチ」のリリースノートを参照してください。
- LogPoint v7.0.0 Hyper-V VHD は、Microsoft Hyper-V Server 2016 以降でサポートされます。
- LogPoint v7.0.0 Hyper-V VHD は、ext4 ファイルシステムをベースにしています。
- LogPoint v7.0.0 Hyper-V VHD は、動的に拡張される VHD ファイルであり、ディスクストレージはオンデマンドでのみ割り当てられます。固定サイズの VHD ファイルは、VHD ファイル作成時にディスクストレージが即座に割り当てられます。Hyper-V Manager アプリケーションの Edit Disk ユーティリティを使用して、VHD を固定サイズの VHD ファイルに変換できます。
- LogPoint v7.0.0 Hyper-V VHD は、1 個の VHD から 1 個の LogPoint インスタンスを起動します。LogPoint の複数インスタンスを起動するには、元の VHD から必要な数のコピーを作成し、それらの各々から LogPoint インスタンスを起動します。
- LogPoint v7.0.0 Hyper-V VHD は、VHD 起動後に行われた変更と設定は、すべて LogPoint によって書き込まれます。ダウンロードした VHD は元の状態で保存し、そのコピーからのみ LogPoint インスタンスを起動することを推奨します。
- LogPoint v7.0.0 Hyper-V VHD は、以下と互換性があります。
  LogPoint Search Master (LPSM) v2.0.0
  Director Fabric v2.0.0
  Director Console v2.0.0

■改善内容

内容	Issue ID
LogPoint は、デフォルトで/, /boot, /opt, /opt/immune/app_store および /opt/immune/storage パーティションを単一の論理ボリュームグループにグループ化するようにしました。さらに、パーティション内のディスク容量を、長期的なストレージ要件に対応するために増加しました。	LP-33946
サポート接続をデフォルトで無効にしました。有効にするには、System Settings >> Support Connection に移動して設定します。	LP-41941
LogPoint のインストーラーは、インストール時にデフォルトで 8GB の専用スワップパーティションを構成するようになりました。スワップパーティションは RAW パーティションとなり、ファイルシステムは割り当てられません。	LP-43698, LP-45359

■バグ修正

内容	Issue ID
1 個の Hyper-V VHD からインストールされたすべての LogPoint インスタンスのマシン ID が同じになっていました。各 LogPoint インストールの最初のブート時に一意のマシン ID が生成されるようになりました。	LP-43131

LogPoint v7.0.0 Azure VHD

■リリースの詳細

Name: LogPoint Azure VHD
Version: 7.0.0
Type: VHD
Release Date: 2022-02-28

■インストール要件

- インストールには、最低 150GB の空きディスク容量が必要です。
- LogPoint v7.0.0 Azure VHD を入手する場合、弊社まで連絡をください。

■主な情報

- LogPoint v7.0.0 Azure VHD は、LogPoint v7.0.0 パッチの全機能を含んでいます。詳細は、「LogPoint v7.0.0 パッチ」のリリースノートを参照してください。
- LogPoint v7.0.0 Azure VHD は、ext4 ファイルシステムをベースにしています。
- LogPoint v7.0.0 Azure VHD は、Waagent に必要なパッケージが含まれています。

■改善内容

内容	Issue ID
LogPoint は、デフォルトで/, /boot, /opt, /opt/immune/app_store および /opt/immune/storage パーティションを単一の論理ボリュームグループにグループ化するようにしました。さらに、パーティション内のディスク容量を、長期的なストレージ要件に対応するために増加しました。	LP-33946
サポート接続をデフォルトで無効にしました。有効にするには、System Settings >> Support Connection に移動して設定します。	LP-41941
LogPoint のインストーラーは、インストール時にデフォルトで 8GB の専用スワップパーティションを構成するようになりました。スワップパーティションは RAW パーティションとなり、ファイルシステムは割り当てられません。	LP-43698, LP-45359

■バグ修正

内容	Issue ID
1 個の Azure VHD からインストールされたすべての LogPoint インスタンスのマシン ID が同じになっていました。各 LogPoint インストールの最初のブート時に一意のマシン ID が生成されるようになりました。	LP-43131

LogPoint v7.0.0 AMI

■リリースの詳細

Name: LogPoint
Version: 7.0.0
Type: AMI
Release Date: 2022-02-28

■インストール要件

- インストールには、最低 150GB の空きディスク容量が必要です。
- LogPoint v7.0.0 AMI を入手する場合、弊社まで連絡をください。その際に AWS Account Number と Deployment Region の情報の提供をお願いいたします。

■注意事項

- LogPoint v7.0.0 AMI は、LogPoint v7.0.0 パッチの全機能を含んでいます。詳細は、「LogPoint v7.0.0 パッチ」のリリースノートを参照してください。

- LogPoint v7.0.0 AMI は、ext4 ファイルシステムをベースにしています。
- LogPoint v7.0.0 AMI は、以下と互換性があります。
  LogPoint Search Master (LPSM) v2.0.0
  Director Fabric v2.0.0
  Director Console v2.0.0

■改善内容

内容	Issue ID
LogPoint は、デフォルトで/, /boot, /opt, /opt/immune/app_store および /opt/immune/storage パーティションを単一の論理ボリュームグループにグループ化するようにしました。さらに、パーティション内のディスク容量を、長期的なストレージ要件に対応するために増加しました。	LP-33946
サポート接続をデフォルトで無効にしました。有効にするには、System Settings >> Support Connection に移動して設定します。	LP-41941
LogPoint のインストーラーは、インストール時にデフォルトで 8GB の専用スワップパーティションを構成するようになりました。スワップパーティションは RAW パーティションとなり、ファイルシステムは割り当てられません。	LP-43698, LP-45359

■バグ修正

内容	Issue ID
1 個の Azure VHD からインストールされたすべての LogPoint インスタンスのマシン ID が同じになっていました。各 LogPoint インストールの最初のブート時に一意のマシン ID が生成されるようになりました。	LP-43131

LogPoint v7.0.0 パッチ

■リリースの詳細

Name: LogPoint
Version: 7.0.0
Type: Major (Patch Release)
Dependency 6.12.2
Release Date: 2022-01-18
Download LogPoint-7.0.0.pak
SHA256: 238d65967c3bcddaa134752bce2be3929c4b07d0b96f9fdd77575d79fd84eec6

■注意事項

- LogPoint v7.0.0 は、以下と互換性があります。
  LogPoint Search Master (LPSM) v2.0.0
  Director Fabric v2.0.0
  Director Console v2.0.0
- LogPoint SOAR はデフォルトでは無効化されています。System Settings >> General から SOAR を有効化することができます。

■新機能

LogPoint SOAR

- LogPoint Security Orchestration, Automation, and Response (SOAR)は、脅威の検出と対応を改善します。LogPoint SOAR は LogPoint SIEM とシームレスに統合され、自動化されたアクティビティに基づく標準的なインシデント対応ワークフローを提供することで、脅威アラートへの対応に必要な応答時間や手動での介入を削減します。
  主要な機能:
  - 複数のソースからセキュリティ脅威のデータおよびアラートを収集。
  - 標準的なワークフローに基づき、標準的なインシデント対応の優先順位付けと実行。
  - サイバー脅威の迅速な調査、封じ込め、除去を、自動化されたインシデントレスポンスによりサポート。
- LogPoint の全ユーザーが SOAR にアクセスできます。そのため、彼らは SIEM インシデントの権限に関係なく、すべてのケースを閲覧できます。
- 詳しくは、オンラインの「Detection, Investigation, and Response」セクションの「Getting Started with SOAR Guide」を参照してください。

ユーザーインターフェイスの更新

- システム全体の使い勝手を向上させました。
- ナビゲーションは左側に移動し、アイコン表示と詳細表示を切り替えられるようにしました。
- ナビゲーションバーから直接、検索テンプレートへアクセスできるようにしました。インシデントもナビゲーションバーの[Investigation]オプションの下に移動しました。
- 検索結果ページとすべてのリストページに[Back](戻る)ボタンを追加しました。
- 右上に[Info](情報)アイコンを追加しました。アイコンをクリックすると、LogPoint のバージョンの詳細が表示されます。

■その他の改善事項

内容	Issue ID
検索テンプレート名をクリックすると、検索テンプレートビューに遷移するようにしました。検索テンプレートを編集するために、[Actions]欄に[Edit]アイコンを追加しました。共有されている検索テンプレートの編集権限またはすべての権限を持つユーザーは、検索テンプレート一覧ページから直接編集できるようになりました。	LP-43805, LP-44829
ユーザー管理機能は、LogPoint Collector モードの一部になりました。Collector モードでもユーザーがパスワードを変更できるようになりました。	LP-17035
アラート通知を設定する際、Jinja のサポートフィールドに{{alertrule_id}}、{{incident_id}} 、 {{logpoint_name}} 、 {{loginspect_ip_dns}} 、{{status}}、{{time_range}}を使用できるようにしました。 また、{{format}}、{{timezone}}、{{type}}、{{user_id}}はすべての通知タイプで使用できるようにしました。以前は、特定の通知タイプでのみ使用できました。	LP-43780
[Create Alert]および[Create Dashboard Widget]ダイアログボックスで、[Query]テキストボックスのサイズを大きくしました。これにより、長いクエリを複数行で確認できるようになったため、クエリの編集やトラブルシューティングが容易になりました。	LP-43616
LogPoint が HTTP 通知の生成に失敗した場合、request_headers、status_code、reason、response_headers、content で構成される詳細な監査ログを表示するようにしました。	LP-43256
MITRE ATT&CK フレームワークに従って、攻撃カテゴリーと攻撃タグをソートするようにしました。新しいソート順は、次のような場合に役立ちます。 ・ テーブルビューおよびカバレッジビューのポップアップダイアログボックスで、attack_id の昇順に従って関連する攻撃タグを検索できます。複数の攻撃カテゴリーで共通の攻撃タグを持つアラートルールについては、攻撃タグの数が接尾辞の一部になりました。 ・ アラート分類ウィジェット、インシデント分類ウィジェット、テーブルビュー、およびカバレッジビューのポップアップダイアログボックスで、MITRE ATT&CK フレームワークの攻撃進行順序に従って、関連する攻撃カテゴリーを識別するようにしました。	LP-43859, LP-43856, LP-43853

■バグ修正

内容	Issue ID
集計機能を持つ rex コマンドや filter コマンドを検索クエリで使用すると、結果が表示されない問題。	LP-43537

すべての権限ではなくオブジェクト権限のみを持つユーザーが、Table キーワードでクエリを検索すると、検索結果が表示されない問題。	LP-42175
LogPoint サービスで例外が発生すると、ダッシュボードが表示されず、アラートがトリガーされない問題。	LP-9589
グルーピングクエリでステップ関数を集約関数といっしょに使用すると、検索とダッシュボードの結果が異なる問題。	LP-43134, LP-44527
SNMP OID を使用して実行中の検索プロセスの数を取得すると、不正な値が返される問題。	LP-43734
UI からカスタムの Syslog TLS 証明書をアップロードすると、LogPoint マシンが他の LogPoint マシンとの接続を確立したり、保持できなくなったりする問題。	LP-44682

■脆弱性の修正

- libnss3 および libnss3-dev には、DER エンコードされた DSA または RSA-PSS 署名を処理する際にヒープオーバーフローの脆弱性が存在しました。

■プラグインの更新

以下のバンドルアプリケーションがアップデートされました。

アプリケーション	アップデートされたバージョン
Alert Rules	5.3.5

以下のバンドルアプリケーションが新規追加されました。

アプリケーション	バージョン
Radius Authentication	6.0.0
OAuth Authentication	6.0.0
SAML Authentication	6.0.0
ADFS Authentication	6.0.0

■削除された機能

- スナップショット機能はなくなりました。

8. LogPoint Version 6.12.2

■リリースの詳細

Name:	LogPoint
Version:	6.12.2
Type:	FlexPatch
Severity:	Optional
Dependency:	6.12.0, 6.12.1
Release Date:	2021-11-15
Download	logpoint_6.12.2.pak
SHA256:	6d1f509bf8bf966356ef0ea6789b45d6291960d6d892fb5a722a55d8e0a9fa05

■注意事項

- LogPoint v6.12.2 は、LogPoint v6.12.0 と LogPoint v6.12.1 にインストールできます。
- LogPoint v6.12.2 をインストールする前に、下記のディスクのディレクトリに空き容量が必要です。

  /opt 5GB

  / 500MB
- LogPoint v6.12.2 は、以下と互換性があります。

  LogPoint Search Master (LPSM) v1.8.0

  Director Fabric v1.8.0

  Director Console v1.10.0 / v1.10.1
- 複数の内部パッケージ、サービス、ファイルパスは、LogPoint v6.12.2 内のアプリケーション環境を標準化するためにアップデートされました。

■改善内容

- ATT&CK v10 アップグレード
  - MITRE ATT&CK フレームワークの Attack Tactics、Attack Techniques、Attack Sub-techniques に関連した Attack Categories と Attack Tags が、ATT&CK v10 にアップグレードされました。
  - ATT&CK v10 に容易にアップグレードできるように Mitre Dataset Updater v6.0.0 plugin を LogPoint v6.12.2 にバンドルしています。
  - Attack technique Launchd (T1053.004)は、廃止予定になり、attack techniques Man-in-the-Middle (T1557)と Man-in-the-browser (T1185)は、Adversary-in-the-Middle と Browser Session Hijacking (T1185) にそれぞれ名称が変更されました。
  - これらのアタックタグで設定した以前のアラートルールは、アップグレード後はこれらのアタックタグを持たなくなるため、新しいタグでアラートルールを再設定する必要があります。

    詳細は以下を参照してください。

https://attack.mitre.org/resources/updates/updates-october-2021/

■修正内容

以下の不具合を修正しました。

修正内容	ID
ベンダーサーチテンプレートを閲覧中に表示を切換えられない問題。	LP-44205
同じベンダーレポートテンプレートを複数回使用できる問題で、My Report Template に冗長なレポートテンプレートがリストされることがありました。 Add アイコンは一度使用すると、ベンターレポートテンプレートから削除されるようになりました。	LP-44176
カスタマイズしたレポートのヘッダーやパラグラフ内の何種類かの Unicode 文字が表示されない問題。ユーザーは日本語、中国語、韓国語の Unicode 文字用にフォントを選択することができるようになりました。	LP-44211
LogPoint v6.9.0 以前にエクスポートしたアラートルールをインポートしてクローンを作成すると、そのアラートはインシデントを生成しない問題。	LP-44111

■脆弱性の修正

以下の Ubuntu 関連のセキュリティの脆弱性に対応しました。

1. BIND の脆弱性:バッファーのオーバーリードを発生させ、サーバーをクラッシュまたはリモートコードを実行させる問題。
2. libcaca のバッファーオーバーフロー問題:メモリ破壊やその他の潜在的な問題を発生させる。
3. gnutls の use-after-free 問題:メモリ破壊やそれが引き起こす問題。
4. lz4 の脆弱性:攻撃者が整数のオーバーフローをトリガーに、範囲外の書込みやクラッシュを引き起こす問題
5. API の EVP_PKEY_decrypt()関数:バッファーオーバーフローを引き起こす問題。
6. v1.9.5 以前の Unbound の脆弱性:範囲外の書込みと圧縮された名称を介して整数のオーバーフローを引き起こす問題。
7. ヒープベースのバッファーオーバーフロー、use-after-free の脆弱性、v1.0.1 以前の libwebp 内の ReadSymbol 関数で使用されている単一化された変数で、データの機密性、整合性、システムの可用性が侵害される問題。
8. X.Org X の LookupCol.c により、リモートの攻撃者が任意のコードを実行できる脆弱性。
9. GNU Screen の脆弱性で、攻撃者が巧妙に細工した UTF-8 の文字シーケンスを介して DoS 攻撃や別の影響を与える問題。

10. libwebp での範囲外の読み取りにより、データの機密性が侵害され、サービスが利用できなくなる問題。

■プラグインの更新

以下のバンドルアプリケーションがアップデートされました。

アプリケーション	アップデートされたバージョン
Recorded Future	6.0.0
StixTaxii	6.0.0
Threat Intelligence	6.0.0
Vulnerability Management	6.0.0
Mitre Dataset Updater	6.0.0

9. LogPoint Version 6.12.1（JTC リリース見送り）

■修正内容

以下の不具合を修正しました。

修正内容	ID
Alert HTTP notifications が、incident_id と logpoint_name Jinjya プレースホルダー変数をサポートしていない問題。	LP-44075
Jinjya テンプレートで extra_info.query を使用した場合、アラートルールの通知を設定している際に検証エラーが発生する問題。	LP-44060
distinct_list 以外のアグリゲータでパラメータとして_ts で終わるフィールドを使用すると検索でエラーになる問題。	LP-44084
120 秒のアイドルタイムアウト後の TLS 接続のシャットダウンで、Syslog collector でログが収集されない問題。	LP-42793

10. LogPoint Version 6.12.0

LogPoint v6.12.0 OVA

■リリースの詳細

Name:	LogPoint OVA
Version:	6.12.0
Type:	OVA
Release Date:	2021-10-06
Download	LogPoint-6.12.0.ova
SHA256:	5b41802f3de558f6c3a1d790adcf4f4f0cea8aaf3b78e6130a5e44d34e2c508c

■注意事項

- LogPoint v6.12.0 OVA は、VMWare ESXi server v6.0 以降にインストールできます。
- LogPoint v6.12.0 OVA は、ext4 ファイルシステムをベースにしています。

LogPoint v6.12.0 Hyper-V VHD

■リリースの詳細

Name:	LogPoint Hyper-V VHD
Version:	6.12.0
Type:	VHD
Release Date:	2021-10-06
Download	LogPoint-6.12.0.vhd
SHA256:	05d188ef43233df457ff0adbfb5f1f1a8456f284833f8f1de205c0049c3715c1

■注意事項

- LogPoint v6.12.0 Hyper-V VHD は、Microsoft Hyper-V Server 2016 以降でサポートされています。
- LogPoint v6.12.0 Hyper-V VHD は、ext4 ファイルシステムをベースにしています。
- 1 つの VHD から LogPoint インスタンスを作成できます。複数のインスタンスを作成する場合、オリジナルの VHD から必要な数のコピーを作成し、その各コピーからそれぞれの LogPoint のインスタンスを作成します。
- LogPoint は全ての変更をその VHD に書き込むので、ダウンロードした VHD はオリジナルの状態で保存し、LogPoint のインスタンスの作成にはコピーを使用するようにしてください。
- LogPoint Hyper-V VHD ファイルは、動的に拡張する VHD ファイルです（ディスクはオンデマンドで割り当てられます）。固定サイズの VHD ファイルは、VHD ファイル作成時にすぐ割り当てられます。固定サイズの VHD ファイルにするには、Hyper-V マネージャアプリケーションの Edit Disk Utility を使用して変換することができます。

LogPoint v6.12.0 Azure VHD

■リリースの詳細

Name: LogPoint Azure VHD
Version: 6.12.0
Type: VHD
Release Date: 2021-10-06

■注意事項

- LogPoint v6.12.0 Azure VHD を入手する場合、弊社まで連絡をください。
- LogPoint v6.12.0 Azure VHD は、ext4 ファイルシステムをベースにしています。

LogPoint v6.12.0 AMI

■リリースの詳細

Name: LogPoint
Version: 6.12.0
Type: AMI
Release Date: 2021-10-06
AMI ID: ami-05a2e6c45efc5954e

■注意事項

- LogPoint v6.12.0 AMI を入手する場合、弊社まで連絡をください。その際に AWS Account Number と Deployment Region の情報の提供をお願いいたします。
- LogPoint v6.12.0 AMIは、ext4 ファイルシステムをベースにしています。

■改善内容

改善内容	ID
cloud-init package が LogPoint AMI に追加されました。これにより、インスタンスを起動する時にコマンドを実行することができます。	LP-42731

以上

日本語マニュアル発行日 2022 年 10 月 22 日

本マニュアル原文:

『LogPoint Release Notes』

ジュピターテクノロジー株式会社 技術グループ