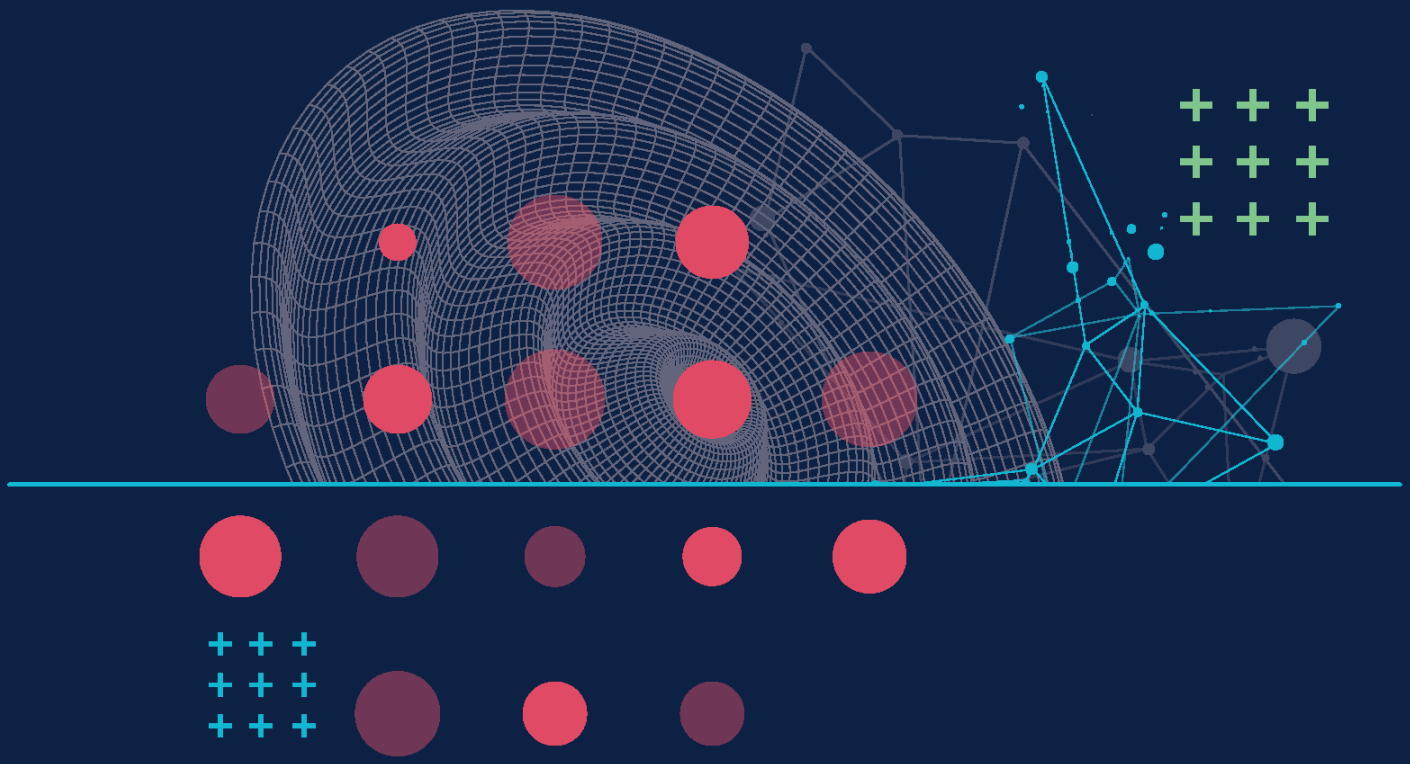

イベントログと脅威検知のベストプラクティス

Australian Government
Australian Signals Directorate

National Cyber Security Centre
a part of GCHQ

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre
PART OF THE GCSB

内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

目　次

要　約

本書は、サイバー脅威を軽減するために、イベントログのベストプラクティスのベースラインを定義する。これは、豪州通信情報局豪州サイバーセキュリティセンター（ASD's ACSC）が、以下の国際的パートナーと協力して作成したものである。

- 米国土安全保障省サイバーセキュリティ・インフラ庁（CISA）、米国連邦捜査局（FBI）、米国国家安全保障局（NSA）
- 英国国家サイバーセキュリティセンター（NCSC-UK）
- カナダサイバーセキュリティセンター（CCCS）
- ニュージーランド国家サイバーセキュリティセンター（NCSC-NZ）及び CERT-NZ
- 内閣サイバーセキュリティセンター（NISC）及び JPCERT/CC
- 韓国国家情報院（NIS）及び NIS のサイバーセキュリティセンター（NCSC-Korea）
- シンガポールサイバーセキュリティ庁（CSA）
- オランダ総合情報保安局 （AIVD） 及び軍情報保安局（MIVD）.

イベントログは、ネットワークを可視化することで、重要なシステムの運用の継続的な提供を支援し、セキュリティと強じん性を向上させる。本ガイダンスは、リソースの制約を考慮しつつ、現在のサイバー脅威環境における組織の回復力を向上させるための提言を行うものである。このガイダンスは、中程度の技術的複雑さの内容となっており、イベントログの基礎を理解していることを前提としている。

効果的なイベントログソリューションは、以下を目的とするものである：

- 重要なソフトウェア構成の変更や新しいソフトウェアソリューションの導入などのサイバーセキュリティイベントが発生した場合に、監視を担当するネットワークセキュリティ担当者にアラートを送信すること
- 悪意のあるアクターによるシステム内寄生（LOTL）)技術の利用や、侵害後の横方向の移動など、サイバーセキュリティインシデントを示す可能性のあるサイバーセキュリティイベントを特定すること
- セキュリティ侵害の範囲と程度を明らかにすることで、インシデントへの対応を支援すること
- アカウントが組織のポリシーに準拠しているかを監視すること
- アラートノイズを減らし、ストレージとクエリー時間に関するコストを削減すること
- ネットワークセキュリティ担当者が、アラートと分析の優先順位付けに基づき、迅速かつ十分な情報に基づく意思決定ができるようにすること
- ログ及びログを記録するプラットフォームが、分析者にとって使用可能であり、パフォーマンスが高いことを確認すること

ログのベストプラクティスでは、以下の 4 つのファクターを検討することが重要である：

1. 企業承認のイベントログポリシー
2. イベントログの収集と相関の一元化
3. 安全なストレージとイベントログの完全性

4. 関連する脅威に対する検知戦略

はじめに

LOTL バイナリ（LOLBins）やファイルレス・マルウェアのような、システム内寄生（Living Off The Land）戦術を使用した悪意のあるアクターの増加によって、効果的なイベントログソリューションを実装し維持することの重要性が強調されるようになっている。共同署名文書である「Identifying and Mitigating Living Off the Land Techniques」（システム内寄生戦術の特定と緩和）で示されているように、APTs （高度かつ持続する脅威）は、システム内寄生戦術を利用して検知を回避している。本書の目的は、クラウド、企業ネットワーク、エンタープライズモビリティ及び OT（オペレーショナル・テクノロジー）ネットワークのイベントログと脅威検知のためのベストプラクティスを詳述することである。本文書のガイダンスは、イベントログと脅威検知の一般的なベストプラクティスに焦点を当てている。しかしながら、LOTL の技術は、それらを検知することが非常に困難であるため、優れたケーススタディーを提供するという特徴がある。

対象

本ガイダンスは、性質上、技術的なものであり、中規模から大規模の組織における者を意図しており、主に以下の層を対象としている。

- IT 及び OT に関する経営層の意思決定者
- IT 及び OT オペレータ
- ネットワーク管理者
- 重要インフラ事業者

ベストプラクティス

企業承認のイベントログポリシー

組織は、企業承認のログポリシーを作成し、実装することで、システム上での悪意ある行為を検知し易くなり、また、組織環境全体で一貫したログの方法をとることができる。ログポリシーは、サービスプロバイダと組織との間の責任分担を考慮すべきである。本ポリシーには、ログに含めるイベントの詳細、使用するイベントログ機能、イベントログの監視方法、ログの保存期間及び収集する価値のあるイベントログを再評価するタイミングを含むものでなければならない。

イベントログの品質

組織は、ネットワークセキュリティ担当者がサイバーセキュリティインシデントを正しく特定する際に役立つ、質の高いサイバーセキュリティイベントをキャプチャすることに焦点を当てたイベントログポリシーを実装することが推奨される。サイバーセキュリティインシデント対応と脅威検知における、イベントログの品質とは、ログの体

裁の良し悪しではなく、収集されるイベントの種類のことをいう。ログの品質は、ネットワーク環境の違い、ログを必要とする理由、重要な資産の違い、組織のリスク選好度などによって変わりうる。

有用なイベントログは、ネットワークセキュリティ担当者が、セキュリティイベントが偽陽性であるか真陽性であるかを識別するためのセキュリティイベント評価能力を強化する。質の高いログを実装することにより、ネットワークセキュリティ担当者は、正常に見えるように設計されたシステム内寄生戦術を見つけやすくなる。

注意）適切にフォーマットされた大量のログをキャプチャすることは、フォレンジック分析シナリオにおいて、インシデント対応者にとって非常に貴重である。しかし、組織は、ログに記録されたデータを容易に利用でき、検索可能な「ホット」データストレージ又は可用性を優先せずより経済的なソリューションを通じて保存される「コールド」データストレージに適切に整理することが推奨される。これは、組織のログのストレージ容量を評価する際の重要な考慮事項である。

質の高いイベントログ収集の優先順位付けにおけるさらなる情報は、CISA が発行した「Guidance for Implementing M-21-3: Improving the Federal Government's Investigative and Remediation Capabilities」を参照のこと [1]。

システム内寄生戦術を用いた悪意のあるアクターの検知を強化するには、イベントログに関する考慮事項に以下が含まれる：

- Linux ベースのシステムの場合、悪意のあるアクターが使用する curl、systemctl、systemd、python 及びその他の一般的な LOLBins の使用をキャプチャするログ
- Microsoft Windows ベースのシステムの場合、悪意のあるアクターが使用する、wmic.exe、ntdsutil.exe、Netsh、cmd.exe、PowerShell、mshta.exe、rundll32.exe、resrv32.exe その他の一般的な LOLBins の使用をキャプチャするログ。ログには、コマンド実行、PowerShell のスクリプトブロックログ及びモジュールログ並びに管理タスクの詳細な追跡がキャプチャされていることを確認する。
- クラウド環境の場合、API コールやエンドユーザーのログインなど、コントロールプレーン操作でのすべてのログを記録する。コントロールプレーンのログは、読み書きの動作、管理上の変更及び認証イベントをキャプチャするように設定されるべきである

キャプチャしたイベントログの詳細

組織のイベントログポリシーの一部として、キャプチャされたイベントログには、ネットワークセキュリティ担当者とインシデント対応者の助けとなる十分な詳細が含まれていなければならない。ログソリューションが、セキュリティに関連するデータをキャプチャできない場合、サイバーセキュリティインシデント検知機能としての有効性に多大な影響を与える。

「*US Office of Management and Budget's M-21-31*」[2] には、該当する場合、イベントログがキャプチャすべき項目の適切なベースラインが概説されている：

- 適切な形式の正確なタイムスタンプ（ミリ秒単位の精度が理想）
- イベントの種類（ステータスコード）
- デバイス識別子（MAC アドレス又はその他の一意の識別子）
- セッション/トランザクション ID
- 自律システム番号

[1] 本ガイダンスは米国連邦民間行政機関を対象とするものであるが、ログのベストプラクティスに関し、すべての団体にとって有用なガイダンスを提供しうる

[2] この覚書は、国家安全保障システムを除く米国連邦情報システムのみを拘束するものであるが、ログのベストプラクティスに関し、すべての団体に有用なガイダンスを提供しうる

- 送信元および宛先 IP（IPv4 及び IPv6）
- ステータスコード
- 応答時間
- 追加ヘッダー（例：HTTP ヘッダー）
- User ID（該当する場合）
- 実行されたコマンド（該当する場合）
- イベントの相関のために、一意なイベント識別子（可能な場合）

注：可能な場合は、すべてのデータを容易に抽出できるようにキーと値のペアの形式とする

オペレーショナル・テクノロジーに関する考慮事項

ネットワーク管理者及びネットワーク運用者は、それぞれの OT ネットワーク内にある OT デバイスを考慮すべきである。ほとんどの OT デバイスは、メモリー及び/又はプロセッサに制約のある組み込みソフトウェアを使用している。ログが過剰な水準になると、それらの OT デバイスの動作に悪影響を及ぼす可能性がある。さらに、そのような OT デバイスは、詳細なログを生成することができない場合があるが、その場合、センサを使用して、ログ機能を補完することができる。帯域外のログ通信、又はエラーコードと既存の通信のペイロードに基づいてログを生成することで、ログの容量に制限のある組み込みデバイスにも考慮することができる。

追加資料

ログに含める詳細事項の例は、以下の資料で見ることができる：

- 豪州通信情報局サイバーセキュリティセンター（ASD's ACSC）の「Information Security Manual (ISM)」には、「Guidelines for System Monitoring」において記録するべきイベントログの詳細が記載されている
- CISA の「*Guidance for Implementing M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities*」には、米国連邦政府組織を対象とした、ログ収集の優先順位付けの別のアプローチが詳述されており、米国連邦の文民行政組織を対象としている
- NIST は、「Guide to Operational Technology (OT) Security」において、イベントログにおける OT に関する考慮事項を概説している
- 検知の使用例については、MITRE ATT&CK®のデータソースのリストを参照することを検討のこと

内容及びフォーマットの一貫性

イベントログを一元化する場合、組織は、JSON 等、構造化されたログ形式の使用を検討すべきである。この形式では、各タイプのログが内容を一貫して（すなわち、スキーム、フォーマット及び順序が一貫していること）キャプチャし表示する。これは、イベントログが中央保管装置に転送される場合に特に重要である。これにより、ネットワークセキュリティ担当者がイベントログを検索し、フィルタリングを行い、関連づけする能力が向上するためである。ログの構造が異なる（又は構造化されていない）可能性があるため、自動でログが規格化される手法を実装することが推奨される。このことは、時間の経過とともに、又は予告なしに変更される可能性がある、例えばソフトウェアや Software-as-a-Service (SaaS) などのログの場合に、重要な検討事項となる。

タイムスタンプの一貫性

組織は、ネットワークセキュリティ担当者がイベントログの間の関係を特定するのを支援するため、正確で信頼できるタイムソースを確立することを検討し、これをすべてのシステムにわたって一貫して使用すべきである。これには、すべてのシステムで同じ日時形式を使用することを含めるべきである。組織は、可能な場合は、主要なタイムソースが劣化、又は使用できない場合に備え、複数の正確なタイムソースを使用するべきである。特に分散システムでは、タイムゾーンと距離は、タイムスタンプが、それぞれのタイムスタンプとの関係においてどのように読

み込まれるかに影響を与えうることに留意すること。ネットワーク所有者、システム所有者及びサイバーセキュリティインシデントの対応者は、これが自身の環境においてどのような影響を及ぼすかを理解しておくよう、推奨される。豪州通信情報局サイバーセキュリティセンター（ASD's ACSC）及び共同執筆者は、組織に対し、一貫したタイムスタンプの収集を確実にするために、以下の推奨事項の実施を検討することを強く求める。

- タイムサーバは、すべての環境で同期化されるとともに検証され、デバイスの起動や再起動などの重要なイベントをキャプチャするように設定すべきである
- UTC を使用することは、タイムゾーンがないだけでなく、夏時間もないという利点があり、推奨される時間基準である
    - ISO 8601 形式を導入し、年を最初に記載し、月、日、時、分、秒、ミリ秒の順に記載する（例：2024-07-25T20:54:59.649Z）
- 時間共有は単一方向とすべきである。OT 環境は、時間を IT 環境と同期させるべきであるが、その逆の同期をすべきではない
- 一部の OT 環境にある資産では、データヒストリアンを実装して、コンピュータシステム上で実行される生産プロセスの時系列データを記録及び保存している場合がある。これらから、OT ネットワークのイベントログデータの追加ソースを得ることができる

追加資料

- 豪州通信情報局サイバーセキュリティセンター（ASD's ACSC）は、重要なイベントカテゴリ、設定、ログの保存期間、及びイベントの転送に関する推奨事項の詳細を記載した「Windows Event Logging and Forwarding」のガイダンスを発行している。
- ログに関する詳細については、CISA のウェブサイトまたは GitHub ページにて中小規模組織向けに公開されている基本的なログ管理機能を提供する無償ソリューション「Logging Made Easy（LME）」を参照のこと。
- AIVD と MIVD の合同技術ユニットである Joint SIGINT Cyber Unit（JSCU）は、フォレンジックの価値と保存の最適化との間の均衡を見いだすことに焦点を当てた Microsoft Windows のイベントログ記録と収集のベースラインを GitHub で公開しており、確認可能である。

イベントログの保存

組織は、サイバーインシデントの調査に使用するのに十分な期間、ログを保存すべきである。デフォルト設定のログ保存期間は、しばしば不十分である。ログの保存期間は、所定のシステムに対するリスク評価と、組織に適用される可能性のある規制要件によって決定されるべきである。ログの保存期間を決定する際には、サイバーインシデントを発見するまでに最大 18 ヶ月を要する場合があること、また、マルウェアによってはネットワーク上に 70～200 日間潜伏してからサイバーインシデントを引き起こすものもあることを考慮しなければならない[3]。ログの保存期間は、組織の管轄内で適用される可能性のある規制要件及びサイバーセキュリティの枠組みにも準拠すべきである。侵入とその影響を確認する上で極めて重要なログについては、長期間保存することを優先すべきである。

保存期間の確認と並行して、ログのストレージ割当ても見直すことが重要である。ストレージ不足がログ保存の障害になることは珍しくない。例えば、多くのシステムではストレージの割り当てがなくなると、古いログを上書きしてしまう。ログを長く保存できるほど、改善が求められる潜在的な侵入ベクトルなど、サイバーセキュリティインシデントの程度を判断できる見込みが高くなる。効果的なセキュリティログの実施には、組織は、ホットストレージ及びコールドストレージのようなデータの階層化を行うべきである。これにより、ログを迅速に取得し、クエリーや脅威検知を容易に行うことができる。

[3] CISA 発行の "First 48": What to Expect When a Cyber Incident Occurs

ログの収集と相関の一元化

以下のセクションでは、企業ネットワーク、OT、クラウドコンピューティング及びモバイルコンピューティングデバイスを使用したエンタープライズモビリティについて、優先順位を付けたログソースのリストを詳述する。優先順位付けでは、その資産が侵害された場合の影響だけでなく、ログが記録された資産が悪意のあるアクターの標的になるリスクを考慮に入れる。また、システム内寄生戦術の特定に資するログソースにも優先順位付けを行う。このリストは、ログソースとその脅威を網羅したリストではなく、優先順位は組織によって異なる可能性があることに留意すること。

企業ネットワークのログの優先順位

企業ネットワークは、さまざまなサイバー脅威に直面する。これには、マルウェア、悪意のある組織内部者及びパッチが適用されていないアプリケーション及びサービスの悪用が含まれる。システム内寄生戦術に関しては、企業ネットワークは悪意のあるアクターに対し、攻撃するためのネイティブツールを提供してしまっている。

豪州通信情報局サイバーセキュリティセンター（ASD's ACSC）及び共同執筆者は、組織に対し、企業ネットワーク内の以下のログソースを優先することを推奨する：

1. 標的となる可能性の高い重要なシステム及び保持データ
2. リモートアクセス、ネットワークメタデータ、及びその基盤となるサーバー用オペレーティングシステムを含むインターネットに接続可能なサービス
3. ID 及びドメインの管理サーバー
4. その他の重要なサーバー
5. バウンダリルーター、ファイアウォールなどのエッジデバイス
6. 管理用ワークステーション
7. 構成管理、性能及び可用性の監視(特権アクセスが使用される場合)、継続的インテグレーション/継続的デリバリ(CI/CD)、脆弱性スキャンサービス、シークレット及び特権管理などの高い権限を与えられたシステム
8. データレポジトリ
9. セキュリティ関連及び重要なソフトウェア
10. ユーザーのパソコン
11. ユーザーアプリケーションログ
12. 組織のユーザー及びサービスアカウントが使用するウェブプロキシ
13. 組織のユーザーが使用する DNS サーバー
14. 電子メールサーバー
15. DHCP サーバー
16. レガシーIT 資産 (重要なサービス又はインターネット対応のサービスで以前に取得されていないもの)

豪州通信情報局サイバーセキュリティセンター（ASD's ACSC）及び共同執筆者は、組織が優先順位の低いログを監視することも推奨している。これには以下が含まれる：

- ハイパーバイザーホストなどの基盤となるインフラ
- プリンターなどの IT デバイス
- アプリケーションゲートウェイなどのネットワークコンポーネント

オペレーショナル・テクノロジー（OT）におけるログの優先順位

歴史的に、IT と OT は、組織内で別々に運用され、異なる機能を提供してきた。テクノロジーの進化とデジタル化の進歩により、これらのネットワークの相互接続と融合が進んでいる。組織は、IT と OT のネットワークを統合し、管理システムと生産工程の間のシームレスなデータの流れを実現しようとしている。これらが統合されたことで、OT ネットワークに新たなサイバー脅威がもたらされている。例えば、悪意のあるアクターは、パッチが適用されていない脆弱性の悪用、マルウェアの配信、重要なサービスに影響を与えるサービス拒否攻撃活動など、IT ネットワークを介して OT ネットワークにアクセスし得る。

豪州通信情報局サイバーセキュリティセンター（ASD's ACSC）及び共同執筆者は、組織に対し、OT 環境において、以下のログソースを優先することを推奨する：

1. エアギャップシステム以外の、安全性とサービスの提供に不可欠な OT デバイス [4]
2. インターネットに接続可能な OT デバイス
3. ネットワーク境界を介してアクセス可能な OT デバイス

OT デバイスがログ記録をサポートしていない、デバイスのログが利用できない又はデバイスのログが非標準フォーマットにおいて利用できるといった場合、OT デバイスを行き来するネットワークトラフィック及び通信がログに記録されていることを確保することを推奨する。

モバイルコンピューティングデバイスを使用したエンタープライズモビリティのログの優先順位

エンタープライズモビリティは、組織のセキュリティ体制において重要な要素である。モバイルデバイス管理（MDM）ソリューションは、組織によるエンタープライズモビリティのセキュリティ管理を可能にするもので、通常はログ機能を含む。エンタープライズモビリティにおいて、効果的なイベントログの目的は、例えば、フィッシング又は悪意のあるアプリケーションやウェブサイトとの通信などにより侵害されたアカウントやデバイスを検知することである。

豪州通信情報局サイバーセキュリティセンター（ASD's ACSC）及び共同執筆者は、組織に対し、エンタープライズモビリティソリューションについて、次のログソースを優先することを推奨する：

1. 組織ユーザーが使用するウェブプロシキ
2. 組織が運用する DNS サービス
3. 組織的に管理されたデバイスのセキュリティ状態
4. 組織的に管理されたデバイスの挙動
5. サインインなどのユーザーアカウントの挙動
6. VPN ソリューション
7. MDM 及び MAM（モバイルアプリケーション管理）イベント [5]

電気通信ネットワークプロバイダと協力して追加の監視が実施されるべきである。係る監視には以下が含まれる：

- シグナリングの悪用
- バイナリ/インビジブル SMS

[4] 優先順位付けされたリストは、遠隔操作を行う悪意あるアクターを検出できるログに焦点を当てている。かかる文脈においては、悪意ある内部者が懸念されない限り、エアギャップシステムのログ収集に高い優先付けを行っていない

[5] MDM 及び MAM イベントは、サーバー側のイベントであることが多いが、モバイルデバイスに入っているソフトウェアによって生じる可能性もある

- CLI スプーフィング
- SIM スワッピングなどの SIM/eSIM に対する行為
- Null 暗号のダウングレード
- 接続のダウングレード(偽ベースステーション)
- ユーザーに対するネットワーク API/クエリー
- ローミングトラフィックの保護
- ローミングステアリング

組織は、MDM ソリューションに登録されている個人所有のモバイルデバイスからログに記録できる項目について、法的な助言を得るべきである。例えば、GPS の位置情報を記録することは規制の対象となる可能性がある。

クラウドコンピューティングのログの優先順位

豪州通信情報局サイバーセキュリティセンター（ASD's ACSC）と共同執筆者は、Infrastructure-as-a-Service (IaaS) 、Platform-as-a-Service (PaaS)または Software-as-a-Service (SaaS)のいずれが実装されているかにかかわらず、管理されているクラウドサービスに従ってイベントログの手法を調整することを推奨する。例えば、IaaS はテナントに対してかなりの量のログ記録の責任を課すのに対して、SaaS はプロバイダに対してかなりの量のログ記録の責任を課す。従って、責任共有モデルはログの優先順位に影響を及ぼすことから、組織は、責任共有モデルを理解するため、クラウドサービスプロバイダと緊密に連携すべきである。ログの優先順位は、異なるクラウドコンピューティングサービスモデルや展開モデル（パブリック、プライベート、ハイブリッド、コミュニティなど）によっても影響を受ける。プライバシーやデータ主権に関する法律が適用される場合、ログの優先順位は、クラウドサービスプロバイダのインフラの場所によっても影響を受ける可能性がある。詳細については、NSA の「Manage Cloud Logs for Effective Threat Hunting」ガイダンスを参照のこと。

組織は、クラウドコンピューティングサービスを使用するに際し、次のログソースを優先するべきである：

1. 標的となりそうな重要なシステム及び保持データ
2. インターネットに接続可能なサービス（リモートアクセスを含む）、及び該当する場合には、それらの基盤となるサーバーオペレーティングシステム
3. クラウドサービスにアクセスし管理する、テナントのユーザーアカウントの使用
4. 管理者による設定変更のログ
5. すべてのセキュリティプリンシパルの作成、削除及び変更のログ（許可の設定と変更を含む）
6. サードパーティのサービス（SAML/OAuth など）に対する認証の成功乃至失敗
7. クラウド API、すべてのネットワーク関連イベント、コンプライアンスイベント、及び課金イベントのログを含むクラウドサービスにより生成されるログ

安全なストレージとイベントログの完全性

豪州通信情報局サイバーセキュリティセンター（ASD's ACSC）及び共同執筆者は、組織に対し、セキュリティで保護されたデータレイクなどの一元化されたイベントログ機能を実装して、ログの集約を可能にし、選択された処理済みのログを、セキュリティ情報・イベント管理（SIEM）ソリューションや拡張検知・対応（XDR）ソリューションなどの分析ツールに転送することを推奨する。市販されている多くのネットワークインフラデバイスでは、ローカルストレージの容量に限りがある。一元化された安全なストレージにイベントログを転送することにより、デバイスのローカルストレージを使い切った場合でもログを失わずに済む。[CPG 2.U] また、ローカルデバイス上で

イベントログの最大ストレージサイズのデフォルト値を適切に構成しておけば、更なる対策となる。サイバーセキュリティインシデントの際には、過去のイベントログの欠如は、頻繁にサイバーセキュリティインシデント対応に悪影響を及ぼしている。

イベントログの安全な輸送とストレージ

豪州通信情報局サイバーセキュリティセンター（ASD's ACSC）及び共同執筆者は、組織に対し、通信中及び保存中のイベントログの完全性を確保するために、TLS（トランスポートレイヤーセキュリティ）1.3 や暗号検証のような安全性メカニズムを実装することを推奨する。組織は、　機密データの記録が要件付けられているイベントログへの保護とアクセス制限を優先するべきである。

不正なアクセス、変更、及び削除からのイベントログの保護

一部の悪意あるアクターは、検知を回避し、またサイバーセキュリティインシデント対応の有効性を遅延又は低下させるために、ローカルシステムのイベントログを改ざん又は削除することが知られているため、イベントログを集約しておくことが重要である。ログには悪意のあるアクターにとって有用な機密データが含まれている可能性がある。その結果、ユーザーがそれぞれ業務で必要とするイベントログにのみアクセスできるようにしておく必要がある。

イベントログ機能は、不正な修正や削除からログを保護できるものでなければならない。正当な要件を備えた者だけが、イベントログの削除や修正、一元化されたログ環境にアクセスするための監査ログの閲覧の権限を有することを確実にしてほしい。ログのストレージは、ネットワークやシステム侵害の際にログが改ざんされるリスクを低減するために、追加のセキュリティ制御を備えた個別のまたはセグメント化されたネットワークに配置されるべきである。また、イベントログは、バックアップもなされなくてはならず、データの冗長性の実行も実装されなければならない。

組織は、一般的な IT 環境から SIEM ソリューションをセグメント化し強化することが推奨される。SIEM は、情報量が豊富で、分析機能が提供されており、組織の検知機能における単一の障害点となり得るため、SIEM は悪意のあるアクターにとって魅力的なターゲットになる。組織は、追加コストや容量の問題を最小限に抑え、最も価値のあるログを受信することを確実にするために、SIEM や XDR にイベントログを送信する前にフィルタリングすることを検討するべきである。

一元化されたイベントログが実現する脅威検知

SIEM のログ取得元となる一元化されたログ機能へのイベントログ集約により、以下を特定することができる：

- ベースラインからの逸脱
    - ベースラインには、インストールされたツールやソフトウェア、ユーザーアカウントの挙動、ネットワークトラフィック、システム間通信、その他該当する項目（該当する場合）を含めるべきである。特権のユーザーアカウントや、ドメインコントローラーなどの重要な資産には特に注意しなければならない
    - ベースラインは、いくつかのユーザーアカウントの正常な挙動の分析を実行し、それらの同一アカウントについて「常に異常」な条件を確立することによって得られる
- サイバーセキュリティイベント
    - 本書の目的上、サイバーセキュリティイベントとは、セキュリティポリシー違反、セーフガードの不成功またはセキュリティとの関連が疑われる未知の状況が生じた可能性を示唆するシステム、サービス又はネットワークの状態をいう
- サイバーセキュリティインシデント

- 本書の目的上、サイバーセキュリティインシデントとは、望ましくないあるいは予期しないサイバーセキュリティイベント、または、そのような事象が連続して発生し、業務運営に支障をきたしたか、又は業務運営に支障をきたす可能性が著しく大きいものをいう

タイムリーな取り込み

イベントログをタイムリーに取り込むことは、サイバーセキュリティイベント及びサイバーセキュリティインシデントを早期に検知する上で重要である。イベントログの生成、収集及び取り込みが遅くなると、組織によるサイバーセキュリティインシデントの特定も遅れることになる。

関連する脅威に対する検知戦略

システム内寄生戦術の検知

豪州通信情報局サイバーセキュリティセンター（ASD's ACSC）及び共同執筆者は、組織に対し、ユーザー及びエンティティの挙動分析機能の実装を検討し、ネットワーク、デバイス又はアカウントの挙動異常を自動的に検知できるようにすることを推奨する。SIEM は、通常時のトラフィックと行為のベースラインと、イベントログとを比較することで、異常な行為を検知することができる。システム内寄生戦術を利用した悪意のアクターの検知においては、挙動分析が重要な鍵となる。以下は、Windows ベースのシステムに侵入するために、脅威アクターがどのようにしてシステム内寄生戦術を活用したかを示すケーススタディーである。

ケーススタディー- Volt Typhoon

2021 年半ば以来、Volt Typhoon は、ほぼ専ら LOTL の技術のみに依存することによって、重要なインフラ組織を標的にしてきた。彼らの攻撃活動は、「KV Botnet」マルウェアに感染した個人所有の SOHO ルータによって可能になった。

Volt Typhoon は、コマンドとスクリプトインタープリタである PowerShell を使用して、次のことを行う：

- リモートシステムの検出[T1059.001、T1018]
- 以下のコマンドを使用して、関連付けられたユーザー及びアカウント名を識別 `Get-EventLog security –instanceid 4624` [T1033]
- wevtutil.exe 及び以下のコマンドを使用して、ログを列挙し、成功したログオンを検索 `Get-EventLog Security` [T1654].

Volt Typhoon は、Active Directory データベース・ファイル NTDS.dit[6]を抽出することによって、有効な認証情報を継続的に取得する。

そのために、Volt Typhoon は、次の事項を行うことが観測されている：

- Windows ネイティブの vssadmin コマンドを実行して、ボリューム・シャドウ・コピーを作成[T1006]
- Windows Management Instrumentation コンソール(WMIC)コマンド[T1047]を使用して ntdsutil.exe を実行し、ボリューム・シャドウ・コピーから NTDS.dit 及び SYSTEM レジストリをコピー
- ドメイン管理者権限を持つ侵害されたユーザーアカウントを使用して、対話型 RDP セッションを介して Microsoft Active Directory Domain Service (AD DS)ドメインコントローラーに横方向に移動[T1021.001]

Volt Typhoon が使用することが観測されているその他の LOTL 技術には、次のものが含まれる：

- Local Security Authority Sub System Service(LSASS)プロセスのメモリー領域からハッシュ化された資格情報にアクセス [T1003.001]
- ntdsutil.exe を使用して、リモート又はローカルの Microsoft AD DS ドメインコントローラーから、ユーザー名とパスワードのハッシュを含むインストールメディアを作成する[T1003.003]
- PowerShell、WMIC 及び ping コマンドを使用して、システムの検出を容易にする[T1018]
- 組み込みの netsh portproxy コマンドを使用して、侵害されたシステムにプロキシを作成し、アクセスを容易にする[T1090]

Volt Typhoon は、システム内寄生戦術を使用して検知をより難しくするが、マルウェアが示す挙動は、通常業務の行為と比較して異常であると判断されるため、その挙動は検知のユースケースの作成に利用することが可能である。

詳細については、MITRE ATT&CK®の Volt Typhoon のページ及び MITRE ATT&CK framework を参照のこと

異常な挙動として次のような例が挙げられる：

- 通常とは異なる時間（勤務時間外、休日又は休暇中など）にログインしたユーザーがいた
- 例えば管理者や人事サービスなど、通常はアクセスしないサービスに、アクセスしたアカウントがあった
- 通常と異なるデバイスでログインしたユーザーがいた

[6] NTDS.dit には、すべてのドメイン・アカウントのユーザー名、ハッシュ化されたパスワード、グループ・メンバーシップが含まれるため、ハッシュをオフラインで解読できる場合には、ドメイン全体の侵害が可能

- 大量のアクセス試行
- 複数の地理的なロケーションからの不可能な移動[7]や同時サインインの事例
- 大量にデータがダウンロード又はエクスポートされた[8]
- 定義されたコンピュータのアクセスや物理的なアクセスログの検証がない、ネットワークへのログイン
- 複数の異なるユーザーとして認証を試みる単一の IP アドレスがあった
- 特に管理者権限のあるアカウントにつき、ユーザーアカウントの作成、又は無効化されたアカウントの再有効化
- あるデバイスが、通常は接続しない他の内部デバイスと通信していることを示すネットフローデータ
- 通常とは異なるスクリプトの実行、ソフトウェアのインストール又は管理ツールの使用
- 予期せぬログの消去
- 通常とは異なる又は不審なパスからのプロセス実行
- Windows Defender 等のセキュリティソフトウェアやログ管理ソフトウェアの設定変更

上記の項目は、悪意のある活動ではなく、正当な行動である可能性があることに注意してほしい。このような場合、実際にサイバーセキュリティイベントの証拠であるかどうかを判断するために、ネットワークセキュリティ担当者によるさらなる調査が必要である。

組織は、ユーザーデバイスなどのエンドポイント上の脅威を検知するため、エンドポイントの検知及び対応ソリューションの実装を検討すべきである。これらのソリューションにより、組織は、悪意のあるアクターによるセキュリティ監視サービスの無効化など、悪意のある活動を監視し、作成イベントをより詳細かつ忠実に処理できるようになる。

本書のガイダンスに従ってイベントログの収集と一元化を改善することで、LOTL の侵害を積極的に調査するための効果的な脅威ハンティングを実施する組織の能力が向上する。組織は、サイバーセキュリティインシデントを検知するための積極的な防御策として、ネットワーク上で脅威ハンティングを行うことを検討すべきである。これは、システム内寄生戦術を用いる悪意あるアクターを検知するために特に効果的な活動である。

また、組織は、潜在的なシステム内寄生戦術の検知の効率を上げるため、次の手法を検討することができる：

- プロセス作成イベントとコマンドラインの監査を含む詳細なログを常に有効にする
  これにより、ログの可視性が向上し、必要に応じて脅威ハンティングが容易になる
- 組織内の正当なバイナリの使用に関するベースラインを確立し、異常な挙動にフラグを立てる
- 異なるオペレーティングシステムに対して進化する脅威の状況に基づいて、特定の SIEM 検知ルールを作成する
  例えば、Microsoft Windows の場合は、powershell.exe、cmd.exe、regedit.exe、Linux の場合は curl、systemctl 及び python でエンコードしたコマンドを使用する

クラウドに関する考慮事項

共同署名文書である「*Identifying and Mitigating Living Off the Land Techniques*」には、クラウド環境向けの詳細な検知ガイダンスが含まれている。その中で、クラウドプロバイダのセキュリティサービスで機械学習による検知機能が利用できる場合、組織は、ログ分析を強化するために、これらの機能を活用し、複数のソースからリアルタイムでログデータを提供することを検討すべきであると述べている。機械学習を利用することで、悪意のある行為

[7] 不可能な移動は、地理的にかなり離れた複数の IP アドレスからユーザーがログインした場合に発生する(つまり、ログインからログインまでの間に、2 つの IP アドレスの地理的な場所の間を移動することが現実的に不可能な場合)

[8] 大量/連続するデータのエクスポートは、デフォルトでアラートが設定されるようにしなければならない

を示す可能性がある異常な挙動を検知することができる。異常な挙動には、標準的ではない API のコールパターン（特に、セキュリティグループ、クラウドリソースの設定、又は機密データへのアクセスの変更を伴うもの）、通常とは異なるクラウドストレージへのアクセス及び非定型的なネットワークトラフィックなどが含まれる。

オペレーショナル・テクノロジーに関する考慮事項

OT 環境での効果的な検知には、通常、IT 担当者と OT 担当者の両者の専門知識が必要である。したがって、効果的なネットワークセキュリティの実装には、両者の共同作業が必要となる。この協力的なアプローチは、ネットワークセキュリティ担当者が関連する問題を迅速に調査し、OT の専門家がサイバーインシデントに関連する可能性のある運用上の懸念を提起できるようにするのに役立つ。さらに、ネットワークセキュリティ担当者は、リアルタイムのアラートを利用して、OT ネットワーク上に何らかの異常な行為がないかを判断しなければならない。これらのアラートには、安全性データ、可用性データ、ログイン、ログインの失敗[9]、設定の変更、ネットワークのアクセスとトラフィックを含むことができる。組織は、OT 環境のアラートに、別の手法を検討しなければならない場合がある。例えば、OT デバイスが遠隔地又はアクセスが難しい場所にあることがある。

OT 環境で異常な挙動を検知するには、以下を探すこと：

- エンジニアリングツールや設定やツールの予期せぬ使用
- ベンダー又はサードパーティによる、アクセス、メンテナンス方法又は遠隔監視の異常な使用
- オペレーティングシステム、ソフトウェア、ファームウェア、設定又はデータベースの不正な更新又は変更
- コントロールシステムと外部ネットワークとの間の予期せぬ通信、又は通常は通信を行わないコンポーネント間の異常な通信
- 通常のオペレーションに含まれないスクリプトの実行

侵入検知や侵入防止システム（IDS/IPS）は、多くの場合、IT プロトコルのルールを基準に設計されているため、監視やプロセスの分野よりも、OT オペレーションシステムや OT 非武装地帯（DMZ）で有用である場合がある。OT 環境に合わせたものでない限り、又は重要なプロセス制御の外側でない限り、IPS の導入は推奨されない。IPS は、重要な OT デバイスの妨げになるリスクがある。

追加のガイダンス

共同署名文書「Identifying and Mitigating Living off the Land Techniques」

豪州通信情報局サイバーセキュリティセンター（ASD's ACSC）発行文書「Windows Event Logging and Forwarding」

CISA 発行文書「Guidance for Implementing M-21-31: Improving the FederalGovernment's Investigative and Remediation Capabilities」

CISA 発行文書「SCuBA TRA and eVRF Guidance Documents」

NSA 発行文書「Cyber Event Forwarding Guidance」

[9] 成功した認証イベントのすべてが無害なわけではないことに注意する。たとえば、資格情報の盗難や悪意のある内部者など。

NCSC-UK 発行文書「What exactly should we be logging?」

NIST 発行文書「SP 800-92 Rev. 1, Cybersecurity Log Management Planning Guide」

NIST 発行文書「Guide to Operational Technology (OT) Security」

米国ホワイトハウス発行文書「M-21-31」

Malcolm | A powerful, easily deployable network traffic analysis tool suite

MITRE ATT&CK®発行文書「Data Sources」